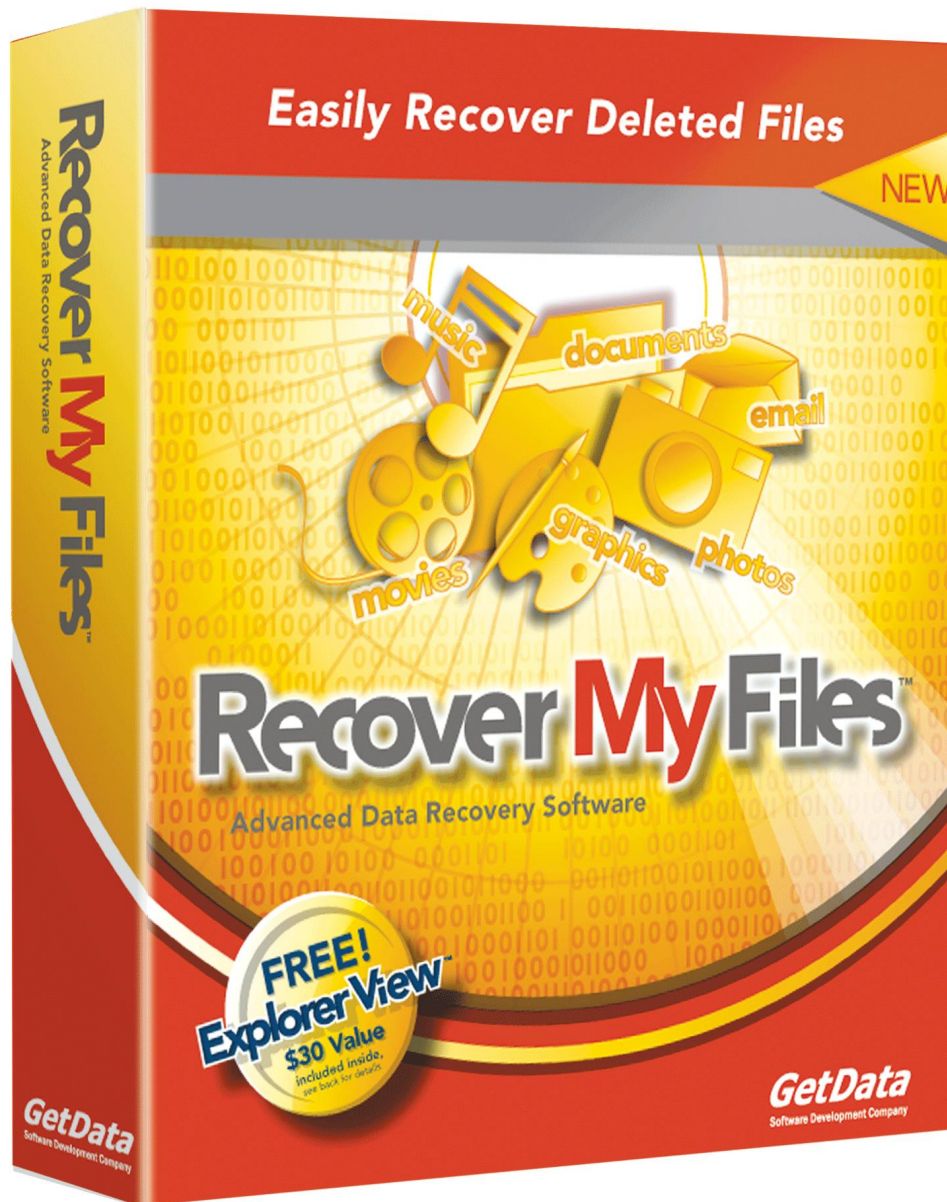# Recover My Files v6

Recover My Files v6
Chapter Contents

Published: 30 January 2017 at 09:35:42

Frequently Asked Questions

How long will a deleted or missing file stay on my drive?

There is no time limit. A deleted file will reside on the drive up until such time as the space it occupies is used to store new data. Once a deleted file has been overwritten by new data it has been destroyed. If you have suffered data loss, minimize the use of the computer until such time as you have finished your data recovery efforts.

How long should it take to recover a formatted drive?

Most drive recoveries can be completed in less than 2 hours with all files recovered. Greatest time savings can be made by knowing when to best stop a search. Rarely is it necessary to scan an entire drive in order to get back all data. See 0 for more information.

Will Recover My Files recover all my data?

The sooner that data recovery is attempted after a loss the greater the possibility that 100% of the data can be recovered (the more a problem drive is used after a data loss, the greater the risk that new data is written to the drive and the missing files are overwritten and destroyed). If you have accidentally formatted a drive, or have lost a drive letter, and have not written new data to the drive, you should expect 100% recovery. If you have reset or reinstalled Windows and have minimized the use of the computer since that time, you should expect from 90 - 100% recovery.

Of course there are situations where the chance of data recovery is greatly reduced. For example, if you have restored a backup to a formatted drive and the drive is now half full, only 50% of the drive can now be searched for previous data.

The bottom line is that you will only know what data can be recovered once your try. Download and run Recover My Files in evaluation mode to see what can be found. If you can find and preview your files, then purchase a key to save them to another drive.

Will Recover My Files find my original file and folder structure?

Yes. Recover My Files is designed specifically to recover a missing file and folder structure. If the file and folder structure is destroyed, the content of files can still be recovered as "Lost Files", by searching for individual file structures on the drive.

How do I know if Recover My Files can find my missing files?

Download and Run Recover My Files in evaluation mode. Look through the search results and click on the files to preview their content. If you can see pictures and read the documents, recovery has been successful and you can purchase a key, enter it into the program, and save your files to another drive.

Can I search for deleted files in a specific folder? Do I have to search the whole drive?

Searching for deleted files over the entire drive is a very fast process. Recover My Files reads the file index for all files on the drive in less than 1 minute. Run a "Recover Files" search "Deleted Files (Recommended)" and then look in the "Deleted" view to see only deleted files, or switch to "Folder" view and navigate to the specific folder. If you do not find the files then try a Recover Files search for "Deleted and Lost Files" (this is a longer search).

My drive makes a clicking noise

An abnormal clicking or grinding noise is a sign of a physical drive failure. Continued use of a drive in this state can cause additional damage and may lead to permanent data loss. The drive should be immediately powered down and assistance sought from a hardware data recovery service.

Will Recover My Files repair my drive?

No. Recover My Files is a data recovery tool, not a drive repair tool. Recover My Files is designed specifically so that it will not change the content of the drive being searched. When you locate your files you <u>must</u> save the files to another drive.

How do I permanently erase data from a drive?

Data is permanently erased by overwriting it with new data. Wiping and secure delete programs (available by searching with Google) permanently erase data by writing new data, usually the character "0", over the old. Once this has taken place the only data that can be recovered is the 0's.

Does a format of a drive permanently remove data?

A format is not a destructive process (unless special format instructions are applied). Do not write any new data to the formatted drive. Run a "Recover Drive" search with Recover My Files and you should get 100% recovery.

I have reset or re-installed Windows. Can I get my data back?

Yes, recovery of the old file and folder structure is possible after a reset or re-install of Windows. Run a "Recover Drive" search.

I find hundreds of pictures on my drive - where did these come from?

Each time you (or another user on the computer) visits a web page the pictures on the page are written into your internet browsers web cache (designed to make the loading of web pages faster by reading the pictures from the hard drive instead of the remote computer). When this cache becomes full, the older content is automatically deleted by Windows. These pictures are found in a search with Recover My Files.

Does Recover My Files work on an iPhone or an iPod Touch?

Apple protects the iPhone, iPad and iTouch so that the hard drive cannot be viewed as a drive letter on the PC. For this reason Recover My Files cannot be used to recover data from these devices. Recover My Files will however work with other iPods that can be placed into "drive mode".

How many times can I use Recover My Files?

A purchased license key can be used to activate Recover My Files on two separate computers, e.g. a desktop and a laptop. You may use Recover My Files as many times as you wish on those computers. The software will not expire. Updates to the current version are free (i.e. v6). Existing customers will be offered a discounted upgrade to the next major version release (e.g. from v5 to v6).

How do I get Technical Support?

Technical support is available in this documentation, by email, live chat, and telephone. Please see Appendix 1 – Technical Support.

Data Recovery Fundamentals

DATA RECOVERY FUNDAMENTALS

HARDWARE RECOVERY

A computer hard drive contains drives called platters which are coated with a magnetic storage medium. The platters spin at high speed whilst a "read/write" head moves backwards and forwards in a cushion of air over their surface. The head reads the status of the magnetic material (a positive or negative charge) and writes to the magnetic medium with an electronic pulse.

Figure 1, Simplified schematic diagram of hard drive internals: Image Source: Microsoft MSDN

Learn more: http://www.youtube.com/watch?v=kdmLvI1n82U
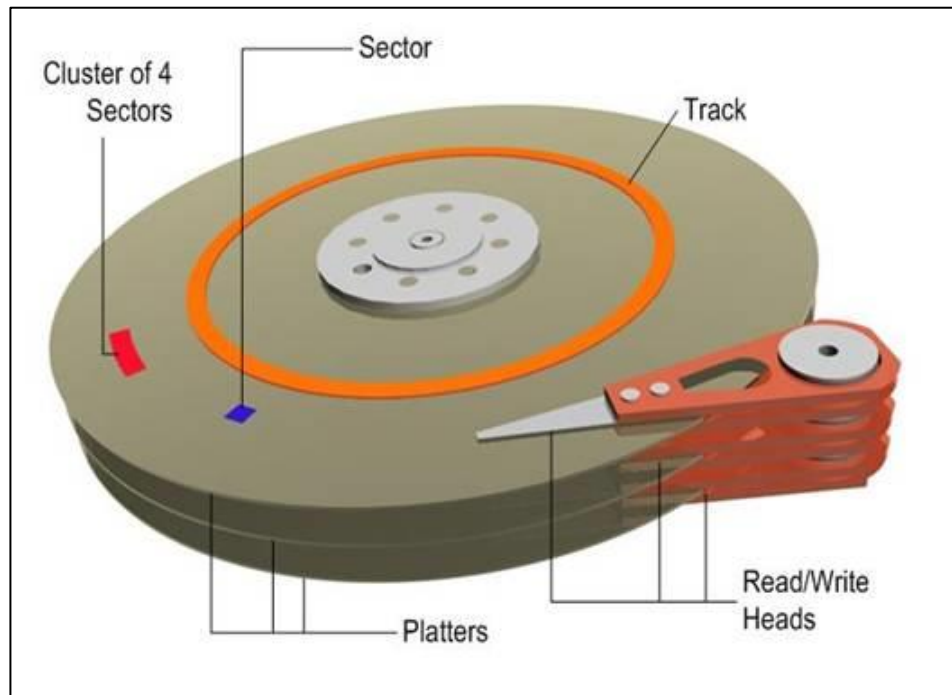
Like any mechanical device, a computer hard drive can physically fail. The most common failures are:

- **Head crash**: Where the read/write heads make contact with the platter surface. This can present as a grinding or whining noise.

- **Failure of the drive spindle / motor mechanism**, used to rotate the platters;

- **Failure of the "actuator arm"** used to move the read/write heads over the drive. This can present as a loud clicking noise caused by the actuator arm striking the inside of the drive case.

In these situations the drive should be immediately powered down and assistance sought from a hardware data recovery service. Continued use of a drive in these situations can lead to greater physical damage and permanent data loss.

Another common hardware failure is **loss of power to a drive**. In the case of external USB drives this problem may be addressed by swapping the drive into a different

USB case. However an equally common cause of a power failure is a short circuit in the drives printed circuit board (PCB). Whilst it is possible to swap a faulty PCB with an identical replacement, it is recommended that inexperienced users have this be performed by a hardware data recovery service.

SOFTWARE RECOVERY

A "logical hard drive structure" refers to the configuration of the hard drive to store data. The principle logical drive structures are:

Partition

> When a hard drive is configured to store data, a "partition" is created. The partition acts as the container for the file-system and files. A hard drive can contain one or more partitions.

File-system

> A partition is formatted with a file-system. Once this takes place the partition is allocated a drive letter, e.g. "D:" Most Windows booting hard drives will be formatted with Microsoft's NTFS (New Technology File-system). However, external USB devices, including camera cards, are usually formatted with the older FAT (File Allocation Table) file-system. This is primarily for compatibility reasons as a FAT file-system can be read by Macintosh computers whereas NTFS cannot.

> The task of the file-system is to keep track of individual files created and stored on the drive. To do this the file-system uses an index at the start of the drive which records the name and location of all files and folders on the drive.

File Storage

> The smallest unit of storage space on a hard drive is a sector. Windows groups sectors into "clusters" into which individual files are stored. A file may occupy one or more clusters depending on its size. A file may be in contiguous clusters, or it can be fragmented and stored in different parts of the drive. The file-system is responsible for tracking the location of the data for each file.

