2004

Forensic analysis of digital evidence from Palm Personal Digital Assistants

Christopher M. McNemar
West Virginia University

Follow this and additional works at: <https://researchrepository.wvu.edu/etd>

Recommended Citation

McNemar, Christopher M., "Forensic analysis of digital evidence from Palm Personal Digital Assistants" (2004). *Graduate Theses, Dissertations, and Problem Reports*. 1550.
<https://researchrepository.wvu.edu/etd/1550>

This Thesis is protected by copyright and/or related rights. It has been brought to you by the The Research Repository @ WVU with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you must obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This Thesis has been accepted for inclusion in WVU Graduate Theses, Dissertations, and Problem Reports collection by an authorized administrator of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.

Forensic Analysis of Digital Evidence from Palm Personal Digital Assistants

Christopher M. McNemar

**Thesis submitted to the
College of Engineering and Mineral Resources
at West Virginia University
in partial fulfillment of the requirements
for the degree of**

**Master of Science
In
Computer Science
With Emphasis On
Computer Forensics**

**Roy S. Nutter, Jr., Ph.D., Chair
John M. Atkins, Ph.D.
Bojan Cukic, Ph.D.**

Lane Department of Computer Science and Electrical Engineering

**Morgantown, West Virginia
2004**

**Keywords: PDA Forensics, Palm Forensics, Digital Forensics, Digital Image Analysis,
Digital Evidence
Copyright 2004 Christopher M. McNemar**

ABSTRACT

Forensic Analysis of Digital Evidence from Palm Personal Digital Assistants

Christopher M. McNemar

Personal Digital Assistants are becoming more affordable and commonplace. They provide mobile data storage, computational, and network abilities. When handheld devices are involved in a crime, forensic examiners need tools to properly retrieve and analyze data present on the device. Unfortunately, forensic analysis of handheld devices is not adequately documented and supported.

This report gives an overview of Palm handheld development and current forensic software related to Personal Digital Assistants. Procedures for device seizure, storage, imaging, and analysis are documented. In addition, a tool was developed as part of this work to aid forensic examiners in recovering evidence from memory image files.

Table of Contents

CHAPTER 1: Introduction	1
1.1 Statement of Problem.....	1
CHAPTER 2: Palm Development History	2
2.1 1990s	3
2.2 2000.....	4
2.3 2001.....	4
2.4 2002.....	4
2.5 2003.....	5
2.6 2004.....	5
CHAPTER 3: Software	6
3.1 Palm Utilities	6
3.1.1 Palm Desktop	6
3.1.2 Palm Debugger.....	6
3.2 Palm DD.....	8
3.3 Unix Duplicate Disk.....	10
3.4 Palm OS Emulator	10
3.5 Paraben's PDA Seizure	11
3.6 EnCase	13
3.7 Forensic Toolkit	15
3.8 Hex Editors	15
CHAPTER 4: Device Seizure	17

4.1 Expansion Cards	19
4.1.1 Storage Cards	19
Compact Flash Cards	20
Multi-Media Cards	21
Secure Digital Cards	21
4.1.2 Functionality Cards	22
4.2 Packaging and Transport.....	23
CHAPTER 5: Device Storage	25
CHAPTER 6: Device Imaging.....	26
CHAPTER 7: Device Analysis	28
7.1 Raw Image Analysis	28
7.2 ImageView	30
7.2.1 ImageView Design.....	30
7.2.2 ImageView Execution.....	32
7.2.3 Considerations	34
7.3 POSE.....	35
7.4 Password Protection.....	40
7.5 Retrieval of Palm Passwords	40
7.6 Retrieval of Encrypted Memory	41
CHAPTER 8: Conclusions and Future Work	42
8.1 Conclusions	42
8.2 Future Work	42

Bibliography.....	44
APPENDIX A: ImageView Source Code.....	46
APPENDIX B: Summary Sheet.....	49

Table of Figures

Figure 1. Graffiti stroke required to enable the Palm Console Mode	7
Figure 2. Graffiti stroke required to disable automatic power-off.....	7
Figure 3. Deleting a Memo	9
Figure 4. Making a Record Private	9
Figure 5. Files Recovered with Paraben's PDA Seizure	12
Figure 6. Acquisition Options in Encase	14
Figure 7. Palm Image in EnCase.....	15
Figure 8. Device Seizure	19
Figure 9. Compact Flash Card	20
Figure 10. Multi-Media Card	21
Figure 11. Secure Digital Card	21
Figure 12. Wi-Fi Card	22
Figure 13. GPS Receiver.....	22
Figure 14. Palm and Modem.....	22
Figure 15. Binary Image Viewed With WordPad.....	29
Figure 16. Binary Image Viewed With UltraEdit	29
Figure 17. Mixed Binary and Text Image Viewed With UltraEdit	30
Figure 18. ImageView Execution	32
Figure 19. ImageView Address Book.....	33
Figure 20. ImageView MemoPad	33
Figure 21. MD5SUM Before and After ImageView Execution.....	34

Figure 22. POSE Running m100 ROM	35
Figure 23. POSE Running m100 ROM with m100Skin.....	36
Figure 24. POSE View of Date Book	38
Figure 25. POSE View of Address Book.....	38
Figure 26. POSE View of To Do List.....	39
Figure 27. POSE View of MemoPad	39

CHAPTER 1: Introduction

This paper will seek to both summarize and expand on recommended procedures and the software available for those conducting a forensic examination of a Personal Digital Assistant.

A PDA provides a mobile and compact means to store digital information. A PDA can provide a criminal with a means to store contact information, credit card numbers, images, and numerous files to help them in their illegal endeavors. To narrow the focus of this paper, specifically Palm brand devices running the Palm OS[®] have been addressed.

This document will first seek to present a brief history of the Palm platform. It will then cover other software that will aid a forensic examiner. These software programs will include imaging tools, analysis programs, and miscellaneous tools that examiners will find useful. The topics of evidence seizure and transportation will then be addressed, followed by coverage of device imaging using the PDD utility. Finally, three types of image analysis will be discussed: viewing the raw output of the image, viewing the image using the ImageView utility designed in conjunction with this thesis, and loading the image into the Palm OS Emulator.

