Mount Image Pro



V7 User Manual

Published: 14-Apr-25 at 09:58:29

Chapter Contents

Published: 14-Apr-25 at 09:58:28

Chapter 1 - Introduction 5

1.1 Introducing Mount Image Pro 6

Chapter 2 - Installation 9

2.1 System Requirements 10

2.2 Download 10

2.3 Installation 10

2.4 Uninstall Mount Image Pro 13

Chapter 3 - Purchase 15

3.1 Purchase 16

Chapter 4 - Activation 19

4.1 Activation 20

4.2 Software Key Activation 21

4.3 Dongle Activation 25

4.4 Network Activation 27

Chapter 5 – Quick Start 29

5.1 Quick Start 31

Chapter 6 – Mount Types 32

6.1 Mount Types – Summary 33

6.2 Disk 34

6.3 File System 36

Chapter 7 – Graphic User interface (GUI) 37

7.1 The Mount Image Pro GUI 39

7.2 GUI Mount 40

7.3 GUI Unmount 46

7.4 GUI View 46

7.5 GUI Options 46

Chapter 8 – Mount Non Windows File Systems 49

8.1 Mount MAC HFS/APFS 50

Chapter 9 – Mount DD Forensic-Images 53

9.1 Mount DD Forensic-Images 54

Chapter 10 - RAID 55

10.1 RAID - Introduction 56

10.2 Preparation 56

10.3 Mounting a RAID 57

Chapter 11 –Network Devices 61

11.1 Mount a Remote Network Device 63

Chapter 12 – Command Line Use 67

12.1 Windows Path Evnironment Variable 68

12.2 Command Line Functions 70

12.3 Software Developers Kit (SDK) 82

Chapter 13 - Legal 83

13.1 This User Guide 84

13.2 Copyright 84

13.3 License Agreement 84

13.4 Disclaimer 85

Appendix 1 - Technical Support 87

Appendix 2 – Mount Types 88

Appendix 2 - Write Blocking 89

Appendix 6 - Definitions 91

Appendix 4 - Index 97

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 1 - Introduction

In This Chapter

CHAPTER 1 - INTRODUCTION

1.1 Introducing Mount Image Pro 6

1.1.1 Program Uses 7

1.1.2 Supported Image Formats 7

1.1.3 Program Features 8

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

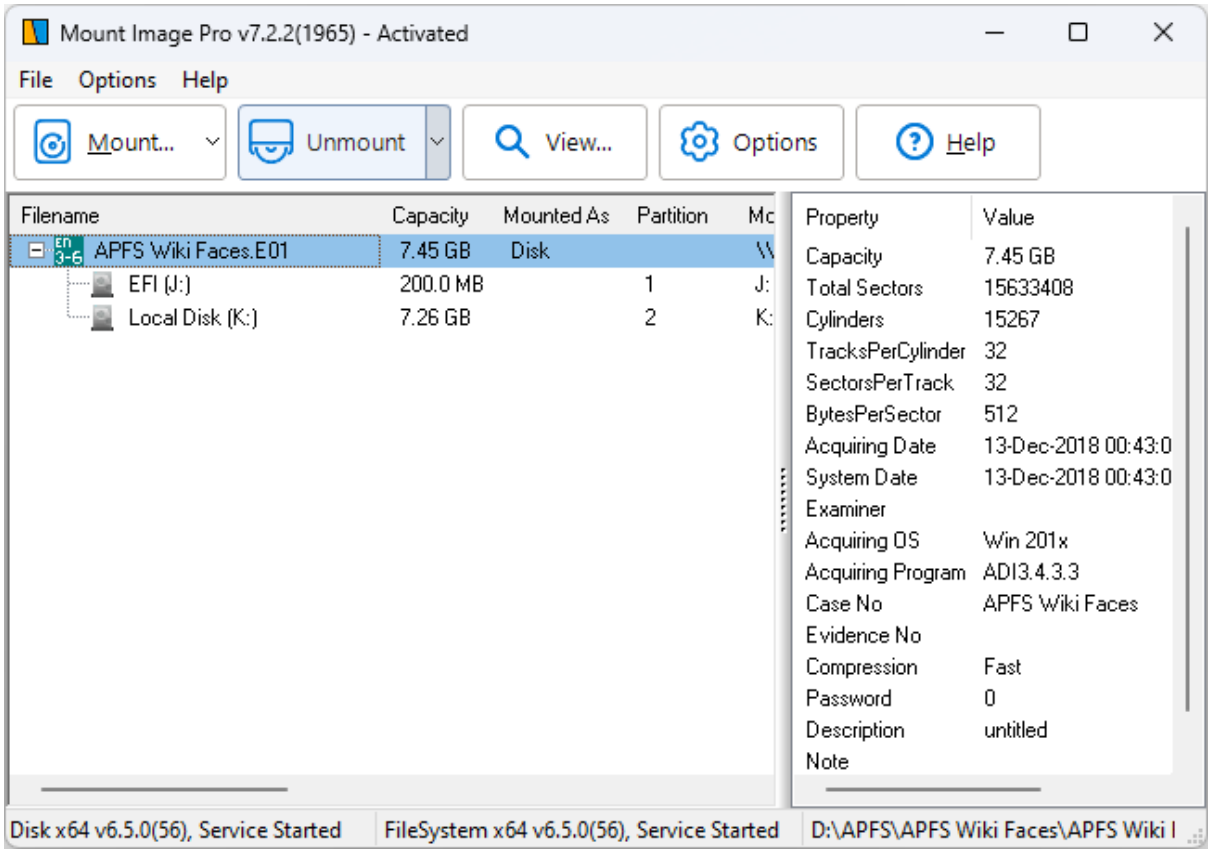
1.1 INTRODUCING MOUNT IMAGE PRO

Mount Image Pro is a utility used to mount forensic forensic-images or physical devices under Windows. A mounted drive can be then examined in a forensically sound environment.

Figure 1: Mount Image Pro v7



Figure 2: Mount Image Pro v7 GUI



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

PROGRAM USES

Mount Image Pro is primarily used by computer forensic examiners, investigators, and lawyers. It facilitates fast access to the contents of physical disks or forensic forensic-images in a read-only environment without the need for high end forensic software. Mount Image Pro is commonly used to:

- Quickly browse the contents of a mounted drive using familiar programs such as Windows Explorer;
- Run third party programs on mounted drives, including:
    - Virus scanners, spyware, Trojan and malware tools.
    - Stenography tools.
    - Keyword indexing tools.
    - Data recovery programs.
    - Other forensic programs that require disk access.

1.1.1 SUPPORTED IMAGE FORMATS

Mount Image Pro supports mounting of the following file formats:

- Access Data .AD1;
- Apple DMG;
- EnCase .E01, Ex01, .L01, Lx01;
- Forensic File Format .AFF;
- ISO (CD and DVD images);
- Microsoft VHD;
- NUIX MFS01;
- ProDiscover;
- SMART;
- Unix/Linux DD and RAW images;
- VMWare.
- Xways Container File.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

1.1.2 PROGRAM FEATURES

Mount Image Pro features include:

- Mount as read only or simulate disk writes.
- Mount the physical drives into Windows disk management.
- Mount from the command line.
- Mount Logical Evidence Files (LEF) created by EnCase® and FTK.
- Mounts NTFS, FAT, FAT16, FAT32 and HFS, APFS file systems.
- Is compatible with third party file system drives such as HPFS, Linux EXT2/3/4.
- Works with physical and logical images.
- Mount images via a network from a central server.
- Create DOS batch files to mount multiple images.
- Show or hide deleted files.
- Mount files without Windows security permissions.
- Mount RAID devices.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 2 – Installation

In This Chapter

CHAPTER 2 - INSTALLATION

2.1 System Requirements 10
2.2 Download 10
2.3 Installation 10
2.3.1 Silent Installation 13
2.3.2 Windows Autoplay Setting 13
2.4 Uninstall Mount Image Pro 13

2.1 SYSTEM REQUIREMENTS

Administrator: It is recommended to install and use Mount Image Pro as local administrator user (or at a minimum a user account with full administrator rights).

Windows UAC: It is recommended to use Mount Image Pro with Windows User Account Control (UAC) disabled (or at a minimum set to low).

Hardware/OS: Mount Image Pro requires the following minimum specification:

- Windows XP, 2003, Vista, Win 7, 2008, Win 8, 10, Server 2008-2016;
- Pentium IV 1.4 GHz or faster processor;
- 1GB RAM;
- 32bit and/or 64bit compatible.

Supports Third party file system drivers such as:

- MAC: http://www.paragon-software.com/home/hfs-windows/;
- EXT: http://www.paragon-software.com/home/extfs-windows-pro/.

2.2 DOWNLOAD

The latest version of Mount Image Pro is available for download at www.mountimage.com. The software requires activation with either:

- A 30 day evaluation software key;
- A purchased software key;
- A purchased USB activation dongle.

See Chapter 4 for more information.

2.3 INSTALLATION

Recommendations prior to installation:

- Close then exit any running instance of Mount Image Pro present in the Windows task bar;
- Uninstall previous versions.

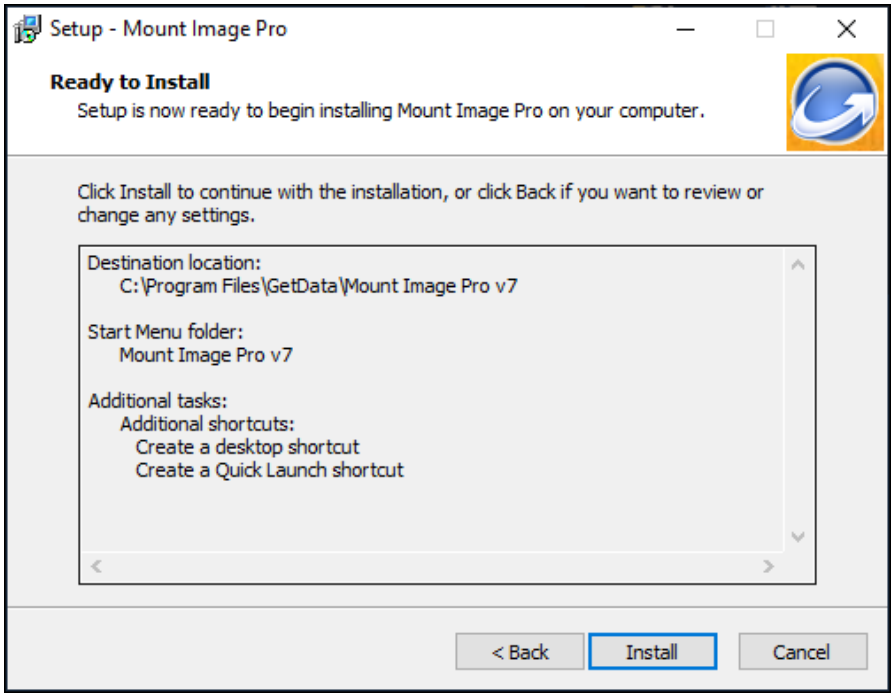
To **install Mount Image Pro**:

- It is recommended that Mount Image Pro be installed as Administrator user (or an account with administrator privileges) so that disk driver installation has the maximum privilege available.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

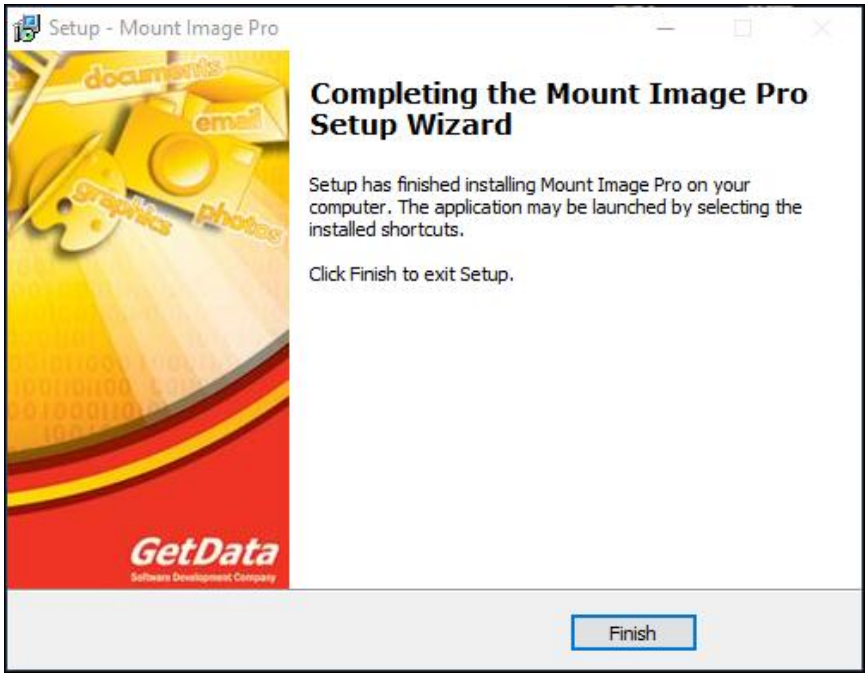
- Run the installation file **ForensicExplorer-Setup.exe** (or ForensicExplorer-Evaluation-Setup.exe if you are installing the 30 day evaluation version).
- Follow the setup instructions.

Figure 3: Mount Image Pro installation



1. Follow the setup instructions and confirm the setup summary by clicking the **Install** button;

Figure 4: Finalize installation



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

2. A successful install will display the following screen. Click **Finish** to confirm.

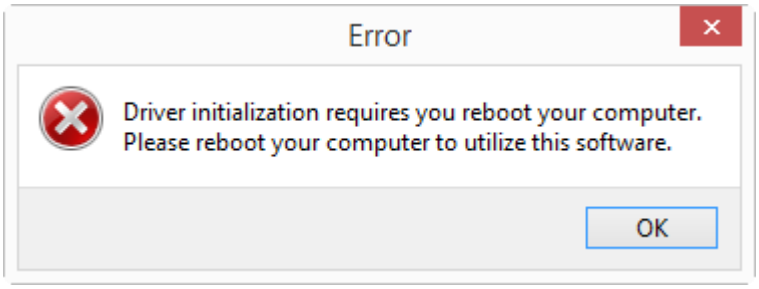
3. Run Mount Image Pro from the installed desktop icon:

Figure 5: Desktop icon



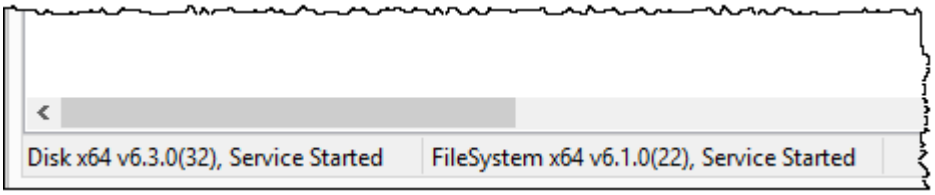
4. Mount Image Pro requires the installation of disk drivers. If prompted with the following message a system restart is required:

Figure 6: Disk driver initialization



Upon restart, check that the drives are installed correctly, as shown in xx below:

Figure 7: Mount Image Pro drivers



5. At the completion of the installation, confirm the drive status in the information bar at the bottom of the Mount Image Pro GUI. If the status **Disk Driver not installed**, use the Windows CMD to uninstall drivers, reboot and reinstall drivers (see CMD DriverInstall below).

6. If this message continues, check user privileges and/or security software that may be blocking driver installation and reinstall.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

2.3.1 SILENT INSTALLATION

Some third party vendors require silent Mount Image Pro installation (i.e. the GUI is not visible to the end user). To execute a silent installation, use the following Command Line options:

"C:\Downloads\MountImagePro-(v[X.X.X.XXX]).exe" /AUTOREG=XXXX-XXXX-XXXX /VERYSILENT

Where the path points to the setup file and XXXX-XXXX-XXXX is replaced by the product activation key. Ensure that:

1. Mount Image Pro is not already running on the user's computer;
2. Activations are available on the key.

2.3.2 OFFLINE INSTALLATION

When install MIP on an offline computer, use the /OFFLINE Command Line option (v7.2.2.1970 and above). This can assist in the automated deployment of Mount Image Pro so that it does not attempt an online update of Codemeter:

"C:\Downloads\MountImagePro-(v[X.X.X.XXX]).exe" /OFFLINE

2.3.3 WINDOWS AUTOPLAY SETTING

When a disk is mounted the **Windows Control Panel > AutoPlay** options determine whether Windows Explorer is automatically launched. This option can be turned off in the **Removable Drives** options by selecting **Take No Action**.

2.4 UNINSTALL MOUNT IMAGE PRO

To uninstall Mount Image Pro:

1. Unmount all drives.
2. If Mount Image Pro appears in the Windows Task bar, right click on the task bar icon and select Exit.
3. From Windows > Start > All Programs > Mount Image Pro select the uninstall option; or Use Control Panel > Uninstall; and follow the installation prompts.

Any remaining folders in the Program Files installation path can be removed manually.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 3 - Purchase

In This Chapter

CHAPTER 3 - PURCHASE

3.1 Purchase 16

3.1.1 Software Key v's Dongle Activation 16

3.1.2 Purchase Online 16

3.1.3 Purchase Orders 16

3.1.4 Resellers 16

3.1.5 Purchase Maintenance 17

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

3.1 PURCHASE

Mount Image Pro is available for purchase online, via purchase order, or via forensic software resellers.