These structures are summarized in Figure 2 below:

Figure 2, hard drive structure
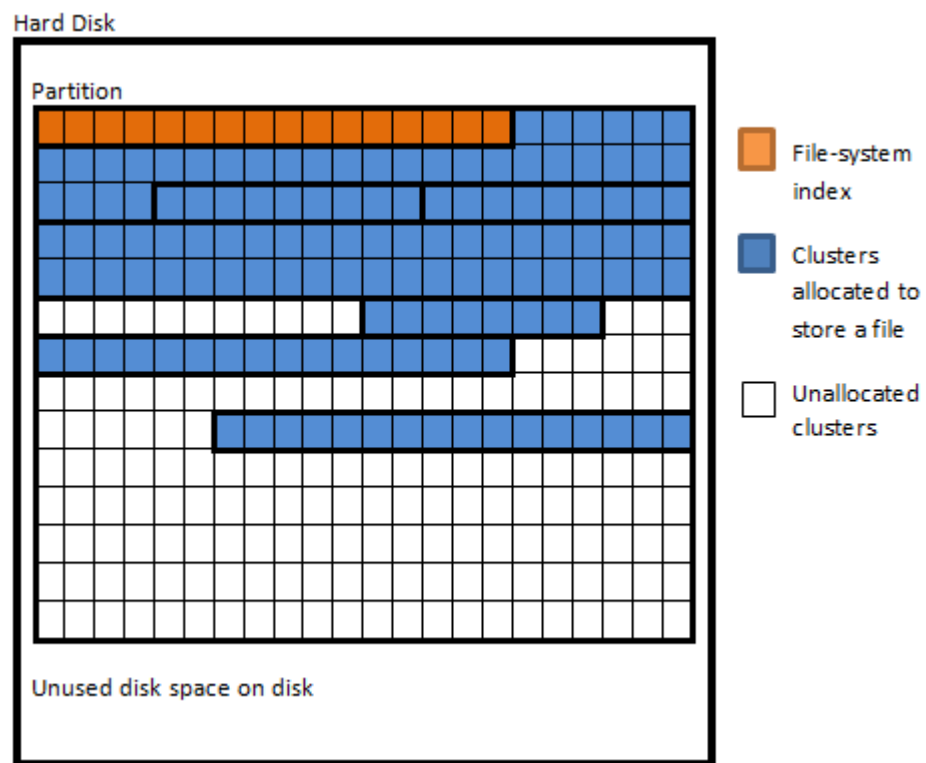
Software data recovery deals with data loss at a "logical" level, meaning that whilst the hardware is working correctly, a software problem (e.g. an accidental format) has caused files to go missing.

PARTITION RECOVERY

A partition error usually manifests itself in a drive letter that suddenly disappears and a drive becomes blank, RAW or unallocated.

The highest level of recovery performed by Recover My Files is to locate and read a missing or damaged partition. If successful, partition recovery is very fast; because once the missing partition is identified the entire contents of the partition become available.

FILE-SYSTEM RECOVERY

Deleted Files

When a file is deleted from a Windows computer the record for that file in the file-system index (the FAT or MFT) is marked to show that it is a deleted file. The clusters on the drive where the data for the file is stored are now considered unallocated (i.e. available for new storage). At this point in time, the deleted file can easily be located by reading the file-system index record, locating the list of deleted files, and going to the clusters to recover the data.

However, continued use of a computer after a deletion will lead to new data being written to the hard drive. If new data is written to the drive it is possible that:

- The record in the file-system index is re-used for a new file. If this happens, the original file name is overwritten and destroyed as the file name is only stored in the index and not with the file data; and/or,

- One or more of the clusters used to store the original file could be re-used for new data. If this happens, the original file content could become corrupt or totally overwritten and destroyed.

It is for this reason that following a deletion or loss of files, use of the hard drive should be kept to a minimum to avoid new data being written to the drive and to maximize the possibility of recovery.

File and Folder Structure Recovery

If an entire drive has been lost and a partition recovery (described above) is not successful, Recover My Files is designed to search for and rebuild the file-system index. This is particularly important as the file-system index is the only location where file and folder names are stored. Without recovery of the index, the original folder structure and files names will not be known.

Recover My Files searches for individual FAT and MFT records. At the end of a Recover Drive search, these records are rebuilt to display the file and folder structure in the search results screen. The records are used to locate the data on the drive and recover the files.

FILE CARVING FOR LOST FILES

In some data recovery situations partition and file-system recovery is not possible (because the partition, file-system, or individual file-system records have been corrupted or destroyed). In such cases it is possible to recover data by "**File carving**" for "**Lost Files**".

File carving is a well-known data recovery technique used to describe the identification and extraction of file types from unallocated clusters using file signatures. A file signature is *"a constant numerical or text value used to identify a file format or protocol"* (1).

An example of a file signature is shown in Figure 22-6, which is the beginning of a .jpg file in Hex view:

Figure 3, View of .jpg file header

```
ÿØÿà..JFIF.....´.´..ÿá:4Exif..MM.*......
...........ž...........¨................
.......ª...........°.(............1...../
...Â.2..........ò............‡ì..........
Ä¥.....Ð..&>ÆÒ.....@..'...'NPanasonic.DM
C-TZ15.....´........´....Microsoft Window
s Photo Gallery 6.0.6001.18000..2009:07:
19 15:39:02..#,š..........°,.........¸^"
..........^'....... ........0221.....
```

The object of carving is to identify and extract (carve) the file based on this signature information alone. Carrier (2005) describes File carving as:

> *"…a process where a chunk of data is searched for signatures that correspond to the start and end of known file types. The result of this analysis process is a collection of files that contain one of the signatures. This is commonly performed on the unallocate space of a file-system and allows the investigator to recover files that hav no metadata structures pointing to them". (2)*

File carving has both advantages and limitations. These include:

File-system independent

> File carving is essentially file-system independent. A file type will exhibit the same file signature and structure under FAT, NTFS, HFS, EXT2 or other file-systems and can be data carved accordingly.

Time Required:

> A drawback of file carving is that it can take a considerable amount of time to process a large drive. Also, the greater the number of file signatures searched for simultaneously, the more processing required and the longer the search.

Data Fragmentation:

> Without file-system records, it is impossible to track fragmented files. Fragmented files may return as invalid as only the start of the file is located.

No Original File Names

> As file names are stored only as part of the file-system, data carved files cannot be recovered with their original name.

File carving in Recover My Files

In Recover My Files carved files are represented by a carving knife icon. Files are given the naming convention "LostFile_FileType_SectorLocation.xxx". For example, "LostFile_JPG_904063.jpg", which shows that the lost jpg file has been carved from sectors on the drive beginning at sector 904063.

If the file end is not found, but sufficient information is found within the file to suggest it will at minimum be partially recovered, it is assigned a default file size according to that file type. The global default size of lost files can be set in the OPTIONS > SEARCH window (see Chapter - 12.2).

Chapter 1 - Recover My Files v6

In This Chapter

1.1   WHATS NEW IN RECOVER MY FILES V6?

Recover My Files v6 includes major new features:

- **Improved partition recovery**. Faster recovery speed and better validation of duplicate or invalid files.

- New file type signatures for **File carving**.

- Faster **saving and loading** of search results.

- **Automatically validate** search results.

- Powerful new user interface:

    o **Separate views** to group data by **extension, status and date**.

    o **Sort** and **multi sort** files by attributes: name, extension, path, size and date.

    o **Branch plate** to list files from multiple folders.

    o **Text filter tool** to quickly filter search results and find relevant files.

    o **Gallery view** to thumbnail graphics files.

    o **Text** and **Hexadecimal*** views to examine raw data.

    o **Improved file preview**. 300+ supported types with Zoom, rotate, copy, and search.

    o **Multi-screen** support with detachable windows.

    o Save and load **custom screen layouts*.**

- **Create drive images** in DD, E01 and AFF format.

(* Feature requires the Professional or Technician software license option)

1.2   INTRODUCING RECOVER MY FILES V6

Recover My Files v6 is data recovery software written by GetData Pty Ltd and available for download from www.recovermyfiles.com.

First released in 2002, Recover My Files version 6 is the result of more than ten years of ongoing development. In that time Recover My Files has been translated into 9 different languages and is sold in retail channels in countries including the USA, Germany, France, Japan, UK, and Holland. Since 2002 Recover My Files has sold more than 500,000 licenses worldwide.

Who uses Recover My Files?

Recover My Files is primarily purchased by home users for use on computers, cameras

and other media devices. It enables cost effective data recovery at a fraction of the price of a commercial data recovery service.

Recover My Files is also widely used by business. It is recommended recovery software by support services companies including DELL, IBM and HP. In 2012, USA retail chain Office Depot rolled out Recover My Files nationwide to their tech services department to perform data recovery services for its customers.

Recover My Files was originally developed for use by law enforcement in computer forensics. Today it is widely used by law enforcement agencies worldwide including the FBI, the USSS and the UK Metropolitan police.

What makes Recover My Files different from other data recovery products?

Recover My Files uses advanced partition recovery and File carving techniques. It combines a flexible graphic user interface (GUI) with advanced sorting, filtering, and searching technology. It enables access to all areas of physical, logical and disk imaged media, including Windows System files and unallocated drive space.

Recover My Files is designed with the following key principles:

- To enable a user to **accurately determine if their files can be recovered** prior to purchasing a license. This is primarily achieved via the display window which shows the content of files found.

- **It will not alter the contents of a drive being searched**. Recover My Files is designed as a data recovery tool, NOT a drive repair tool. It will not write to or change the content of the original hard drive. If Recover My Files is not the solution, the user can seek a new solution without any change to the status of the problem drive.

1.3   WHEN CAN RECOVER MY FILES BE USED?

Recover My Files is ideal for recovery of:

- Deleted Files (including files emptied from or bypassing the Windows Recycle Bin);

- Missing files lost through the corruption of a Windows file-system;

- Formatted Drives;

- RAW Drives;

- Corrupt Drives;

- Unallocated Drives;

- Missing Drive Letters;

- Data lost through a Windows Operating System reset or reinstall.

1.4   ON WHAT TYPE OF MEDIA CAN RECOVER MY FILES BE USED?

Recover My Files will work on all types of computer storage media. This includes:

- Hard drives, including external USB drives

- USB sticks, Thumb Drives, Pen drives or other USB media

- Camera cards

- Hardware and software RAID (JBOD, RAID 0,1,5)

- iPods, MP3 players and Dictaphones

Or any other storage device which is shown under windows as a hard drive (Recover My Files v6 does NOT support recovery from iPhone or iPad hard drives as Apple restrict access to these devices).

1.5   SUPPORTED FILE-SYSTEMS

Recover My Files v6 has full Unicode support and can recover files created in any language.

Recover My Files supports the recovery of:

- Windows FAT12/16/32/exFAT, NTFS, file-systems;

- Macintosh HFS, HFS+ file-systems;

1.6   SUPPORTED DRIVE IMAGE FORMATS

Recover My Files supports the analysis of the following drive image formats:

- DD or RAW;

- EnCase®.E01;

- Safeback® v2;

- Forensic File Format .AFF

- SMART®

- VMWare®

- ProDiscover®

- Microsoft VHD

- Apple DMG.

Chapter 2 - Evaluating Recover My Files

In This Chapter

CHAPTER 2 – EVALUATING RECOVER MY FILES

2.1   RUNNING IN EVALUATION MODE

You are encouraged to download Recover My Files and run it in evaluation mode free of charge. The search results screen enables the user to see the content of files found (i.e. view the pictures and read the documents). An example is shown in Figure 4 below.

The software that you download and run in evaluation mode is the FULL VERSION. The only limitation in evaluation mode is that it is not possible to save files.

If, **based on the search results**, you decide that you wish to **save files**, then **purchase a product activation key**, enter it into the program, and save the files to another drive. You do not need to run a second search once you have purchased a key.

Purchasing and activating Recover My Files does not change the search results. The only function of the product activation key is to enable the ability to save files.

For more information, see 10.1 - Validating a successful recovery.

Figure 4, Recover My Files running in evaluation mode and previewing search results
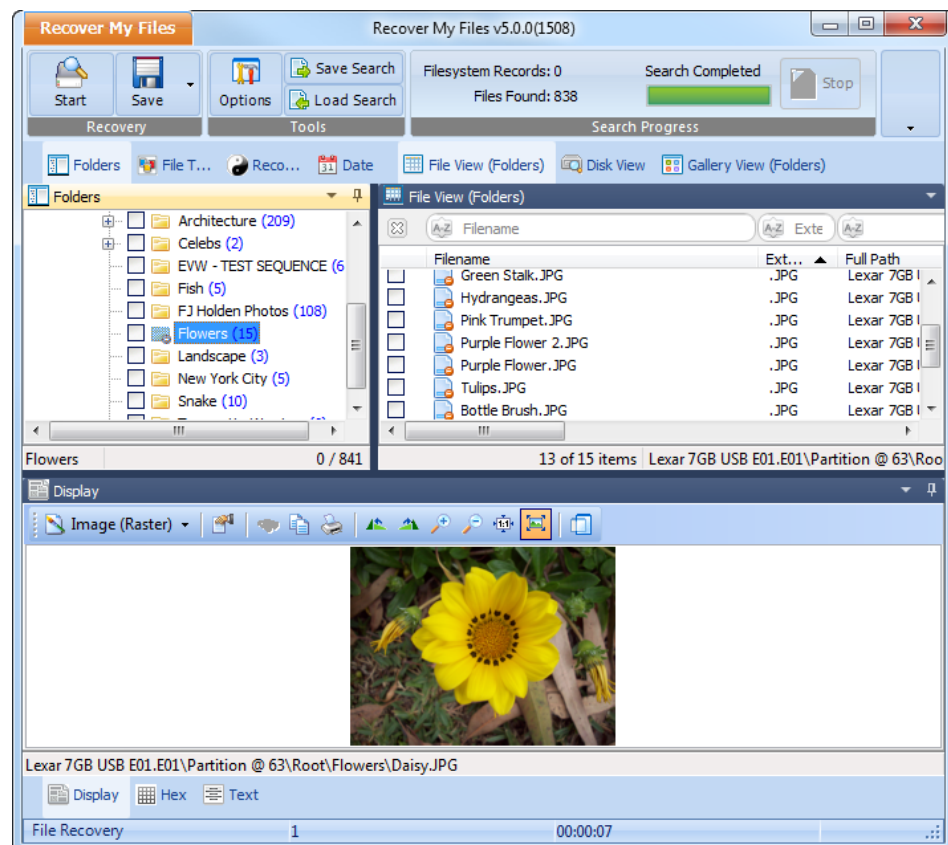
Chapter 3 - Installation

In This Chapter

Page | 2 5

3.1   WHERE SHOULD I INSTALL RECOVER MY FILES?

If you have suffered a data loss, you should, if possible, **avoid writing new data to the storage media on which the files were lost**. When new data is written to a storage media, it can overwrite and destroy deleted files so that they can no longer be recovered.

