

An overview and examination of digital PDA devices under forensics toolkits.

Krishnun Sansurooah
School of Computer and Information Science (SCIS)
Edith Cowan University Perth, Western Australia.
Email: ksansuro@student.ecu.edu.au

Abstract

Personal Digital Assistants most commonly known as PDAs are becoming more and more fashionable and affordable in the working environment. With the advent and rapidly increasing technology these handled devices are now targeted by a lot of person with criminal intentions. But unfortunately crime does not choose its technology and nowadays those ultra light handhelds are getting more and more involved in crimes. This therefore become an onerous task for the forensics examiners who needs the proper forensics tools to investigate the information held on these devices. The purpose of this report will browse the current forensics toolkits available and analyze some targeted PDAs.

Keywords

PDA, Forensics Analysis, Encase, PDA Seizure, Image Acquisition, PDA Memory

INTRODUCTION

Today's technology is advancing rapidly and when it comes to handheld devices it's even growing quicker especially in their capabilities and in their use. With this increasing technology, it is not a surprise to come across those devices be either PDAs or smart phones which can contain as much processing power as would have held a normal desktop couple of years ago. With those amazing handheld devices, their storage capacities are phenomenon and keep increasing even though these digital devices are getting ultra light in weight.

Being concerned by this evolution, it is therefore necessary that nowadays, the analysis of those handheld devices be combined with the existing digital forensic procedures and methodologies already in place to keep up with the technology. However, most PDAs that are on the market follow similar basic designs, but obviously differs in their operating system (OS), and their hardware components which in turn, unfortunately does not facilitate the forensic data acquisition on the handheld devices without modifying their actual or current state. Having therefore mentioned that this process is not quite easy to performed, the data acquisition can still be performed on the PDAs through some of the currently existing forensic software for that type of acquisition.

To narrow the focus of this research paper, the digital handheld devices looked after would be Palm devices running the Palm OS. This paper will also take into consideration of the different forensic tools available for the acquisition on Palm OS and will not emphasizes on data acquisition on WinCE or Windows mobile phone or Microsoft Pocket.

BACKGROUND

According to Kruse & Heiser (2002) the preservation, identification, acquisition, documentation, interpretation and reporting of computer or digital data is defined as digital forensics. The field of digital forensics has long emphasizes on the seizing and recovering of evidence from a personal computer. But nowadays, criminal are running in parallel with the technology and are hence using the latest up to date devices to achieve to their need in committing illegal activities. With this evolution, the life of forensic experts have become more complicated and forensically acquire these handheld digital devices be either smart phones, pagers, and PDAs have unfortunately become an onerous task.

According to Kruse and Heiser (2002) there are three stages in the acquisition of data for the basic methodology which are as described below:

1. The acquisition of evidence should be performed without modifying or corrupting the original source
2. The acquired evidence needs to be authenticated when raised to the original evidence.

3. The acquired evidence should be analyzed without any alteration to it.

Following Kruse and Heiser (2002) the first stage entails the procedures that need to be observed and fully recorded and documented in the early phases of forensic analysis. These procedures would be

- a) Gathering and collection of evidence
- b) The correct handling of evidence
- c) Maintaining the chain of custody
- d) Identifying the evidence collected
- e) The methods of transporting the evidence
- f) And finally, how the evidence is stored or presented

The second stage described by Kruse and Heiser (2002) in the basic methodology demands that the acquired evidence is verified against the original source. This is a very crucial step in the task of a forensic expert or analysis as this will determine whether the piece of evidence is review from a legally acceptable and presentable process with all the necessary documents to support this finding, especially if these findings are to be pursued to court of law. In a report on digital forensics, McKemmisk (1999) reported that there are four rules to be observed when acquiring evidence for a criminal investigation to be pursued in a court of law.

Those rules to be observed are:

- i) Minimize the handling of original data source.
- ii) Account for any changes in the original data
- iii) Use are follows the rules of evidence, especially when it comes to use of software tools for the acquisition of the evidence

To achieve this composition of acquired evidence versus the original source, the best and most current and reliable way would be archived by electronically fingerprinting the evidence and time stamping both calculated by hashes with cryptographic hashing algorithms such as MD5 Sum check or SHA1 Check. This method is quite reliable in ensuring that the digital evidence in ensuring that the digital evidence has been imaged properly and hence allowing and maintaining the chain of evidence due to the high volatility of the digital evidences.

Using the hashing algorithms allow the digital evidences to be presented in a court of law on the basic that when the incriminated digital device is initially acquired and stored, it can at a later stage be crossed verified to the original source to show and prove that no alteration has occurred during the acquisition of evidence thus keeping the original source intact.

Finally, Kruse and Heiser (2002) elaborate on the analysis of the acquired evidence without any alteration to it by ensuring that the original evidence source has not been found or altered. This process is normally conducted on the imaged copy which is an exact bit wise copy of the original source. This analysis normally starts with examining the files and then a further analysis of physical image or search for either deleted or hidden files. To conduct this process, there are some forensic tools that can be used in the instance of Encase V4, Autopsy, Hexadecimal editors which are toolkits available for refining search though the ASCII and hexadecimal deleted files.

DIGITAL HANDHELD DEVICES

According to Canalys (2004), the market of digital handheld portable devices has known a considerable growth and keeps growing in the working environment and also for personal use these digital music or mp3 players, smart phones and without excluding the most common personal digital assistants (PDAs). With the growing technology these PDAs have widely evolved and nowadays are equipped with in-built memory with a minimum capacity of 128 MB and some even more whereas Apple Computer (2004) has announced its digital music player with a capacity higher than 40 GB.

With all these digital devices, the PDAs have been designed to overcome the physical constraints set by either personal computer (PCS) or even laptops. Some of the major advantages that PDAs offer compared to PC or laptops are illustrated below:

- i) They are compact and ultra light thus allowing mobility to the uses;
- ii) They store user data on volatile memory, the Random Access Memory (RAM) and Read Only Memory (ROM) for the operating system (OS)

- iii) They also suspend processor when powered off, to avoid consuming time when rebooting.
- iv) They comprise with organizing functionality in the instance of emails, calendars and memos.
- v) They also offer the ability to synchronize data with a personal computer.

Having therefore enumerated those major differences of the PDAs, it is therefore very difficult and very challenging to soundly forensic those digital devices without the proper and specialized forensic toolkits and also the proper procedures due to the PDAs architecture. In the PDA family there are at present 3 main OS which shares the market. Those are Palm OS, Microsoft Pocket PC and finally portable Linux-based OS which regardless of their brand or family, those digital devices all support some basic functionalities such as contact, email, task management and calendar known as Personal Information Management (PIM) applications. And since we are turning to the new age of technology evolution, the PDAs market share is tending to split into only 2 categories now with are the most 2 dominant ones Palm OS and Microsoft Pocket PC. Another ability of the Palm nowadays is that it has the ability to communicate through wireless medium, surf on the web and even provide editing facilities for electronic document. While those PDAs allow a high level of mobility to their users, they also add up another special aspect to their reputation when it comes to storage of data on the PDAs by introducing the use of removable media such as external media cards with enormous capacities ranging from 128 MB to 4 GB thus making the PDAs more desirable for the users or the criminals.

REMOVABLE MEDIA

Forensic analysis of these removable media is quite similar in the process of analyzing hard drive. These media can therefore be removed and then inserted in a card reader, then an exact image is performed and then forensically examined as unlike the Random Access Memory (RAM) on a device, the removable media is non-volatile and therefore requires no source of prove to retain its data.