1.1 Statement of Problem

The field of Digital Forensics has long focused on seizing and recovering evidence from personal computers (PCs). However, many criminals are now using electronic devices other than PCs to commit illegal activities. Cellular telephones, pagers, and Personal Digital Assistants (PDAs) are only a few of the devices that must now be examined by forensic investigators. Even though

the Digital Forensics sector is relatively new, there are commonly accepted practices and industry-standard software to aid forensic examiners in the investigation of PCs. However, forensic tools for non-PC devices have not kept pace.

CHAPTER 2: Palm Development History

Table 1. Palm Development History

Year	Number of New Handhelds	New Features	Notable Events
1990s	9	Wireless Internet	3Com purchased Palm Computing
2000	4	Color Screens	Palm open for trade on the NASDAQ
2001	4	More Memory Electronic Mail Internet Connectivity	
2002	6	Bluetooth-enabled Integrated Wireless	Palm OS 5.0
2003	7	Built-In Camera Audio/Video Playback JAVA enabled	Palm OS is added to non-PDA devices such as GPS receivers and cellular telephones
2004	3 ¹	MP3	

¹ As of the writing of this report.

2.1 1990s

Palm Computing was founded in 1992 and acquired by US Robotics, a telecommunications hardware manufacturer, in 1995. Four years after the company opened, Palm introduced the Pilot 1000 handheld. In March of 1997, Palm Computing debuted their next generation of PDAs, the Palm Pilot Professional and Personal Editions. In the fall of 1997, 3Com purchased US Robotics, and thus obtained Palm Computing Inc. In December 1997, Palm began licensing its Palm OS® Platform. The Palm OS® Platform powers products produced by Aceeca, AlphaSmart, Fossil, Foundertech, Garmin, GSPDA, Kyocera, Lenovo, palmOne, QTech, Samsung, Sony, Symbol, and Tapwave (1). A year after the introduction of the Palm Pilot series, Palm introduced the Palm III organizer, the third generation of the Palm Pilot handheld based on the Palm OS® platform.

In 1999, Palm Computing produced several notable accomplishments with the launch of the Palm IIIx, Palm V, Palm IIIe, and Palm Vx handheld organizers. Along with these, Palm introduced the Palm VII Connected Organizer. The Palm VII Connected Organizer gave users wireless access to the Internet. A report published by the International Data Corporation in May 1999, announced that Palm had 73% of the US market and over 68% worldwide for handheld products.

2.2 2000

In February 2000, Palm debuted their first color-enabled models, the Palm IIIc color handheld and the expandable Palm IIIxe handheld. Later that year, the Palm VIIx and the Palm m100 were introduced. This year also saw Palm open for trade on the NASDAQ, in addition to a new partnership with IBM to provide e-Business solutions.

2.3 2001

Four new models were added to the m series in 2001. The models extended the power of the Palm line by adding more memory, e-mail capability, Internet connectivity, color, and other features. Another additional package for the Palm is the PalmDataViz's Documents To Go Software, which allows users to view Microsoft documents on their handhelds.

2.4 2002

The Palm handhelds that debuted this year were Bluetooth-enabled, included integrated wireless, and provided secure access to online resources such as America Online's Instant Messenger and wireless e-mail. Palm OS 5.0 was introduced. In addition, the Palm Zire was the first model marketed for under one hundred dollars, moving Palm into the realm of the general public.

2.5 2003

In 2003, Palm OS was added to non-PDA machines such as GPS handhelds from GARMIN and cellular telephones. Palm devices now have multimedia capabilities with built-in digital cameras, audio/video playback, and high-resolution color screens. Some Palm devices are also JAVA enabled.

2.6 2004

In 2004, two color Zire handhelds were added to the Palm family. These handhelds are able to take digital pictures and videos. They are also capable of acting as an MP3 player. The two models, like their predecessors, are Bluetooth enabled. Palm Corporation also collaborated with several cellular service providers such as Sprint and T-Mobile to market their line of smart phones (2).

CHAPTER 3: Software

3.1 Palm Utilities

3.1.1 Palm Desktop

Palm Desktop is distributed by Palm with their handhelds. It allows users to manage data that is stored on their handhelds and provides date, address, and memo entry. This provides users with a more functional way to enter text. Data on the handheld is input via a stylus and a touchpad that interprets the user's pen strokes. Palm Desktop also provides functionality for the installation of third-party software on the Palm and for the performance of HotSync operations. HotSync is the software from Palm that is responsible for synchronizing data between a Palm handheld and a desktop computer. This utility allows backup and transfer of data between the PC and the handheld.

3.1.2 Palm Debugger

The Palm Debugger provides low-level system debugging for Palm applications. The Palm Debugger is included on all Palm handhelds and in the Palm OS Emulator. To enter the Palm OS Console Debugger on a device, the user must draw the shortcut symbol, which is a lowercase, cursive "L." Then tap the stylus twice to generate a dot, followed by the number "2":

Figure 1. Graffiti stroke required to enable the Palm Console Mode

This command will cause the device to enter the console mode and wait for communication. In addition, this mode opens a serial port, which will drain power over time. A soft reset will be needed to exit this mode. To perform a soft reset, depress the reset button on the back of the handheld using a blunt instrument such as a paper clip (3, pg. 7-8).

In addition, to enter the Console Debugger, examiners may also wish to disable the device's automatic power-off feature. This will prevent the device from turning off in the process of device imaging. To deactivate the automatic off, the user must draw the shortcut symbol, which is a lowercase, cursive "L." Then tap the stylus twice to generate a dot, followed by the number "3".

Figure 2. Graffiti stroke required to disable automatic power-off

The user will still be able to turn the device off and on using the device's power button. To reactivate the automatic power-off feature, a soft reset will be required.

3.2 Palm DD

Palm DD, or PDD, was designed by Grand Idea Studios for imaging all devices running Palm OS. This program and its source code is freely available from their website, <http://www.grandideastudio.com/>. These devices currently include consumer-based PDAs, telephones integrated with PDA functionality, and barcode and wireless integration for industrial applications.

In addition to providing a physical bit-by-bit image of the specified memory card, PDD extracts and displays the following device information:

- Card Number
- Manufacturer Name
- Creation Date
- Processor Type
- Free RAM
- ROM Used By OS
- Card Name
- Card Version
- Palm OS Version
- RAM Size
- ROM Size
- Flash ID (if available) (4, pg. 2)

The image provided by the PDD utility includes applications, databases, passwords, and anything else on the Palm device. Database fragments and records that have been marked for deletion may also appear in the image. However, deleted records will only be found if the user has selected the “Save archive copy on PC” option when deleting a record:

Figure 3. Deleting a Memo

If this is the case, the record will remain until the next successful HotSync operation. Users also have the choice to mark their records as Private. This sets a flag in the header requiring users to enter the password to view the record. Since the PDD utility bypasses the Palm OS, these records will be included in any image files made.