Avoid installing new programs, saving new files, or if it is digital camera media taking new photographs or video until you have had the opportunity to attempt data recovery. If you are dealing with a RAW or Unallocated hard drive, do not format the drive.

The best methodology, if possible, is to connect the problem drive to another computer as the secondary drive. This enables you to install your data recovery software on the C: drive of the 'good' computer, and then scan the secondary 'problem' drive to recover your files. This methodology makes it far less likely that Windows, or you, will write new data to the drive.

Of course this methodology is not always practical, as you may well have lost your files from your current C: drive and have no alternative than to continue to use Windows on this PC. If this is the case, limit your use of the computer until you have the opportunity to search for your deleted files.

Recover My Files is a small program (i.e. less than 20mb), so installation of the program onto the problem drive, whilst not recommended, is a small risk.

3.2   SYSTEM REQUIREMENTS

Recover My Files requires:

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

When performing data recovery on large drives a high specification computer is recommended.

3.3   DOWNLOAD

The latest version of Recover My Files is available for download from www.recovermyfiles.com or by using this direct download link http://download.getdata.com/RecoverMyFiles-Setup.exe.

The download is for the **full version** of Recover My Files. When run in evaluation mode it runs with all features active (other than the ability to save files). If the software is later activated with a purchased key, the type of license key purchased (e.g. Standard,

Professional or Technician) determines what features will be available once the program is activated. There is not a separate download link for different versions.

<div style="background-color:#4472C4;color:white;padding:4px;">

3.4   INSTALL

</div>

To install Recover My Files:

1. It is recommended that Recover My Files be installed using an **administrator** user account.

2. Run the installation file **RecoverMyFiles-Setup.exe**. You will be presented with the installation splash screen showing the version number, as shown in Figure 5 below:

Figure 5, Recover My Files setup splash screen

3. Click **Next** and follow the onscreen setup instructions.

The following windows will appear during the installation process:

1. Recover My Files License agreement. Answer the question and click **Next;**

2. Enter the correct installation path or accept the default path (**C:\Program Files\GetData\Recover My Files v6**) and click **Next;**

Figure 6, Installation: Program path

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

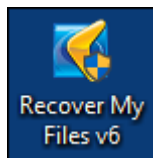**Figure 7, Installation: Finalize installation options**

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

Figure 8, Installation: Finish installation

5. Run Recover My Files from the installed desktop icon:

Figure 9, Recover My Files v6 Desktop icon

Or from the Windows programs menu: "Windows Start > All Programs > Recover My Files v6\Recover My Files v6".

Included with the installation is the drive imaging program Forensic Imager (see Chapter 14). Forensic Imager is also run from the Windows program menu: Windows programs menu: "Windows Start > All Programs > Recover My Files v6\Disk Imager".

3.5   UNINSTALL

To uninstall Recover My Files open the Windows Control Panel and in the "Programs" section use the "Uninstall option.

A successful removal will show the following message:

Figure 11, Successful un-install

3.5.1 DEACTIVATING RECOVER MY FILES

The uninstall process described above does not deactivate a license key. To deactivate a license-key follow the instructions in section 5.4.
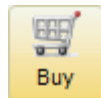
Chapter 4 - Purchase

In This Chapter

4.1 NEW PURCHASE

Recover My Files is available for purchase online, via purchase order, or resellers.

4.1.1 PURCHASE ONLINE

Recover My Files can be purchased online at http://www.recovermyfiles.com.

The purchase page can be accessed directly by using the "Buy" button in the program toolbar:

Figure 12, Recover My Files toolbar "buy" button

Please visit the purchase page for pricing, volume discounts and software bundle options. Full credit card and PayPal payment options are available.

DELIVERY OF THE SOFTWARE ACTIVATION KEY

Your software activation key is displayed on a **web page at the end of the purchase process** and is also sent to the purchase email address.

If there is a delay in your credit card provider authorizing the transaction, your software activation key will be provided only by email and only after credit card or PayPal authorization takes place.

DELIVERY OF A PURCHASED CD

For an additional $14.95 a CD can be purchased with your order. This price **includes shipping** worldwide. (Note: GetData is not responsible for any customs, excise, or import duty applied by other agencies). Your CD is produced on demand with the latest version at the time of your order. A CD is sent by regular post. Please allow 6-10 days for delivery.

SOFTWARE UPGRADE GUARANTEE

At the time of purchase GetData offer a "Recover My Files Software Upgrade Guarantee". This means that you can pre-purchase a key for the next major version release (i.e. v5 to v6) at a discounted price. When the next major version is released a key will be automatically sent to the purchase email address as well as being accessible by logging into the GetData site.

4.1.2   PURCHASE ORDERS

Purchase Orders are available to government and corporate entities. Approved customers may place purchase orders on 30 day terms.

Purchase Orders can be placed online at http://www.recovermyfiles.com/data-recovery-software-purchase.php by following the purchase order instructions in the checkout, or by directly 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

4.1.3   RESELLERS

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

4.2 TYPES OF LICENSE

Recover My Files v6 has three license types: Standard; Professional; and Technician. Each license is sold with a **software activation key** which is valid for installation on **two computers** (e.g. a desktop and a laptop).

4.2.1 STANDARD LICENSE

The Standard License has features suitable for most data recovery needs for Windows PCs, external drives, camera cards, iPods, MP3 players and other media.

4.2.2 PROFESSIONAL LICENSE

A Professional License has added features for more technically advanced recoveries and users. These include:

- RAID recovery (see Chapter 13);

- Macintosh HFS file-system recovery;

- Linux EXT2 file-system recovery;

- Hexadecimal data view (see 6.5.2);

- The ability to customize screen layout (see Chapter 15).

4.2.3 TECHNICIAN LICENSE

A Technician license has the features of the Professional version, but in addition to the software activation key, the Technician License comes with a **USB hardware activation dongle**.

The dongle contains its own key, making the license transportable from PC to PC. When the dongle is inserted into the USB port, Recover My Files is activated. When the dongle is removed, it returns to evaluation mode.

4.2.4   COMPARISON OF LICENSE FEATURES

The following table provides a comparison of license features. Note: Recover My Files has a single download. The software activation key controls the available features:

Features	Evaluation Mode	Standard $69.95	Professional $99.95	Technician $349.95
Save files		✔	✔	✔
Key **valid for 2 PCs**		✔	✔	✔
Recover deleted files	✔	✔	✔	✔
Recover drives	✔	✔	✔	✔
Preview and gallery	✔	✔	✔	✔
Text view	✔	✔	✔	✔
Branch plate view	✔	✔	✔	✔
FAT (EX,12,16,32,64)	✔	✔	✔	✔
NTFS (NTFS 3,4,5)	✔	✔	✔	✔
HFS, HFS+ (MAC)	✔	✔	✔	✔
Create disk images	✔	✔	✔	✔
Scan disk images	✔		✔	✔
RAID recovery	✔		✔	✔
Customize layout	✔		✔	✔
Hex view	✔		✔	✔
USB activation dongle Commercial use				✔

To upgrade between licenses, e.g. from a Standard to a Professional please contact sales@getdata.com.

4.3   UPDATES WITHIN VERSION PURCHASED

Updates to Recover My Files v6 are **free** (e.g. updates from 6.1 to 6.2). An update can be installed over an existing version. An update requires a restart of Recover My Files.

The latest version is available by:

- download from www.recovermyfiles.com;

- using the direct download link:
  http://download.getdata.com/RecoverMyFiles-Setup.exe; or

Click on the **Update** button on the program tool bar (requires an internet connection):

4.4   UPGRADE FROM A PREVIOUS VERSION

If you have purchased a previous version of Recover My Files (i.e. versions 1 - 5), you are entitled to purchase v6 at a discounted rate. To do this:

1. Visit www.recovermyfiles.com and access the login page via the "Account" link (or go directly to https://support.getdata.com/my/);

2. Login to your customer account using your purchase email address;

   a. If you do not know your password, use the "Forget your password" link and it will be sent to your email address.

   b. If you have changed your email address since your purchase, please contact sales@getdata.com for assistance.

3. Click on the Key tab to display your old orders and license keys;

4. Click the upgrade to Recover My Files v6 link;

5. Checkout via the shopping cart at the discounted price.

Your software activation key for Recover My Files v6 will be provided on a web page at the end of the purchase process. It will also be sent to the email address used in the purchase.

For further assistance, contact sales@getdata.com.

4.5   UPGRADE BETWEEN VERSIONS (E.G. STANDARD TO PRO)

It is possible to upgrade an existing license, e.g. from a Standard to a Professional. Please contact sales@getdata.com for assistance.

The new software activation key is entered by selecting the "Upgrade" button in the program toolbar:

Recover My Files must be restarted for the upgraded features to become available.

Chapter 5 - Activation

In This Chapter

5.1   SOFTWARE KEY ACTIVATION - HOW IT WORKS

A license of Recover My Files is sold with a **software activation key**. The key is valid for activation on **two computers** (e.g. a desktop and a laptop). For more information on license options, see 4.2, "Types of License".

Recover My Files uses a **hardware lock activation system**. Each computer is identified to the GetData activation server by a "**hardware ID**", a unique number calculated using specific internal hardware components of the pc.

The license may be installed an unlimited amount of times on an activated computer. Even if it is necessary to enter the key into the software again, it does not count as an activation (as long as the hardware ID does not change).

5.1.1   MAXIMUM ACTIVATIONS REACHED

When an attempt to activate a license on a third computer is made (i.e. a computer with a new hardware ID), the activation server will return the message "max activations reached".

If you need to install Recover My Files on multiple computers a Technician license is the best option. In addition to the two software activations, a USB hardware activation dongle is provided. This makes the license portable as the dongle can be moved from PC to PC. When the dongle is inserted the software is activated, when it is removed, the software returns to evaluation mode. Should you wish to upgrade to a Technician license please contact sales@getdata.com.

5.2   ONLINE ACTIVATION

Activate Online where the computer on which the software is being installed is connected to the internet.

1.   Click the "Activate" button on the tool bar of the main program screen to open the program activation window:

2.   Select **Online** Activation and click **Next**:
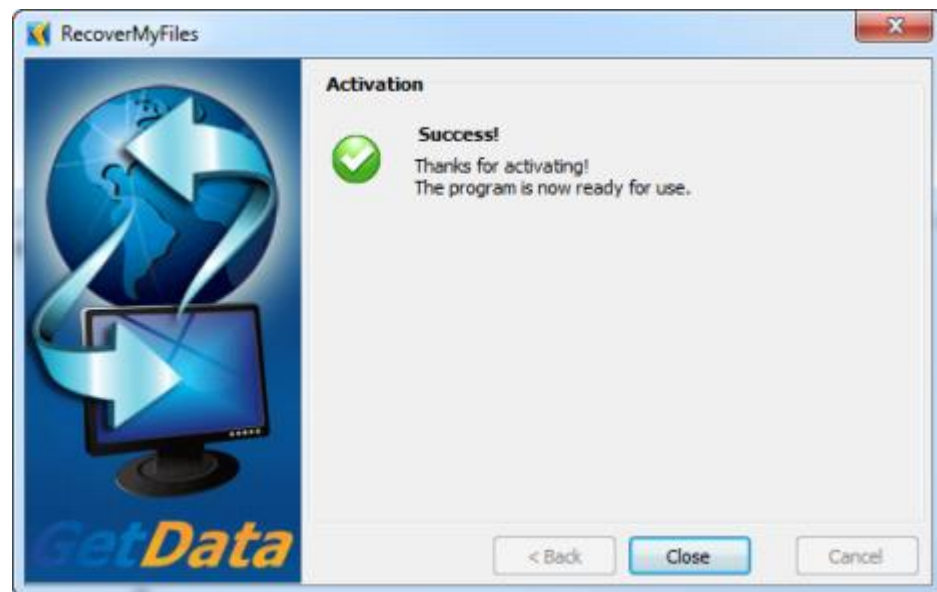
Figure 13, Online activation wizard

3. **Enter the license key** that you received with your purchase (the license key was displayed on a web page at the end of the purchase process and also sent to the email address provided in the order). Click **Next**:

Figure 14, Enter license key

4. The following screen shows a successful activation:

Figure 15, Successful activation message


5.2.1   TROUBLESHOOTING ONLINE ACTIVATION

If the software does not activate, it usually relates to a problem in communicating with the GetData internet activation server. The most common reasons for this are a firewall or proxy server:

Figure 16, Online activation blocked by firewall or proxy server
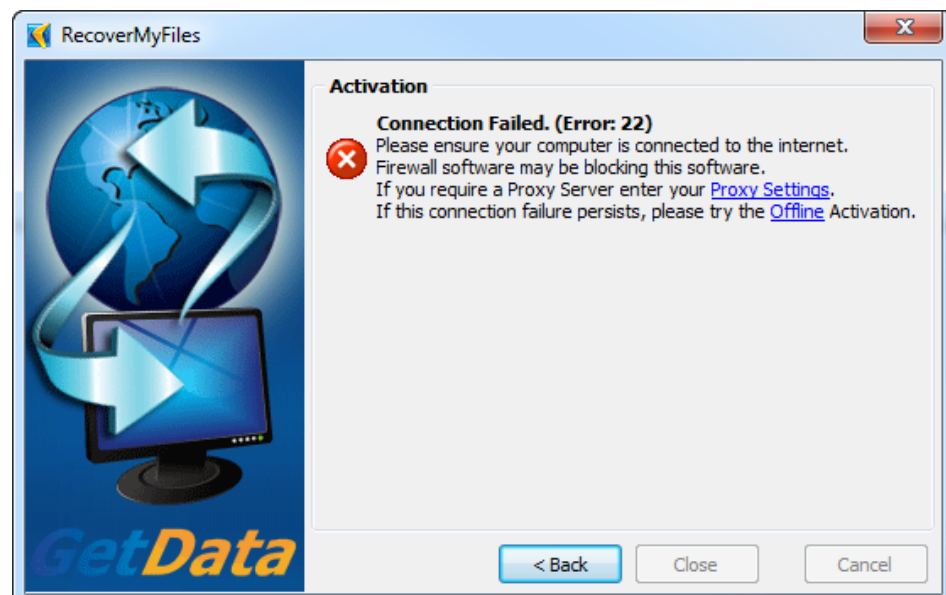
Please adjust your firewall settings and try again. If you are blocked by a proxy server, click on the "proxy settings" link (shown above) and enter the required settings into the following window:

Copyright GetData 2002 - 2017, All rights reserved.
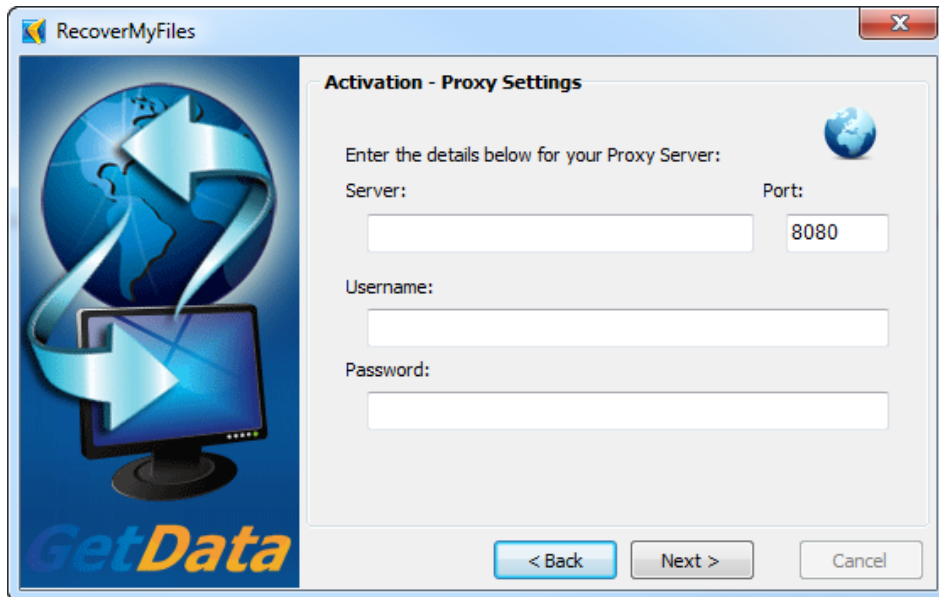
If you are still unable to activate online, please try the offline activation method described below. If problems persist, please contact technical support quoting the exact activation error message.

5.3   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 18, Offline activation wizard
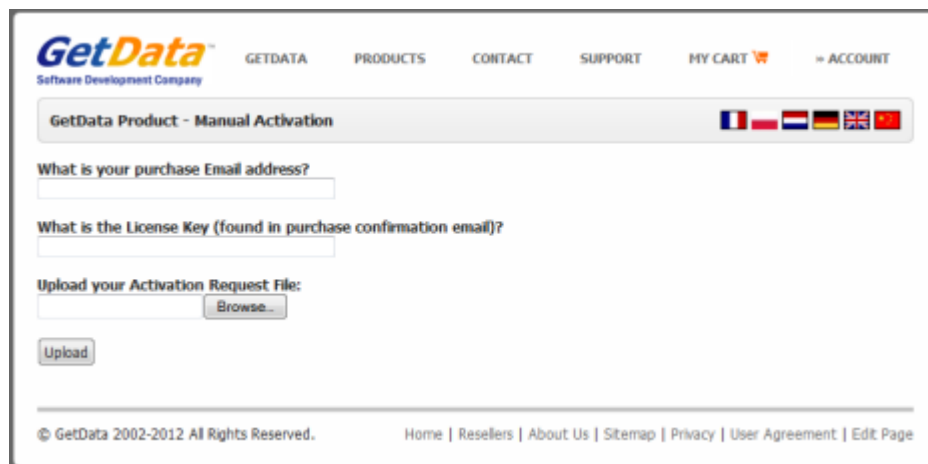
2. Click on the Export button to export and save the license file "GetData.GDActRequest":

Figure 19, Offline activation (evaluation version), export of license file

3. Using a web browser on any internet connected computer, go to https://support.getdata.com/offline-wibu.php and enter the required details:
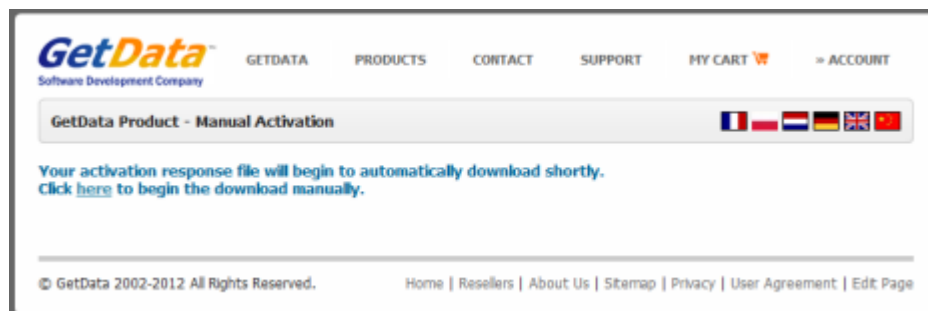
Figure 20, Offline activation (evaluation version), upload of license file and activation details

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.

Figure 21, Offline activation (evaluation version), download of license file

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

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:

5.3.1   TROUBLESHOOTING OFFLINE ACTIVATION

Some web browser security settings may prohibit the upload or download of the "GetData.GDActRequest" and/or "GetData.GDActResponse" files. If upload or download is blocked:

1. Try an alternate web browser, e.g. Firefox or Opera; or

2. Send the "GetData.GDActRequest" file to support@getdata.com and we will generate and return the "GetData.GDActResponse" file to you.

5.4   DEACTIVATING A SOFTWARE KEY LICENSE

A software license key is valid for concurrent installation on two computers (e.g. desktop and a laptop). To move a software key to another computer it is necessary to deactivate and existing installation (if both activations have been used) to free a license.

To de-activate the software on a computer, follow these instructions (an Internet connection is required):

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

2. In the left-hand column of the License Manager click on the picture of the "GetData Virtual CmStick".

3. Under the Product list click on the entry for Recover My Files.

4. 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, the software should no longer appear under products. You can then apply this key to a different computer.

5.5   DONGLE ACTIVATION (TECHNICIAN LICENSE)

A Recover My Files Technician license is sold with a **software activation key** and **a USB hardware activation dongle**.

The dongle contains its own activation key. It essentially makes the license portable as the dongle can be moved from PC to PC. When the dongle is inserted the software is activated, when it is removed, the software returns to evaluation mode. Should you wish to upgrade to a Technician license please contact sales@getdata.com.

5.5.1   IDENTIFYING YOUR RECOVER MY FILES DONGLE

Your Recover My Files dongle is a Wibu CodeMeter brand. It is identified by the serial number on the USB insert section, as shown in Figure 15 below:

Figure 23, Recover My Files Wibu Codemeter dongle showing serial number

5.6   LOST KEY

Lost software activation key

To locate your Recover My Files activation key, log into your GetData customer account. Either:

- Visit www.recovermyfiles.com and click on the **Account** link; or,

- Go directly to https://support.getdata.com/my/

Where you can locate a record of your purchase, including your activation details. If you do not know your account password, use the "forgot your password" link. To change your purchase email address, please contact support@getdata.com.

Lost Dongle

To replace a missing activation dongle, contact sales@getdata.com. A replacement fee may apply.

Chapter 6 - User Interface

In This Chapter

6.1   INTRODUCING THE RECOVER MY FILES V6 INTERFACE

The Recover My Files Graphic User Interface (GUI) is broken down into the following areas:

1.   Toolbar (top)

2.   Tree pane (left)

3.   List pane (right)

4.   Display pane (bottom)

5.   Status bar (bottom)

As shown in Figure 24 below:

Figure 24, Recover My Files main screen

The Recover My Files v6 GUI is however **highly configurable**. The Tree, List and Display panes hold different "**data views**" used to present search results to the user. Each of the data views can be moved and re-attached to the other pane, or completely detached from the main program screen. Customized screen layouts can be saved and loaded as required. Refer to Chapter 15 for further information on customizing the interface.

6.2   TOOLBAR (TOP)

At the top of the program tool bar is the Recover My Files drop down menu, shown in Figure 25 below:

Figure 25, Recover My Files drop down menu

The drop down menu contains the following unique functions:

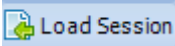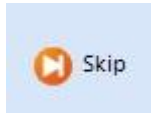**Export CSV file**:   Exports the listing of current search results to as CSV file.

Print Report: Prints a listing of the current search results to an installed printer. A confirmation message is displayed showing the number of pages that will be printed.

Disk Imager: Runs the disk imaging program used to acquire sector copies of drives. See Chapter 14 – Drive Imaging.

Exit: Closes Recover My Files. A confirmation prompt is provided if search results are currently listed.

The other functions in the drop down menu are replicated in the toolbar icons, described as follows

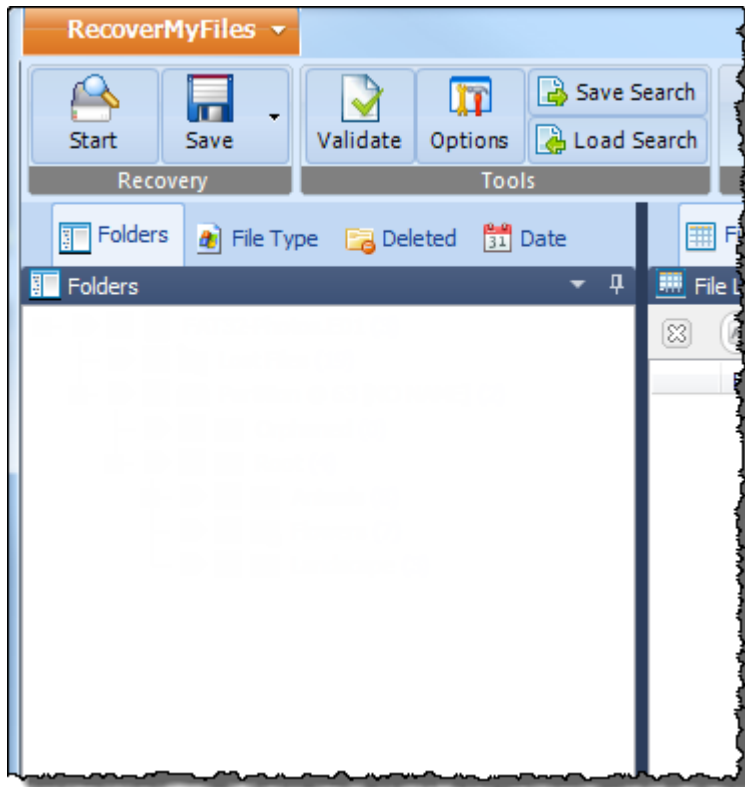|	
	Opens the start search wizard.
	Opens the save dialogue to save search results. See Chapter 10 – Saving Files.
	Runs the File Type Validation Tool

Options	Opens the program options window. See Chapter 12 - Options.
Save Session / **Load Session**	Used to save and load a listing of search results. See Chapter 10 – Saving Files.
Skip	Used to stop the progress of a search.
Update	Checks for program updates. An internet connection is required.
About	Opens the program "about" window, which contains version, activation and support information.
Help	Opens this support documentation.
Buy	Links to the program purchase page at www.recovermyfiles.com
Activate	Opens the program activation window. Also used to upgrade between licenses, e.g. Standard to Professional.