Even though removable media are part of the PDAs, the analysis of such media will not be covered in this report but a brief overview of these removable media are described below even small in size, they can however hide enormous amount of data if not gigabytes of data in relation 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 side of it. They are designed for PCMCIA-ATA; it normally has a 16-bit data bus, and is used more as a hard drive than as the RAM. The flash memory technology is a non-volatile storage media solution that retains its information once power is suppressed from the card. Compact Flash cards are about the size of a matchbook (length-36mm, width-42.8 mm, thickness-3.3 mm for Type I and 5mm for Type II) and consume a minimum amount of power.

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

A Multi-Media Card (MMC) is also a solid-state disk card but with a lower number of pins (7-pin connector). It has a 1-bit data bus and same as the compact card, it is hence 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. Those Multi-Media Cards are about the size of a postage stamp but do have in the same family a reduced size Multi-Media cards (RS-MMC) which is half the size of the standard MMC card. Even though they were designed to fit mobile phones, it can nevertheless be used with PDAs.

- ***Hitachi Microdrive***

Hitachi Microdrive digital media is a rotating mass storage device with high-capacity, contained in a Compact Flash Type II having a 16-bit data bus. A micro glass disk is opted as the storage media, which is obviously more fragile than solid-state memory and which do require energy to rotate. As in for the flash memory cards, the 6GB Microdrive storage card is preloaded with a FAT32 file system required to authorize storage over 2GB. In doing so, more space can be easily accessed according to Hitachi Global Storage Technologies (2004).

- ***Secure Digital (SD) Card***

SD Card Association (2004) mentioned that the Secure Digital (SD) memory cards can be compared to the solid-state design of MMC cards. However, the SD card slots often can accommodate MMC cards as well with their 9-pin connector and 4-bit data bus; it can therefore allow a quicker transfer rate. SD cards do offer an erasing in erasure-prevention option so that data cannot be deleted accidentally. Another option that is offered by the SD card is the security controls for content protection (in other words Content Protection Rights Management). MiniSD cards are also available and do run on the same principle but in a more compact with the same hardware

bus and same interface as in SD cards. It does offer the same prevention as SD cards but in a smaller dimension depending on their capacity.

- **Memory Stick:**

Following Memorystick.com Business Center (2004), memory sticks are also solid-state memory in a smaller size. It has a 10-pin connector and a 1-bit data bus. Same as SD cards, it also has an erasure-prevention switch in build in it to stop the card's content to be erased unintentionally. It therefore offers higher capacity in storage media and quicker transfer rates than standard memory sticks.

PDA HARDWARE AND SOFTWARE

As mentioned earlier, PDA support a set of core Personal Information Management (PIM) capabilities and most of the PDA allow communicating wirelessly through networks with validation and authentication. Therefore data stored on a PDA can be synchronized with either a laptop or desktop PC and would hence facilitate using a synchronization protocol. These protocols can be used to transfer all kinds of data be either text, audio, jpeg images and archive file format

PALM OS ARCHITECTURE

According to Grand & Mudge (2001), the Palm OS are built-in applications which are stored into the Read Only Memory (ROM) while both the user and application data rest into the Random Access Memory (RAM). In a report , Tanker B (2004) stated that add-on utilities are also used frequently to back up PIM data onto ROM. In an article published from the Palm OS Programmer's Companion (2004) that Palm OS split the total available RAM into 2 logical areas which are dynamic RAM area and storage RAM area. The Dynamic RAM area is compiled into a single heap and therefore used the working areas for temporally allocations, independents of the RAM mounted on a typical desktop system. However, the rest of the RAM is hence designed as storage RAM area to be used by when holding non-volatile user data. In Palm OS the memory storage in compiled into records which in turn are held in database – here the equivalence of files. The different layers of the Palm OS architecture comprise of Application, Operating System, Software API & hardware drivers and Hardware. Figure 1 below online the different layers level and their relationship in between when communication is effected

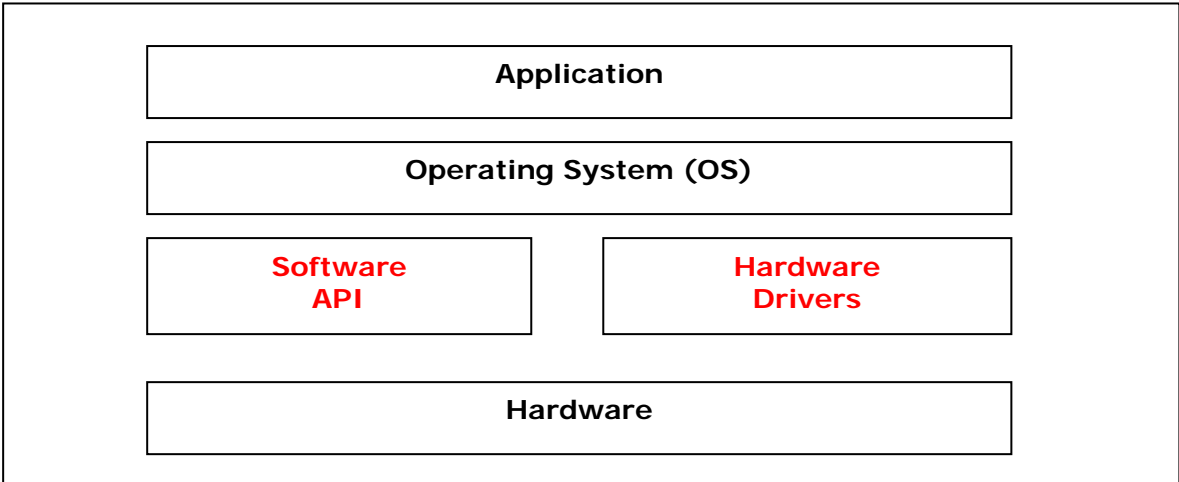


Figure1. Demonstrate the different layers of the Palm OS architecture.

With technology increasing at the tremendous rate, the latest PDA comes with so many advantages bundled to it which makes its very likely to be possessed by everyone which have a 'busy life' due to its considerable capacity of memory, its powerful micro processors with wireless communication devices embedded on such as wireless, infrared, and Bluetooth technology. A generic hardware diagram of the system level microprocessor is illustrated in Figure 7 below.

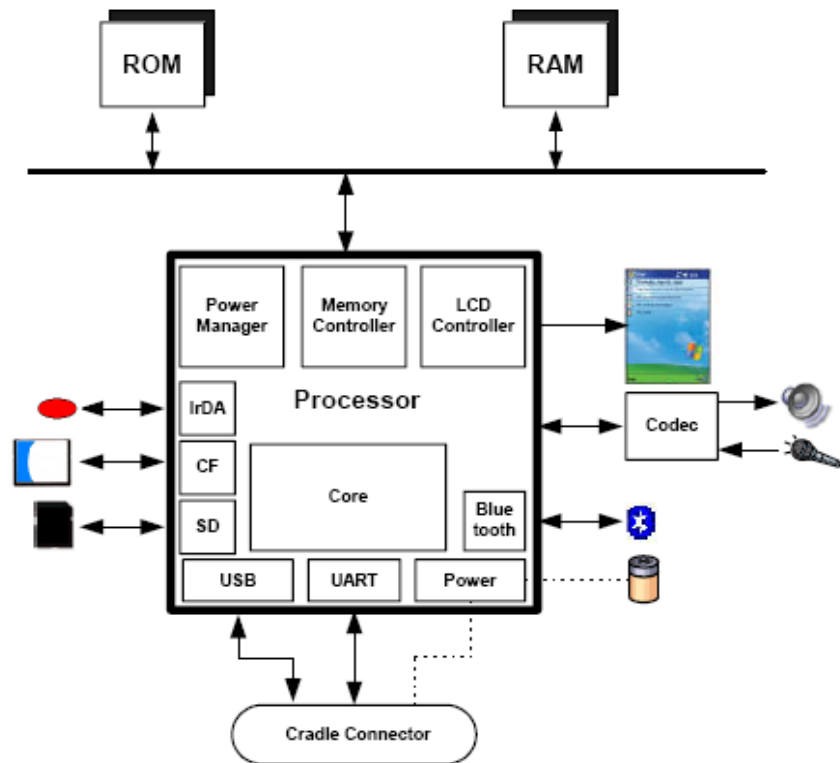


Figure 2. Illustrates the generic hardware diagram of the system level microprocessor