3.1.1 SOFTWARE KEY V'S DONGLE ACTIVATION

Mount Image Pro is sold with a **software activation key** which is provided at the time of purchase. A software key is **hardware locked** to the computer on which it is used. A USB **activation dongle** can be added to the purchase. The dongle contains its own activation key and makes the license transportable from PC to PC. For more information on activation, see Chapter 4.

Forensic Explorer customers: Please note that if you purchase **Forensic Explorer** (www.forensicexplorer.com) you will receive a USB activation dongle that contains a key for **both Forensic Explorer** and **Mount Image Pro**.

3.1.2 PURCHASE ONLINE

Mount Image Pro can be purchased online at http://www.mountimage.com.

Forensic Explorer with Mount Image Pro can be purchased online at http://www.forensicexplorer.com.

3.1.3 PURCHASE ORDERS

Purchase Orders can be placed by Government and Corporate entities by contacting GetData head office:

GetData Pty Ltd
Suite 204, 13A Montgomery Street
Kogarah,
New South Wales, 2217
Australia
Ph: +61 2 82086053
Fax: +61 2 95881195
Email: sales@getdata.com

Or by secure post:

GetData Forensics Pty Ltd
P.O. Box 71
Engadine, New South Wales, 2233
Australia

Or via your forensic reseller.

3.1.4 RESELLERS

For a list of approved resellers, please contact GetData via: sales@getdata.com or via the contact details above.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

3.1.5 PURCHASE MAINTENANCE

A purchase of Mount Image Pro **includes 12 months maintenance** giving access to updates and support. The maintenance date is displayed on the Mount Image Pro splash screen:

Figure 8: Mount Image Pro splash screen



When the **maintenance has expired**, Mount Image Pro will continue to work, however you may only use the latest available version prior to the expiration of your maintenance period.

To purchase additional maintenance online:

1. Visit the following web page: www.mountimage.com;
2. Select the option to purchase maintenance renewal;
3. Complete the checkout process.

Mount Image Pro maintenance is sold in increments of 1 year.

To apply the maintenance update, follow the instructions in section 4.3.1.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 4 - Activation

In This Chapter

CHAPTER 4 - ACTIVATION

4.1 Activation 20

4.2 Software Key Activation 21

4.2.1 Online activation 21

4.2.2 Offline activation 22

4.2.3 Deactivate a computer 24

4.3 Dongle Activation 25

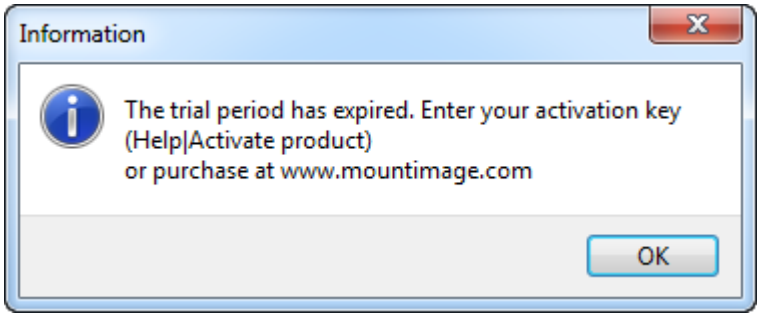
4.3.1 Dongle maintenance 25

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

4.1 ACTIVATION

Mount Image Pro uses the Wibu Codemeter software protection system. If Mount Image Pro has not been activated, the following message is displayed:

Figure 9: Running Mount Image Pro prior to activation



To activate Mount Image Pro either a **Software Key** (referred to by Wibu Codemeter as a 'Virtual Dongle') or a **USB hardware dongle** is required.

A **Software key** is hardware locked to the computer on which it is entered. A software key can only be moved to another computer if it is first deactivated (see 4.2.2 below).

A **USB hardware dongle** contains its own key. The dongle makes the key transportable from PC to PC. When the dongle is inserted, Mount Image Pro is activated. When the dongle is removed, Mount Image Pro returns to evaluation mode.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

4.2 SOFTWARE KEY ACTIVATION

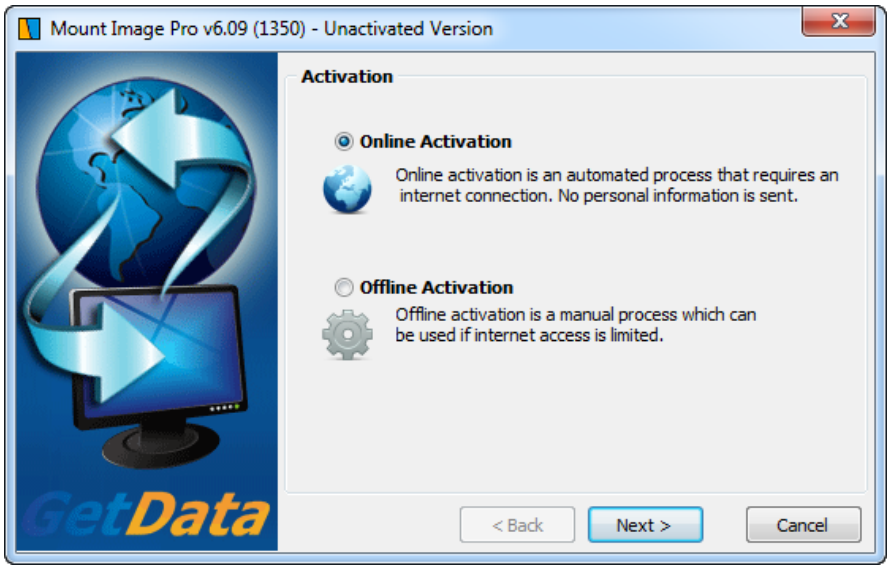
IMPORTANT: Install and activate Mount Image Pro as **Administrator** of the **local computer**. It is **NOT** sufficient to be **domain administrator**. Domain administrators should run the installation executable as the **local administrator** (right click > run as > input local administrator credentials).

To open the software activation window, select **Help > Activate product.**

Online activation:

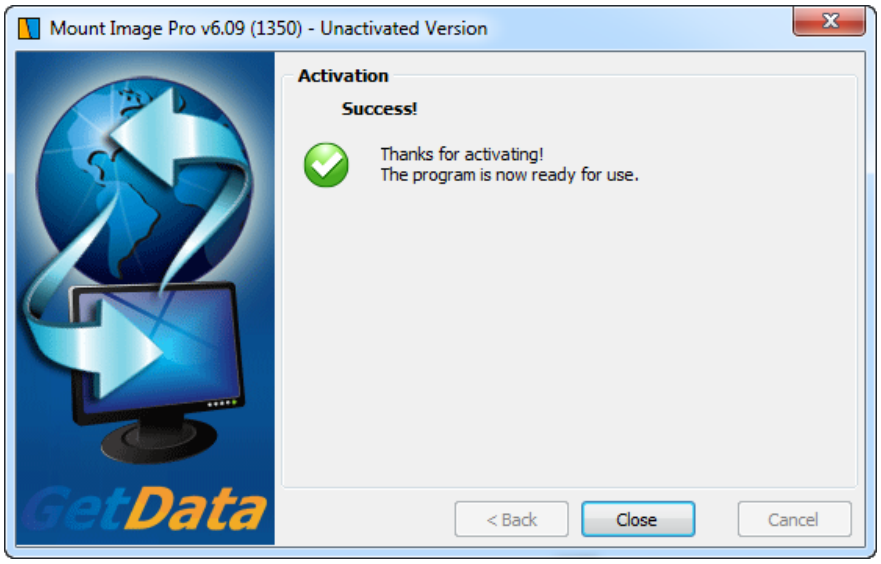
If the computer on which Mount Image Pro is to be activated is connected to the internet enter the sowftwae key into the field provided and click Next (as shown in Figure 10 below):

Figure 10: Online activation, 30 day trial version



A successful activation message will display the following screen, as shown in Figure 11 below:

Figure 11: Successful software key activation message



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

4.2.1 OFFLINE ACTIVATION

Where the computer on which the software is being installed is not connected to the internet, a separate internet connected computer can be used to activate. The activation process involves:

- Exporting a license file from the software;
- Uploading the license file, together with your purchase email address and license key at a web site (using any internet connected computer);
- Downloading the validated license file and importing it back into the software.

To activate an offline computer:

1. Click the Offline Activation button and click Next;

Figure 12: Activation wizard



2. Click on the Export button to export and save the license file "GetData.GDActRequest":

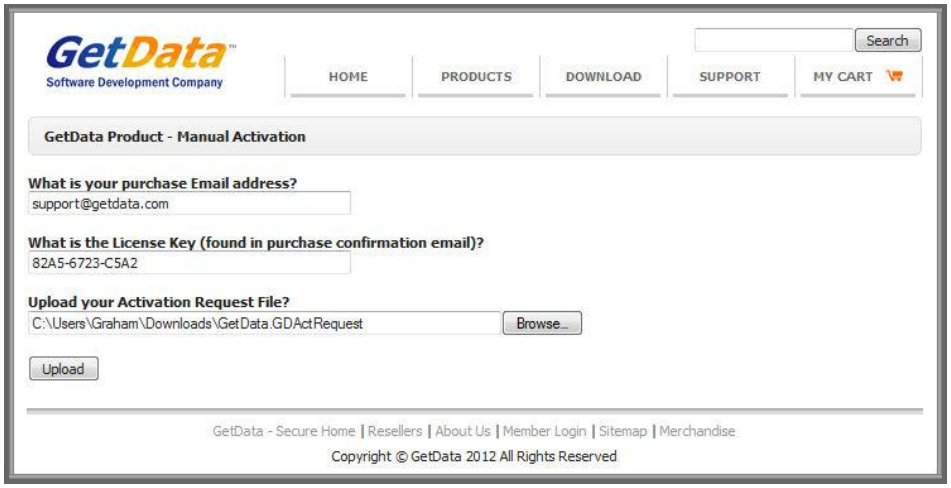
© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 13: Offline activation (evaluation version), export of license file



3. Using an web browser on any internet connected computer, go to http://getdata.com/offline and enter the required details:

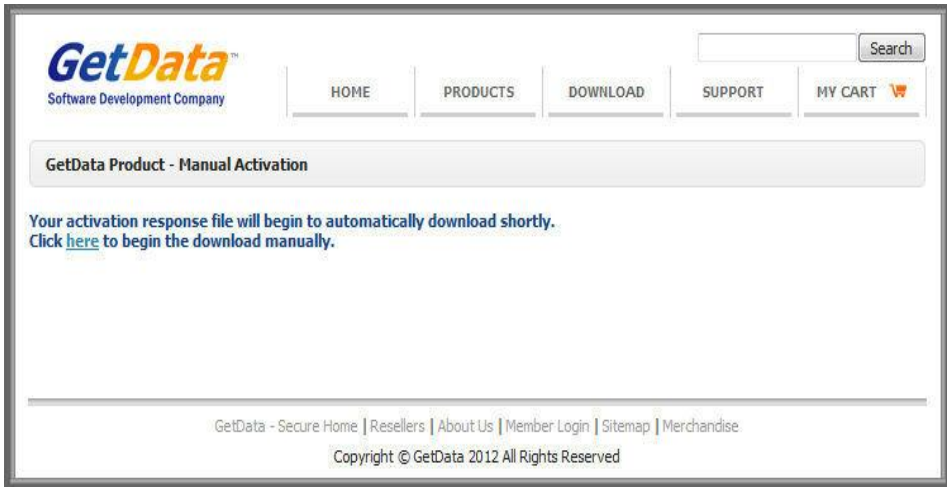
Figure 14: Offline activation (evaluation version), upload of license file and activation details



4. Click the Upload button to send the details to the activation server. The details are validated by the activation server and the file "GetData.GDActResponse" is returned to you.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 15: Offline activation (evaluation version), download of license file



5. Save "GetData.GDActResponse" and take it back to the offline computer on which you will be activating the software.

6. Once the "GetData.GDActResponse" file is back on the offline computer, click the Import button to import the file into the software. The software is now activated.

4.2.2 DEACTIVATE A COMPUTER

To remove a software activation key from a computer:

1. An Internet connection is required;

2. Download and run the GetData License Manager from http://download.getdata.com/support/LicenseManager.exe;

3. In the left hand column of the License Manager click on the "GetData Virtual CmStick";

4. Under the Product list you should see an entry for Mount Image Pro. Click on it to highlight it;

5. Press the "Delete" button. A confirmation message will appear "The LicenseManager is now going to communicate with GetData License servers to update your dongle(s)". Click OK to proceed.

   The "Debug Log" tab will report the status. A successful removal is identified by "Update Success!". When you return to the "Dongles" tab, Mount Image Pro should no longer appear.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

4.3 DONGLE ACTIVATION

Mount Image Pro is activated using a **Wibu Codemeter USB hardware dongle** which is delivered to your by courier following your purchase (see Chapter 3 - Purchase, for more information on purchasing Mount Image Pro).

The dongle contains its own activation key. The dongle makes the license transportable from PC to PC. When the dongle is inserted, Mount Image Pro is activated. When it is removed, Mount Image Pro returns to evaluation mode.

The dongle has a unique identification number inscribed on the part of the dongle that is inserted into the USB port, as shown in Figure 16 below. Include this number in correspondence with GetData:

Figure 16: Unique Wibu Codemeter dongle identification number



The Wibu Codemeter dongle is **driverless** and requires no special installation.

4.3.1 DONGLE MAINTENANCE

Once a maintenance update has been purchased, to update maintenance on your Wibu Codemeter dongle:

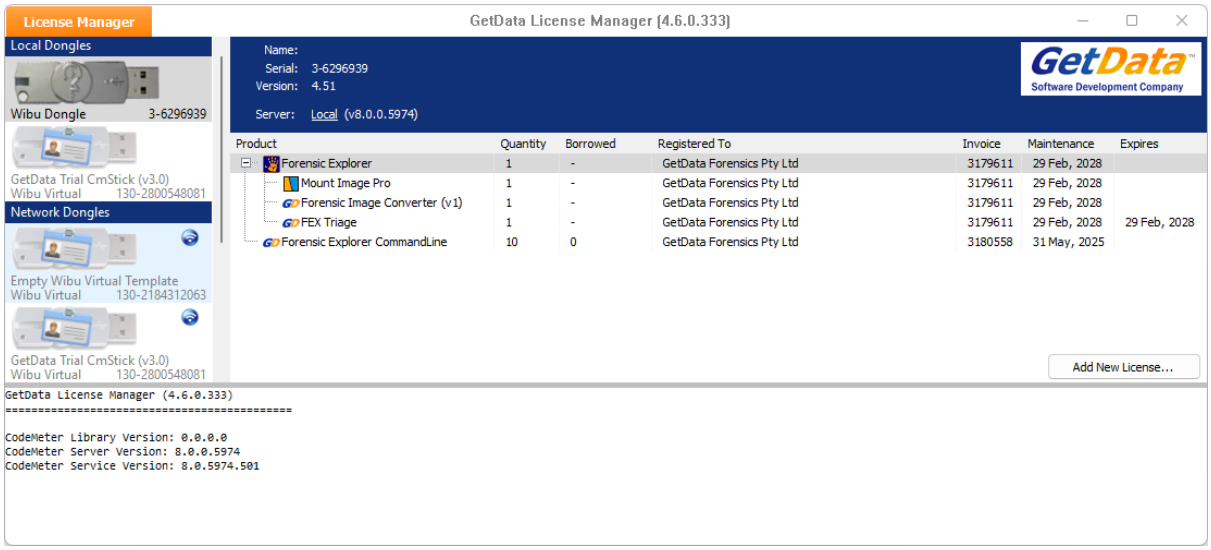
1. On a computer which has **internet access**, **insert your Wibu Codemeter dongle** into a USB port. Remove any other Wibu Codemeter dongles that you may have for other products.

2. Run the **GetData License Manager** located in the installation folder of Mount Image Pro. The default location is: **C:\Program Files\GetData\Mount Image Pro vx\License Manager.exe**

3. The GetData License Manager will **detect your Wibu Codemeter dongle**, as shown in Figure 17 below. The existing Maintenance expiration date is displayed in the Maintenance column:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 17: GetData License Manager



4. **Select "Mount Image Pro"** from the product list and press the **ADD button**.

5. In the **Add Licenses** window, enter the "**License**" key that you received with your renewal order. Press the **Search** key.

6. Select the renewal from the available product list. Then click the **Apply** button.

7. Return to the main screen of the License Manager. Click the refresh button to display the new maintenance date.

For further assistance in applying maintenance updates to your Mount Image Pro dongle, please contact support@getdata.com (see Appendix 1 - Technical Support for full contact details).

