

Quick **Start** Guide



Paraben's®

P2 Commander® System

P2 Commander® + Forensic Replicator®

For use with Microsoft® Windows® XP/Vista/7

Paraben's P2 Commander 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 P2 Commander 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
- Basics of Reporting

There are many other aspects and features available in P2 Commander that are covered in the main electronic Help File.

Introducing P2 Commander

Paraben P2 Commander is a comprehensive forensics tool for examining disk drives, media, and disk images to find, organize, and analyze several different file types including:

- Documents
- Text files
- E-mail files
- Network email files
- Chat logs
- Graphics files
- Deleted files
- Archive/compressed files
- Windows registry
- Databases files
- Applications
- XML files

P2 Commander lets you sort the files into categories, preview the files, view text and hex information for the files, and hash the files to ensure that they haven't been changed or corrupted. You can use P2 Commander to analyze all data present on a computer hard drive regardless of whether the files have been previously deleted.

P2 Commander Related Applications

Paraben manufactures two applications related to P2 Commander that let you create and read disk images:

-Paraben Forensic Replicator


-Paraben P2 Explorer

Paraben Forensic Replicator

Paraben Forensic Replicator is a tool that lets you image disk drives, USB drives, and other storage media connected to a computer. This tool creates verified flat file images of the media in question and is court accepted as a forensic imaging tool. Refer to the help files that come with Paraben Forensic Replicator to learn how to create and save disk images.

P2 Explorer

P2 Explorer is a free application that lets you mount disk images and access them as if they were a read-only drive on your computer. It assigns a drive letter to each mounted virtual hard drive on your computer. Once mounted, you can access files and applications as though they were installed on your computer.

 **Caution:** Malware and other malicious software contained in an image can infect your computer if accessed using P2 Explorer.

Installing and Configuring P2 Commander

The installation process has three parts:

- Installation
- Registration
- Installation of the FOCH database (optional)

After installing P2 Commander, you must register the program. Without a registration P2 Commander can only be used for 30 days or 23 uses. This section outlines the installation process.

Computer System Requirements

The following computer system requirements are needed to use P2 Commander.

- Operating system: Microsoft Windows 2000 or later 32 bit OS.
- RAM: 1 GB, (1.5 GB recommended)
- .Net Framework version 2.0 or later.

Installing P2 Commander

P2 Commander Installation files have been provided for you on the same drive as your dongle. Go to the P2 Commander directory and select the setup files.

To install P2 Commander

1. On the welcome screen, click **Install Now**
2. When the install wizard displays, click **Next**.
3. Accept the license agreement, click **Next**.
4. Do one of the following:
 - Type the location on the folder where you want to install P2 Commander, click **Next**.
 - Click **Browse** and select the location of the folder where you want to install P2 Commander, than click **Next**.
 - Click **Next** to keep the default location.
5. Click **Install**.

Registration (*IACIS 2010 Version*)

Install P2 Commander from your IACIS Thumb Drive Dongle or from your registration site account at <http://register.paraben-forensics.com>

Your IACIS Thumb Drive is Your Dongle:

Once you have installed Device Seizure, simply make sure your IACIS Thumb Drive Dongle is plugged into the machine whenever you are running Device Seizure.

Updating P2 Commander:

IACIS users will receive free updates for one year (until April 2011). When a new version is released, a special version will be available for IACIS users. You can log into your registration site account using your Product ID (PID) found on your packaging and download the latest version.

Upgrading P2 Commander:

The IACIS version of P2 Commander is identical to the regular version except for the type of Dongle. In order to continue receiving new versions of P2 Commander after the first year, you will simply need to purchase an annual maintenance subscription (currently only \$220).

Installing the FOCH Database

The FOCH (Filter Out Common Hash) database is a set of hashed files that are associated with many common operating systems. When installed; P2 Commander uses this set of hashed files to filter out these common files so that it doesn't have to sort and rehash them each time you do a scan.

If you received P2 Commander on a CD, the FOCH database should have arrived in the package on a separate CD. If not; the FOCH database can be downloaded from the Internet (instructions below). When you start P2 Commander there is a link at the bottom of the information in the Welcome screen. You can download it using this link.

To install the Foch Database

1. Do one of the following:
 - Open P2 Commander. In the welcome screen click:
 - **Download the database from Paraben's site.**
 - Download the database directly from:
 - **<http://www.paraben-forensics.com/downloads/foch.exe>**
2. Start the Foch.exe application.
3. Type the location where you want to place the database. It should be in folder named CommonFiles (NIST) placed in the root directory where you installed P2 Commander. The correct location is provided by default if you selected the default location for installing P2 Commander.
4. Click **Install**.