Figure 4. Making a Record Private

The PDD utility partially uses Palm's OS Console Mode Debugger to acquire information and create the memory image. Because of this, no additional software has to be installed on the seized Palm device. In addition, the PDD utility can sometimes image devices if the device is password protected. This allows examiners to view the contents of the device even if the examiner does not know the password. An image can be obtained as long as the device is

imaged before the password protection is activated. However, if the lock option is activated or the Palm is turned off, password protection may be activated.

3.3 Unix Duplicate Disk

The Unix Duplicate Disk, or DD, should be a tool with which most forensic examiners are familiar. The DD utility makes a bit-by-bit image of any compatible file system that can be forensically examined. The command works like the above PDD utility, but operates directly on the device. This operation is invoked either by a remote connection or directly from the command line. Operating software on the device is not desirable since it can change the contents of the device and possibly destroy or overwrite part of the file system if used incorrectly.

3.4 Palm OS Emulator

The Palm OS Emulator (POSE) was developed by the Palm Corporation to run on desktop computers. The POSE software emulates the hardware of most Palm models based on ROMs available on the Palm website (5). The software was originally intended as a means for developers to debug and test their Palm applications. The ability to download various ROMs allows developers to test on a wide-range of platforms that they normally would not have access to. However, the POSE software can also be used for forensic examinations. Once a seized Palm's ROM memory has been imaged, the image can be loaded into the POSE program. This process allows an investigator to work with an image of the seized device in its original format without compromising the integrity of the original evidence. The examiner can view and run

applications just as the original user would have. Application databases such as phone records, memos, and notes can easily be viewed. Running images in the POSE software also allows investigators to easily take screenshots and present them as evidence. Investigators can even apply skins to POSE to give it the appearance of the seized device.

3.5 Paraben's PDA Seizure

Paraben's PDA Seizure (6) is the only commercial software package focused specifically on PDA forensics. The PDA Seizure software package has a wide range of abilities including:

- USB support on Palm PDA
- Built-in recovery of Palm password (Prior to Palm OS 4.0)
- Enhanced viewing of file data
- Complete physical and logical acquisition for Palm PDA devices
- Built-in searching and bookmarking
- Textual and Hexadecimal views of data available
- HTML reporting
- Verification of image integrity
- Internal viewing of data files
- Internal viewing of graphic files
- Files compatible with POSE

File Path	File Name	Type	Create Date	Modify Date	Attributes	Size	Status	L...	MD5 Hash
	Registry					3,966	Registry		3050A80D
	MemImage					3,680	MemoryImage		F2C4410A
{Program Files\Win default.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		23	Acquired	RAM	6BD33A62
{My Documents\ Welcome To W	.wma		2000/01/01 20	2000/01/01 20:A		24	Acquired	RAM	818AA698
{My Documents\Te Vehide Mileage	.pxt		2000/01/01 20	2000/01/01 20:HRA		7,498	Acquired	RAM	9C91BBEFe
{My Documents\Te To Do.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		2,616	Acquired	RAM	0F7982DEE
{My Documents\Te Phone Memo.p	.psw		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	9443F21C
{My Documents\Te Memo.psw	.psw		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	523694AF
{My Documents\Te Meeting Notes	.psw		2000/01/01 20	2000/01/01 20:HRA		1,908	Acquired	RAM	40FB8E424
{My Documents\Te Blank Documer	.psw		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
{My Documents\Te To Do.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		3,096	Acquired	RAM	B25EAC50
{My Documents\Te Phone Memo.p	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	7F2CCAB0
{My Documents\Te Memo.pwi	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	CAC4C826
{My Documents\Te Meeting Notes	.pwi		2000/01/01 20	2000/01/01 20:HRA		1,592	Acquired	RAM	B876D7DE
{My Documents\Te Blank Note.pw	.pwi		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
{Windows\Home M HP game butt	.lnk		2000/01/01 20	2000/01/01 20:A		18	Acquired	RAM	72E4BACB
{Windows\Home M HP backup.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		20	Acquired	RAM	8DA836DA
{Windows\Home M Regional Sett	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	E0723177E
{Windows\Home M Network.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AD4F5D1A
{Windows\Home M Clock.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	2FA61C9B
{Windows\Home M Modem.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AC946E0E
{Windows\Home M PC.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	C02FC610
{Windows\Home M Today.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	6A65E55E
{Windows\Home M Buttons.lnk	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	7CFAA908

Figure 5. Files Recovered with Paraben's PDA Seizure²

The PDA Seizure software relies upon an integrated version of Grand Studio's PDD utility, detailed above. PDA Seizure also incorporates support for Palm's POSE software to view and analyze evidence. PDA Seizure is able to override password protection for any Palm model running an operating system earlier than Palm OS 4.0. For Palm OS 4.0 or newer, Paraben recommends the use of their password recovery software, Paraben's Decryption Collection. In order for Paraben's Decryption Collection to recover a Palm password, the software will need to be run on the desktop machine that the Palm HotSynced with. Without either the password override or the recovered password, PDA Seizure will not be able to acquire a device image.

² Image obtained from <http://www.paraben-forensics.com/>

NOTE

“PDA Seizure uses the Palm HotSync protocol for some portion of memory imaging. Because of this, the Last HotSync Date is modified on the Palm Device. Depending on how the acquisition process is implemented, there may be issues of only retrieving data that is known to the OS as being a database, so the acquisition would miss obfuscated or hidden forms of data” (4, pg. 12).