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

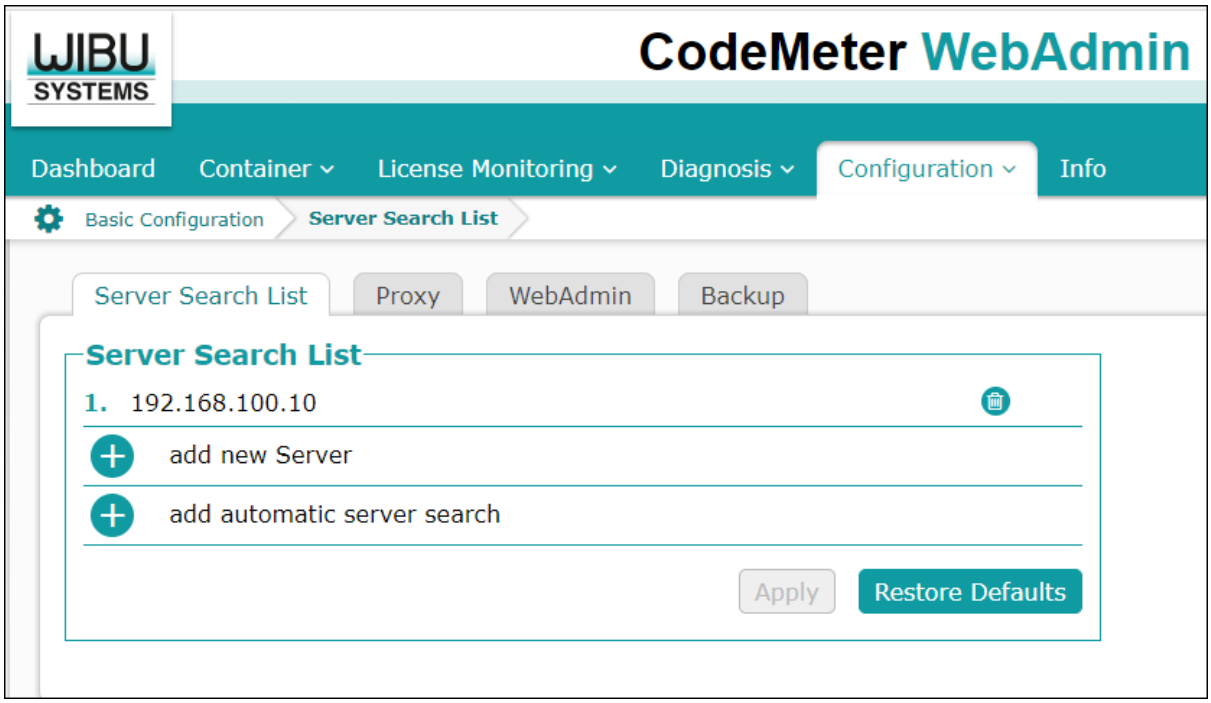
4.4 NETWORK ACTIVATION

The Wibu Codemeter activation system enables you to use your local dongle to activate a remote internet connected computer:

On the **local computer** with the Codemeter dongle is inserted run the **Network Server**:

1. Download the latest **Codemeter Runtime for Windows User** from http://www.wibu.com/downloads-user-software.html
2. Run **CodeMeter WebAdmin** by browsing to http://localhost:22350/ConfigServer.html.
3. Select **Configuration > Server** from the menu, as shown in Figure 18 below:

Figure 18: CodeMeter WebAdmin



4. In the **Sever** window heck **Run Network Server** and press the **Apply** button.
5. Ensure that the selected **Network Port** 22350 is not blocked by your firewall.
6. Restart the CodeMeter Service.
    a. Run the **CodeMeter Control Center** by clicking the CodeMeter icon in the Windows Task tray;
    b. Select **Processes > Stop CodeMeter Service**;
    c. Then **Start CodeMeter Service**.

    The Wibu CodeMeter Network Server can also be configured using the following registry setting:

    HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion
    IsNetworkServer=1

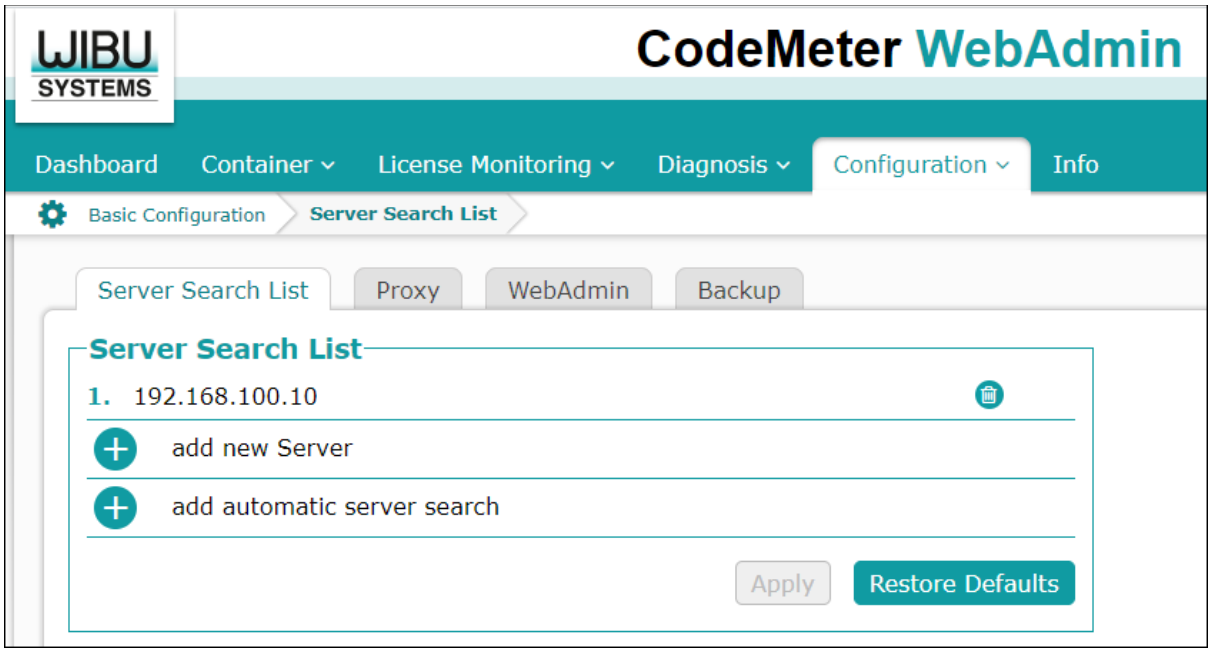
On the **client computer**:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

7. Install Mount Image Pro.

8. Browse to http://localhost:22350/Configuration.html:

Figure 19: Wibu CodeMeter Local Host Configuration



9. Click the **add** button and add the IP address of **Network Server** and press **Apply**.

10. Start Mount Image Pro. It should detect the remote dongle license and activate.

    The client computer can also be configured using the following registry key setting:

HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion\ServerSearchList\Server1
Address=192.168.100.10

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 5 – Quick Start

In This Chapter

CHAPTER 5 – QUICK START

5.1 Quick Start 31

5.1.1 IMPORTANT – Before you begin 31

5.1.2 Quick Start GUI Mount 31

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

5.1 QUICK START

5.1.1 IMPORTANT – BEFORE YOU BEGIN

Write Protect Physical Devices:

An accepted principal of computer forensics is that wherever possible source data to be analyzed in an investigation should not be altered by the investigator. If physical media such as a hard drive, USB drive, camera card etc. is a potential source of evidence, it is recommended that when the media is connected to a forensics workstation it is done so using a write block device. See Appendix 2 - Write Blocking for more information.

Virus & Malware

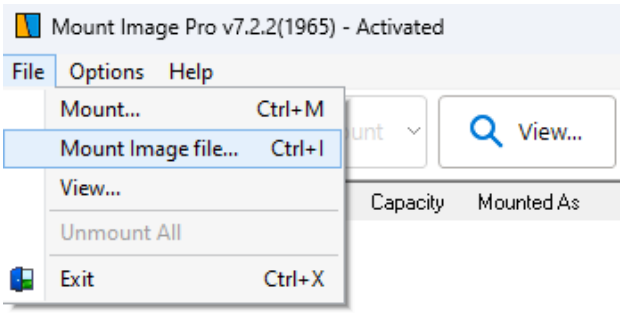
An investigator should be aware of the inherent risks of mounting third party data to a forensic workstation. Appropriate virus and malware protection should be used at all times.

5.1.2 QUICK START GUI MOUNT

To **mount** a forensic-image from the GUI:

1. **Install** Mount Image Pro (see Chapter 2);
2. **Activate** Mount Image Pro (see Chapter 4);
3. To mount an image:
    a. In the top text menu of the GUI, select **File > Mount Image File**, and navigate to and open the required image:

Figure 20: Mount Image file...



Or;

    b. In the button toolbar, click **Mount** > **Add Image**, then navigate to and open the required image. The image will then be added to the **Device Selection** window. Once added, click the **Mount** button.

4. In the **Mount** window, select to mount as a **Disk** or **File System** (described in more detail in Chapter 6). Select the required options and click **OK** to mount.
5. The image will then mount on the Windows File System and will be accessible via Windows Explorer

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 6 – Mount Types

In This Chapter

CHAPTER 6 – MOUNT TYPES

6.1 Mount Types – Summary 33

6.2 Disk 34

6.2.1 Disk - Compatible Forensic-Image types 34

6.2.2 Disk - Recommendations 34

6.2.3 BitLocker Drives 34

6.3 File System 36

6.3.1 File System - Compatible Forensic-image types 36

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

6.1 MOUNT TYPES – SUMMARY

Mount Image Pro offers different mount methods:

- Disk (with our without Plug and Play);
- File System.

The following table provides a summary of the differences between these mount types:

Mount	Disk	File System
Existing Windows security settings apply	Yes	No
26 forensic-image limit (available drive letters)	Yes (No if MIPDisk Folder is used)	No
Access entire physical drive with 3rd party tools	Yes	No
Disk is shown in Windows Disk Management (* with PNP option)	Yes	No
Display deleted files	No	Yes
Display unallocated clusters as a file	No	Yes
Display Windows system files (MFT, FAT, VBR etc.)	No	Yes

More information about each mount type is provided below.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

6.2 DISK

Disk is used to mount a forensic-image and display the physical disk and / or partitions as if the physical drive were connected to the local computer.

Disk with **Plug-and-Play** emulates the connection of a physical USB disk to the computer and adds the disk into **Windows Disk Management**. Plug-and-Play is used when the investigator needs access to the physical disk or partitions as a Windows managed drive.

6.2.1 DISK - COMPATIBLE FORENSIC-IMAGE TYPES

The Disk option can be used with the following forensic-images and devices:

Disk	
Forensic-image of physical disk	Yes
Forensic-image of logical disk	Yes
Physical device (e.g. connected HDD)	Yes
Logical forensic-Image File (.AD1, .L01)	No

6.2.2 DISK - RECOMMENDATIONS

When using the Disk option existing Windows security permissions inside the forensic-image are applied in the mount. Care must be taken to ensure access to all required data. It is recommended that:

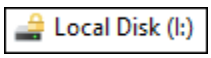
- **Administrator** access is used to examine a mounted image to ensure that maximum file security privileges are available;
- Be aware that Windows will apply its **exiting security schema** to the mounted image;
- Be aware of other Windows features such as **Symbolic Links** which may affect the way data is displayed.

6.2.3 BITLOCKER DRIVES

Mount Image Pro v7 supports the mounting of **BitLocker** encrypted partitions. BitLocker is a full disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes.

To mount a BitLocker drive, follow the Mount Disk instructions. The BitLocker partition will mount under Microsoft Windows and display the following folder icon:

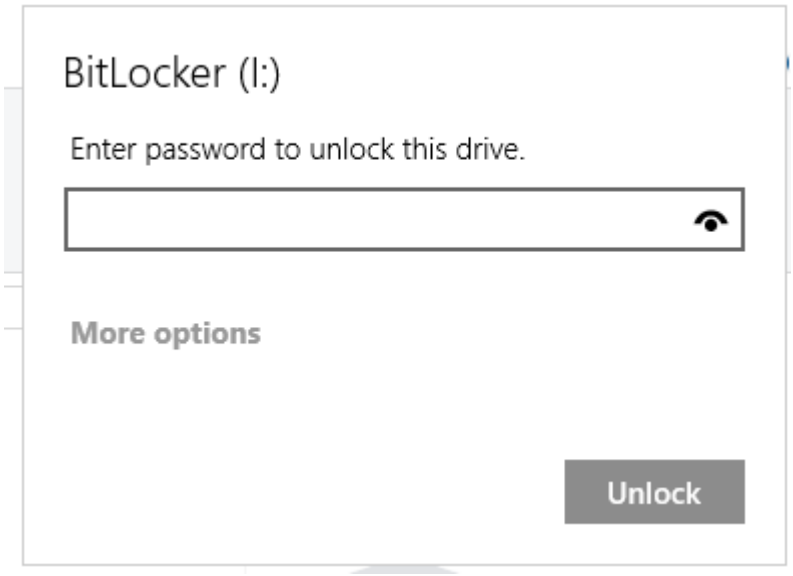
Figure 21, Window BitLocker drive icon



When clicking on a BitLocker encrypted drive in Windows the following window should appear:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 22, BitLocker password window



You **must have** either the **BitLocker password** or a **BitLocker Recovery Key** to be able to access a BitLocker protected partition (see https://support.microsoft.com/en-au/help/17133/windows-8-bitlocker-recovery-keys-frequently-asked-questions for more information) .

Enter the **BitLocker password** or **BitLocker recovery key** to display the contents of the drive.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

6.3 FILE SYSTEM

File System uses the Mount Image Pro file-system driver to mount and display the contents of the forensic-image. As Mount Image Pro has control, there is greater flexibility as to the way in which the contents of the forensic-image is displayed.

The File System option is used to:

- Over-ride Windows security permissions;
- Mount File Systems that Windows does not recognize, e.g. APFS;
- Override Windows folder management (symbolic links, hard links etc.);
- Group multiple mounted image files under the one folder;
- Control whether to display Windows system files;
- Control whether to display deleted files.

NOTE: File Systems are mounted as read only (i.e. it is not possible to delete items from the mounted Windows File System).

6.3.1 FILE SYSTEM - COMPATIBLE FORENSIC-IMAGE TYPES

The Mount Disk option can be used with the following forensic-images and devices:

File System	
Forensic-image of physical disk	Yes
Forensic-image of logical disk	Yes
Physical device (e.g. connected HDD)	Yes
Logical forensic-Image File (.ad1, .l01)	Yes

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 7 - GUI

In This Chapter

CHAPTER 7 – GRAPHIC USER INTERFACE (GUI)

7.1 The Mount Image Pro GUI 39

7.2 GUI Mount 40

7.2.1 Device Selection Window 40

7.2.2 Mount Options 41

7.2.3 Mounted Images and Devices 45

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

7.1 THE MOUNT IMAGE PRO GUI

Important: It is recommended that Mount Image Pro be run as **administrator** to be certain that permissions enable access to physical devices and image files.

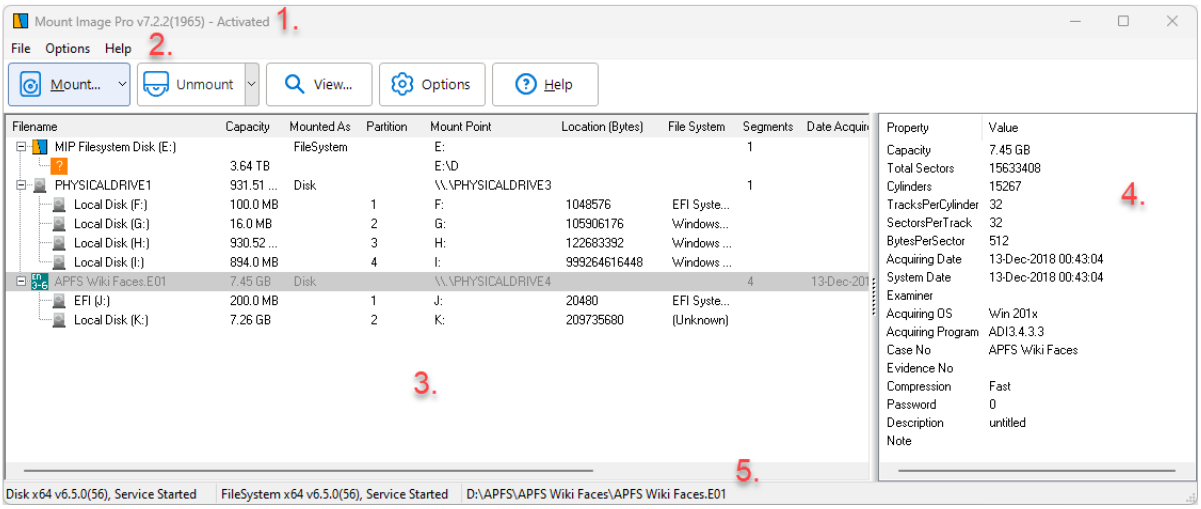
For most users, the mounting and un-mounting of forensic-images or devices will take place in the Mount Image Pro GUI (Graphic User Interface).

To o**pen the Mount Image Pro GUI**:

- Run Mount Image Pro Windows Start menu; or
- Double click on the desktop icon; or
- If Mount Image pro is already running, double click on the MIP icon in the Windows Task Bar.

The Mount Image Pro GUI is divided into 5 sections shown in Figure 23 below:

Figure 23: Mount Image Pro GUI showing mounted images



1. **Title Bar**:
   Shows the Mount Image Pro version number and activation status.

2. **Text Menu**:
   Gives text menu access to program options, including: Mount; Unmount and Exit.

3. **Main Window**:
   Lists the currently mounted forensic images or devices.

