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

Draft Special Publication 800-72

Guidelines on PDA Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

NIST Draft Special Publication 800-72

Guidelines on PDA Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

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 20899-8930

August 2004

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

Technology Administration
Phillip J. Bond, Under Secretary 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 Special Publication 800-series reports on 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 Special Publication 800-72
Natl. Inst. Stand. Technol. Spec. Publ. 800-72, xx pages (Mon. 2004)
CODEN: XXXXX

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2002

Acknowledgements

The authors, Wayne Jansen and Rick Ayers from NIST wish to express their thanks to colleagues who reviewed drafts of this document. In particular, their appreciation goes to Murugiah Souppaya and Tim Grance from NIST, Karen Kent from Booz-Allen-Hamilton, Barry Grundy from NASA – Office of Inspector General, Rick Mislan from Ferris State University, and Eoghan Casey from Knowledge Solutions LLC for their research, technical support, and written contributions 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 and those who contributed input during the public comment period.

Table of Contents

TABLE OF CONTENTS V

LIST OF FIGURES VII

LIST OF TABLES VIII

EXECUTIVE SUMMARY 1

1. INTRODUCTION 2

1.1 AUTHORITY 2
1.2 PURPOSE AND SCOPE 2
1.3 AUDIENCE AND ASSUMPTIONS 3
1.4 DOCUMENT STRUCTURE 3

2. BACKGROUND 4

2.1 DEVICE CHARACTERISTICS 4
2.2 PALM OS 6
2.3 POCKET PC 9
2.4 LINUX 12
2.5 GENERIC STATES 14

3. FORENSIC TOOLS 16

3.1 PALM DD (PDD) 16
3.2 PILOT-LINK 17
3.3 POSE 17
3.4 PDA SEIZURE 18
3.5 ENCASE 18
3.6 DUPLICATE DISK (DD) 19
3.7 CUSTOM TOOLS 19

4. PROCEDURES AND PRINCIPLES 20

4.1 ROLES AND RESPONSIBILITIES 20
4.2 EVIDENTIAL PRINCIPLES 21
4.3 PROCEDURAL MODELS 22

5. PRESERVATION 25

5.1 SEARCH 27
5.2 RECOGNITION 27
5.3 DOCUMENTATION 28
5.4 COLLECTION 28

6. ACQUISITION 33

6.1 UNOBSTRUCTED DEVICES 34

6.2 OBSTRUCTED DEVICES 36
6.3 TANGENTIAL EQUIPMENT 39
7. EXAMINATION AND ANALYSIS 43
7.1 LOCATING EVIDENCE 43
7.2 APPLYING TOOLS 45
8. REPORTING 48
9. REFERENCES 50

List of Figures

Figure 1: Generic Hardware Diagram 5

Figure 2: Palm OS Architecture 8

Figure 3: Windows CE Architecture 10

Figure 4: Linux Architecture 13

Figure 5: Generic State Diagram 15

Figure 6: ROM/RAM Storage Assignments 35

Figure 7: Alternative ROM/RAM Assignments 36

List of Tables

Table 1: An Overview of Representative PDA models 5

Table 2: PDA Forensic Tools……. 16

Table 3: Action Matrix…….....30

Table 4: Interoperability Among POS Tools….....33

Table 5: Cross Reference of Sources vs Objectives. 44

Executive Summary

Forensic specialists periodically encounter unusual devices and new technologies normally not envisaged as having immediate relevance from a digital forensics perspective. Existing forensic guidelines lean heavily on classical computer forensics. The reason for most guides to limit the breadth of content is: technology changes at such a rapid pace. This guide provides an in-depth look into Personal Digital Assistants (PDAs) and explains technologies used in PDAs and their impact on the procedures for forensic specialists. It covers the characteristics of three families of devices: Pocket PC, Palm OS, and Linux based PDAs and the relevance of various operating systems associated. This guide deals with situations encountered during the collection and examination of digital information present on PDAs for preserving valuable evidence as well as available tools for acquisition and examination.

The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with PDAs, and to prepare forensic specialists to deal with new situations when they are encountered. The guide is not all-inclusive nor is it a mandate for the law enforcement community. However, from the principles outlined and other information provided, agencies should nevertheless find the guide helpful in setting policies and procedures.

The information in this guide is best applied in the context of current technology and practices. Every situation is unique, as are the experience of the forensic specialists and the tools and facilities at their disposal. The judgment of the forensic specialists should be given deference in the implementation of the procedures suggested in this guide. Circumstances of individual cases and International, Federal, State, local laws/rules and organization-specific policies may also require actions other than those described in this guide. As always, close and continuing consultation with legal council is advised.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this guide in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guide has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this guide should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

This guide provides basic information on PDAs, aspects desirable for law enforcement investigations and considerations when subjecting a PDA to an examination and analysis. The guide focuses mainly on the characteristics from the following families of PDAs: Pocket PC, Palm, and Linux based PDAs. It also covers provisions to be taken into consideration during the course of an incident or investigation. It includes discussion on evidence preservation, device identification, content acquisition, documentation and reporting.

The guide is intended to address common circumstances, involving computer based electronic data from PDAs and associated electronic media that may be encountered by organizational security staff and law enforcement investigators. It is also intended to compliment existing guidelines, which focus mainly on equipment seizure, and delve more deeply into issues related to PDAs and their examination and analysis.

Procedures and techniques presented in this document are a compilation of the authors' opinions and references taken from existing forensic guidelines. 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. Readers are advised to apply the recommended practices only after consultation with management and legal officials for compliance with laws and regulations (i.e., local, state, federal, and international) that pertain to their situation.

1.3 Audience and Assumptions

The intended audience is varied and ranges from response team members handling a computer security incident to organizational security officials investigating an employee-related situation to forensic examiners involved in criminal investigations. The practices recommended in this guide are designed to highlight key principles associated with the handling and examination of electronic evidence, in general, and PDAs in particular. Readers are assumed to have a basic grounding in classical computer forensics involving individual computer systems (e.g., personal computers) and network servers. Because of the constantly changing nature of handheld devices and related forensic procedures and tools, readers are expected to take advantage of other resources, including those listed in this guide, for more current and detailed information.

1.4 Document Structure

The guide is divided into the following nine sections:

- Section 1 (this section) describes an authority, purpose and scope, audience and assumptions, and document structure.
- Section 2 is an overview on PDAs, including an overview of common operating systems and generic operating states.
- Section 3 discusses present-day PDA forensic tools and with which types of devices they work.
- Section 4 provides general information on procedures and principles that apply to PDA forensics.
- Section 5 discusses considerations for preserving digital evidence associated with PDAs.
- Section 6 examines the process of acquisition of both obstructed and unobstructed devices, as well as common types of peripheral equipment.
- Section 7 outlines common sources of evidence on PDAs and the features and capabilities of tools for examination.
- Section 8 discusses the reporting of findings.
- Section 9 contains a list of references used in this guide.

2. Background

The digital forensic community faces a constant challenge to stay on top of the latest technologies that may be used to reveal relevant clues in an investigation. Personal Digital Assistants (PDAs) are commonplace in today's society, used by many individuals for both personal and professional purposes. PDAs vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. In the event that a PDA is encountered during an investigation, numerous questions arise: What should be done? How should the PDA be handled? How should valuable or potentially relevant data contained on the device be examined? The key to answering these questions is an understanding of the hardware and software characteristics of PDAs.

This section provides an overview of the hardware and software capabilities of Palm, Pocket PC, and Linux-based PDAs. The overview provides a summary of general characteristics and, where useful, focuses on a particular model or software version that best illustrates key features of such products. Developing an understanding of the components and inner workings of these devices (e.g., PC vs. PDA memory) is a pre-requisite to understanding the criticalities involved when dealing with digital devices. PDA memory is volatile (i.e., RAM) and requires power to maintain data unlike a personal computers hard disk. Handheld device technologies are changing rapidly, with new products and features being introduced regularly. Because of the fast pace with which handheld device technologies are evolving, this discussion represents a snapshot of the handheld area at the present time.

2.1 Device Characteristics

Most types of PDAs have comparable features and capabilities. They house a microprocessor, read only memory (ROM), random access memory (RAM), a variety of hardware keys and interfaces, and a touch sensitive, liquid crystal display. The operating system (OS) of the device is held in ROM. Several varieties of ROM are used, including Flash ROM, which can be erased and reprogrammed electronically with OS updates or an entirely different OS. 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 combination Secure Digital (SD) [1]/MultiMedia Card (MMC) [2] slots support memory cards and peripherals such as a digital camera or wireless communications card. Wireless communications such as infrared (i.e., IrDA) or Bluetooth may also be built in. Figure 1 presents a diagram representing the generic core components of most PDAs.

The latest high-end PDAs are equipped with system-level microprocessors that minimize the number of supporting chips and considerable memory capacity, giving the user the performance of a desktop machine.

[1] The Secure Digital home page can be found at: http://www.Sdcard.org

[2] The MultiMediaCard home page can be found at: http://www.mmca.org

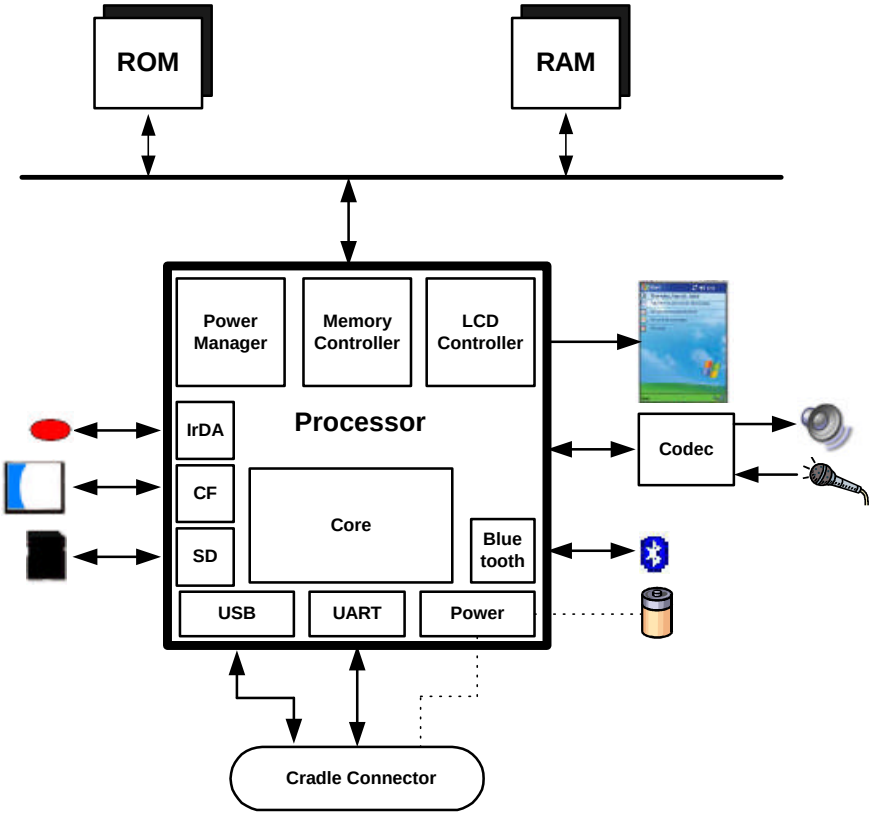

Figure 1: Generic Hardware Diagram

Different devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Devices also have expansion capabilities (e.g., I/O and memory card slots, device sleeves, and external hardware interfaces) that can occur between devices. Furthermore, PDA capabilities are sometimes combined with those of other devices such as cell phones, global positioning systems, and cameras to form new types of hybrid devices. Table 1 highlights the general characteristics of selected Palm, Pocket PC (re-branded as Windows Mobile in 2003), and Linux PDA models, which highlight this diversity. Characteristics of a wider range of PDAs can be found on manufacturer and vendor Web sites, as well as product review sites.[3,4]

Table 1: An Overview of Representative PDA models

	Tungsten T2	iPAQ Pocket PC H5555	Zaurus SL-5600
OS	Palm OS 5.2.1	Windows Mobile 2003 Premium	Linux Embedix v2.4.18, Qtopia v1.5.0
Processor	144 MHz TI OMAP 1510 Dual core 192 Mhz DSP enhanced ARM-based	400 MHz Intel XScale PXA-255	400 MHz Intel Xscale PXA-250

[3] For an online comparison of older PDA models see: http://www.davespda.com/resources/compare/

[4] For PDA product reviews and prices of current models see http://www.cnet.com

ROM	8 MB Flash	48 MB Flash (17 MB available for user storage)	64 MB Flash
RAM	32 MB	128 MB	32 MB
Size	4.0” x 3.0” x 0.6”	5.43" x 3.3" x .63"	6.2” x 3.2" x 0.8"
Display	320x320 TFT Active Matrix, 65,536 colors	240x320 Color reflective thin film transistor (TFT) LCD, 65,536 colors	480x640, 4’’ diagonal, 65,536 colors, CG Silicon LCD (transflective TFT)
Input	Touch-screen, Handwriting recognition, soft keyboard, voice	Touch-screen, Handwriting recognition, soft keyboard, voice, 5-way navigation button	Touch screen, Handwriting recognition, QWERTY keyboard
Wireless	IrDA, Bluetooth	IrDA, Bluetooth, Wi-Fi	IrDA
Card Slots	SD/MMC slot	SD/MMC slot Type II CF slot	SD/MMC slot Type II CF slot
Expansion	None	Optional expansion sleeves for PCMCIA cards, CF cards, and accessories	Expansion jacket with CF slot and battery USB 1.1 host connector (mini type A)
Battery	1 fixed, rechargeable Lithium Ion Polymer	1 removable, rechargeable Lithium Ion Polymer	1 removable, rechargeable Lithium Ion

Regardless of the PDA family, all devices support a set of basic Personal Information Management (PIM) applications, which provide Address Book, Appointment, Mailbox, and Memo Management capabilities. 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.