The toolbar is also the place where search progress is reported to the user. Messages relating to the current search are displayed with the progress bar.

6.3   TREE PANE (LEFT)

The Tree pane is the top left hand window of the search results screen.

Figure 26, Tree pane

The tree pane is the default location for the data views Folders, File Type, Deleted and Date.

Navigation

To navigate the Tree pane data views:

• Use the keyboard arrow keys to traverse, expand and contract a tree;

• Double click a folder to drill down into its sub folders;

• Click the ⊞ and symbols to expand and contract the tree hierarchy;

• Right click and use "Expand" to expand the currently selected folder, or "Expand All" to expand all folders; use "Contract" to contract the currently selected folder, or "Contract All" to contract all folders.

Clicking on a folder in the Tree pane data views lists the contents of the folder in the adjacent List pane (described in 6.4 below).

Tree Pane Icons

The following icons are used in the Tree pane data views:

A device, e.g. a hard drive or camera card

Active (booting) partition

Partition

An expandable branch (folder structure)

An active folder

A deleted folder

Selection Box

Folders listed in the Tree pane data views are preceded by a **selection box** ☑. The selection box is ticked to indicate that a file or folder is to be saved (Learn more about saving files in Chapter 10). A tick in a selection box for a file or folder will also show in any other data view in which that file is displayed.

Branch Plate   **NEW**
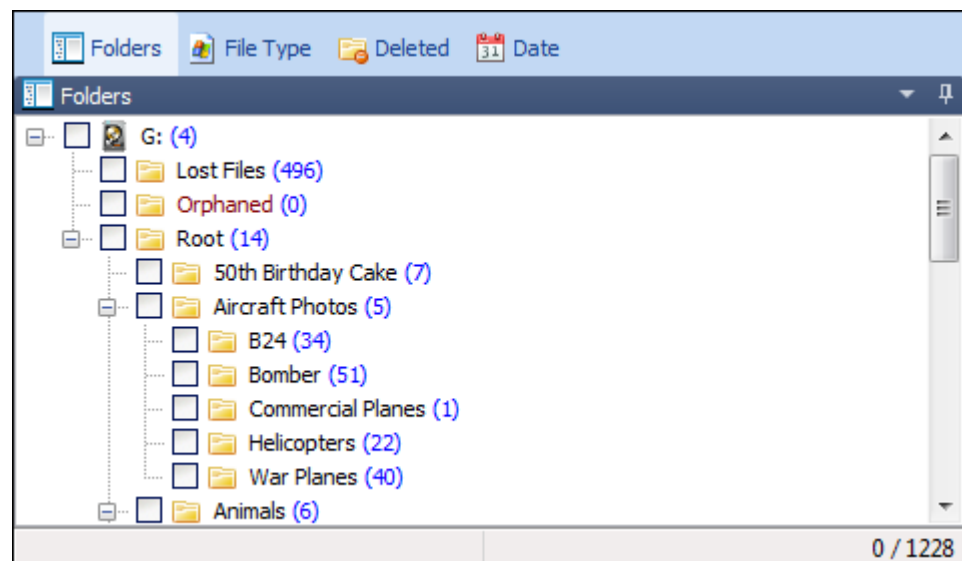
A powerful feature of the Tree pane data views is the "**branch plate**" . The branch plate allows the entire contents of a folder and its subdirectories to be displayed in a list in the adjacent list view. (Learn more about branch plating in Chapter 12.1.1).

6.3.1   FOLDERS VIEW

Folders view displays all the folders on the examined drive:

Figure 27, Tree pane, Folders view

Elements in Folders view include:

📁 Lost Files

> The Lost Files folder contains the results of File carving (See Data Recovery Fundamentals at the start of this manual for more information). The Lost Files folder is created in both a Recover Files (for "deleted and lost files") and a Recover Drive search.

💾 Partition @ [Sector Number] (Recover Drive search only)

> A partition appears in a Recover Drives search only. This is a partition which exists on the hard drive and is not missing or deleted. Folders and files in this partition (which are not deleted, lost or orphaned), should be accessible with Windows Explorer.

📁 Orphaned

> Orphans are deleted folders and files for which the original parent folder is unknown.

📁 Root

> The Root folder (also referred as root directory) is the first level folder of a folder hierarchy. A root folder will exist in both an existing and a recovered partition.

📁 Recovered [File-system] Partition @ [Sector Number] (Recover Drive search only)

> A recovered partition folder is created in a Recover Drive search only. Its name describes the type of File-system that has been found, and the sector number where it is located. This is where missing file and folder structure will be found in a drive recovery.

6.3.2   FILE TYPE VIEW

The File Type view sorts files by extension. This view shows all files on the examined drive.

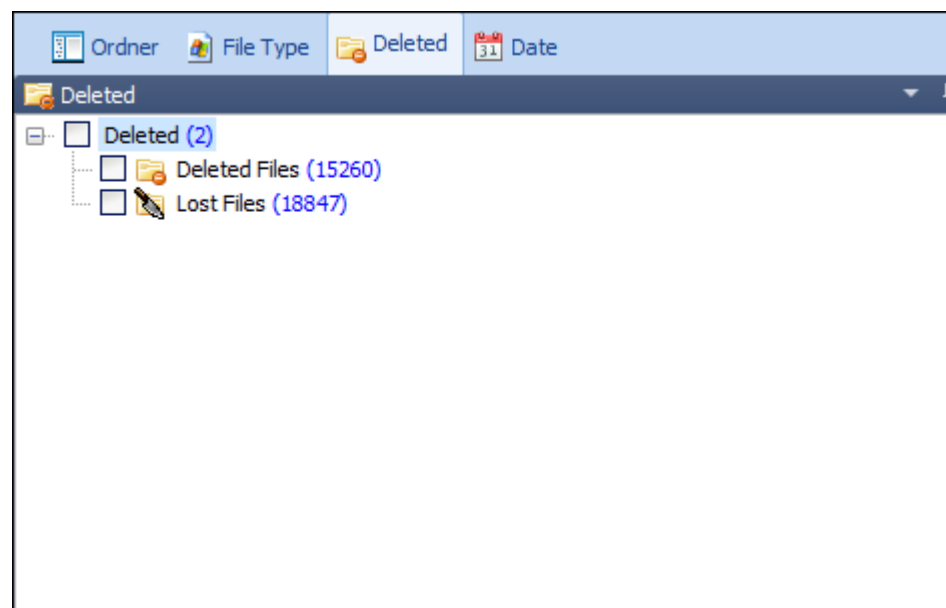**Figure 28, Tree pane, File Type view**
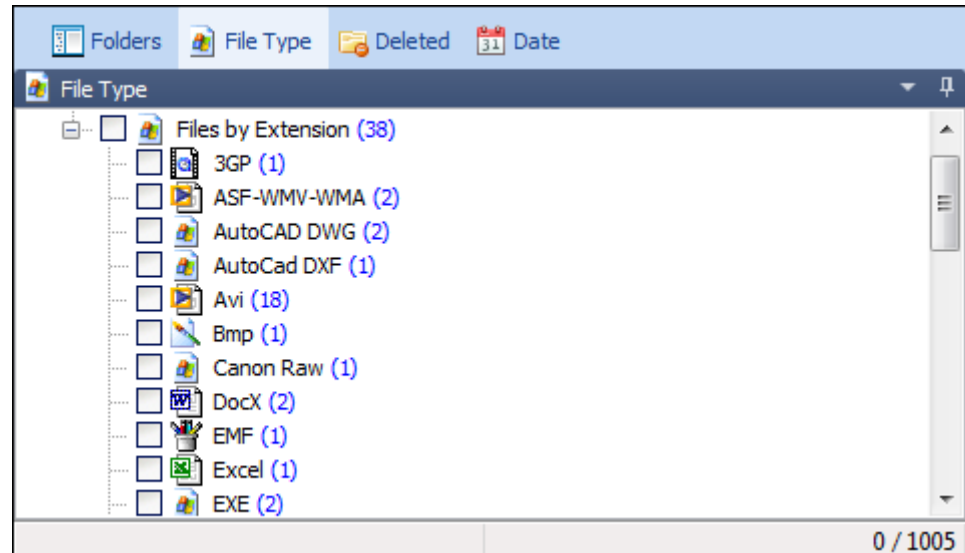
6.3.3   DELETED VIEW

This view shows those files marked by the file-system as deleted and the lost files carved from the free space.
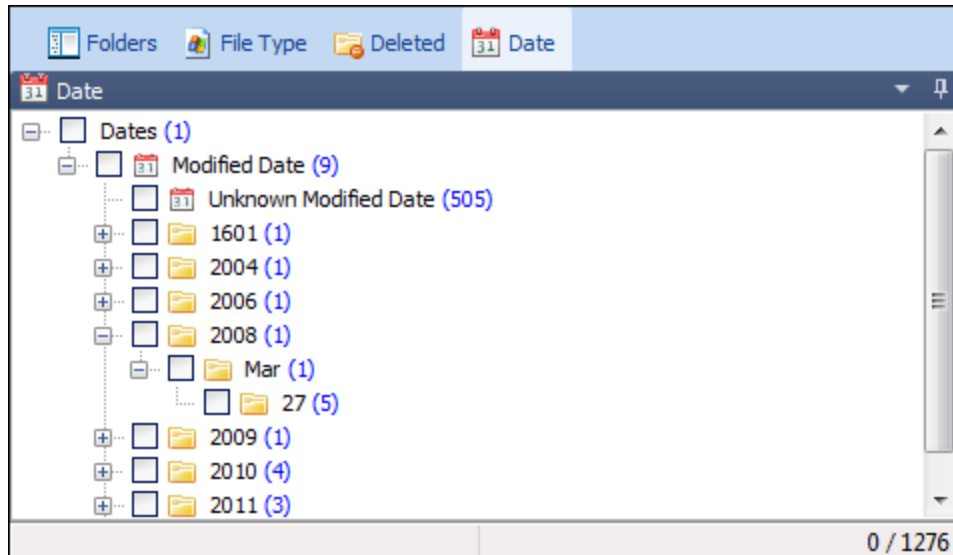
Figure 29, Tree pane, Deleted view

6.3.4   DATE VIEW

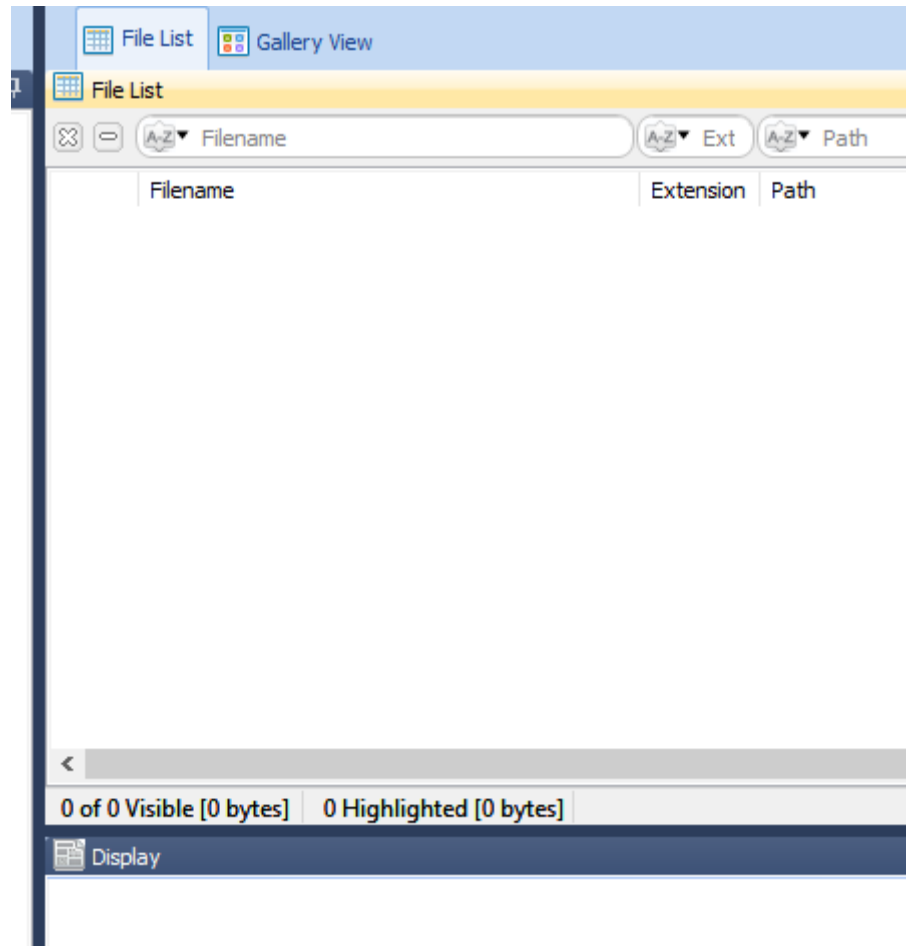The date view sorts files by date, grouping by year, month and day. This view shows all files on the examined drive.

Figure 30, Tree pane, Date view

6.4   LIST PANE (TOP RIGHT)

The top right window of the Recover My Files v6 screen is the "List" pane. The List pane is the default location for **data views:** File List and Gallery View.