4. **Property Window**:
   Lists the properties for the currently selected forensic-image in the Main Window;

5. **Status Bar**:
   Provides the status of the Mount Image Pro Disk and File System drivers. Provides the path to the currently selected forensic-image in the Main Window.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

7.2 GUI MOUNT

To **mount a forensic-image** using the GUI:

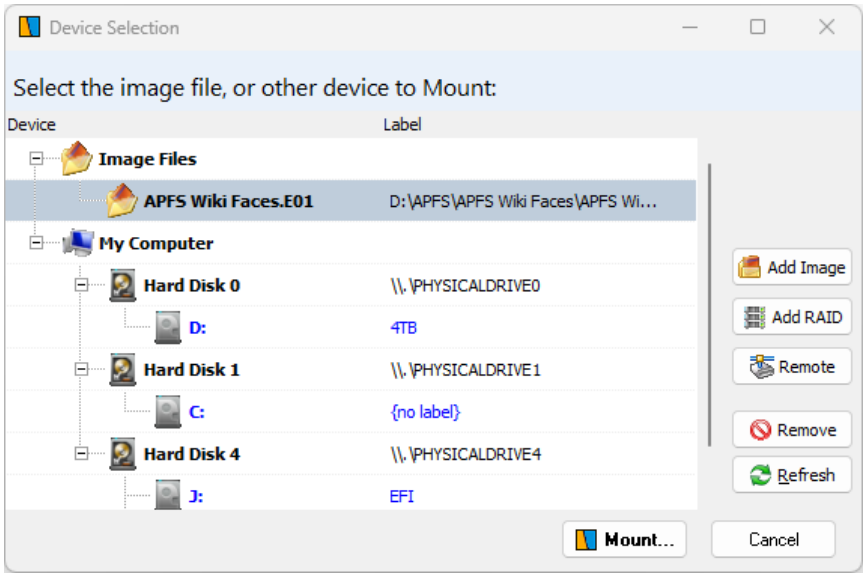
1. From the top text menu, select **File > Mount Image File**, browse to and select the required image, then proceed to 7.2.2 below;
2. **Or**, use the Device Selection window, described in xx below.

7.2.1 DEVICE SELECTION WINDOW

The Device Selection window is used to give access to:

- Local physical devices; or,
- Forensic-image files that have been previously added to the list.

Figure 24: Mount Image Pro Device Selection window



TO SELECT A DEVICE TO MOUNT

To **mount a local device**;

1. In the Device Selection window (shown in Figure 24 above), expand **My Computer** using the plus icon and select the required Hard Disk or logical drive letter and click the **Mount** button.

TO ADD A FORENSIC-IMAGE TO MOUNT

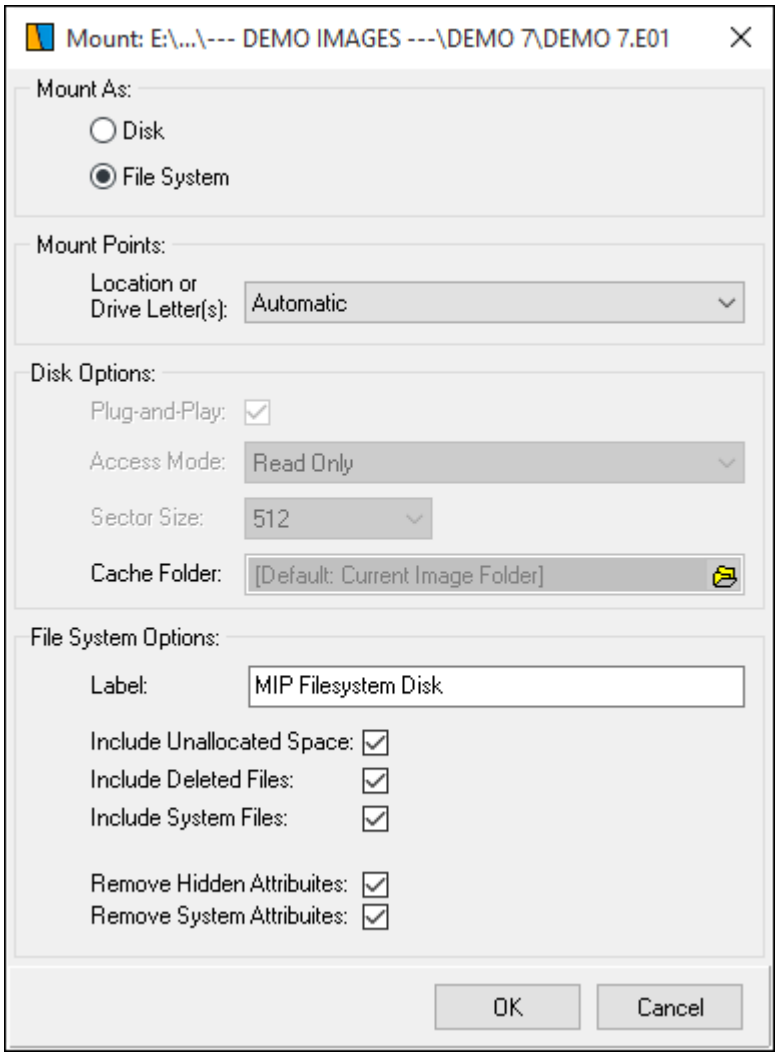
1. In the Device Selection window click on the **Add Image** button;
2. Browse to the required image and select Open. The forensic-image is then added to and becomes available in the Device Selection window. Once added, the forensic-image will remain in the Device Selection window for quick reference until it is removed.
3. Select the required image and click the **Mount** button.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

7.2.2 MOUNT OPTIONS

The **Mount** window is then displayed which gives a choice of mount type, **Disk** or **File System** and configuration options.

Figure 25: Mount options window



Location or Drive Letters:

Automatic:

Mount Image Pro will select the next available drive letter to commence mounting partitions.

Select a drive letter:

The user selects the drive letter of the mount. If multiple partitions are to be mounted, the selected drive letter is the starting drive.

Additional Location or Drive Letter options are detailed below that are specific to Disk or File System mounts.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

DISK OPTIONS

Disk is used to mount a forensic-image and display the physical disk and/or partitions as if the physical disk was connected to the local computer. (See – Mount Types, Chapter 6 for more information on the difference between a Disk and a File System mount).

The following Disk configuration options are provided:

Location or Drive Letters (options specific to Disk):

None (Physical Only)

A drive letter will not be allocated. The physical disk only will be mounted. Use this option if a third party tool need only access the physical disk.

MIPDISK Folder (non-plug-and-play)

The disk will be mounted into a folder on the existing file system. The folder path is specified in the registry key:

Computer\HKEY_CURRENT_user\Software\GetData\Mount Image Pro v7\Configuration

Access Mode

When using the Disk option (a partition within the image), it is possible to set the “Access Mode" to either:

Read Only:

The partition is mounted as a read only drive where no changes to the mounted drive letter are possible. For example, if a user attempts to deleted a file on a mounted drive letter the Windows operating system will return a message the at the drive is read only;

Write to Null:

All disk writes are dropped. Windows caches changes made to the mounted drive. For example, if a user deletes a file in the mounted image, the file is deleted from the mounted drive. Note that it is NOT possible to change the content of the image file. When the image is remounted, all files will be re-displayed.

Write to Cache:

See **Cache Folder** below.

Sector Size

The sector size of the image can be adjusted for certain image types, e.g. DD, ISO.

Plug-and-Play

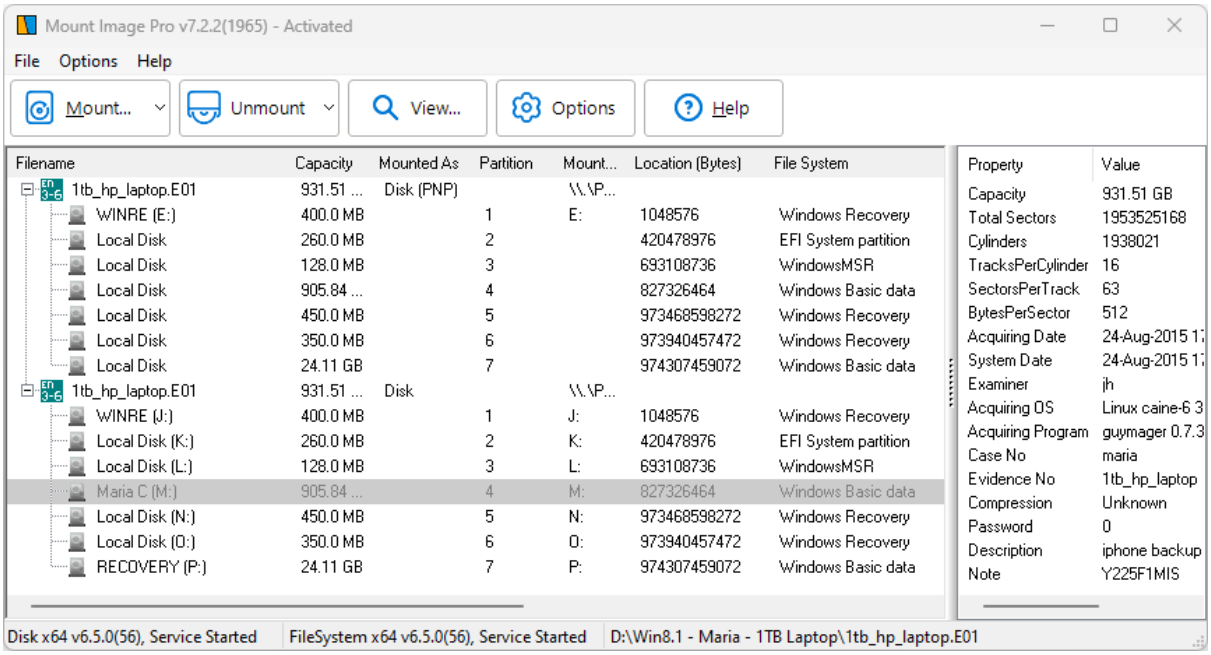
Plug-and-Play emulates the connection of a physical USB disk to the computer. Windows is responsible for the management of the mounted image. One advantage is that the disk is added to **Windows Disk Management** giving the investigator access to the physical disk at a system level.

Important considerations when using Plug-and-Play

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Display of hidden and system partitions:

When Plug-and-Play is used Windows may not display hidden or system partitions. In the example below the forensic-image **1tb_hp_laptop.E01** of a Windows 8 computer is first mounted using Plug-and-Play and then mounted again without:



The Plug-and-Play mount allocates E:\ drive to data partition. Additional Windows Recovery and system partitions are shown in the GUI but are not allocated drive letters. The Non-Plug-and-Play mount allocates M:\ drive to data partition and also allocates J:, K:, L:, N:, O:, P:, to the Windows Recovery and system partitions.

Disk Signature Collisions

A disk signature is a “four-byte identifier offset 0x1B8 in a disk’s Master Boot Record, which is written to the first sector of a disk. Windows uses disk signatures internally to map objects like volumes to their underlying disks and starting with Windows Vista, Windows uses disk signatures in its Boot Configuration Database (BCD), which is where it stores the information the boot process uses to find boot files and settings” (1)

A Disk Signature Collision means that Mount Image Pro will not PNP mount the same disk twice. “Windows requires the signatures to be unique, so when you attach a disk that has a signature equal to one already attached, Windows keeps the disk in “offline” mode and doesn’t read its partition table or mount its volumes”. The solution described detail in Mark Russinovich’s Blog (http://blogs.technet.com/b/markrussinovich/archive/2011/11/08/3463572.aspx) is to use Windows Disk Management’s online menu option to generate a new random disk signature (note that the image cannot be mounted read-only for this method to be used).

Cache Folder

The cache folder holds the location of the cache file. The default cache folder is the same path as the current image file. The cache path can be modified. The current value is stored in the registry key:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Computer\HKEY_CURRENT_USER\Software\GetData\Mount Image Pro v7\Configuration\DefaultCacheDir

A cache file is created when the **Access Mode > Write to Cache** menu option is selected. The **cache file** is named **[Image Name].gdcache**. A cache file stores any writes to the mounted Disk so that the mounted disk operates as an autonomous Read/Write disk. Any changes to the disk (e.g. file deletes) will be maintained in the cache file.

IMPORTANT: If a disk is remounted and has an existing cache file from a previous mount, the new mount will reflect the changes made in the previous mount. To reset the disk to its original state, unmount the image, delete the cache file, and mount again.

FILE SYSTEM OPTIONS

File System: uses Mount Image Pro's own driver to display the content of the forensic-image. File Systems are always mounted as read only. (See – Mount Types, Chapter 6 for more information on the difference between a Disk and a File System mount).

Location or Drive Letters (options specific to Disk):

The user selects the drive letter of the mount. If a previous File System has been mounted, the user can select an **Existing** drive and mount additional File Systems to it. Using this technique, a Filesystem mount is not limited by the number of drive letters available on the forensic workstation.

Label

This option sets the Windows label for the mounted disk. The default label is "MIP File System Disk".

Include Unallocated Files

This option controls whether unallocated space is added to the mounted image. If checked, unallocated space is added as files, including a file for:

- Unallocated clusters
- Lost OS clusters

Include Deleted Files

This option controls whether deleted files are added to the mounted image (Deleted files are those that have a valid file system record, e.g. a MFT record, that marks the file as deleted). Deleted files are shown in the mounted image in Windows Explorer with **"[Deleted]**" appended to the file name.

Show System Files

This option controls whether system files are included in the mounted image. System Files include:

- Orphaned: Orphans are deleted folders and files for which the original parent folder is unknown.
- NTFS Volume Boot Record.

Remove Hidden Attributes (Recommended)

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Checking this option removes the Windows hidden attribute from mounted files so that they are visible under Windows.

Remove System Attributes (Recommended)

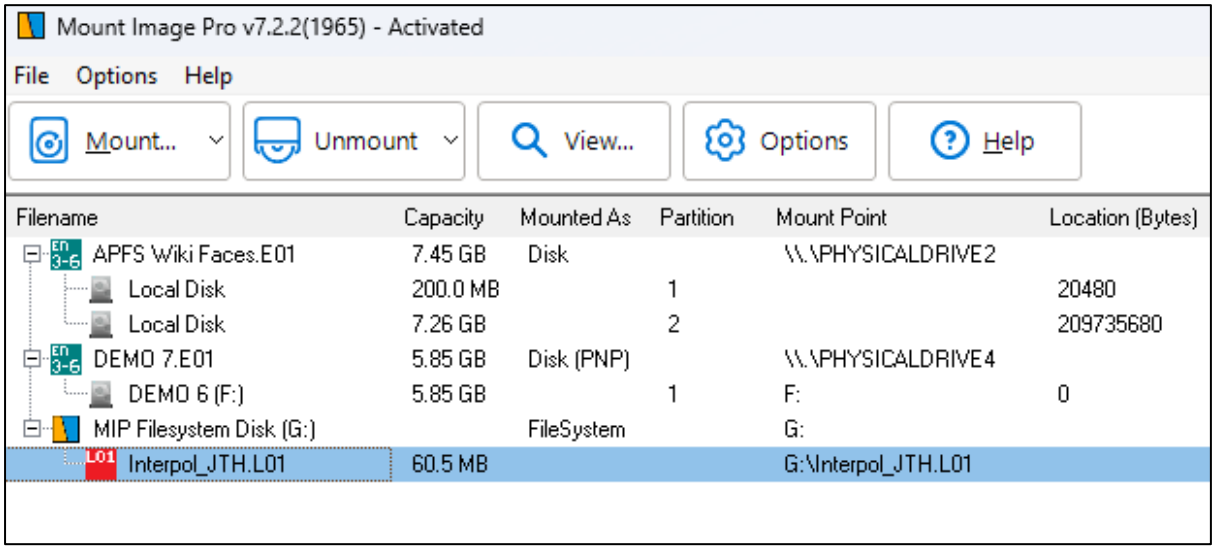
Checking this option removes the Windows system attribute from mounted files so that they are visible under Windows.

Click **OK** to mount the image or device.

7.2.3 MOUNTED IMAGES AND DEVICES

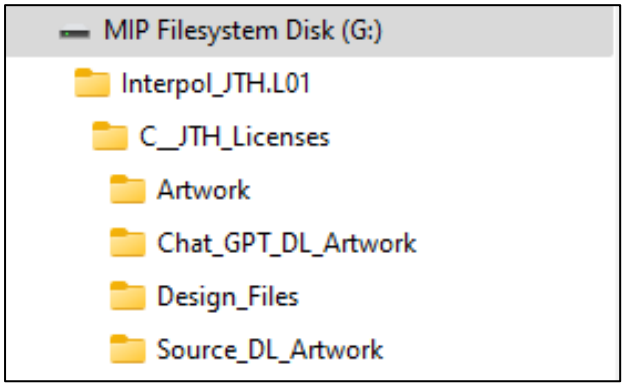
Mounted devices or images are then displayed in the Mount Image Pro GUI Main Window, as shown in Figure 26 below:

Figure 26: Mount Image Pro GUI showing 3 mounted image files



The mounted drives will now be available on the local File System. Right click on the image and select **Explore** from the menu to quickly access the image contents in Windows Explorer.

Figure 27: Windows Explorer showing the 3 mounted image files listed in Figure 26 above



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

7.3 GUI UNMOUNT

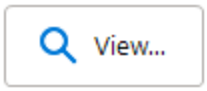
To unmount from the GUI:

- Right click on the device or image and select **Unmount** or **Unmount All** from the drop down menu; or;
- Click the **Unmount** icon and select **Unmount** or **Unmount All** from the drop down menu.

When Mount Image Pro is exited, all existing mounts are unmounted.

7.4 GUI VIEW

The **View** button in the toolbar enables the addition of the device or image to the Mount Image Pro GUI without mounting the image. This option is used to view the properties of the device or image in the GUI.



Use **unmount** to remove a viewed image from the GUI.

