

paraben's

Phone Recovery **STICK**

Paraben's Phone Recovery Stick

v. 4.5

User Manual

Contents

About Phone Recovery Stick	3
What's New!.....	3
Getting Started	4
System Requirements	4
How to Use the Phone Recovery Stick	4
Application User Interface	5
Understanding the User Interface	5
Main Page.....	5
Data Page.....	5
Main Menu	7
Recovering Data.....	8
Recovery Prerequisites	8
Recovering Data from the Android OS Based Device.....	9
Working with Workspaces.....	12
About Workspaces	12
Creating New Workspace.....	12
Opening Existing Workspace.....	12
Validating Workspace.....	12
Closing Workspace.....	13
Viewing Android OS Based Device Data.....	13
Recovered Data.....	13
Acquired Data from Phone and Memory Card.....	14
Device Properties	18
Searching Data.....	19
Exporting Data	20
Exporting Data to MS Excel	20
Bookmarks.....	21
Accessing Bookmarks	21
Adding Bookmark	21
Editing Bookmark	21
Deleting Bookmark	21
Troubleshooting	22
Creating Log Files	23
Phone Recovery Stick Options	24
Additional Information and Training	25

About Phone Recovery Stick

Welcome to Paraben's Phone Recovery Stick!

This program allows investigators to recover data from Android OS based devices including SMS and MMS text messages. Also, you can view and analyze other acquired data from the Android OS based device, including contacts, messages, call history, Internet Browser data, installed application data, graphics, and multimedia files.

What's New!

Added Support for Android 7 & 8: Added support for deleted data recovery for devices running Android 7 & 8. Please note that devices must be rooted.

Please note: Data recovery for rooted devices supporting KNOX is not possible in this version. For a list of devices that support KNOX, please visit <https://www.samsungknox.com/knoxportal/files/GalaxyDevicesSupportingKNOX.pdf>

Getting Started

System Requirements

The following requirements must be met to use Phone Recovery Stick:

- Phone Recovery Stick requires Windows Vista or newer 32 or 64-bit operating system.
- To use the Export to Excel feature, you must install Microsoft Excel on your computer and you must add the .Net Framework programming tools during the installation process.

How to Use the Phone Recovery Stick

To start using Phone Recovery Stick, do the following:

1. Plug the Phone Recovery Stick into the USB port of your computer.
2. Double-click the **PhoneRecoveryStick.exe** file.
3. If drivers for Android devices are not installed, the PhoneRecoveryStick.exe file will initialize their installation. Follow the installation wizard if needed.
4. When installation is finished, remove the Phone Recovery Stick from the USB port. We also recommend you to restart the computer to make sure installation has been completed correctly.
5. Plug the Phone Recovery Stick into the USB port of your computer.
6. Double-click the **PhoneRecoveryStick.exe** file.
7. The Phone Recovery application main window opens.
8. Now you are able to perform data acquisition and recovery as it is described below.

Application User Interface

Understanding the User Interface

The Phone Recovery Stick interface includes the following parts:

- **The Main page:** This page contains information about Phone Recovery Stick and two buttons that let you open the existing workspace or start recovery process from the Android OS based device.
- **The Data page:** On this page, the recovered data and other acquired data received from the device is displayed.
- **The Main menu:** The menu provides access to the main functionality of Paraben's Phone Recovery Stick.

Main Page

The Main page of Phone Recovery Stick opens at the program start-up.

It contains the following elements:

- A toolbar.
- Short description of Phone Recovery Stick.
- Two icons: **Start Recovery** and **Open Workspace**.
- A link to the Data page if there is any data in the workspace.

From the Main page, you can do the following:

- Start recovery process from the Android OS based device.
- Define program options.
- Open an existing workspace.
- Move to the Data page.
- Rename the currently opened workspace.
- Export workspace data to Excel.

Data Page

The Data page opens when data recovery process finishes, you open a workspace, or you click the Back to Data link on the Main page.

The Data page contains the following elements:

- A list of data categories.

Phone Recovery **STICK**

- The Data pane in which data is displayed.
- The name of the device from which data was recovered.
- A Search Text field.
- The Details pane, including the Properties tab, the Bookmarks tab, the Acquisition Details pane, the Extended View tab, and the Search Results tab.
- A link to the Main page.

From the Data page, you can do the following:

- View the recovered data.
- View the properties of the device from which you recovered data.
- Search text data in the workspace.
- Create and access bookmarks.
- Define program options.
- Open an existing workspace.
- Go to the Main page.
- Save the opened workspace using a different name.
- Export workspace data to Excel.



Main Menu

File Menu

The File menu contains basic file options for working with Phone Recovery Stick.

Menu Item	Description
Open Workspace	Opens a saved workspace.
Save As	Saves the open workspace under a different name.
Start Recovery	Closes the open workspace and displays a screen from which you can select a device to scan.
Export to Excel	Exports the content of the workspace as an MS Excel (.xls) file.
Exit	Shuts the Phone Recovery Stick down.

View Menu

The View menu lets you display tools in the Phone Recovery Stick user interface.

Menu Item	Description
Properties	Opens the Properties pane containing properties of the acquired device.
Bookmarks	Opens the Bookmarks pane containing created bookmarks.
Acquisition Details	Opens the Acquisition Details pane containing information on device acquisition.
Extended View	Opens the Extended View pane for viewing advanced information on recovered data and some application data (e-mails, etc.)
Search Results	Opens the Search results pane containing results of the recent search.

Tools Menu

The Tools menu lets you check for Phone Recovery Stick updates and define logging and folder options.

Menu Item	Description
Options	Allows you to define logging options and the default folder for saved workspaces.
Validate Workspace	Runs a hash encryption algorithm on a workspace data to ensure the data has not been altered.
Check for Updates	Connects to the Paraben's site to download updates.

Help Menu

The Help menu gives access to this help file, information about the Phone Recovery Stick application, and displays registration data.

Menu Item	Description
Help	Opens Phone Recovery Stick user documentation.
About Qt	Provides data about the Qt tool, licensed for use in Phone Recovery Stick.
About	Displays the Phone Recovery Stick description and the version number.

Recovering Data

Phone Recovery Stick allows you to recover data from Android OS based device.

