National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

NISTIR 7100

PDA Forensic Tools:

An Overview and Analysis

Rick Ayers
Wayne Jansen

NISTIR 7100

PDA Forensic Tools:
An Overview and Analysis

Rick Ayers
Wayne Jansen

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20988-8930

August 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report
67 pages (2004)

Abstract

Digital handheld devices, such as Personal Digital Assistants (PDAs), are becoming more affordable and commonplace in the workplace. They provide highly mobile data storage in addition to computational and networking capabilities for managing appointments and contact information, reviewing documents, communicating via electronic mail, and performing other tasks. Individuals can store and process personal and sensitive information independently of a desktop or notebook computer, and optionally synchronize the results at some later time. As digital technology evolves, the capabilities of these devices also continues to improve rapidly, taking advantage of new forms of removable media, faster processors that consume less power, touch screens with higher pixel resolution, and other components designed specifically for mobile devices. When handheld devices are involved in a crime or other incident, forensic examiners require tools that allow the proper retrieval and speedy examination of information present on the device. This report gives an overview of current forensic software, designed for acquisition, analysis, reporting of data discovered on PDAs, and an understanding of their capabilities and limitations.

Purpose and Scope

The purpose of this report is to inform law enforcement, incident response team members, and forensic examiners about the capabilities of present day forensic software tools that have the ability to acquire information from Personal Digital Assistant (PDAs) running the following Operating Systems: Palm OS, Pocket PC, and Linux. An overview of each tool describes the functional range and facilities for acquiring and analyzing evidence contained on PDAs. Generic scenarios were devised to mirror situations that often arise during a forensic examination of PDAs and associated media. The scenarios were used to reveal how selected tools react under various situations. Though generic scenarios were used in analyzing forensic tools, the procedures are not intended to serve as a formal product test or as a comprehensive evaluation. Additionally, no claims are made on the comparative benefits of one tool versus another. The report, instead, offers a broad and probing perspective on the state of the art of present-day forensic tools for PDA devices.

It is important to distinguish this effort from the Computer Forensics Tool Testing (CFTT) project, whose objective is to provide measurable assurance to practitioners, researchers, and other users that the tools used in computer forensics investigations provide accurate results. Accomplishing this goal requires the development of rigorous specifications and test methods for computer forensics tools and the subsequent testing of specific tools against those specifications, which goes far beyond the analysis described in this document. The CFFT is the joint effort of the National Institute of Justice, the National Institute of Standards and Technology (NIST), the Office of Law Enforcement Standards (OLES), the U. S. Department of Defense, Federal Bureau of Investigation (FBI), U.S. Secret Service, the U.S. Immigration and Customs Enforcement (BICE), and other related agencies.[•]

Procedures and techniques presented in this report are a compilation of the authors' opinions and references from existing sources. The publication is not to be used as a step-by-step guide for executing a proper forensic investigation when dealing with new technologies such as PDAs, or construed as legal advice. Its purpose is to inform readers of various technologies and potential ways to approach them from a forensic point of view. Before applying the material in this report, readers are advised to consult with management and legal officials for compliance with laws and regulations (i.e., local, state, federal, and international) that pertain to their situation.

Audience

The primary audience of the PDA Forensic Tool document is law enforcement, incident response team members, and forensic examiners who are responsible for conducting forensic procedures related to digital handheld devices and associated removable media.

[•] For more information on this effort see: **www.cftt.nist.gov**.

Table of Contents

Acknowledgements

The authors, Rick Ayers and Wayne Jansen from NIST, wish to express their thanks to colleagues who reviewed drafts of this document. In particular, their appreciation goes to Murugiah Souppaya, Arnold Johnson and Tim Grance from NIST, Rick Mislan from Ferris State University, Ronald van der Knijff and Coert Klaver from the Netherlands Forensic Institute, Eoghan Casey from Knowledge Solutions LLC, and Rob Griesacker from the DoD Cyber Crime Institute for their comments and technical suggestions to this document. The authors would also like to express thanks to all others who assisted with our internal review process, including Susan Ballou from NIST's Office of Law Enforcement Standards, Al Lewis from the U.S. Secret Service and Summer Undergraduate Research Fellowship (SURF) Program intern Brendan Farrar-Foley.

This report was sponsored by Dr. Bert Coursey of the Department of Homeland Security (DHS). The Department's support and guidance in this effort are greatly appreciated.

Introduction

Computer forensics involves the preservation, identification, extraction, documentation, and analysis of computer data. Computer forensic examiners follow clear, well-defined methodologies and procedures that can be adapted for specific situations. Such methodologies consists of the following steps:

- Prepare a forensic copy (i.e., an identical bit-for-bit physical copy) of the acquired digital media, while preserving the acquired media's integrity.
- Examine the forensic copy to recover information.
- Analyze the recovered information and develop a report documenting the incriminating information uncovered.

As digital devices and technology continue to evolve, forensic tools need to advance in a lockstep fashion. Forensic toolkits are intended to facilitate the work of examiners, allowing them to perform the above-mentioned steps in a timely and structured manner, and improve the quality of the results. This paper discusses available forensic tools, highlighting the facilities offered and associated constraints on use.

Most PDAs follow a similar basic design and offer comparable capabilities. While similar in principle, the various families of PDAs on the marketplace differ in such areas as interaction style, Operating System (OS), and hardware components. This paper focuses on the Pocket PC and the Palm OS platforms, two of the most popular families of devices, with some additional discussion on Linux based PDAs. Together the three families comprise the majority of the pure PDA devices currently available and in use. The remainder of this paper provides an overview of PDAs, memory cards, and forensic toolkits; describes the scenarios used to analyze the toolkits; gives the findings from applying the scenarios; and summarizes the conclusions drawn.

Background

PDAs differ in several important ways compared with personal computers (PCs). For example, PDAs are designed for mobility, hence compact in size and battery powered; they store user data in volatile memory instead of a hard disk; and they hibernate, suspending processes when powered off, to avoid a time-consuming reboot when powered on again. Due to the design and architecture, PDAs require specialized forensic tools and procedures distinct from those tools used for single PC systems and network servers.

Forensic examiners involved with handheld devices require a basic understanding of the characteristics of the different types of PDAs they can encounter. Fortunately, most types of PDAs have comparable features and capabilities. They house a microprocessor, flash read only memory (ROM), random access memory (RAM), a variety of hardware keys and interfaces, and a touch sensitive, liquid crystal display. RAM, which normally contains user data, is kept active by batteries whose failure or exhaustion causes all information to be lost. Compact Flash (CF) and Secure Digital (SD)/MultiMedia slots support memory cards and peripherals, such as wireless communication cards. The latest high-end PDAs are equipped with fast processors and considerable memory capacity, giving the user performance comparable to a desktop machine from only a decade ago. Moreover, PDA capabilities are sometimes combined with those of other devices such as cell phones, global positioning systems (GPS), and cameras to form new types of hybrid devices. Table 1 illustrates the range of hardware components found in present-day pure PDA devices.

Table 1: Hardware Component Range

	Low End	Middle	High End
Performance	16 MHz Motorola Dragonball processor 2 MB non-flash ROM 2-8 MB RAM	206 MHz StrongARM processor 16, 32 MB flash ROM 16, 32, or 64 MB RAM	400 MHz or higher XScale processor 48MB or more flash ROM 128 MB RAM
Display	Grayscale LCD, 16 shades, no backlight 160 x 160 pixels	Color LCD, 65,536 colors, backlit 240 x 320 pixels	Color LCD, 65,536 colors, backlit 640 x 480 pixels or greater
Audio	Built-in alarm speaker	Built-in speaker Stereo headphone jack	Built-in speaker Stereo headphone jack Microphone
Expansion	None	SD/MMC slot or CF card slot (Type I or II)	SD/MMC slot and CF card slot (Type II) Device modules/sleeves
Wireless	Infrared (IR) port	IR port Integrated WiFi or Bluetooth	IR port Integrated WiFi and Bluetooth
Battery	Disposable or Rechargeable	Rechargeable, but not user replaceable	Rechargeable and user replaceable

The two dominant families of PDA devices revolve around two operating systems: Microsoft Pocket PC and Palm OS. Regardless of the PDA family, all devices support a set of basic Personal Information Management (PIM) applications, which include contact, calendar, e-mail, and task management. Most devices also provide the ability to communicate wirelessly, review electronic documents, and surf the web. PIM data residing on a PDA can be synchronized with a desktop computer and automatically reconciled and replicated between the two devices, using synchronization protocols such as Microsoft's Pocket PC ActiveSync protocol and Palm's HotSync protocol. Synchronization protocols can also be used to exchange other kinds of data (e.g., individual text, images, and archive file formats). Information not obtainable directly from the PDA can often be retrieved from a personal computer to which the device has been synchronized. Further information on PDA operating systems can be found in the NIST Special Publication 800-72, Guidelines on PDA Forensics.[1]

[1] Available at: **http://csrc.nist.gov/publications/drafts.html#sp800-72**

Removable Media

Examiners typically encounter various types of removable media in an investigation. The size of the various media designed for handheld devices is noteworthy insofar as it is quite small, about the size of a coin, and easy to overlook. Though small in size, the capacities can be quite large, on the order of gigabytes (GB) of memory. Unlike RAM within a device, removable media is non-volatile storage and requires no battery to retain data. Below is a brief overview of several common storage media in use today that may contain significant information related to an investigation. Fortunately, such media can be treated similarly to a removable disk drive, and imaged and analyzed using conventional forensic tools. All that is needed is an appropriate reader for the memory card in question.

Compact Flash Cards (CF):[2]
Compact Flash memory is a solid-state disk card with a 50-pin connector, consisting of two parallel rows of 25 pins on one edge of the card. Compact Flash cards are designed for PCMCIA-ATA functionality and compatibility, have a 16-bit data bus, and are used more as a hard drive than as RAM. They use flash memory technology, a non-volatile storage solution that retains its information once power is removed from the card. Compact Flash cards are about the size of a matchbook (length-36.4 mm, width-42.8 mm, thickness-3.3 mm for Type I and 5mm for Type II) and consume a minimal amount of power.

Hitachi Microdrives:[3]
The Hitachi Microdrive digital media is a high-capacity, rotating mass storage device that is in a Compact Flash Type II package with a 16-bit data bus. A tiny glass disk serves as the storage media, which is more fragile than solid-state memory and requires energy to spin. Similar in function to the solid-state Flash memory cards, the 4GB Microdrive storage card is preformatted with a FAT32 filesystem. FAT32 is required to allow for storage over 2GB. By moving to FAT32, more storage space can be accessed, but cameras and other devices must support the newer filesystem. Many digital cameras and most PDAs support FAT32.

Multi-Media Cards (MMC):[4]
A Multi-Media Card (MMC) is a solid-state disk card with a 7-pin connector. MMC cards have a 1-bit data bus. As with CF cards, they are designed with flash technology, a non-volatile storage solution that retains information once power is removed from the card. The cards contain no moving parts and provide greater protection of data than conventional magnetic disk drives. Multi-Media Cards are about the size of a postage stamp (length-32 mm, width-24 mm, and thickness-1.4 mm). Reduced Size Multi-Media cards (RS-MMC) also exist. They are approximately one-half the size of the standard MMC card (length-18mm, width-24mm, and thickness-1.4mm). Though they were designed specifically for mobile phones, they can potentially be used with PDAs. An RS-MMC can be used in a full size MMC slot with a mechanical adapter. A regular MMC card can be also used in RS-MMC card slot, though part of it will stick out from the slot.

---

[2] Image courtesy of Micron.
[3] Photograph © 2004 Hitachi Global Storage Technologies. Used by Permission.
[4] Image courtesy of Micron.

Secure Digital (SD) Cards:[5]
Secure Digital (SD) memory cards (length-32 mm, width-24 mm, and thickness-2.1mm) are comparable to the size and solid-state design of MMC cards. In fact, SD card slots often can accommodate MMC cards as well. However, SD cards have a 9-pin connector and a 4-bit data bus, which afford a higher transfer rate. SD memory cards feature an erasure-prevention switch. Keeping the switch in the locked position protects data from accidental deletion. They also offer security controls for content protection (i.e., Content Protection Rights Management). MiniSD cards are an electrically compatible extension of the existing SD card standard in a more compact format (length-21.5 mm, width-20 mm, and thickness-1.4 mm). They run on the same hardware bus and use the same interface as an SD card, and also include content protection security features, but have a smaller maximum capacity potential due to size limitations. For backward compatibility, an adapter allows a MiniSD Card to work with existing SD card slots.

Memory Sticks:[6]
Memory sticks provide solid-state memory in a size similar to, but smaller than, a stick of gum (length-50mm, width-21.45mm, thickness-2.8mm). They have a 10-pin connector and a 1-bit data bus. As with SD cards, memory sticks also have a built-in erasure-prevention switch, to protect the contents of the card. Recently introduced, Memory Stick PRO cards offer higher capacity and transfer rates than standard memory sticks. Memory Stick Duo is another, more recent development that is about two-thirds the size of the standard memory stick (length-31mm, width-20mm, thickness-1.6mm). An adapter is required for a Memory Stick Duo to work with standard memory stick slots.

[5] Image courtesy of Lexar Media. Used by permission.
[6] Image courtesy of Lexar Media. Used by permission.

PDA Forensic Toolkits

Unlike the situation with personal computers, the number and variety of toolkits for PDAs and other handheld devices is considerably limited. Not only are there fewer specialized tools and toolkits, but also the range of devices over which they operate is typically narrowed to only the most popular families of PDA devices – those based on the Pocket PC and Palm OS. Moreover, the tools require that the examiner have full access to the device (i.e. the device is not protected by some authentication mechanism or the examiner can satisfy any authentication mechanism encountered). While a couple of toolkits support a full range of acquisition, examination, and reporting functions, the remaining tools focus mainly on a single function. Table 2 lists open-source and commercially available tools and the facilities they provide for each PDA family. The abbreviation NA means that the tool at the left of the row is not applicable to the device at top of the column.

Table 2: PDA Forensic Tools

	Palm OS	Pocket PC	Linux
PDA Seizure	Acquisition, Examination, Reporting	Acquisition, Examination, Reporting	NA
EnCase	Acquisition, Examination, Reporting	NA	Examination, Reporting
pdd	Acquisition	NA	NA
pilot-link	Acquisition	NA	NA
POSE	Examination, Reporting	NA	NA
dd	NA	NA	Acquisition

Forensic tools acquire data from a device in one of two ways: physical acquisition or logical acquisition. Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a disk drive or RAM chip), while logical acquisition implies a bit-by-bit copy of logical storage objects (e.g. directories and files) that reside on a logical store (e.g., involving several disk drives). The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e., a logical view), versus memory as seen by the processor and other related hardware components (i.e., a physical view). In general, physical acquisition is preferable, since it allows any data remnants present (e.g., unallocated RAM or unused filesystem space) to be examined, which otherwise would go unaccounted in a logical acquisition. Physical device images are generally more easily imported into another tool for examination and reporting. However, a logical acquisition provides a more natural and understandable organization of the information acquired. Thus, it is preferable to do both types of acquisition, if possible.

PDA Seizure

Paraben's PDA Seizure version 2.5.0.0[7] is a forensic software toolkit that allows forensic examiners to acquire and examine information on PDAs for both the Pocket PC (PPC) and Palm OS (POS) platforms. Paraben's product currently supports Palm OS up to version 5, Pocket PC 2000-2003 (up to Windows CE 4.2), ActiveSync 3.5, and HotSync. PDA Seizure's features include the ability to produce a forensic image of Palm and Pocket PC devices, to perform

[7] Additional information on Paraben products can be found at: **http://www.paraben-forensics.com/pda.html**

examiner-defined searches on data contained within acquired files, and to generate a report of the findings. PDA Seizure also provides book-marking capabilities to organize information, along with a graphics library that automatically assembles found images under a single facility, based on the graphics file extension of acquired files.

During the acquisition stage of a PPC device, the connectivity of the device and ActiveSync is required. A guest account must be used to create a connection and avoid synchronization between the device and the PC. For Palm devices, the PDA must first be put into a debug mode, commonly referred to as console mode,[8] and all active HotSync applications must be closed. Once the memory image of a Palm OS device is acquired, the user will be prompted to select the HotSync button on the device to acquire the logical data separately. The logical data is also represented in the RAM file that was acquired through the physical acquisition stage. Palm's HotSync protocol is used to gain communication with the device to do a logical acquisition.

EnCase

EnCase version 4.15[9] is a well-known forensic software toolkit that provides acquisition of suspect media, search and analytical tools, and data capture and documentation features. Although more widely used for examining PCs, EnCase does also support Palm OS devices. Currently, there is no support for Pocket PC. EnCase allows for the creation of a complete physical bit-stream image of a source device. Throughout the process, the bit-stream image is continually verified by CRC (Cyclical Redundancy Checksum) blocks, which are calculated concurrent to acquisition. The resulting bit-stream image, called an EnCase evidence file, is mounted as a read-only file or "virtual drive" from which EnCase proceeds to reconstruct the file structure utilizing the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the device without affecting the integrity of the original data.