In addition to the PDA Seizure software, Paraben also markets a PDA Seizure Toolbox. The PDA Seizure Toolbox includes cables, power adapters, batteries, and adapters to seize and image over 35 different PDAs. Most of the included hardware is designed to function with multiple types of handhelds. The PDA Seizure Toolbox can interface with the following brands and models:

- iPAQ Series-3100, 3600, 3700, 3800, 3900
- Jornada Series-520, 540, 560
- Cassiopeia Series-E-125, EM500, EG-800
- Clie Series-All Available
- Visor Series-All 5 series
- Palm Series-III, IIIC, HandEra, 330, VII, VIIx, IIIxe, IIIx, IIIE, Palm Pilot, Pilot, V, Vx, m100, m105, m500, m505, m515, m125, m130, i705 (7)

3.6 EnCase

Guidance Software’s EnCase is normally used to examine personal computers, but can also be used to examine supported Palm PDAs. This commercial product can be obtained through Guidance Software’s website at <http://www.guidancesoftware.com/>. The latest version of

EnCase supports the IIX, IIIxe, V, VII, and m series Palms. The software works much the same as it does for normal PC drives. The Palm PDA is placed in its cradle and EnCase is opened. The Palm must then be turned on and put into console mode. After that, the Palm can be added as a device and an image acquired. If the device is password protected, the password must be entered during the Acquire process. EnCase does not provide any functionality to bypass or decrypt device passwords.

Figure 6. Acquisition Options in Encase³

The resulting image will be a physical bit image. EnCase Examiner will then proceed to extract files, folders, data, and images from the memory image. The examiner can view these files based on their type and related application, as seen below.

³ Image obtained from <http://www.guidancesoftware.com>

Figure 7. Palm Image in EnCase⁴

3.7 Forensic Toolkit

The AccessData Forensic Toolkit is a commercial package that offers law enforcement and corporate security professionals the ability to perform computer forensic examinations. The Forensic Toolkit features file filtering and search functionality. Forensic Toolkit's customizable filters allow examiners to sort through files to quickly find evidence. AccessData's Forensic Toolkit version 1.50a does not support forensic analysis of PDAs. However, at the time of this writing, AccessData was planning on implementing support for acquisition and imaging of PDAs with the release of Forensic Toolkit 2.0 (8).

3.8 Hex Editors

A hex editor is a program that allows users to view the raw contents of binary files and data. Hex editors will display the raw data on one side and the hex value on the other. If a commercial

⁴ Image obtained from <http://www.guidancesoftware.com>

analysis program such as Encase or PDA Seizure is not used for the examination, a hex editor will be crucial. A hex editor will also display the entire image file, instead of the extracted and cosmetically altered data that commercial analysis tools display. This will allow examiners to view the entire contents of the image, even those items that the commercial programs may filter out as extraneous.

CHAPTER 4: Device Seizure

The utmost care has to be taken when obtaining a PDA device from a crime scene. In many cases, PDA memory is more volatile than that of personal computers. All handhelds are typically powered by either an alkaline or a lithium-ion battery. If the device loses power, the chance of recovering data is negligible. In cases where the device is powered by alkaline batteries, fresh batteries should be inserted. In cases where the power is supplied from a lithium-ion battery, the device should be placed on a charging cradle or a new battery inserted. Even though PDAs of both types hold a small capacitance charge to provide power during battery changes, these actions have the potential to alter data on the handheld. Therefore, it is necessary that any imaging and documentation should be conducted beforehand (9, pg. 29). Additionally, PDAs are not as common as personal computers, leaving Crime Scene Investigators with less experience dealing with handhelds. In any case when the Crime Scene Investigator is unsure how to best proceed with evidence collection, it would be advisable to contact a Digital Forensic Examiner.

Once a crime scene is secured, a topic not covered in this document, evidence collection must begin. With respect to PDAs, handhelds will be found in one of the following states:

1. Powered On
2. Powered Off

And one of the following two states:

1. Device in Cradle and Connected to PC

2. Device out of Cradle

The device will be either Powered On or Powered Off. In addition, it will either be Connected to the PC or Have No PC Connection. Before any other steps are taken, the screen should be photographed and the information that is displayed recorded.

If the device is in a cradle, the PC interface connection should be terminated by first unplugging the cable from the handheld and then from the PC. This prevents the computer from altering any data that is contained on the handheld. If the device is on and the power is low, the power source should be immediately replaced or recharged. If the handheld loses power, the chance of successfully recovering data from the seized device is small. The necessary power adapter should be part of any forensic seizure kit. If the device is on, an image should be taken and then the device should be powered down. It is important to obtain an image as soon as possible because powering the device down might result in the loss of evidence.

Whenever a Crime Scene Investigator takes any action with handhelds or peripherals, the action should be thoroughly documented. Documentation should include what was done, when it was done, and for what reason. To aid Crime Scene Investigators, Figure 8 has been developed.

Figure 8. Device Seizure

4.1 Expansion Cards

Palm devices may also come with a wide-range of peripherals and cards. These cards generally serve one of two purposes: providing more storage or expanding functionality.

4.1.1 Storage Cards

Storage cards come in three varieties: Compact Flash, Multi-media, and Secure Digital. The function of these cards is to provide additional storage beyond that in the handheld. For this reason, it is important to seize any storage cards that can be found when seizing the Palm. These cards can hold variable amounts of data, ranging from two megabytes to one gigabyte. Storage

cards still in Palm handhelds should not be removed by the Crime Scene Investigator. Instead, the card should be left in place and packaged with the handheld.

Compact Flash Cards

Figure 9. Compact Flash Card⁵

A Compact Flash memory card, as pictured in Figure 9, is a solid-state disk card with a 50-pin connector. The pins provide a connection between the memory and the Compact Flash drive in the electronic device. Compact Flash cards are more similar to hard drives than RAM. They are designed with flash technology, a non-volatile storage solution that does not lose its information once power is removed from the card. The cards contain no moving parts and are rugged, providing greater protection of data than conventional magnetic disk drives.

Compact Flash Type I cards weigh a half-ounce and are the size of a matchbook, 1.6" long, 1.4" high, and .13" thick. They are thinner than Type II cards, which are 1.6" long, 1.4" high, and .19" thick. Both cards have two parallel rows of 25 pins on one edge of the card.

⁵ Image obtained from <http://www.crucial.com>

Multi-Media Cards

Figure 10. Multi-Media Card⁶

A Multi-Media Card, as pictured in Figure 10, is a solid-state disk card with a 7-pin connector. The pins provide a connection between the memory and the electronic device. Multi-Media Cards are more similar to hard drives than RAM. They are designed with flash technology, a non-volatile storage solution that does not lose its information once power is removed from the card. The cards contain no moving parts and are extremely rugged, providing much greater protection of data than conventional magnetic disk drives. Multi-Media Cards weigh 2 grams and are about the size of a postage stamp, 1.26" x .94" x .06".