PDA SOFTWARE

Together with the purchase of a Palm OS, there is some software that comes along with the handheld digital devices which therefore ease the user to synchronize its Palm OS with its computer system at a later stage.

- **PALM DESKTOP**

This software which is normally delivered on the purchase of a Palm enable the user to organize and manage the data which they have stored on their PDA earlier and it therefore helps the user to trace back what editor took place where and when. In other words, it looks after date, address and any memo entry at that time thus providing the user with a more convenient way of making his/her entry into the Palm.

Together with the Palm Desktop, it also allows to install HotSync Operations. HotSyn has been developed by Palm which enables the user to synchronize the data between a personal computer and the digital handheld device. It therefore, gives the user the capability of transferring data between the digital device and the personal computer, which can be also used on a back in case that data came to be lost with the draining of the battery.

- **PALM DEBUGGER**

The Palm Debugger used in Palm commands is usually carries out in low-level system debugging. This debugger is attached on all Palm devices and into the Palm OS Emulator

According to Fernandes (2003), there are two different modes that Palm PDAs can enter which are “Debug Mode” and “Console Mode” The Palm Debugger which is included on all Palm handhelds provides a low-level system debugging for Palm application. This would therefore describe Fernandes (2003) first mode

PDA FILE SYSTEM

In Palm OS technology, the use of Hot file system differs from the traditional system. According to the Palm memory architecture give a detailed illustration of the Palm OS memory structure and analyzer the essential building blocks of the Palm memory Figure 3 outlines the pattern view of the RAM showing the layer of the dynamic RAM area and the storage RAM area.

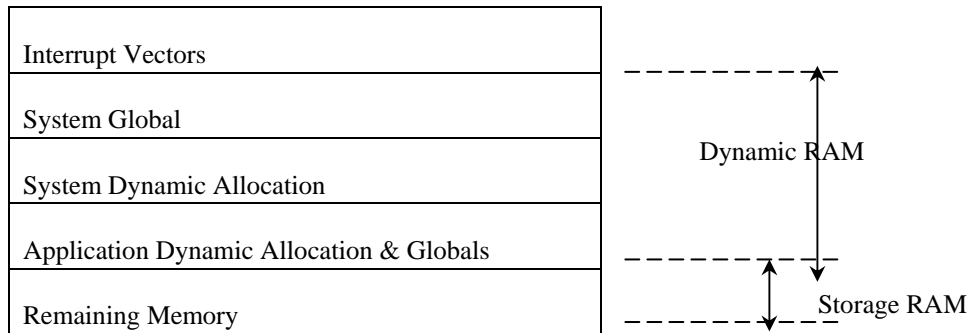


Figure 3. outlines the pattern view of the Dynamic RAM and the Storage RAM.

Dynamic RAM can be compared to the RAM sitting onto a typical personal computer system but in Palm OS the size of the dynamic RAM area would depend on the version of the OS and on the total available memory onto the device and this would keep changing continuously during the usage of the handheld device whereas the remaining RAM is used as storage RAM area similar to using a disk drive

FORENSICS AND PDA

With the increase of those powerful digital handheld devices, the methodologies and procedures in place for the analysis of digital forensics is being re-examined, re-considered and re-executed to adapt to the new age of digital handheld devices such as PDAs, portable digital music devices and mobile phones. Having to reconsider the methodological approach to these new handheld devices, the two most crucial parts in soundly forensically examining those devices are the acquisition stage and the authentication stage as in any basic computer forensic analysis. However, in the case of Palms this task would be most delicate and important as it should be delicately and correctly carried out to maximize accuracy on the Palm which in fact rejoins what have been mentioned earlier that most PDAs depend on transitional storage.

A crucial aspect of the PDA vis-à-vis the acquisition and analysis in the use of their memory – i.e. both the RAM and the ROM – when it comes to the storage of data on the PDA and their OS as RAM storage is volatile, the PDA is powered by a battery that allows the memory to be kept alive and hence conduct the operation needed such as storing of data on the PDA. Yet, carrying forensic analysis or acquisition on this device would be very risky as such operation would definitely require draining the battery power hence causing all data in the RAM to be lost similarly as on a PC when it is switched off, which discards the data on the RAM. Therefore much care and consideration should be given in the acquisition of PDAs which are quite delicate handheld devices in comparison to personal computers.

FORENSIC TOOLKITS:

When it comes to forensic acquisition and analysis of PDA, the variety and number of toolkits are very limited compared with PCs or workstations. The specialized toolkits are very limited and are restricted to the most popular PDA handheld devices based on either Pocket PC or Palm OS.

In the section of this paper, a more in-depth analysis of the forensics acquisition would be emphasis on Palm OS. As in for Linux based devices forensic acquisition can be achieved by using the 'dd' utility similarly as in Linux desktop and hence later be injected into a forensic tool such as Encase or Autopsy. Considering that Palm OS have been around longer than its competitors, the pool of forensic tools available for such practice is much wilder compared with the other handheld devices. Also consideration should be given that the forensic examiner

has full access to the handheld devices. Having examined some of the forensics toolkits available, a table has been designed to tabulate the different facilities that these tools often.

TOOLS	PALM OS	POCKET PC	LINUX BASED
Encase	ACQ / EXA / REP	N/A	EXA/REP
PDA Seizure	ACQ / EXA / REP	ACQ / EXA / REP	N/A
Pilot-Link	ACQ	N/A	N/A
POSE	EXA/REP	N/A	N/A
pdd	ACQ	N/A	N/A
dd	N/A	N/A	ACQ

Legend

ACQ – Acquired	EXA – Examined	REP – Reported	N/A – Not Available
----------------	----------------	----------------	---------------------

Table 1: PDA Forensic Toolkits.

Actually acquisition of data from a device is carried into 2 different ways:

1. Physical acquisition – in this particular type of acquisition, an exact copy bit-by-bit is collected of the entire physical storage which can be either a RAM chip or a Disk drive.
2. Logical acquisition – which implies an exact copy bit-by-bit of the logical storage such as file and directories, involved residing on a logical store which could be several disk drives. The actual difference however lays in between the memory as separate by a process through the OS facilities, known as logical views against the memory as interpreted by the processor and other related hardware components known as physical view.