EnCase allows for files, folders, or sections of a file to be highlighted and saved for later reference. These marks are called bookmarks. All bookmarks are saved in case files, with each case having its own bookmark file. Bookmarks can be viewed at any time and can be made from anywhere data or folders exist. Reporting features allows examiners to view information from a number of perspectives: all acquired files, single files, results of a string search, a report, or the entire case file created.

Palm dd (pdd)

`pdd`[11] is a Windows-based tool developed by @stake[10] that performs a physical acquisition of information from Palm OS devices. `pdd` is designed to work with the majority of PDAs running on the Motorola DragonBall processor. Communications are established by putting the Palm device into console mode. During the acquisition stage, a bit-for-bit image of the device's memory can be obtained. The data retrieved by `pdd` includes all user applications and databases. `pdd` is strictly a command line driven application without features such as graphics libraries, report generation, search facilities, and bookmarking capabilities. Once the information has been acquired, two files are generated: pdd.txt, which generates device specific information, and the

[8] Additional information on console mode can be found at: **http://www.ee.ryerson.ca/~elf/visor/dot-shortcuts.html**
[9] Additional information on Guidance software products can be found at: **http://www.guidancesoftware.com/**
[11] Additional information on pdd and Palm devices can be found at: **http://lists.jammed.com/forensics/2001/11/0014.html**
[10] Additional information on @stake can be found at: **http://www.atstake.com/research/tools/forensic/**

user-redirected file containing a bit-by-bit image of the device. Examiners face the challenge of carefully examining the output, which is in binary form, some of which happens to be ASCII characters. Files created from `pdd` can be imported into a forensic tool, such as EnCase, to aid analysis; otherwise the default tool is a hex editor. As of January 2003 `pdd` will no longer be updated or supported, however, version 1.11 source code is available and should remain available for use, as defined in its included license. Paraben has integrated the `pdd` engine into the PDA Seizure software.

Pilot-Link

pilot-link[12] is an open source software suite originally developed for the Linux community to allow information to be transferred between Linux hosts and Palm OS devices. It runs on a number of desktop operating systems besides Linux, including Windows and Mac OS. About thirty command line programs comprise the software suite. Unlike pdd, which uses the Palm debugger protocol for acquisition, pilot-link uses the Hotsync protocol. The two programs of interest to forensic examiners are pi-getram and pi-getrom, which respectively retrieve the contents of RAM and ROM from a device, similar to the physical acquisition done by pdd. Another useful program is pilot-xfer, which allows the installation of programs and the backup and restoration of databases. pilot-xfer provides a means to logically acquire the contents of a device. The contents retrieved with these utilities can be manually examined with either the Palm OS Emulator (POSE), a compatible forensics tool such as EnCase, or a hex editor. pilot-link does not provide hash values of the information acquired. A separate step must be carried out to obtain needed hash values.

POSE

POSE[13] is a software program that runs on a desktop computer under a variety of operating systems, and behaves exactly as a Palm OS hardware device, once an appropriate ROM image is loaded into it. The emulator program imitates the hardware of a DragonBall processor. Built-in PIM applications (e.g., calendar, contact, e-mail, task management, etc.) run properly and the hardware buttons and display react accurately. ROM images can be obtained from the PalmSource Web site or by copying the contents of ROM from an actual device, using pdd, pilot-link, or a companion tool provided with the emulator.

Loading actual RAM-based databases (e.g., extracted using pilot-link) into the emulator allows an examiner to view and operate the emulated device in a similar fashion as having the original. Though originally developed to run, test, and debug Palm OS applications without having to download them to an actual device, POSE also serves as a useful tool for doing presentations or capturing screen shots of evidence found on the emulated device from within the databases loaded from a seized device. POSE can be configured to map the Palm OS serial port to one of the available serial ports on the desktop computer or to redirect any TCP/IP calls to the TCP/IP stack on the desktop. With some experimentation, the HotSync protocol can even be run between the desktop computer and the virtual device being emulated, over a looped back serial connection or a redirected TCP/IP connection.

[12] Additional information on pilot-link can be found at: **http://www.pilot-link.org**
[13] Additional information on POSE can be found at: **http://www.palmos.com/dev/tools/emulator/**

Duplicate Disk (dd)

The duplicate disk (`dd`) utility is similar to `pdd` insofar as it allows examiners to create a bit-by-bit image of the device. However, `dd` is different from the other tools described above, insofar as it executes directly on the PDA and must be invoked via a remote connection or command line input. As one of the original Unix utilities, dd has been around in one form or another for decades. Unlike the other tools described above, dd executes directly on the PDA. An image of the device can be obtained by connecting to the PDA, issuing the `dd` command, and dumping the contents elsewhere, for example, to auxiliary media such as a memory card or across a network session to a forensic workstation. If used incorrectly, `dd` may destroy or overwrite parts of the filesystem. As with `pdd`, `dd` produces binary data output, some of which contains ASCII information. Images outputted from `dd` may be imported for examination into a forensic tool, such as EnCase, if the filesystem is supported. A `dd` created image may also be mounted in loop-back mode on a filesystem-compatible Linux machine for logical file analysis.

Miscellaneous Tools

Other tools available from a hardware or software manufacturer to backup data or develop software for a device or device family may aid an investigation. For example, Microsoft has developed a tool called ActiveSync Remote Display (`ASRDisp`) that allows ActiveSync to connect to a Pocket PC device and display its full functionality in a virtual device window on the desktop, as if performing actions on the physical device itself. After the target device data has been acquired, a full backup via ActiveSync could be created and the backup restored on an identical device for presentation purposes. The `ASRDisp` utility is part of the Windows Mobile Developer Power Toys suite.[14]

Another means of presenting data is to use a Pocket PC emulator and the shared folder functionality available. Again, after device acquisition has taken place, examiners can export out individual files gleaned from the device to a specific folder present on the forensic workstation. The shared folder allows information to be imported into the emulator and presents all data in the Storage Card folder on the Pocket PC Emulator.[15] This allows examiners to present relevant information virtually. Emulators for all versions of the Pocket PC OS can be downloaded at the Microsoft site.

[14] The Windows Mobile Developer Power Toys suite can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyId=74473FD6-1DCC-47AA-AB28-6A2B006EDFE9&displaylang=en
[15] The Pocket PC 2003 Emulator can be downloaded at: **http://www.microsoft.com/downloads/details.aspx?FamilyID=5c53e3b5-f2a2-47d7-a41d-825fd68ebb6c&displaylang=en**

Synopsis of PDA Seizure

PDA Seizure has the ability to acquire information from either Pocket PC or Palm OS Platforms. Regardless of the type of PDA, the proper investigative steps must be followed for each device. PDA Seizure allows the examiner to connect a device via a USB or a Serial connection. Examiners must have the correct cables and cradles to ensure connectivity, compatible synchronization software, and a backup battery source available. Synchronization software allows examiners to create a guest partnership between a PC/notebook and the device/PDA being investigated (e.g., Microsoft ActiveSync/Palm HotSync software).

Pocket PC

The acquisition of a Windows CE device is done through PDA Seizure with the aid of Microsoft's ActiveSync communication protocol. During the ActiveSync connection an examiner creates a connection as a "Guest" to the device. The "Guest" account is essential for disallowing any synchronization between the PC and the device before acquisition. Before the acquisition of information begins, PDA Seizure places a 4K program file "`CESeizure.dll`" on the device in the first available block of memory, which is then removed at the end of acquisition. Paraben indicated that PDA Seizure uses the `dll` to access unallocated regions of memory on the device.

To access the remaining information, PDA Seizure utilizes Remote API (RAPI)[16], which provides a set of functions for desktop applications to communicate with and access information on Windows CE platforms. These functions are accessible once a Windows CE device is connected through ActiveSync. RAPI functions are available for the following:

- Device system information – includes version, memory (total, used, and available), and power status
- File and directory management – allows retrieval of path information, find specific files, permissions, time of creation, etc.
- Property database access – allows information to be gleaned from database information present on the device
- Registry manipulation – allows the registry to be queried (i.e., keys and associated value)

Palm OS

The acquisition of information on a Palm OS device entails the forensic examiner exiting all active HotSync applications and placing the device in console mode. Console mode is used for physical acquisition of the device. In order to put the Palm device in console mode, the examiner must go to the search window (press the magnifying glass by the Graffiti writing area), enter via the Graffiti interface the following symbols: lower-case cursive L, followed by two dots (results in a period), followed by writing a 2 in the number area. For acquiring data from a Handspring Visor device, the keystroke used is slightly different. Instead of the above command, the shortcut used is a lower-case cursive L followed by a dot, and then writing a 2 while depressing the up button. This keystroke sequence works for most Handspring devices. Console mode is device specific and the correct sequence of graffiti characters can be found at the manufacturer's web site. All items on a Palm PDA are stored in a database of some type.

[16] Additional information on RAPI can be found at: **http://www.cegadgets.com/artcerapi.htm**

These databases or files are copied to a PC/notebook and itemized on the screen during the acquisition process. The Palm File Format (PFF) conforms to one of the three types defined below:

- **Palm Database (PDB) –** A record database used to store application or user specific data.
- **Palm Resource (PRC)** – A resource database similar to the PDB. The applications running on Palm OS are resources containing code and user interface resource elements.
- **Palm Query Application (PQA) –** A Palm database containing world-wide-web content for use with Palm OS wireless devices.[17]

During the installation procedure of PDA Seizure, the Palm OS Emulator (POSE)[18] is also installed on the PC/notebook. POSE is used to view data associated with the Palm device within a desktop environment. The acquired data appears exactly as it would on the device with the use of a virtual PDA. The use of POSE allows one to view data that are not supported by PDA Seizures' internal viewers. The following steps outline the actions to be taken to use POSE with PDA Seizure.

- Install POSE – This is done during the installation of PDA Seizure
- Acquire evidence from device
- From the PDA Seizure Menu Bar select: Tools -> Export All Files
- Exporting All files creates two subfolders: Card0-RAM and Card0-ROM
  - Instead of downloading a compatible ROM images examiners should use the ROM acquired, due to the possibility of ROM upgrades.
- Start POSE: Tools -> Palm Emulator
  - Select New -> Star a new emulator session

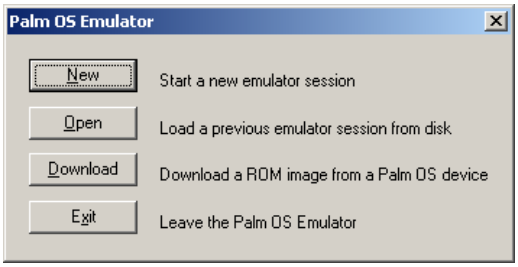


Figure 1: Pose - Start Emulator

  - Select the ROM file -> Other -> Select the ROM image that was saved to the Card0-ROM folder

[17] PQA is expected to be discontinued soon; information about the status of PQA can be found at: **http://kb.palmone.com/SRVS/CGI-BIN/WEBCGI.EXE?New,Kb=PalmSupportKB,ts=Palm_External2001,case=obj(10646**
[18] Additional information on POSE can be found at: **http://www.palmos.com/dev/tools/emulator/**

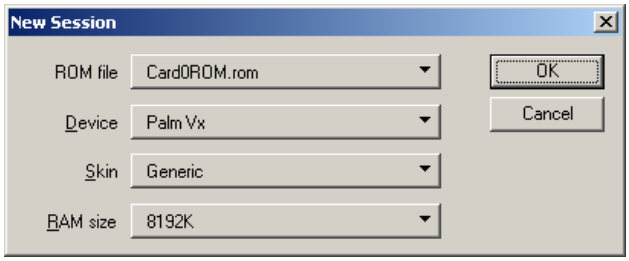


Figure 2: POSE - Select ROM/Device

Once the ROM file is selected the POSE session will begin. To view specific files in the POSE session, simply drag and drop individual files of type: PRC, PDB, PQA, and PSF files onto POSE emulator screen from the exported folders. The screen shot below is an example of what POSE looks like after importing the ROM/RAM of the acquired device. POSE is useful for providing virtual demonstrations and capturing screen shots of relevant information as shown in Figure 3 below.

Figure 3: POSE Emulator

POSE is not a proprietary application associated with PDA Seizure and can be downloaded separately and used with other forensic applications that have the ability to acquire a ROM image and associated database files.

Acquisition Stage

There are two methods to begin the acquisition of data from the PDA device. The acquisition can be enacted through the toolbar using the Acquire icon or through the Tools menu and selecting Acquire Image. Either option starts the acquisition process. With the acquisition process, both files and memory images can be acquired. By default, the tool marks both types of data to be acquired. Once the acquisition process is selected, the acquisition wizard illustrated below in Figure 4 appears to guide the examiner through the process.

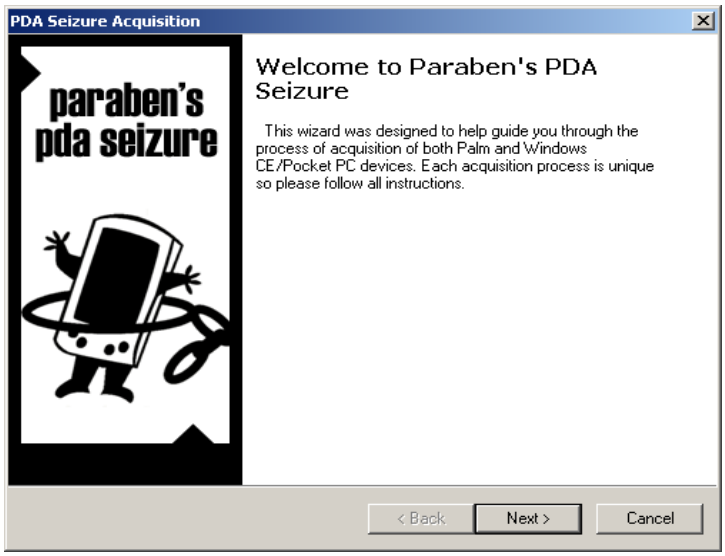
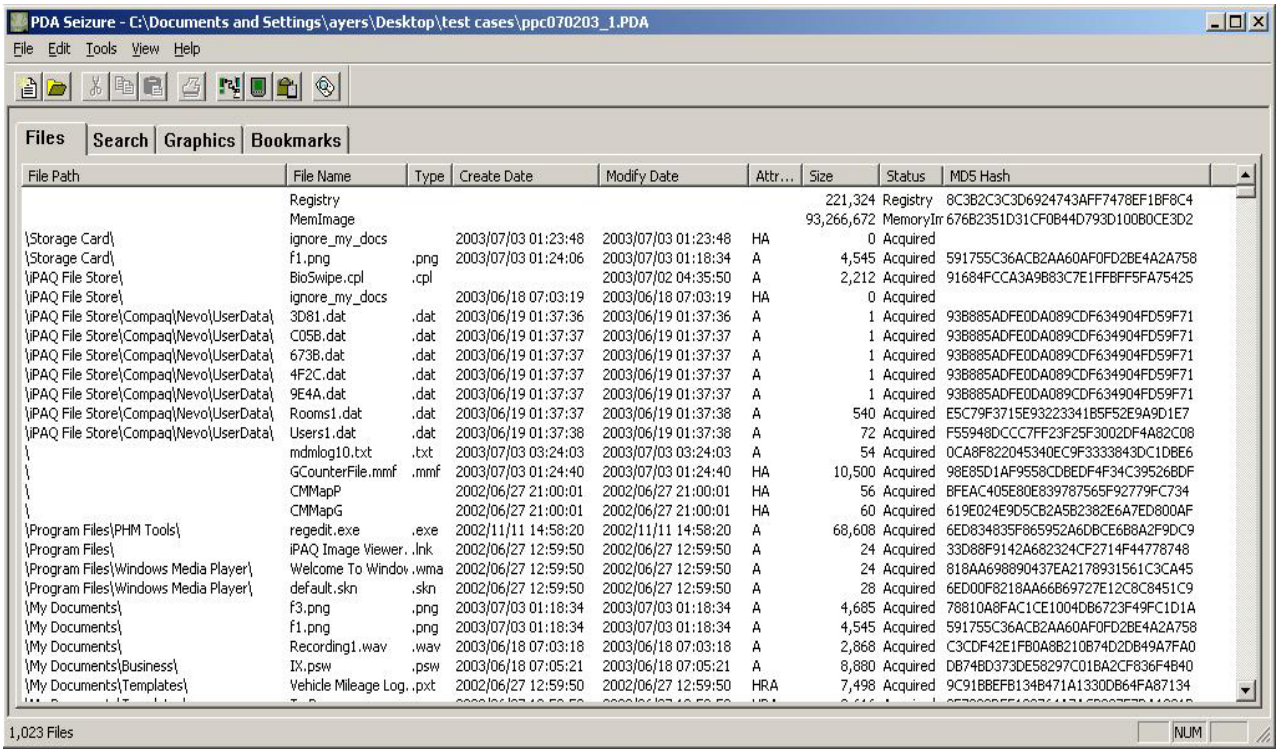


Figure 4: Acquisition Wizard

Figure 5 below contains an example screen shot of PDA Seizure during the acquisition of a Pocket PC (PPC) device, displaying the various fields provided by the interface.