Android devices vary by manufacturer. Each manufacturer has the ability to modify the device and it can affect the support of the device within Phone Recovery Stick. Paraben tests on a variety of devices from a variety of manufacturers, but that does not guarantee 100% support of all Android devices running a particular firmware because of these manufacturer differences. If your device firmware is supported, but your device does not process, please gather the logs and send them to our support team. This will allow us to add modifications in future releases to account for the manufacturer differences on the device you were processing.

WARNING: Phone Recovery Stick places recovered data in a temporary workspace that is automatically created in the workspace folder. The folder location is defined in the Options menu and has a *Workspace<number>.ds* name. When you close the workspace, you must save it or you will lose the data.

Recovery Prerequisites

Before the recovery process starts, do the following:

1. Turn on the device.
2. Make sure that the device battery is completely charged.
3. Connect the Android OS based device to the computer with a data cable. Use the USB connection mode to recover data from the Memory Card.
4. Enable the USB debugging mode on your device.

Depending on the version of the Android OS, the USB debugging mode is enabled as follows:

- For Android OS up to version 4.0: In the device menu, select Settings->Applications->Development and select the USB debugging option.
- For Android OS from 4.0 and up to 4.2: In the device menu, select Settings->Developer options and select USB debugging.
- For Android OS 4.2 and newer: In the device menu, select Settings->About device/tablet and tap Build number 7 times, then go back to Settings, select Developer options, and then select USB debugging.

Recovering Data from Android OS Based Device

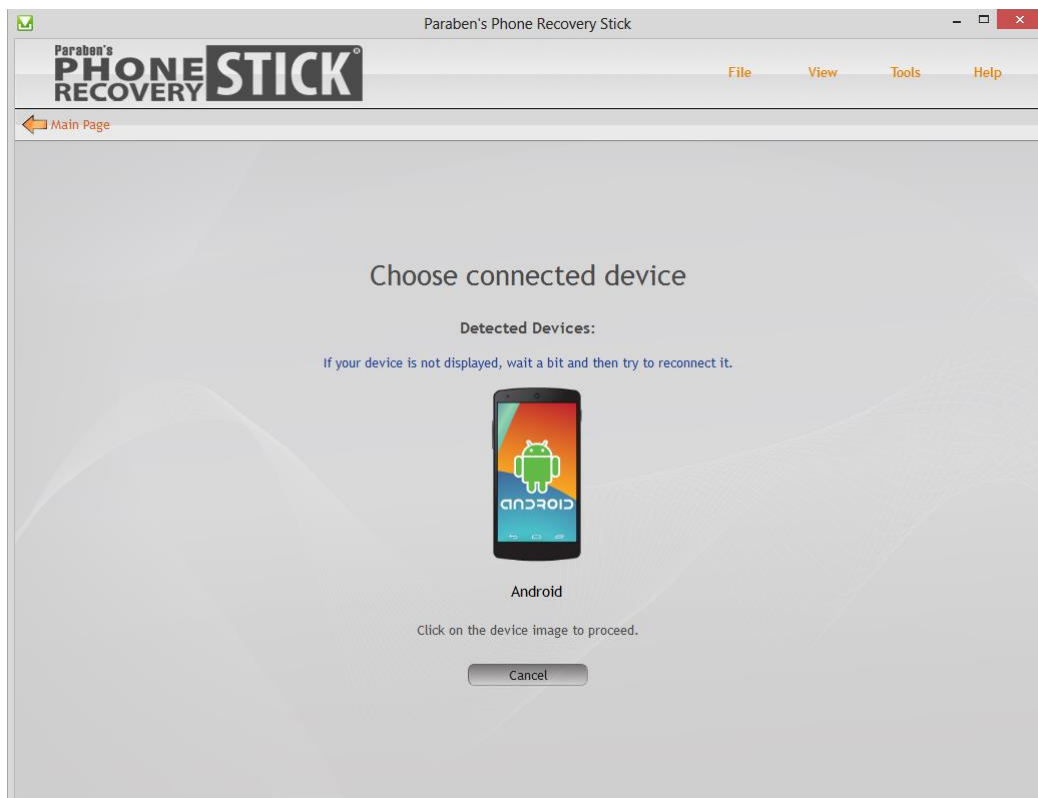
The Phone Recovery Stick acquires data and recovers the deleted data from Android OS based devices. This section explains how to recover data from your Android OS based device.

Please note, before acquisition starts, the device file system will be unlocked. For this purpose, the AndroidService.apk installation package is written to the /data/local/tmp folder, and the com.paraben.service service is installed to the system folder with applications. They will be removed automatically after the recovery finishes.

To recover data from the Android OS based device:

1. Do one of the following:
 - Click **Start Recovery** on the Main page.
 - Click **File > Start Recovery**.
 - Press **F5**.
2. Click the image of the device you want to scan. If multiple devices are connected to your computer, multiple images are displayed.

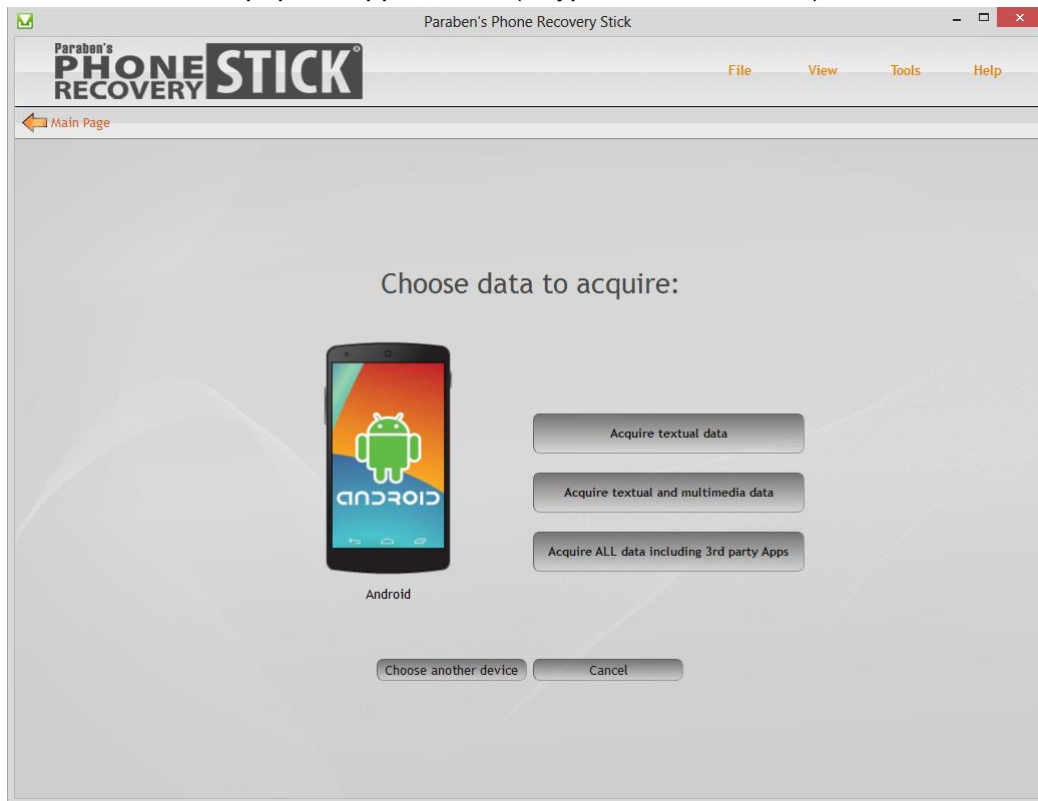
NOTE: If your device does not appear in the list in several seconds after the connection, try to disconnect it and then connect it back again.



