

Quick **Start** Guide



Paraben's[®]

Device Seizure[®]

Paraben's Device Seizure

Getting Started Guide



Contact Information

Mailing Address

P.O. Box 970483
Orem, UT 84097-0483
USA

After Hours Support

1.801.369.8210

Email Support

forensicsupport@paraben.com

Forensic Support

Business Hours:
9:00 AM to 5:30 PM MST

Main Fax

1.801.796.0610

Main E-mail

forensics@paraben.com

Product Information

Main Phone
1.801.796.0944

What you will find in this guide...

This guide was designed to make the process of using Paraben's Device Seizure easy. We have included the basic information for:

- Registration of the product
- Use of the dongle and associated dongle manager
- Basics of Starting a case
- Sorting through evidence
- Exporting data
- Basics of Reporting
- Helpful Hints

There are many other aspects and features available in Device Seizure that are covered in the main electronic Help File.

Introducing Device Seizure

Welcome to Paraben's Device Seizure this program is designed to allow investigators to acquire the data contained on cell phones, smart phones, GPS, Hybrids, MP3 and PDA devices without affecting data integrity. With cell phones, 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.

There are many updates that are released for Device Seizure because of the types of devices that are acquired with the software. Please be sure to register your tool to ensure that you are always using the latest version of the software.

Device Seizure Related Items

PCME

Paraben Certified Mobile Examiner is an extensive certification course for mobile forensic examiners. Details about this as well as Paraben's Mobile Forensic Training can be found at:

www.paraben-training.com

StrongHold Technology

Paraben's patented faraday technology is leading the way when it comes to the proper seizure and protection of mobile wireless evidence, More information at www.paraben.com

Link2

Link2 is Paraben's free link analysis software that can be downloaded from your registration site account once you have registered your license of Device Seizure.

Installing and Configuring Device Seizure

The installation process has two parts:

- Installing
- Licensing

Without a license, Device Seizure can be used for 30 days or 23 uses. This section outlines the installation process.

Computer System Requirements

Paraben's Device Seizure was designed to run on a Windows 2000 or newer 32-bit operating system. 64-bit systems are not recommended for Device Seizure use because of problems with the mobile drivers and the 64-bit systems.

Windows .NET Framework 2.0 is required.

Installing Device Seizure

When you place the installation CD in your computer, the auto-run feature launches the installation program that guides you through the installation process. If the auto-run feature needs to be started manually, you can click `autorun.exe` in the root directory of the installation CD.

To install Device Seizure:

1. Start the Device Seizure installation application.
2. Click on the **Next** button on the welcome window.
3. Accept the license agreement, then click **Next**.
4. Do one of the following:
 - Type the location on the folder where you want to install Device Seizure, then click **Next**.
 - Click **Browse** and select the location of the folder where you want to install Device Seizure, then click **Next**.
 - Click **Next** to keep the default location.
5. Select the features to install. Select drivers to install. Click on the **Next** button.
6. Choose whether you want to install drivers or not, then click **Next**.
7. You are now ready to begin the installation. Click on the **Install** button.
8. Drivers installation is performed during the installation.

9. The Device Seizure Installation is now complete. Please visit Paraben's Registration Site to register your product.

Using a Dongle Key

You will receive a dongle from Paraben with the license installed. If you need to update a dongle that you use for another Paraben application, call Paraben technical support.

Working in Device Seizure

When your license key is in place, you can begin using Device Seizure. If you have not yet obtained a license, Device Seizure functions for 30 days or 23 uses.

