NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

Paraben Device Seizure

Version 4.3

EVALUATION REPORT

July 2012

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.
Michael Terminelli, ACE
Randy Becker, CFCE
Jacob Fonseca
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates.

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009 NCJ 225375.

Overview

With the world becoming more mobile every day, law enforcement encounters more cellphones and mobile devices in their investigations. Many tools exist on the market to process these mobile devices, but every tool does not support every device.

Paraben states that their product Device Seizure can acquire and analyze data from over 4,000 mobile phones, PDAs and GPS devices. Device Seizure is a software platform that installs onto a computer workstation and includes a driver pack designed to maintain forensic integrity of device acquisitions. Device Seizure also includes a toolbox of cables and hardware for connecting devices to the workstation.

Product Information

The following information is from Paraben's website:

> "Device Seizure is an advanced forensic acquisition and analysis tool for examining cellphones, PDAs and GPS devices. Device Seizure now includes software and hardware so you have everything you need to get started in mobile forensics. Don't settle for half the data. Most commercial cellphone forensic software only gets logical data files. That's like doing an investigation on half a crime scene. If a tool doesn't have advanced analysis features, it's probably because they don't get enough data to analyze. Deleted data and user data such as text messages and images can often be found in a physical data dump of a phone. Device Seizure was designed from the ground up as a forensic grade tool that has been upheld in countless court cases."

Product Description

The following information is from the Device Seizure user guide:

> "Paraben's Device Seizure is designed to allow investigators to acquire the data contained on cellphones, smartphones, GPS, Hybrids, MP3 and PDA devices without affecting data integrity. With cellphones, it is designed to retrieve data such as phone numbers, dates, times, pictures, call history and full data dumps (similar to flasher dumps). It also provides ways to search and add bookmarks to important data. For Hybrids and PDA devices, the software is designed to acquire, search, and report on all data associated with most versions of the Palm OS, Windows CE/Pocket PC, Symbian, iPhone and RIM BlackBerry devices."

Special Features

The following information is from the Paraben's website:

> "Most commercial or free software is designed to not only view data but to upload data. This is not a safe way to perform a forensic examination. In fact, even some software marketed as forensic software warns of possible data loss. Device Seizure does not allow data to be changed on the device. Paraben can also add support for unsupported cellphone models from supported manufacturers with simple log files and a little time. Add all this together and there's no comparison for forensic acquisition, analysis and reporting of handheld device data.

Paraben focuses on the physical level of acquisition, offering more physical downloads of devices than any other company. Logical data acquisitions can't acquire more data than the device Operating System was designed to allow. The physical acquisition plug-in is unique to Paraben, offering memory imaging on most of the devices supported in Device Seizure, which is where most deleted data** can be recovered.

**Please Note: Paraben's SIM Card Seizure and Paraben's Device Seizure are able to recover deleted SMS data associated with transmission of text data on a GSM network. However, some cell/mobile phones store SMS on the actual device rather than the SIM card. If that is the case, the recovery of this data may or may not be possible using Device Seizure, depending on the specific device model. As with any deleted data, recovery depends on whether or not the information has been overwritten with new information. Because of these factors, Paraben cannot guarantee the recovery of deleted data."

Target Customers

The target customers for Paraben's Device Seizure are state and local law enforcement organizations that maintain a separate unit for forensic examinations of digital media. Device Seizure is a forensic grade acquisition tool that is capable of creating reports that can be customized with an organization's and investigator's information and notes. These reports are created and presented in an easy-to-read format.

Law Enforcement Applications

Device Seizure is designed to assist state and local law enforcement with the acquisition of and reporting on both logical and physical examinations of mobile devices such as cellphones, PDAs and GPS devices.

Test Bed Configuration

Prior to downloading the software program, the online user manual was reviewed. The manual is informative and contains screenshots of the installation, configuration and use of the program. It is important to be sure to install the actual program and the driver pack, which will allow the workstation to connect to the device being acquired. A detailed explanation of each type of report that can be generated is provided in the online user manual.

The test machine is a Dell Optiplex 760 with a clean Windows 7 x64 installation, 4GB of RAM and a 2.66 GHz Intel Core 2 Duo processor. Installed on the test machine were both the Device Seizure application and the Device Seizure driver pack.

The phones that were selected for testing represent the different types of widely used phone technologies (CDMA and GSM).