3. Select one of the following acquisition options and click the corresponding button to start acquisition:
 - **Acquire textual data:** This type of acquisition takes the shortest time. SMS, Call Logs, Notes, calendar, etc. will be acquired and recovered.

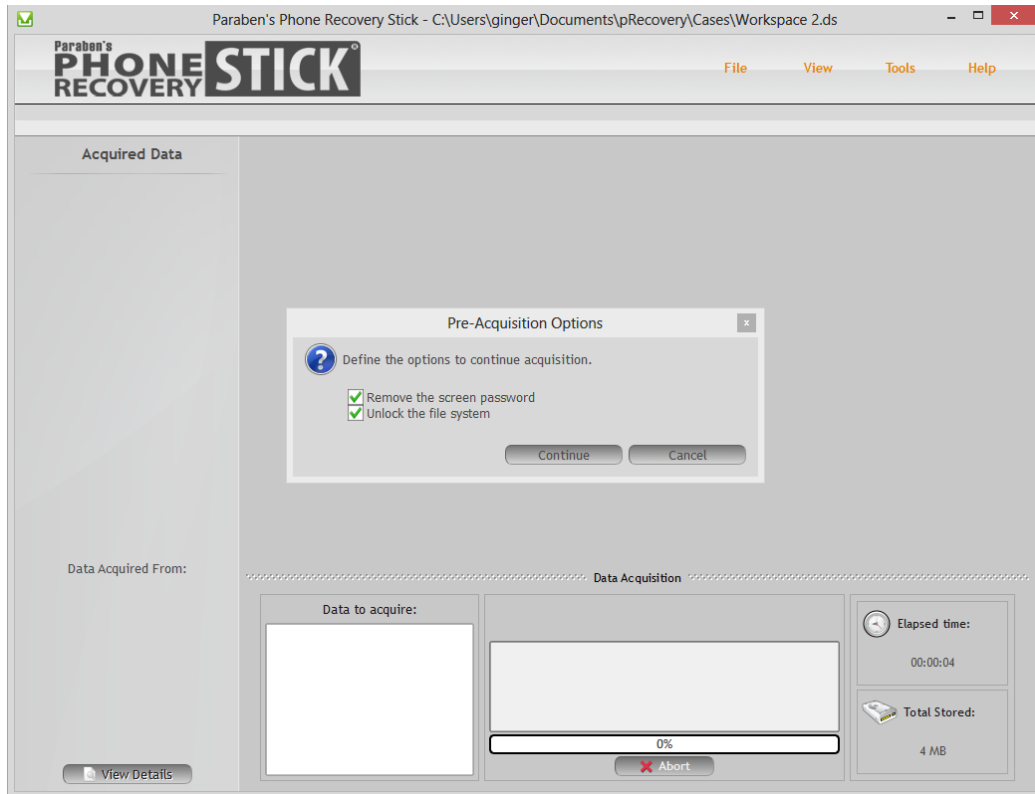
Phone Recovery **STICK**

- **Acquire textual and multimedia data:** This type of acquisition allows acquiring graphics and multimedia along with the textual data.
- **Acquire all data including 3rd party Apps:** This type of acquisition takes the longest time. Acquired data will contain not only text data and multimedia, but a full list of applications installed on the device, the list of their permissions, and data from most popular applications (Skype, Facebook, etc.).



4. Before acquisition starts, you need to select additional options:

- Select **Remove the screen password** to remove any screen password protection on the device (password, graphical password, and PIN). This feature is available only for Android OS up to version 4.1.
NOTE: If the screen password still appears after removal, simply draw any pattern to remove a graphical password or enter and confirm a new PIN or password.
- Confirm device file system unlocking by selecting **Unlock the file system**. This action is required to perform the acquisition.
NOTE: Unlocking a device file system does not damage the device or any data on it.



5. A message might appear asking you to allow the USB debugging on the device. Click **OK** in the message in Phone Recovery Stick and tap **OK** in the message that appears on the device.
6. The recovery process starts.

NOTE: During the acquisition and recovery, messages might appear on the device:

- If the Waiting For Debugger message appears on the device, do not close this message, otherwise the acquisition will fail. We guarantee that this does not affect data integrity on the device.
- If the Choose Connection Mode message reappears on the device, please choose the mode.

Working with Workspaces

About Workspaces

A workspace is a file with a **.ds** extension that contains information recovered from a single Android OS based device.

Creating New Workspace

When you start data recovery, Phone Recovery Stick creates a new temporary workspace. The workspace is named **Workspace<number>.ds**. By default, the workspace is saved in the current Windows user folder. The workspace is also updated after you create a bookmark. You can change the default location where a workspace is saved, and you can use the **Save As** function to relocate and rename a saved workspace.

To create a workspace:

1. Start the data recovery process. See [Recovering Data from Android OS based device](#).
2. Click **File > Save As**, then click **Save**.

To define the default workspace folder:

1. Click **Tools > Options**, then type the new name and browse to the folder you want to use.
2. Click **Save**.

To change the name of a workspace:

1. Open the workspace that you want to change.
2. Click **File > Save As**.
3. Browse to the location where you want to save the workspace, then type the new name.