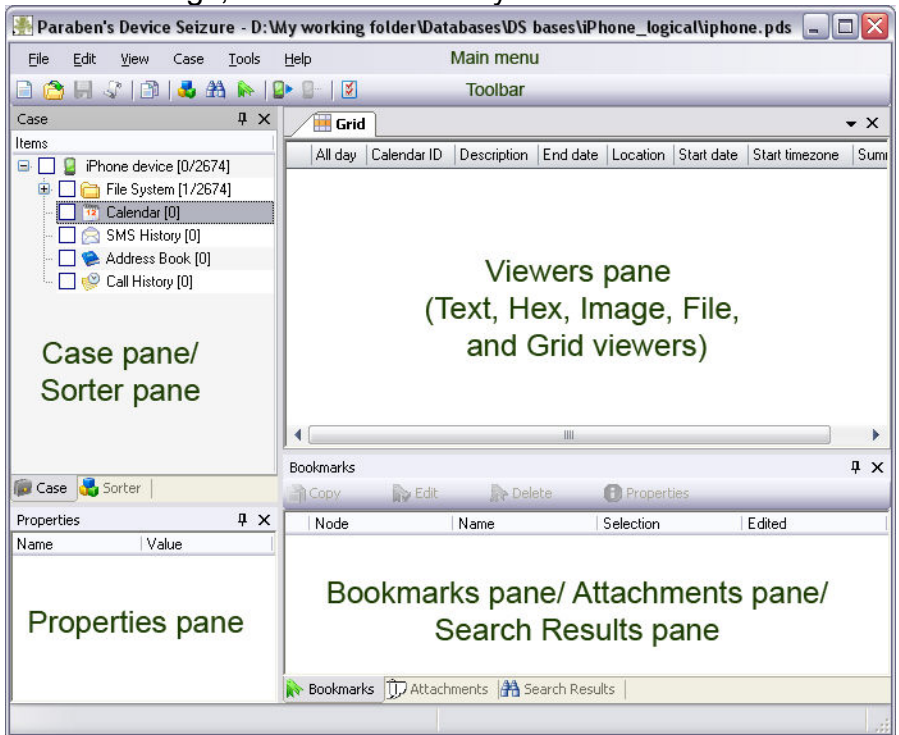
Exploring the Device Seizure the Interface

The Device Seizure has four main information panes as shown in the following image.

The panes are:

- Case pane/Sorter pane – Upper left – The Case pane displays the data stored in the case in a tree-view structure. The Sorter pane displays binary data sorted by file types.
- Viewers pane – Upper right – Displays the data in a parsed or un-parsed format. Depending on the data type, Text viewer, Hex viewer, Image viewer, File viewer, or Grid viewer will be available.
- Properties pane – Lower left – Displays acquired data properties including hash codes, size, manufacturer, etc. Data in this pane can be sorted and copied through the right-click menu.
- Attachments pane – Lower right – Displays files attached to the case.
- Bookmarks pane – Lower right – Displays information about all bookmarks that were made allowing you to move easily through the case.
- Search Results pane– Lower right – Displays the results of performed searches.

NOTE: You can add, remove, or resize panes as you work to see more or less information. The panes can also be dragged and organized in any way. If you want to reset the display to the default settings, in the main menu you can click **View > Restore Layout**.



Device Seizure Data Examination Process

When you work in Device Seizure, there are several functions that you need to be familiar with and perform in order to store and examine the evidence. The functions include:

- Create a case
- Acquire data
- Examine data
- Create reports
- Export data

Each of these is outlined in this guide, but more comprehensive information is available in the help files that are located in Device Seizure under the Help menu.


Creating a Case

When you initially start Device Seizure, you need to create a case. There are two ways of creating a new case:

- **Automatic**
- **Manual**

To create a new case automatically, click on the **Create Case** button on the Welcome page that appears at Device Seizure start-up. The **case<n>.pds** case is created automatically in the folder defined in the Device Seizure options. The Acquisition wizard opens. If you cancel the acquisition, the case is deleted.

To create a new case manually:

1. In the main menu, click **File > New Case** or in the tool bar, click the New Case icon. () or use the hotkeys **CTRL+N**.
2. The standard **Windows New Document** dialog appears so you can navigate to the location of the new case and type its name. You may press the **Enter** key or the **Save** button in the Windows New document dialog window.
3. The **Paraben's Device Seizure Case Information wizard** opens automatically. In this window you can enter information about the case.

NOTE: This information is displayed in reports that you create. Filling it can be done at any time, so you can skip this stage by clicking on the **Cancel** button.

Acquiring Data

After creating your case, you need to acquire data from your device.

Data acquisition is the automatic collection of data from the device. It starts by using a data cable to connect the device to the computer and ends when the folder with a name corresponding to the name of the device containing the data is added to the currently opened case.


NOTE: the process for data acquisition completely depends on the type of device from which data is acquired. For more information, consult the help file.

Generally, acquisition process consists of four steps:

- Preparation step: Preparing your device to being acquired. Consult the help file to get more information about preparing your device to acquisition. Some devices require to be turned off or additional settings on the device should be defined before acquisition.
- Selection Step: Starting the acquisition wizard.
- Acquisition step: Reading data from the device.
- Final Step: Finishing the acquisition.