Secure Digital Cards

Figure 11. Secure Digital Card⁷

The Secure Digital (SD), as pictured in Figure 11, card's low battery consumption makes it ideal for use in battery-powered products. Data on the Secure Digital Music Initiative (SDMI)-

⁶ Image obtained from <http://www.palmone.com/>

⁷ Image obtained from <http://www.palmone.com/>

compliant SD memory card is accessible using either an SD interface or a serial peripheral interface, providing quick and dependable data transmission.

4.1.2 Functionality Cards

Besides storage, peripheral cards also can be used to expand the functionality of Palm handhelds. The visual appearance of these cards can vary, but samples were obtained from the Palm Corporation website and are displayed in Figure 12, Figure 13, and Figure 14.

Figure 12. Wi-Fi Card

Figure 13. GPS Receiver

Figure 14. Palm and Modem

If these cards are connected to the handheld and found in an On state, the Crime Scene Investigator should eliminate the possibility of further communication between the PDA and another source, such as a router or computer, to keep evidence intact. The cards should then be removed and packaged in a special isolation envelope to prevent further communication. In the case of finding a GPS receiver, the forensic examiner may be able to retrieve data that will place the exact location of the handheld at a specific time. This may even lead to placing the handheld user at the scene of a crime, or tracking criminal activities.

4.2 Packaging and Transport

Before packaging the seized evidence, all collected items should be properly documented, labeled, and inventoried. This documentation should contain:

- Who obtained the item
- Where it was obtained (in relationship to other evidence)
- When it was obtained
- All steps that were taken in obtaining it:
 - Disconnecting cables
 - Device imaging
 - Any type of input
- Any images of the evidence as found by the investigator

When packaging seized evidence, all magnetic media should be placed in anti-static packaging, or paper bags if none are available. Placing media in standard plastic bags should be avoided because such materials can produce static electricity that can damage the media. When placing the media in packaging, folding, bending, and scratching should be avoided because it can damage the data contained on the discs. Handhelds should be wrapped in anti-static bubble wrap and packaged in the same manner as magnetic media. All cords, connectors, and cradles should be packaged along with the handheld. If possible, a diagram should be included showing how the handheld was connected to the computer when it was seized.

When placing seized evidence in a vehicle for transport, it should be placed away from any magnetic sources. Magnetic sources can include, but are not limited to, radio transmitters, speaker magnets, and heated seats. The interior of the car should not be excessively hot, cold, or humid. In addition, evidence should not be stored in a vehicle for prolonged periods of time. Seized electronics should be secured in the vehicle in such a way as to minimize shock and unnecessary vibrations. A chain of custody should be kept. To maintain a *credible* chain of custody, evidence should be “stored in a tamper-proof manner, where it cannot be accessed by unauthorized individuals” (10, pg. 200).

CHAPTER 5: Device Storage

Due to the volatile state of PDA memory, handhelds should immediately be checked into a forensic laboratory to be processed, and the evidence custodian should be informed 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. Steps include periodic monitoring of the power level. 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 (11).

While the device is in storage, an accurate log should be kept. It is not enough to know the current location of the evidence. A tracking log should be kept of the movement and possession of the evidence at all times. Forensic Examiners should be able to track the location of the original data source from the time it comes into the investigator's possession until any legal or civil proceedings have been concluded. More so, the evidence handler must control and audit physical access to the data while it is in law enforcement's possession. It is important to keep accurate and precise logs and notes because any documentation done by the examiner could be used for legal purposes. In addition, the investigator should ensure that the state of the evidence is the same as it was when seized.

CHAPTER 6: Device Imaging

Forensic analysis should be conducted only on the acquired image. This allows forensic examiners to start from the same base image. In addition, working directly on the seized device can lead to data corruption. This corruption can occur through user error, malicious programming, or normal operations. Unless a credible image can be made of the device, valuable evidence can be destroyed or compromised.

Two image files are used below as examples. The example PDA was imaged by the PDD utility. The first was an image of the Read Only Memory (ROM), and is named “m100_ROM.” The second was an image of the Random Access Memory (RAM), and is named “m100_RAM.” The process of producing the memory image is not covered in this thesis since it has already been documented in “pdd: Memory Imaging and Forensic Analysis of Palm OS Devices” by Joseph Grand (4). When imaging the handheld, it will be necessary to make multiple images. This is because the PDD utility will only image the RAM or ROM memory separately. An image of the Flash memory and any attached storage cards will also be needed. Users should consult the PDD manual for these options.

The RAM portion of a Palm handheld is divided into two partitions. The first of these is the Dynamic RAM. Dynamic RAM includes the program heap, short-term data, and global variables. RAM memory is used as runtime memory for program execution as well as

permanent storage of data. The size of the RAM partition will vary based on application needs and the Palm model (12).

The ROM portion stores the Operating System databases and standard applications found on Palms. These standard applications include a calculator, memo pad, and address book. Newer versions of Palm handhelds use Flash memory in place of ROM memory. Whether the memory is classified as ROM or Flash, this is where user applications and databases are stored. These files can provide a significant amount of information once extracted. The databases found in Palm memory are similar to computer files, except that they are stored as a sequence of memory blocks called records instead of in one contiguous area (5, pg. 5).

CHAPTER 7: Device Analysis

7.1 Raw Image Analysis

By using a hex viewer or text editor, examiners can view the entire memory image. The example ROM and RAM image file from a Palm m100 are each over two megabytes in size. Modern Palms generally have 64 megabytes of RAM storage, which can be a time consuming process to manually view. To increase the difficulty, add the analysis of a Compact Flash, Secure Digital, or Multi-Media storage card. Each of these cards can hold up to 1 gigabyte of data each. Investigators will quickly run into the same problem as when examining computers: too much data to efficiently sort through.