Opening Existing Workspace

Workspaces created by Phone Recovery Stick (*.ds files) can be opened from the user interface.

To open an existing workspace, do one of the following:

- On the **Main** page, click **Open Workspace**.
- In the **File** menu, select the **Open Workspace** item.
- Press **Ctrl+O**.

When you open a new workspace, the currently opened workspace closes. Unsaved information is lost.

Validating Workspace

Using data validation you can check if the workspace data has been altered.

To validate a workspace:

1. Open an existing workspace with acquired data.
2. In the main menu, select **Tools > Validate Workspace** or press **CTRL+L**.
3. The data validation process starts.
4. When the validation process finishes, you will see the message with validation results.

Closing Workspace

The workspace closes when any other workspace opens or Phone Recovery Stick shuts down.

Viewing Android OS Based Device Data

The Phone Recovery Stick receives three types of data from the Android OS based device:

- Recovered data from the phone and recovered Multimedia and Graphics from the Memory Card.
- Acquired data from the phone and Memory Card.
- Device properties.

NOTE: Data is recovered only for Android OS version 4.4.2 and lower.

Recovered Data

Phone Recovery Stick recovers the following types of data:

- SMS messages (both incoming and outgoing)
- MMS messages (both incoming and outgoing) shown as not parsed binary data
- Call history
- Contacts (only numbers)
- Calendar events
- Multimedia files
- Application data

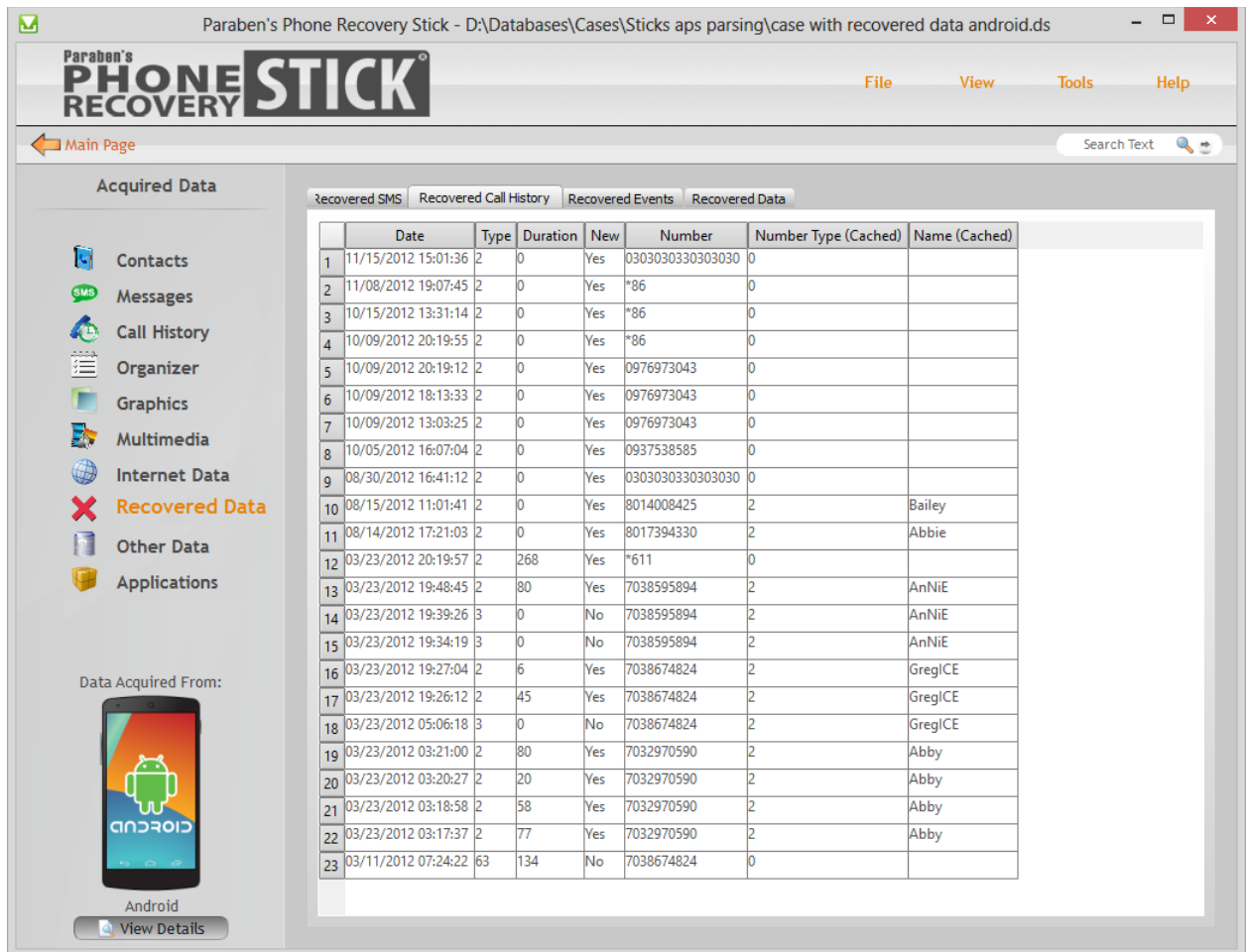
To view the recovered data, select the **Recovered Data** category. The recovered data is parsed and displayed in grids. There is a separate tab for each type of the recovered data. The number of columns for each category depends on the category type.

You can view the records in the not parsed format in the **Recovered Data** tab. The selected record opens in the **File viewer** below the **Data pane**.

Phone Recovery **STICK**

To change the code page for the opened record, select the required encoding in the drop-down list.

To close the File viewer for the record, click **Close**.



Acquired Data from Phone and Memory Card

Acquired data from an Android OS based device and from the Memory Card consists of text data, multimedia data, and application data. The amount of data depends on the selected type of the acquisition.

The categories of acquired data are displayed to the left of the **Data page**. Click the category name to view its content.