To acquire data from your device:

1. Prepare your device for acquisition:
 - Check to make sure the device is charged.

- Choose the proper cable or cradle for your device.
 - Check that drivers from USB connection are installed.
 - Define connection properties if necessary.
 - Insert a SIM card if your device uses any.
1. In the main menu, select **Tools > Data Acquisition** or click the **Data Acquisition** icon . You can also click on the **Create Case** button on the Welcome page on program start-up (the case will be created automatically).
 2. The **Paraben's Device Seizure Acquisition wizard** opens. Click on the **Next** button on the Welcome page.
 3. Select the type of device you are going to acquire.
 4. Select the appropriate connection type. Click on the **Next** button.
 5. Select data that will be acquired. Use the **Select All/Unselect All** buttons to make quick selection/discard all selections.
 6. The acquisition starts.

NOTE: some devices require your interaction during the acquisition process. For more information, consult the help file.

Examining Files

After acquiring data, the next step, obviously is to examine it to determine what you have acquired. Device Seizure gives you several options for examining files and data sources.

These include the following tools:

- Grid viewer: It allows you to view data such as Call logs, SMS messages, Phonebooks, Datebooks.
- Text viewer and Hex viewer: It allows you to view not parsed text data in the text and hex format.
- Image viewer: It allows you to see graphics.
- File viewer: It allows you to see the file in its original format (table, Word document, etc.).

To view parsed text data:

1. In the Case pane, expand the folders until you reach the file you want to look at.
2. The file content is displayed in the Viewers pane in the grid form.
3. You can define columns width, columns order, perform grouping and sorting of data in the grid.

To view not parsed data contents:

1. In the main menu, click **View > Viewers**, and ensure that all viewer options are selected.
2. In the Case pane, expand the folders until you reach the file you want to look at.
3. The file content is displayed in the Viewers pane. Select the appropriate tab to see information in the format you want.
4. Click the edge of the pane to resize it if necessary.

To view images:

1. In the main menu, click **View > Viewers**, and ensure that File viewer option is selected.
2. In the Case pane, choose the image file you want to look at.
3. The file content is displayed in the Viewers pane. Select the **Images** tab to see the image.
4. Use buttons in the bottom part of the Image viewer to **resize** an image and **rotate** it.

Sorting

Sometimes it is important to sort data by filetypes. Device Seizure allows you to view data sorted in a special Sorter pane.

There are two types of sorting:


- **General sorting:** The data is sorted by filetypes.
- **Advanced sorting:** The data is sorted by filetypes and all graphic files are selected.

You can sort acquired data manually or automatically after the acquisition finishes.

To fill the Sorter manually:

For general sorting, in the main menu select **Tools > Fill Sorter** or click on the **Fill Sorter** button




For advanced sorting, in the main menu select **Tools > Advanced Sorter** or click on the **Advanced Sorter** button .



To fill the Sorter automatically:

To fill the Sorter automatically immediately after the acquisition, click **Yes** on the confirmation window that appears at the end of the acquisition process.

To view data in the Sorter:

1. Click on the **Sorter** icon  at the bottom of the screen.
2. The Sorter pane can easily be turned on/off by checking the **View - Windows - Sorter** option.

Creating Reports

A Device Seizure report is a report of the currently opened case that is suitable for printing, e-mailing, etc.


A report can be generated in one of the following forms:


- **HTML Tree View Report:** a file in HTML format (*.html) with easy navigation and clearly shown tree structure
- **HTML Simple Report:** a file in HTML format (*.html) in which all data is shown in a series
- **HTML Investigative Report:** a file in HTML format (*.html) specially designed for convenient printing of case data. It can include only the following information: Case Information, Phone model information, Phonebook/Address book, SMS History, Call Logs, Datebook/Calendar, Photos/Images, Unparsed Data, Waypoints (for GPS)
- **Simple Text Report:** a file in text format (*.text) in tab delimited format
- **Simple *.csv Report:** a file in *.csv format, in which data is represented in the form of the tables and can be opened by Microsoft Office Excel
- **Excel Spreadsheet Report:** a file in the *.xls format, in which data is represented in the form of the Microsoft Office Excel spreadsheets.

When you create reports, you can select specific files or rows in grids that you want to add to the report. You can select this information by checking the boxes to the left of the files in the Case pane and boxes to the left of the rows in the grid viewer. You can also add all data from the case to the report without checking anything. A report can be created **for the entire case** or **for selected portions of the case**.