Working in P2 Commander

Once P2 Commander is registered with either a license key or with a dongle you are ready to start using the program.

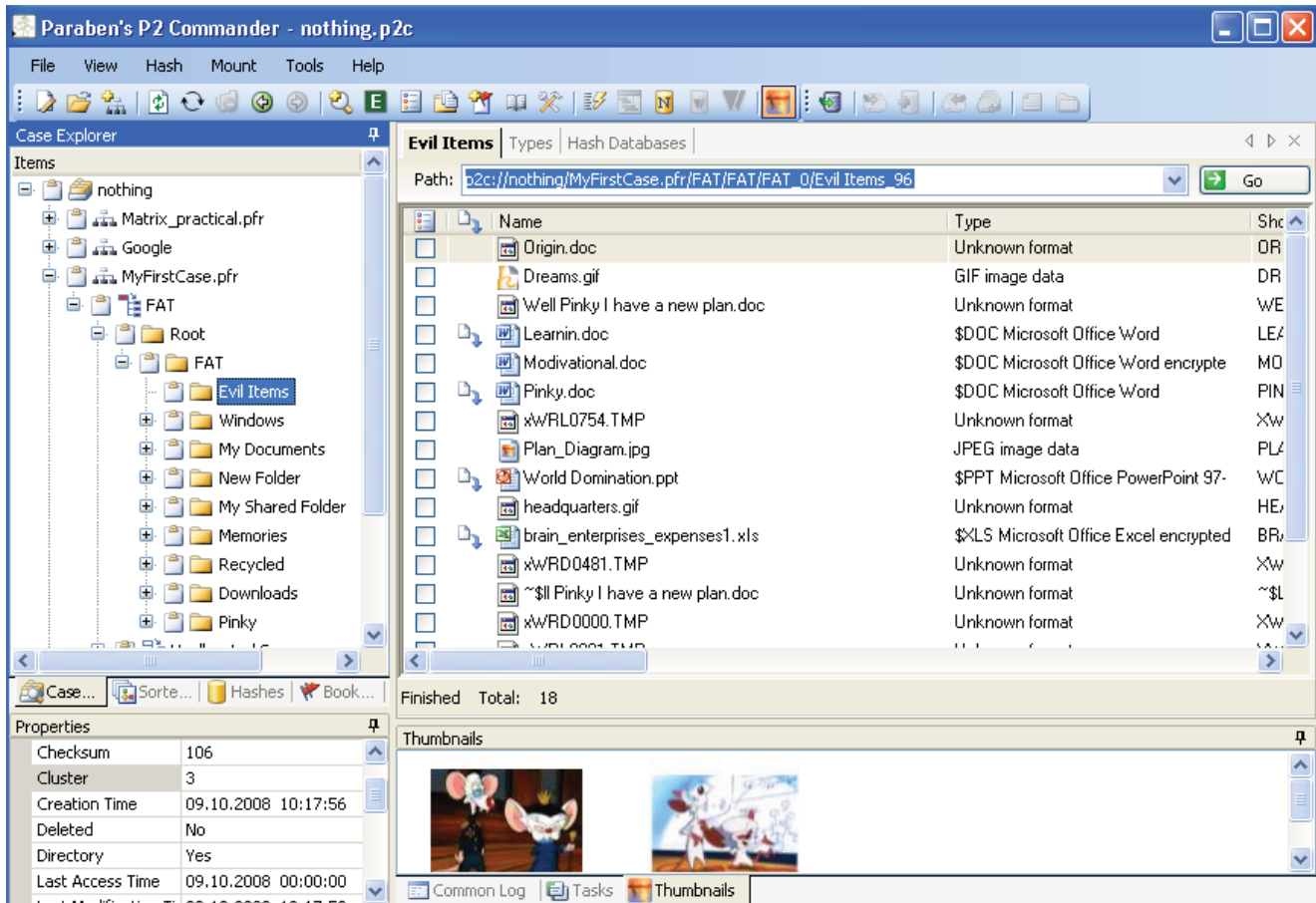
Exploring the P2 Commander interface

P2 Commander has four main information panes as shown in the following image.

The panes are:

- Evidence pane – Upper left – Displays the file system and files found in the evidence items.
- Files pane – Upper right – Displays files in a folder of groups of files that have been sorted.
- Properties pane – Lower left – Displays file properties.
- Information view pane – Lower right – Shows file data including images, thumbnails, text, and HEX data.