7.5 GUI OPTIONS

To set GUI options, click on the **Options** button in the toolbar:

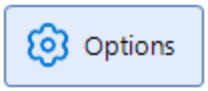
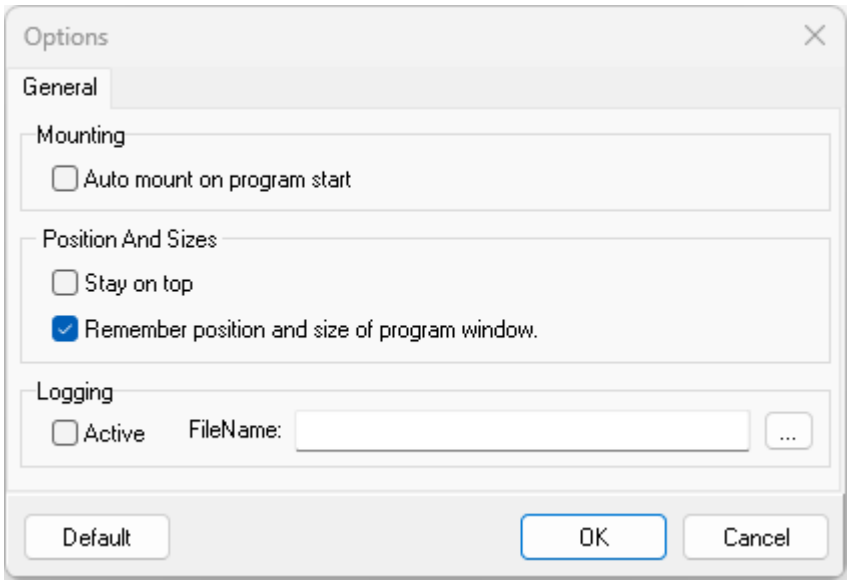


Figure 28: Mount Image Pro Options window



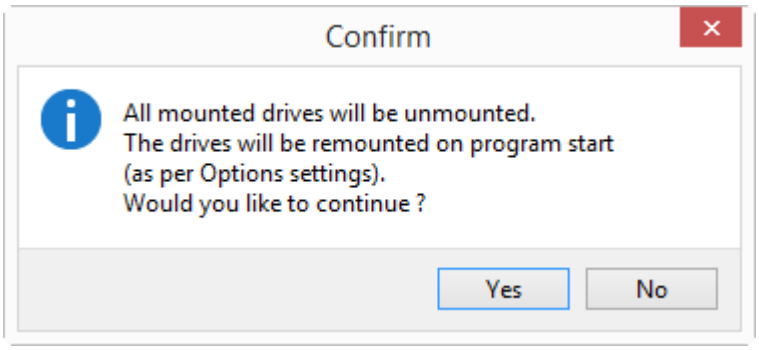
Auto mount on program start:

When this option is selected Mount Image Pro will attempt to remount the currently mounted devices or images when Mount Image Pro is next started.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

The following Mount Image Pro exit confirmation message is displayed when this option is active:

Figure 29: Exit confirmation message - Mount on start



Stay on top:

This option forces the Mount Image Pro GUI to stay at the top of all other onscreen windows.

Remember position and size of program window:

Preserves the current size and position of the GUI for next launch.

Logging:

Generates a log to the specified file.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 8 – Non Windows Images

In This Chapter

CHAPTER 8 – MOUNT NON WINDOWS FILE SYSTEMS

8.1 Mount MAC HFS/APFS 50

8.1.1 MAC – file system - using MIP driver 50

8.1.2 MAC - DisK – Third party FIle System Driver 50

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

8.1 MOUNT MAC HFS/APFS

Two different methods are used to mount a MAC drive on a Windows computer:

1. **File System** using the Mount Image Pro HFS driver (recommended);
2. **Disk** with a third party file system driver installed on the forensic workstation.

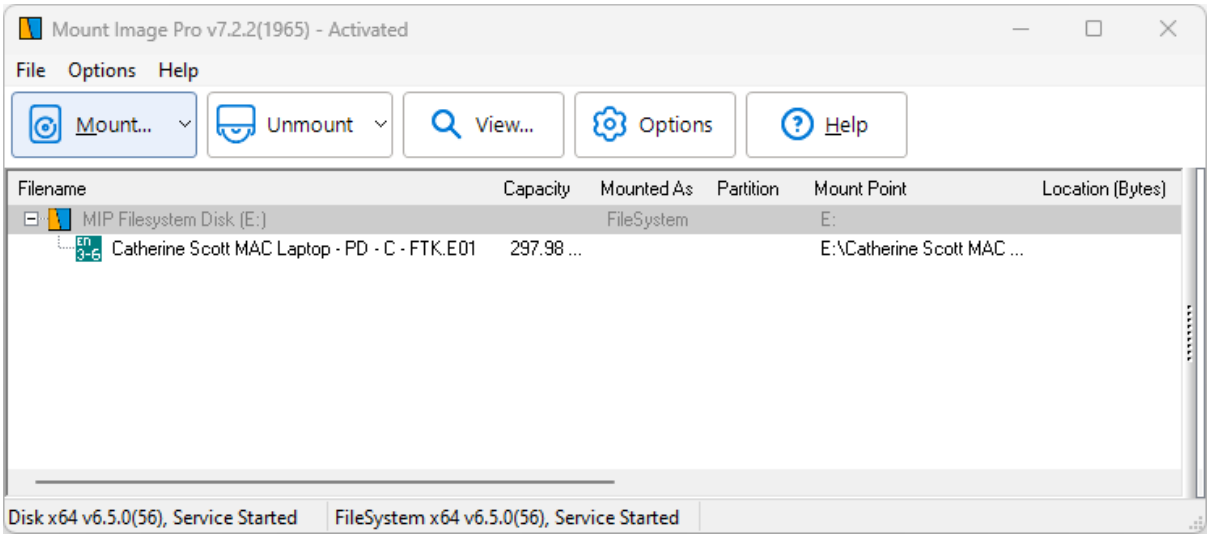
More information is provided below.

8.1.1 MAC – FILE SYSTEM - USING MIP DRIVER

To mount using the **Mount Image Pro MAC HFS file system driver**:

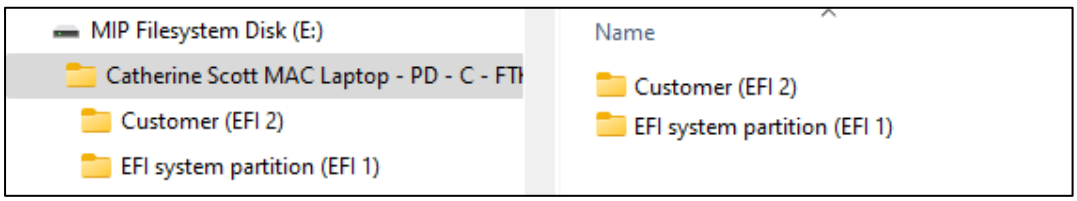
1. Follow the mount instructions in section 7.2 above. In the mount Options window select **File System**;
2. The MAC partitions will be available under the **MIP Filesystem Disk**, as shown in Figure 30 below:

Figure 30: Mount File System for a MAC HFS drive



View the MAC files in Windows Explorer:

Figure 31: Windows Explorer showing a MAC drive mounted as a File System



8.1.2 MAC - DISK – THIRD PARTY FILE SYSTEM DRIVER

If third party MAC file system driver is used, the **EXTFS Windows Pro** driver from **Paragon Software** is recommended (http://www.paragon-software.com/home/hfs-windows/).

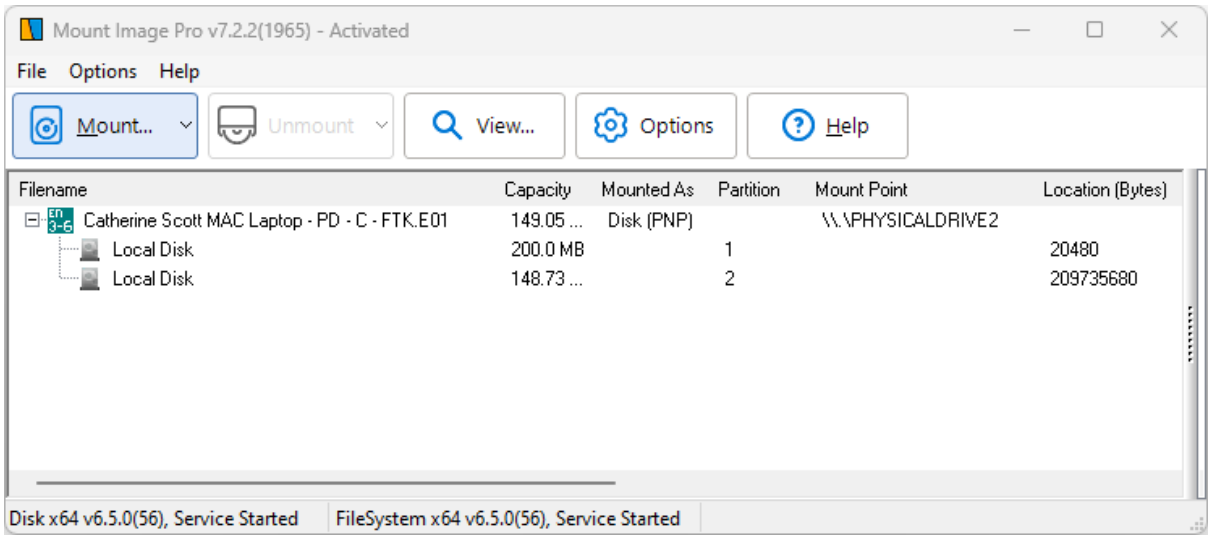
© Copyright GetData Forensics 2002 - 2025, All rights reserved.

To mount and display files using a **third party file system driver**:

1. Ensure that the MAC third party driver is installed and running;

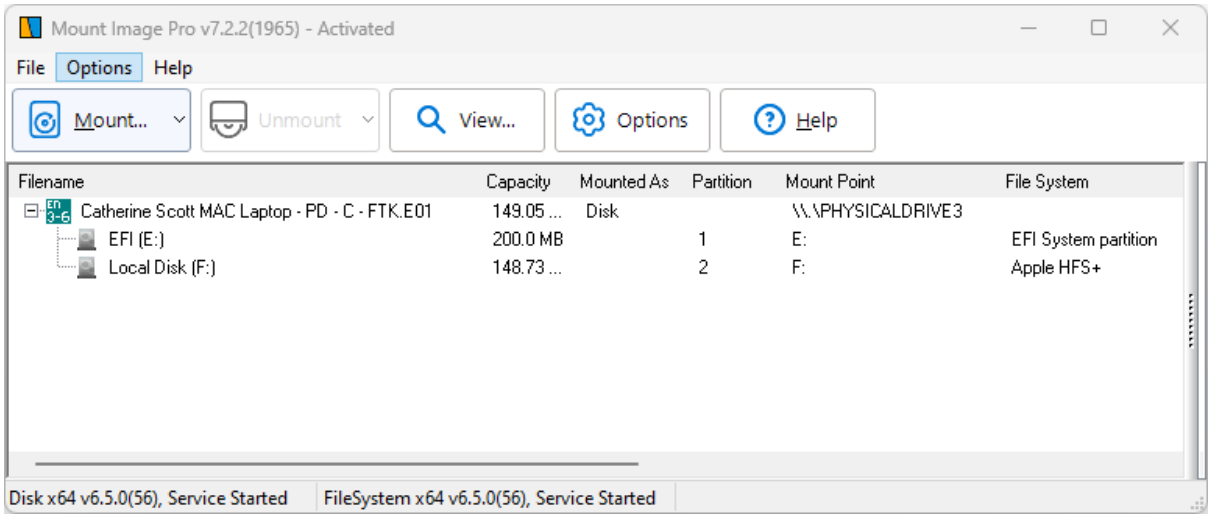
2. Follow the mount instructions in section 7.2 above. In the mount Options window select **Disk** without **plug and play**;

Figure 32: MAC drives mounted as Disk



The third party driver will detect and display the MAC file system:

Figure 33: MacDrive displaying the contents of a MAC drive Disk mount



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 9 – DD Images

In This Chapter

CHAPTER 9 – MOUNT DD FORENSIC-IMAGES

9.1 Mount DD Forensic-Images 54

9.1.1 Mount a Segmented DD images using a Descriptor File 54

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

9.1 MOUNT DD FORENSIC-IMAGES

A single RAW or DD forensic-image can be mounted normally using the GUI or Command Line interface.

A segmented RAW or DD forensic-images ending with the extensions .001, .002, .003 etc. can be mounted normally using the GUI or Command Line interface.

9.1.1 MOUNT A SEGMENTED DD IMAGES USING A DESCRIPTOR FILE

If the image segments do NOT have .001, .002, .003 etc. extensions, follow these instructions:

Creating a Descriptor File

The descriptor file is a text file that contains a list of all raw forensic-images that make up the complete image set. The file extension of the descriptor file should always be '.RAW', even though it is a text file. Inside the text file are the ordered list of the file names of the individual files that make up the entire image.

How to Create Your Descriptor File

A descriptor file is a plain text file which simply lists forensic-image names. Blank lines and leading/trailing blanks are allowed and lines starting with # are ignored as comment lines. Any combination of Carriage Return and Line Feed are allowed as new line delimiters.

Relative paths in a descriptor file are resolved first from the current directory, then from the descriptor file's location.

If the size of the described forensic-image is not a multiple of 512, the capacity of the file is rounded down to a multiple of 512 and exceeding area is not used. E.g. if a file is 5200 bytes, it is treated as a 5120 byte file:

Example of a Descriptor File:

This is a comment line
image01.dat
image02.dat
image03.dat

This file should be saved as "descriptor-file.raw". The file can be saved in any location on your drive. Make sure it contains a valid path to the location of the image segments. Then run Mount Image Pro and select the descriptor file as the file to mount.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 10 – RAID

In This Chapter

CHAPTER 10 - RAID

10.1 RAID - Introduction 56

10.2 Preparation 56

10.3 Mounting a RAID 57

10.3.1 Hardware RAID, known configuration: 57

10.3.2 Software RAID 58

10.3.3 Once the correct RAID layout is identified 59

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

10.1 RAID - INTRODUCTION

Mount Image Pro supports the analysis of the following types of RAID:

JBOD

JBOD (Just a Bunch of Disks) is a term to describe the grouping of odd-sized drives into one larger useful drive. For example, a JBOD could combine 3 GB, 15 GB, 5.5 GB, and 12 GB drives into a logical drive at 35.5 GB, which is often more useful than the individual drives separately.

RAID 0

A RAID 0 (also known as a stripe set or striped volume) splits data evenly across two or more disks (striped) with no parity information for redundancy. It is important to note that RAID 0 was not one of the original RAID levels and provides no data redundancy. RAID 0 is normally used to increase performance, although it can also be used as a way to create a small number of large disks out of a large number of small physical ones.

A RAID 0 can be created with disks of differing sizes, but the storage space added to the array by each disk is limited to the size of the smallest disk. For example, if a 120 GB disk is striped together with a 100 GB disk, the size of the array will be 200 GB.

RAID 1

RAID 1 is a mirrored set with parity. Typically, it consists of two physical drives, one being an exact copy of the other. The RAID Array continues to operate so long as at least one drive is functioning. Using RAID 1 with a separate controller for each disk is sometimes called *duplexing.*

RAID 5

A RAID 5 uses block - level striping with parity data distributed across all member disks. Distributed parity means that if a single drive fails the array is not destroyed. Upon a drive failure, any subsequent drive reads can be calculated from the distributed parity of the functioning drives. A single drive failure in the set will result in reduced performance of the entire set until the failed drive has been replaced and rebuilt.

10.2 PREPARATION

When dealing with RAID drives, care should be taken in the forensic acquisition phase to document as much information as possible as to the RAID configuration.

Successful RAID setup in Mount Image Pro will be assisted by knowledge of the following:

- Is it a hardware or software RAID? (A hardware RAID usually has a separate RAID controller card);
- What is the RAID format, JBOD, RAID 0, 1, 5, other? (Are the drives in the raid identical in size and capacity? This information may be obtained from the system administrator or setup documentation).
- What is the RAID stripe size? (this information may be determined from the RAID controller)
- How many physical disks make up the RAID?

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

- What is the sequence of the physical disks in the RAID? (Noting or photograph the RAID controller port numbers may assist to determine drive sequence).

- Is the RAID complete and functioning? Are there missing drives?

10.3 MOUNTING A RAID

A RAID can be constructed and added to Mount Image Pro using:

1. Physical disks (Note: When using physical disks a hardware write blocking device is recommended to preserve forensic integrity);

2. Forensic Forensic-images; or,

3. A combination of both physical disks and forensic forensic-images.

To add a RAID drive to a case:

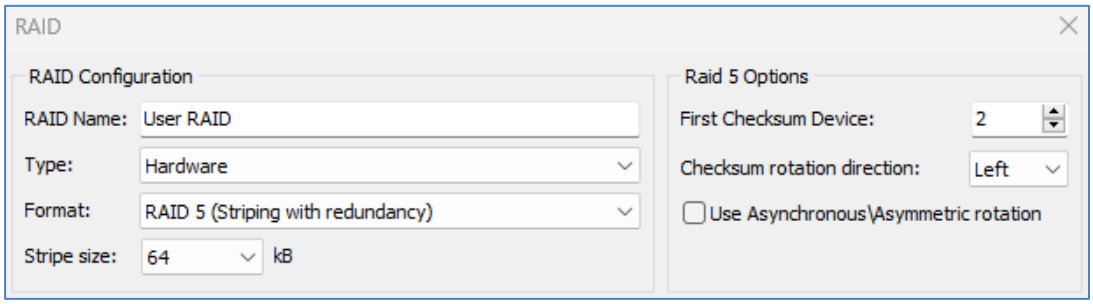
1. Click the button to add a device to the current case.