2.2 Palm OS

Palm established itself as the early leader in the PDA market. Early Palm OS devices use 16- and 32-bit processors (e.g., 32-bit processors process instructions on numbers that are 32-bits long) based on the Motorola DragonBall MC68328-family of microprocessors. More recent devices use StrongArm and XScale microprocessors.[5] Older Palm devices tend to be driven by alkaline batteries instead of lithium-ion batteries, used in new models.

The Palm OS is stored in ROM, while applications and user data are stored in RAM. Add-on utilities also exist to back up PIM data (e.g., Address Book, Datebook, ToDo, Memo Pad) onto available ROM. Palm OS system software logically organizes ROM and RAM for each Palm powered handheld into one or more memory modules known as a card. Each memory card can contain ROM, RAM, or both. A handheld device can have one card, multiple cards, or no cards. The main suite of applications provided with each Palm powered handheld is built into ROM. This design permits the user to replace the operating system and the entire application’s

[5] For Palm OS and device related material see http://www.palmsource.com/palmos/

suite by installing a single replacement module. Additional or replacement applications and system extensions can be loaded into RAM.

The Palm OS divides the total available RAM store into two logical areas: dynamic RAM and storage RAM. Dynamic RAM is used as working space for temporary allocations, and is analogous to the RAM installed in a typical desktop system. The remainder of the available RAM on the card is designated as storage RAM and is analogous to disk storage on a typical desktop system. Because power is always applied to the memory system, both areas of RAM preserve their contents when the handheld is turned "off" (i.e., is in low-power sleep mode). All of storage memory is preserved even when the handheld is reset explicitly. As part of the warm boot sequence (i.e., a soft reset), the system software reinitializes the dynamic area, and leaves the storage area intact. The entire dynamic area of RAM is used to implement a single heap that provides memory for dynamic allocations. From this dynamic heap, the system provides memory for dynamic data such as global variables, system dynamic allocations (TCP/IP, IrDA, and so on, as applicable), application stacks, temporary memory allocations, and application dynamic allocations. As part of the cold boot sequence (i.e., a hard reset), in addition to reinitializing the dynamic area, the storage area is erased [PPC04].

The Palm is arranged in memory chunks called “records,” which are grouped into “databases.” The Palm OS “databases” can be thought of as files. The Palm file format (PFF) conforms to one of the three types defined below:

- **Palm Database (PDB)** – A record database used to store application data, such as contact lists, or user specific data.

- **Palm Resource (PRC)** – A resource database similar to the PDB. The applications running on Palm OS are resources containing application code and user interface objects.

- **Palm Query Application (PQA)** – A Palm database containing world-wide-web content for use with Palm OS wireless devices.

With Palm OS, because all applications share the same dynamic RAM, they can interfere with each other’s data. Buffer overflow attacks are also easily implemented [Ket00].

The latest Palm PDAs offer two expansion modes providing an increase in functionality: the Palm Universal Connector System and Palm Expansion Card Slot. The Universal Connector System allows GPS receivers, wireless modems, keyboards, and other peripherals to interact with the device via a USB enabled connection. The Palm Expansion Card Slot accommodates MultiMediaCard (MMC) and Secure Digital (SD) cards. MMC card modules are removable solid-state memory of similar size and design to SD memory Cards. Besides memory, SD cards may also incorporate other types of peripherals such as wireless communications or camera cards.

The Palm OS is divided into the following layers: Application, Operating System, Software API, Hardware Drivers, and Hardware. Figure 2 illustrates the relationship between layers. The software Application Programming Interface (API) provides software developers with a degree of hardware independence, allowing applications to execute under different hardware environments by recompiling the application. Developers have the freedom to bypass the API and directly access the processor, providing more control of the processor and its functionality.

However, this comes at the expense of increased security risks due to malicious applications. The Palm OS does not implement permissions on code and data. Therefore, any application can access and modify data [Kin01].

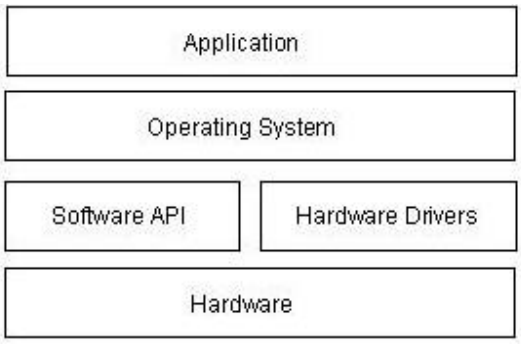

Figure 2: Palm OS Architecture

Other handheld device manufacturers have licensed the Palm OS for use in their own line of equipment. Versions of the Palm OS can be divided into three ranges: those before version 4.0, those from version 4.0 to 5.0, and those from 5.0 onward to version 6. A number of vulnerabilities were identified in versions before 4.0 and subsequently fixed. In particular, the user login password was shown to be vulnerable and easily reversed [Kin01]. Version 4.0 also introduced initial support for filesystems on removable memory cards. Versions before 5.0 execute only a single program at a time, while 5.0 and after support multiprocessing. Versions 5.0 and above switched emphasis away from the DragonBall family of microprocessors to the StrongArm family[6], with emulation support of legacy applications previously developed for DragonBall.

Palm OS devices offer built-in security features to provide protection for individual entries/records and the ability to lock the device when the user turns the device off. Locking individual records allow users to mark records as private and not be displayed unless the proper password is provided. However, records marked private can be accessed, read, and copied through other means [Ket00]. The ability to lock a device requires users to enter the correct password before access is granted to the application screen. In early versions of Palm OS, weak password encoding is easily reversed and the encoded block of data that contains the password during a HotSync can be intercepted [Kin01]. Third party products exist that provide users with the ability to encrypt sensitive data and enhance overall security [Pmd02].

Palm devices include an RS232-based "Palm Debugger" providing source and assembly level debugging, entered by issuing a keystroke combination. Two interfaces exist that monitor the serial port for communication. "Console Mode" interacts with a high-level debugger and is used mostly for manipulation of databases. "Debug Mode" is typically used for assembly- and register-level debugging [Kin01].

[6] For Palm OS and device related material see http://www.palmsource.com/palmos/

2.3 Pocket PC

Pocket PC grew out of the success of the Palm PDA and the realization that a market existed for similar devices that had more processing power and networking capabilities. Microsoft entered the handheld device market with the Windows CE (WinCE) operating system, which was later augmented with additional functionality to produce Pocket PC (PPC).[7] Windows CE supports a multi-tasking, multi-threaded environment, inherited by Pocket PC. Applications running under Windows CE are protected from interfering with each other through memory management [Ket00]. Windows CE and PPC have evolved in tandem from versions WinCE 2.0/PPC 2000 to WinCE 3.0/PPC 2002 to WinCE 4.1/PPC 2003 (PPC 2003 was re-branded as Windows Mobile 2003), through a number of feature upgrades. For example, early versions of ActiveSync were susceptible to brute force password attacks and DoS attacks when synchronizing over a network [Meu02] and subsequently corrected. Vulnerabilities present on earlier devices may provide a means of bypassing authentication mechanisms allowing forensic investigators to have access to data.

Pocket PC runs on a number of processors, but primarily appears on devices having Xscale, ARM, or SHx processors. Various Pocket PC devices have ROM ranging from 32 to 64MB and RAM ranging from 32 to 128MB. PIM and other user data normally reside in RAM, while the operating system and support applications reside in ROM. An additional filestore can be allocated in unused ROM and made available for backing up files from RAM. One or more card slots, such as a Compact Flash (CF) or Secure Digital (SD) card slots, are typically supported. Additionally, some manufactures provide expansion capabilities, such as extension sleeves or modules that allow other technologies to be incorporated. The majority of Pocket PC devices use a lithium-ion battery. In order to prevent data loss in the event that battery power is low the lithium-ion battery must be re-charged via the cradle, a power cable, or removed and replaced with a charged battery.

The architecture of Windows CE is shown in the Figure 3 below [Ges03]. The services are grouped in a number of modules, which can be included or excluded when building an image for a specific target system. Everything from the bottom up to the programming and communications interfaces level is part of the operating system; above that are the applications. Due to the majority of the Windows CE operating system being written in the C language, the kernel is portable to different processors (e.g., Manufactures produce PDAs with different processors such as: Shx, StrongArm, XScale, etc.) by recompiling the code for a specific architecture.

[7] For Windows CE/PPC device related material see http://www.microsoft.com/mobile/pocketpc/default.asp

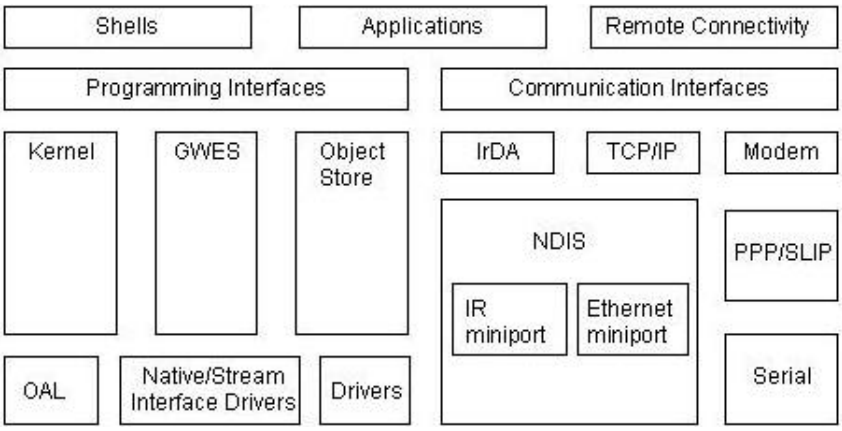

Figure 3: Windows CE Architecture

The Original Equipment Manufacturer (OEM) Adaptation Layer (OAL) is the layer between the Windows CE kernel and the hardware consisting of a set of functions related to system startup, interrupt handling, power management, profiling, timer and clock. It allows an OEM to adapt Windows CE to a specific platform. An OEM must write the OAL for any custom hardware present.

Like other operating systems, Microsoft Windows CE implements device drivers, whose purpose is to manage and interface with hardware devices. Device drivers link an OS and a device, making it possible for the OS to recognize the device and to allow communications to be established between hardware and applications. A device driver can be either monolithic or layered. Monolithic drivers implement their interface directly in terms of actions on the device they control. Layered drivers separate the implementation into two layers – an upper layer, which exposes the driver's native or stream interface, and a lower layer that performs the hardware interactions. Network drivers are based on the Network Driver Interface Specification (NDIS) model used by Windows NT. Only Miniport drivers are currently supported.

The Graphics, Windowing, and Events Subsystem (GWES) is the interface between the user, the application, and the operating system that contains most of the core Windows CE functionality. GWES is an integrated graphics device interface (GDI), window manager, and event manager. The GWES module is the most highly componentized portion of the Windows CE operating system and consists of two subgroups: User and GDI. User refers to the part of GWES that handles messages, events, and user input from keyboard and mouse or stylus. GDI refers to the part of GWES that is responsible for graphical output. The GDI is the GWES subsystem that controls how text and graphics are displayed. GDI is used to draw lines, curves, closed figures, text, and bitmap images.

The generic term – object store, refers to three types of persistent storage supported by Windows CE: file system, registry, and property databases. Standard Win32 functions provide access to the files and registry, while new Windows CE-specific API functions provide access to property databases and certain registry features. The subset of Win32 and other Microsoft APIs that have been implemented in Pocket PC allow a system to fulfill the requirements of an embedded PC application, yet keep the programmability similar to that of PCs. The maximum size of the object store is 256MB in Windows CE .NET. The object store is built on an

internal heap that resides in RAM, ROM, or both. The internal heap provides a transaction model that uses logging to ensure the integrity of the object store data.