File Path	File Name	Type	Create Date	Modify Date	Attr...	Size	Status	MD5 Hash
	Registry					221,324	Registry	8C3B2C3C3D6924743AFF7478EF1BF8C4
	MemImage					93,266,672	MemoryIm	676B2351D31CF0B44D793D100B0CE3D2
\Storage Card\	ignore_my_docs		2003/07/03 01:23:48	2003/07/03 01:23:48	HA	0	Acquired	
\Storage Card\	f1.png	.png	2003/07/03 01:24:06	2003/07/03 01:18:34	A	4,545	Acquired	591755C36ACB2AA60AF0FD2BE4A2A758
\iPAQ File Store\	BioSwipe.cpl	.cpl		2003/07/02 04:35:50	A	2,212	Acquired	91684FCCA3A9B83C7E1FFBFF5FA75425
\iPAQ File Store\	ignore_my_docs		2003/06/18 07:03:19	2003/06/18 07:03:19	HA	0	Acquired	
\iPAQ File Store\Compaq\Nevo\UserData\	3D81.dat	.dat	2003/06/19 01:37:36	2003/06/19 01:37:36	A	1	Acquired	93B885ADFE0DA089CDF634904FD59F71
\iPAQ File Store\Compaq\Nevo\UserData\	C05B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFE0DA089CDF634904FD59F71
\iPAQ File Store\Compaq\Nevo\UserData\	673B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFE0DA089CDF634904FD59F71
\iPAQ File Store\Compaq\Nevo\UserData\	4F2C.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFE0DA089CDF634904FD59F71
\iPAQ File Store\Compaq\Nevo\UserData\	9E4A.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFE0DA089CDF634904FD59F71
\iPAQ File Store\Compaq\Nevo\UserData\	Rooms1.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:38	A	540	Acquired	E5C79F3715E93223341B5F52E9A9D1E7
\iPAQ File Store\Compaq\Nevo\UserData\	Users1.dat	.dat	2003/06/19 01:37:38	2003/06/19 01:37:38	A	72	Acquired	F55948DCCC7FF23F25F3002DF4A82C08
\	mdmlog10.txt	.txt	2003/07/03 03:24:03	2003/07/03 03:24:03	A	54	Acquired	0CA8F822045340EC9F3333843DC1DBE6
\	GCounterFile.mmf	.mmf	2003/07/03 01:24:40	2003/07/03 01:24:40	HA	10,500	Acquired	98E85D1AF9558CDBEDF4F34C39526BDF
\	CMMapP		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	56	Acquired	BFEAC405E80E839787565F92779FC734
\	CMMapG		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	60	Acquired	619E024E9D5CB2A5B2382E6A7ED800AF
\Program Files\PHM Tools\	regedit.exe	.exe	2002/11/11 14:58:20	2002/11/11 14:58:20	A	68,608	Acquired	6ED834835F865952A6DBCE6B8A2F9DC9
\Program Files\	iPAQ Image Viewer..	.lnk	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	33D88F9142A682324CF2714F44778748
\Program Files\Windows Media Player\	Welcome To Windo	.wma	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	818AA698890437EA2178931561C3CA45
\Program Files\Windows Media Player\	default.skn	.skn	2002/06/27 12:59:50	2002/06/27 12:59:50	A	28	Acquired	6ED00F8218AA66B69727E12C8C8451C9
\My Documents\	f3.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,685	Acquired	78810A8FAC1CE1004DB6723F49FC1D1A
\My Documents\	f1.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,545	Acquired	591755C36ACB2AA60AF0FD2BE4A2A758
\My Documents\	Recording1.wav	.wav	2003/06/18 07:03:18	2003/06/18 07:03:18	A	2,868	Acquired	C3CDF42E1FB0A8B210B74D2DB49A7FA0
\My Documents\Business\	IX.psw	.psw	2003/06/18 07:05:21	2003/06/18 07:05:21	A	8,880	Acquired	DB74BD373DE58297C01BA2CF836F4B40
\My Documents\Templates\	Vehicle Mileage Log..	.pxt	2002/06/27 12:59:50	2002/06/27 12:59:50	HRA	7,498	Acquired	9C91BBEFB134B471A1330DB64FA87134

Figure 5: Acquisition Screen Shot (PPC)

After PPC acquisition, PDA Seizure reports the following for each individual files: File Path, File Name, File Type, Creation and Modification Dates, File Attributes, File Size, Status, and an MD5 File Hash. Validation of file hashes taken before and after acquisition can be used to determine whether files have been modified during the acquisition stage.

During the acquisition process, `CESeizure.dll` is executed to acquire unallocated memory regions. The examiner is prompted with check boxes to select one or all of the following before acquiring information on the PPC device: Acquire Files, Acquire Databases, Acquire Registry, and/or Acquire Memory. Each file acquired can be viewed in either text or hex mode, allowing examiners to inspect the contents of all files present. In order to view the files, examiners must use one of the following options: export the file, launch a windows application based upon the file extension (Run File's Application); or, for Palm devices, view the file thru the POSE.

Search Functionality

PDA Seizure's search facility allows examiners to query files for content. The search function searches the content of files and reports all instances of a given string found. The screenshot shown below in Figure 6 illustrates an example of the results produced for the string "`Bioswipe.cpl`". Neither wildcard characters, such as an asterisk, appear to be supported, nor do facilities for examining a subset of the files by directory, file type, or file name.

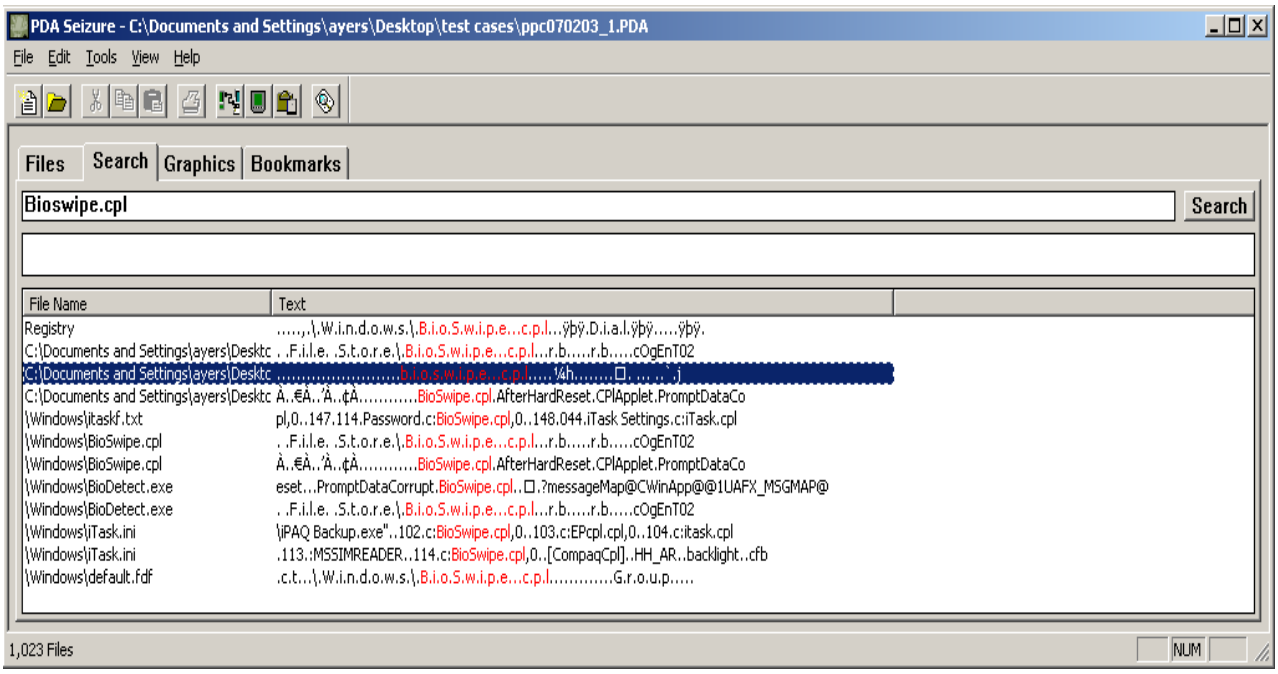


Figure 6: File Content String Search (PPC)

Additionally the search window provides an output of memory related to the string search provided by the examiner. This allows examiners to scroll through sections of memory and bookmark valuable information for reporting to be used in judicial, disciplinary, or other proceedings. Figure 7 illustrates an excerpt of a string search done on the name "Doe" and the contents shown from the memory window.

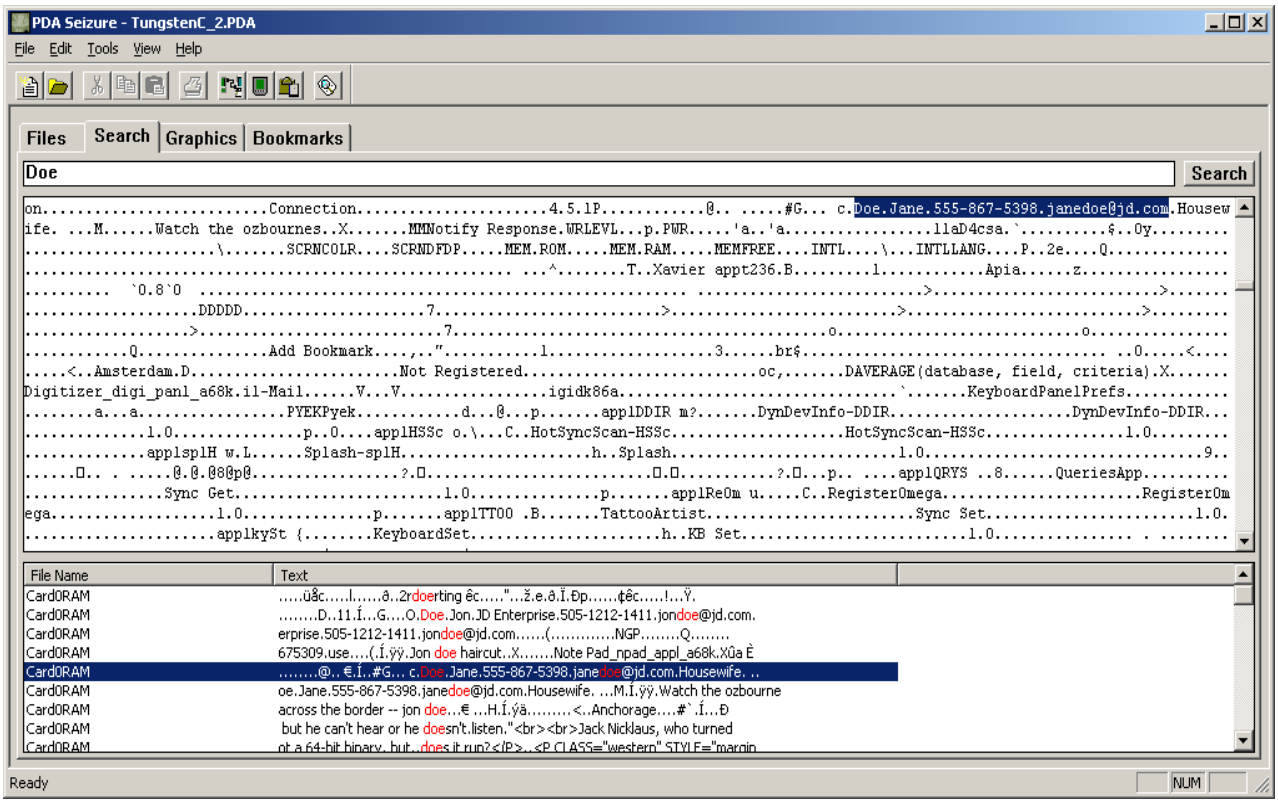


Figure 7: Memory Content String Search (PPC)

Graphics Library

The graphics library enables examiners to examine the collection of graphics files present on the device, identified by file extension. Deleted graphics files do not appear in the library. A significant improvement to the graphics library would be to identify and include graphics files, based upon file signature (i.e., known file header and footer values) versus file extension. Manually performing file signature identification is very time consuming and may cause key data to be omitted. If deleted graphics files exist, they must be identified via the memory window by performing a string search to identify file remnants. However, recovery of the entire image is difficult, since its contents may be compressed by the filesystem or may not reside in contiguous memory locations, and some parts may be unrecoverable. It also requires knowledge of associated data structures to piece the parts together successfully. Figure 8 shows a screen shot of images acquired from a Pocket PC 2002 device.

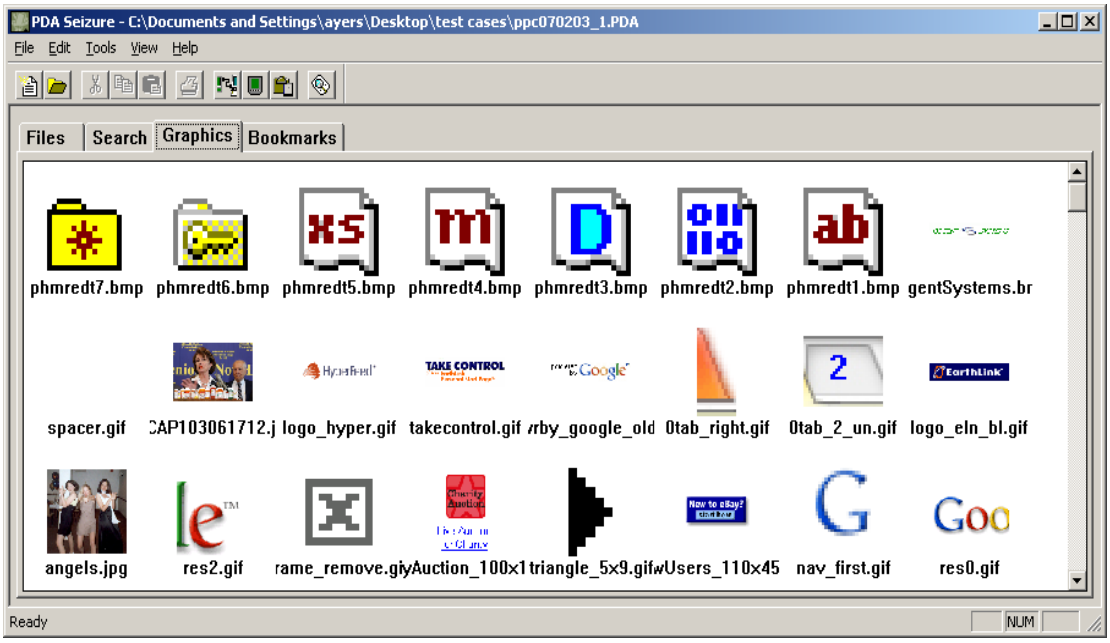


Figure 8: Graphics Library (PPC)

Bookmarking

During an investigation, forensic examiners often have an idea of the type of information for which they are looking, based upon the circumstances of the incident and information already obtained. Bookmarking allows forensic examiners to mark items that are found to be relevant to the investigation. Such a capability gives the examiner the means to generate case specific reports containing significant information found during the examination, in a format suitable for presentation. Bookmarks can be added for multiple pieces of information found and each individual file can be exported for further analysis if necessary. Illustrated in Figure 9 below is an example of the creation of a bookmark on a graphics file found on the storage card. As mentioned earlier, the files found and bookmarked can be exported to the PC and viewed with an application suitable for the type of file in question.