2. In the Device Selection window, click on the 

button. This opens the RAID configuration window.

10.3.1 HARDWARE RAID, KNOWN CONFIGURATION:

Enter the RAID configuration information:



and follow the instructions to add and test the RAID:

HARDWARE RAID, UNKNOWN CONFIGURATION:

If you do NOT know the parameters of your hardware RAID drive, Mount Image Pro will attempt to identify the way in which the RAID was configured. To do this:

1. Set the RAID type to "**hardware**";

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

2. **Add the drives (or forensic-images) in the correct sequence**, or, if the correct sequence is unknown, add them in the order that is believe to be most correct;

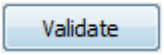
3. Click on the "**Find Layout**" button to find a suggested configuration. A suggested configuration is indicated by a **green tick** next to each added drive.

> **Important:**
>
> A suggested configuration is based on the information available from the drives. However, due to the complexity of a RAID structure, there may be more than one configuration that returns this result. A suggested configuration should be tested by adding the image to the case to determine if individual files can be accessed and previewed.
>
> **If Find Layout did not return a suggested configuration, or,**
> **The suggested configuration did not result in a successful recovery;**
>
> If the Find Layout button did not return green ticks for each added drive, or the continued recovery from a suggested configuration did not work, try the following:
>
> 1. click on the "Probable Solutions" tab to view suggested configurations for the RAID;
> 2. change the "stripe size", RAID Options and drive sequence as suggested;
> 3. click the "Test Layout" button to test the modified configuration;
> 4. add the RAID drive to the case.

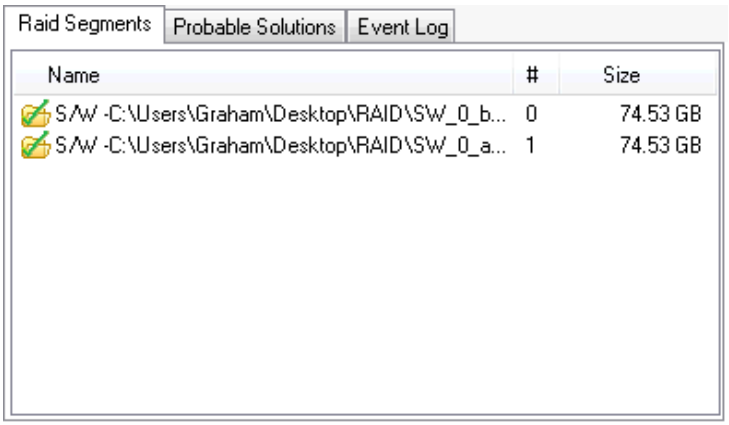
10.3.2 SOFTWARE RAID

If it is a software RAID:

1. Set the "Type" of RAID to "software".

2. Press 

to confirm a valid software RAID. A valid software RAID will show with green ticks on the added drives (or forensic-images):



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

10.3.3 ONCE THE CORRECT RAID LAYOUT IS IDENTIFIED

Once the correct RAID layout has been identified, click **OK** to add the configured RAID drive to the Device Selection window.



Select the RAID drive and click **OK** to add the drive to the case.

Once the RAID drive is added, select and preview individual files to ensure that the RAID drive is correctly configured and access to all files in the RAID has been achieved.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 11 – Network Devices

In This Chapter

CHAPTER 11 –NETWORK DEVICES

11.1 Mount a Remote Network Device 63

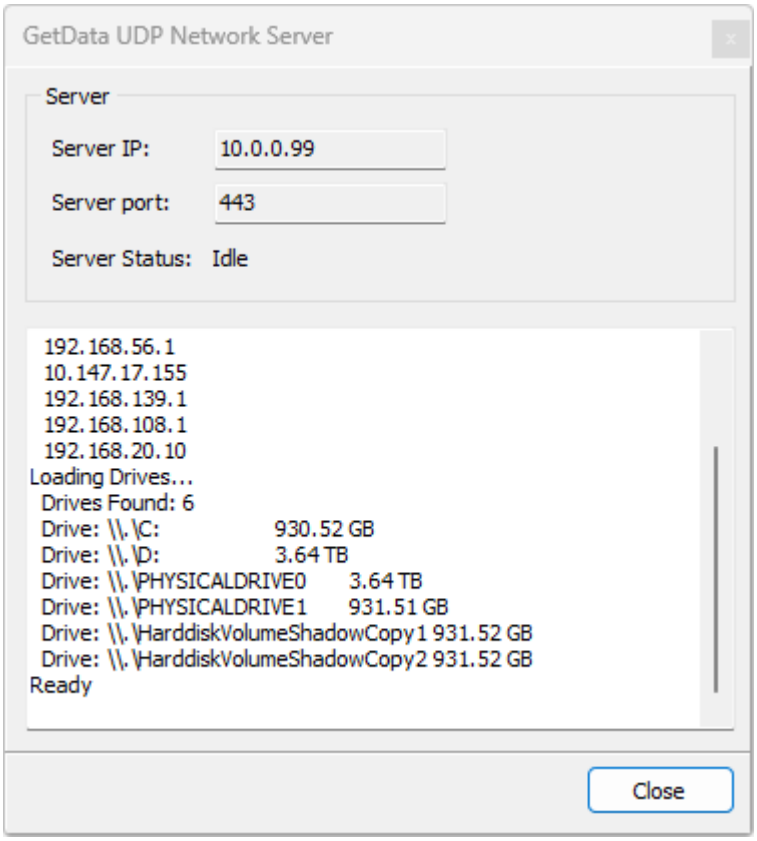
© Copyright GetData Forensics 2002 - 2025, All rights reserved.

11.1 MOUNT A REMOTE NETWORK DEVICE

Mount image Pro has the capability to mount remote device across a network using the UDP protocol (User Datagram Protocol is one of the core members of the Internet Protocol Suite).

To mount a network device:

1. Run the **GetDataNetworkServer.exe** on the remote computer (this file is located in the Mount Image Pro installation folder). The following screen appears;



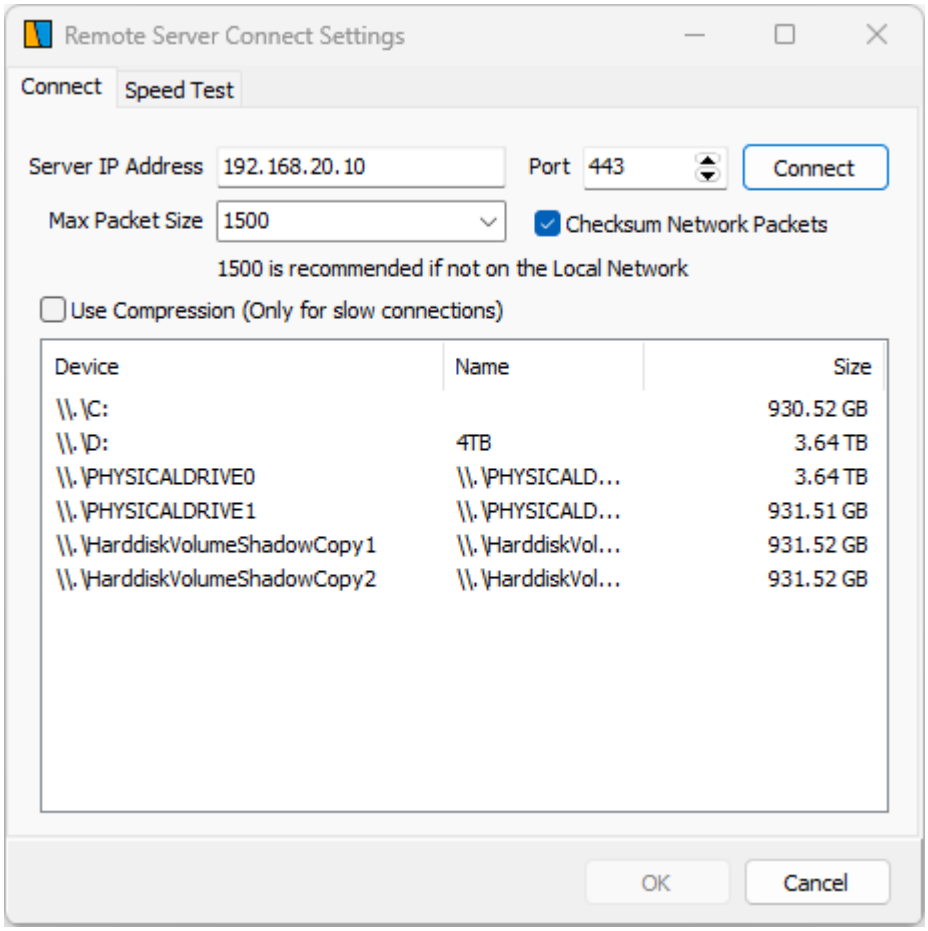
2. The server enters “idle” mode for the connection from Mount Image Pro.

   Note: It may be necessary to configure firewall settings on the remote computer to enable remote access to the GetData UDP Network Server.

3. In the Device Selection window, click on the Remote button to open the **Remote Server Connection Settings** window:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 34: Network Mount - Remote Server Connection Settings



Server IP Address:

Enter the IP address of the remote computer as displayed in the Server IP filed of the GetData UDP Network Server.

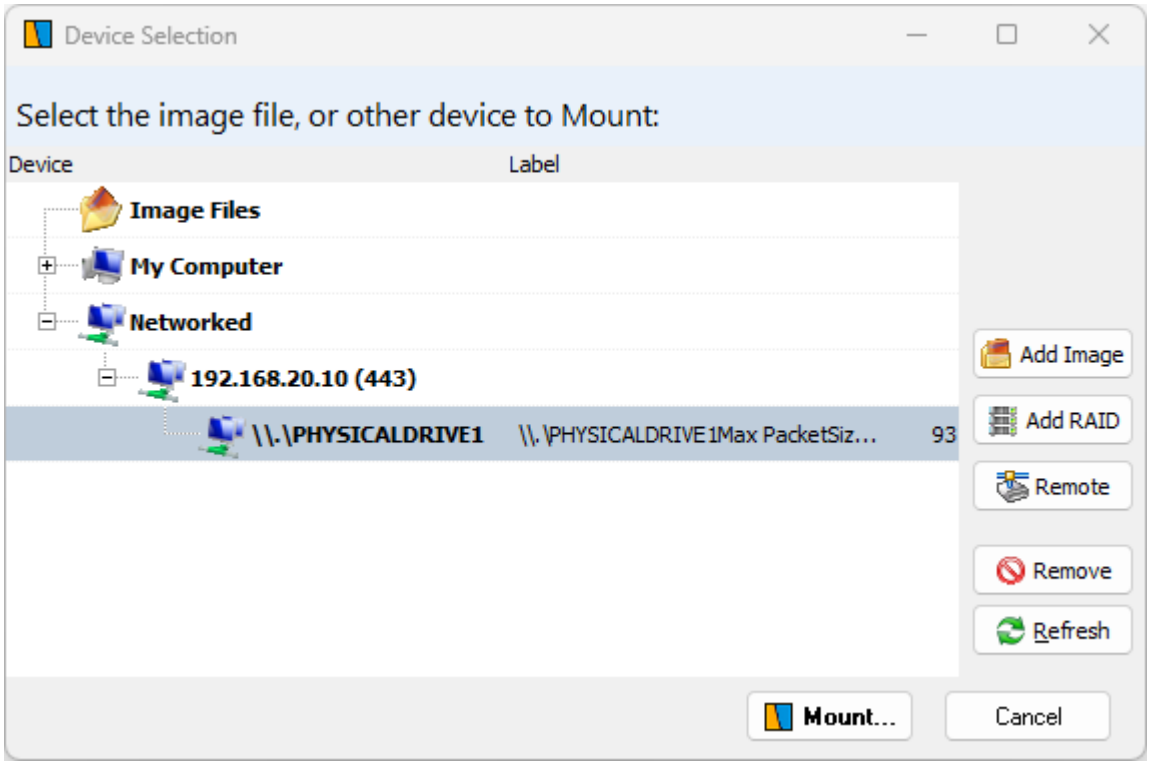
Port:

Ensure the Port number uses the same port as the GetData UDP Network Server.

4. Click the Connect button to view the available physical and logical devices on the remote computer. Select the required device and click OK. The selected device should now appear under the Networked section of the Device Selection window, as shown below:

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Figure 35: Device Selection window showing a UDP network drive



Select the network device and click the **Mount** button.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 12 – CMD Line

In This Chapter

CHAPTER 12 – COMMAND LINE USE

12.1 Windows Path Evnironment Variable 68

12.2 Command Line Functions 70

12.2.1 HELP 70

12.2.2 START 71

12.2.3 STATUS 72

12.2.4 MOUNT 73

12.2.5 UNMOUNT 76

12.2.6 VIEW 77

12.2.7 LOOKUP 78

12.2.8 HIDEGUI / SHOWGUI 79

12.2.9 CLOSE 80

12.2.10 DRIVE STATUS 81

12.2.11 Driverinstall 82

12.2.12 DriverUnisntall 82

12.3 Software Developers Kit (SDK) 82

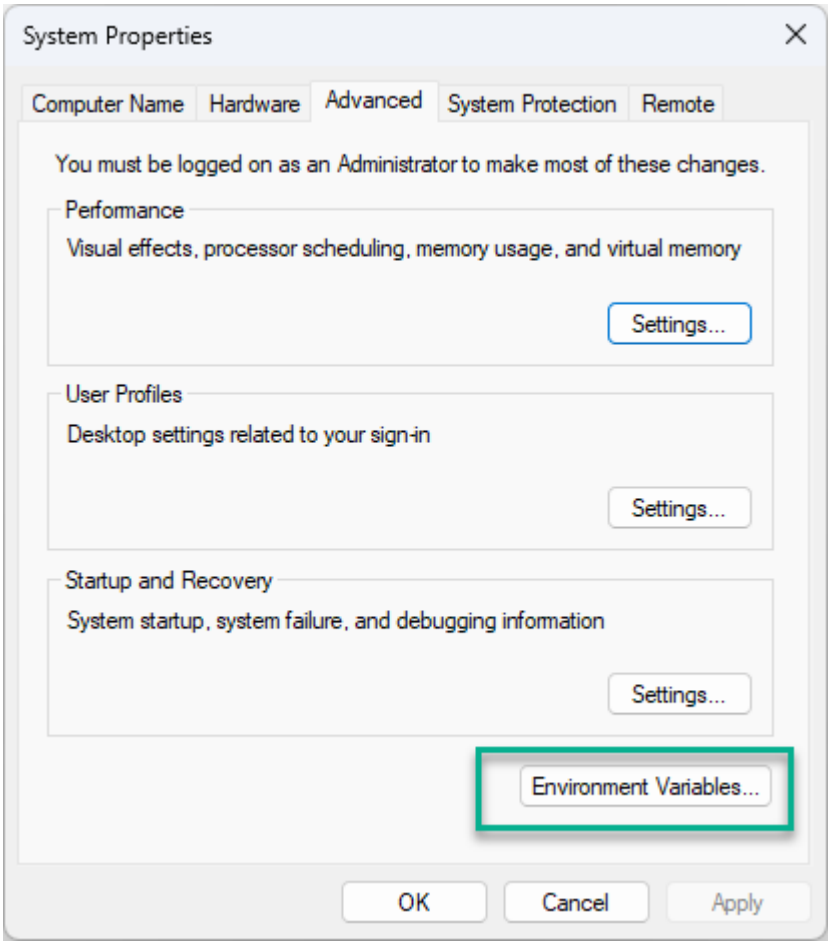
© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.1 WINDOWS PATH EVNIRONMENT VARIABLE

Setting the PATH environment variable will simplify your command line use of Mount Image Pro. Setting the PATH variable means that you can execute 'MIP' commands from the command line within any DOS folder, rather than having to issue the commands from the MIP installation folder.