The Windows CE file system allows a file to be stored both in RAM and ROM. When a file stored in RAM has the same name as a file stored in ROM, the actual RAM file shadows the ROM file. A user who tries to access a shadowed file gains access to only the RAM version. However, when the RAM version is deleted, the ROM version of the file is accessible. This feature is useful for upgrading files that come with a device as ROM files.

Property databases are repositories of information that can be stored, searched, and retrieved by associated applications. To reduce space, compression techniques are also applied automatically. These databases provide a common way to manage persistent information on the device.

The Windows CE registry is a database that stores information about applications, drivers, system configuration, user preferences, and other data. The purpose of the registry is to provide a single place for storing all the settings for the system, applications, and user. The registry is always stored in RAM and consequently is volatile. If there is no registry available in RAM, Windows CE can regenerate a default one from a file stored in ROM.

The Windows CE OS supports four types of memory:

- **RAM** – RAM is allocated into two separate areas: Object Store and Program Memory. The partitioning of main memory can be controlled by the end-user via an application level control and can be adjusted without rebooting. A paged virtual-memory management system is used to allocate program memory.

- **Expansion RAM** – is supported in addition to main system RAM providing users with extra storage. The Expansion RAM is mapped into virtual memory after a cold boot and appears identical in the virtual memory map to the OS as system RAM.

- **ROM** – The ROM memory space contains miscellaneous data files like audio files, fonts and bitmaps. These are generally compressed and decompressed when brought into system RAM for usage. The ROM memory space also contains support for uncompressed executables, applications and DLLs for eXecute In Place (XIP) operation. The Windows CE OS allows individual elements to be designated as XIP or demand paged during the image build process.

- **Persistent Storage** – Much of the support for persistent storage is oriented around removable storage cards. For example, files (executables, data, users files) stored in persistent storage are memory mapped into system RAM for use.

Pocket PC devices offer users the ability to set a power-on password that can be made up of a 4-digit numeric or a stronger alphanumeric password up to 29 characters long. Additionally, users have the ability to set a timeout that locks the device when not in use for the pre-defined specified amount of time. If passwords are incorrect, to discourage brute force attacks each new attempt takes longer. If a password is forgotten, the only way to unlock the device is by performing a hard-reset and re-synching data. Some recent models of Pocket PC devices have integrated a fingerprint biometric for additional security that can be used in tandem with 4-digit or alphanumeric passwords.

Pocket PC allows the hardware developer, system integrator, or developer to determine which services are incorporated in their Pocket PC version. Pocket PC devices do have the ability to incorporate trusted environments where the OS kernel verifies applications and libraries before loading them. Three possibilities exist: the software module may be trusted without restrictions, trusted with the restriction that no privileged function calls or registry access can be done, or not trusted at all [Aho01].

Pocket PC devices can have significantly different bootloader[8] functionality. The device manufacturer determines the range of functionality with two exceptions – the bootloader must be able to load the OS and have the ability to upgrade to a more recent OS. Some early versions of Pocket PC devices provided documentation on specific key chord sequences (e.g., pressing buttons 2, 4, power button, and the reset button) that would boot into a specific mode known as "Parrot mode." The device must be connected via the serial connector and a terminal emulator is used to establish communications with the bootloader and issue commands. Parrot mode has a rich command set that would allow register values to be set, display memory contents, set memory contents, display the virtual address mapping table, backup memory to storage cards (CF/SD), the ability to restore memory from storage, and many other operations.

2.4 Linux

Linux, a popular open source operating system for servers, which is used on desktop computers, has also appeared on a number of PDA devices. Linux is a true multi-tasking, 32-bit operating system that supports multi-threading. Besides commercial distributions that come preinstalled by PDA manufacturers, Linux distributions are also available for a range of Pocket PC and Palm OS devices. The success of Linux-based PDAs rests on the open source model and its ability to engage the software development community to produce useful applications.

The most common Linux PDA in the U.S. is the Sharp Zaurus. The first Zaurus model, the SL-5500, introduced a couple of years ago uses Embedix[9], an embedded Linux kernel from Lineo, and Qtopia desktop environment from Trolltech for the windowing and presentation technology. Embedix is based on a networked kernel with built-in support for WiFi, Bluetooth, and wireless modem technologies, as well as associated security and encryption modules. The device has a StrongARM processor, 16 MB of ROM, 64MB of RAM, and a 3.5-inch 240x320-pixel color LCD. As with Palm and PPC, the Zaurus' power source is a lithium-ion battery. There are both Compact Flash (CF) and SD slots (the SD slot will also accept MMC). A small QWERTY keyboard is integrated into the device and becomes visible by sliding down the thumb pad and application button panel.

Embeddix Linux refers to a commercial distribution. While most Linux distributions include the same utilities, libraries, drivers, and windowing frameworks, differences occur with what patches, modules, included utilities, and how the installation, configuration and upgrade is

[8] The bootloader is responsible for loading the run-time image into memory and jump to the OS startup routine.

[9] For more information on Embedix see http://www.lineo.com

performed. A minimal Embedded Linux system[10] requires three crucial elements: a boot utility, the Linux micro-kernel, and an initialization process. User applications based upon personal use can be added for self-customization of the device.

Linux distributions are also available for HP's iPAQ, Dell's Axim, and other PDAs but require the user to install over the existing OS. For example, iPAQ devices come pre-installed with Microsoft's Windows for Pocket PC. Linux can replace the Microsoft OS in the unit's flash ROM [Hal01, Zwi02]. A popular Linux distribution for the iPAQ is the Familiar[11] distribution, a lightweight package with Python and XFree86 with anti-aliased fonts, using the Blackbox window manager. Familiar also includes a packaging system called ipkg, which is like Redhat or Debian packages for desktop Linux. For the latest news on Linux-based handheld devices, Web sites should be monitored regularly. [12]

Figure 4 gives a conceptual architecture for the Linux operating system. The Linux operating system is responsible for memory management, process and thread creation, interprocess communication mechanisms, interrupt handling, execute-in-place (XIP) ROM filesystems, RAM filesystems, flash management, and TCP/IP networking.

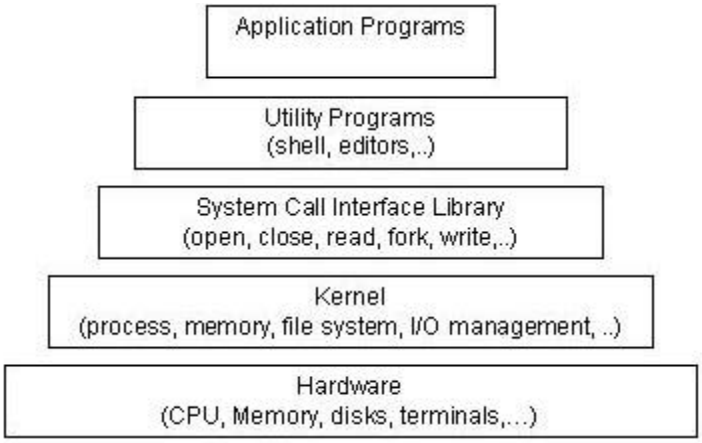

Figure 4: Linux Architecture

The Linux kernel is composed of modular components and subsystems that include device drivers, protocols, and other component types. The kernel also includes the scheduler, the memory manager, the virtual filesystem, and the resource allocator. APIs, programming interfaces that provide a standard method by which the Linux kernel can be expanded, glues these to the core of the Linux kernel. Data flows from the system call interface requesting a service from the file or process control subsystem, which in turn requests a service(s) from the hardware. The hardware then provides the service to the kernel and passes data back up through the kernel to the system call interface. Control flow is passed from the system call, to the appropriate subsystem, down to the hardware, and then back up to the system call interface.

---

[10] For more information on Embedded Linux Systems see http://www-106.ibm.com/developerworks/linux/library/l-embl.html

[11] For more information on the Familiar OS see http://familiar.handhelds.org for more information

[12] For the latest on Linux devices see http://www.linuxdevices.com

Concurrency issues, however, may allow the control of a process to be transferred to another during a context switch in either direction.

Linux offers comprehensive support for security that has been part of the operating system from the very beginning, including user identification and authentication, access control on files and directories based on owner (user/group/all), logging of security-relevant activities, and various levels of network encryption (Point-to-Point Tunneling Protocol (PPTP), IP Security Protocol (IPsec), Secure Shell (SSH) etc.) Processes running in Linux are also protected from interfering with other processes running on the same machine [Ket00]. Scaled down Linux operating systems that run on PDAs have been found to contain security vulnerabilities in design and implementation that affect system security. For example, the screen-locking passcode on the Zaurus that provides users with protection against unauthorized users, creates the same salt value[13] every time the passcode is set. This weakens security due to the ability to generate a passcode table and find consistent values to determine the device password [Cha02]. Third party security solutions exist and can be incorporated for additional security to device and file access.

The bootloader is firmware that is the first code to be executed upon powering on the device responsible for initializing hardware, arrange a block of contiguous physical memory for the kernel/root and loading the kernel and the root filesystem. Linux based PDA bootloaders tend to have a rich and well documented command set. For instance, documentation exists on handhelds.org that give step by step instructions on how one can convert a PPC based device into a Linux based device. Linux based bootloaders can accept serial connections or read a flash memory card, which enables Linux images to be transferred to the device and upgrades performed. Similarly, images can also be obtained via a serial connection or output to a memory card.

2.5 Generic States

The simplest view of a computing device, such as a desktop computer, is that it is in either an on or off state. However, further amplification is needed, particularly for PDAs, whose behavior is a bit more complex. Figure 5 gives a high level diagram that illustrates the various states in which a PDA can be at any time, along with the transitions that can occur to cause a change of state. While a more detailed state diagram is possible, the following four states provide a simple but comprehensive generic model that applies to most PDAs:

- **Nascent State –** Devices are in the nascent state when received from the manufacturer – the device contains no user data and observes factory configuration settings. The PDA must be charged to a minimum voltage level to be usable and gain initial entry to the nascent state, performed by holding down the power button to power on the device. Any user action transitions the device out of this state. This state can be attained again by performing a hard reset or letting the battery drain, which clears both the filesystem and dynamic working memory and restores factory settings.

- **Active State –** Devices that are in the active state are powered on, performing tasks, and able to be customized by the user and have their filesystems populated with data. If a soft reset is performed, the device returns back to the active state after clearing

[13] Salt values are used so that two identical passwords yield a different hash/numerical value.

working memory. If user authentication mechanisms are enabled, they are asserted on transition to this state.

- **Quiescent State –** The quiescent state is a dormant mode that conserves battery life while maintaining user data and performing other background functions. Context information for the device is preserved in memory to allow a quick resumption of processing when returning to the active state. Pressing the power button when in an active or semi-active state to power off the device, or the triggering of an inactivity timer when in the semi-active state causes a transition to the quiescent state.

- **Semi-Active State –** The semi-active state is a state in between active and quiescent. The state is reached by a timer, which is triggered after a period of inactivity allowing battery life to be preserved by dimming the display and taking other appropriate actions. The semi-active state returns to the active state when a screen-tap or a soft reset occurs. Devices that do not support a semi-active state need only a single inactivity timer for a transition from active to quiescent state.

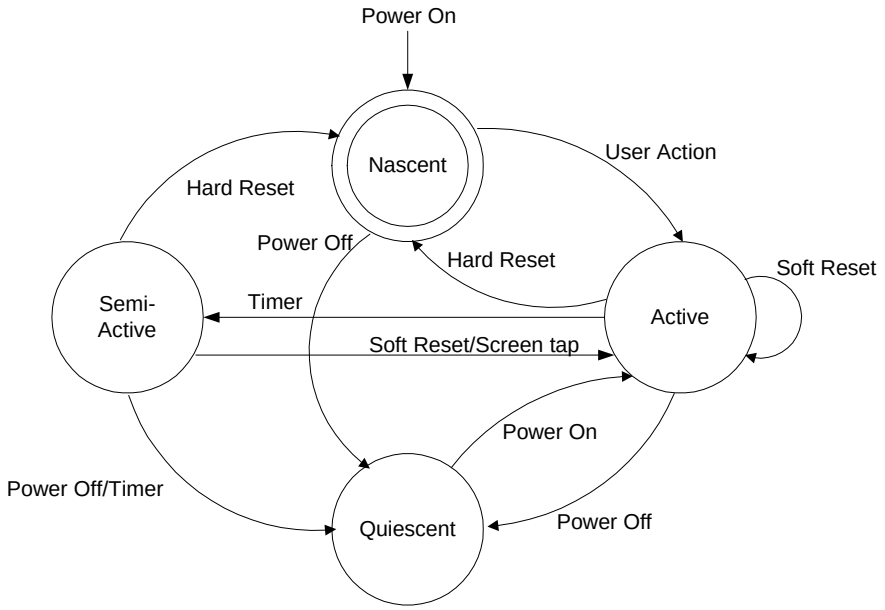

Figure 5: Generic State Diagram

The bottom line is simple – *a PDA device with sufficient battery power is never really turned off, since processes are active even when no visible cues are present.* For discussion purposes, a device can be said to be "off" if it is in the quiescent state and "on" if it is in any of the remaining states. Similarly, a device can be said to be "cleared" and devoid of data when in the nascent state, though slight deviations can apply. For example, some of the more recent PDAs are beginning to include a feature to backup important PIM data on flash memory, where it can be retained and restored if a hard reset is performed on the device. In addition, some Linux handheld distributions, such as the Familiar distribution from handhelds.org, use flash memory for their filesystem to avoid loss of data when a hard reset occurs. In such situations, the nascent state must be interpreted accordingly.