If no commercial forensic program is used, examiners will have to view the memory image directly. This can be difficult to do because of the size and binary nature of the memory image. A binary memory image file is computer-readable but not easily human-readable. All executable programs are stored as binary files, as are most numeric data files. In contrast, text files are usually stored in binary coded ASCII. When the binary memory image is viewed using a standard text editor such as WordPad, the program assumes it is in ASCII form. This assumption causes text to be displayed in what appears to be garbage characters as seen in Figure 15.


```

00028c40h: 00 2A 02 00 44 96 00 04 32 10 00 00 0B 00 46 ; .*..D-..2.....F
00028c50h: 72 65 64 65 72 69 63 6B 00 46 72 65 64 00 35 35 ; rederick.Fred.55
00028c60h: 35 2D 36 36 36 36 00 55 01 00 00 2A 02 00 44 A9 ; 5-6666.U...*..D@
00028c70h: 00 04 32 10 00 00 00 0B 00 42 69 6C 64 65 72 73 ; ..2.....Bilders
00028c80h: 6F 6E 00 42 69 6C 6C 00 35 35 35 2D 32 32 32 32 ; on.Bill.555-2222
00028c90h: 00 55 00 00 00 2A 02 00 44 BC 00 04 32 10 00 00 ; .U...*..D%.2...
00028ca0h: 00 0B 00 43 61 72 72 6F 6C 73 6F 6E 00 43 61 72 ; ...Carrolson.Car
00028cb0h: 6F 6C 00 35 35 35 2D 33 33 33 33 00 00 00 00 28 ; ol.555-3333....{
00028cc0h: 02 00 44 CF 00 04 32 10 00 00 00 0B 00 44 65 6E ; ..Dİ..2.....Den
00028cd0h: 73 6F 6E 00 44 65 6E 6E 69 73 00 35 35 35 2D 34 ; son.Dennis.555-4
00028ce0h: 34 34 34 00 00 00 00 28 02 00 44 E1 00 04 32 10 ; 444....{..Dá..2.
00028cf0h: 00 00 00 0B 00 45 64 77 61 72 64 73 00 45 64 64 ; .....Edwards.Edd
00028d00h: 69 65 00 35 35 35 2D 35 35 35 35 00 00 00 00 2A ; ie.555-5555....*
00028d10h: 02 00 44 F3 00 04 32 10 00 00 00 0B 00 41 6E 64 ; ..Dó..2.....And
00028d20h: 65 72 73 6F 6E 00 41 6E 64 72 65 77 00 35 35 35 ; erson.Andrew.555
00028d30h: 2D 31 31 31 31 00 01 00 00 2A 02 00 45 06 00 04 ; -1111....*..E...
00028d40h: 32 10 00 00 00 0B 00 47 6C 65 6E 73 6F 6E 00 47 ; 2.....Glenson.G
00028d50h: 6C 65 6E 64 61 00 35 35 35 2D 37 37 37 37 00 55 ; lenda.555-7777.U
00028d60h: 01 00 00 2A 02 00 45 19 00 04 32 10 00 00 00 0B ; ...*..E...2.....
00028d70h: 00 48 61 72 72 69 73 6F 6E 00 48 61 72 72 79 00 ; .Harrison.Harry.
00028d80h: 35 35 35 2D 38 38 38 38 00 55 00 00 00 E0 01 00 ; 555-8888.U...à..

```

Figure 17. Mixed Binary and Text Image Viewed With UltraEdit

7.2 ImageView

To assist the investigator, a small program is provided herein that simply filters non-printable characters and sends only text strings to a separate file. The source code for this program is presented in Appendix A. This program is written in C++ and can be run against any file image. The design and operation of this program is given below.

7.2.1 ImageView Design

The ImageView program will ask the user to input the filename of the memory image. ImageView will then prompt the user for the name of the file to which results will be output, and the minimum string length to look for. A minimum string length will allow users to filter out

text that might not meet the criteria of their investigation. Once the user has entered the runtime options, ImageView will proceed to open the binary image file and the ASCII output file in succession. If there are problems opening either of these files, the program will terminate. ImageView then proceeds to create two dynamically sized buffers based on the size of the image file. The first of these buffers, the input buffer, will be populated with the binary data from the image file.

This input buffer will then be systematically searched for characters that meet the following criteria:

- ❖ The character must be a printable character.
- ❖ It must meet one of the two following conditions:
 - Is it an alphanumeric character?
 - a b c d e f g h i j k l m n o p q r s t u v w x y z
 - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 - 0 1 2 3 4 5 6 7 8 9
 - Is the character a punctuation mark?
 - ! " # % & ' () ; < = > ? [\] * + , - . / : ^ _ { | } ~

Furthermore, if the character would begin a new string, it must not be equal to the symbol for unused memory. The default character in ImageView is 'U.' The string is then stored in the output buffer and subsequently written to the ASCII output file. This process continues until the

entire input buffer has been traversed. After the entire file has been analyzed, the files are closed and the buffers are freed.

7.2.2 ImageView Execution

ImageView was run with the RAM and ROM images produced earlier with the PDD utility. The resulting output files were named RAM.dat and ROM.dat respectively and the minimum string length was set at three characters. An example of this run can be seen in Figure 19.

```
C:\WINNT\system32\cmd.exe

F:\Thesis\imageview\Debug>imageview
Image File: m100_RAM
Output File: RAM.dat
Minimum String Length: 3

F:\Thesis\imageview\Debug>imageview
Image File: m100_ROM
Output File: ROM.dat
Minimum String Length: 3

F:\Thesis\imageview\Debug>_
```

Figure 18. ImageView Execution

The m100_RAM file and the m100_ROM file were both 2,048 KB in size. However, the resulting RAM.dat file was 15 KB and the ROM.dat was 403 KB. This was a significant reduction in the amount of data that forensic examiners will have to visually examine.

Furthermore, the appearance of the data is much better than viewing the raw image file, as seen in Figure 20 and Figure 21.