To install Device Seizure on the test machine, the following steps were performed:

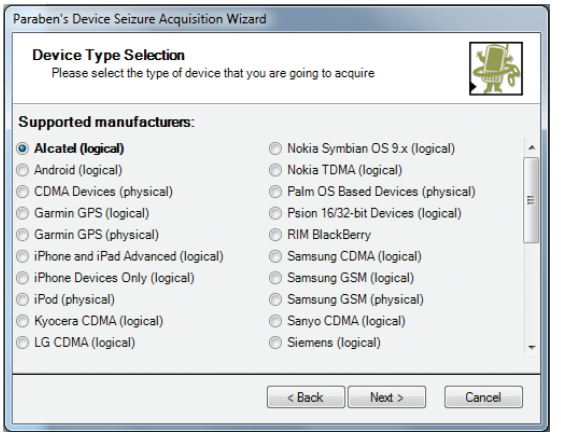
1. Downloaded the Device Seizure software and the Device Driver Pack from Paraben's website.
2. Executed the installer for the Device Seizure software, which includes the hardware licensing dongle driver.
3. Executed the installer for the Device Driver Pack to install components that will allow the computer to connect to a wide variety of devices.

Evaluation and Testing of Paraben Device Seizure

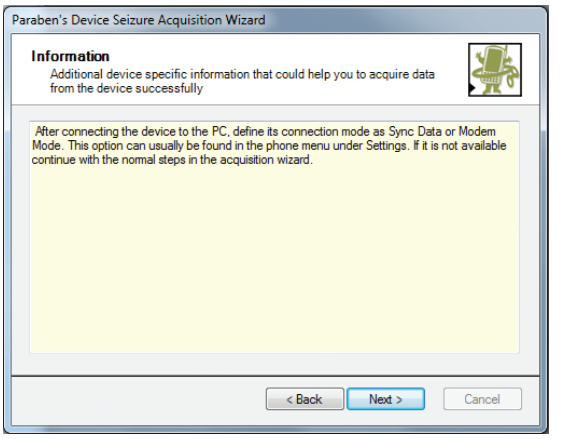
The Device Seizure interface allows the user to perform extractions and analysis of mobile devices. To start using the software, these general steps must be followed to acquire data from a device:

1. Launching the application displays a dialog allowing the user to begin an acquisition, open an existing case or create a new case.

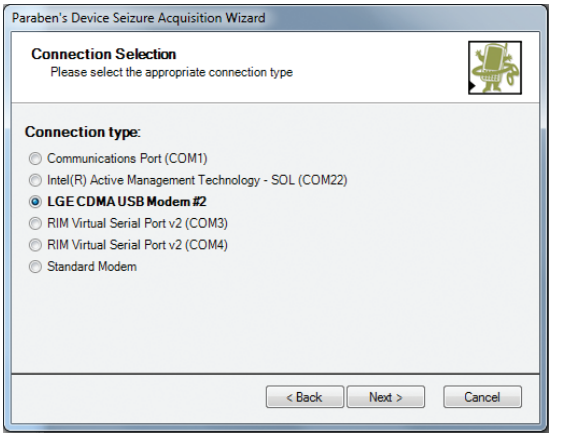
2. After selecting Data Acquisition, a dialog wizard is launched that walks the user through the process of acquiring a device. The first dialog allows the user to select the model and type of device.



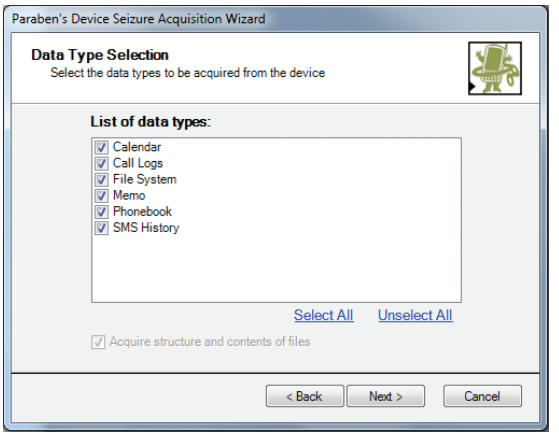
3. The next dialog provides instructions specific to the device to the user. For example, how to set the device into a special data mode to allow for acquisition and any special connection instructions.