Moreover, physical acquisition is much more preferred compared to logical acquisition due to its numerous advantages. With physical acquisition, deleted files and other small remaining pieces of data are looked into closely which could be missed out while carrying a logical acquisition. Another aspect of physical acquisition which is once more preferred to logical acquisition is that physical device images can easily be imported in a different forensic toolkit for examination and reporting. Yet, logical acquisition has an advantage in providing a more natural and readable organization of the data acquired. Having looked at both types of acquisitions, it is recommended that both methods are practiced when undergoing forensic acquisition and analysis of Palm OS.

This is also the concern of using non-forensic tools for the acquisition process which normally focuses on the logical acquisition using an available protocol for device synchronization thus allowing a flow of communication to the handheld device as opposed to a debugging protocol that can be dedicated in acquiring a memory image. With those non-forensic tools which support a two-way communication, the flow of information issues will be raised up when such non-forensic tools are unconcerned and negligent with modifications happening leading to avoid checking hashes of acquired images of the PDA before and after the acquisition stage henceforth losing the integrity of the images acquired which will definitely be questionable at time of court. Such example would be when a tool unwillingly modifies time stamp on the PDA device such as time and date of last synchronization.

According to Casey (2000), some tools of Palm OS devices require that the device to be placed in ‘*console delay mode*’, maintaining the option of a soft reset after collection. This soft reset triggers huge compilation and therefore deleted records may be overwritten. This being a double edge sword allow non-forensic tools to retrieve the evidence relevant to the information or data gathered or might cause evidential information or data to be overwritten or altered as mentioned earlier in the time stamping leading to the loss of unrecoverable pieces of data or information evidence.

ENCASE FORENSIC TOOLKIT (Version 4)

Encase being a commercial forensic software toolkit claims to be one of the fully integrated software that allow forensic examiners to acquire suspected PDAs, search and analyze those media with the feature to generate reports in a simple environment. It also automatically generates finger prints, i.e. generation of hash values for both individual and group files and data capture hence, providing the examiner with immediate verification of

any suspected acquired evidence. Even though Encase is more widely used for the examination of PC, it includes the support for Palm OS handhelds. The latest Encase software (Version 4) does support the Palms family including Palm IIX, Palm IIIxe, Palm V, PalmVx and Palm m series. According to Guidance Software (2004), Encase also support internal macro programming language, multiple cases and multiple acquisitions. The choice of using Encase for forensic analysis of Palm OS devices resides is the strength that it can generate an entire physical bit-stream image of the Palm OS device which continuously compared the Cyclic Redundancy Checksum (CRC) blocks. This bit-stream image is being identified as an Encase evidence file which can therefore be mounted as a “virtual drive” permitting the forensic examiner to search and analyze the content of the device using either physical or logical perspective.

Moreover, Encase have the option to save files, folders or partial sections of a file for later reference known as bookmarks. These bookmarks are recorded in the case files with each having a unique bookmark file and can therefore be accessed and consulted at a later stage.

Encase software is relatively important in the writing of this paper due to its ability to acquire Palm OS devices which can be accessed and analyzed like any other raw image imported into the forensic toolkit. It is one of the most complete and fully integrated software for an examiner to search and analyze a Palm based PDA but unfortunately Encase does not support analysis of other PDA in the name of Windows Pocket PC or Linux based PDAs. However, the examiner must not limit him to using only Encase as forensics toolkit for the acquisition and the examination of PDAs as there are also other forensic tools available on the markets which are described further in this paper.

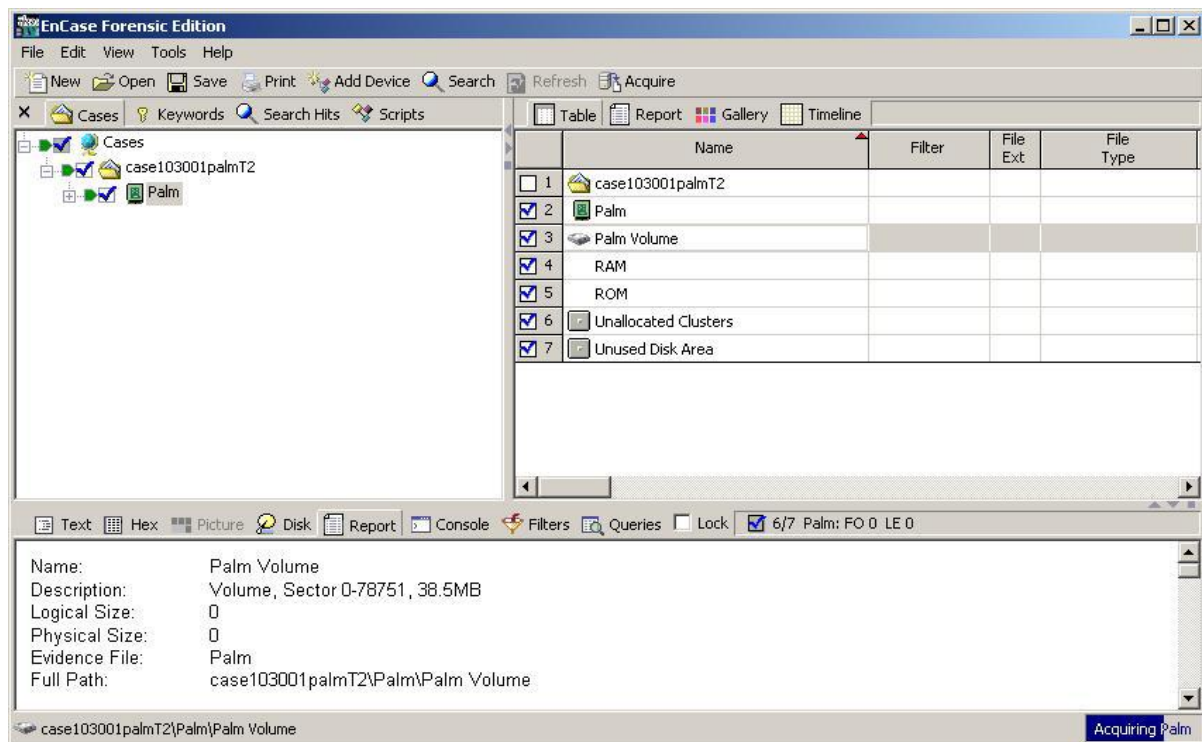


Figure 4 shows an acquisition phase by Encase.

PDA SEIZURE TOOLKITS

Another interesting toolkit which has been developed by Paraben is known as Paraben’s PDA Seizure. The latest version of PDA Seizure 3.03 allows the forensic investigator to acquire data, conduct an analysis of the acquired data and finally create a report. Contrary to Encase, PDA Seizure has been developed and adapted for either Palm OS devices or Microsoft Pocket PC and can therefore acquire both digital devices.

One amongst the features of the Paraben PDA Seizure is that it can create a forensic image of the handhelds and allow the investigator to conduct searches on the data acquired earlier, and later to execute a report generation of its findings.