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



P2 Commander Data Examination Process

P2 Commander has several important functions that you will need to be familiar with and perform in order to store and examine the evidence. The functions include:

- Create a case
- Add evidence
- Sort files
- Examine files
- Create reports
- Export data


Each of these is outlined in this guide. More comprehensive information is available within the Help files located in P2 Commander under the Help menu.

Creating a Case

When you initially start P2 Commander you need to create a case. If you attempt to add evidence before creating or opening a new case the New Case wizard will prompt you to name the case file so that it can store your case data. This ensures that your case data is automatically saved and reduces the risk of information loss due to equipment failure.

Creating a case consists of naming the file and providing details related to the case. The New Case wizard provides you with fields that you can use to type your file information.

To create a new case

1. From the main menu click **File > New Case**. Or, in the tool bar; click the New Case icon. 
2. In the Welcome tab, click **Next**.
3. In the Case Properties tab, do the following:
 - Enter a name for your case in the Case Name field. The case name is required and serves as the name of the file in which your case is stored. Initially P2 Commander saves your case in the folder where P2 Commander is installed. Case names should be descriptive to easily locate them later.
 - Enter a description of the case. While not required, this data can be very useful if time has passed and you are re-examining a case, or if someone else needs to look at the case.
 - Click **Next**.

4. In the Additional Information tab type the following information: (This step is optional)

- Investigator name
- Agency/Company
- Phone number
- Fax number
- Email address
- Comments

Each field in this tab uses menus that remember information you have previously typed.

Click **Finish**.

NOTE: This information displays in reports that you create.

Adding Evidence

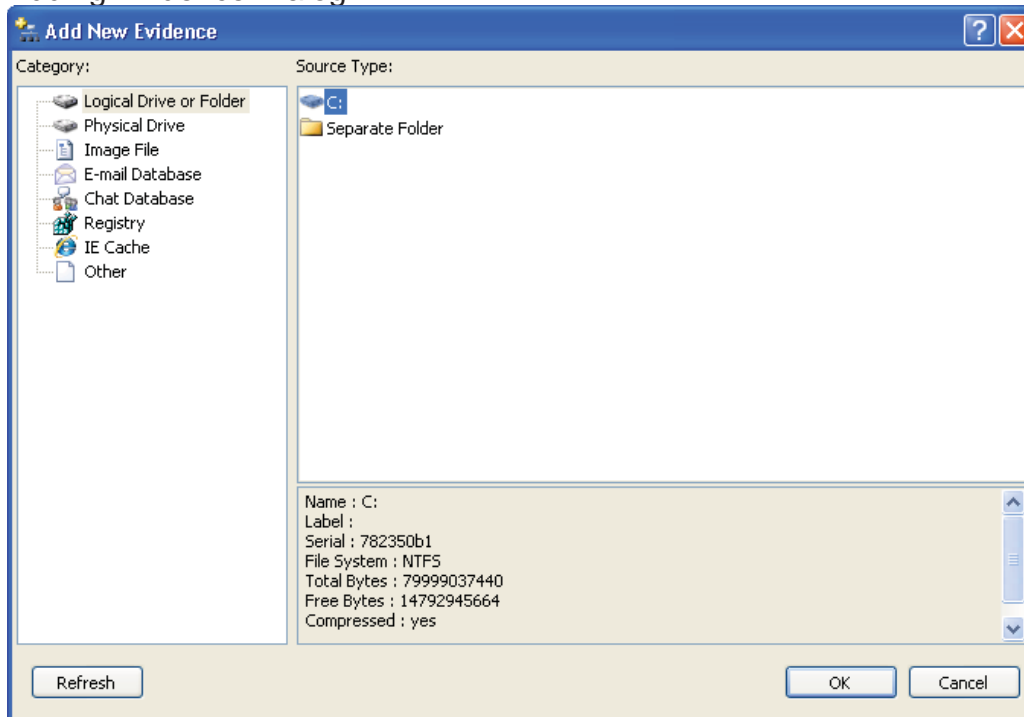
After creating your case you need to add the evidence. Adding evidence is the process of selecting which files and information that you want to search. P2 Commander lets you specify any of several data storage types. These include:

- *Logical drive or folder* – Reads the files and folders that are stored on the hard drive in hierarchical order. You can select an entire disk, or a folder on the disk.
- *Physical drive* – Reads all data on the disk regardless of whether it is stored in a logical folder on the disk drive or not.
- *Image file* – Reads a stored hard drive image. Has the ability to read images in most common formats. Has an auto-detect capability as well.
- *E-mail database* – You can select from one of many current email applications, or you can use the auto-detect function.
- *Chat database* - You can select from one of many current online chat applications, or you can use the auto-detect function.
- *Registry files*
- *Other* – Reads OLE storage and archive or compressed files.