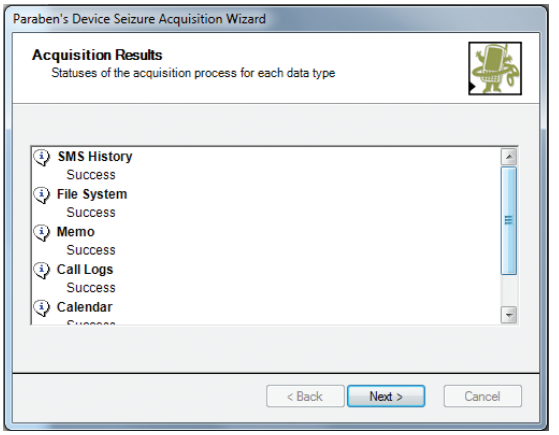
4. Device Seizure will scan the computer for available ports and display a list for the user to select the correct device.



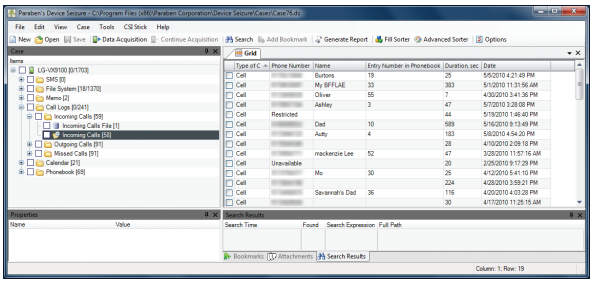
5. Device Seizure displays a list of the available device features that it supports for acquisition. The user may select one or all of the available options.

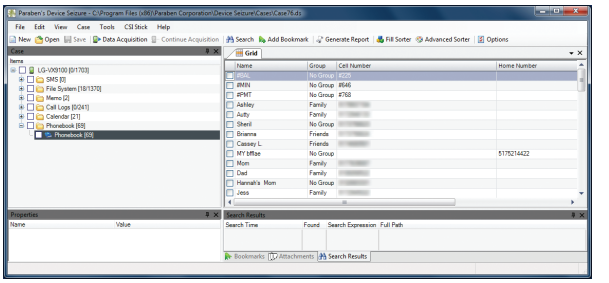


6. Device Seizure will begin the acquisition process and will display a dialog with the results being either successful or failing upon completion.

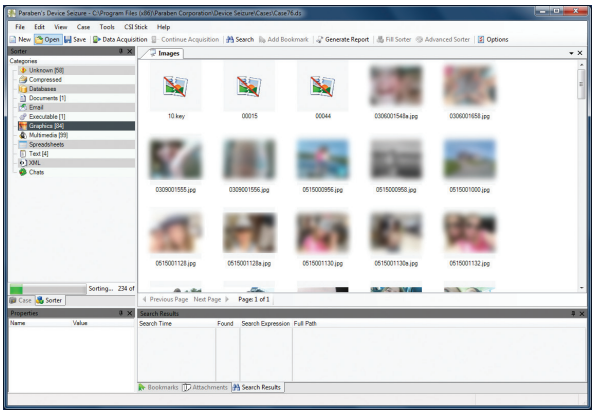


Once these steps are completed, the user can browse through the collected data. There are two views within the user interface. The first is the case view. In this view all of the collected data is displayed in a tree in the left pane of the main display. The next two screen-shots show this view while selecting incoming calls and phonebook in the left pane.

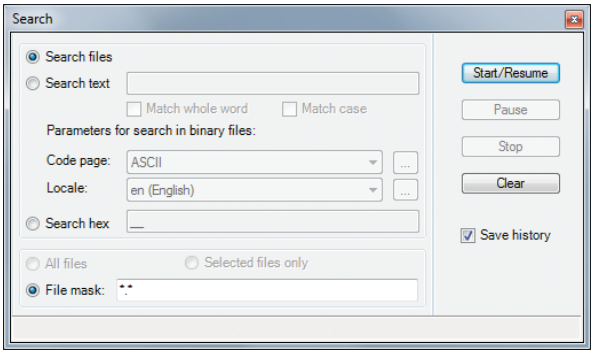




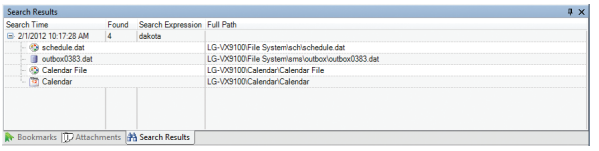
Device Seizure also includes an advanced sorter, which places the extracted files into categories based on file type (e.g., graphics, multimedia, text, etc). The next screenshot shows the advanced sorter tab selected in the lower left pane. The graphics category has been selected in the left pane and the results are displayed in the right pane.