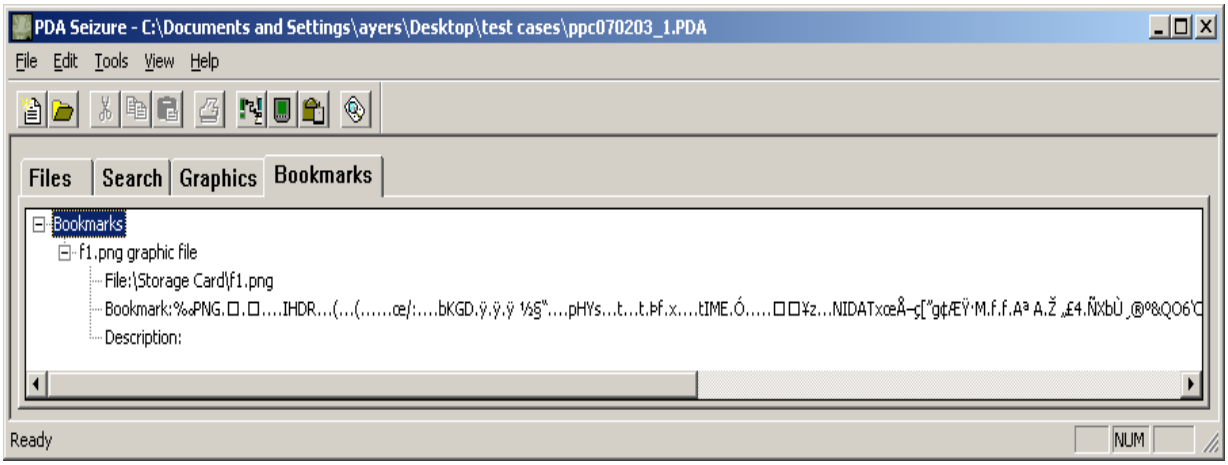


Figure 9: Bookmark Creation (PPC)

Additional Tools

Export All Files: Examiners have the ability to export all files reported after the acquisition stage has been completed. After the files have been exported, a folder is created, based upon the case file name, with two subfolders: one each for RAM and ROM. Depending upon the type of file, the contents can be viewed with an associated desktop application or with a device specific emulator.

PDA File Compare: PDA Seizure has a built-in function that compares acquisition files. To operate the compare feature, one file is loaded into the program then compared via the Tools menu option to another file. The files are compared based on hash codes. The results are shown in a dialog box listing the file name, the result of the compare, and the size in each `.pda` file. Double-clicking a file, or highlighting a file and clicking the "Show Files" button, pops-up a side-by-side hex view of the two files with the differences shown in red. PDA File Compare is illustrated below in Figure 10.

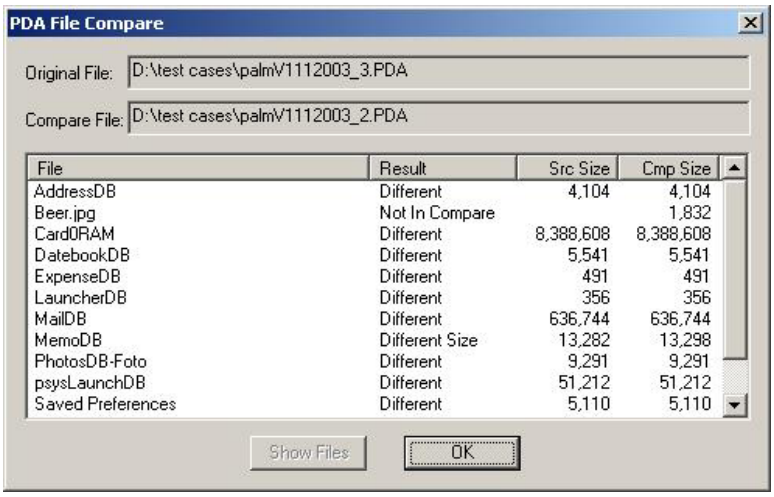


Figure 10: PDA File Compare (Palm OS)

PDA Seizure File View: Below, illustrated in Figure 11, is an example of PDA Seizure's File Viewer. Files that have not been deleted have the option to be viewed in either text or hex, or with the "Run File's Application" function, which calls an associated application to display the data on the examiner's local machine. The latter allows graphics and other file types that are not in a standard flat ASCII file format to be viewed.

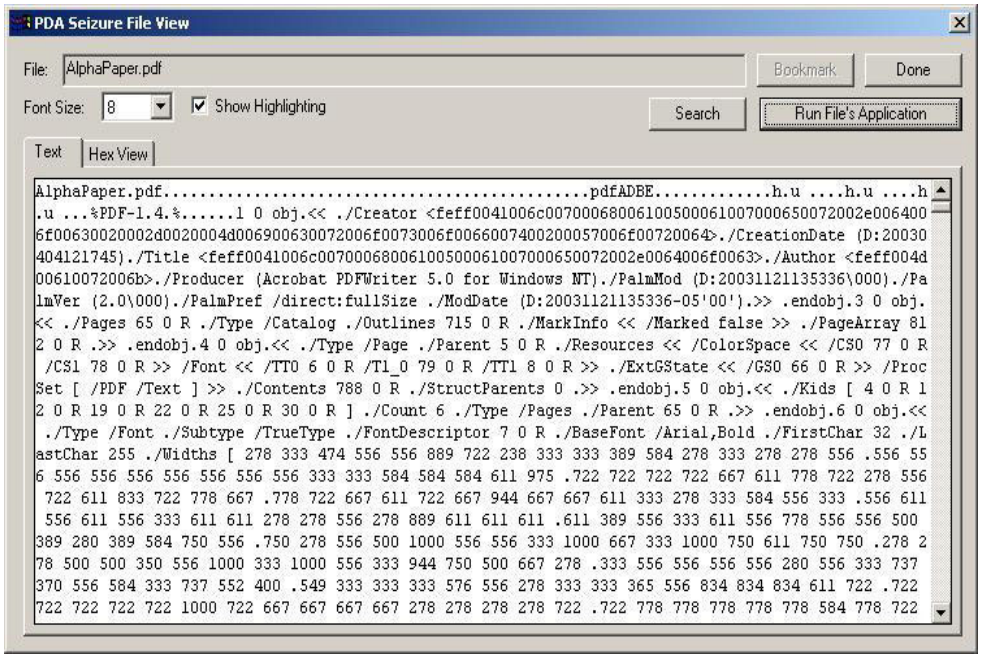


Figure 11: File View (Palm OS)

Report Generation

Reporting is an essential task for examiners. PDA Seizure provides a user interface for report generation that allows examiners to enter and organize case specific information. Each case contains an identification number and other information specific to the investigation for reporting purposes, as illustrated in Figure 12 below.

Once the report has been generated, it produces a `.html` file for the examiner, including files that were book-marked, total files acquired, acquisition time, device information, etc. If files were modified during the acquisition stage, the report identifies them.

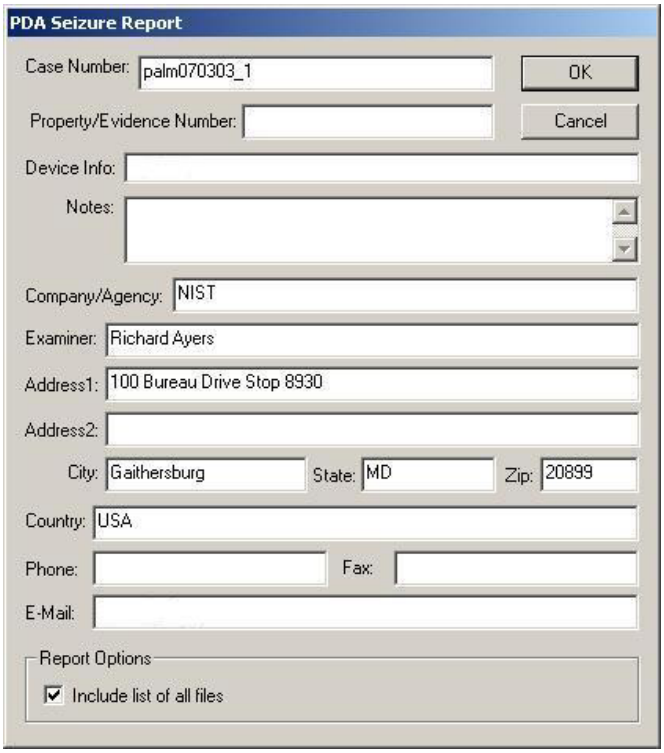


Figure 12: Report Generation

Password Cracking

PDA Seizure has the ability to crack passwords for the Palm OS prior to version 4.0. Due to a weak, reversible password-encoding scheme, it is possible to obtain an encoded form of the password, determine the actual password, and access a users private data. Password cracking for Windows CE is not supported. Screenshots illustrated below outline the process of obtaining the password of a locked device. The first step is to select Decode Password.

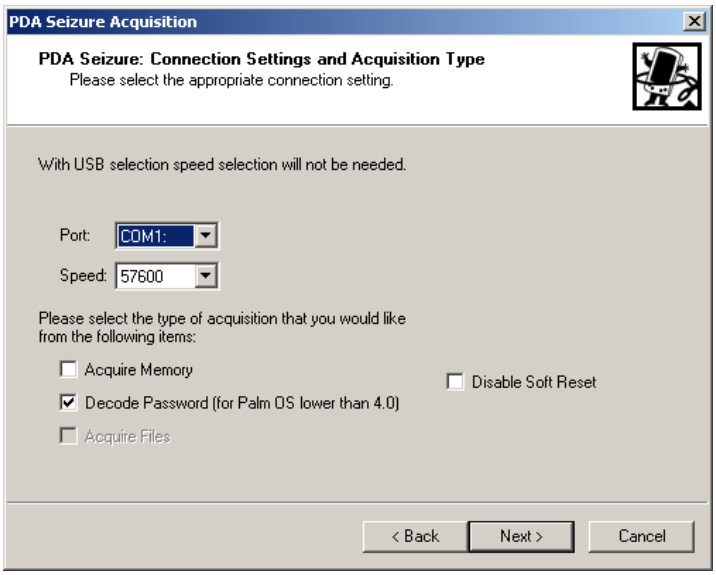


Figure 13: Password Crack Step 1 (Palm OS)

Once the examiner has selected Decode Password, the next step is to put the device into console mode. After the device is in console mode, the password shows up on the screen as illustrated below in Figure 14, allowing examiners the ability to unlock the device and begin normal acquisition of information.

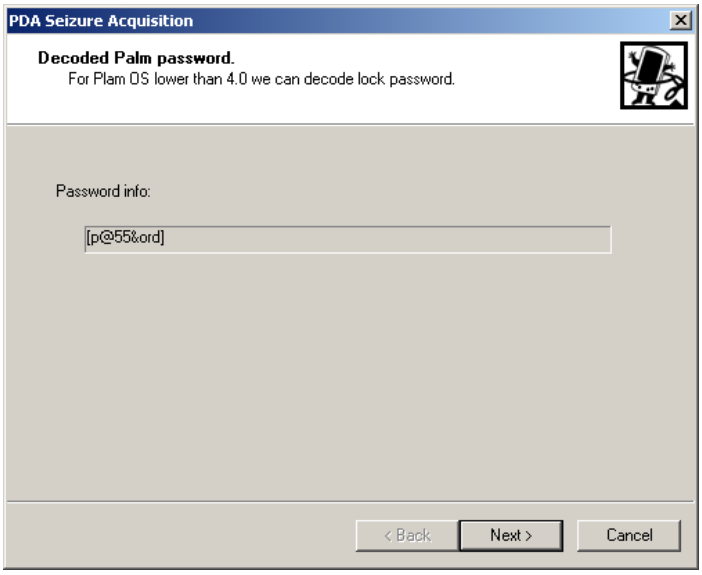


Figure 14: Password Crack Step 2 (Palm OS)

Synopsis of EnCase

EnCase has the ability to acquire information from PDA devices from the Palm OS family. In order to start the acquisition process, the Palm device must be put into console mode, using the same steps applied as stated earlier for PDA Seizure. Console mode is achieved by pressing the search icon, then entering the following using the Graffiti interface: a lower-case cursive L, followed by two dots and finally the number 2. Console mode is device specific and the correct sequence of graffiti characters can be found at the manufacturer's web site. Forensic examiners must exit all active HotSync applications before acquiring information. After the device has been successfully imaged, the examiner leaves console mode by resetting the device. Resetting the device is extremely important to preserve battery life, since the power consumption rate is significantly higher in console mode than in normal mode.

Acquisition Stage

The Acquisition Stage allows forensic examiners to acquire data from Palm handheld devices. The examiner begins by creating a case on the PC. Once the case has been created, the next step is to add the device. During this step, communications from the PC to the PDA is checked to determine proper connectivity and the device must be put into console mode. Once the device has been successfully added, the examiner should see a screen similar to the one illustrated below in Figure 15.

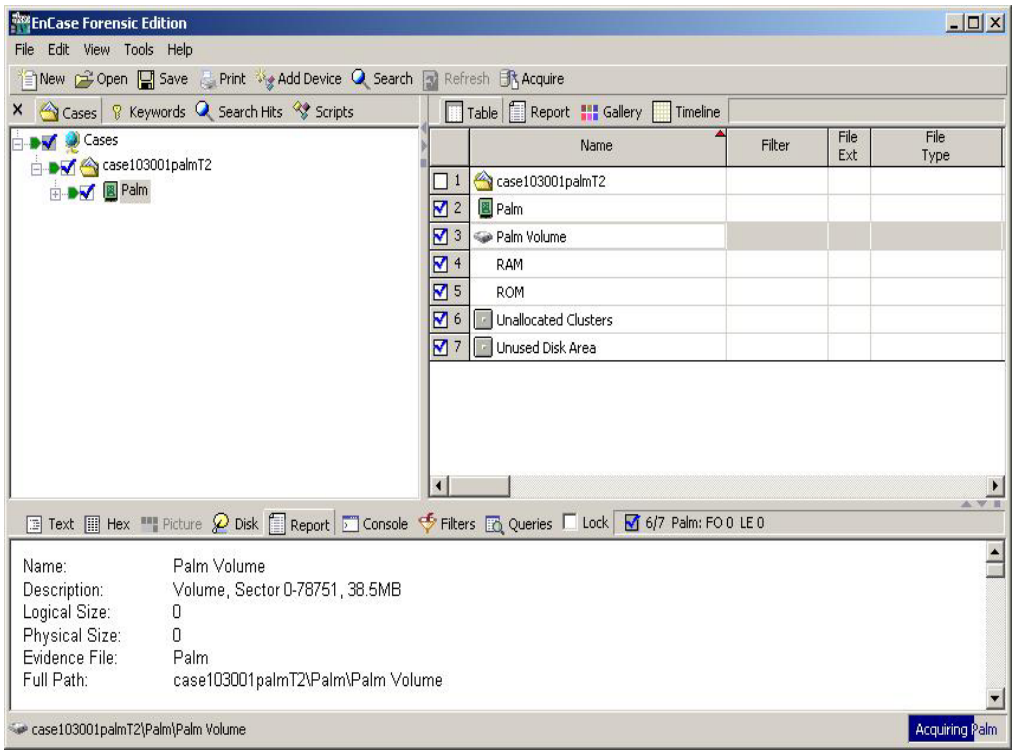


Figure 15: Acquisition Stage

The next step is to acquire information from the handheld device by clicking the "Acquire" button.

Search Functionality

EnCase houses a bank of examiner specified keywords that enable the examiner to search for all strings relative to the case in a single query. Predefined searches also can be used to return e-mail addresses, contact names, URLs, etc. The forensic examiner can add case specific keywords related to the investigation. The more keywords supplied and the amount of media to be searched determines the time frame the search process takes. On average, a search for six keywords on a Palm OS device takes approximately 30 minutes, but allows the examiner to search simultaneously for all keywords relevant to the case. Figure 16 below shows the Search functionality.

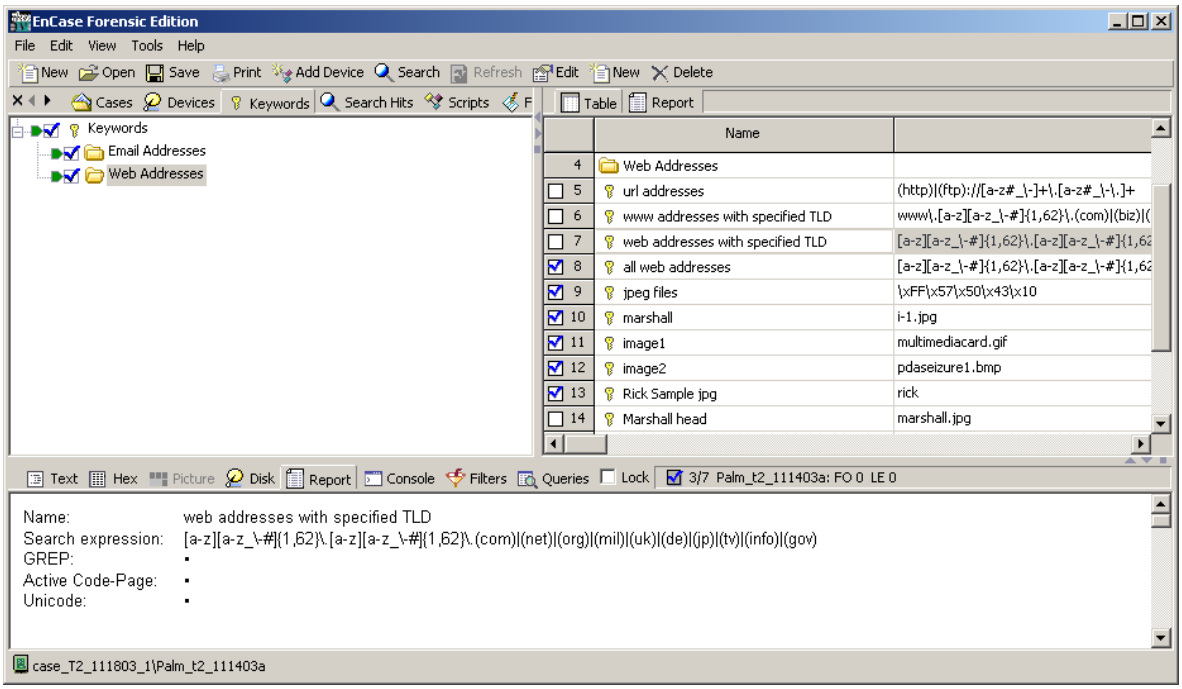


Figure 16: Keyword Screen

The user interface to the search engine contains the following check boxes, illustrated below in Figure 17, to eliminate unnecessary hits and allow for more defined searches:

- Case Sensitive – Keywords are searched in the exact case specified in the text box.
- Active Code-Page – Allows the ability to enter keywords in different languages.
- GREP – The keyword is a regular expression to search using the global regular expression post advanced searching syntax.
- Unicode – The Unicode standard attempts to provide a unique encoding number for every character, it uses 16-bits to represent each character.
- RTL Reading – The RTL Reading option will search for the keyword in a right-to-left sequence.
- UTF7 – Has the quality of encoding the full BMP repertoire using only octets with the high-order bit clear. UTF-7 is mostly obsolete, to use when searching for older Internet content.
- UTF8 – UTF8 is commonly used in transmission via Internet protocols and in web content.