One of the advantages of P2 Commander is the ability to have many different types of evidence in one case for analysis. For example if I am processing a case that is a hard drive, and a network e-mail storage (MS Exchange EDB) I can add them both to one case and

search them all at once. You have up to 64 Terabytes (theoretical) of data that can be stored in a case.


Adding Evidence Dialog:

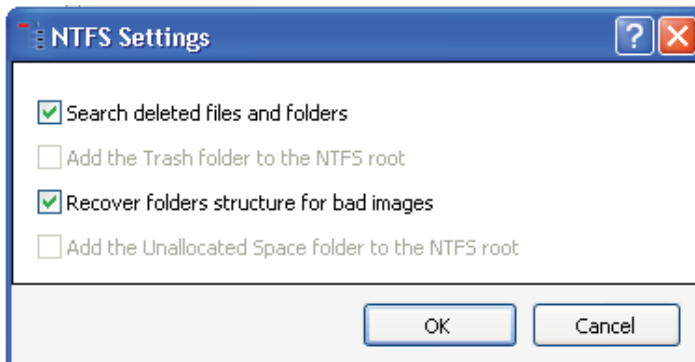


Note: When using the auto-detect function you have the option to select a file or folder. For most file and data sources you should select File. Only select Folder if the object you want to search is the actual folder itself. For most auto-detect options you should select the file and P2 Commander will determine what type of file it is.

To add evidence

Create a case. See Creating a Case on page 15.

1. Click the Add Evidence icon  or click **File >Add Evidence**.
2. In the Add New Evidence screen select the type of evidence that you want to add; then click **OK**.
3. Browse to the file or folder you want to select; then click **OK**.
4. Type the name for the evidence. By default this is the name of the object you select when you browse. It is the name that displays in the list of evidence objects. Click **OK**.
5. Select from the options you want to use when adding the evidence; then click **OK**.



- Search Deleted Files and Folders – looks for data that may have once resided in the folder of object, but was deleted.
- Add Trash folder to the NTFS root – If you are searching a disk drive this places the hidden trash files directly under the root for the evidence item.
- Recover folder structure for bad images – If the items being scanned have been corrupted this feature attempts to restore the data to its original state
- Add the unallocated space folder to the NTFS root – Adds a folder for data located in unallocated space on the hard drive. Unallocated space includes space that is not used by the file system and space outside of formatted areas.

NOTE: Some options in this step are not available with specific types of evidence.

After you add the evidence it displays in the case evidence pane of the application. The pane can be expanded making it easier to view, sort, and examine the files.

Sorting Files

After evidence is added you can sort the files into categories and related file types. This lets you quickly search for suspicious graphics, text, email, or chat files. P2 Commander automatically sorts files into the following types:

- Documents
- Email
- Chat
- Spreadsheets
- Graphics
- Databases
- Executable
- Compressed
- Multimedia
- Text
- XML
- Encrypted
- Others
- Image Analyzer Results
- Unallocated Files

The Image Analyzer results are populated with images that meet the specifications for probability of containing pornographic/illicit content. These settings can be configured to be more or less precise.

The *Unallocated Files* Menu Items in the sort can be expanded to show all of the above categories. These categories are populated with files and data found in unallocated disk space on the computer.

To sort files

1. In the tab menu at the bottom of the evidence pane, click **Case Explorer**.
2. In the Case Explorer list, right click an item. You can select a top level item, or drill down into the files and select a sub-folder.
3. In the drop-down menu, click **Sorting**.
4. Check the boxes next to the sorting options you want to use; then click **Next**. The options are:
 - Save current wizard options as the default
 - Sort deleted data
 - Sort unallocated space
 - Sort file slack – (unused space between the end of the file data and the end of the disk cluster that the file is stored in)
 - Calculate hash codes for partitions
 - Use Image Analyzer – Looks for pornographic content

- Sort recursively (Email Databases, OLE storages, Archives, Etc.) – Searches through these data sources for attached or compressed files that can be opened and sorted.
5. If you enabled the Image Analyzer; configure the settings for analyzing images, then click **Next**. Analyzer settings include:
 - Engine sensitivity – a higher setting finds more pornographic content, but also includes more false positives.
 - Use file filter – Ignores files larger or smaller than the options you select.
 - Ignores files outside of the height and width sizes you specify. Settings are specified in number of pixels.
 6. If you enabled sorting of email databases and compressed files, select the types of data you want to find in your search, click **Finish**.