Figure 31, List pane

To **navigate** in the List pane:

•   Use the keyboard arrow keys to move up and down the list;

•   Double click a folder to drill down into its sub folders; or

Files in the List window are preceded by a **selection box** ✅. The selection box is ticked to indicate that a file or folder is to be saved. A tick in a selection box for a file or folder will also show in any other data view in which that file is displayed. Learn more about saving files in Chapter 11.

6.4.1   FILE LIST

File List lists the file name and metadata (extension; size; path; modified, created; etc.) of the currently highlighted folder/s in the Tree pane. The Tree pane view name is

appended in brackets (e.g. "File View (Folders)" in Figure 32 below) to identify the source of the list.

File view is also the window in which a sort or filter is applied (described further below).

Figure 32, List pane, File view
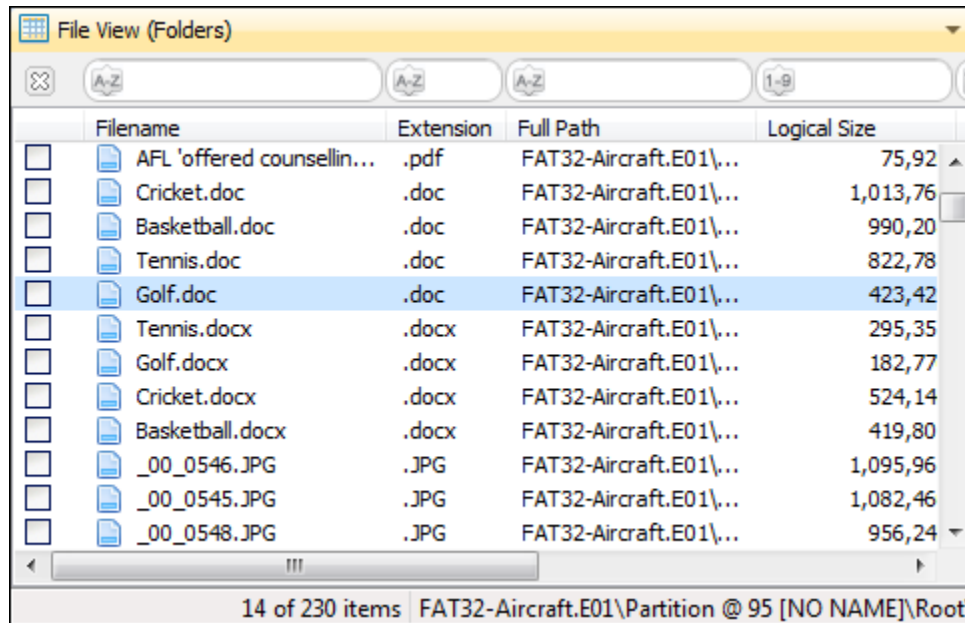
The following icons are used in File view:

	Free space on drive (Space on the physical drive which is not in use)
	Free space in partition (Space inside a partition which is not in use)
	Unallocated clusters on FAT volume
	Unallocated clusters on NTFS volume
	An active file
	An active folder
	A deleted file
	A deleted folder
	A system file
	A lost file

The following metadata columns are used in File List:

File Name:	The name of the artifact (system file, partition etc.) or the name of the file.
Extension:	The suffix to the file name, for example .jpg, which indicates the file format. This column reports the given file extension only and does not validate it as correct.
Is Deleted	The state of the file. A deleted file shows a state of "Yes" in this column.
Full Path:	Displays the full location of the file.
Logical Size:	The size of the file in bytes.
Modified:	The date and time that a file was opened, edited, and saved.
Created:	The date and time a file was created in its current storage location (not necessarily the original creation date of the file itself).

SORT
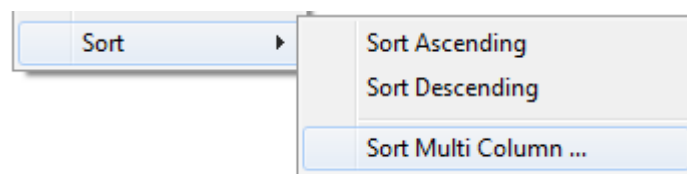
To sort by a **single column**, double click on the column heading, e.g. "Filename". An arrow will appear showing the direction of the sort. Double click again on the column heading to reverse the sort:

Figure 33, Single column sort

The same single column sort result can be achieved by right clicking on the column, selecting the "Sort" menu item and selecting to "Sort Ascending" or "Sort Descending":

Figure 34, Multi column sort menu
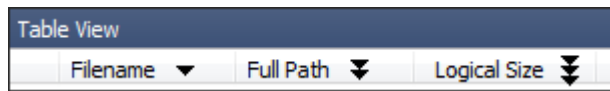
To sort by **multiple columns** using the CTRL key:

1. **Double click on the first column heading**, e.g. "Filename". An arrow will appear showing the direction of the sort. Double click again on the column heading to reverse the sort;

2. **Hold down the SHIFT key** on the keyboard;

3. **Double click on the second column heading**, e.g. "Filename". A double arrow will appear to indicate that it is the second column in the sort.

4. Continue to add columns to the sort by following steps 1 to 3 above.

Figure 35, Sort by FileName, then Full Path, then Logical Size

The same results can be achieved with the right click menu:

1. **Right click in the List view** and select: **Sorting** > **Sort Multi Column.** The "Sort Column Selection" window is displayed:

Figure 36, Multi column selection window

Visible columns are shown in the left hand window:

2. Select the required sort columns;

3. Add the required sort columns to the right hand window;

4. Use the "Move Up" and "Move Down" buttons to set the order on which to sort the columns;

5.   Click the "Sort" button to apply the sort.
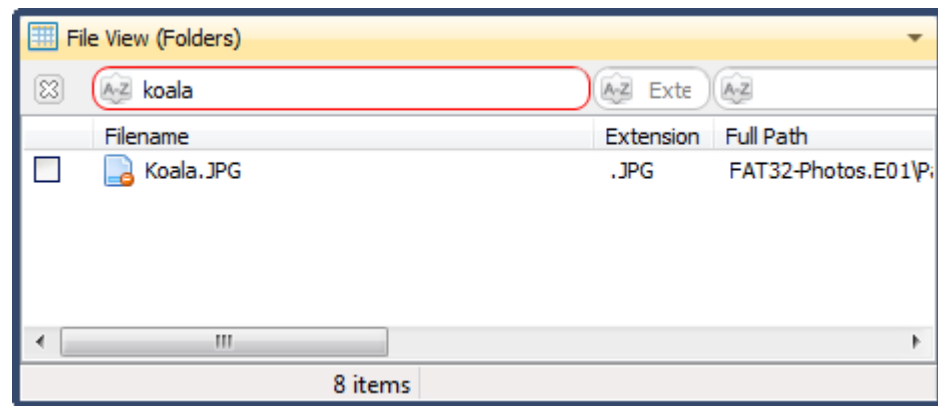
To remove a multiple column sort:

Release the SHIFT key and double click on a column heading to return to a single column sort.

TEXT FILTER

The **text filter tool** is applied in List view and allows instant text filtering on column data. It is situated above the List view column headings. When the filter is applied, the outline of the filter box/s turns red in color, as shown in Figure 37 below;

Figure 37, Text filter tool

The text filer tool is visible by default. To show or hide the tool:

1.   Right click on the File view window;

2.   From the drop down menu, select "Text Filter Tool":

To **apply a text filter**:

1.   Type into the filter field above the column heading:

   i.   ⌐A-Z⌐ Requires A-Z characters;

   ii.   ⌐1-9⌐ Requires numbers 1 - 9;

   iii.   ⌐8⌐ Requires a date format.

2.   As text is typed into the filed the displayed content updates based upon the typed criteria.

To **apply multiple column text filters**:

1. Enter the filter criteria into the field above each column heading. Multiple text filters are joined with the "and" operator.

To **remove a column filter/s**:

1. Remove the text from each text filter field used; or

2. Close the text filter by clicking the ⊠ icon in the checkbox column heading.

6.4.2   GALLERY VIEW

Gallery view is used to thumbnail graphics files (jpg, bmp and png) in the currently highlighted folder/s.

Figure 38, Gallery view thumbnails

Graphics displayed in Gallery view are determined by the **selection made in the Tree pane** (left window).

If a single folder is selected, the graphics inside that folder will be displayed. The branch plate option (see 12.1) can be used to display all graphics on the drive at one time.

The default setting in Gallery view is to **render and display thumbnails 1 page ahead**. For each page displayed, the following page is also rendered and is available to the user after a page down command or use of the scroll bar.

In some situations it may be advantageous to render all available images.

To **cache thumbnails to RAM**;

1. **Select** or **branch plate** the required folders in the Tree pane data view to display the gallery view thumbnails;

2. **Right click in the gallery view** window and select "**Cache All Images**"

Thumbnails will be cached to RAM. A rotating drive will appear in the bottom right hand corner of the gallery view window to indicate that caching is in progress.

The size and number of graphics displayed is controlled by moving the slide-bar in the footer of this window from small to large.

Figure 39, Gallery view scale bar

The Gallery view tab can also be detached from the *File* List view pane and re-sized displayed as a standalone window (see the chapter on "Customizing the Interface" for more information).

6.5   DISPLAY WINDOW (BOTTOM)

The display window enables the user to view the content of the currently highlighted file. This is done using three different data views: Display; Hex; and Text.

6.5.1   DISPLAY

The File Display view uses GetData's **Explorer View** technology to display the content of hundreds of different file types:

Figure 40, Display view

FAT32-Photos.E01\Partition @ 63 [NO NAME]\Root\Animals\Koala.JPG

Note that the file Display tab is a preview only. It is NOT intended as an exact render of how the file would have appeared to the end user when opened with its creating application.

If a file type is selected where a display is not available, or the file is corrupt, an error message will display in this window. The display view will default to Hex or Text view.

Depending on the type of file being displayed, the following icons become available in the File Display tab:

	Zoom out
	Zoom in
	Rotate Right degrees
	Rotate left 90 degrees

Print

Search (text or hex modes)

Full 1:1 picture size and ratio

Fit picture to screen size

Detach picture and display full screen

Audio buttons

The following options are also available by right clicking the preview window:

Figure 41, *Display* **view right click options**

Copy		Ctrl+C
Find		Ctrl+F
Counter Clockwise Rotate		
Clockwise Rotate		
Zoom In		
Zoom Out		
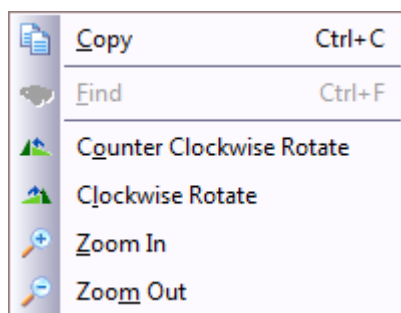
6.5.2   HEX VIEW

⚠️ The hex view tab is a **Professional & Technician license** feature only. It will not appear when Recover My Files is activated with a Standard license key. (See 4.2.4 for a comparison of license features).

The Hex tab shows a hexadecimal/ASCII view of the currently highlighted file.

Figure 42, Hex view

6.5.3   TEXT VIEW

The Text tab shows the selected file as ASCII text.

Figure 43, Text view

Chapter 7 - Best Power Settings

In This Chapter

7.1   DATA RECOVERY POWER SETTINGS

Depending on the type of search, the size of a hard drive and the speed of the computer, a search with Recover My Files can take a number of hours. Recover My Files contains code to keep the target drive awake during the search. However, there may still be situations where the target drive will power down or go into sleep mode. For example, if there is a time gap between the finish of the search and the return of the user to the computer.

For this reason it is recommended that power settings be changed to provide continuous power to the drive being searched. This is particularly important in a drive recovery where the hard drive no longer has a drive letter, or has become unallocated or RAW. In these situations Windows may not to correctly identify the connected hardware and maintain power to the drive.