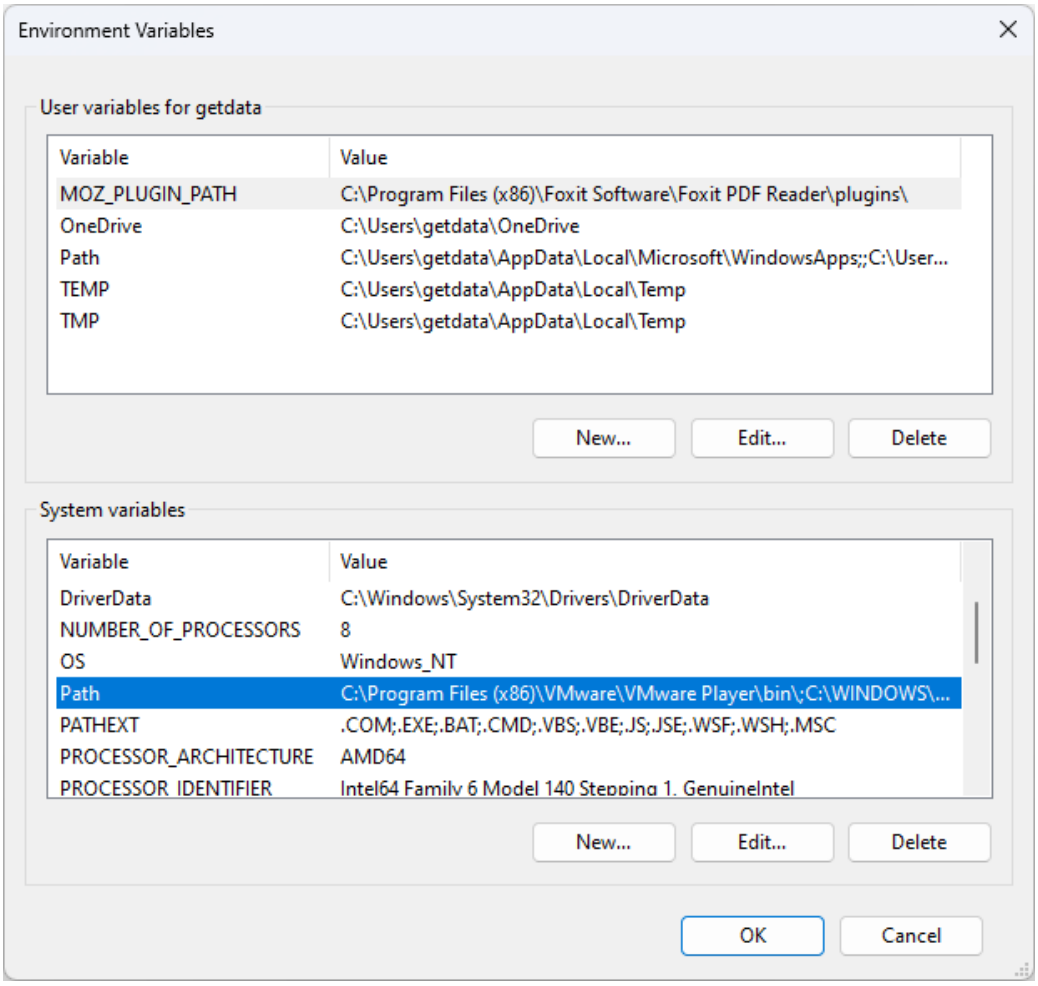
To add MIP to the Windows PATH:

1. Open the Windows **Control Panel**;
2. Select **System > Advanced System Setting**;

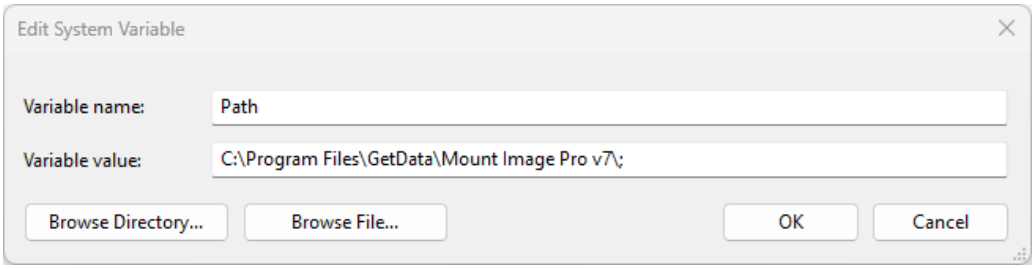


3. In the Environment Variables window, click on **System variables > Path** and then click the **Edit…** button;

© Copyright GetData Forensics 2002 - 2025, All rights reserved.



4. Edit the path to insert the installation location of Mount Image Pro, for example: **C:\Program Files\GetData\Mount Image Pro v7**, as shown below:



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2 COMMAND LINE FUNCTIONS

IMPORTANT: The examples in this section show command line functions issued when MIP has been added to the Windows path. To learn more, refer to xx above.

12.2.1 HELP

The **HELP** command provides an overview of the available command line functions.

MIP HELP

To execute the HELP command, at the command prompt type:

C:\MIP HELP

The following information appears:

```
Usage :
MIP.exe command [options]
Usage :

  START              Starts MIP GUI
  STATUS             Print status information
  MOUNT              Mount a disk image as a virtual drive
  UNMOUNT            Unmount a disk image
  VIEW               Print disk image information
  LOOKUP             Lookup mounted drive letters or forensic-image(s)
  HIDEGUI            Hides MIP GUI
  SHOWGUI            Shows MIP GUI
  CLOSE              Closes MIP GUI
  DRIVERSTATUS       Print MIP driver status
  DRIVERINSTALL      Installs MIP drivers (Requires ADMIN Rights)
  DRIVERUNINSTALL    Uninstalls MIP drivers (Requires ADMIN Rights)
  HELP               Displays command help

All commands and options are case insensitive.
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.2 START

The **START** command starts the GUI and displays its status.

The help command: **C:\MIP HELP START** provides the following information:

```
C:\>MIP HELP START
Usage :
  MIP.exe START
  Starts MIP GUI
```

MIP START

To execute the START command, at the command prompt type:

C:\MIP START

The MIP GUI will then display.

If the command is executed when he MIP GUI is already open, the following output is returned:

```
C:\MIP START
 GUI Status: RUNNING
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.3 STATUS

The **STATUS** command provides information about the running status of MIP.

The help command: **C:\MIP HELP STATUS** provides the following information:

```
C:\>MIP HELP STATUS
Usage :

 MIP.exe STATUS

 Print status information

 This command prints the following information:
  Driver running state
  Driver start type (AUTO/MANUAL)
  Driver start/stop permission
  Driver file path
  Driver file version
  Number of disk devices
  Service running state
  Service start type (AUTO/MANUAL)
  Service start/stop permission
```

MIP STATUS

To execute the STATUS command, at the command prompt type:

C:\MIP STATUS

A successful start should return the following information in the CMD window:

```
C:\>MIP STATUS
Driver File       : C:\Windows\system32\DRIVERS\MIPDISKPNP.v6.sys
Driver Version    : 0.6.0.0
Number of Disks   : 0
Start Type        : AUTO
Start/Stop        : Administrators, Power Users
Driver Status     : RUNNING

Helper Service    : RUNNING
Start Type        : DISABLED
Start/Stop        : Administrators, Power Users
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.4 MOUNT

The **MOUNT** command is used to mount the image or device.

The help command: **C:\MIP HELP MOUNT** provides the following information:

```
C:\>MIP HELP MOUNT
Usage :

  MIP.exe MOUNT imagefile

  Mount a disk image as a virtual drive

Options :

  /D:#  PhysicalDrive Number
        By default, the first available drive number above 10 is used
  /L:a  Drive letters to use
        By default, the first available drive letter is used
  /P:#  Partition number to assign drive letter
        By default, drive letters are assigned to all mountable partitions
  /S:#  Disk sector size (default is 512)
  /A:T  Access method: ReadOnly [T or RO] (default)
                Read/Write emulation [F or RW]
  /MT:# or /T:# Mount type:
        1 or MD = Disk (default)
        2 or FS = File System
        3 or MP = Disk PNP
  /E    File System to be mounted to an Existing File System disk (/L)
  /PNP or /B Use Plug-and-Play
  /O:a  Multiple mounting options
        P = Mounts physical drive only
        S = Show System files in file system
        U = Show Unallocated files in file system
        D = Show Deleted files in file system.
  /W:#  Time to wait for the mounting process (in seconds)
  /XML  Format the output in XML
```

See below for examples.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

MOUNT - DISK EXAMPLES

The following show examples of mounting a disk:

Example 1: Disk – Mount E01 with default settings

C:\MIP MOUNT IMAGE1.E01

No switches used.

Example 2: Disk – Mount E01 – Specified drive letter – As read only

C:\MIP MOUNT IMAGE1.E01 /MT:MD /L:T /A:RO

Switches used:

/MT:MD	= Mount Type is Mount Disk
/L:T	= Logical drive use starts at T:
/A:RO	= Access is Read Only

MOUNT – FILE SYSTEM EXAMPLES

Example 3: File System Mount – Mounts a L01 and AD1 to the same drive letter

E:\>MIP MOUNT /L:T /T:2 "E:\1406JT2.L01"
E:\>MIP MOUNT /L:T /T:2 /E "E:\AD1-FTK-GetData4GSD-C.ad1"

Switches used:

/L:T	= Logical drive use starts at T:
/T:2	= File System mount type
/E	= Mounts the second image to the existing drive

CMD line output shown below:

```
E:\>MIP MOUNT /L:T /T:2 "E:\1406JT2.L01"

Mounting in progress, wait...

Image "E:\1406JT2.L01" contains no partition(s).
Access Mode: Block Mode
------------------------------------
PhysDrive    Not bootable
  Capacity is:  11.84 GB
  Is HardDisk:  False
  Is Optical:   False
  Label is:
  Type is:
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

```
E:\>MIP MOUNT /L:T /T:2 /E "E:\AD1-FTK-GetData4GSD-C.ad1"

Mounting in progress, wait...

Image "E:\AD1-FTK-GetData4GSD-C.ad1" contains no partition(s).
Access Mode: Block Mode
------------------------------------
PhysDrive    Not bootable
  Capacity is:  896.2 MB
  Is HardDisk:  False
  Is Optical:   False
  Label is:
  Type is:
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.5 UNMOUNT

The **UNMOUNT** command is used to unmounts the image or device.

The help command: **C:\MIP HELP UNMOUNT** provides the following information:

```
C:\> MIP HELP UNMOUNT
Usage :

  MIP.exe UNMOUNT /D:# or /L:a or /ALL

  Unmount a disk image

Options :

  /D:#  Physical drive number which can be obtained using LOOKUP command
        Use '*' to unmount all existing disks
  /L:a  Partition drive letter
  /ALL  Unmount all existing disks
  /F or /Q Suppress prompting and force all images to close.
  /W:#  Time to wait for the unmounting process (in seconds)

Drives cannot be dismounted while they are used by any other programs. Although
you can force to close the image by answering to do so when asked or by using the /F
option, you should be aware that to forcibly closing an image may lead to loss of data
or unexpected behavior of the operating system.
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.6 VIEW

The **VIEW** command is used to view information about the mounted image.

The help command: **C:\MIP HELP VIEW** provides the following information:

```
C:\>MIP HELP VIEW
Usage :

  MIP.exe VIEW imagefile or /D:# or /L:a or /ALL

  Print disk image information

Options :

  /D:#  Physical drive number which can be obtained using LOOKUP command
  /L:a  Partition drive letter
  /ALL Display information about all mounted images. (Default)
  /XML  Format the output in XML
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.7 LOOKUP

The **LOOKUP** command is used to return information about mounted drives and forensic-images.

The help command **C:\MIP HELP LOOKUP** provides the following information:

```
C:\>MIP HELP LOOKUP
Usage :

  MIP.exe LOOKUP imagefile or /L:a

  Lookup mounted drive letters or forensic-image(s)

Options :

  /D:#  Physical drive number which can be obtained using LOOKUP command
  /L:a  Partition drive letter
  /XML  Format the output in XML

Print the following information for the image or drive letter:
  Mounted Forensic-image Names
  Drive Letters and Partition Numbers List
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.8 HIDEGUI / SHOWGUI

The **HIDEGUI** and **SHOWGUI** commands are used to hide or show the MIP GUI.

In Example 4 below the MIP GUI is hidden prior to the mount of the image:

Example 4: Hiding the GUI before mounting an image

```
C:\>MIP HIDEGUI
GUI Status: RUNNING

C:\>MIP MOUNT IMAGE1.E01
Mounting in progress, wait...

Image "C:\IMAGE1.E01" contains no partition(s).

Access Mode: Block Mode
------------------------------------
PhysDrive    Not bootable
  Capacity is:  7.47 GB
  Drive Letter: \\.\PHYSICALDRIVE4
  Is HardDisk:  True
  Is Optical:   False
  Label is:
  Type is:      Physical

C:\>
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.9 CLOSE

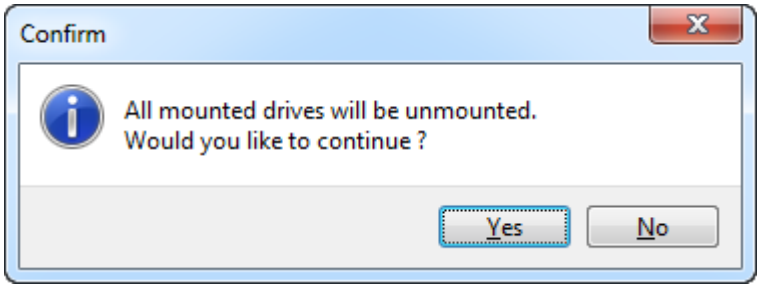
The **CLOSE** command is used to unmount all image files and close the MIP GUI.

The help command **C:\MIP HELP CLOSE** provides the following information:

```
C:\>MIP HELP CLOSE
Usage :
  MIP.exe CLOSE
  Closes MIP GUI
```

MIP CLOSE

If images are mounted at the time the **MIP CLOSE** command is issued, the following window will display and require user action:



To avoid this message, all images should first be unmounted before the close command is issued. For example:

Example 5: Unmounting all before close

```
C:\>MIP UNMOUNT /ALL
Closing all mounted images...
The image(s) is closed.

C:\>MIP CLOSE
GUI Status: CLOSED
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.10 DRIVE STATUS

The **DRIVERSTATUS** command returns information about the install MIP drivers. This command is generally used for troubleshooting installation or operation.

```
C:\>MIP DRIVERSTATUS

================================
Fetching 64bit PNP Status...
================================

Installed Modules: 1
ServicePath: C:\Windows\system32\DRIVERS\MIPDISKPNP.v6.sys
FileVersion: 6.0.7.10
ServiceStatus: Started
MarkedForDeletion: False
RebootRequired: False
InfPath: C:\Windows\inf\oem135.inf
InfValues:
  ServiceName: MIPDISKPNP.v6
  HardwareId: root\mipdisk_storlib_bus_v6
  ClassName: MIPDiskStorageLib
  ClassGuid: {803821A4-46BF-4D3D-9916-32FA68EC74BA}
PNP DevicePresent: True

================================
Fetching 64bit FileSys Status...
================================

Installed Modules: 1
ServicePath: C:\Windows\system32\DRIVERS\MIPFS.v6.sys
FileVersion: 6.0.2.21
ServiceStatus: Started
MarkedForDeletion: False
RebootRequired: False
InfPath: C:\Windows\inf\oem136.inf
InfValues:
  ServiceName: MIPFS.v6
  HardwareId: root\mipfs_storlib_bus_v6
  ClassName: MIPFSStorageLib
  ClassGuid: {DC7F5B75-7C53-42AE-8611-9C2B5A46530F}
PNP DevicePresent: True
```

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

12.2.11 DRIVERINSTALL

The **DRIVERINSTALL** command installs MIP drivers. Administrator rights are required.

12.2.12 DRIVERUNISNTALL

The **DRIVERUNINSTALL** command uninstalls the MIP drivers.

12.3 SOFTWARE DEVELOPERS KIT (SDK)

Mount Image Pro does not have a SDK or DLL. However third party applications can interface directly with Mount Image Pro using the CMD Line functions detailed in this chapter.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Chapter 12 - Legal

In This Chapter

CHAPTER 13 - LEGAL

13.1 This User Guide 84

13.2 Copyright 84

13.3 License Agreement 84

13.4 Disclaimer 85

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

13.1 THIS USER GUIDE

This user guide is provided for information purposes only. All information provided in this user guide is subject to change without notice.

Please check the website, www.forensicexplorer.com for the latest version of the software and documentation.

13.2 COPYRIGHT

This user guide and its content is © copyright of GetData Forensics Pty Ltd. All rights reserved.

Any redistribution or reproduction of part or all of the contents in any form is prohibited without the express written permission of GetData Forensics Pty Ltd.

Products and corporate names appearing in this user guide may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation into the owners' benefit, without intent to infringe.

Specific trademark owners who are well established in the field of computer forensics software and whose products and terminology have become synonymous with forensics include:

Guidance Software (www.guidancesoftware.com), EnCase®;

Access Data (www.accessdata.com), Forensic Tool Kit® (FTK®);

Xways forensics (http://www.winhex.com), X-ways forensics®.

13.3 LICENSE AGREEMENT

GetData Forensics Pty Ltd ACN 143458039 ("GetData") is the developer of the software program Mount Image Pro. Permission to use Mount Image Pro and / or its documentation (the "Software") is conditional upon you agreeing to the terms set out below. By installing or otherwise using the Software you agree to be bound by the terms of this agreement. If you do not wish to accept the terms, do not install or use the Software.

GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData. Unauthorized copying or modification of the Software will entitle GetData to immediately terminate this Agreement.

A single license of the software permits you to use the Software on a single computer. In the event that you have purchased multiple licenses, you may install and use the Software concurrently on multiple computers equivalent to the number of licenses that you have purchased. Unless you have purchased multiple licenses, this license does not permit you to load or use the Software on a network server or similar device which permits access by multiple computers.

You are not permitted to share the product activation information provided to you for this Software with other users.

GetData shall have the right to check license details at any time in any reasonable manner.

GetData may from time to time revise or update the software and may make such revisions or updates available subject to payment of the applicable license fee.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.

The Software is protected under United States law and international law and international conventions and treaties. You may not rent, lease, sublicense, assign or otherwise transfer use of the Software to others without the express written permission of GetData. Doing so will entitle GetData to immediately terminate this Agreement.

Except to the extent applicable law specifically prohibits such restrictions, you may not reverse engineer, reverse compile, disassemble or otherwise modify the Software in any way.

You are solely responsible for protecting yourself, your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any damages suffered from the use of the Software.

BY USING THE SOFTWARE, YOU EXPRESSLY AGREE THAT ALL RISKS ASSOCIATED WITH THE PERFORMANCE AND QUALITY OF THE SOFTWARE IS ASSUMED SOLELY BY YOU. YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE EXERCISED YOUR INDEPENDENT JUDGEMENT IN ACQUIRING THE SOFTWARE.