3. Forensic Tools

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. Linux based devices can be imaged with dd and analyzed with the use of a compatible tool (e.g., EnCase). Since Palm OS devices have been around the longest, more forensics tools are available for them than for other device families. Table 2 lists open-source and commercially available tools known to the authors and the facilities they provide: acquisition, examination, or reporting. The abbreviation NA means that the tool at the left of the row is not applicable to the device at top of the column. With one exception (i.e. versions of Palm OS prior to 4.0), these tools require that the examiner have unobstructed access to the device to acquire its contents.

Table 2: PDA Forensic Tools

	Palm OS	**Pocket PC**	**Linux PDA**
pdd	Acquisition	NA	NA
Pilot-Link	Acquisition	NA	NA
POSE	Examination	NA	NA
PDA Seizure	Acquisition, Examination, Reporting	Acquisition, Examination, Reporting	NA
Encase	Acquisition, Examination, Reporting	NA	Examination, Reporting
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., a filesystem partition). 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 in raw form by the processor and other related hardware components (i.e., a physical view).

Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present (e.g., unallocated RAM or unused filesystem space) to be examined, which otherwise would go unaccounted. Physical device images are generally more easily imported into another tool for examination and reporting. However, a logical structure has the advantage that it is a more natural organization to understand and use during examination. Thus, it is preferable to do both types of acquisition, if possible.

3.1 Palm dd (pdd)

Palm dd (pdd) is a Windows-based command line tool that performs a physical acquisition of information from Palm OS devices [Gra02]. PDA Seizure utilizes pdd version 1.10 to extract information from a Palm OS device. pdd is designed to work with the majority of PDAs

running the Palm OS in 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 contains device-specific information, and the 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. pdd does not provide hash values for the information acquired. However, a separate procedure can be used to obtain needed hash values. As of January 2003, pdd is no longer supported, however, version 1.11 source code is available and should remain available for use, as defined in the included license.

3.2 Pilot-Link

Pilot-link 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 use the Hotsync protocol. The two programs of interest to forensic specialists 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 POSE, a compatible forensics tool such as EnCase, or with 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.

3.3 POSE

POSE (Palm OS Emulator) 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 is loaded into it. The emulator program imitates the hardware of a DragonBall processor. Built-in PIM applications (e.g., Datebook, Address Book, To Do, 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 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 device it is emulating, over a looped back serial connection or a redirected TCP/IP connection.

3.4 PDA Seizure

Paraben's PDA Seizure version 2.5.0.0 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 acquire a forensic image of Palm and Pocket PC devices, to perform examiner-defined searches on data contained within acquired files, generate hash values of individual 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. 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, used to access unallocated regions of memory on the device. To access the remaining information, PDA Seizure utilizes the Remote API (RAPI) protocol, which provides a set of functions for desktop applications to communicate with and logically access information. For Palm devices, the PDA must first be put into a debug mode, commonly referred to as console mode, and all active HotSync applications must be closed. Once the memory image of a POS device is acquired, the user is 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.

3.5 EnCase

EnCase version 4.15 is a well-known forensic software toolkit that provides acquisition of suspect media, search and analytical tools, hash generation of individual files, 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, but the ability to import a data dump of Linux based PDAs exists. 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.

3.6 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. As one of the original Unix utilities, dd has been around in one form or another for decades. 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. However, if used incorrectly, dd may destroy 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 analysis. The standard version of dd does not provide hash values for the information acquired. However, a separate procedure can be used to obtain needed hash values.

3.7 Custom Tools

Where possible, established procedures should guide the technical process of acquisition, as well as the examination of evidence. However, some situations demand specialized procedures and methods be applied. Procedures must be tested to ensure that the results obtained are valid and independently reproducible. The development and validation of the procedures should be documented and includes the following steps [DOJ04]:

- Identifying the task or problem
- Proposing possible solutions
- Testing each solution on an identical test device and under known control conditions
- Evaluating the results of the test
- Finalizing the procedure

4. Procedures and Principles

Investigations and incidents are handled in various ways depending upon the circumstances of the incident, the gravity of the incident, and the preparation and experience of the investigation team. Digital investigations are comparable to crime scenes where investigative techniques used by law enforcement have been applied as a foundation for the creation of procedures used when dealing with digital evidence. This section provides an overview of various procedural models and principles that have been proposed.

4.1 Roles and Responsibilities

Regardless of the type of incident, the various types of roles involved are similar. Planning for incidents should address how existing personnel fulfill these roles when responding and conducting an investigation. A generic set of roles and associated responsibilities can be identified. They include First Responders, Investigators, Technicians, Forensic Examiners, and Forensic Analysts. In a given situation, a single individual may perform more than one role. Nevertheless, it is useful to distinguish distinct roles and their associated responsibilities.

First Responders are trained personnel who arrive first on the scene of an incident, provide an initial assessment, and activate the appropriate level of response. The responsibilities of First Responders are to secure the incident scene, call for the appropriate support needed, and assist with evidence collection.

Investigators plan and manage preservation, acquisition, examination, analysis, and reporting of electronic evidence. The Lead Investigator is in charge of making sure that activities at the scene of an incident are executed in the right order and at the right time. The Lead Investigator maybe responsible for developing the evidence, preparing a case report, and briefing any findings and determinations to senior officials.

Technicians carry out actions at the direction of the Lead Investigator. Technicians are responsible for identifying and collecting evidence and documenting the incident scene. They are specially trained personnel who seize electronic equipment and acquire digital images resident within memory. More than one technician is typically involved in an incident, because different skills and knowledge are needed. Sufficient expertise should be available at the scene to address all distinct digital apparatus involved in the incident.

Evidence Custodians protect all evidence gathered that is stored in a central location. They accept any evidence that is collected by Technicians, ensure that it is properly tagged, check it into and out of protective custody, and maintain a strict chain of custody.

Forensic Examiners are specially trained personnel who reproduce images acquired from seized equipment and recover digital data. Examiners make the data visible. Examiners may also acquire additional, more elusive data from a seized device, using highly specialized equipment, intensive reverse engineering, or other appropriate means unavailable to Forensic Technicians.

Forensic Analysts evaluate at the product of the Forensic Examiner for its significance and probative value to the case.

4.2 Evidential Principles

As a backdrop to any investigation basic principals have been proposed for dealing with digital evidence. Digital evidence has both physical and logical aspects. The physical side of it involves hardware components, peripherals, and media, which may contain data or the means to access it, while the logical side deals with the raw data extracted from a relevant information source. The Good Practice Guide for Computer based Electronic Evidence [ACPO2] suggests four principles when dealing with digital evidence.

- No actions performed by investigators should alter/modify data contained on digital devices.
- Individuals accessing original data must be trained and have the ability to explain their actions.
- An audit trail must be created, documenting each investigative step.
- The Authoritative figure is responsible for ensuring the above-mentioned procedures are followed.

The Proposed Standards for the Exchange of Digital Evidence [IOCE], suggest a similar set of principals for the standardized recovery of computer-based evidence:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

The above sets of principles aim to ensure the integrity and accountability of digital evidence through its entire life cycle. Proper handling of evidence is always vital for it to be admissible in a judicial proceeding. However, different standards often apply to different types of investigations: “The level of training and expertise required to execute a forensics task will largely depend on the level of evidence required in the case.

The Daubert method, a set of standards that serve as a guide when dealing with evidence in a court of law, proposes a number of reliability factors, which should be kept in mind when applying and reporting about a scientific technique used [Oco04]:

- **Testability** – Has the scientific theory or technique been empirically tested? According to K. Popper (1989) in The Growth of Scientific Knowledge, "the criterion on the scientific status of a theory is its falsifiability, refutability, and testability."

- **Acceptance** – Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.

- **Error Rate** – What is the known or potential error rate? Scientific measures generally have associated error rates, which can be estimated with a fair amount of precision. Known threats exist against the validity and reliability in any test (experimental and quasi-experimental) of a theory.

- **Credibility** – What is the expert's qualifications and stature in the scientific community? Does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?

- **Clarity** – Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This criterion is assumed to be incorporated in Daubert implicitly.

In general, even outside of law enforcement investigations, evidence should be collected in a manner that makes it likely that the evidence could be admissible in court. It may not be obvious when an investigation is initiated, for example, when a computer security incident is first detected, that a court action will ensue. Important evidence might be overlooked, improperly handled, or accidentally destroyed before the seriousness of the incident is realized.

4.3 Procedural Models

The Electronic Crime Scene Investigation – A Guide for First Responders, produced by the U.S. Department of Justice [DOJ01], offers the following suggestions when approaching a digital crime scene.

- **Secure and Evaluate the Scene** – Steps should be taken to ensure the safety of individuals and protecting the integrity of evidence.

- **Document the Scene** – An ongoing process that creates a record of the scene to be recorded for reporting.

- **Evidence Collection** – Collection of traditional and digital evidence without damaging or altering the integrity of the evidence.

- **Packaging, Transportation, and Storage** – Documentation of packaged evidence should be performed maintaining chain of custody.

Incident Response [Man01], an "Incident Response Methodology" proposes the following phases when encountering an incident or performing a digital investigation.

- **Pre-incident preparation** – Training, education, and understanding on how to respond to an incident.

- **Detection of incidents** – Develop techniques on how to detect suspect activities.

- **Initial Response** – Confirm that an incident has occurred and obtain volatile evidence.

- **Response strategy formulation** – Respond to incident based upon knowledge of all known facts collected from the Initial Response phase.
- **Duplication (forensic backups)** – Based upon the scenario, either create a physical forensic image or a live retrieval of evidence.
- **Investigation** – Determine what happened, who did it and how the incident can be prevented in the future.
- **Security measure implementation** – Apply security measures to isolate and contain infected systems.
- **Network monitoring** – Monitor network traffic for ongoing or additional attacks.
- **Recovery** – Restoration of the victim system to a secure, operational state.
- **Reporting** – Document all of the details and investigative steps taken throughout the incident.
- **Follow-up** – Learn from the incident by reviewing how and why it happened and make necessary adjustments.

Research conducted at the U.S. Air Force [USAF] proposes the following steps when dealing with a forensic investigation.

- **Identification** – Recognize and determine the type of incident.
- **Preparation** – Prepare tools, techniques, search warrants, authorizations, and management approval.
- **Approach Strategy** – Maximize untainted evidence collection while minimizing the impact upon the victim.
- **Preservation** – Isolate, secure and preserve the state of physical and digital evidence.
- **Collection** – Record the physical scene and duplicate digital evidence.
- **Examination** – Search for evidence relating to the suspected crime.
- **Analysis** – Determine significance, reconstruct fragments of data and draw conclusions based on the evidence found. The Analysis phase may go through numerous iterations until a theory has been supported.
- **Presentation** – Summarize and provide an explanation of conclusions.
- **Return Evidence** – Ensure physical and digital property is returned to the proper owner.

Each of the above procedural models and evidential principals contains key points that should be considered when dealing with digital evidence. Every incident or investigation is distinct and, therefore, it is difficult to prescribe a definitive A to Z approach. The remaining sections

follow a simple framework of four topical areas: obtaining an exhibit, making a forensic copy of its contents, obtaining evidence from the forensic copy, and reporting on the evidence obtained and process used. They are respectively referred to within this document as *preservation*, *acquisition*, *examination and analysis*, and *reporting*.

5. Preservation

Evidence preservation is the process of seizing suspect property without altering or changing the contents of data that reside on devices and removable media. It is the first step in digital evidence recovery. The section begins with a generic introduction to preservation then provides a more in-depth look at PDA-specific guidance.

Preservation involves the search, recognition, documentation, and collection of electronic based evidence. In order to use evidence successfully, whether in a court of law or a less formal proceeding, it must be preserved. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially loosing permanently valuable information about an incident.