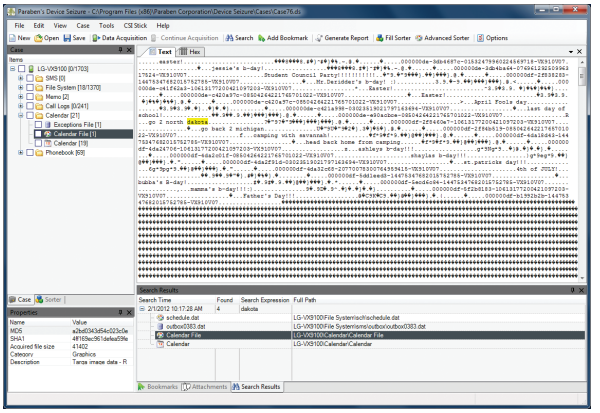
The search feature includes support to search through the acquired files. The search can be for file names and extensions or for text or hex values.

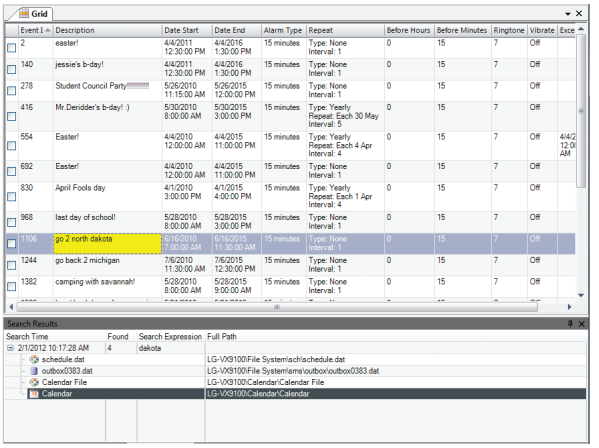


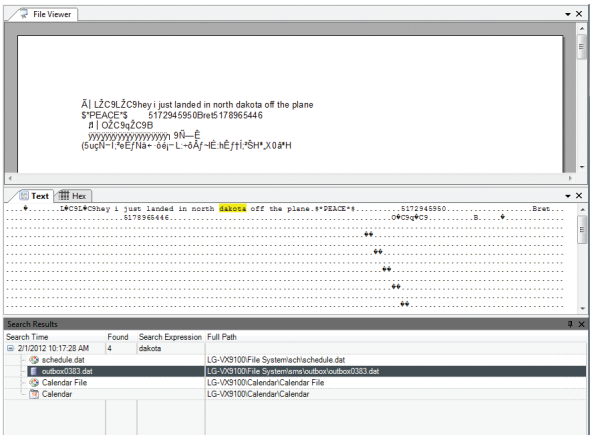
The search results are displayed in the bottom pane of the main interface. The results are displayed in a tree format that shows the number of hits for each search. A search result can be expanded to list all of the files where the search hit was located.



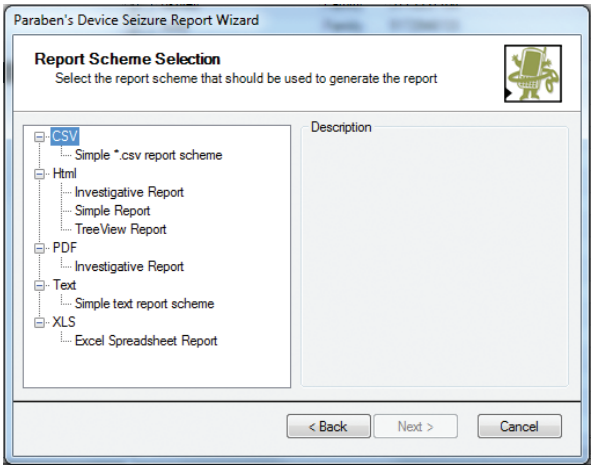
When a search result hit is selected, the file is displayed in the right pane of the interface. Depending on what type of hit is selected, the display will show the hexadecimal location of the data, the data as it has been interpreted from the hex, or it will display the hex and text representation simultaneously. All of these examples can be seen in the next screenshots.