Frederick	Whoops,
Fred	don't
555-6666	want
Bilderson	anyone
Bill	see
555-2222	this.
Carrolson	Good
Carol	thing
555-3333	DELETED
Denson	it.
Dennis	This
555-4444	note
Edwards	tells
Eddie	All
555-5555	About
Anderson	illegal
Andrew	activity.
555-1111	Good
Glenison	thing
Glenda	made
555-7777	
Harrison	
Harry	
• 555-8888	

Figure 20. ImageView MemoPad

Figure 19. ImageView Address Book

ImageView will not modify the image file. This has been verified by using md5sum to create a hash value before and after ImageView execution. As seen in Figure 22 below, the hash has not changed. However, it is recommended that forensic examiners use a software or hardware write blocker to insure that no modifications are made to image files.

```
C:\WINNT\system32\cmd.exe

F:\Thesis\imageview\Debug>md5sum m100_RAM
31efe0275f9ecc80e41ec6d0ce446294 *m100_RAM

F:\Thesis\imageview\Debug>imageview
Image File: m100_RAM
Output File: RAM.dat
Minimum String Length: 3

F:\Thesis\imageview\Debug>md5sum m100_RAM
31efe0275f9ecc80e41ec6d0ce446294 *m100_RAM

F:\Thesis\imageview\Debug>_
```

Figure 21. MD5SUM Before and After ImageView Execution

7.2.3 Considerations

ImageView was originally planned to be able to recognize the difference between address, memo, and date files. However, after research, this was found to be infeasible. The internal memory file format of Palm devices is not documented by the Palm Corporation. Research was done in order to determine the memory format by visual inspection of the image files, but no results were forthcoming. In addition, “The in-memory format of Palm databases is subject to change and is not documented by Palm, Inc.” (13, pg. 8). If the in-memory file format could be discovered, a forensic analysis program that relied on a set format would no longer properly function. It is for this reason that ImageView was designed to recover only plaintext from the memory image.

7.3 POSE

Once a complete ROM image has been made of a Palm handheld, it can be loaded into Palm's OS Emulator as previously described in Section 3.4. Additionally, ROM images can be downloaded from the Palm website for the majority of Palm handhelds. By obtaining the ROM from one of these two sources, examiners can have a test system identical to the seized device.

When the ROM image from the seized device was loaded into the POSE, the program acted as if it were a Palm m100 with all of the default factory functionality, Figure 23.

Figure 22. POSE Running m100 ROM

Further, when the appropriate m100 skin was added, the device appeared identical as well, as seen in Figure 24.

Figure 23. POSE Running m100 ROM with m100Skin

This is useful if an investigator wants to get a feel for how the seized device functions without using it. Unfortunately, the POSE software cannot import the accompanying date from the ROM image to populate the program with the user's databases. This does not give the POSE program much forensic significance.

However, if a computer is seized along with the Palm, there is a possibility that the user databases are saved on the computer. If the computer has the Palm Desktop software installed and the user has performed a HotSync operation with the PC, there is a high likelihood that the

user databases are backed up. If this is the case, POSE can be configured to HotSync with the seized PC. Once the appropriate ROM has been loaded into POSE, POSE and the Palm Desktop must be configured. POSE and the Palm Desktop software must be configured to look to the desktop computer instead of a default COM port. These configuration changes are detailed in *Using Palm OS Emulator* that is packaged with the POSE software.

NOTE

No operations should be performed directly on seized evidence. All analysis and activity should be conducted on images of seized devices.

This process was conducted on the Palm m100 that was imaged earlier in this document and the accompanying desktop computer that it was HotSynced with. The Palm Desktop software proceeded to populate the virtual Palm with the backed up databases. If this process is conducted on a seized handheld, the forensic examiner will have a similar device on which to view evidence. It will also allow a forensic examiner to present evidence to an audience without compromising the source of the evidence and to easily take screenshots to add to their report. The following screenshots illustrated in Figures 24 through 27 were taken of POSE loaded with m100 ROM and HotSynced with the Palm Desktop.

Figure 24. POSE View of Date Book

Figure 25. POSE View of Address Book

Figure 26. POSE View of To Do List

Figure 27. POSE View of MemoPad

In addition, POSE can create a bound emulator. This emulator is a stand-alone executable that does not need external ROM, session, skin files, or the Palm OS Emulator software. When the program is reset, it will restore the original configuration of the bound executable. This is a useful way to allow people other than the forensic examiner to handle the evidence.

The POSE software should not be used as a substitute for examining memory images of seized Palm devices, since the only information that is loaded into the POSE program is that saved to

the desktop. Users could have added, deleted, or altered data on their handhelds that will not be reflected in the most current backups that Palm Desktop produces.

7.4 Password Protection

Password protection will not keep forensic examiners from viewing the contents of image files.

However, if a device is password-protected, examiners may have trouble imaging the device.

The Palm OS Console Debugger can be entered even if the Palm lock function is active. If the lock function is active, users must enter a password before the device becomes operational.

However, the command can still be given to put the device in Console Debugger Mode. Devices running a Palm OS newer than 3.5.2 have removed this back door. If the Palm OS 4.0 or newer is in place, examiners will have to input the correct password to image the device if the lock is active. However, the lock function might not be active when the device is found. That is one reason why it is important to image a device that is powered on before actually turning it off.

Turning a device off can often times result in the system lock becoming active.

7.5 Retrieval of Palm Passwords

It is possible to determine the password used on a given Palm device through a variety of means (14). The inherent application of this is to determine the password that may be used on other devices such as desktop computers, email accounts, and other systems that support better password encryption. The encoded password is stored on the Palm device in the Preferences

database. Depending on the length of the unencrypted password, there are two different encoding schemes.

“For passwords of four characters or less, an index is calculated based on the length of the password and the string is XOR’ed against a 32-byte constant block. For passwords greater than four characters, the string is padded to 32 bytes and run through four rounds of a function which XOR’s against a 64-byte constant block” (15, pg. 2-3). Since the encoding scheme is known, and is relatively weak, it is possible to reverse the encryption to obtain the password. This is illustrated in two proof-of-concept tools from @stake. The first, “PalmCrypt” runs on the PC. It will encode or decode ASCII password blocks. The second, “NotSync” runs on a second Palm and retrieves the password by imitating the HotSync process.

7.6 Retrieval of Encrypted Memory

Applications that include encrypted data can also be of significance. When encrypted data such as a database or record is selected to be opened, it is decrypted and the plaintext is stored in RAM memory for a short length of time. Often, the plaintext data is not cleared until the device is turned off. If the device is imaged before the plaintext is cleared, the plaintext data will still be in memory and can be recovered. That is the second reason why it is important to image a device that is powered on before turning it off. Turning a device off can often times result in the plaintext being re-encrypted.

CHAPTER 8: Conclusions and Future Work

8.1 Conclusions

PDAs are becoming more widely used among the population. Forensic examinations of PDA handhelds make up a small part of computer forensics. However, the yield of possible evidence is too great to be ignored. The field of PDA Forensics is new and the tools discussed in this document have just recently been developed. Moreover, many devices are hybrid PDAs. They double as cellular telephones and pagers. The development of forensic software must take into account these new devices. The depth of forensic knowledge about these PDA devices must increase. There currently is no standard methodology for conducting credible examinations.