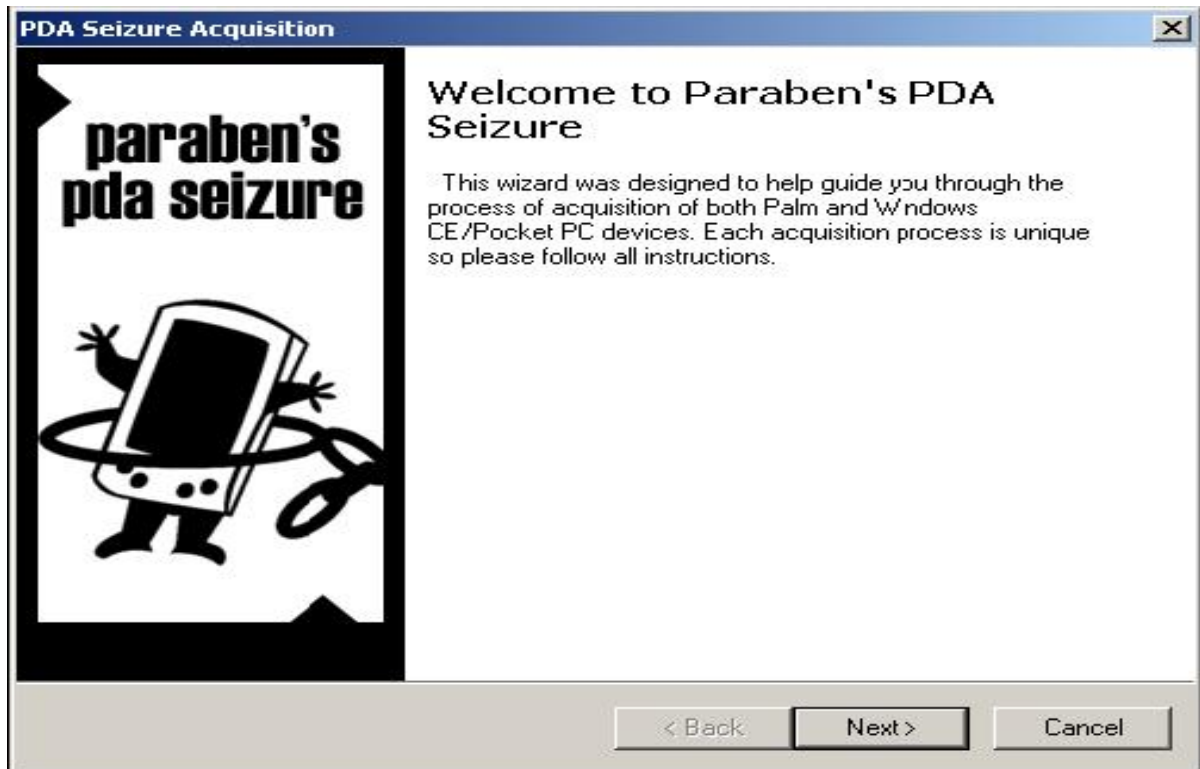


Figure 5 shows the acquisition wizard of the PDA Seizure

Another advantage of the PDA Seizure software is that it allows the investigator to analyze or search the registry of those devices thus choosing the type of acquisition is either physical or logical images as mentioned earlier.

PalmSource Inc.(2002) mentioned that PDA Seizure is preferred to Encase as it not only acquires images of the RAM and/or ROM, but it can also download the entire individual database off the Palms which can therefore be injected though Palm OS Emulators.

To acquire images in Palm OS, the PDA must first be entered into the '*debug mode*', most commonly referred to as '*console mode*' and all active HotSync applications should be exited. This is achieved by entering as Short keystroke combination by drawing a cursive 'L' character and taps the stylus twice to number "2" illustrated in the figure 6 below.



Figure 6 shows how to type in the cursive 'L' followed by the Dot and the number '2' to put the Palm in 'Console Mode'

This '*console mode*', once enable will listens on the RS232 serial port and the Universal Serial Bus (USB) port for communication from the host. Once the image of the Palm OS memory is acquired, the investigator is requested to select the HotSync button on the PDA but his time to acquire the logical data which need to be performed separately even though it has been acquired through physical acquisition. However, the forensic investigator has to bear in mind that during the "*Console Mode*" stage, the power consumption will significantly increased and has to ensure that the Palm has sufficient battery power before engaging into the acquiring process.

File Path	File Name	Type	Create Date	Modify Date	Attr...	Size	Status	MD5 Hash
	Registry					221,324	Registry	8C382C3C3D6
	MemImage					93,266,672	MemoryInr	676B2351D31
\Storage Card\	ignore_niy_docs		2003/07/03 01:23:48	2003/07/03 01:23:48	HA	0	Acquired	
\Storage Card\	f1.png	.png	2003/07/03 01:24:06	2003/07/03 01:18:34	A	4,545	Acquired	591755C36AC
\IPAQ File Store\	BioSwipe.cpl	.cpl	2003/07/02 04:35:50	2003/07/02 04:35:50	A	2,212	Acquired	91684FCCA3A
\IPAQ File Store\	ignore_niy_docs		2003/06/18 07:03:19	2003/06/18 07:03:19	HA	0	Acquired	
\IPAQ File Store\Compaq\Nevo\UserData\	3D81.dat	.dat	2003/06/19 01:37:36	2003/06/19 01:37:36	A	1	Acquired	93B885ADFEO
\IPAQ File Store\Compaq\Nevo\UserData\	C05B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFEO
\IPAQ File Store\Compaq\Nevo\UserData\	673B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFEO
\IPAQ File Store\Compaq\Nevo\UserData\	4F2C.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFEO
\IPAQ File Store\Compaq\Nevo\UserData\	9E4A.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	93B885ADFEO
\IPAQ File Store\Compaq\Nevo\UserData\	Rooms1.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:38	A	540	Acquired	E5C79F3715E
\IPAQ File Store\Compaq\Nevo\UserData\	Users1.dat	.dat	2003/06/19 01:37:38	2003/06/19 01:37:38	A	72	Acquired	F55948DCCC7
	mdmlog10.txt	.txt	2003/07/03 03:24:03	2003/07/03 03:24:03	A	54	Acquired	0CA8F822045
	GCounterFile.mmf	.mmf	2003/07/03 01:24:40	2003/07/03 01:24:40	HA	10,500	Acquired	96E85D1AF95
	CMMMapP		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	56	Acquired	BFEAC405E80
	CMMMapC		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	60	Acquired	619E024E905
\Program Files\PHM Tools\	regedit.exe	.exe	2002/11/11 14:58:20	2002/11/11 14:58:20	A	68,608	Acquired	6ED834835F8
\Program Files\	iPAQ Image Viewer.lnk	.lnk	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	33D88F9142A
\Program Files\Windows Media Player\	Welcome To Window.wma	.wma	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	818AA698890
\Program Files\Windows Media Player\	default.skn	.skn	2002/06/27 12:59:50	2002/06/27 12:59:50	A	28	Acquired	6ED00F8218A
\My Documents\	f3.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,685	Acquired	78810A8FAC1
\My Documents\	f1.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,545	Acquired	591755C36AC
\My Documents\	Recording1.wav	.wav	2003/06/18 07:03:18	2003/06/18 07:03:18	A	2,868	Acquired	C3CDF42E1FB
\My Documents\Business\	IX.psw	.psw	2003/06/18 07:05:21	2003/06/18 07:05:21	A	8,880	Acquired	DB74BD373DE
\My Documents\Templates\	Vehicle Mileage Log.pxt	.pxt	2002/06/27 12:59:50	2002/06/27 12:59:50	HRA	7,498	Acquired	9C91B8EFB3

Figure 7 illustrate an acquisition of a PDA through PDA Seizure

PILOT – LINK

Open source software developed and designed by Linux community to provide a communication bridge between Linux host and Palm OS digital devices which is known as pilot-link. This software is thus comparable with other platforms such as Mac OS and Windows. Pilot-Link uses the HoySync protocol for acquisition which is of interest to the forensic investigator. Normally there are 2 types of programs which are of interest to the investigators which are pi-getram and pi-getrum which basically extract the content stored on either the RAM or the ROM of any device. Another interest piece of software is the pilot-xfer, which install program and create backup and allow restoration of databases hence provide a means of logically acquiring the content of a device. Once acquired, the retrieved contents can therefore be manually searched through or analyzed using either Encase or POSE or a HEX Editor. Pilot-Link does not support any generation of hashing algorithms of the acquired information which unfortunately to be have generated by a different utility to match them for comparison.