Besides, you can add case information and bookmarks to the report.

To create reports

1. Open the case that you want to generate a report for.
2. Select **File - Generate Report** in the main menu or click the **Generate Report** button  on the toolbar or use the **CTRL+R** hotkeys.
3. The **Paraben's Device Seizure Report Wizard** opens. Click on the **Next** button.
4. Select the format of the report. Click on the **Next** button.

5. Select the report mode (**Entire Case/Selected Items Only**) Define report options:
 - **Include case information:** Select this option if you want to see the information about the case and its hash codes in your report.
 - **Include attachments:** Select this option if you want to see attached files in the report.
 - **Open report after generating:** Select this option to open the generated report automatically.
 - **Bookmark Sorting Type:** In the drop-down list, select the type of Bookmarks sorting in the report.
6. Click on the **Browse** button  to select the report's name and its location. Click on the **Next** button.
7. Check the selections you made. If something is wrong click **Back**, if everything is correct click the **Next** button.
8. Report generation starts.

Exporting Files

Device Seizure lets you export data from the case as separate files and export selected rows of the grid to CSV. You can use the check boxes in the Case pane to select which files and folders you want to export.

You can:


- **Export a Separate Node (binary or grid)**
- **Export the Entire Case or a Part of it (selected nodes)**
- **View the File With an External Viewer**

To export one node contents as a separate file:

1. Select the node to be exported.
2. In the main menu select **File>Export To** or use the hotkeys **CTRL+E** or right-click on the name and select **Export To**.
3. Select the name of the file and the save location.

To export a case or a part of the case:

1. If you export specific data, navigate to the data in the pane and check the corresponding boxes.
2. In the main menu, select **File > Batch Export**.

3. The **Paraben's Device Seizure Export Wizard** opens. Click on the **Next** button on the Welcome page.
4. Select **Export type** for the data you want to export. Select **Common export** to export the case to separate files and folders as they are. Select **Export to archive** to export the case to an archive. In this case, folders and files will be present, but they are stored in one archive file. Click on the **Next** button.
5. Select **Export mode** for the data you want to export: the entire case or the selected items only. Click on the **Next** button.
6. Click on the **Browse button**  to select the destination folder for the **Common export** export type. In this folder, another folder with the name of the case will be created automatically. For the **Export to archive** export type, an archive name and path to it are required. Click on the **Next** button.
7. Check the information you have entered (if it is not correct, you can return by clicking **Back**). If it is correct, start exporting by clicking the **Next** button. All data will be exported in its original format.

Additional Features

This quick start guide has the basic features you need to begin working in Device Seizure. However, Device Seizure has a powerful set of additional features that you can use to make your analysis easier and more complete. These are listed in this section with a brief description. Complete documentation for each is available in the Device Seizure help files.

- Search – Lets you look for text strings and data in the hexadecimal format in the case.
- Bookmarks - Lets you create bookmarks to navigate in the case quickly.
- Attachments – Lets you attach external files to the case.
- Importing – Lets you import data received by other programs to the case (RIM BlackBerry Backup, iPhone OS 1.x-2.x Backup, iPhone OS 3.x Backup and Deployable Device Seizure cases are supported).
- The SIM Cloner – Lets you duplicate identification files from a GSM SIM card to a blank card.
- The CSI stick support - Lets you import data acquired by the CSI Stick from cell phones (Motorola, LG, and Samsung) into a Device Seizure case file for analysis.
- Device Seizure Comparer – Lets you compare Device Seizure cases.

Connection Problems

Are you having problems connecting your device with Device Seizure? Listed below are the general types of manufacturer devices you may be examining, we've included some basic tips on connecting to these devices successfully in the order shown.

Nokia Symbian

Nokia

Motorola iDen

Motorola

Samsung

LG

Palm Treo

Palm Pre

Android

Nokia Symbian:

Upon connection, Nokia Symbian devices usually require examiners to designate a connection mode. This option will usually appear on the phone once it is connected to the computer as "PC Suite."

Nokia:

Upon connection, many Nokia cell phones require the examiner to designate a connection mode. To connect to the phone with Device Seizure, choose “PC Sync.” The “PC Sync” option will either appear on the phone screen automatically, upon plug-in, or it can be found under the settings menu of the Nokia phone.