This document provides:

1. An introduction to commercial and freeware software that is already available
2. Offers suggestions on the forensic process as it relates to Personal Digital Assistants
3. Introduces a tool to aid forensic examiners in recovering evidence from images of seized devices

8.2 Future Work

It is hoped the future work can be done to discover the in-memory file format. With this knowledge, the ImageView program can be revised to separate records and denote their type, such as address, date, or memo.

In addition to further research, an addition to Digital Forensics curriculum should be made. The suggested Forensic Course Development as published by the ACM (16) does not include topics in PDA forensics. An addition to this curriculum to cover Personal Digital Assistants is highly recommend to give forensic examiners the proper training to conduct examinations on these devices.

Bibliography

- [1] Palm Media Backgrounder, http://www.palmsource.com/press/media_back.html.
- [2] Palm Historical Background, <http://www.palmone.com/us/company/corporate/timeline.html>.
- [3] Palm, Inc., "Palm OS Programming Development Tools Guide," DN 3011-006, Nov. 2003.
- [4] Grand, Joseph, "pdd: Memory Imaging and Forensic Analysis of Palm OS Devices," @stake, Inc., Cambridge, MA, Mar. 2002, http://www.atstake.com/research/reports/acrobat/pdd_palm_forensics.pdf.
- [5] Palm OS Emulator (POSE), <http://www.palmos.com/dev/tools/emulator/>.
- [6] Paraben PDA Seizure, http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=107.
- [7] Paraben PDA Seizure Toolbox, http://www.paraben-forensics.com/catalog/product_info.php?products_id=111.
- [8] Parry, Jessica, Email Correspondence, AccessData, Nov. 2004.
- [9] Jansen, Wayne, "Guidelines on PDA Forensics," National Institute of Standards and Technology, Draft Special Publication 800-72, Aug. 2004.
- [10] Mandia, Kevin, *Incident Response & Computer Forensics, Second Edition*, New York:McGraw-Hill, 2003.
- [11] *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, Jul. 2001.
- [12] Lin, Chi-Yi and Kuo, Sy-Yen and Huang, Yennun, "A Checkpointing Tool for Palm Operating System," *IEEE Proceedings of the International Conference on Dependable Systems and Networks*, pg 71-76, Jul. 2001.
- [13] Palm, Inc., "Palm File Format Specification," DN 3008-004, May 2001.
- [14] Kingpin and Midge, "Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats," *Proceedings of the 10th USENIX Security Symposium*, Aug. 2001.

[15] Kingpin, "PalmOS Password Retrieval and Decoding (A092600-1)," @stake, Inc., Cambridge, MA, Sep. 2000,
<http://www.atstake.com/research/advisories/2000/a092600-1.txt>.

[16] Troell, Luther and Pan, Yin, and Stackpole, Bill, "Forensic Course Development," *Conference on Information Technology Education: Proceeding of the 4th Conference on Information Technology Curriculum*, pg. 265-269, 2003.

APPENDIX A: ImageView Source Code

```
#include <stdio.h>
#include <stdlib.h>
#include <iostream.h>
#include <ctype.h>

#define FALSE 0
#define TRUE 1
#define MAX_FILENAME 15
#define MEM_CHAR 'U'

int main () {

    // Declarations
    FILE * infile;
    FILE * outfile;
    long lSize;
    long sofar = 0L;
    long sstart;
    int i;
    int lptr;
    int min_len;
    int in_string;
    char * inbuff;
    char * outbuff;
    char image_file[MAX_FILENAME];
    char output_file[MAX_FILENAME];

    //Get input from user
    cout << "Image File: ";
    cin >> image_file;
    cout << "Output File: ";
    cin >> output_file;
    cout << "Minimum String Length: ";
    cin >> min_len;

    //Open Input & Output Files
    infile = fopen (image_file, "rb" );
```

```

if (infile==NULL) {
    cout << "infile:" << image_file << " cannot be opened.\nProgram terminating";
    exit (1);
}
outfile = fopen (output_file, "w" );
if (infile==NULL) {
    cout << "outfile:" << output_file << " cannot be created.\nProgram terminating";
    exit (1);
}

// Obtain File Size of Input File
fseek (infile , 0 , SEEK_END);
lSize = ftell (infile);
rewind (infile);

// Allocate Memory for the Input File
inbuff = (char*) malloc (lSize);
if (inbuff == NULL) exit (2);
outbuff = (char*) malloc (lSize);
if (outbuff == NULL) exit (3);

// Copy Input File Into Buffer
fread (inbuff, 1, lSize, infile);

// Search INBUFF
for (i = 0; i < lSize; i++) {
    if (in_string && isprint(inbuff[i]) && (isalnum(inbuff[i]) || ispunct(inbuff[i]))) // We
are in a string

        outbuff[lptr++] = inbuff[i];
    else
        if (isprint(inbuff[i]) && isalnum(inbuff[i]) && ((inbuff[i] != 'U') && (inbuff[i+1]
!= MEM_CHAR))) { // Would this start a string?
            outbuff[lptr++] = inbuff[i]; // Start a New String
            in_string = TRUE; // Currently in a String
            sstart = i+sofar; // Mark String Start
        }
        else
            if (in_string) { // End of string?
                if (lptr >= min_len) { // Of specified size?
                    outbuff[lptr] = '\0'; // Terminate the string

```

```

        fprintf(outfile, "%s\n", outbuff); // Print String to file
    }
    in_string = FALSE;
    lptr = 0;
}

// Close Files and Clear Buffers
fclose (infile);
fclose(outfile);
free (inbuff);
free (outbuff);

//terminate
return 0;

```


APPENDIX B: Summary Sheet

Device Seizure Flow Chart:

l... 2

To Activate Console Debugger

l... 3

To Deactivate Automatic Power Off

Notes for Password Protected Devices:

Image the device before powering down to prevent data loss.

WARNING

Powering down the device can cause password protection to be activated.

Notes for Encrypted Memory:

Image the device before powering down to prevent data loss.

WARNING

Powering down the device can cause the memory to be encrypted

WHEN IN DOUBT CONTACT YOUR LOCAL FORENSIC EXAMINER FOR MORE INFORMATION