TO THE EXTENT PERMITTED BY LAW, GETDATA SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF GETDATA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE IS MADE AVAILABLE BY GETDATA "AS IS" AND "WITH ALL FAULTS". TO THE EXTENT PERMITTED BY LAW, GETDATA DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, CONCERNING THE QUALITY, SAFETY OR SUITABILITY OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR THAT THE SOFTWARE IS ERROR FREE.

IF ANY CONDITION OR WARRANTY IS IMPLIED INTO THIS AGREEMENT UNDER ANY APPLICABLE LEGISLATION CANNOT BE EXCLUDED, OR IF NOTWITHSTANDING THE EXCLUSION OF LIABILITY ABOVE GETDATA IS OTHERWISE LIABLE TO YOU, THEN TO THE EXTENT PERMITTED BY LAW THE LIABILITY OF GETDATA FOR BREACH OF THE CONDITION OR WARRANTY WILL BE LIMITED TO ONE OR MORE OF THE FOLLOWING AS DETERMINED BY GETDATA IN ITS ABSOLUTE DISCRETION:

(i) IN THE CASE OF GOODS, (A) THE REPLACEMENT OR SUPPLY OF EQUIVALENT GOODS OR THE REPAIR OF THE GOODS; OR (B) THE PAYMENT OF THE COST OF REPLACING THE GOODS, ACQUIRING EQUIVALENT GOODS, OR HAVING THE GOODS REPAIRED; AND

(ii) IN THE CASE OF SERVICES, THE SUPPLYING OF THE SERVICES AGAIN OR THE PAYMENT OF THE COST OF HAVING THE SERVICES SUPPLIED AGAIN.

This agreement cannot be changed or altered except by a written document signed by you and GetData. This agreement is governed by the laws in force in New South Wales, Australia. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of New South Wales, Australia.

13.4 DISCLAIMER

The software available for down loading through Internet sites and published by GetData Forensics Pty Ltd (“GetData”) is provided pursuant to this license agreement. GetData encourages you to know the possible risks involved in the download and use of the Software from the Internet. You are solely responsible for protecting yourself, your data, your systems and your hardware used in connection with this software. GetData will not be liable for any damages suffered from the use of the Software.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

BY USING THIS SOFTWARE, YOU EXPRESSLY AGREE THAT ALL RISKS ASSOCIATED WITH THE PERFORMANCE AND QUALITY OF THE SOFTWARE IS ASSUMED SOLELY BY YOU. GETDATA SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF GETDATA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE IS MADE AVAILABLE BY GETDATA "AS IS"; AND "WITH ALL FAULTS" GETDATA DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, CONCERNING THE QUALITY, SAFETY OR SUITABILITY OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. FURTHER, GETDATA MAKES NO REPRESENTATIONS OR WARRANTIES AS TO THE TRUTH, ACCURACY OR COMPLETENESS OF ANY INFORMATION, STATEMENTS OR MATERIALS CONCERNING THE SOFTWARE THAT IS CONTAINED IN GETDATA'S SOFTWARE DOWNLOAD SITE. IN NO EVENT WILL GETDATA BE LIABLE FOR ANY INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES HOWEVER THEY MAY ARISE AND EVEN IF GETDATA HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Appendix 1 - Support

APPENDIX 1 - TECHNICAL SUPPORT

GetData Forensics Pty Ltd has its headquarters in Sydney, New South Wales, Australia.

SUPPORT

Documentation: http://www.mountimage.com/support

Email Support: support@getdata.com

Phone Support: USA: (866) 723-7329

Or;

Sydney, Australia: +61 (0)2 8208 6053
Hours: Australian Eastern Standard Time, 9am - 5:30pm Mon - Fri

HEAD OFFICE

GetData Forensics Pty Ltd
Suite 204, 13A Montgomery Street
Kogarah, New South Wales, 2217
Australia

Phone: +61 (0)2 82086053

Fax: +61 (0)2 95881195

Hours: Australian Eastern Standard Time, 9am - 5:30pm Mon – Fri

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Appendix 2 – Mount Types

APPENDIX 2 – MOUNT TYPES

The following table summarizes the differences between Disk and File System mounts:

Mount	Disk	File System
Existing Windows security settings apply	Yes	No
26 forensic-image limit (available drive letters)	Yes (No if MIPDisk Folder is used)	No
Access entire physical drive with 3rd party tools	Yes	No
Disk is shown in Windows Disk Management (* with PNP option)	Yes	No
Display deleted files	No	Yes
Display unallocated clusters as a file	No	Yes
Display Windows system files (MFT, FAT, VBR etc.)	No	Yes

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Appendix 2 - Write Blocking

APPENDIX 2 - WRITE BLOCKING

IMPORTANT:

An accepted principal of computer forensics is that, wherever possible, source data to be analyzed in an investigation should not be altered by the investigator.

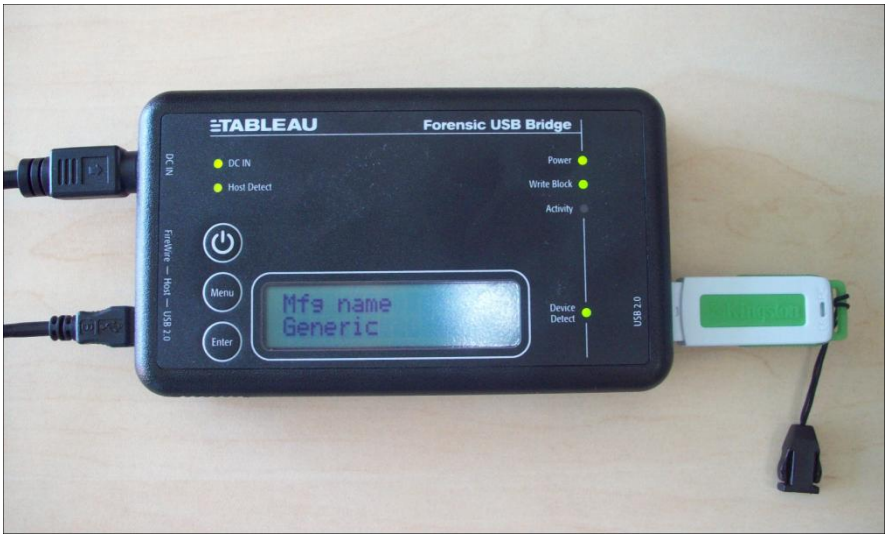
If physical media such as a hard drive, USB drive, camera card etc. is a potential source of evidence, it is recommended that when the media is connected to a forensics workstation it is done so using a write block device.

A write block is usually a physical hardware device (a write blocker) which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined device and maintain “forensic integrity”.

There are a wide variety of forensic write blocking devices commercially available. Investigators are encouraged to become familiar with their selected device, its capabilities and its limitations.

Shown below is a Tableau USB hardware write block. The source media, an 8 GB Kingston USB drive is attached and ready for acquisition or analysis:

Tableau USB write block with USB as the source drive



© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Appendix 3 - Definitions

APPENDIX 6 - DEFINITIONS

Alternate Data Stream	An Alternate Data Stream (ADS) is a feature of the NTFS file system. ADS were originally included in Windows NT for compatibility with Macintosh HFS file systems resource fork and a data fork. The ADS provides a means to allow programmers to add additional metadata to be stored for a file, without adding this data directly to the file. The additional data is attached as a stream which is not normally visible to the user.
ANSI character set	The ANSI character set was that standard character encoding for English versions of Microsoft Windows, including Windows 95 and NT. The ANSI format stores only the 128 ASCII characters and 128 extended characters, using 1 byte per character. Not all of the Unicode characters are supported.
ASCII	The American Standard Code for Information Interchange (ASCII) is a 7-bit character encoding scheme that allows text to be transmitted between electronic devices in a consistent way. The ASCII character set comprises codes 0–127, within which codes 0–31 and 127 are non-printing control characters. The addition of Codes 128–255 make up the Extended ASCII character set (see http://www.ascii-code.com/ for more information) (2).
Cluster	A cluster is the smallest logical unit of disk storage space on a hard drive that can be addressed by the computers Operating System. A single computer file can be stored in one or more clusters depending on its size.
Cluster Boundaries	A cluster boundary refers to the start or the end position of a cluster (a group of sectors). If a file is fragmented (stored in non-contiguous clusters), the fragmentation happens at the cluster boundary, as there is no smaller unit of storage space that can be addressed by a computer. Examining data at cluster boundaries can be an important technique to improve the speed of some search routines. For example when file carving for file headers, it is faster to search the cluster boundary (i.e. the beginning of a cluster) rather than a sector by sector search of the drive.
Code page	Code page is another term for character encoding. It consists of a table of values that describes the character set for a particular language. When a keyword search is conducted in Mount Image Pro, the correct code page should be selected.
Computer forensics	Computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data with a view to presenting evidence in a court of law.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Compound File	A compound file is a file that is a container for other files or data, such as a .Zip or .Pst (Microsoft Outlook mail file).
Data carve	See file carve.
Deleted File	A deleted file is one which has been marked as deleted by the file system (usually as a result of being sent to and emptied from with Recycle Bin). A deleted file can be recovered by reading the file system record for the file, then reading and restoring the file data. As long as the data for the file is intact (i.e. the space once occupied by the file has not been used to store new data) the recovered file will be valid. In some cases the file system record itself can be overwritten and destroyed. If this is the case the file can only be recovered by "file carving". Because file and folder information is only stored with the file system record, a carved file does not retain its original file or folder name.
Device	A device refers to the electronic media being examined. It usually refers to a physical device, such as a hard drive, camera card etc., but can also mean the forensic image of a device in DD, E01 or other formats.
Directory	See Root Directory
Directory Entry (FAT)	A component of the FAT file system. Each file or folder on a FAT partition has a 32 byte directory entry which contains its name, starting cluster, length and other metadata and attributes.
Disk Slack	The area between the end of a partition and the end of the disk. It is usually considered to be blank, but can hold remnants of previous disk configurations or could be used to purposely hide data.
E01	A forensic file format used to create disk forensic-images. Developed by Guidance Software (http://www.guidancesoftware.com/)
FAT	FAT (File Allocation Table) is the file system that pre-dates NTFS. Once popular on Windows 95, 98 and XP, it is now primarily used on memory cards, usb drives, flash memory etc. due to its simplicity and compatibility between Operating Systems (e.g. Windows and MAC). For more information see: http://www.forensicswiki.org/wiki/FAT
FAT Slack	The unused space in the last cluster of the FAT where the logical size of the FAT does not fill the complete cluster.
File Slack	The unused space in the last cluster of a file where the logical size of the file does not fill the complete cluster. The file slack can contain fragments of old data previously stored in that cluster.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

File system	The organization of files into a structure accessible by the Operating System. The most common types of file systems used by Widows are FAT and NTFS. Others include EXT (Linux) and HFS (MAC).
Folder	See Root Directory
Forensic Image	A "forensic image is a file (or set of files), used to preserve an exact "bit-for-bit" copy of data residing on electronic media. Using non-invasive procedures, forensic software is used to create the forensic-image. The image contains all data, including deleted and system files, ad is an exact copy of the original. Most forensic imaging software integrate additional information into the forensic-image at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an "acquisition hash", which can be later used to validate the integrity of the image. The forensic forensic-image acts as a digital evidence container that can be verified and accepted by courts.
Forensic Integrity	In computer forensic the term “forensic integrity” commonly refers to the ability to preserve the evidence being examined so that it is not altered by the investigator or the investigative process. This enables a third party to conduct an independent examination of the evidence on an identical data set. Forensic integrity is usually achieved through the use of write blocking devices (to protect original media from being changed) and the forensic image process (the acquisition of an identical copy which can be re-verified at a later date.)
Fragmented File	The distribution of a file on a disk so that it's written in non-contiguous clusters.
Free Space	Free space is often used to describe unallocated clusters, the available disk storage space that is not allocated to file storage by a volume. Free space can however also refer to the unused area of a disk.
Hash	A Hash is a mathematical calculation to generate a unique value for specific data. The chances of two files that contain different data having the same hash value are exceedingly small. The most common hash algorithms in use are MD5, SHA1 and SHA256.
Hex	Hexadecimal is a base 16 numbering system. It contains the sixteen sequential numbers 0-9 and then uses the letters A-F. In computing, a single hexadecimal number represents the content of 4 bits. It is usually expressed as sets of two hexadecimal numbers, such as “4B”, which gives the content of 8 bits, i.e. 1 byte.
Forensic-Image	See Forensic Image.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

LEF	See Logical Evidence File
Live Boot	Live Boot is a function of Forensic Explorer (www.forensicexplorer.com) which enables the boot of a forensic image file containing a booting file system (Windows and Linux currently supported). To Live Boot an image Forensic Explorer v3 (or above), Mount Image Pro v7 (or above) and VMWare (Work Station or Player) are required. For more detail see the Forensic Explorer user manual.
Logical Evidence File (LEF)	A Logical Evidence File is a forensic image containing specific files, rather than the traditional image of an entire volume or physical disk. They are usually created during a preview where an investigator identifies file based evidence worthy of preservation, when an image of the entire volume or device is not warranted. Common Logical Evidence File formats are L01, created by EnCase® ® forensic software (www.guidancesoftware.com) or AD1 by Access Data's Forensic Tool Kit ® (www.accessdata.com).
Logical file space	The actual amount of space occupied by a file on a hard drive. It may differ from the physical file size, because the file may not completely fill the total number of clusters allocated for its storage. The part of the last cluster which is not completely filled is called the file slack.
Master boot record (MBR, Boot Sector)	The very first sector on a hard drive. It contains the startup information for the computer and the partition table, detailing how the computer is organized.
Master File Table (MFT)	*"On an NTFS volume, the MFT is a relational database that consists of rows of file records and columns of file attributes. It contains at least one entry for every file on an NTFS volume, including the MFT itself. The MFT stores the information required to retrieve files from the NTFS partition".* (3))
NTFS	The Windows New Technology File System (NTFS) superseded FAT. It was released with Windows NT and subsequently Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7. It uses a Maser File Table (MFT) to store the information required to retrieve files from the NTFS partition.
Partition	A part of a hard disk that can have an independent file system.
RAID	Redundant Array of Independent Disks.
Root Directory/Folder	A directory is a container used to organize folders and files into a hierarchical structure. The root (also referred as the root folder or root directory) is the first level folder of the hierarchy. It is analogous to the

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

	root of a tree, from which the trunk and branches arise. A directory that is below the root is called a subdirectory. A directory above a subdirectory is called its parent directory. The root is the parent of all directories. "Directory" was a more common term when DOS use was prolific (The "DIR" command is used in DOS to list the contents of a directory). Directories are now more commonly referred to as "Folders".
Sector	A sector is a specifically sized unit or storage on a hard disk. A sector on a hard disk usually contains 512 bytes. A group of sectors forms a cluster, which is the lowest level of storage space which can be addressed by an Operating System (e.g. Windows).
Symbolic Link	A file or folder which references another file or folder in a different location in the File System. A symbolic link contains a text string that is automatically interpreted and followed by the operating system as a path to another file or folder.
Unallocated Clusters	Unallocated clusters (also referred to as unallocated space or free space) are the available disk storage space that is not allocated to file storage by a volume. Unallocated clusters can be a valuable source of evidence in a computer forensics examination because they can contain deleted files or remnants of deleted files created by the Operating System and / or computer users.
Unicode	Unicode is an international standard for processing and displaying all types of text. Unicode provides a unique number for every character for all languages on all platforms.
Volume	A collection of addressable sectors that are used to store data. The sectors give the appearance of being consecutive, but a volume may span more than one partition or drive.
Write Block	A hardware device or software program that prevents writing to an examined device. A write block is designed to maintain the 'forensic integrity' of an examined device by demonstrating that changes to the content of the device were not possible.

© Copyright GetData Forensics 2002 - 2025, All rights reserved.

Appendix 4 - Index

APPENDIX 4 - INDEX

Access Mode
  Virtual Disk, 46
Activation
  Dongle, 19
  Evaluation version offline, 22
  Evaluation version online, 21
Auto mount
  Startup, 50
BitLocker, 37
Command Line. *See* CMD Line
Copyright, 88
Data Views
  Summary, 74
Disclaimer, 89
Disk Label
  File System mount, 48
Dongle. *See* Activation
Environment Variable. *See* Path
File slack
  Definition, 96
GUI, 43
Help
  CMD Line, 74
HIDEGUI
  CMD Line, 83
Installation, 10
JBOD, 60
License agreement, 88
Live Boot, 98
Logging, 51
Module
  File System, 57
Mount
  CMD Line, 77
  GUI, 44
Mount Types
  Summary Of, 36
Options
  GUI, 50
  Mount, 45
Path, 72
Plug-and-Play
  Virtual Disk, 46
Property Window
  GUI, 43
Purchase orders, 16
RAID, 60
  Hardware, 61
  Software, 62
SDK, 86
Sector Size
  Virtual Disk, 46
Status Bar
  GUI, 43
Stay on top, 51
Support, 91
Technical support, 91
Uninstall, 13
Unmount
  CMD Line, 80
  GUI, 49
View, 50
  CMD Line, 81
Virtual disk
  Compatible Image Types, 37
Virtual Disk, 37
  Mount Options, 46
Virtual File System, 39
Windows Path. *See* Path

© Copyright GetData Forensics 2002 - 2025, All rights reserved.