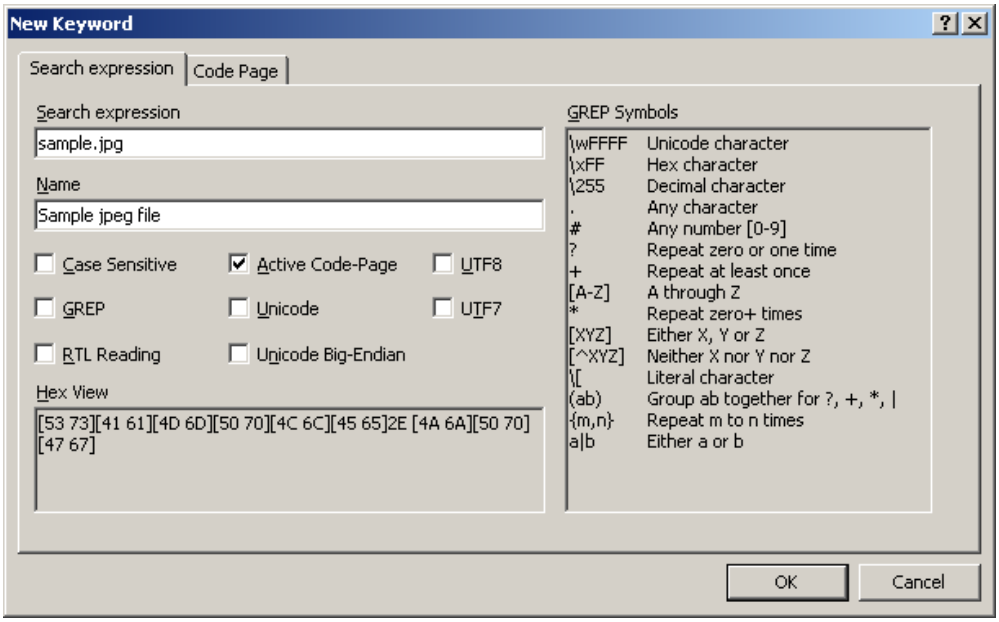


Figure 17: Search Expression Screen

The Search expression also allows the examiner to use complex search expressions involving the following notation:

- \wFFFF (Unicode Character)
- \xFF (Hex)
- \255 (decimal)
- . (any character)
- # (any number)
- ? (repeat zero or one time)
- + (repeat at least once)
- [A-Z], (A through Z)
- '*' (repeat zero + times)
- [XYZ] (Either X, Y, or Z)
- [^XYZ] (Neither X nor Y nor Z)
- \[(literal character)
- '(ab)' Group ab together for ?, +, *, |
- {m,n} Repeat m to n times
- a|b (Either a or b).

Figure 18 below contains a screen shot that illustrates the results an examiner typically sees after running a search.

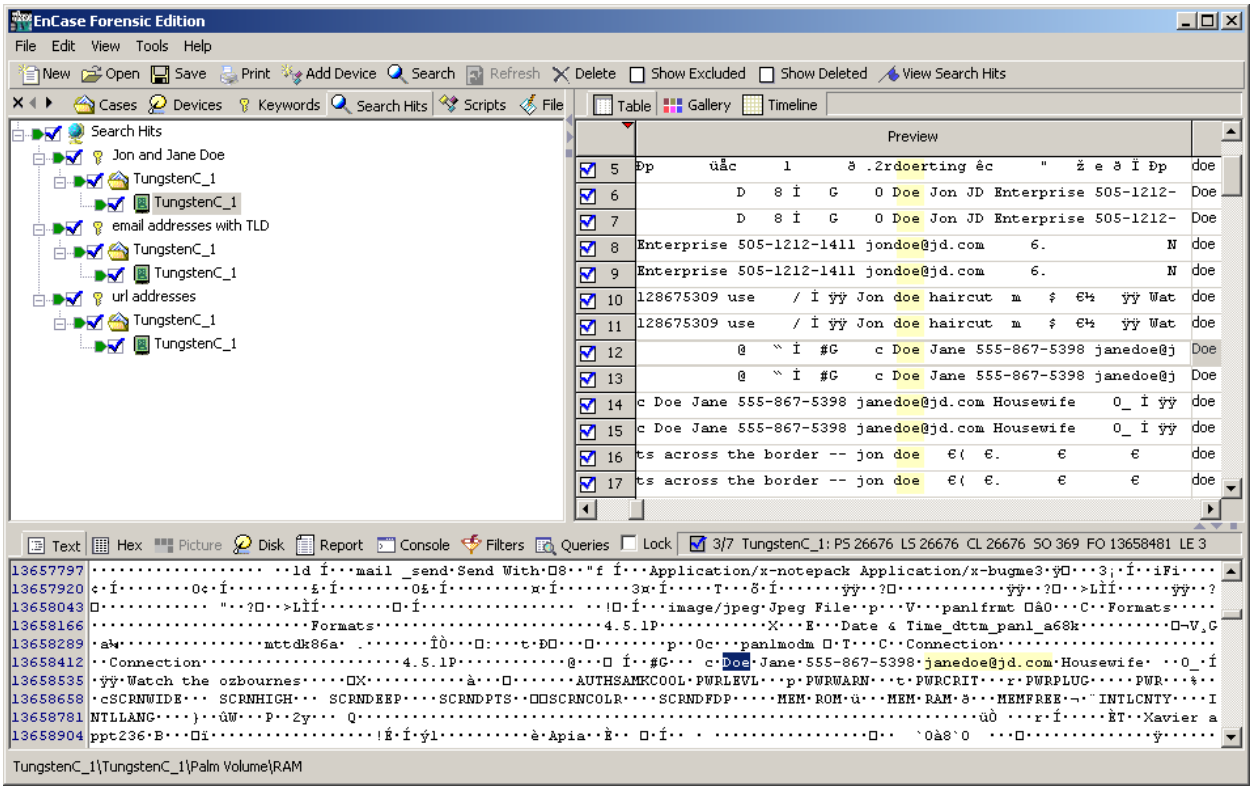


Figure 18: Search Results

The left pane allows examiners to view the keyword specifics (e.g., e-mail addresses or web addresses, etc.). The right pane displays any matches found based upon the keyword(s) previously defined. The output can be exported to a text file. Specific addresses, URLs, etc. can be bookmarked as the forensic examiner comes across relevant information. Figure 19 illustrates a small excerpt that displays all URL, e-mail, and web address information after the export function has been performed.

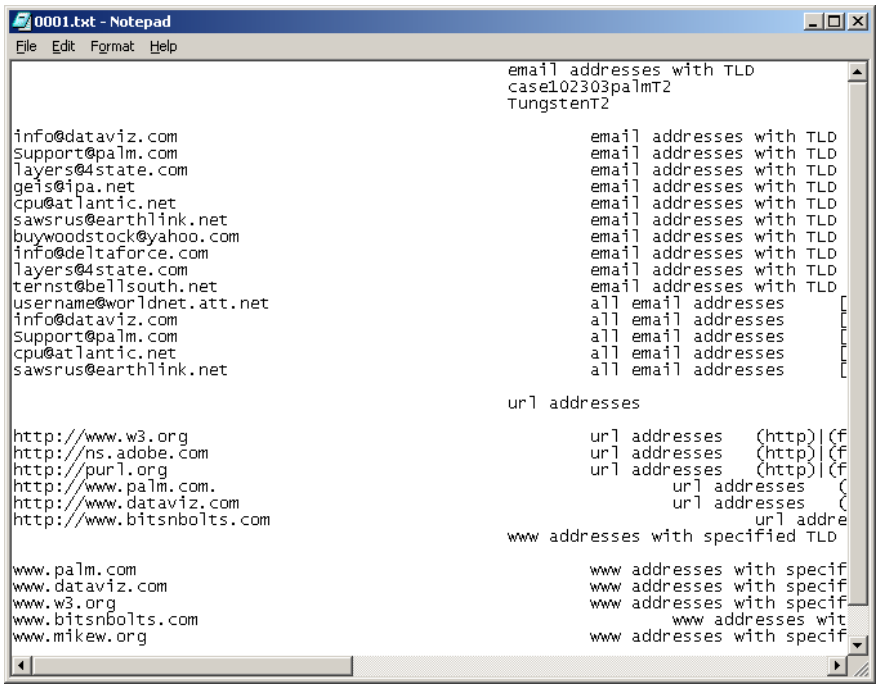


Figure 19: Exported Results

Examiners do not necessarily have to export the selected hits to an ASCII text file, since the option to include selected hits in a final report is also provided. This facility gives the examiner the ability to produce professional reports for future evaluation. The reports are dependent upon the amount of information found and can be extremely large due to the fact that each hit shows the generalized regular expression pattern used to find the information.

Scripts

EnCase has built-in scripts that allow the examiner to perform the following tasks:

- Consecutive Sectors: This script searches the disk for sectors that are filled entirely with a specified character. The results of the scan are saved in the bookmarks.
- Find Unique E-mail Address List: This script searches through selected files for a "basic" e-mail signature, this is further checked out using a built-in EnScript function. Once a good hit is found, it is added to a list, so that if the same address is found, it will not be added again.
- Graphics File Finder: This script searches for user specified graphics files of the following types: `.emf`, `.jpg`, `.gif`, and `.bmp` files. After the script has been compiled and run, all graphics files of the specified type are displayed in the graphics library. In addition examiners can craft a customized graphics file finder for additional graphics files (e.g., `.png` files).
- Valid Credit Card Finder: This script will bookmark valid VISA, MasterCard and AmEx numbers. All valid credit card (CC) hits will be bookmarked in the folder "All CC Hits". The first occurrence of each CC hit will be bookmarked in "Unique CC Hits".

Each of the above scripts are run producing a bookmark of the results, which allow the forensic examiner to evaluate the following: a table view of the data, a gallery for pictures (e.g., `.jpg`, `.bmp`, `.emf`, `.gif`, etc.), a timeline, and the generated report from the script.

Graphics Library

After a script to find all examiner specified types of graphics files has been compiled and run, the output creates a bookmark of the data produced from the script. On the right-pane, the examiner has four views of the search results: table, gallery, timeline, and report. A table view lists each individual file with information such as file size, file offset, file path, etc., while the gallery tab provides the examiner with the ability to quickly browse through all graphics files found on the suspects device. A timeline view allows examiners to look at patterns of file creation, editing, and last accessed times. The report view displays the final report. Figure 20 shows an example of the graphics library. The lower pane displays individual pictures that are highlighted.

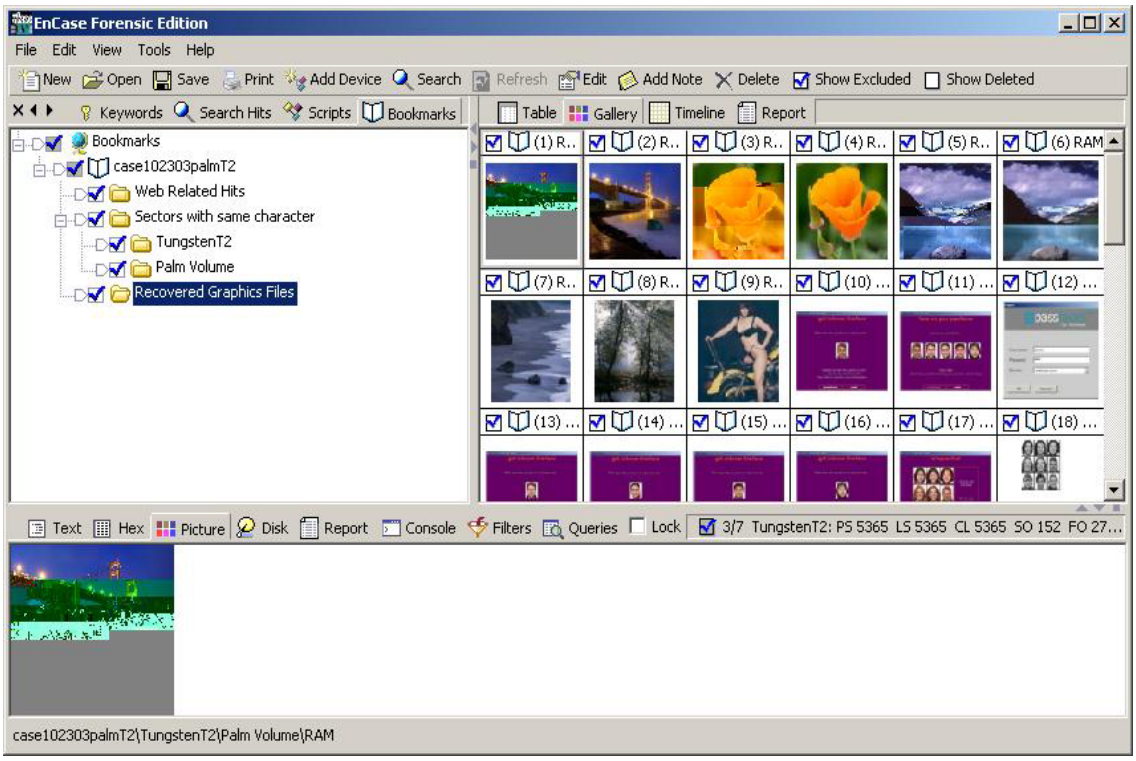


Figure 20: Graphics Library

EnScript & Filters

EnScript is a programming language, compatible with the ANSI C++ standard for expression evaluation and operator meanings. The language involves a small subset of C++ features. EnCase has integrated EnScript into its forensic software, allowing forensic examiners the ability to write and compile their own customized scripts. This customized scripting facility provides the ability to extract data specifics relative to the case.

Filters allow forensic examiners to limit the information that is shown within EnCase. For instance, an examiner might like to view only a particular type of file, modified between a given set of dates. Whenever filters are run, a query with the filter's name is created and activated. Filters can be combined together to create complex queries using AND/OR logic. Although the number of files currently residing on PDAs tends to be small, they are likely to increase as device storage capabilities continue to improve. Therefore, the power of EnScript and Filters integrated into EnCase allows examiners the ability to keep abreast of these developments,

through prewritten scripts that can speed the investigative process and lessen the chance of omitting valuable information.

Report Generation

The final phase of a forensic examination is reporting the findings. The report should be organized and presented in a readable format that the target audience will understand. EnCase is designed to help the examiner bookmark and export the findings in an organized manner so a report can be generated quickly upon completion of the examination.

EnCase provides several methods for generating a report. The report has the option to be generated in two formats: Microsoft Word Document and HTML. Some examiners prefer to break up the report into several sub-reports inside a word-processing program, with a summary report document directing the reader to their contents. Other examiners create paperless reports burned to compact disc, using a hyperlinked summary of sub-reports and supporting documentation and files. EnCase gives the examiner the option to customize and organize the contents of the report. The Report view reports the information it has about the current folder/volume selected, such as date and time stamps and file permissions. Examiners can combine multiple generated reports based upon the information found.