PALM OS EMULATOR (POSE)

Palm OS Emulator (POSE) is software that was developed by the Palm Corporation that run on Desktop computers under different operating system and would give the exact replica of how a Palm OS device would behave once the appropriate ROM has been loaded. However, the POSE software can also be categorized into the forensic toolkit for the investigators.

Once the image has been acquired using either pilot-link or another acquisition tool and loaded into the emulator, the investigator will have the possibility to work with on image of the seized handheld in its original source without any tampering occurring thus allowing the investigator to an application same as would the original user do.

Although POSE was software that was originally developed to run, test and debug Palm OS applications without having to physically download them onto the device, it can also be configured to map Palm OS serial port to one of the available port of a PC. This emulator also reveal as a useful tool for capturing screen shots of evidences found on incriminated or seized devices.

Then the acquired images are transferred onto a PC which can have different file formats also known as Palm File Format (PFF) which matches to one of the three types described below by Howlett (2001)

- a) **Palm Database (PDB):** A record which is used to store application or user data.
- b) **Palm resource (PRC):** Palm application file that is uncompressed and can be installed directly from your PC to your Palm during synchronization.
- c) **Palm Query Application (PQA):** A Palm file containing www content for use with Palm OS wireless devices.

While the Palm OS Emulator (POSE) is installed on the PC, PDA Seizure should also be installed. POSE is therefore used to search for data in association with the PDA device within a desktop environment. The use of the emulator hence allows the examiner to have a closer look to the data that are not held by the internal viewers of the PDA Seizure.

A brief outline of the steps that should be performed while installing POSE with PDA Seizure.

- 1) Install the POSE emulator during the installation of PDA Seizure
- 2) Perform acquisition from the PDAs.
- 3) Select tools from the PDA Seizure Menu Bar and then Export All Files
- 4) Exporting All files will lead to the creation of 2 subfolders.
 - a) Card0-RAM and
 - b) Card0-ROM
- 5) Examiners should use the ROM acquired instead of downloading a ROM images, because of the ROM upgrades.
- 6) Start POSE
 - a) Select Tools and then Palm Emulator
 - b) Select New and then start a new emulator session

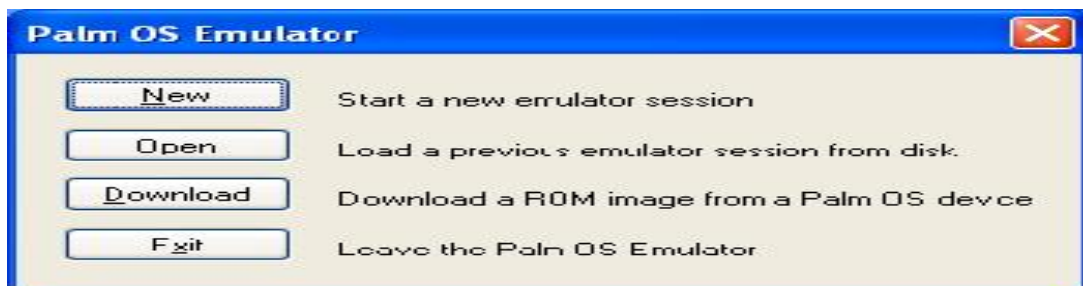


Figure 8 shows how to start the Palm OS Emulator.

- 7) Select the ROM file
- 8) Choose Other
- 9) Select the ROM image that was saved to the Card0-ROM folder.



Figure 9 shows how to select the ROM or device

Having selected the different ROM or device, the POSE will start the session and to be able to view specific files in the POSE you just have to drag and drop the different files of nature PRC, PDB, PQA onto the POSE emulator. Figure 9 shows an illustration of how the POSE emulator would look like after having loaded the imported acquired ROM or RAM of the handheld. POSE is a very useful way to perform virtual displays and confining these screen shots of relevant information as demonstrated below.

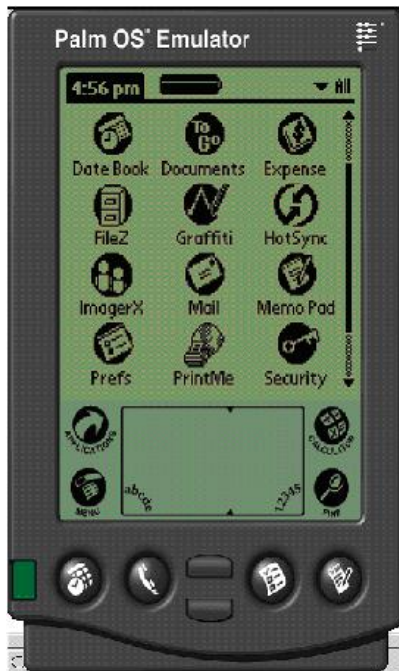


Figure 10 shows how the POSE emulator would look like after having loaded the imported acquired ROM or RAM.

PALMDD (pdd):

Designed by Grand Idea Studio; Palmdd or pdd can be used for imaging all devices running Palm OS. It is a window-based command line tool that allows the investigator to carry out the physical acquisition of data from Palm OS handhelds. The process carried out during the acquisition stage, is a bit-for-bit image of the memory's device is collected. Since pdd is a command line driven application, some features such as graphic libraries, generation of report, search facilities are not included. However, when the information has been acquired, two files are created, one containing the device-specific information such as RAM and ROM size, processor type, OS version and the second one, with the bit-for-bit image of the PDA. The created files in pdd can then be exported to a different forensic toolkit in the instance of Encase or Autopsy or simply by using a hexadecimal editor according to Carrier (2002).

DUPLICATE DISK 'dd':

The duplication disk 'dd' tools is similar to pdd and which is so far most familiar to forensic investigators as being one of the original Unix utilities which has been around for decades. To use the 'dd' command, the PDA needs to be connected directly to a PC and executing the 'dd' command and hence dumping the content in another location.

But this operation should be carefully carried out as 'dd' may destroy part of the file system thus overwriting the stored data. Images created with 'dd' can be imparted into different forensic toolkit or can be mounted onto a Linux machine for analysis. Same as pdd, 'dd' does not support the creation of hash values which need to be carried out by another utility.

ANALYSIS OF THE FORENSIC TOOLS

In order to measure the scopes of the forensic toolkits mentioned earlier in this paper, the approach of a very basic methodology was applied. The first step would be gathering a set of handheld digital devices which would be used for forensic examination. Also a set of recommended tasks would be expected to be performed on the collected devices and finally after acquiring the images of the devices with the different available toolkits, we

will try to find out if the outcomes of any activities carried out could lead to the recovery of any remnant information.

Having carried out these predefined set of tasks, a table would be generated to illustrate whether the forensic tools have met the required tasks or miss out the stated tasks or whether it has exceeded the expected outcomes or fell below.

Basically, each case will define a set of activities ranging from the data acquisition to file formats and device settings. Even though that these scenarios were not supposed to be comprehensive, they however, try to condense the situations that are most frequently encountered while conducting analysis or examination on a PDA such as data hiding, data purging, etc. This is therefore illustrated below in table 2.