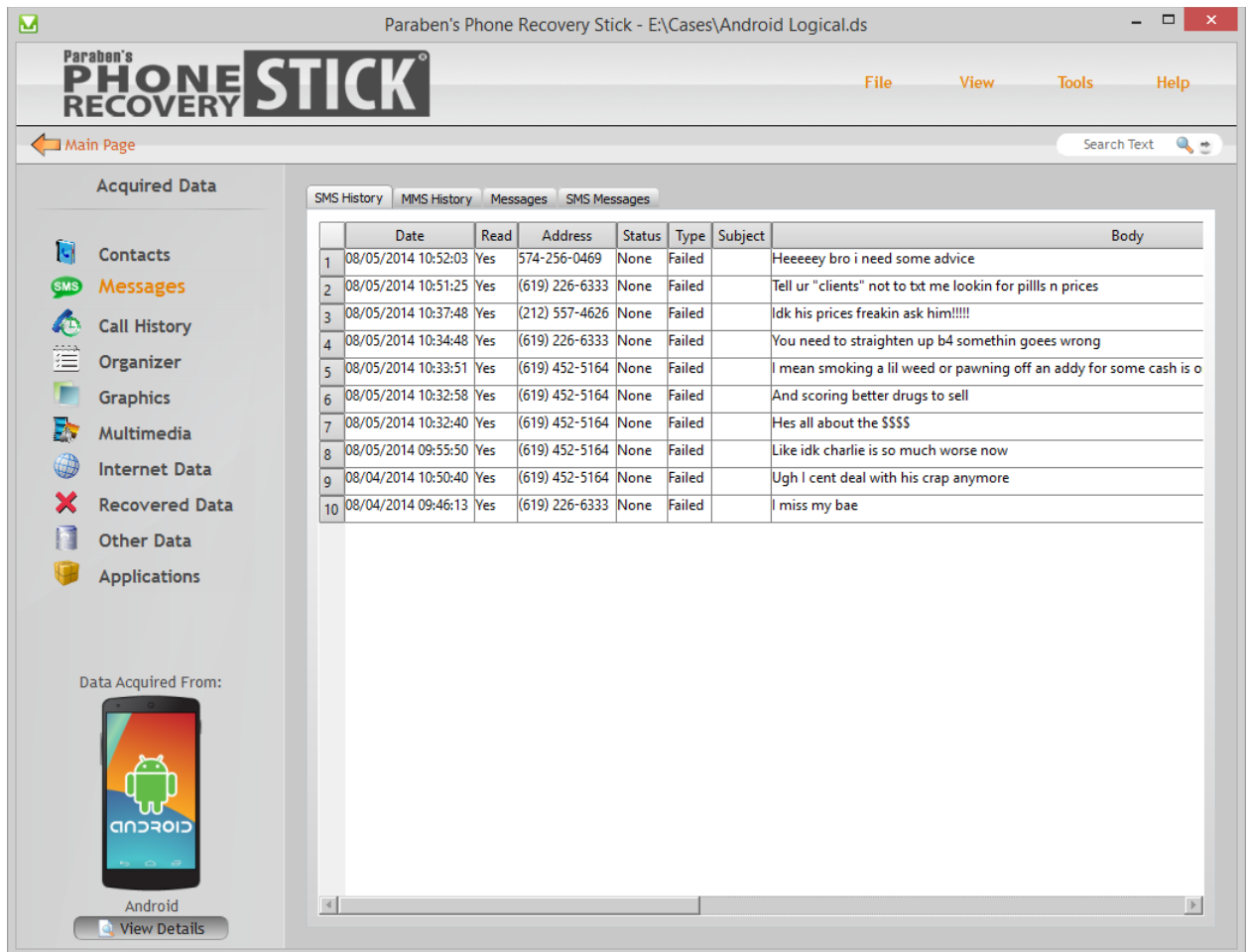
Text data includes the following categories:

- **Contacts:** The device phonebook.
- **Messages:** The device SMS and MMS messages.
- **Call History:** The device call logs.

Phone Recovery **STICK**

- **Organizer:** The device calendar and events.
- **Internet Data:** Includes URL and Search history.
- **Other Data:** This data includes Android OS based device system settings.

Data from each category is displayed in a grid to the right of the Data page. There can be several tabs in the grid if data contains sub-categories.



Multimedia data includes **Graphics** and **Multimedia** categories.

This data is displayed as thumbnails. You can click a file to view it. The file opens in the same pane. If necessary (for big images), it scales to fit the window size. To return to thumbnails, click the scaled image.

You can also use external viewers to view multimedia data. **To open the image in the external viewer**, right-click it and select **Open with**.



Application data includes a full list of installed applications, parsed application data for the most popular applications, and the permission list, which includes the full list of permissions an application has and the application suspicion rate basing on its permissions. Data is displayed in three tabs: the first tab displays application permissions, the second tab includes the list of all installed applications, and the third tab displays the parsed application data in the tree-view structure.

NOTE: Application list is acquired for any Android OS version. Application data is acquired only for Android OS version 4.4.2 and lower.

Application data for the following applications is parsed: Whisper, WhatsApp, KIK, LinkedIn, Jott Messenger, TextFree, TextPlus, V Kontakte, Facebook, Facebook Messenger, Pinger, Skype, and Google Chrome.

Phone Recovery STICK

Paraben's PHONE RECOVERY STICK

Application Permissions | Installed Application List | Application Data

Icon	Application Name	Version	Malware Suspect	Application Permissions	**MODIFY_PHONE_STATE
1	Google App	4.5.13.16.arm	Highly Suspect	Data >>	0
2	Google Play services	7.0.99 (1809214-034)	Highly Suspect	Data >>	1
3	Google Play Store	5.5.12	Highly Suspect	Data >>	0
4	textPlus	5.9.9	Highly Suspect	Data >>	0
5	Chrome	41.0.2272.96	Suspect	Data >>	0
6	Email	4.1	Suspect	Data >>	0
7	Facebook	30.0.0.19.17	Suspect	Data >>	0
8	Google Play Music	5.9.1854R.1904527	Suspect	Data >>	0
9	Google+	5.4.0.92311906	Suspect	Data >>	0
10	Messenger	28.0.0.44.274	Suspect	Data >>	0
11	VK	3.12	Suspect	Data >>	0
12	Currents	2.3.0	Low Suspect	Data >>	0
13	Earth	8.0.2.2334	Low Suspect	Data >>	0
14	ES File Explorer	3.2.5.3	Low Suspect	Data >>	0