The DOJ's Electronic Crime Scene Investigation report covers this subject in detail [DOJ01]. The guide offers principles, policies, and procedures to follow when encountering a digital evidence scene. The reader is directed to that report for additional information. The following is a summary of the key points to observe.

- **Securing and Evaluating the Scene:**
  - Ensure the safety of all individuals at the scene.
  - Protect the integrity of traditional and electronic evidence.
  - Evaluate the scene and formulate a search plan.
  - Identify potential evidence.
  - All potential evidence should be secured, documented and/or photographed.
  - Conduct interviews.
- **Documenting the Scene**
  - Create a permanent historical record of the scene.
  - Accurately record the location and condition of computers, storage media, other digital devices, and conventional evidence.
  - Document the condition and location of the computer system, including power status of the computer (on, off, or in sleep mode).
  - Identify and document related electronic components that will not be collected.
  - Photograph the entire scene to create a visual record as noted by the first responder.
- **Collecting Evidence**

- Handle computer evidence, whether physical or digital, in a manner that preserves its evidentiary value.

- Recover non-electronic evidence (e.g., written passwords, handwritten notes, bland pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs).

- **Packaging, Transporting, and Storing Evidence**

  - Take no actions to add, modify, or destroy data stored on a computer or other media.

  - Avoid high temperatures and humidity, physical shock, static electricity, and magnetic sources.

  - Maintain chain of custody of electronic evidence, document its packaging, transportation and storage.

    - ***Packaging Procedure***

      - Properly document, label, and inventory evidence before packaging.

      - Pack magnetic media in antistatic packaging (paper or antistatic plastic bags).

      - Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, removable media, etc.

      - Properly label evidence containers.

    - ***Transportation Procedure***

      - Avoid magnetic sources (e.g., radio transmitters, speaker magnets).

      - Avoid conditions of excessive heat, cold, or humidity while in transit.

      - Avoid shock and excessive vibrations.

    - ***Storage Procedures***

      - Ensure evidence is inventoried in accordance with authoritative policies.

      - Store evidence material in a secure area away from temperature and humidity extremes.

      - Protect evidence material from magnetic sources, moisture, dust, and other harmful particles or contaminants.

The remaining subsections provide supplemental information related to PDAs, following the paradigm of search, recognition, documentation, and collection.

5.1 Search

When the investigator and forensic technicians arrive at the scene with the appropriate authorization to examine the suspect's surroundings (e.g., a search warrant, consent from the owner), they should proceed cautiously and follow the necessary steps to ensure that the device arrives at the forensics laboratory without data depletion. Incorrect procedures during the seizure can cause critical information to be lost. Awareness of device specific issues and an understanding of various families of devices and their characteristics and accessories (e.g., power consumption, battery type, cradles, and power supplies) are essential.

For PDAs, evidence sources include: the device, device cradle, power supply, and associated peripherals, media, and accessories. Removable media varies from the size of a stamp to a stick of gum, which can be hidden and extremely difficult to find. Most often removable media can be identified through the number and placement of pins or pin receptacles located on the media that establish an interface with the device. The surrounding area and rooms other than where the device was found should be searched to ensure related evidence is not overlooked. Equipment associated with the PDA, such as memory cards or PC's synched with the PDA, may hold more valuable than the PDA itself.

By accident or deliberate action, electronic equipment may be found in a damaged state. Devices or media with visible external damage do not necessarily prevent data from being extracted from them. Damaged equipment should be taken back to the lab for further investigation. It may be possible to repair damaged components on a device and restore it to working order for examination and analysis. The memory components may also be repaired/examined locally, or removed and examined by a specially trained examiner.

5.2 Recognition

In order to proceed effectively, the exact type of device must be identified. Suspects may attempt to thwart specialists by altering the device to conceal its true identity. Device alteration could range from removing manufacturer labels to filing off logos. In addition, the operating system may be modified or completely replaced and appear differently, as well as behave differently than before.

If digital devices such as PDAs are in the "on" state the type of device can be identified by the operating system, which is more consistent in device identity rather than a logo. Though the two dominant operating systems are Pocket PC and Palm OS, PDAs that are manufactured to run one OS have the ability to run an alternative operating system. For example, distributions of Linux available from handhelds.org can be loaded and run on a variety of Pocket PC devices. Similarly, versions of Linux, such as Linux DA, exist for Palm OS devices.

Each Operating System has particular applications intertwined within the main GUI (Graphical User Interface) i.e. icons such as Word, Explorer, Memo Pad, Terminal, etc. Other clues that allow identification of a device are the following: the cradle interface, manufacturer serial number, the cradle type, power supply, etc. Any synchronization software discovered on an associated PC also helps to differentiate among operating system families.

5.3 Documentation

Evidence must be accurately accounted for and identified. The labeling process should document: the case number, a brief description, signature, and the date and time the evidence was collected. Additionally, the crime scene should be photographed alongside a report documenting the state of each digital device/personal computer (personal computers may contain useful data that has not been synchronized with the owners PDA). This is helpful if questioned about the environment at a later time [Kru01].

A record of all visible data should be created. All digital devices (PDAs) that may possibly store data should be photographed with all peripherals cables, cradles, power connectors, removable media, and connections. If the device is in an active or semi-active state the contents screen should be photographed and, if necessary, recorded manually. Other characteristics such as any LED activity (e.g., blinking) or physical connectivity should also be noted. It is desirable to have an individual in charge to perform evidence custodian duties at the scene alongside a partner responsible for documentation of evidence, during the collection phase [Kru01].

Actions taken on the system to view and record other undisplayed volatile data affect the remaining evidence. For example, running an application to view memory allocation or running processes will overwrite parts of memory. Moreover, it risks activating Trojan horse code hidden within the application.

The chain of custody procedure is a simple yet effective process of documenting the complete journey of evidence through the life of the case. Carefully maintaining the chain of custody not only protects the integrity of evidence, but also makes if difficult for a defense attorney to successfully argue that the evidence was tampered with [Kru01]. It should answer the following questions:

- Who collected it? (i.e., devices, media, associated peripherals, etc.)
- How and where? (i.e., how was the evidence collected and where it was located)
- Who took possession of it? (i.e., individual in charge of seizing evidence)
- How was it stored and protected in storage? (i.e., evidence-custodian procedures)
- Who took it out of storage and why? (i.e., on-going documentation of individuals name and purpose for checking-out evidence)

Documentation to all of the above questions must be maintained and filed in a secure location for current and future reference.

5.4 Collection

The collection process often involves dynamic and volatile information that may be lost unless precautions are taken at the scene of the incident or crime. The “Good Practice Guide for Computer Based Electronic Evidence” guide [ACPO] suggests the following procedures when dealing PDAs:

- On seizure, the PDA should not be switched on.
- To prevent the PDA from being accessed while still sealed in the evidence bag, it should be placed in an envelope then sealed before being put into an evidence bag.
- Where the PDA is fitted with only a single rechargeable battery, the appropriate power adaptor should be connected to the device with the cable passing through the evidence bag so that it can be kept on charge.
- If the PDA is switched on when found, consideration should be given to switching it off in order to preserve battery life, noting of the time and date of the process and documentation/photographs of the current device state before packaging as above.
- A search should be conducted for associated memory devices, such as SD, MMC, or CF semiconductor cards, microdrives, and USB tokens.
- Any power leads, cables, or cradles relating to the PDA should also be seized, as well as manuals.

PDAs maintain user data in a volatile state powered by either an alkaline or lithium ion battery source. The device design determines the type of battery source provided; batteries may be rechargeable or replaceable. If devices lose power over a specific time frame, the chances of recovering all data from the seized device are minuscule. Before a technician can bag and tag digital devices, the present power state must be considered. For example, the device may be receiving power from a cradle plugged into an outlet and fully charged, the suspect may have recently removed the batteries out of the device to clear memory, or the device may be extremely low on battery power.

In cases where devices are powered by alkaline batteries, fresh batteries should be inserted lessening the chance of data loss before seizing the evidence without altering the state of the device. Installing fresh batteries is a normal routine for PDA users especially those that run alkaline based devices, but there are risks involved. Pulling the batteries out and installing new batteries alters the state of the device; therefore, it is vital that the technician take note of the current state of the device along with photographs of the current device state beforehand.

Devices powered by a lithium-ion battery source should either be plugged into a compatible cradle, keeping a charge to the battery, or a new lithium-ion battery should be inserted. Lithium-ion based devices usually have a cigarette-lighter cable that will allow an evidence custodian to keep charge to the device while in transit. PDAs keep a small capacitance charge to the device allowing volatile data to remain safe for a short amount of time during battery replacement. In order to take advantage of this, batteries must be replaced quickly to prevent loss of data. If the device is powered on, a photograph of the current state of the device should be taken. If possible the current state of the device should not be altered until arrival at the forensic lab.

5.4.1 Other Conditions

Besides the battery level, many other factors can influence the actions a technician takes in a given situation to preserve evidence when the device is found in the on state. They include whether the device is cradled, is synchronizing with or communicating through a host computer, has an active wireless transmitter, and so on. Table 3 provides a list of common

conditions and associated actions for the forensic technician to consider in meeting the identified goal.

Table 3: Action Matrix

Index	Condition/Goal	Actions
1	**Device on** - Maintain device in active state and with an adequate power level - Acquire image at earliest opportunity	- If the power level is low, immediately replace batteries or charge with the proper device power adaptor - Create an image of the device - Leave the device on - Maintain an adequate power level with the proper device power adaptor or replacement batteries
2	**Device off** - Acquire image at earliest opportunity	- Leave the device in the off state - Power the device on and check current battery power (Lead investigator must give authority) - See condition 1
3	**Device in cradle** - Eliminate the possibility of further communication activity	- Pull the USB/serial interface connection from the PC - If the device is on, see condition 1 - If the device is off, see condition 2 - Seize the cradle and cords
4	**Device out of cradle** - Collect related evidence material	- If the device is on, see condition 1 - If the device is off, see condition 2 - Seize the cradle and cords
5	**Wireless (WiFi, Bluetooth, etc.) on** - Eliminate the possibility of further communication activity	- See condition 1 - Properly package the device in an envelope, anti-static bag, and an isolation envelope, eliminating the possibility of connectivity from another machine/device - Remove wireless enabled cards
6	**Wireless (WiFi, Bluetooth, etc.) off** - Collect related evidence material	- See condition 1 - Properly package the device to eliminate wireless activity from occurring - Remove wireless enabled cards
7	**Card in expansion card slot(s)** - Avoid triggering further activity within the device	- Avoid removing any peripheral/media cards (e.g., CF, SD, MMC)
8	**Card not in expansion card slot(s)** - Collect related evidence material	- Seize any associated peripheral/media cards (e.g., CF, SD, MMC)

9	**Expansion sleeve attached** - Avoid triggering further activity within the device	- Avoid removing the expansion sleeve - Avoid removing any peripheral/media cards (e.g., CF, SD, MMC) from the sleeve - If wireless/networked connectivity is occurring see condition 5
10	**Expansion sleeve removed** - Collect related evidence material	- Seize the expansion sleeve - Seize any associated peripherals/media cards (e.g., CF, SD, MMC)

5.4.2 Modified Devices

A number of considerations need to be made when handling a device. For example, pressing the power button, synchronization button or the usual contacts, calendar, to-do list, and tasks PIM buttons on the device could potentially trigger an alteration of state. More interesting, however, are the modifications to the software applications and operating system that can be made to the device from these actions. The following is a list of common classes of modifications that can occur:

- **Key Remapping** – It is relatively straightforward to remap a hardware key to perform a different function than the default. In general, a key press or combination of key presses can be made to launch an arbitrary program.

- **Malicious Programs** – Common utilities or functions can be replaced with versions that contain a Trojan horse designed to alter or damage data present on the device. For example, tools exist that allow users to capture, update, and replace ROM images with preferred applications, such as improved Web browsers. Trojan-bearing programs could conditionally be activated or suppressed based on conditions such as input parameters or hardware key interrupts. Watchdog applications could also be written to listen for specific key chord events and carry out actions such as wiping the device clean.

- **Security Enhancements** – Many organizations and individuals enhance their handheld devices with add-on security mechanisms. A variety of visual login, biometric, and token-based authentication mechanisms are available for use as replacements or supplements to password mechanisms. Improper interaction with a mechanism could cause the device to lock down and even destroy its contents. This is particularly a concern with security tokens whose presence is constantly monitored and whose removal from a card slot or other device interface is immediately acted upon.