No	Area	Actions Taken	Expectations
1.	PIM Applications – To find out whether the forensic tool can trace out deleted information related to the PIM applications such as memos, calendar, emails, and contacts and to do list.	Creation of some PIM files on the Palms, delete some entries made and then acquire the contents of the Palms, and display the information.	Expecting that all PIM – related information on the Palm OS can be found and recorded if it has not previously been deleted. Also that part of information or data be recovered and recorded.
No	Area	Actions Taken	Expectations
2.	Web/ Email Application – To find out if the tool can trace out any web site or email message information obtain via wireless network or synchronized from a PC.	Allow the Palm to visit some websites and make use of email, acquire the contents, try deleting some email on purpose, try to locate display the URL used or visited headers of email messages.	Expecting that data about the most recent visited websites, web mail and recent email activities can be traced out and reported and partial email data can be traced out and recorded.
3.	Graphic File – To find out if the tool can trace out and compile the different graphic files that were viewed on the device.	Enter several types of graphic images, acquire the content, locating and displaying the images.	All files having the common file extensions such as .jpg, .gif, .bmp, .tif and other can be traced back, reported and comprehensively located and displayed.
4.	Compressed File – Try to find out if the root can locate and acquire text, images and other compressed archive files such as .zip formats and less known archive such as .tar .gz tgz .rgv or self extracted exe files.	Load the PDA with several types of files acquired the contents of the PDA, try to locate and display the filename and file contents.	Text, images and other information acquired on the compressed files format be found and reported.
5.	Device Content – To find out if the tool used was successful in acquiring the content of the device.	Install the forensic toolkit on a PC, try to connect with device and start acquisition, and verify gathered data.	Hoping that information sitting on the PDA has been acquired successfully.
6.	Erased File – Find out the tool can trace and recover deleted files from PDA which involves 2 types: Attempt recovery before and after synchronization with a PC.	It involves in the creation of one or more files, delete the files, acquire the device and try to locate the deleted file.	All deleted files can be traced out, recovered and reported.

7.	Memory Cards – Try to find out if the forensic tool can acquire individual files stored on removable memory cards which are inserted into the device and if the deleted files can be retraced and recovered.	Put a memory card with a file system in the memory slot of the PDA, delete some files on the memory card, acquire the device, trace out the selected content of the file, including deleted files should be reported.	All input files that have been injected at very start can be traced out, recovered and reported.
8.	Password protection – Find out if the tool can retrieve the users' password to acquire the device.	Enable the password on the palm OS, use any utility to crack the password when acquire the Palm OS device. If the password cannot be obtained try to crack the password.	That the device could still be acquired even the password is turned on.

Table 2 illustrates the different scenario possibilities that may be faced by the examiner when in real life.

Having already defined what would be the expected results, the mentioned scenarios are hence applied to the different Palm OS devices under examination to find out to which extent the forensic tools meets the expected list.

Table 3 below illustrates the different forensic toolkits used against the targeted Palm OS devices and their release version and what we note in that most of the devices used in this experiment come with the operating system already pre-installed by their manufacturer.

Devices	Encase	PDA Seizure	dd	Version
Palm III	✓	✓	N/A	3.0
PDA Palm V	✓	✓	N/A	3.0
Dd Palm Vx	✓	✓	N/A	3.3
Tungsten C	✓	✓	N/A	5.2.1

Table 3. Different forensics toolkits available to analyze the Palm.

Legend

N/A	Not Available
------------	----------------------

Having already identified the forensic toolkits and the targeted devices, under examination, we tabulate the result of each case and hence compared to the predefined expectation illustrated in table 2 to see whether the forensic tool met the expected result.

To achieve this, a scoreboard needs to be defined to determine the different level reached by the forensic tool.

The following entries describe the different actions. “Exceed” in where the forensic tool has overcome the expected result. “Expected” in when the software has met the predefined expectations. “N/F” found would indicate that the toolkit has not been able to meet any expected results. “Poor” would be classified as not having met the expectation and finally “Not Available” would define scenarios that were not subject to the device.

The results are illustrated in Table 4 to the exception of the exception on Tungsten C handheld devices which involve the removable media which was related to deleted file recovery.

OUTCOMES OF ENCASE TOOLKIT

The cases were carried out using a Windows XP Pro machine together with the targeted Palm devices.

Scenarios/ Cases	Palm III	Palm V	Palm Vx	Tungsten C
1. PIM Application	Exp	Exp	Exp	Exp
2. Web/Email Application	N/A	N/A	N/A	Exp
3. Graphic File	Exp	Exp	Exp	Exp
4. Compressed File	N/A	N/A	N/A	Exp
5. Device Content Acquisition	N/F	Exp	Exp	Exp
6. Erased File	Poor(2)	Poor(2)	Poor(2)	Poor(2)
7. Memory Card	N/A	N/A	N/A	Poor(3)
8. Password Protection	N/A	N/A	N/A	N/A

Table 4 shows the targeted Palms under Encase forensics toolkit.

Legend

N/F – Not Found	Exp – Expected	Poor – Poor	N/A – Not Available
-----------------	----------------	-------------	---------------------

- 1- Encase being unsuccessful, another method was chosen to perform the acquisition with pdd.
- 2- Only some files were recovered, not entirely.

▪ Detailed analysis of the different Palms III/V/Vx using Encase (v4)

1. **PIM Application:** All the action PIM data was found and reported and all deleted PIM data was also recommend.
2. **Web/Email applications:** Not Applicable
3. **Graphic File:** All graphic files even the .jpg were found and reported. Note that .jpg were connected when the data was synched and displayed in the graphic library
4. **Compressed File:** Not Applicable as when the .zip files were transferred to the Palm, the files were automatically uncompressed before being uploaded
5. **Device Content Acquisition:** Encase could not acquire the Palm device thus having to use pdd for successfully acquiring the Palm which took approximately 25 minutes. The analysis was then imported to Encase as a raw image
6. **Erased File:** Most of the erased files were recovered and reported. Some partial data of graphic files were found but could not be displayed in the graphic library. We note that if HotSync was carried out after the file deletion took place but prior to acquisition stage, the files would be lost for good.
7. **Memory Card:** Not Applicable
8. **Password Protection:** Not Applicable as the Encase software does not include password creating feature.

▪ Detailed analysis of the Palms Tungsten using Encase (v4)

1. **PIM Application:** All the active PIM data was found and reported and most deleted PIM data was recovered expected for calendar and contact information.
2. **Web/Email Application:** Tungsten C has got 802.11b inbuilt capabilities thus allowing sending and receiving email and browse the internet. All visited websites were traced back and reported with all their data such as .tif, text, etc. All emails send out or received were found and reported.
3. **Compressed File:** Not Applicable.
4. **Erased File:** Most of the erased files were recovered and reported. Some partial data of graphic files were found but could not be displayed in the graphic library. We note that if HotSync was carried out after the file deletion took place but prior to acquisition stage, the files would be lost for good.
5. **Device content Acquisition:** Device was successfully acquired within 30 minutes.
6. **Memory Card** – As SD card were used but nothing could be found because the media is a removable one.
7. **Password Protection:** Not Applicable as the Encase software does not include password creating feature.

OUTCOMES OF PDA SEIZURE TOOLKIT

With PDA Seizure, the targeted Palm devices need to be put in console mode and all active HotSync applications must be exited before beginning the physical acquisition. The Paraben PDA Seizure used is the version 3.03 and were opted to acquire file and memory. If the handheld is password protected, the decode password option should be chosen before any acquisition is carried out and during acquisition stage the investigator is requested to press the HotSync button on the cradle to begin logical acquisition using the HoySync protocol.