Data Acquired From: Android

PERMISSIONS FOR Google Play services

**Highly Suspect:

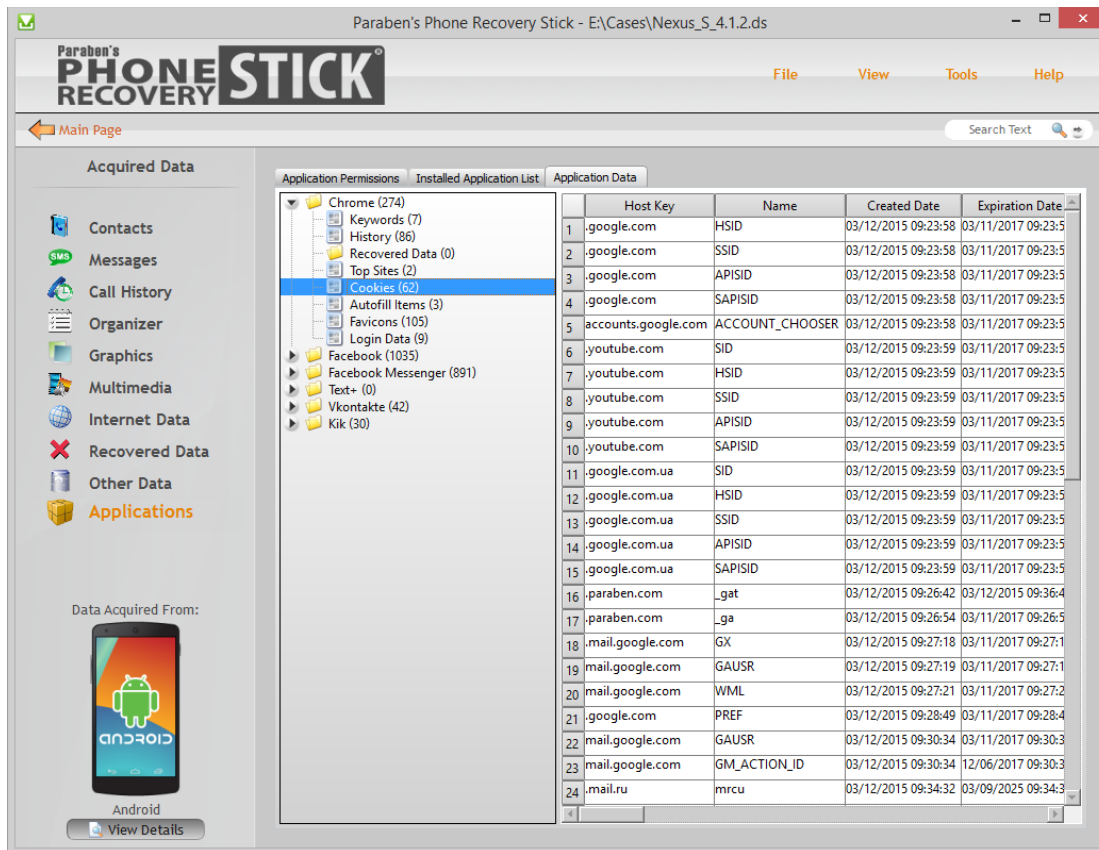
- android.permission.MODIFY_PHONE_STATE
- android.permission.READ_FRAME_BUFFER
- android.permission.CAPTURE_AUDIO_OUTPUT
- android.permission.CAPTURE_SECURE_VIDEO_OUTPUT
- android.permission.CAPTURE_VIDEO_OUTPUT
- android.permission.BLUETOOTH_PRIVILEGED
- android.permission.CALL_PRIVILEGED
- com.android.voicemail.permission.READ_VOICEMAIL
- android.permission.WRITE_PROFILE
- android.permission.BODY_SENSORS

Paraben's PHONE RECOVERY STICK

Application Permissions | Installed Application List | Application Data

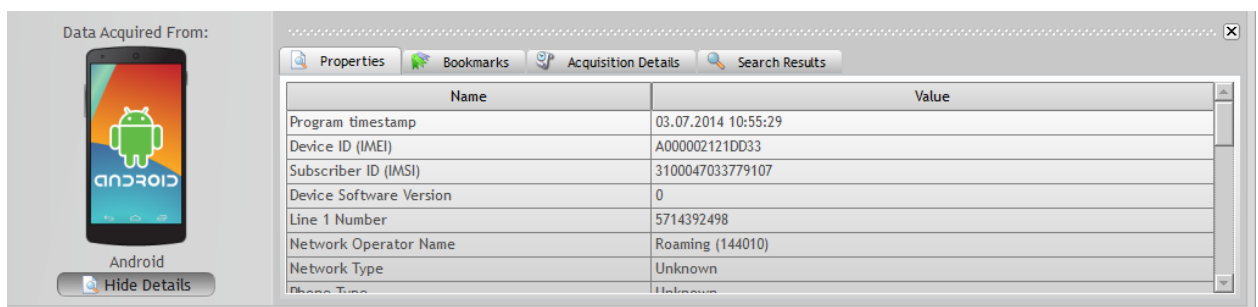
Icon	Application Name	Version	Internal Application Name	Category	Manufacturer
1	Chrome	41.0.2272.96	com.android.chrome	Communication	Google Inc.
2	Facebook	30.0.0.19.17	com.facebook.katana	Social	Facebook
3	Kik	8.3.0.678	kik.android	Unknown	Kik Interactive
4	Messenger	28.0.0.44.274	com.facebook.orca	Communication	Facebook
5	textPlus	5.9.9	com.gogii.textplus	Social	textPlus
6	VK	3.12	com.vkontakte.android	Social	VKontakte
7	Currents	2.3.0	com.google.android.apps.currents	Unknown	Unknown
8	Earth	8.0.2.2334	com.google.earth	Unknown	Unknown
9	Email	4.1	com.google.android.email	Unknown	Unknown
10	ES File Explorer	3.2.5.3	com.estrongs.android.pop	Unknown	Unknown
11	Gmail	4.1.2	com.google.android.gm	Communication	Google Inc.
12	Google App	4.5.13.16.arm	com.google.android.googlequicksearchbox	Unknown	Unknown
13	Google Play Books	3.4.9	com.google.android.apps.books	Unknown	Unknown
14	Google Play Movies & TV	3.8.8	com.google.android.videos	Unknown	Unknown
15	Google Play Music	5.9.1854R.1904527	com.google.android.music	Unknown	Unknown
16	Google Play Newsstand	3.4.1	com.google.android.apps.magazines	Unknown	Unknown
17	Google Play services	7.0.99 (1809214-034)	com.google.android.gms	Unknown	Unknown
18	Google Play Store	5.5.12	com.android.vending	Unknown	Unknown
19	Google Text-to-speech Engine	3.4.6.1819666.arm	com.google.android.tts	Unknown	Unknown
20	Google+	5.4.0.92311906	com.google.android.apps.plus	Unknown	Unknown
21	Street View	1.8.1.2	com.google.android.street	Unknown	Unknown
22	TalkBack	4.2.0	com.google.android.marvin.talkback	Unknown	Unknown
23	YouTube	10.18.55	com.google.android.youtube	Unknown	Unknown

Data Acquired From: Android



Device Properties

The properties of the Android OS based device from which data was recovered are displayed in the **Properties** tab of the **Details** pane. Click **View Details** to open the details pane.