7.2   SETTING HIGH PERFORMANCE POWER IN WINDOWS 7

To set high performance **power settings** in **Windows 7**:

1. **Open** the **Windows Control Panel**;

2. In the top right hand corner of Windows Control Panel type "**Power**" into the "**Search Control Panel**" box. In the filtered Control Panel view click "**Power Options**", as shown in Figure 40 below;

Figure 44, Windows Control Panel Power Options
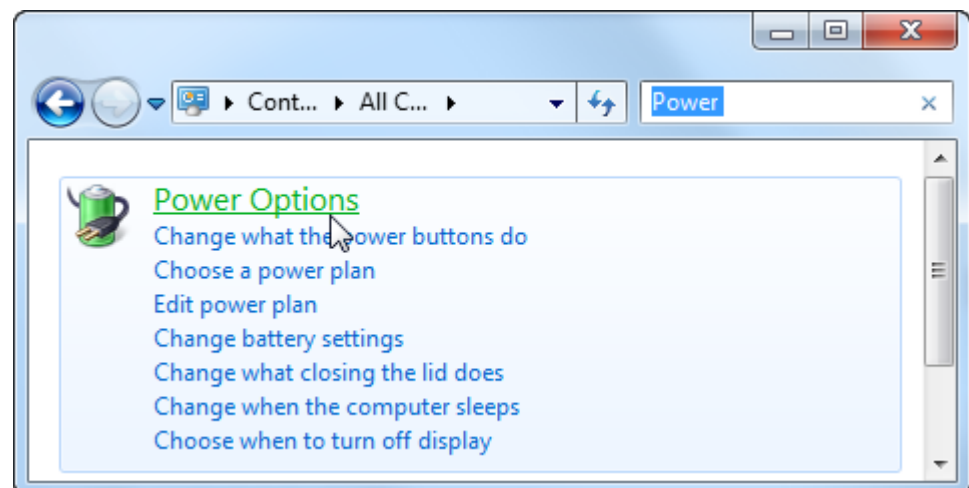
3. Most computers will be set by default to "Balanced". To perform the data recovery, change to "**High Performance**" by clicking the radio button next to this option. Then click on the "**Change Plan Settings**" link, as shown Figure 45 below:

Figure 45, High Performance, Change plan settings
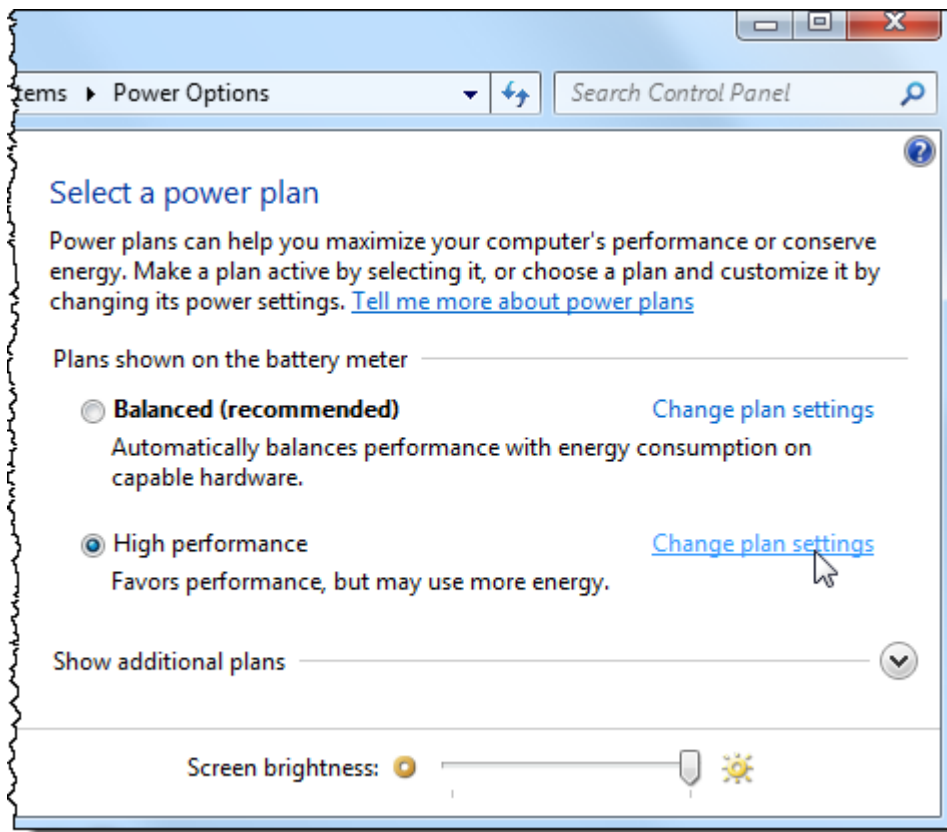
4. Then in the following window, click on the "**Change Advanced Power Settings" Link**, as shown in Figure 46 below:

Figure 46, Change advanced power settings
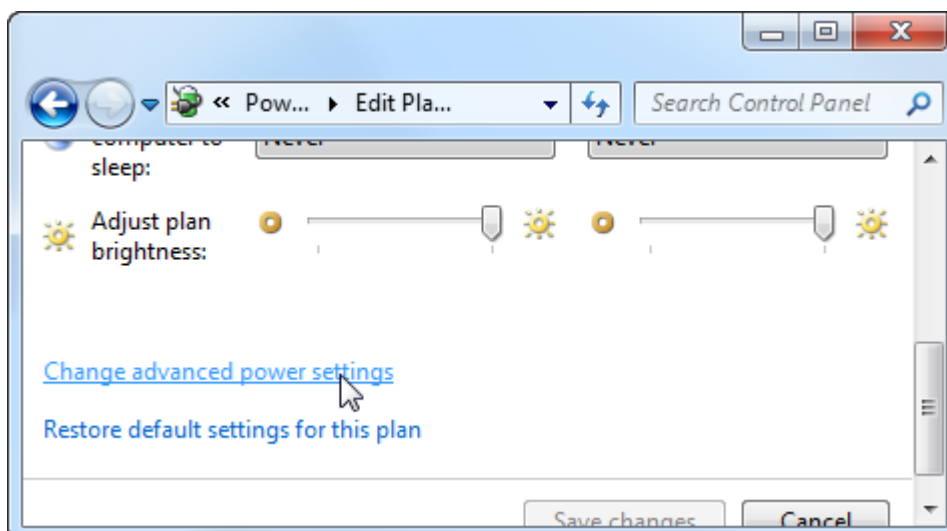
5. This will open the advanced Power Settings window shown in Figure 47 below:

Figure 47, Power Options, Advanced settings
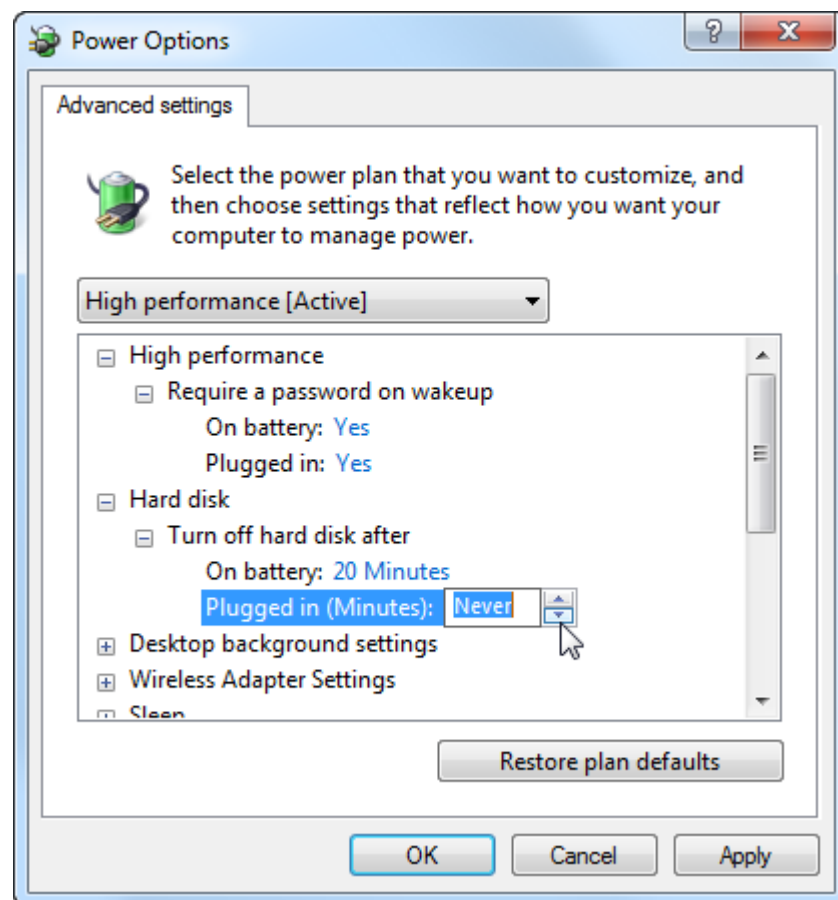
6. Also adjust and apply the following settings:

    - "Turn off hard drive after: Plugged in (Minutes)" = **Never**

    - Sleep > Sleep After > Plugged in = **Never**

    - Allow Hybrid Sleep > Plugged in = **Off**

    - Hibernate After > Plugged in = **Never**

    - USB Settings > USB selective suspend setting > Plugged in = **Disabled**

You now have the best power settings to run a data recovery. When your recovery is complete, reset the High Performance power settings by clicking the "**Restore plan defaults**" button in the above window. You may then also return to the "Balanced (recommended)" power option.

Chapter 8 - Recover Files

In This Chapter

8.1   QUICK START - RECOVER FILES

START

Deleted files, emptied from or bypassed
Recycle Bin, deleted by a virus or Trojan, or
lost by some other means.

Minimize Disk Usage
Minimize the use of the problem hard disk. If
the disk is your current C: drive, consider
connecting the drive to another computer as
a secondary drive to run the recovery.

Review Your PC Power Settings
Consider changing PC power settings to
"High Performance" for data recovery
(see Chapter 7)

Download Recover My Files
Download and install Recover My Files.
Preferably install on a different hard disk.
(See Chapter 3)

Run Recover My Files
In the wizard window select "Recover Files".
Click Next.

Select the Drive Letter
In the drive selection window, select the
problem drive letter.
Click Next.

Start a New Search

Search for "Deleted and Lost Files"

Select required file types

Click Next

Select "Search for Deleted Files"

Click Start

No

Review Search Results

Use different views (e.g. Folders, File Type, Recovered, Gallery View) to locate your files.

Do jpegs and documents preview in the display (bottom) window?

Click on the Validate button to validate results.

Determine from the results if you wish to save the files.

Save List of Search Results

Consider saving a list of the search results as a .rsv file that can quickly be loaded later, by clicking the Save Session button.

Purchase a Key

Purchase a software license key at www.recovermyfiles.com.

Key is provided on a web page at the end of the purchase process and also by email.

Offline Activation

If PC not online, use another internet connection for offline activation process.

(See 5.3, Offline Activation)

Online Activation

Is the PC online?

Open the software activation window. Enter the software activation key.

(See 5.2, Online Activation)

Select Files to be Saved
In the search results window, select the files to be saved (tick the boxes). Select those files which preview or validate.
Check space required to save (status bar).

Save Files
Press Save Files button and select the destination drive. Files must be saved to a different drive.
Click OK to start the save process.

Review the Saved Files
Check the destination drive to ensure that the files have saved correctly. Open and test files with their creating applications (e.g. Word, XLS).

Files are recovered
Once you have confirmed that your data has been successfully recovered, assess what you now wish to do with the problem drive. E.g. Use Windows to copy the recovered files back onto it, or replace the problem hard drive with a new drive.

8.2   WHEN TO USE A RECOVER FILES SEARCH

A "**Recover Files**" search is best used when:

- individual files have been **deleted** and **emptied from the Windows Recycle Bin**;

- files have been **deleted** and **bypassed the Windows Recycle Bin**;

- files have been **deleted by a virus, Trojan or worm**;

- a file of the same name has **saved over** another important file;

- Files have been lost by some other unknown cause.

8.3   BEFORE YOU BEGIN

Minimize Drive Use

Deleted files will remain on a computer up until such time as they are overwritten by new data. For this reason you should minimize the use of the drive on which the files were lost until such time as you have had the opportunity finish your data recovery.

Recovering Data from a C: Drive

Your C: drive is the most vulnerable to new data simply because it is where Windows is running. If practical you may consider connecting the drive to another PC as a secondary and then using that computer to run the search. In critical situations, you may also consider taking a drive image (a sector by sector copy of the entire drive) and working on the image rather than the original drive. For more information see Chapter 15 - Drive Imaging.

Many users may not have the available resources to move the hard drive to another computer. Recover My Files is a relatively small program (less than 20mb), so whilst installing on the problem drive is not ideal, it is a limited risk.

Review your PC power settings

When running a Recover Files search it can be advantageous to boost your PC power settings so that problems are not encountered with drives powering down during the recovery or the save process. See Chapter 7 for more information.

8.4   RUNNING A RECOVER FILES SEARCH

To run a **Recover Files** search:

1. Run Recover My Files. In the wizard, lick the "**Recover Files**" icon (if the Wizard screen is not open, click the Start icon in the toolbar) and click the **Next** button:

2. In the drive selection window **highlight** the **drive letter** from which the files are missing and click **Next.**

⚠️ Drive not listed: See 11.1 - Troubleshooting drive selection.

⚠️ Working with image files: See 14.3 - Recovering data from an image file.

Figure 48, Drive selection screen

The Device Selection window includes the following information:

Label: Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used).

Size: The size column contains the size of the physical or logical device. Note that the actual size of the drive is usually smaller than what the drive is labeled. Drive manufacturers usually round up the drive capacity, so a 453.99 GB drive in this screen may be sold as 500GB.

FS: The File-system on the drive, e.g. FAT, NTFS or HFS;

Type: Describes the way in which the drive is connected to the computer.

3. Select the File Recovery options:

Figure 49, Search for deleted files

8.4.1 SEARCH FOR DELETED FILES

Each file on a Windows computer has a record in the file-system index (e.g. the FAT or MFT). When a file is deleted, the record is updated with a deleted file marker. The clusters on the drive used to store the file data are now considered unallocated (i.e. available for new storage). However the file content remains in those clusters. A search for deleted files reads the entire file-system index, including records for deleted files, and displays the file content.

To search for **deleted files:**

1. Select the "**Search for deleted files.**" option;

2. Click the **Start** button.

Recover My Files will then commence to read the file-system. This search will take less than 20 minutes to complete. At the completion of the search review the search results as described in 8.5 below. If files are **NOT** found, try the option to "Search for deleted files, and then search for selected Lost File types".