5.4.3 Transport and Storage

Once the device is ready to be seized, the forensic specialists should seal the device in a static proof bag and tag it. Isolation bags also exist for shielding a device's radio transmission. The individual who seizes the device must sign and date the tag to initiate a chain of custody. The device may also be packaged to allow a power adaptor to be connected to the device through a hole in the bag, as a means for keeping the power level high. Digital devices are fragile and easily damaged. When a device is transported it should be handled carefully and adequately

protected from shock, breakage, and extreme temperature. Due to the volatile state of PDAs, they should immediately be checked into a forensic laboratory to be processed and the evidence custodian made aware of the situation. Battery powered devices held in storage for more than a few days risk power depletion and data loss, unless steps are taken to avoid this outcome.

Storage facilities that hold evidence should provide a cool, dry environment appropriate for valuable electronic equipment. All evidence should be in sealed containers, in a secure area with limited access.

6. Acquisition

Acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media. Acquisition should occur at a forensics laboratory once the seized information has been safely checked in. The advantage of performing acquisition at the scene is that loss of information due to battery depletion, damage, etc. is avoided. However, finding a controlled setting in which to work, having the appropriate equipment, and satisfying other prerequisites may not occur at the scene, but instead be available within a laboratory setting. For the purpose of the discussion, in this section a laboratory environment is presumed.

Once the device has arrived at the forensic laboratory, the forensics examiner begins the acquisition with identification of the device. The type of device and operating system present on the device determines the route to take for the creation of a sound bit-for-bit image or otherwise acquiring the contents of the device. Only a few different forensic software tools that image PDAs currently exist and no one application at this moment handles the full range of devices on the market [Aye04]. The type of PDA and operating system, therefore, generally dictates which application to utilize for a case.

Normally, the forensic toolkit used for acquisition is also the one used for examination and analysis. Where there is a choice among more than one tool for acquisition, such as with Palm OS devices, interoperability among some acquisition and examination tools may exist, as shown in Table 4 (e.g., acquiring data with one tool and analyzing results with another). Interoperability is an important aspect for consideration, since some tools may be limited to specific operating system versions (e.g., POSE being limited to version 4.x and below) or may not support certain device models. Moreover, occasionally one forensic tool may fail to acquire information from a specific device, while another tool works without problems.

Table 4: Interoperability Among Palm OS Examination Tools

	POSE	**PDA Seizure**	**Encase**
pdd	Accepts ROM image, but pdd does not output individual databases	Accepts ROM and RAM images produced, with only partial functionality	Accepts ROM and RAM images produced
Pilot-Link	Accepts ROM image and individual databases created respectively with pi-get rom and pilot-xfer	Accepts ROM, RAM and individual databases created respectively with pi-getrom, pi-getram and pilot-xfer	Accepts ROM, RAM and individual databases created respectively with pi-getrom, pi-getram and pilot-xfer
PDA Seizure	Built-in version of POSE accepts acquisition output implicitly	Works implicitly	Accepts ROM and RAM images produced
Encase	Accepts individual databases produced	Accepts ROM and RAM images produced, with only partial functionality	Works implicitly

Forensics examiners are advised to experiment with various toolkits on non-evidence devices to find out which acquisition tools work efficiently with particular device types, and also to determine the degree of interoperability among different acquisition and examination tools for a device family. Besides gaining familiarity with the capabilities of the tool, experimentation allows special purpose search filters and custom configurations to be set up in advance of use in an actual case. In addition, software updates from the manufacturer can be installed.

Regardless of whether the device is Pocket PC, Palm, or Linux-based, in order to acquire data from it, a connection must be established from the specialist's forensics station to the device. Before performing an acquisition, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer that are applied to the tool. Once the connection has been established, the forensic software suite can proceed to properly acquire data from the device.

Unlike desktop machines or network servers, present day PDAs have no hard disk and rely instead completely on semiconductor memory. Specialized software exists for producing an image of the device. However, the contents of the device are continually changing, even when switched off (i.e., in the quiescent state). Two back-to-back acquisitions of a device using the same tool produce different results overall, though the majority remains identical. To image a PDA device's memory, the device has to be switched on, which is a major difference from PCs. This effectively means that the first evidentiary principle mentioned in section 4 – *actions taken should not modify data contained on the device* – cannot be complied with, strictly speaking. Therefore, the goal with PDA acquisition is to change the evidence in memory as little as possible and then only in the knowledge of what is happening internally, placing more importance on ensuring adherence to the second and third evidentiary principles, which stress the competence of the specialist and the generation of a detailed audit trail [ACPO].

After an acquisition is finished, the forensic specialist should always confirm that the entire contents of a device were captured correctly (i.e., verify RAM/ROM size ensuring consistency with the device). On occasion, a tool may fail its task without any error notification and require the specialist to reattempt with either the same tool or another tool. Similarly, some tools do not work well with certain devices as others do, and may fail with an error notification. Thus, when possible, it is advisable to have multiple tools available.

6.1 Unobstructed Devices

An unobstructed device is a device that does not require a password or other authentication technique to be satisfied to be granted access to the device. From anecdotal information, most devices seized in investigations appear to fall into this category. As mentioned earlier, when seizing an "Unobstructed Device" caution should be utilized to avoid, for example, altering the state of the device by pressing key chord sequences that have the potential to corrupt or erase valuable evidence.

In general, a PDA has four main categories of storage to consider: the operating system code, including the kernel, device drivers, and system libraries; dynamically allocated memory for executing operating system applications and storing and executing additional user applications loaded onto the device, user storage for various types of data files, including text, images, and sounds; and critical data backup of important PIM application information and data files. The characteristics of these four categories range from highly stable to extremely volatile. These

differences combined with the characteristics of a specific operating system, determine how ROM and RAM are used to support each storage category.

Figure 6 illustrates the most typical arrangement. Flash ROM is used mainly to hold the operating system code and optionally, any PIM data or files backed up by the user into the remaining space. Flash memory has a limited life of approximately 100,000 erase cycles. RAM is used for dynamic storage and user file storage. A soft reset (i.e., warm boot) typically reinitializes the dynamic storage in RAM, but leaves user file storage untouched, while a hard reset (i.e., cold boot) reinitializes both. Complete draining power from the PDA has the same effect as a hard reset. ROM is unaffected by either a soft or hard reset.

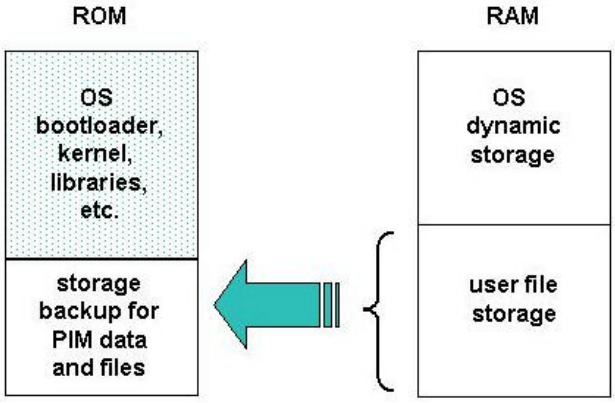

Figure 6: ROM/RAM Storage Assignments

A common alternative memory arrangement is shown in Figure 7. Here user file storage resides in Flash ROM with the operating system code, which avoids the need for backup utilities, since the storage is persistent and unaffected by resets and power drainage. The relative sizes of ROM and RAM are normally sized differently (i.e., more ROM and less RAM) when compared to the earlier arrangement to provide commensurate capacity. To keep user file storage in ROM versus RAM, a specialized filesystem is required to avoid quickly reaching the lifetime of that media. File systems such as JFFS2 (The Journaling Flash File System, version 2) are designed specifically to manage flash memory usage carefully. For example, JFFRS2 prevents rewrite of an entire sector to erase a single byte and ensures that different areas of memory are used in rotation to manage wear.

Because a limited number of forensic tools exist for acquisition of ROM and RAM contents from a PDA, the choice is often simple. One main consideration is to maintain compatibility with the toolkit eventually used in examination and analysis, since interoperability among different PDA tools, especially commercial case file formats, is not guaranteed.

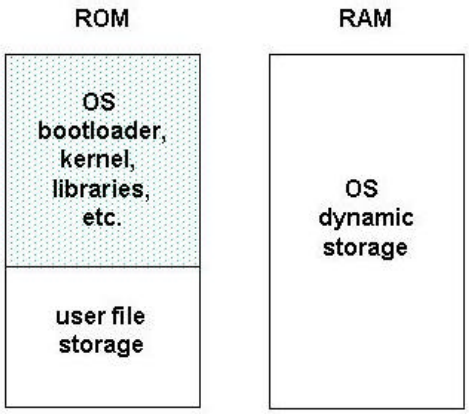

Figure 7: Alternative ROM/RAM Assignments

In order to preserve the integrity of the data, examiners should handle the original evidence as little as possible. Generally, it is recommended to first create a "master copy" of the device. The master copy is later used to create additional mirror images used strictly for analysis and examination of evidence [Gas03]. Either an SHA1 or MD5 hash should be performed to ensure that the additional images created from the forensic copy have consistent checksums.

6.2 Obstructed Devices

Obstructed devices typically refer to devices that are shut off (i.e., in the quiescent state) and require successful authentication using a password or some other means to gain access. Password protected devices normally require the expertise of a specially trained forensic specialist to gain access to the device contents, while maintaining integrity of the information and avoiding damage to the device. A number of ways exist to extract data from obstructed devices. They fall into three classes: investigative, software-based and hardware-based methods.

Software and hardware-based methods are often developed specifically for a particular device or narrow class of device. In developing a method, the following actions should be considered for determining possible approaches:

- Contacting the device manufacturer for information on known backdoors and vulnerabilities that might be exploited.
- Reviewing manufacturer specifications and other documentation when formulating plausible exploits.
- Contacting commercial evidence recovery professionals that specialize in handheld devices.
- Searching Internet sites for developer, hacker, and security information.

- Contacting device maintenance and repair companies, as well as commercial organizations that provide architecture information on handheld device products.[14]

6.2.1 Investigative Methods

Investigative methods are procedures the investigative team can apply, which require no forensic software or hardware tools. The most obvious methods are the following:

- **Ask the suspect** – If a device is protected with password, PIN, token, or other authentication mechanism involving knowledge-based authentication, the suspect can be queried for this information during the initial interview.

- **Review seized material** – Passwords are frequently written down on a slip of paper and kept with or near the device, or on the suspect's person, such as within a wallet, and may be recovered through visual inspection.

- **Manually supply commonly used input** – Users may weaken a mechanism by the way in which it is used. For example, if a device requires a 4-digit PIN, an examiner may wish to try the combination 1-2-3-4, as one of the three guesses that are allowed before the device is completely locked down [Kni02].

6.2.2 Software-based Methods

Software-based methods involve software techniques used to break or circumvent authentication mechanisms. While some general-purpose software techniques and tools may apply to a class of PDA devices, most of the techniques are specialized for a specific model within a class. When a specialized technique is developed, it is normally programmed and tested on an identical test device. Software-based methods include the following:

- **Exploit known weaknesses in authentication** – If an authentication mechanism is weak, it may be possible to exploit the weaknesses to defeat it. For example, early password protection schemes on Palm OS PDAs obfuscated the password using a reversible algorithm [Kin01], allowing it to be recovered easily from devices running version 4.0 or earlier, using a utility. Similarly, early versions of the Pocket PC Active Sync protocol allow unlimited authentication attempts to be made without penalty, allowing a dictionary attack of commonly used passwords to be attempted. In addition, some systems may have a reserve password or master password built into the authentication mechanism, which allows unfettered access when entered [Kni02].

- **Gain access through a backdoor** – Manufacturers often build in test facilities or other backdoors that an examiner can exploit to obtain information. For example, the bootloaders on some PDA devices support functions that among other things allow device memory to be read and copied or transmitted. For instance, the iPAQ 3900 and other models in that product series support the parrot bootloader, an unadvertised utility so named because of the bird that appears on the display [Log01]. When triggered by a specific combination key chord and provided appropriate commands via the serial port, the bootloader returns the contents of memory or copies it to a

[14] For handheld device architecture information see http://www.portelligent.com/prodserv.asp

memory card. Similarly, the penguin bootloader for Linux handheld devices allows memory to be copied to a memory card.

- **Exploit known system vulnerabilities** – Mobile systems may possess system vulnerabilities within a standard interface protocol that an examiner can exploit to bypass authentication and gain access to information. For example, access to the device may be possible via a misconfigured network service [Cha02], a flaw in a standard networking protocol supported by the device, or an error in the protocol's implementation making it susceptible to an attack method such as buffer overflow. Possible communications interfaces for exploitation include the serial, USB, IrDA, Bluetooth, WiFi, and GSM/GPRS facilities.