Synopsis of pdd

As mentioned earlier, pdd was developed to acquire information from PDA devices from the Palm OS family. pdd is a command line driven application that outputs a binary file. To analyze the output, the examiner has a couple of options: examining the content with a hex editor, similar tool, importing the image into EnCase or some other forensic tool capable of reading and interpreting the image and presenting the information in a form more conducive for examination. In order to successfully import the image into EnCase, the examiner needs to create a new case, add a raw image, and select the partition type. Because pdd is no longer supported and Paraben has integrated the pdd engine into PDA Seizure, only a brief summary of pdd is provided here.

pdd creates two output files:

- One named pdd.txt, which contains device specific information. Below is an example of pdd.txt output.

```
Current Time: Mon Oct 06 14:43:50 2003 UCT
Card Number: 0
Card Name: PalmCard
Manufacturer: Palm Computing
Card Version: 0001
Creation Date: Thu Mar 05 10:05:47 1998 UCT
Palm OS Version: 3.0.0
Processor Type: Motorola DragonBall 68328
RAM Size: 2097152 bytes
Free RAM: 2056776 bytes
ROM Size: 2097152 bytes
ROM Used By OS: 1150972 bytes
Flash ID: 508115F80WHG-U
Image Output File: Standard output
Image Memory Type: RAM
Starting Address: $10000000
```

- The image file is created and named by the user by redirecting the output to it, i.e., pdd > filename.txt. The contents of the file contain a combination of binary and ASCII characters. If the output is not redirected to a file, the raw image is displayed on the screen.

A complete bit-by-bit image can be acquired from a device running the Palm OS. A CRC-16 checksum ensures the integrity of every packet transferred to the device. After the acquisition stage, PIM data can be viewed with a standard ASCII or hex editor. The PIM data is displayed in clear text allowing examiners to search through data contents such as contact, calendar, e-mail and task-management items. Examiners must have knowledge of file header/footer signatures to allow identification of binary files. Binary files are extremely difficult to extract and view with an appropriate application since their contents are not human readable or always in contiguous memory. Before the pdd acquisition process begins, the Palm device must be put in console mode and forensic examiners must exit all active HotSync applications. The Palm OS console mode debugger is used to acquire memory card information and to create the image of the selected memory region.

Synopsis of Pilot-link

The pilot-link software can be used to obtain both ROM/RAM from palm devices and data can be imported into the Palm OS Emulator (POSE) or the individual files can be viewed with a standard ASCII, hex editor or compatible forensic application. Additionally, the data created from pilot-link can be imported into other compatible forensic applications. Once the software is installed and configured, communications between the PC and the device can begin. RAM and ROM are dumped from the device with the following commands: `pi-getrom` and `pi-getram`.

In order to prepare data to be imported into POSE the following commands are issued:

- `pi-getrom`: Generates a ROM image of the device.
- `pi-getram`: Generates a RAM image of the device.
- `pilot-xfer –b <dir>`: Typically used for backup purposes.

`Pilot-xfer` allows the user to import databases (i.e., `.prc`, `.pdb`, and `.pqa)` into POSE allowing a virtual view of the data contained on the device.

A few other useful pilot-link commands are the following:

- `addresses`: Dumps the palm address book.
- `memos`: Exports memos from Palm in a standard mailbox format.
- `pilot-clip`: Exports data from the Palm clipboard.
- `pilot-file`: Dissects and allows a view of detailed information about the Palm Resource Database, Palm Record Database and the Palm Query Application files.
- `pilot-undelete`: Turn archived records into normal records.
- `pilot-xfer`: Backup, restore, install & delete Palm databases.
- `read-expenses`: Export Palm Pro Expense database into text format.
- `read-ical`: Export Palm Datebook and ToDo databases into an Ican calendar.
- `read-todos`: Export Palm ToDo database into generic text format.
- `reminders`: Export Palm Datebook into a 'remind' data file.

Synopsis of dd

Distributions of the Linux OS are available for a number of handheld devices from the Pocket PC and Palm families. They require the owner of the device to replace the existing OS with the Linux distribution. Several handheld device manufacturers have also adopted Linux as their default OS. While a few different ways exist for the examiner to obtain information from Linux-based PDAs, examiners must be comfortable with the Linux OS to ensure that all necessary modules are loaded (i.e., usbserial and usbnet) and function correctly. Each step taken during the investigation must also be well documented to allow, for example, a reconstruction of events in a court of law, if necessary.

The `dd` utility has the ability to acquire information from Linux-based PDAs. In order to perform a data dump, the examiner must have an established connection with the device (e.g., `telnet`/`ssh`). After the connection is complete and the examiner is logged in as root, issuing the `dd` command dumps and compresses the data contents to the device's peripheral memory card or to a forensic workstation. The `dd` (duplicate disk/data dumper) utility has a multitude of options available. Listed below are some of `dd`'s main arguments:

- `if=` Specifies the input file
- `of=` Specifies the output file
- `bs=` Specifies the block size, or how much data is transferred in one operation
- `count=` Specifies how many blocks to transfer
- `skip=` Specifies the number of blocks to skip at the beginning of the input file
- `conv=` Specifies data conversion

The `conv=` option allows examiners to image drives that are damaged or restore drives from computer systems with different byte ordering. For instance, the flags `conv=sync`, `noerror` specifies not to stop on a read and, if there is a read error, pad the output with 0x00.

Before issuing the `dd` command, it is advantageous to use a `df` command first to determine which parts of the filesystem to dump. After the data contents have been written to the memory card or hard disk, they can be viewed and searched on the PC by importing the raw image into an available tool, such as a hex editor, or a forensic tool, such as EnCase. Another technique for viewing device data is to mount the `dd` created image in loop-back mode on a Linux machine. This procedure allows all the files to be accessed as if the filesystem was local to the device. Graphics files can be viewed directly with an appropriate graphics tool (e.g., `gqview`).

Other ways besides `dd` exist to acquire data from Linux-based PDAs. The choice is dictated by the characteristics of the handheld device being examined. Two other common alternatives are `scp` and the system backup/restore utilities which provide a logical view of the data. In order to `scp` (secure copy) data from the device to the examiner PC, the openssh package must be installed. If `scp` is already installed on the device, a copy of the filesystem can be made with an `scp` command such as the following: `scp -r root@lnx24:/root/home/username/`. The backup/restore utility present on many Linux distributions (e.g., Lineo, Familiar, etc.) can be used to capture data from Linux-based PDAs. The backup function makes use of removable media and stores the image on a memory card, which can then be restored on a comparable PDA for a duplicate copy.

Analysis Overview

Scenarios

To understand the capabilities of the forensic tools described in the previous chapters, a series of scenarios were developed. The scenarios begin with content acquisition and move progressively toward more interesting situations involving common applications, file formats, and device settings. The scenarios are not intended to be exhaustive or to serve as a formal product evaluation. However, they attempt to cover a range of situations commonly encountered when examining a device (e.g., data obfuscation, data hiding, data purging) and are useful in determining the features and functionality afforded an examiner.

Table 3 below gives an overview of these scenarios, which are generic to all PDAs. For each scenario listed, a description of its purpose, method of execution, and expected results are summarized. Note that the expectations are comparable to those an examiner would have when dealing with the contents of a hard disk drive as opposed to a PDA. Though the characteristics of the two are quite different, the recovery and analysis of information from a hard drive is a well-understood baseline for comparison and pedagogical purposes. Note too that none of the scenarios attempt to confirm whether the integrity of the data on a device is preserved when applying a tool – that topic is outside the scope of this document, as mentioned earlier.

Table 3: Scenarios

Scenario	Description
Device Content Acquisition	Determine if the tool can successfully acquire the contents of the device. • Initiate the tool on a forensic workstation, attempt to connect with the device and acquire its contents, verify that information has been obtained. • Expect that information residing on the device can be successfully acquired.
PIM Applications	Determine whether the tool can find information, including deleted information, associated with Personal Information Management (PIM) applications such as calendar, contacts, e-mail synched with a PC, and task lists. • Create various types of PIM files on the device, selectively delete some entries, acquire the contents of the device, locate and display the information. • Expect that all PIM-related information on the device can be found and reported, if not previously deleted. Expect that remnants of deleted information can be recovered and reported.

Scenario	Description
Web/E-mail Applications	Determine whether the tool can find a visited web site and exchanged e-mail message information obtained by a wireless network enabled device through an 802.11b access point. • Use the device to visit specific web sites and exchange e-mail, acquire the contents of the device, selectively delete some e-mail, locate and display the URLs of visited sites, headers of e-mail messages, and any associated data acquired (e.g., images, text, etc.). • Expect that information about most recent web, web-mail, and e-mail activity can be found and reported. Expect that remnants of deleted e-mail information can be recovered and reported.
Graphics File Formats	Determine whether the tool can find and display a compilation of the graphics formatted files acquired from the device. • Load the device with various types of graphics files, acquire the contents of the device, locate and display the images. • Expect that all files with common graphics files formats (i.e., `.bmp`, `.jpg`, `.gif`, `.tif`, and `.png`) can be found, reported, and collectively displayed.
Compressed File Archive Formats	Determine whether the tool can find text, images, and other information located within compressed-archive formatted files (i.e., `.zip`) residing on the device. • Load the device with various types of file archives, acquire the contents of the device, find and display selected filenames and file contents. • Expect that text, images, and other information contained in common compressed archive formatted files can be found and reported.
Other Compressed Archive Formats	Determine whether the tool can find text, images, and other information within other, less common, archive formats (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar`, and self-extracting `.exe`). • Load the device with various types of file archives, acquire the contents of the device, find and display selected filenames and file contents. • Expect that text, images, and other information contained in the compressed archive formatted files can be found and reported.

Scenario	Description
Deleted Files	Determine if the tool can recover files deleted from the device. Two variants exist: recovery attempted before and after synchronizing the device with a PC. • Create one or more files on the device; delete a file, acquire the contents of the device, and attempt to locate the deleted file. • Expect that all deleted files can be recovered, reported, and, if an image, displayed.
Misnamed Files	Determine whether the tool can recognize file types by header information instead of file extension, and find common text and graphics formatted files that have been misnamed with a misleading extension. • Load the device with various types of common text (e.g., `.txt`) and graphics files (e.g., `.bmp`, `.jpg`, `.gif`, and `.png`) purposely misnamed, acquire the contents of the device, locate and display selected text and images. • Expect that all misnamed text and graphics files residing on the device can be recognized, reported, and, if an image, displayed.
Peripheral Memory Cards	Determine whether the tool can acquire individual files stored on a memory card inserted into the device and whether deleted files would be identifiable and recoverable. • Insert a memory card containing a populated filesystem into an appropriate slot on the device, delete some files, acquire the contents of the device, find and display selected files and file contents, including deleted files. • Expect that the files on the memory card, including deleted files, can be properly acquired, found, and reported in the same way as expected with on-device memory.
Cleared Devices	Determine if the tool can acquire any user information from the device or peripheral memory, after a hard reset has been performed. • Perform a hard reset on the device, acquire its contents, and find and display previously available filenames and file contents. • Expect that no user files, except those contained on a peripheral memory card, if present, can be recovered.

Scenario	Description
Password Protected Devices	Determine whether the tool can obtain the user's password to acquire the contents of the device. • Enable the password on the device, apply any utilities to crack the password, acquire the contents of the device. • Expect that the user's password cannot be obtained, except for those devices with older, more vulnerable operating systems.

In the chapters that follow, the above scenarios are applied to different families of PDA devices to determine the extent to which a given tool meets the expectations listed.

Devices

To apply the various forensic tools against the scenarios, several PDAs from different device families served as the target device under examination. Table 4 summarizes the various operating system and device combinations used with each tool. An entry of NA (Not Applicable) within the table indicates that the tool listed in the corresponding row heading does not support the device family listed in the corresponding column heading. Other entries indicate the operating system version and processor type of the target devices used with a tool. Nearly all the devices listed come with the respective operating system preinstalled by their manufacturer. However, the Linux column contains a modified device on which a distribution of Linux for handheld devices was installed for this exercise.

Table 4: Target Devices

	Pocket PC	Palm OS	Linux
PDA Seizure	Jornada 548 (PPC 00) iPaq 3875 (PPC 00) iPaq 3970 (PPC 02) iPaq 5455 (PPC 03)	Palm III (3.0) Palm Vx (3.3) Visor Platinum (3.5) Tungsten C (5.2.1)	NA
EnCase	NA	Palm III (3.0) Palm Vx (3.3) Visor Platinum (3.5) Tungsten C (5.2.1)	Zaurus SL-5000 (Lineo 2.4.6)[a,b]
dd	NA	NA	Zaurus SL-5000 (Lineo 2.4.6)[c] iPaq 3970 (Familiar version 2.4.19)[d]

[a] The Lineo distribution of the Linux 2.4.6 kernel came preinstalled on this device

[b] EnCase accepts various filesystem images for analysis, including Ext2fs used by this device

[c] dd was used to acquire device contents and produce a filesystem image, but not used for analysis

[d] The Familiar distribution of Linux (**http://familiar.handhelds.org/**) was installed on the iPaq 3970 device listed in column one

The target devices within a device family, while not extensive, cover a range of operating system versions and processor types, as well as other hardware components. These variations were

intended to uncover subtle differences in the tools' behavior. Table 5 highlights the key characteristics of each target device.

Table 5: Target Device Characteristics

	Performance	Expansion	Wireless
Jornada 548	133Mhz Hitachi SH3 processor 16MB ROM/ 32MB RAM	CF card slot (Type I)	IrDA infrared port
iPaq 3875	206 MHz Intel StrongArm processor 32 MB flash ROM 64 MB RAM	SD/MMC card slot	IrDA infrared port
iPaq 3970	400MHz Intel Xscale processor 48MB flash ROM 64 MB RAM	SD/MMC card slot[a] CF Expansion sleeve[b]	IrDA infrared port Integrated Bluetooth
iPaq 5455	400MHz Intel Xscale processor 48MB flash ROM 64 MB RAM	SD/MMC slot or CF card slot (Type II)	IrDA infrared port Integrated 802.11bWiFi and Bluetooth
Palm III	16 MHz Motorola Dragonball processor 2 MB flash ROM 2 MB SRAM	None	IrDA infrared port
Palm Vx	20 MHz Motorola Dragonball EZ processor 2 MB flash ROM 8 MB RAM	None	IrDA infrared port
Visor Platinum	33 MHz Motorola Dragonball VZ processor fixed ROM 8 MB RAM	Springboard module expansion slot	IrDA infrared port
Tungsten C	400MHz Intel XScale processor 64MB RAM 16MB Flash ROM	SD/MMC slot	IrDA infrared port Integrated 802.11b WiFi
Zaurus SL-5000	206 MHz Intel StrongARM processor 64MB DRAM and 16MB Flash ROM	SD/MMC and CF (Type II) card slots	IrDA infrared port

[a] When the Linux OS was installed on the device, the SD functionality of the slot was not supported

[b] The CF sleeve was used in the scenarios only when the Linux OS was installed on the device

PDA Seizure Outcome – Pocket PC

The scenarios were performed using a Windows 2000 machine with the target Pocket PC devices. The average acquisition time took between 30 to 60 minutes, depending upon the amount of memory and the connection (i.e., USB vs. Serial). Recall that Paraben utilizes RAPI calls to acquire most of the information, in lieu of imaging and analyzing memory contents. The ActiveSync protocol must be running and connectivity must be established for RAPI to acquire information from the device. The following options were selected for all PPC devices tested: acquire files, memory, registry, and databases.

Jornada 548

The following scenarios were executed on an HP Jornada 548 running Pocket PC 2000.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 30 minutes.

PIM Application Files: All active PIM information was found and reported. Deleted PIM information was recovered for the Calendar, Tasks, and E-mail (Address, Subject, and Body text) and reported. Deleted Contact information was not recoverable.

Web/E-mail Applications: Not Applicable - The Jornada does not have built-in 802.11b networking capabilities.

Graphics File Formats: The following graphics files were found, reported, and displayed in the graphics library: `.bmp`, `.jpg`, `.gif` files. `.tif` and `.png` files were reported in the graphics library, but the images were not displayed. However, they could be exported and viewed with an external viewer.

Compressed File Archive Formats: Text files compressed with WinZip were found and reported. Graphics files were found and reported, but not decompressed and displayed automatically in the graphics library. Therefore, manual means were used to locate these files.

Other Compressed Archive Formats: Text files in archive formats: `.tar`, `.tar.gz`, `.tgz`, `.rar`, and `.exe` were found and reported. Graphics files were found and reported, but not decompressed and displayed in the graphics library. However, they could be exported and viewed with an external viewer.

Deleted Files: Filenames of deleted files were recovered and reported. However, file content was not recoverable. The results were the same both before and after synchronization.

Misnamed Files: Files with unassociated extensions are not recognized by file header and treated accordingly. Therefore, manual means are needed to properly identify the file type and launch the appropriate viewer.

Peripheral Memory Cards: A CF card was used for this scenario. All active files stored on the memory card were found and reported. Deleted files were not recoverable, but searches

performed on filenames returned positive results. However, as noted earlier, other ways exist to examine the contents of the memory card directly and recover those files.