NOTE: You can only sort one set of data at a time. To sort a new set of data; right-click the sorted data object and in the menu click **Clear Sorting**.
 7. To see the sorted files; in the tab menu of the evidence pane click **Sorted Files**.

Examining Files

After sorting the files the next step is to examine and determine what you have acquired. P2 Commander gives you several options for examining files and data sources. These include the following tools:

- Text viewer
- Hex viewer
- File viewer
- Email viewer
- Chat viewer
- Thumbnails viewer
- File slack hex viewer
- File slack text viewer

When you select a file or folder the appropriate options display in the tabs located in the information view pane. For example; if you select a folder that has no graphics the thumbnails tab is unavailable. The information displays in the pane when you click the tab.

To view files and file information

1. In the main menu click **View > Viewers** and ensure that all viewer options are selected.
2. In the Evidence pane expand the folders until you reach the folder or files you want to look at. If you want to examine a specific file click it in the Files pane.
3. In the Tab Menu at the bottom of the pane click the appropriate tab to see the information displayed in the format you want. For example; click HEX to view the HEX for the file.
4. Click the edge of the pane to resize it if necessary.

NOTE: File properties including size, creation date, and similar file properties display in the File Properties pane in the lower left of your screen


Creating Reports

P2 Commander lets you export four different standard reports. The reports types include:

- *HTML investigative report* – This creates a graphical report in HTML format. The report lets you add all evidence and include thumbnails of files and links to files in the report. The report lets you select the types of evidence you want to display and has many options for adding or leaving out evidence.
- *Simple text report* – This report exports to a .txt file. It provides options for including or leaving out specific information, but all evidence is listed in text format.
- *CSV text report* – Exports information into a spreadsheet. This has options similar to the text report.
- *HTML evidence summary report* – Gives a brief overview of the evidence for managers and supervisors.

When creating reports you can select specific files and information 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 Files pane. You can also export all evidence.


To create reports

1. If you want to create a report that shows specific data; navigate to the data in the Case Explorer tab of the Evidence pane and then in the Files pane check the box next to the files or folders you want to include.
2. Click the Report icon () or from the main menu, click **File > Generate Report**.
3. In the initial screen of the report wizard select the type of report and the location where you want to save the report. By default the report and all associated files are saved in a new folder using the file name of the case.
4. Click through the remaining screens in the wizard and select the options you want to display in your reports. These include: File Types, File Properties, Case Information, create a report with all evidence or only selected files, etc. The report options change depending on the type of report you select. For complete information on all report options see the help files in P2 Commander.
5. Click **Finish** to begin the process of creating the report. The creation process might take several minutes depending on the size and options you select when creating the report.

Exporting Files

P2 Commander lets you export files and folders found in the evidence to your computer or a location you specify. P2 Commander exports the files along with a hash file that can be used to ensure the data isn't changed. You can use the check boxes in the Files pane to select which files and folders you want to export.

To export files and folders:

1. In the Files pane, check the boxes next to the files and folders you want to export.
2. Click the Export icon () , or in the Main Menu; click **Tools > Export**.
3. Browse to the location where you want to place the evidence; then click **OK**.

Additional Features

This quick start guide has the basic features you need to begin working in P2 Commander. However; P2 commander has a powerful set of additional features that you can use to make your analysis easier and more complete. These features are listed in the section below with a brief description. Complete documentation for each is available in the P2 Commander Help files.

- Search – look for text strings in the evidence.
- Sorted Files Search – search for files by type, size, creation date, on hash data.
- Mount Image tools – mount disk images to your computer and use them as if they were a part of your operating system.
- Hashing tools – create and manage your file hash data. It also lets you create hash-based exclusion databases for files common to computers on your network.
- Bookmarks – Creates links to quickly find locations and files in the evidence.
- Case History – Displays a list of tasks and processes performed that relate to the case. Lists times with the events.
- Options wizard – change and save the default settings for P2 Commander.
- Graphical options – determine which panes display when you open P2 Commander. Also, resize and close panes when necessary.
- Files pane tabs. – navigate between multiple windows in P2 Commander and view the information contained in each.

There are many additional resources available through the primary help file for P2 Commander 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**