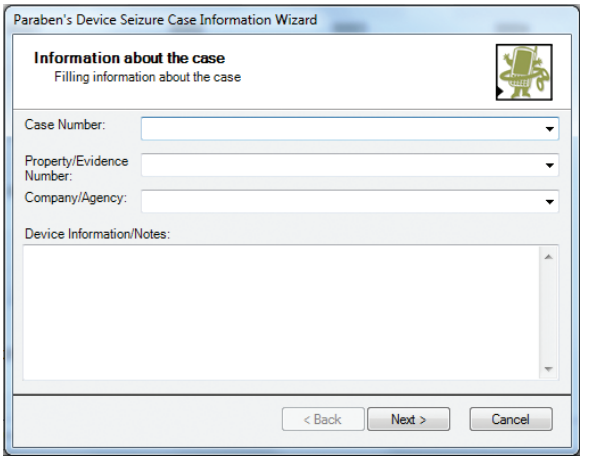




Reports can be generated in CSV, HTML, PDF, text or XLS formats.



The report can include the entire case or only items selected by the user, and the user can enter his or her case data to be included with the generated report.



Test 1 – Samsung SPH-M300

This test was performed to determine how well Device Seizure acquires data from a Samsung SPH-M300.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected Samsung CDMA (logical) and clicked Next.
6. Selected Samsung Mobile Modem #2 as the connection type and clicked Next.
7. Checked off all options including Calendar, Call History, File System, Notes, Phonebook, SMS History and ToDo History from the Data Type menu and clicked Next.
8. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully, except for Notes and Call History, which are unsupported according to Device Seizure.

Device Seizure found one sent SMS, 35 phonebook contacts, zero ToDo tasks, zero calendar events and zero calls in the call history. The results matched the data found when manually examining the phone, except for the phonebook and call history. On the phone, there are actually 95 contacts, and there were several outgoing, incoming and missed calls in the call history. The file system was successfully extracted.

Test 2 – LG Rumor

This test was performed to determine how well Device Seizure acquires data from an LG Rumor.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected LG CDMA (logical) and clicked Next.
6. All of the connection types available were attempted, but none could make a connection to the phone.
7. The phone was put into modem mode as instructed by Device Seizure.
8. Selected LGE CDMA USB Modem #4 as the connection type and clicked Next.
9. Checked off all options including Calendar, Call Logs, File System, Memo, Phonebook and SMS History from the Data Types menu and clicked Next.
10. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully, except for Memo and Call Logs because of a read error. Device Seizure suggests reacquiring the device.

The acquisition was reattempted several times without success, with only Call Logs or Memo checked off in the Data Types menu.

Device Seizure found 10 received SMS, three sent SMS, two calendar files with no data and 19 phonebook contacts. The results matched the data found when manually examining the phone except for the calendar, which has two scheduled events. The file system was successfully extracted. Call logs and memos failed to extract.

Test 3 – Nokia 6085h

This test was performed to determine how well Device Seizure acquires data from a Nokia 6085h.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected Nokia GSM (logical) and clicked Next.
6. The phone was put into PC Sync mode as instructed by Device Seizure.
7. Selected USB (DKU-2, CA-53, DKE-2) as the connection type and clicked Next.
8. Checked off all options including Calendar, Call Logs, Chat Settings, File System, FM Station, GPRS Access Points, Logos, MMS Settings, Notes, Phonebook, Profiles, SMS History, SyncML Settings, ToDo List and WAP from the Data Types menu and clicked Next.
9. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully.

Device Seizure found 86 phonebook contacts, zero calls in the call history, zero calendar events, one item in the ToDo list, zero SMS history, zero profiles, zero WAP, five GPRS access points, eight logos, zero chat settings, zero FM stations, zero MMS settings, zero notes and zero SyncML settings. The results match the data found when manually examining the phone, except for the SMS history. On the phone, there are actually several sent and received SMS messages. The phonebook could not be verified because it could not be accessed without a SIM card in the phone. This could likely be remedied by cloning a SIM card. The file system was successfully extracted.

Physical Extraction

The following steps were performed to extract physical data:

1. Connected the phone to the PC using the USB cable (driver was already installed).
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected Nokia GSM (physical) and clicked Next.
6. Selected USB (DKU-2, CA-53, DKE-2) as the connection type and clicked Next.
7. Checked off all options including Calendar, Call Logs, Permanent Memory, Phonebook and SMS History from the Data Types menu and clicked Next.
8. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully.

Device Seizure found zero calendar events, 20 incoming calls, 20 missed calls, 20 outgoing calls and zero SMS history. The results match the data found when

manually examining the phone, except for the SMS history and call history. On the phone, there are actually several sent and received SMS messages and zero calls in the call history. This suggests that Device Seizure has recovered the deleted call history. The PM memory was successfully extracted.