6.2.3 Hardware-based Methods

Hardware-based methods involve a combination of software and hardware to break or circumvent authentication mechanisms. Few general-purpose hardware-based methods apply to a general class of PDA devices. Most of the techniques are specialized for a specific model within a class. As with software-based methods, when a specialized technique is developed, it is normally developed using a test device identical to the one under examination. The device manufacturer may also provide useful information and tools for extracting data. Hardware-based methods include the following:

- **Gain access through a hardware backdoor** – Hardware backdoors, such as interfaces for debugging, production testing, or maintenance, may be used to gain access to memory. For example, some devices have active hardware test points on the circuit board that can used to probe the device. Many manufacturers now support the JTAG (Joint Test Action Group) standard, which defines a common test interface for processor, memory, and other semiconductor chips, on their devices [Int96]. Forensics examiners can communicate with a JTAG-compliant component by utilizing software and an add-in hardware controller in a PC card slot or a special purpose stand-alone programmer device to probe defined test points. The JTAG testing unit can send commands and data to the JTAG-compliant component and return the results to the unit for storage and rendition [Xjt03]. JTAG gives specialists another avenue for imaging devices that are locked or devices that may have minor damage and cannot be properly interfaced otherwise.

- **Examine memory independently of the device** – An experienced examiner may be able to examine memory chips directly on the device and extract information from them. For example, the Netherlands Forensic Institute has developed a general-purpose tool for examining a wide range of memory chips. Once physically connected via a memory clip, the tool is able to not only read and store memory contents, but also overwrite them [Kni02].

- **Reverse engineer the device to find and exploit a vulnerability** – Reverse engineering involves retrieving the operating system code from the ROM of a PDA identical to the one under examination and analyzing the code to understand its use of the device hardware. With the understanding gained, any plausible vulnerabilities noted can be systematically tested to determine a useful exploit technique. For example, for a password authentication mechanism, it may be possible using memory injection to overwrite the password with a known value or replace the authentication

program with a version that always authenticates successfully [Kni02]. Similarly, flipping two bits in a data structure, which determine whether or not the start-up password is active and configured, may turn off the mechanism completely, as reported for the XDA PDA/phone hybrid device [Its].

- **Infer information by monitoring physical device characteristics** – Techniques that monitor power consumption or other device characteristics have been shown to be effective in systematically determining the password or PIN. For example, forensic specialists report that the passwords of some electronic organizers have been uncovered by determining the address area of the password and, as characters are entered, systematically monitoring the data and address bus of those memory locations to reveal the value one character at a time [Kni02]. Differential power analysis, which has been shown to be effective in gaining information from smart cards, is another technique that could be applied [Aig].

- **Use automated brute force** – If a password mechanism has no restrictions on the number of manual attempts made and the examiner had time to spare, a brute force dictionary attack could be attempted. Normally, this approach would be out of the question. However, with automated keystroke entry, it is plausible. For example, the Netherlands Forensic Institute developed, an automated password entry system for devices with a keyboard and screen. Equipped with a robot arm and video camera the unit can systematically enter passwords until the correct entry is detected or, in the worst case, the keys become damaged [Kni02].

6.3 Tangential Equipment

Tangential equipment includes devices that contain memory and are associated with a PDA. The two main categories are memory cards and host computers to which a PDA has synchronized its contents. Surprisingly, USB memory drives, which are a common peripheral for host computers, are generally not a factor for PDAs because of interface issues.

PDAs, especially higher end models, typically support Compact Flash (CF), Secure Digital (SD), Multi-Media Cards (MMC), and other types of removable media designed specifically for handheld devices, which can contain a significant amount of data. Like RAM and ROM, memory cards are typically semiconductor memory. They normally are used as auxiliary user file storage, backup of important PDA content, or a means to convey files to and from the device. The physical sizes of memory cards supported by handheld devices is noteworthy insofar as they are quite small, about the size of a coin, and easy to overlook. Therefore, investigators should take their time and thoroughly search the premises, when seizing material. Data can be acquired from removable media with the use of a media reader and a forensics application used to image hard drives.

The data contained on a PDA is often resident on a personal computer, due to the capability of a PDA to synchronize or otherwise share information among one or more host computers. Such personal computers or workstations are referred to as synched devices. Because of synchronization, a significant amount of valuable evidence on a PDA, if not all, may also be resident on the suspect's laptop or personal computer, and recovered using a conventional computer forensic tool for hard drive acquisition and examination.

USB drives, sometimes referred to as thumb drives, are chewing-gum-pack size hardware components with a USB connector at one end, and built as a printed circuit board within a plastic housing that encases a processor and memory. USB memory drives can be treated similarly to a removable disk drive, and imaged and analyzed using conventional forensic tools.

6.3.1 Synched Devices

Synchronization refers to the process of resolving differences in certain classes of information, such as e-mail, residing on two devices (i.e., a PDA and PC), such that both retain most current versions, which reflect any actions taken by the user (e.g., deletions) on one device or the other. Depending on how the suspect's device is configured, a significant amount of informative data may reside locally on the personal computer. When a connection is established between the device and the PC, the user may communicate through the following types of account:

- **Guest Account** – By setting up a guest account no data is automatically synchronized with the device and the PC, unless explicitly initiated by the user.

- **User Account** – Upon connection, user accounts synchronized data to and from the device/PC automatically. The data that is synched and which device takes precedence is pre-defined by the user. The majority of handheld users during a sync transfer new data to the device such as: e-mails, contacts, To-Dos, etc.

Synchronization of information may occur at either the record level or at the file level. When done at the file level any discrepancies in the date and time since the last synchronization, result in the latest version automatically replacing the older version. Occasionally manual intervention may be needed if both versions were modified independently since the last synchronization occurred. Record level synchronization is done similarly, but with more granularity whereby only out-of-date parts of a file are resolved and replaced.

With Palm OS devices, record level synchronization is the norm. The core databases that can be synchronized include the following: address, Backup, date book, Note Pad, Quick Install, and todo. With Pocket PC devices, file level synchronization is the norm. The core application files that can be synchronized include the following: Calendar, Contacts, Inbox, Pocket Access, Tasks, Favorites, and AdvantGo. Synchronization software other than that built into the operating system also exists and may provide a more extensive or different set of capabilities. Because it is not unusual for a PDA and PC to be in an unsynchronized state, additional information may be found in one or the other.

Digital devices most frequently are populated with data from the PC during the synchronization process. Although, data from the PDA can be synchronized to the PC, this is strictly user-defined in the synchronization software. Dependent upon the synchronization software and the device type determines where PDA files may be stored on the PC. Each synchronization protocol has a default installation directory, but the locale can be user specified. Palm's HotSync manager keeps a log of data transfers containing: dates, location of the data, and what information was synched.

6.3.2 Memory Cards

A vast amount of memory cards exists on the market today that range from the size of a stamp to a large matchbook. Removable media storage capacity ranges from 32MB to beyond 2GB. As technological advances are made such media becomes smaller and offers larger storage densities. Removable media extends the storage capacity of PDA allowing individuals to store additional files beyond device capacity. Memory cards provide another avenue for sharing data between multiple users that have compatible hardware.

Unlike RAM within a device, removable media is non-volatile storage and requires no battery to retain data. Fortunately, such media can be treated similarly to a removable disk drive, and imaged and analyzed using conventional forensic tools with the use of an external media reader. Data contained on the media can be imaged, searched, and deleted files can be recovered providing possibilities of uncovering evidence. Below is a brief overview of several common storage media in use today that may contain significant information related to an investigation.

- **Compact Flash Cards (CF)** - 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 were 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.

- **Microdrives** - 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 requires energy to spin and is more fragile than solid-state memory. Similar in function to the solid-state Flash memory cards, the 4GB Microdrive storage card is pre-formatted with a FAT32 file system. 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 file system. Many digital cameras and most PDAs support FAT32.

- **Multi-Media Cards (MMC)** - 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.

- **Secure Digital (SD) Cards** - 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** - 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.

- **Extended Memory Cards** - Memory cards may support extensions for additional functionality. For example, the X-Mobile Card from Renesas is a MultiMedia card that contains both a smart card and a memory chip and able to function in either mode.

6.3.3 USB Memory Drives

Many manufacturers produce USB memory drives of various capacities. Currently, however, very few PDA devices support host USB ports, which are needed to interface with these peripherals. Moreover, few if any USB drive manufacturers provide the necessary drivers for PDA operating systems. This situation is understandable giving that a host USB specifications intend that an interface be capable of supporting multiple devices sharing the port, which if permitted would place a significant power drain on the battery of the device. Other factors include the restrictions in mobility that a drive sticking out of the side of a PDA imposes and the preferred alternative of providing one or more slots for memory cards, which insert completely within and are smaller in volume.

As with memory card extensions, USB drives may offer additional capabilities such as a wireless interface. Access to memory contents may also be protected through a built in finger print reader or some other mechanism such as a smart card, which complicates the acquisition process. However, for the reasons mentioned above these peripherals are also not normally associated with PDA devices.

7. Examination and Analysis

The examination process gives light to probative data. The results, gained through applying established scientifically based methods, should describe the content and state of the data in its totality. Such documentation allows all parties to discover what is contained, including information that may have been hidden or obscured. Once all the information is exposed, data reduction can begin, thereby separating relevant from irrelevant information. The analysis process differs from examination in that it looks at the product of the examination for its significance and probative value to the case [ACPO]. Examination is a technical process that is the province of the forensic specialist, while analysis may be done by roles other than the forensic analyst, such as the investigator as well as the forensic examiner or one individual may perform all roles.

The examination process begins after a forensics workstation has been set up with the appropriate tools and a copy of the evidence acquired from the device. If available, the examiner should have studied the case and become familiar with the parameters of the offence, the parties involved, and potential evidence that might be found. It is advisable for the examiner to conduct the examination in partnership with the forensic analyst or the investigator guiding the case construction. The investigator or analyst provides insight into the types of things sought, while the forensic examiner provides the means to find relevant information that might be on the system [Wol03].

If the forensic examiner performs the analysis independently without conferring with the forensic analyst or investigator, the knowledge gained by studying the case should provide ideas about the specific keywords or phrases to use when searching the image acquired from the device. Fortunately, compared with classical examination of individual workstations or network servers, the amount of acquired data, in terms of raw image size, is several orders of magnitude smaller (i.e., Mbytes vs. Gbytes).

Depending on the type of case, the strategy varies. A case about child pornography may begin with browsing all of the graphic images on the system, while a case about an Internet related offence might begin with browsing the Internet history files [Wol03]. Examination often reveals not only potentially incriminating data but also useful information such as passwords, network logon names, and Internet activity. In addition to evidence directly related to an incident, information can be uncovered about the lifestyle of a suspect, their associates, and the types of activities in which they are involved.

7.1 Locating Evidence

Standard PDAs typically offer similar information handling features and capabilities, including Personal Information Management (PIM) applications, support for e-mail, and Web browsing. Hybrid devices that incorporate both PDA and cell phone functionality also exist. Potential evidence on these devices include [DOJ01]:

- Address book
- Appointment calendars/information
- Documents
- E-mail
- Handwriting

- Password
- Phone book
- Text messages
- Voice messages

Generally, there are two types of computer forensic investigations. The first is where some incident has occurred, but the identity of the offender is unknown (e.g., malicious code attack, hacking incident, etc.). The second is where the offender and the incident are both known (e.g., a child-porn investigation). Armed with the knowledge of the circumstances of the incident provides the forensic examiner and analyst to proceed toward the following objectives:

- Gather information about the individual(s) involved {who}.
- Determine the exact nature of the events that occurred {what}.
- Construct a timeline of events {when}.
- Discover what tools or exploits where used {how}.
- Uncover information that explains the motivation for the offense {why}.

Table 5 below provides a cross reference of generic evidence sources found on PDAs and their likely contribution towards satisfying the above objectives. Most of the source information comes from PIM data, and Internet related information. Other support applications that run on the device potentially provide other evidence sources. User files placed on the device for rendition, viewing, or editing are also another important evidence source. Besides graphic files, other relevant file content includes spreadsheets, presentation slides, and similar items. For hybrid devices, such as PDA phones or GPS PDAs, additional evidence sources exist, for example, the last dialed number or coordinates to some destination.

Table 5: Cross Reference of Sources Versus Objectives

	Who	What	Where	When	Why	How
Owner Info	X					
Contacts	X				X	X
Calendar	X	X	X	X	X	X
To Do List	X	X	X	X		X
E-mail Contact	X	X	X	X	X	X
Web URLs/Content		X	X	X		X
Graphic Files	X	X				
Other File Content		X	X	X	X	X

Knowledge and experience with multiple tools for acquiring and examining the contents of PDAs is extremely valuable. For instance, one tool may perform better than another in specific areas such as file identification or search facilities; tools may report, acquire, and examine the contents of acquired data differently; and some tools may be platform specific. Therefore, it is advantageous to use a toolkit that offers the best set of features for recovering and analyzing evidence from a specific device.