Searching Data

The Phone Recovery Stick allows you to search for text data in a workspace.

To search text data:

1. On the **Data** page, in the **Search Text** field (in the upper right corner of the page), type the search string text.
2. Click **Search** or press **Enter**.
3. The search progress is displayed in the **Search Results** tab of the **Details** pane. Click **Abort** to stop the search.
4. When the search finishes, the search results are displayed in the **Search Results** tab of the **Details** pane. Each result is displayed as <Category name>\<Sub-category (tab) name>.
5. Double-click the search result to navigate to it.

When searching, you can use the **Search Word List** option that allows you to load the search expression for a Boolean text search from a file.

To define the words list, create the text file (*.txt). Use the new line for **OR** logic. Words in one line are interpreted with **AND** logic.

To use the Load Words option:

1. On the **Data** page, in the **Search Text** field, click the arrow sign and select **Search Word List**.
2. In the opened window, click **Browse** and navigate to the text file with search expressions.
3. Click **Start Search**.
4. Data will be found according to the defined search expression.

For example:

Expression in the table	Found result	Not found
White cat Black Dog	White cat and dog Black dog White cat and black dog	White snow Gray cat
White Cat with dog Black	White cat with dog Black cat	Gray cat with dog White cat

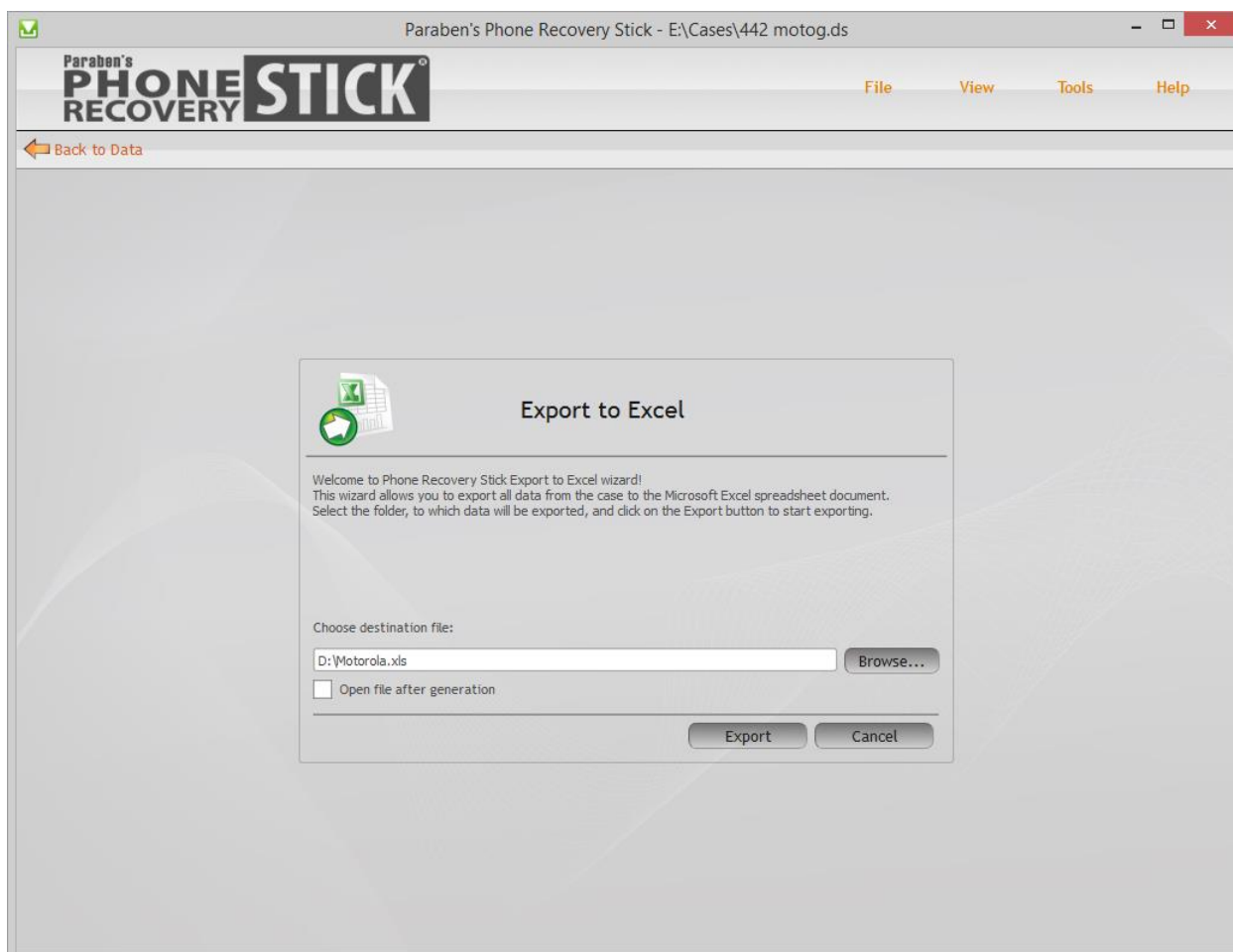
Exporting Data

Exporting Data to MS Excel

You can export data from the workspace as an Excel spreadsheet (.xls file).

To export data:

1. Click **File > Export to Excel**.
2. Click **Browse** to navigate to the destination folder and name the exported file.
3. Check **Open file after generation** to open the exported file.
4. Click **Export**.



Bookmarks

A Bookmark is a pointer to data stored in the workspace.