Motorola iDen:

To successfully connect in Device Seizure, most iDen cell phones require the examiner to place the device into “Airplane,” “Flight,” or “Transmitters Off” mode. These modes can usually be found in the phone menu under Settings>Advanced>Airplane mode or Settings>Advanced>Transmitters.

Motorola:

Many Motorola cell phones are required to be placed into “Data” or “USB” mode before connecting with Device Seizure. This setting can usually be found in the phone menu under Settings>Connection.

Samsung:

Many Samsung cell phones are required to be placed into “PC Studio” or “Modem” mode before acquiring with Device Seizure. These modes can usually be found under the settings menu of the Samsung phone.

LG:

Many LG phones must be placed into “Sync Data” or “Modem Mode” before acquiring with Device Seizure. If this option does not show on the phone upon connection, it can usually be found under the settings menu of the phone.

Palm Treo:

1. Bring the Device Seizure Acquisition Wizard to the window informing you that the device must be placed into console mode.
2. On the Palm Treo, press the Find key (spyglass).
3. When the find box appears, hold down the Alt key and press S, on the keyboard.
4. Press the Alt key.
5. Scroll through the graffiti and choose the cursive, lower case L.
6. Enter a . (dot) on the line after the cursive L.
7. Press next on in the Device Seizure Wizard.
8. **Immediately hold down the Shift key on the Treo and press 2.

** The only indication that the Treo is in console mode is the disappearance of the cursive L and the dot from the find box.

Palm Treo: *(continued)*

If the device fails to connect, in Device Seizure, the Treo must be soft reset by pushing the recessed soft reset button (usually under the battery cover, next to the battery), and the process must be repeated.

The link below will take you to video with instructions on placing a Palm Treo into console mode.

<http://support.paraben.com/video.html>

Palm Pre:

The Palm Pre must be placed into “Developer Mode” before performing a physical data acquisition with Device Seizure. To place a Pre into Developer Mode, follow the steps below:

1. On the main screen of the Pre, press the Launcher button (looks like an up arrow).
2. Type (no spaces): up up down down left right left right B A start.
3. Immediately after typing the code, the “Developer Mode Enabler” will appear on the screen.
4. Press the “Developer Mode Enabler” button on the screen of the Pre.
5. The phone is now in Developer Mode.
6. Acquire the Palm Pre with Device Seizure.

Android:

Android based cell phones must be placed into “debugging” mode before acquiring the device in Device Seizure. To place an Android based device into debugging mode, follow the instructions below:

1. **On the Android based cell phone, navigate to Settings>Application Settings and place a check in the “Unknown Sources” checkbox.
2. On the cell phone, navigate to Settings>Application Settings>Development and place a check in the “USB debugging” checkbox.
3. Connect the cell phone to the USB port on your computer.
4. If using Device Seizure 3.2 you will need to install the Android device drivers, manually, on your computer. After installing the Android drivers, you will need to specify where the drivers have been stored by pointing to their storage folder. Device Seizure 3.3+ installs these drivers automatically.
5. Acquire the Android cell phone using the Android (logical) manufacturer option in Device Seizure.

** Please note that AT&T and Motorola have taken the “Unknown Sources”, found in step 1, out of AT&T devices. Device Seizure does not support these models.

There are many additional resources available through the primary help file for Device Seizure located under the Help menu in the tool. Paraben also offers a variety of resources to help including:

- Paraben Forum
- Paraben Training
- Paraben Tech Support Ticket System

For more information on any of these or Paraben's other forensic technology please visit us at:

www.paraben.com or email us at **forensics@paraben.com**

IMPORTANT: Paraben Product Activation. This product may use technological measures for copy protection. IN SUCH EVENT, YOU WILL NOT BE ABLE TO USE THE PRODUCT IF YOU DO NOT FULLY COMPLY WITH THE PRODUCT ACTIVATION PROCEDURES. Product activation procedures and Paraben's End-User License Agreement will be detailed during installation process of the product, or upon reinstallations of the software product, and may be completed by Internet or Telephone (toll charges may apply). To activate, enter Product ID number included in or on this package (retain this information). This software is subject to the terms and conditions described in the End-User License Agreement (EULA) located either in the product documentation or online within the software product. By using the software product, you indicate that you have read and accepted the terms of the EULA.

Paraben Product ID Label

Each Paraben Product is licensed with a unique Product Identification Number.
Please contact Paraben Corporation if your license or Product ID Number is missing.