Test 4 – Motorola V3

This test was performed to determine how well Device Seizure acquires data from a Motorola V3.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. The driver did not install properly, so the Motorola USB driver for Windows version 5.2.0 was downloaded from Motorola's website and installed.
3. The phone was reconnected to the computer and the driver installed correctly.
4. Launched the Paraben Device Seizure Application.
5. Selected Data Acquisition.
6. Clicked Next to start the Acquisition Wizard.
7. Selected Motorola (logical) and clicked Next.
8. Selected Motorola USB Modem as the connection type and clicked Next.
9. Checked off all options including Call Logs, Events, File System, Phonebook and SMS History from the Data Type menu and clicked Next.
10. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully.

Device Seizure found zero SMS history, zero phonebook contacts, zero calls in the call log, and zero events in the datebook. The results could not be verified because the phone menus could not be accessed without a SIM card. This could likely be solved by cloning a SIM card. The file system was successfully extracted.

Physical Extraction

The following steps were performed to extract physical data:

1. Connected the phone to the PC using the USB cable (driver was already installed).
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected Motorola (physical) and clicked Next.
6. Selected Motorola USB Modem as the connection type and clicked Next.
7. Checked off all options including Call History, Security Information, and SMS and Quick Notes Dump from the Data Type menu and clicked Next.
8. When the acquisition finished, the Sorter was filled.

Results

In the acquisition Results window, all of the data types were extracted successfully.

Device Seizure found 43 received SMS messages, 61 sent SMS messages, 16 quick notes, 10 incoming calls and 10 outgoing calls. It also found security information such as IMEI, firmware version, security lock code, etc. The results could not be verified because the phone menus could not be accessed without a SIM card. Possible explanations for why the logical extraction did not find any SMS history or call history is either because Device Seizure could not extract the data without a SIM card in the phone or the history

was deleted from the phone. This issue could likely be solved by cloning a SIM card.

Test 5 – Apple iPhone 4S

This test was performed to determine how well Device Seizure acquires data from an Apple iPhone 4S.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected iPhone/iPad/iTouch Advanced (Logical) for device type and clicked Next.
6. Selected Apple iPhone Device as the model and clicked Next.
7. Selected Apple iPhone Device in the connection selection and clicked Next.
8. Checked off Backup Data from the Data Type menu and clicked Next.
9. When the acquisition finished, the Sorter was filled.

Results

Device Seizure found and parsed phone information, 5,704 messages, 75 calendar events, 107 address book entries, one note, 100 call history entries, 1,418 graphics, 39 multimedia files and several other small file system artifacts. Some of these artifacts include web cookies, deleted messages and a dynamic library of typed words.

Test 6 – LG C729 Double Play

This test was performed to determine how well Device Seizure acquires data from an LG C729. The device is running the Android Operating System, version 2.3.4.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed to extract logical data:

1. Connected the phone to the PC using the USB cable and waited for the driver to install.
2. Launched the Paraben Device Seizure Application.
3. Selected Data Acquisition.
4. Clicked Next to start the Acquisition Wizard.
5. Selected Android (Logical) for device type and clicked Next.
6. Selected LG-C729-80A012827000849887 in the connection selection and clicked Next.
7. Checked off Browser History, Calendar, Call Logs, Contacts, File System, Media Store, MMS History, Settings and SMS History from the Data Type menu and clicked Next.
8. When the acquisition finished, the Sorter was filled.

Results

Device Seizure found and parsed 26 e-mail contacts, but not list and phonebook entries. Also parsed were 79 call history entries, 17 system settings, 65 audio files, seven images, zero videos and 134 URLs in browser history. SMS message history failed to be extracted from the device on two different attempts. No calendar events were found, although the device did have some events stored.

Conclusion

Paraben's Device Seizure does a good job of reporting extracted information to the user in a readable fashion. It should be noted that deleted information will likely not be recovered with a logical extraction. Physical extractions, if supported for a particular phone, may recover deleted data.

The list of manufacturer and phone types given in the Data Acquisition wizard does not clearly identify which phone models are actually supported. For example, Device Seizure claims to support Motorola GSM phones for logical and physical extraction, but it is not clear which Motorola models are supported for either or both extraction types. It is also not clear which features of the phone can be extracted until the extraction is actually attempted and completed. Also, during testing, some phones could not recover data due to the lack of a SIM card. It is likely that this shortcoming could be overcome by creating a cloned SIM card for examination.