7.2 Applying Tools

Once the acquired image has been copied, the next step is to begin searching the data, creating bookmarks, and developing the contents of a final report. Forensic examination tools are a crucial component in this process as they translate data from raw bit images to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence. It is important to note that tools have the possibility to contain a degree of error. For example, the implementation of the tool may have a programming error; the specification of a file structure used by the tool to translate bits into data comprehensible by the examiner may be in error or out of date; or the file structure itself generated by some other program may have been produced incorrectly, causing the tool to function improperly [Car02]. Therefore, it is essential to have a high degree of trust and understanding of the tool in its ability to properly perform its function. In addition, a knowledgeable suspect may tamper with device information, such as purposefully misnaming a file extension to foil the workings of a tool or apply a wiping tool to remove or eliminate data. Over time, experience with a tool gains an understanding of its limitations, which helps to limit the degree of error.

Forensic Examination of Digital Evidence – A Guide for Law Enforcement, produced by the U.S. Department of Justice [DOJ04], offers the following suggestions for the analysis of extracted data:

- **Timeframe analysis** – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present on the system and the date/time stamps in the filesystem, such as the last modified time.

- **Data hiding analysis** – Detect and recover hidden data that may indicate knowledge, ownership or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files; gaining access to steganographic information detected in images; and gaining access to reserved areas of data storage outside the normal filesystem.

- **Application and file analysis** – Identify information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

- **Ownership and possession** – Identify the individuals who created, modified, or accessed a file, and the ownership and possession of questioned data by placing the subject with the device at a particular time and date, locating files of interest in non-default locations, recovering passwords that indicate possession or ownership, and identifying contents of files that are specific to a user.

The capabilities of the tools, the richness of features, and the operating system (e.g., Windows CE, Palm OS, Linux) and type of device under examination determines what information can be found, recovered, and reported and the amount of effort needed. Areas of variability include the search and recovery of deleted information, information on reset devices, or information within compressed file archives or files with misnamed extensions [Aye04]. For example, some tools used to search for evidence may identify files by file extension where others use a file signature database. The latter is preferable since it eliminates the possibility of

masking data based upon an inconsistent file extension. This is especially true for graphics files of various types, since by their very nature they generally are shrouded from textual searches.

The search engine plays a significant role in the discovery of information used for the creation of bookmarks and final reporting. Searching data for positive results on incriminating evidence takes patience and can be time consuming. Some tools have a simple search engine that matches an input text string exactly, allowing only for elementary searches to be performed. Other tools house more intelligent and feature rich search engines, allowing for grep (generalized regular expression patterns) type searches, including wildcard matches; filtering of files by extension, directory, etc.; and batch scripts that search for specific types of content (i.e., e-mail addresses, URLs, etc.). Similarly, the ability to find and gather images automatically into a common graphics library facility can differ among tools. The greater the tool's capabilities, the more the experience with and knowledge of the tool become valuable for the forensic examiner.

A lot of evidence can be found on victims' or suspects' devices, to uncover evidence, specialists must first gain a background of the suspect and offense and determine a set of terms for the examination. Search expressions should be developed in a systematic fashion, such as using contact names that may be relevant. By doing this, the specialist creates a profile for potential leads that may unveil valuable findings. To eliminate all possibility of omitting valuable evidence, the data should be thoroughly looked through from beginning to end in a memory window provided by either the tool or a hex editor. Additionally, specialists should have a database of file signatures to locate the headers and footers of specific files that may lead to further evidence such as: graphics files, avi files, etc.

Once the data has been thoroughly searched and relevant items bookmarked, it is time to create a report. Many forensics applications come with a built-in reporting facility that imports bookmarked data, allowing the specialist to organize the report, choose its style, and customize other aspects of the report. Reports may include the following: Specialists Name, Case Number, Date, Title, Suspect Name, Categories for evidence, and relevant evidence found. The software-generated report is only a small part of the overall final report. The final report includes the software-generated report alongside the ongoing documentation throughout the entire cycle used to summarize the actions of the forensic examination and present the results of the analysis, including any evidence uncovered.

The following criteria have been suggested as a fundamental set of requirements for forensic tools [Car02], and should be considered when a choice of tools is available:

- **Usability** – the ability to present data in a form that is useful to an investigator
- **Comprehensive** – the ability to present all data to investigator so that both inculpatory and exculpatory evidence can be identified
- **Accuracy** – the quality that the output of the tool has been verified and a margin of error ascertained
- **Deterministic** – the ability for the tool to produce the same output when given the same set of instructions and input data.

- **Verifiable** – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results.

Other factors in choosing among software tools include the following items:

- **Quality** – technical support, reliability, and upgrade version path
- **Capability** – supported feature set, performance, and richness of features with regard to flexibility and customization
- **Affordability** – cost versus benefits in productivity

8. Reporting

Reporting is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigation of a case. Reporting depends on all participants carefully maintaining a record of their actions and observations, reporting the results of tests, and explaining the inferences drawn from the evidence. The basis of a good report is solid documentation, notes, sketches, photographs, and tool generated reports

Reporting of the results of a forensics examination tend to follow predefined templates, customized as required by the specific circumstances of each investigation. Reports of forensic examination results should include all the information necessary to identify the case and its source, outline the test results and findings, and bear the signature of the individual responsible for its contents. In general, the report may include the following information [DOJ04]:

- Identity of the reporting agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination, including serial number, make, and model
- Identity and signature of the examiner
- The equipment and set up used in the examination
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation
- Details of findings:
    - Specific files related to the request
    - Other files, including deleted files, that support the findings
    - String searches, keyword searches, and text string searches
    - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity

- Graphic image analysis
- Indicators of ownership, which could include program registration data
- Data analysis
- Description of relevant programs on the examined items
- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies

- Report Conclusions

Many forensics software applications have reporting facilities built-in. Examiners should include only relevant findings in the report to minimize size and confusion amongst those reviewing it. Automated reports typically contain the following key components: Case Number, Date, Examiner Name, Suspect Name, and Files Acquired (showing hash, ASCII data, graphical representation of data, etc.).

Digital evidence, as well as the tools, techniques and methodologies used in an examination, are subject to being challenged in a court of law. Proper documentation is essential in providing individuals the ability to re-create the process from beginning to end. Although, evidence presented is always subject to question. As part of the reporting process, making a copy of the software used and including it with the output produced is advisable. This is especial pertinent for custom tools, since confusion about the version of the software used to create the output is eliminated, should it become necessary to reproduce forensic processing results at a later time. The same practice applies to commercial software tools, which could be upgraded after an examination is completed [NTI].

9. References

[ACPO] Good Practice Guide for Computer-based Electronic Evidence, Association of Chief Police Officers, <URL: http://www.nhtcu.org/ACPO%20Guide%20v3.0.pdf>.

[Aho01] Jukka Ahonen, PDA OS Security: Application Execution, Helsinki University of Technology, Seminar on Network Security, Fall 2001, <URL: http://www.tml.hut.fi/Studies/T-110.501/2001/papers/jukka.ahonen.pdf>.

[Aig] Manfred Aigner, Elisabeth Oswald, Power Analysis Tutorial, Seminar Paper, Institute for Applied Information Processing and Communication, <URL: http://www.iaik.tu-graz.ac.at/aboutus/people/oswald/papers/dpa_tutorial.pdf>.

[Aye04] Rick Ayers, Wayne Jansen, PDA Software Tools: Overview and Analysis, NIST Interagency Report (IR) 7100, April 2004.

[Cha02] Steve Chapin, Douglas F. Calvert, David Walter, K. Reid Wightman, Niranjan Sivakumar, Multiple Security Vulnerabilities in Sharp Zaurus, Beyond Security Ltd, November 2002, <URL: http://www.securiteam.com/securitynews/5GP0G0A7PO.html>.

[Car02] Brian Carrier, Defining Digital Forensic Examination and Analysis Tools, Digital Forensics Research Workshop II, August 2002, <URL: http://www.dfrws.org/dfrws2002/papers/Papers/Brian_carrier.pdf>.

[DOJ01] Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice, NCJ 187736, July 2001, <URL: http://www.ncjrs.org/pdffiles1/nij/187736.pdf>.

[DOJ04] Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice, NCJ 199408, April 2004, <URL: http://www.ncjrs.org/pdffiles1/nij/199408.pdf>.

[Gas03] Ty Gast, Forensic Data Handling, Security Assurance Group, White Paper, 2003, <URL: http://www.securityassurancegroup.com/PDF/SAG-forensics-data-handling.PDF>.

[Ges03] Windows CE Embedded PC: Developer's Documentation, Version 3.0, Gesytec GmbH, August 2003, <URL: http://www.gesytec.de/common/pdf-downloads/epc/embedded-pc.pdf>.

[Gra02] Joseph Grand, pdd: Memory Imaging and Forensic Analysis of Palm OS Devices, Proceedings of the 14th Annual FIRST Conference on Computer Security Incident Handling and Response, June, 2002, <URL: http://www.first.org/events/progconf/2002/d3-04-grand-paper.pdf>.

[Hal01] Chris Halsall, Linux on an iPAQ, Linux DevCenter, O'Reilly Media, Inc., June 2001, <URL: http://www.linuxdevcenter.com/pub/a/linux/2001/06/01/linux_ipaq.html>.

[Int96] Designing for On-Board Programming Using the IEEE 1149.1 (JTAG) Access Port, Intel, Application Note, AP-630, November 1996, <URL: http://www.intel.com/design/flcomp/applnots/29218602.PDF>.

[Its] XDA Bootloader, ITSX, <URL: http://www.itsx.com/index.html?pocketpc-bootloader.html~mainFrame>

[Ket00] Arto Kettula, Security Comparison of Mobile OSes, Helsinki University of Technology, Seminar on Network Security, Fall 2000, <URL: http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/kettula.pdf>.

[Kin01] Kingpin and Mudge, Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats, August 2001, pp. 135-152, Proceedings of the 10th Usenix Security Symposium, <URL: http://www.usenix.org/events/sec01/full_papers/kingpin/kingpin_html>.

[Kni02] Ronald van der Knijff, Embedded Systems Analysis, Chapter 11, Handbook of Computer Crime Investigation, Edited by Eoghan Casey, Academic Press, 2002.

[Kru01] Warren G. Kruse II, Jay G. Heiser, Computer Forensics – Incident Response Essentials, Pearson Education, September 26, 2001.

[Log01] Brett Logsdon, Compaq iPAQ Parrot Talks: How to flash your ROM by the backdoor, Pocket PC Passion, February 2001, <URL: https://www.pocketpcpassion.com>.

[Man01] Kevin Mandia, Chris Prosise, Incident Response: Investigating Computer Crime. McGrawHill Osborne Media, 2001.

[Meu02] Pascal Meunier, Sofie Nystrom, Seny Kamara, Scott Yost, Kyle Alexander, Dan Noland, Jared Crane, ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs, Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), June 2002, <URL: http://www.cs.nmt.edu/~cs553/paper3.pdf>.

[NTI] Computer Evidence Processing Steps, New Technologies Inc., <URL: http://www.forensics-intl.com/evidguid.html>.

[Oco04] Thomas R. O'connor, Admissibility of Scientific Evidence Under Daubert, North Carolina Wesleyan College, March 2004, <URL: http://faculty.ncwc.edu/toconnor/daubert.htm>.

[Palm] Palm Security White Paper, date, <URL: http://www.palm.com/enterprise/resources/securing/index>.

[Pmd02] Palm Security, How-To Guide, pdaMD.com, 2002, <URL: http://www.pdamd.com/vertical/tutorials/palmsecure.xml>.

[PPC04] Palm OS Programmer's Companion, Volume I, PalmSource, Inc., May 2004, <URL: http://www.palmos.com/dev/support/docs/palmos/CompanionTOC.html>.

[USAF] Mark Reith, Clint Carr, and Gregg Gunsch. An Examination of Digital Forensic Models, International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3 <URL: http://www.ijde.org/docs/02_fall_art2.pdf>.

[Wol03] Henry B.Wolfe, Evidence Analysis, Computers and Security, May 2003, Volume 22, Issue 4, pp. 289-291, <URL: http://www.sparksdata.co.uk/elseforms/order/COSE%202201.pdf>.

[Xjt03] JTAG testing with XJTAG, Version 0.1, XJTAG, March 2003, <URL: http://www.xjtag.com/images/TestingWithXJTAG.pdf>.

[Zwi02] Thomas Zwinger, Leif Laaksonen, Linux on an iPAQ PDA, @CSC, CSC - Finnish IT Center for Science, Issue 3, 2002 <URL: http://www.csc.fi/lehdet/atcsc/atcsc3-2002/ipaq.pdf>.