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button. A CF card containing data was present. No previous data or personal information on the device was found after acquisition. The data contained on the CF card, however, was recoverable. During the acquisition stage the following error occurred illustrated below in Figure 21:

Figure 21: Runtime Error

Although this error occurred, the acquisition process finished and the device imaged successfully. Another error illustrated below in Figure 22 arose after performing a hard reset.

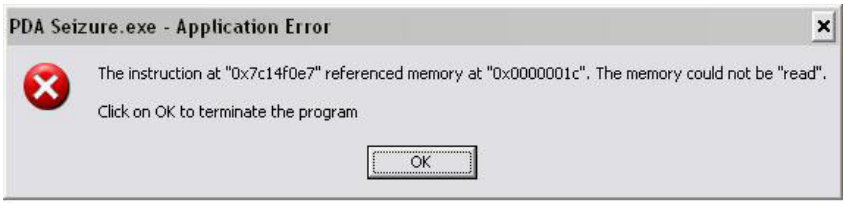


Figure 22: Application Error

Password Protected Devices: Not Applicable - If a 4-digit pin or alphanumeric password is employed for user authentication, ActiveSync prompts for the information. Until the proper entry is made, communications/connectivity is not permitted.

IPaq 3875/3970/5455

The following Scenarios were executed on iPaq 3875, 3970, and 5455 series devices, with different versions of the OS, PPC 2000 through 2003 respectively.

Device Content Acquisition: Pocket PC 2003, officially known as Windows Mobile, requires ActiveSync 3.7 to synchronize data between a PC and the device. However, PDA Seizure version 2.5.0.0 was not able to successfully make a connection to the device with ActiveSync 3.7. In order to acquire information, ActiveSync 3.7 had to be uninstalled and replaced with ActiveSync 3.5. Thereafter, acquiring information proceeded as expected, with no connectivity problems encountered. The acquisition process for the devices, took approximately 30-60 minutes.

PIM Application Files: All active PIM information was found and reported. None of the deleted PIM information was recoverable for the iPaq 5455 device. For the iPaq 3875/3970 devices, deleted e-mail information (i.e., Address, Subject, and Body text) was found and reported. Other deleted PIM information on the 3875/3970 series was not recoverable.

Web/E-mail Applications: The iPaq 5455 has built-in 802.11b, which was used to send and receive e-mails wirelessly and visit various sites. All web activity/data was stored in the `\Windows\Profiles\guest\Temporary Internet Files\Content.IE5\` directory. All visited web sites and their associated data (i.e., gifs, text, etc.) was found and reported. All URLs of visited web sites were found and reported. All e-mails sent or received via web-mail were found and reported. Remnants of deleted e-mail were recovered.

Graphics File Formats: The following graphics files were successfully found, reported, and displayed in the graphics library: `.bmp`, `.jpg`, and `.gif` files. `.tif` and `.png` files were reported in the graphics library, but the image were not displayed. However, they could be exported and viewed with an external viewer.

Compressed File Archive Formats: Text files compressed with WinZip were found and reported. Graphics files were found and reported, but not decompressed and displayed automatically in the graphics library. Therefore, manual means were used to locate these files.

Other Compressed Archive Formats: Text files in archive formats `.tar`, `.tar.gz`, `.tgz`, `.rar`, and `.exe` were found and reported. Graphics files were found and reported, but not displayed in the graphics library.

Deleted Files: Filenames of deleted files were recovered and reported. However, file content was not recoverable. Deleted files were not recoverable either before or after synchronization.

Misnamed Files: Files with unassociated extensions are not recognized by file header and treated accordingly. Therefore, manual means are needed to properly identify the file type and launch the appropriate viewer.

Peripheral Memory Cards: An SD card was used for this scenario for both the 3970 and 5455 devices. All active files stored on the memory card were found and reported. Deleted files were not recoverable. However, as noted earlier, other ways exist to examine the contents of the memory card directly and recover those files.

Cleared Devices: A hard reset was performed on the device by pressing and holding buttons 1, 4, and the reset button. An SD card containing data was present. No previous data or personal information on the device was found after acquisition. The data on the SD card, however, was recoverable.

Password Protected Devices: Not Applicable - If a 4-digit pin or alphanumeric password is employed for user authentication, ActiveSync prompts for the information. Until the proper entry is made, communications/connectivity is not permitted. On the iPaq 5455 series the

situation is more complicated, an alpha-numeric/PIN password must be supplied together with a biometric fingerprint, via the built-in fingerprint scanner.

PDA Seizure Outcome - Palm OS

The scenarios were performed using a Windows 2000 machine with the target Palm devices. The average acquisition time took between taking approximately 20-40 minutes, depending upon the amount of memory and the connection (i.e., USB vs. Serial). The Palm device must be put in console mode and forensic examiners must exit all active HotSync applications to begin physical acquisition. Paraben integrates the `pdd` engine into their software for imaging Palm devices.

The following acquisition options were selected: acquire files and acquire memory. If the device is password protected and the Palm OS is version 4.0 or lower, the decode password option should be selected before attempting to acquire information. Before the acquisition process begins, the examiner is prompted with a Card Selection screen asking to select the cards for which physical memory images are desired: Card 0 (Main System) - both the RAM image and the ROM images were selected. During the acquisition stage, the examiner is prompted to press the HotSync button on the cradle to begin logical acquisition using the HotSync protocol. In order to transfer files to the Palm devices the Quick Install protocol was used.

The Palm OS supports only the jpeg format for graphics files. Therefore, when files of type `.bmp`, `.gif`, `.png`, etc. are transferred to the device, they are automatically converted to the `.jpg` format. Graphics viewer software such as irFanView[19] was used to display files of graphic content.

Palm III/Palm Vx

The following scenarios were conducted on a 3Com Palm III device running Palm OS 3.0 and a Palm Vx running Palm OS 3.3.

Device Content Acquisition: The Palm III/Palm Vx device contents were successfully acquired. The acquisition process took approximately 20 to 30 minutes.

PIM Application Files: All active PIM information was found and reported. The deleted PIM information was partially recoverable. Deleted items in the Calendar and ToDo list were not recoverable, while deleted entries in the Contact List and Memo List were recovered.

Web/E-mail Applications: Not Applicable - The Palm III/Palm Vx devices do not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

[19] Additional information can be found at: **http://www.irfanview.com**

Other Compressed Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: Not Applicable - The Palm III/Palm Vx devices do not contain removable media slots for cards such as Compact Flash (CF) or Secure Digital (SD).

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button, followed by pressing the up key at the prompt to erase all data. When a hard reset was performed on the devices no user data was recoverable.

Password Protected Devices: The following types of passwords were used: 4 to 8 numeric, 8-12 alphanumeric, 8-12 alphanumeric with special characters. PDA Seizure cracked all passwords in approximately 2 seconds.

Visor Platinum

The following scenarios were conducted on a on a Handspring Visor Platinum running Palm OS 3.5.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 10-20 minutes.

PIM Application Files: All active PIM information was found and reported. All deleted PIM information was recovered.

Web/E-mail Applications: Not Applicable - The Visor does not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Palm device via the Quick Install protocol the files are automatically uncompressed before being uploaded to the device.

Other Compressed Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: Not Applicable - The Visor device does not contain removable media slots for cards such as Compact Flash (CF) or Secure Digital (SD).

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button. Remnants of files transferred to the device using an application such as Documents-to-Go were recoverable. Remnants of files created locally on the device with a PIM application such as Memo Pad were not found after acquisition.

Password Protected Devices: The following types of passwords were used: 4 to 8 numeric, 8-12 alphanumeric, 8-12 alphanumeric with special characters. PDA Seizure cracked each password under 2 seconds.

Tungsten C

The following scenarios were conducted on the Palm Tungsten C running Palm OS 5.2.1.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 30-40 minutes.

PIM Application Files: All active PIM information was found and reported. Most deleted PIM information was recovered, however, there were few instances where deleted PIM information had a few characters missing, but nevertheless was comprehensible.

Web/E-mail Applications: The Tungsten C has built-in 802.11b, which was used to send and receive e-mails wirelessly and visit various sites. All visited web sites and their associated data (i.e., gifs, text, etc.) were found and reported. All URLs of visited web sites were found and reported. All e-mails sent or received via web-mail were found and reported. Remnants of deleted e-mail were recovered.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Palm device via the Quick Install protocol the files are automatically uncompressed before being uploaded to the device.

Other Compressed Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: An SD card was used for this scenario. No active or deleted files on the memory card were found and reported. However, as noted earlier, other ways exist to examine the contents of the memory card directly and recover those files.

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button. Files transferred to the device using an application such as Documents-to-Go were not recoverable. Remnants of files created locally on the device with a PIM application such as Memo Pad were found after acquisition.

Password Protected Devices: Not Applicable - Because the version of the OS is greater than 4.0, PDA Seizure could not crack passwords on the Tungsten C device, as expected.

EnCase Outcome - Palm OS

The scenarios were performed using a Windows 2000 machine with the target Palm devices. The average acquisition time took between 10 to 40 minutes. EnCase does not support Pocket PC devices, therefore, scenarios were not performed on PPC devices.

Palm III

The following scenarios were conducted on a 3Com Palm III device running Palm OS 3.0.

Device Content Acquisition: EnCase was unable to acquire data present on the Palm III device. The device was successfully acquired using `pdd`. During the preview stage, EnCase threw a fatal exception error on the device, forcing a reset. Connectivity between the device and the PC was tested and successful. Therefore, a marriage of `pdd` and EnCase was utilized for acquisition and analysis. The acquisition process took approximately 20 minutes. The analysis of the data was performed by importing the output from `pdd` into EnCase as a raw image.

PIM Application Files: All active PIM information was found and reported. All deleted PIM information was recovered.

Web/E-mail Applications: Not Applicable - The Palm III does not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Other Compressed Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: Not Applicable - The Palm III device does not contain removable media slots for cards such as Compact Flash (CF) or Secure Digital (SD).

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button, followed by pressing the up key at the prompt to erase all data. No user data was recoverable.

Password Protected Devices: Not Applicable - EnCase does not include password cracking facilities.

Palm Vx

The following scenarios were conducted on a Palm Vx device running Palm OS 3.3.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 20 to 30 minutes.

PIM Application Files: All active PIM information was found and reported. Most deleted PIM information was recovered, except for Calendar information and a few instances where deleted PIM information had a few characters missing, but nevertheless was comprehensible.

Web/E-mail Applications: Not Applicable - The Palm Vx does not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Other Compressd Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: Not Applicable - The Palm Vx device does not contain removable media slots for cards such as Compact Flash (CF) or Secure Digital (SD).

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button, followed by pressing the up key at the prompt to erase all data. Remnants of deleted files were found after acquisition.

Password Protected Devices: Not Applicable - EnCase does not include password cracking facilities.

Visor Platinum

The following scenarios were conducted on a Handspring Visor Platinum running Palm OS 3.5.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 10 to 20 minutes.

PIM Application Files: All active PIM information was found and reported. All deleted PIM information was recovered.

Web/E-mail Applications: Not Applicable - The Visor does not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the Visor device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Other Compressd Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid type for the Palm OS.

Peripheral Memory Cards: Not Applicable - The Visor device does not contain removable media slots for cards such as Compact Flash (CF) or Secure Digital (SD).

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button. Remnants of files transferred to the device using an

application such as Documents-to-Go were recoverable. Remnants of files created locally on the device with a PIM application such as Memo Pad were not found after acquisition.

Password Protected Devices: Not Applicable - EnCase does not include password cracking facilities.

Tungsten C

The following scenarios were conducted on the Palm Tungsten C running Palm OS 5.2.1.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took approximately 30-40 minutes.

PIM Application Files: All active PIM information was found and reported. Most deleted PIM information was recovered, except for Calendar and Contact information and a few instances where deleted PIM information had a few characters missing, but nevertheless was comprehensible.

Web/E-mail Applications: The Tungsten C has built-in 802.11b, which was used to send and receive e-mails wirelessly and visit various sites. All visited web sites and their associated data (i.e. gifs, text, etc.) were found and reported. All URLs of visited web sites were found and reported. All e-mails sent or received via web-mail were found and reported. Remnants of deleted e-mail were recovered.

Graphics File Formats: All graphics files except for type `.jpg` were converted to the `.jpg` format when the data was synched. All graphics files of type `.jpg` were found, reported and displayed in the graphics library.

Compressed File Archive Formats: Not Applicable - When compressed files (i.e., `.zip` files) are transferred to the device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Other Compressed Archive Formats: Not Applicable - When compressed files (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar` and `.exe`) are transferred to the Palm device via the Quick Install protocol, the files are automatically uncompressed before being uploaded to the device.

Deleted Files: The majority of the contents of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be automatically displayed in the graphics library. If a HotSync was performed after files were deleted, but before the acquisition stage, the files were not recoverable.

Misnamed Files: Not Applicable - The Quick Install protocol looks at the type of file to determine if the file signature is consistent with the extension and if it is a valid file type for the Palm OS.

Peripheral Memory Cards: An SD card was used for this scenario. No active or deleted files on the memory card were found and reported. However, because the media is removable,

EnCase was used in a different manner to acquire information from the card (see Removable Media below). EnCase version 4.18 reportedly provides support for a Virtual File System (VFS) module, allowing memory cards to be mounted and read while in the device.[20]

Cleared Devices: A hard reset was performed on the device by pressing and holding the reset button while pressing the power button. Files transferred to the device using an application such as Documents-to-Go were not recoverable. Remnants of files created locally on the device with a PIM application such as Memo Pad were found after acquisition.

Password Protected Devices: Not Applicable - EnCase does not include password cracking facilities.

Removable Media

The following test was conducted using a PC connected to a memory card reader with the SD card.

Media Content Acquisition: Removable media (i.e., MMC, SD, CF cards, etc.) was acquired by EnCase using a memory card reader, which treats the card placed in the reader as a hard disk. The acquisition time for a 64mb card was approximately 1 to 2 minutes.

Deleted Files: All active and deleted files on the card were found and reported.

[20] For more information on the VFS module see: **http://www.guidancesoftware.com/products/modules/EnCaseVFS.shtm**

EnCase Outcome - Linux

The scenarios were performed using a Windows 2000 machine with one of the target Linux devices. EnCase does not support direct acquisition of Linux PDA devices. However, it does allow import of numerous types of filesystem images for analysis, including version 2 of the Extended Filesystem (Ext2fs), the de facto standard for Linux. The Zaurus SL-5000 device sports a version of Linux developed for embedded systems by Lineo, which uses Ext2fs. `dd` was used to image the filesystem on the device, as described in the `dd` Outcome chapter, and the output imported to EnCase.

The Familiar distribution of Linux for the iPaq device relies on flash ROM for its filesystem, instead of RAM. Flash memory has a limited life of approximately 100,000 erase cycles. Unfortunately, Ext2fs does not provide good management of flash memory erasures, needing to rewrite an entire sector to erase a single byte, nor does it ensure that different areas of memory are used in rotation to manage wear. Instead of using Ext2fs, the Familiar distribution uses JFFS2 (The Journaling Flash File System, version 2), which was designed specifically to overcome these problems. Because EnCase currently does not support JFFS2 images, testing for the iPaq device occurs only in the dd Outcome chapter.

Zaurus SL-5000

The following scenarios were conducted on the Zaurus SL-5000 running Lineo 2.4.6.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took between 2 to 5 minutes, utilizing `dd` to create the image. After the acquisition stage, the information was analyzed by importing the image into EnCase. Further discussion on how to properly image a Linux based PDA using `dd` is discussed in the `dd` Outcome chapter.

PIM Application Files: All active PIM information was found and reported. All deleted PIM information was recovered.

Web/E-mail Applications: Not Applicable - The Zaurus does not have built-in 802.11b networking capabilities.

Graphics File Formats: All graphics files were found, reported and displayed properly in the graphics library.

Compressed File Archive Formats: Text files compressed with WinZip were found and reported. Graphics files were found and reported, but not decompressed and displayed automatically in the graphics library. Therefore, manual means were used to locate these files.

Other Compressed Archive Formats: All files regardless of compression type (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar`, and `.exe`) were obtainable after acquisition and able to be viewed via EnCase.

Deleted Files: The filename and remnants of file content of text files were recovered and reported. Remnants of graphics files were recovered and reported, but not able to be

automatically displayed in the graphics library. The results were the same both before and after synchronization.

Misnamed Files: All misnamed text and graphic files were found and reported based on file signature. Therefore, renaming files with inconsistent file extensions has no effect.

Peripheral Memory Cards: Not Applicable - Although `dd` could be run on the device to acquire the contents of the card onto another memory card/forensic workstation and analyze the results with a forensic tool such as EnCase, making a forensically sound copy of the card on a forensic workstation is more straight forward and affects the device less.

Cleared Devices: A hard reset was performed on the device by removing the battery cover and pressing and holding the reset button. A CF card containing data was present. No previous data or personal information on the device was found after acquisition. The data contained on the CF card, however, was recoverable.