Quick Install protocol was used for the transferring of files to the Palm. Given that Palm OS supports only the jpeg format; therefore all other formats when transferred was connected to the .jpg format.

- *Detailed analysis of the different Palms III/V/Vx using PDA Seizure (v3.03)*
 1. **PIM Application:** All active PIM data was found and reported. The deleted PIM data was partly recovered compared to deleted item in the calendar and TO DO list were not recovered whereas deleted data from contact List and Memo list was traced back.
 2. **Web/Email Application:** Not applicable
 3. **Graphic Files:** All graphics were found but graphic type were connected to .jpg format
 4. **Compressed File:** Not applicable
 5. **Device Content Acquisition:** It took 30 minutes and were successfully acquired
 6. **Erased File:** Most of the erased files were recovered and reported. Some partial data of graphic files were found but could not be displayed in the graphic library. We note that if HotSync was carried out after the file deletion took place but prior to acquisition stage, the files would be lost for good.
 7. **Memory Card:** An SD card was used but nothing could be found because the media is a removable one
 8. **Password protection:** Not Applicable as the Encase software does not include password creating feature

Scenarios/ Cases	Palm III	Palm V	Palm Vx	Tungsten C
1. PIM Application	Exp	Exp	Exp	Exp
2. Web/Email Application	N/A	N/A	N/A	Exp
3. Graphic File	Exp	Exp	Exp	Exp
4. Compressed File	N/A	N/A	N/A	N/A
5. Device Content Acquisition	Exp	Exp	Exp	Exp
6. Erased File	Poor1	Poor1	Poor1	Poor1
7. Memory Card	N/A	N/A	N/A	N/F2
8. Password Protection	Exp	Exp	Exp	N/A

Table 5 shows the targeted Palms under PDA Seizure toolkit

Legend

N/F – Not Found	Exp – Expected	Poor – Poor	N/A – Not Available
-----------------	----------------	-------------	---------------------

- 1 – Some data was recovered but not the entire content
- 2 – Memory Card was not discovered and its contend not acquired

Tungsten C

Password Protection – Not Applicable because the OS version is higher than 4.0 hence PDA Seizure could not crack the password.

CONCLUSION

The outcome produced in this paper reveals that to perform forensic acquisition of PDA devices is not an easy task and with technology advancing rapidly this practice becomes more and more difficult for forensic investigators specially when it comes to acquire images off such devices which are used to store run-time

information which sometimes can be updated and altered on a frequently time basics. PDA forensic is a growing area in mobile forensic. However, the forensic toolkits used in this paper behaved as expected. Therefore it is crucial that the forensic investigator knows the limits of the used tool and also when to and how to turn to other forensic tools as means of examination in order to maintain a chain of custody. The outcomes of this experiment definitely emphasizes on proper documentation especially when dealing with mobile handheld devices such as Palm. The investigator should by all means ensure that every actions are fully documented even the slightest change of time or environment to prove that no temping of data has occurred.

REFERENCES

- Ayers, R. & Jansen W. (2004). PDA Forensic Tools: An Overview and Analysis. Retrieved May 3, 2007 from NIST: <http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf>
- Canalys. (2004). Global Mobile Device Market Shows Tremendous Growth. Retrieved May 25, 2007, from <http://www.canalys.com/pr/2004/r2004081.htm>
- Carrier, B. (2005). File System Forensic Analysis. Addison Wesley Professional.
- Cheong, K.,W. & Wong, L., W. (2005) Forensic Image Analysis of Familiar-based iPAQ. Retrieved May 12, 2007, from <http://www.forensicfocus.com/downloads/familiar-ipaq-forensic-analysis.pdf>
- CompactFlash Association. (2004). CompactFlash Association Homepage. Retrieved April 22, 2007, from <http://www.compactflash.org/>
- Fernandes, L. (2003). Palm OS dot short-cuts. Retrieved May 18, 2007, from <http://www.ee.rverson.ca/~elf/visor/dot-shortcuts.html>
- Frichot, C (2004). An Analysis of the Integrity of Palm Images Acquired with PDD. Retrieved May 11, 2007, from http://scissec.scis.ecu.edu.au/publications/2004_FRICHOT_ACNIFC_Analysis_of_the_Integrity_of_Palm_Images_Acquired_with_PDD.pdf
- Grant, J. (2002). Pdd: Memory Imaging and Forensic Analysis of Palm OS Devices. Retrieved May 26, 2007 from http://www.grandideastudio.com/files/security/mobile/pdd_palm_forensics.pdf
- Guidance Software. (2004). Encase Forensic Edition: The Standard in Computer Forensics. Retrieved May 30, 2007, from <http://www.encase.com/products/downloads/efe-datasheet.pdf>
- Hillerman, G. (2003). Palm OS File Format Specification. Retrieved May 17, 2007 from <http://www.palmos.com/dev/support/docs/fileformats/FileFormatsTOC.html>
- Hitachi Global Storage Technologies. (2004). Hitachi Global Storage Technologies Product Information. Retrieved April 11, 2007, from <http://www.hgst.com/portal/site/en/menuitem.a994b57654279b5daa67bca4bac4f0a0/>
- Howlett, A., (2001) Palm OS Programmer's FAQ. Retrieved May 31, 2007 from http://palmtops.about.com/od/pdaglossary/g/PRC_File.htm
- InformIT (2005). PDA Forensics. Retrieved May 18, 2007, from <http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=104>
- Jansen, W., & Ayers, R. (2004). Guidelines on PDA Forensics. Retrieved May 19, 2007 from <http://www.csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf>
- Kruse II, W. G., & Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials. Boston: Addison- Wesley.
- McKemmish, R. (1999). What is Forensic Computing? Canberra, Australia: Australian Institute of Criminology.

- Memorystick.com Business Center. (2004). Memory Stick Media Capacity. Retrieved April 12, 2007, from <http://www.memorystick.com/en/ms/variety1.html>
- Multimediacard Association. (2004). MMCA: Home Page. Retrieved April 12, 2007 from <http://www.mmca.org/>
- PalmSource (2004). Palm OS® Programmer's Companion Volume I. Retrieved April 27, 2007, from <http://www.palmos.com/dev/support/docs/palmos/Memory.html>
- PalmSource Inc. (2002). Palm OS Emulator (Version 3.5). Retrieved April 22, 2007, from http://www.access-company.com/developers/documents/docs/emulator/Emulator_Front.html
- PalmSource Inc. (2004). Memory | Palm OS Programmer's Companion. Retrieved May 25, 2007, from <http://www.palmos.com/dev/support/docs/palmos/Memory.html>
- PalmSource Inc. (2004b). PalmSource | Palm OS. Retrieved May 29, 2007, from <http://www.palmsource.com/palmos/>
- Paraben Corporation. (2005). PDA Seizure. Pleasant Grove, UT.
- PaulEggleton (2005). FamiliarFaq. Retrieved May 17, 2007, from <http://handhelds.org/moin/moin.cgi/FamiliarFaq#head-87a7fac0185ca2be60ecd1a946827adef5921208>
- SD Card Association. (2004). Concept of SD memory Card. Retrieved April 12, 2007, from http://www.sdcard.org/sd_memorycard/index.html

COPYRIGHT

Krishnun Sansurooah ©2006. The author/s assigns SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.