Bookmarks include the following information:

- Item (the name of the first cell of the row to which the bookmark is pointing)
- Name (the name of the bookmark)
- Details (the description of the bookmark)

Accessing Bookmarks

Bookmarks are displayed in the **Bookmarks** tab of the **Details** pane.

To view bookmarks:

1. Do one of the following:
 - Click **View > Bookmarks**.
 - On the Data page, click **View Details** (in the bottom left corner).
2. To view the data to which bookmark is pointing, double-click the bookmark.

Adding Bookmark

To add a bookmark:

1. Select data to be bookmarked (it can be either a cell of the grid or a row).
2. Right-click the item and select **Add to Bookmarks**.
3. Type a name and a description for the bookmark, and then click **Save**.

Editing Bookmark

To edit a bookmark:

1. Open the **Bookmarks** tab of the **Details** pane.
2. Right-click the bookmark and click **Edit**, or, from the menu, click **Manage > Edit**.
3. Edit the bookmark name and description, and then click **Save**.

Deleting Bookmark

To delete a bookmark:

1. Open the **Bookmarks** tab of the **Details** pane.
2. Highlight the bookmark to delete.
3. Right-click the bookmark and select **Delete**, or, from the menu, click **Manage > Delete**.

4. Select **Delete All** to delete all bookmarks.

Troubleshooting

The following section provides answers for some common issues that you may encounter when using Phone Recovery Stick.

Problem: The Android OS based device hung. What do I do?

Solution: Reset the Android OS based device.

Problem: The Android OS based device doesn't connect to the computer. What to do?

Solution: Please try one of the following:

- The Android OS based device battery might need to be recharged.
- If that does not work, disconnect other USB devices from your computer and connect the Android OS based device to a different USB 2.0 port on your computer.
- If that does not work, turn the Android OS based device off and turn it on again.
- If that does not work, restart your computer and reconnect the Android OS based device to your computer.

Problem: The Android OS based device doesn't connect to PC in USB connection mode. What do I do?

Solution: Some Android OS based devices (for example, LG P925) can only be connected to the PC using mass storage mode and charging mode. However, data from the Memory Card will not be recovered using this mode.

Problem: When I launch the stick, all functions are disabled and a message appears asking me to activate the program, although the stick worked fine before. What happened?

Solution: Most probably you have renamed the stick drive. In this case, you need to rename the stick back to Droid Stick.

Creating Log Files

Phone Recovery Stick has three options for logging support built right in:

- The **Plug-in Log** option creates a text file log of the recovery based on the plug-in activity.
- The **Serial Log** option logs all traffic across the communication port.
- The **GUI Log** option logs all events that happened in the Phone Recovery Stick interface during one program session.

Logs contain useful information for resolving issues and adding support for new models.

The GUI Log is created automatically and rewritten each time when Phone Recovery Stick is restarted. The Plug-in Log and the Serial Log are optional. The best practice is to leave these logging options turned off unless you encounter a problem. Then enable both logging options and replicate the problem. These logs may be needed if you call tech support to assist you.

To enable the Plug-in Log and the Serial Log creating:

1. Click **Tools > Options**.
2. Check **Serial Logs, Plugin Logs**, or both.
3. Click **Save**.

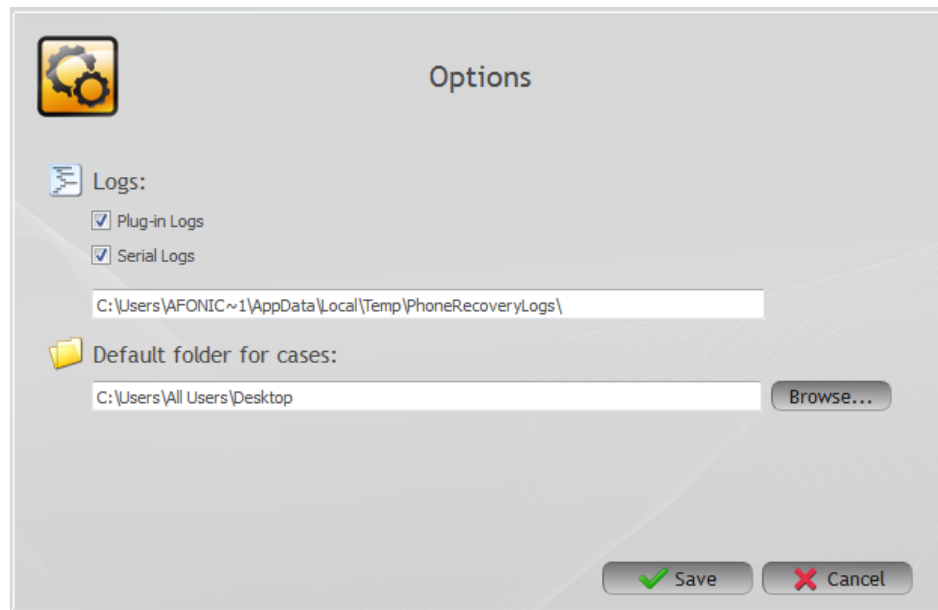
NOTE: All logs are created in the user folder (by default, **C:\Documents and Settings\{user name}\logs** in Windows XP and **C:\Users\Default\AppData\Local\Temp\logs** in Windows 7). The Plug-in Log and the Serial Log are overwritten when a new recovery process is performed using the same plug-in.

Phone Recovery Stick Options

To define Phone Recovery Stick options, select **Tools-Options**.

Phone Recovery Stick options are the following:

- **Logs:** You can define what logs will be created during the recovery process. The **Plug-in logs** option creates a text file log of the recovery process based on the plug-in activity and the **Serial logs** option logs all traffic across the communication port. If you have any problems with Phone Recovery Stick, send the logs to Paraben. The logs destination path is displayed below the logs checkboxes in the Options window.
- **Default Workspace Folder:** When the recovery process starts, a new workspace is automatically created in the default workspace folder. When you close such a workspace, you are proposed to save it under other name. If you do not want to save the workspace, click **No** and the workspace will be deleted. Make sure that there is enough space on the disk on which the default workspace folder is stored.



Additional Information

Paraben Corporation offers a variety of tools for investigations. These tools include iRecovery Stick for Android devices, Data Recovery Stick for deleted data recovery of a computer, Chat Stick for review and recovery of instant messaging data, and the Porn Detection Stick for the recovery and detection of illicit materials.

For any details on any of these products, please visit us at www.paraben-consumer.com