Password Protected Devices: Not Applicable - EnCase does not include password cracking facilities.

dd Outcome - Linux

The scenarios were performed using a Gentoo Linux (2.6.0) workstation with the following devices: Zaurus SL-5000 and an iPaq 3970. The Zaurus contains a compact flash and secure digital slot, and comes preloaded with the Lineo version of Linux. The iPaq device contains a secure digital slot and normally comes preloaded with PPC. However, the default operating system was replaced with the Familiar distribution of Linux for this exercise. The `dd` utility was used to create a sound forensic bit-by-bit image of both devices. Where necessary, a hex editor was used to examine the image. However, an attempt was made in each case to mount the `dd` created image in loop-back mode on the Linux workstation for logical analysis. This procedure allows the data from the image to be viewed in the same manner as if the filesystem was local to the workstation. Moreover, graphics files can be viewed with a graphics tool (i.e., `gqview`), eliminating the task of extracting binary data based upon header and footer information.[21] The examiner should first create a directory off of /mnt and issue the following command:

```
Mount –t ext2 <filename.dd> /mnt/<directory> -o loop
```

The above command is targeted specifically at the Zaurus image that is type Ext2. In order to perform these operations for the iPaq running Familiar, the Linux machine's kernel must be patched with the proper code for the JffS2 filesystem, if the kernel is less than 2.4.10. Recall too, that unlike the Zaurus, the iPaq configured with this distribution of Linux relies on flash ROM for its filesystem, instead of RAM.

In order for a successful communication link to be established, all necessary software modules must be installed on the Linux PC.[22] The Gentoo distribution of Linux running kernel 2.6.0 was used for testing. The following steps describe the major actions that were taken to allow a successful communication link to be established between the Zaurus PDA and the Linux PC:

- Zaurus: `passwd root` <enter> <enter> - This sets the root password to null
- Zaurus: Configure the IP address thru the network and sync application i.e. 192.168.129.201 broadcast 192.168.129.255 netmask 255.255.255.0
- Zaurus: Edit `/etc/securetty` and add ttya1 – ttya7
- Zaurus: Edit `/etc/inetd.conf` and uncomment out all occurrences of telnet
- Zaurus: Run `/etc/usbcontrol serial`
- PC: `modprobe usbserial`
- PC: `modprobe usbnet`
- Zaurus: Press the sync button on the cradle to start the hotplug process then,
- PC: `hotplug start`
- PC: `ifconfig usb0 192.168.129.200 netmask 255.255.255.255 up`
- PC: `route add –host 192.168.129.201 usb0`
- PC: telnet to the device and login as root

Similar steps were used for the iPaq.

[21] A more detailed explanation can be found at: **http://www.linux-forensics.com/linuxintro-LEFE-2.0.5.pdf**
[22] Additional information on connecting to Linux based PDAs can be found at: **http://www.linux-usb.org/USB-guide/c122.html**

Zaurus SL-5000

The following scenarios were conducted on the Zaurus SL-5000 running Lineo 2.4.6. In order to properly image the device a telnet connection was established. After the completing the connection and logging in as root, the following commands were executed, capturing the image on a Compact Flash (CF) card in a specified file (i.e., zaurus.dd.gz) for subsequent analysis: ·

- `dd if=/dev/mtdblock1 | gzip -c9 > /usr/mnt.rom/cf/home_zaurus.dd.gz`
- `dd if=/dev/ram1 | gzip -c9 > /usr/mnt.rom/cf/dev_zaurus.dd.gz`

Another approach to dump the contents of a Linux device is to use netcat (`nc`). Netcat is a UNIX utility that is able to read/write data across a TCP/UDP network connection. This technique allows examiners to extract data when the device card slot is occupied. The following steps allow the image to be stored on the machine acquiring the data from the device.

- *Open two terminals (T1 and T2) on the machine that is acquiring data from the device*
- *T1: telnet to the LNX2.4-SA*
- *T2:* `nc -l -p 9000 | dd of=/dir/filename.dd`
- *T1:* `dd if=/dev/mtdblock1 | nc 192.168.129.200 9000`

The following commands:
"`nc -l -p 9000 | dd of=/dir/filename.dd`" listens on port 9000 and takes the receiving data and pipes it to the second half of the specified above command, writing the output file to the specified directory.

"`dd if=/dev/mtdblock1 | nc 192.168.129.200 9000`" creates an image of the device and pipes the image to the specified IP/listening port.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took between 2 to 5 minutes. After acquisition, the image was examined via a standard hex editor and also mounted in loop-back mode and examined with various Linux freeware tools.

PIM Application Files: All active PIM information was found and reported. Most deleted PIM information was recovered except for e-mail messages ready to be sent upon a network connection.

Web/E-mail Applications: Not Applicable - The Zaurus device does not have built-in 802.11b networking capabilities.

Graphics File Formats: In order to view graphics files of various types (i.e., `.bmp`, `.jpg`, `.gif`, `.png`, `.tif`) contained on the device, the `dd` image was mounted in loop back mode. All the images were found, reported, and displayed using `gqview`.

Compressed File Archive Formats: Text files compressed with WinZip were found and reported using `grep`. Graphics files were found and reported using `gqview`, but not decompressed and displayed automatically.

Other Compressed Archive Formats: All files regardless of compression type (i.e., `.tar`, `.tar.gz`, `.tgz`, `.rar`, and `.exe`) were obtainable after acquisition. Text based files do not produce positive results on file content, but successfully show the filename and extension.

Deleted Files: The filename and remnants of file content of text files were recovered and reported using a hex editor. Remnants of graphics files were recovered and reported, but not able to be displayed. The results were the same both before and after synchronization.

Misnamed Files: All misnamed text files were found and reported using `grep`. Misnamed graphic files were found, reported, and displayed using `gqview`, regardless of file extension.

Peripheral Memory Cards: Not Applicable - Although `dd` could be run on the device to acquire the contents of the card onto another memory card and analyze the results with a forensic tool such as EnCase, making a forensically sound copy of the card on a forensic workstation is more straightforward and affects the device less.

Cleared Devices: A hard reset was performed on the device by removing the battery cover and pressing and holding the reset button. A CF card containing data was present. No previous data or personal information on the device was found after acquisition. The data contained on the CF card, however, was recoverable.

Password Protected Devices: Not Applicable - No password recovery tools were available to use. Though, a weakness in the encryption algorithm used on the Zaurus has been noted.[23]

IPaq 3970

The following scenarios were conducted on an iPaq 3970 running Familiar version 2.4.19 with OPIE version 1.0.2. In order to image the device an ssh connection was established and the following commands were executed, capturing the image on a Compact Flash (CF) card:

- `dd if=/dev/root of=/mnt/hda/opie.dd bs=1024 count=32256`
- `cardctl eject.`

In order to mount the resulting JFFS2 filesystem image in loopback mode, the proper patches must be applied to the Linux kernel of the PC. The JFFS2 patches were applied, but errors were returned when attempting to mount the image. For this reason, the technique could not be used in the scenarios below as was done previously for the Zaurus. Because the JFFS2 filesystem compresses file content, locating information manually was a difficult and tedious process. Therefore the results of the scenarios below could be improved with specialized tools capable of interpreting and decompressing the filesystem contents.

Device Content Acquisition: The device contents were successfully acquired. The acquisition process took between 2 to 5 minutes. After acquisition, the information was investigated via a standard hex editor.

[23] For more information see **http://xforce.iss.net/xforce/xfdb/9535**

PIM Application Files: All active PIM information was found and reported from the following files: `datebook.xml`, `addressbook.xml` and `todolist.xml`, which correspond respectively to the Calendar, Address Book, and ToDo List. Deleted PIM information was not recoverable.

Web/E-mail Applications: Not Applicable - The iPaq was not configured for wireless activity.

Graphics File Formats: Graphics files had to be identified manually by header/footer information. None of the graphics files were found, except for `.png` files.

Compressed File Archive Formats: Text and graphics files compressed with WinZip were found by manually locating and extracting the archive file by file header, then decompressing and displaying the data with an appropriate viewer.

Other Compressed Archive Formats: Text and graphics files in archive formats `.tar.gz`, `.tgz`, `.rar`, were found by manually locating and extracting the archive file, then decompressing the files and displaying the data with an appropriate viewer. Text and graphics files in archive formats `.tar` and `.exe` files were not able to be extracted and viewed with an appropriate viewer.

Deleted Files: The filename and remnants of file content of text files were recovered and reported, using a hex editor. Remnants of graphics files were recovered and reported, but not able to be displayed. The results were the same both before and after synchronization.

Misnamed Files: Misnamed text files were not found using a hex editor. Misnamed graphics files were found by manually locating and extracting the files by file header and displaying the data with an appropriate viewer. Except for `.png` files none of the graphics files were found.

Peripheral Memory Cards: Not Applicable - Although `dd` could be run on the device to acquire the contents of the card onto another memory card and analyze the results with a forensic tool such as EnCase, making a forensically sound copy of the card on a forensic workstation is more straightforward and affects the device less.

Cleared Devices: A hard reset was performed on the device by pressing buttons 1, 4, and the reset button. Some files on the device were found after acquisition with difficulty. To verify that no data was deleted from the device, information was examined directly on it via the user-interface. The data on the CF card was also recoverable.

Password Protected Devices: Not Applicable - Though vulnerabilities may exist with the Familiar distribution of Linux. No attempt was made at password recovery.

Summary

The tools studied in this report, while having their limitations, can significantly improve the efficiency of a knowledgeable examiner. The discussion and tables appearing in this chapter summarize the results for each tool studied, when compared against the predefined expectations defined earlier in Table 3. The entry "Meet" indicates that the software met the expectations of the scenario for the device in question. Similarly, "Below" indicates that the software fell short of fully meeting expectations; "Above" indicates that the software surpassed expectations; and "Miss" indicates that the software unsuccessfully met any expectations. "NA" indicates scenarios that were not applicable for the device.

Table 6 summarizes the scenario results for PDA Seizure. As seen from its contents, PDA Seizure demonstrated results that met or exceeded expectations in the majority of cases. On Palm OS devices, for those scenarios where outcomes were below expectations, all except one, involving memory cards on the Tungsten C, were related to deleted file recovery. Recovery of deleted files on PDAs depends on a number of factors including available memory space on the device, storage recovery algorithms, and hardware characteristics. Similarly, deleted file recovery was the situation that plagued Pocket PC devices, affecting all but two scenarios, Graphics File Formats and Misnamed Files. For the former scenario, `.tif` and `.png` graphic formatted files were not handled automatically as with other graphic formats and displayed in the graphics library. For the latter, misnamed file extensions were not able to be identified by file header/footer signatures.

Table 6: PDA Seizure – Scenario Outcome

Scenario	Device					
	Joranda 548	iPaq 38/39xx	iPaq 5400	Palm III/Vx	Visor	Tungsten C
Device Content Acquisition	Meet	Meet	Meet	Meet	Meet	Meet
PIM Applications	Meet	Meet	Miss[a]	Meet	Meet	Meet
Web/E-mail Applications	NA	NA	Meet	NA	NA	Meet
Graphics File Formats	Below[b]	Below[b]	Below[b]	Meet	Meet	Meet
Compressed File Archive Formats	Meet	Meet	Meet	NA	NA	NA
Other Compressed Archive Formats	Meet	Meet	Meet	NA	NA	NA
Deleted Files	Below[c]	Miss[d]	Miss[d]	Below[e]	Below[e]	Below[e]
Misnamed Files	Miss[f]	Miss[f]	Miss[f]	NA	NA	NA
Peripheral Memory Cards	Below[g]	Below[g]	Below[g]	NA	NA	Miss[h]
Cleared Devices	Meet	Meet	Meet	Meet	Above[i]	Above[i]

Scenario	Device					
	Joranda 548	iPaq 38/39xx	iPaq 5400	Palm III/Vx	Visor	Tungsten C
Password Protected Devices	NA	NA	NA	Meet	Meet	NA

[a] No PIM data was recovered
[b] Not all graphics formats were supported for display
[c] Some file-related information was recovered, but no file content
[d] No information about deleted files was recovered
[e] Some file-related information and file content was recovered, but not all
[f] Files with altered extensions were not recognized
[g] Deleted files were not recovered, but were recoverable through other means
[h] Memory card was not discovered and its contents acquired
[i] Surprisingly, some information was recovered after a hard reset of the device

EnCase produced results for Palm OS devices comparable to PDA Seizure as shown in Table 7. The one notable exception was that EnCase failed to acquire information from the Palm III device. However, the device was imaged with `pdd` and the output imported into EnCase to exercise the remaining scenarios. The same approach was followed to examine the Zaurus, a Linux device, for all but the Device Content Acquisition scenario. Recovery of deleted files again were the main cause of unmet expectations.

Table 7: EnCase – Scenario Outcome

Scenario	Device				
	Palm III	Palm Vx	Visor	Tungsten C	Zaurus
Device Content Acquisition	Miss[a]	Meet	Meet	Meet	NA[b]
PIM Applications	Meet	Meet	Meet	Meet	Meet
Web/E-mail Applications	NA	NA	NA	Meet	NA
Graphics File Formats	Meet	Meet	Meet	Meet	Meet
Compressed File Archive Formats	NA	NA	NA	NA	Meet
Other Compressed Archive Formats	NA	NA	NA	NA	Meet
Deleted Files	Below[c]	Below[c]	Below[c]	Below[c]	Below[c]
Misnamed Files	NA	NA	NA	NA	Meet
Peripheral Memory Cards	NA	NA	NA	Miss[d]	NA
Cleared Devices	Meet	Meet	Above[e]	Above[e]	Meet

Scenario	Device				
	Palm III	Palm Vx	Visor	Tungsten C	Zaurus
Password Protected Devices	NA	NA	NA	NA	NA

[a] Acquisition was performed using @stakes `pdd` utility, after EnCase was unsuccessful

[b] Acquisition was performed using the duplicate disk (`dd`) utility

[c] Some file related information was recovered, but not all

[d] Memory card was not discovered and its contents acquired

[e] Surprisingly, some information was recovered after a hard reset of the device

Table 8 below shows the scenario outcome for `dd` applied two Linux-based PDAs: Zaurus and an iPaq with the Familiar distribution of Linux installed. Because `dd` is no more than an acquisition tool, other utilities and techniques were used to examine the resulting image. This situation required more effort to complete the scenarios and also lacked tracking and reporting facilities provided by the complete forensic toolkits. Nevertheless, in the case of the Zaurus device, results were achieved that are comparable to those of EnCase. That was not true, however, in the case of the iPaq, since no automated means were available to interpret and decode the JFFS2 filesystem image for examination, which proved to be difficult manually. Ironically, the results for the iPaq should have been much better than reported, but was affected by the inability to decompress and extract manually all information located.

Table 8: Duplicate Disk (dd) – Scenario Outcome

Scenario	Device	
	Zaurus SL-5000	IPaq 3970
Device Content Acquisition	Meet	Meet
PIM Applications	Meet	Below[a]
Web/E-mail Applications	NA	NA
Graphics File Formats	Meet	Below[b]
Compressed File Archive Formats	Meet	Meet
Other Compressed Archive Formats	Meet	Below[c]
Deleted Files	Below[d]	Below[d]
Misnamed Files	Meet	Meet
Peripheral Memory Cards	NA	NA
Cleared Devices	Meet	Above[e]

Scenario	Device	
	Zaurus SL-5000	IPaq 3970
Password Protected Devices	NA	NA

[a] Only Partial PIM information was found

[b] File related information was discovered, but unable to display graphics except for `.png` files

[c] Some file related information was discovered, but unable to extract text and graphics files from .tar and .exe archives

[d] Some file-related information and file content was recovered, but not all

[e] Since the device maintains the filesystem in ROM, all information was recovered after a hard reset of the device

Conclusions

Forensic examination of PDA devices is a small part of computer forensics, in general. Consequentially, PDA forensic tools are a relatively recent development and in their early stages of maturity. While the tools discussed in this paper performed well and have adequate functionality, new versions can be expected to improve and therefore meet investigative requirements.

As with any software, it is important for an examiner to understand the functionality and scope of forensic tools being used. It is especially critical for an examiner to understand a tool's limitations and when to turn to other means of examination. Proper detailed documentation of the functionality of a tool is essential. However, practice with a tool in mock examinations can help the examiner gain an even better understanding of the tool's capabilities and limitations, which often involve subtle distinctions. It also provides the opportunity to customize facilities of the tool for later use.

Personal Digital Assistants are becoming ubiquitous and widely used for personal and business use. Hybrid devices such as PDAs doubling as a cell phone are also on the rise. New devices are becoming more affordable and accepted among the general public for both personal and business usage. The development of forensic software must evolve with technological advances in PDAs, allowing data from these devices to be acquired. This document provides a starting point on how data is acquired from PDA devices and associated removable media.