8.4.2 SEARCH FOR DELETED FILES, THEN SEARCH FOR SELECTED "LOST FILE" TYPES

As the name suggests "**Search for deleted files, then search for selected "Lost File" types"** runs the search for deleted files (described above), then sequentially scans the remaining area of the drive for "Lost" files.

A **lost file** is a file that is located by f**ile carving**. File carving is a sequential search of the drive to find file headers for the specified file types. Learn more about lost files at the beginning of this manual - Data Recovery Fundamentals. This search should be run when:

- The "Search for deleted files" option did NOT find the missing files;

- When you wish to be certain that all possible data on the drive is located and recovered.

To **search for deleted and lost files**:

1. Select the "**Search for deleted files, then search for selected Lost File types**" option and click the **Next** button (shown in Figure 49). The file type selection window will open:

Figure 50, File type selection window
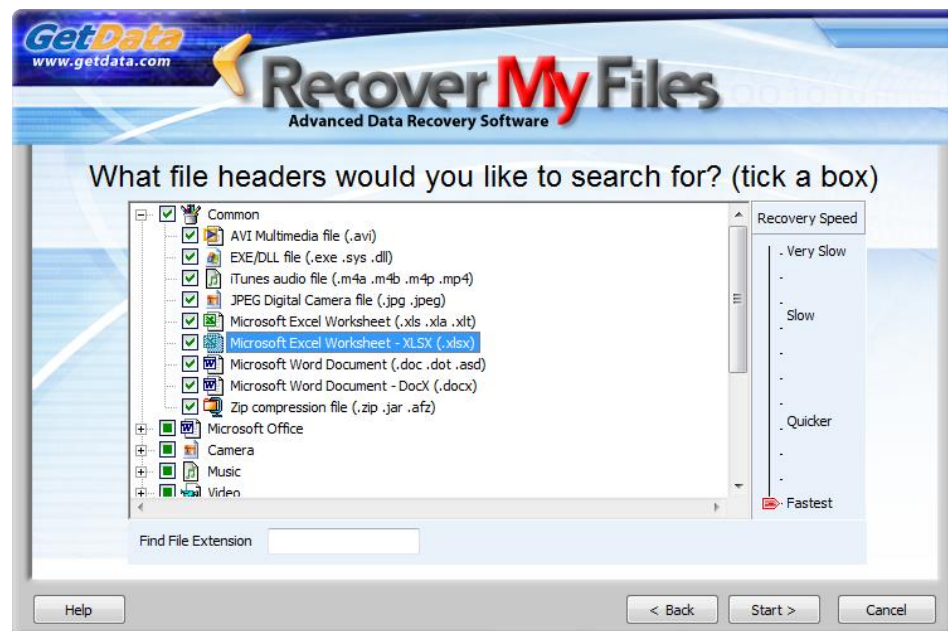
2. Place a **select tick** in the box next to the file types that you wish to recover. The file types in this list have a known structure that can be identified if found on the drive (a full list is provided at Appendix 2 - File carving). To search for a file type, type the extension into the "Find File Extension" search box.

   Important: The more file types that are selected, the more resource intensive the search is and the longer the search will take. It is suggested that you do not perform a Lost File search for more than 10 files at any one time. A sequential search of a large hard drive, e.g. 2TB or more containing many files may take up to 24 hours.

3. Click the **Start** button to commence the search. A search for deleted files (described in 9.2.1 above) will commence.

4. The start of the lost files search is indicated by the message "**Scanning block xxxxx of xxxxx for lost files**" above the progress bar.

5. Lost file are placed in the Lost Files folder. As the search progresses, review the search results (as described below). If the missing files are located, stop the search and save the files.

8.5   RECOVER FILES SEARCH RESULTS

Click the ⊞ icon in the search results screen to expand folders. Use the different data view and sort and filter functions to determine if the missing files have been located (see Chapter 6 for more information).

In the search results screen deleted items are identified by the following icons:

Deleted folder

Deleted file

Lost file

The available data views are summarized as follows:

Deleted view

The Deleted view is a fast way to locate relevant files as it shows <u>only</u> deleted files. The folders in the Deleted view describe the way in which each of the deleted files has been identified, i.e. "Deleted" or "Lost".

Figure 51, Tree pane, Deleted view

Folders view

The Folders view shows all files and folders on the examined drive. The "**Root**" folder contains the existing folder and file structure on the drive. Deleted files and folders are located inside the Root folder and should appear in their original location prior to delete.

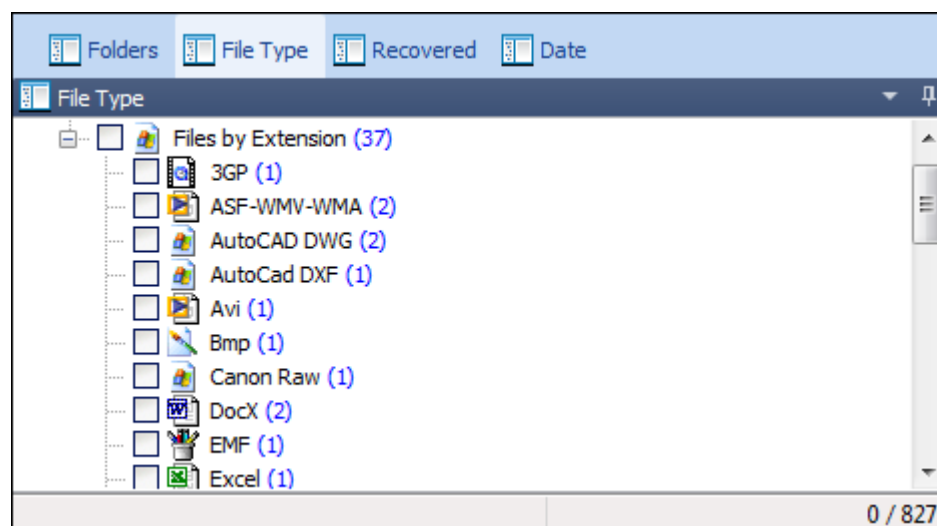Lost and Orphaned files are placed in their own folders under the partition in which they were found.

File Type view
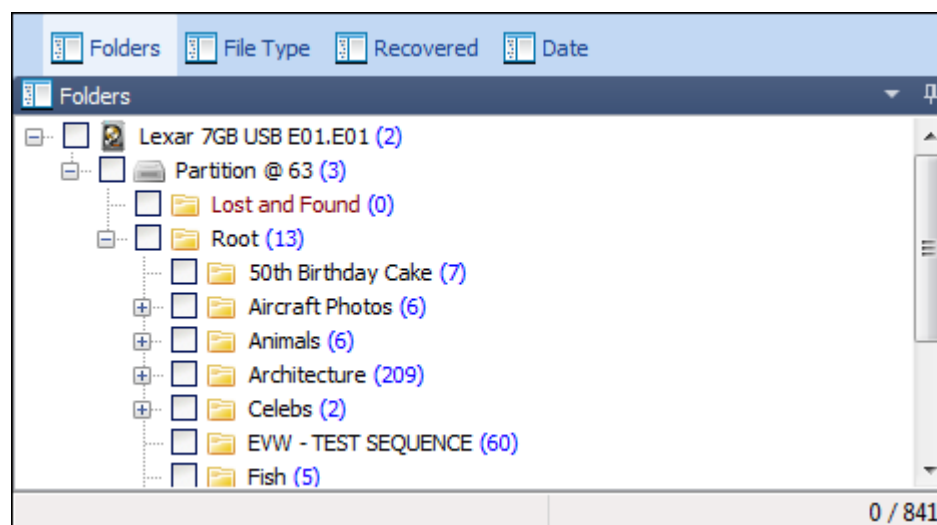
The File Type view sorts files by extension. This view shows all files on the examined drive. Select a file type, and then look for the deleted file icons. It is also helpful to sort by the "Is Deleted" column in this view.
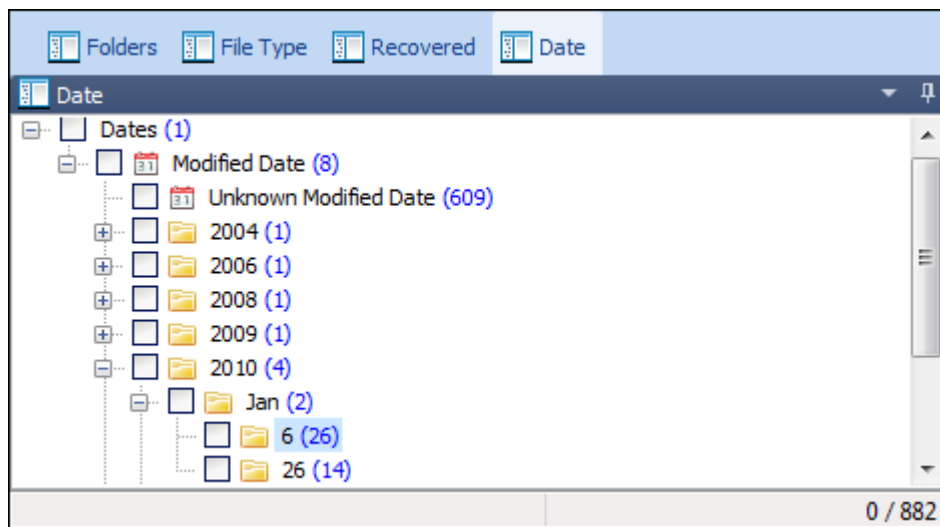
Date view

The date view groups files by date. This view shows all files on the examined drive. Look for the deleted file and folder icons.

Figure 54, Tree pane, Date view

Validating search results and saving files

To learn how to validate the search results and save files, see "Chapter 10".
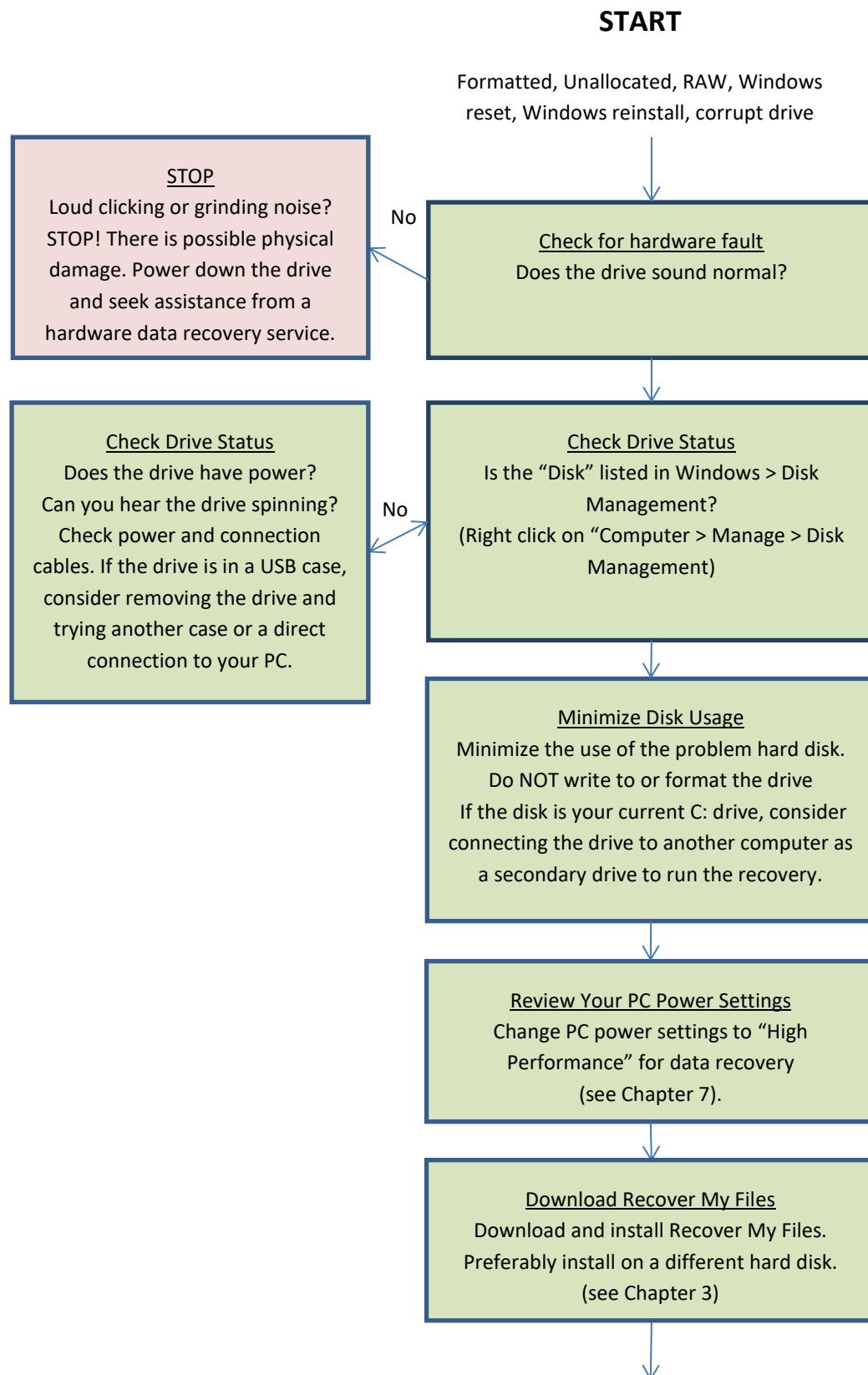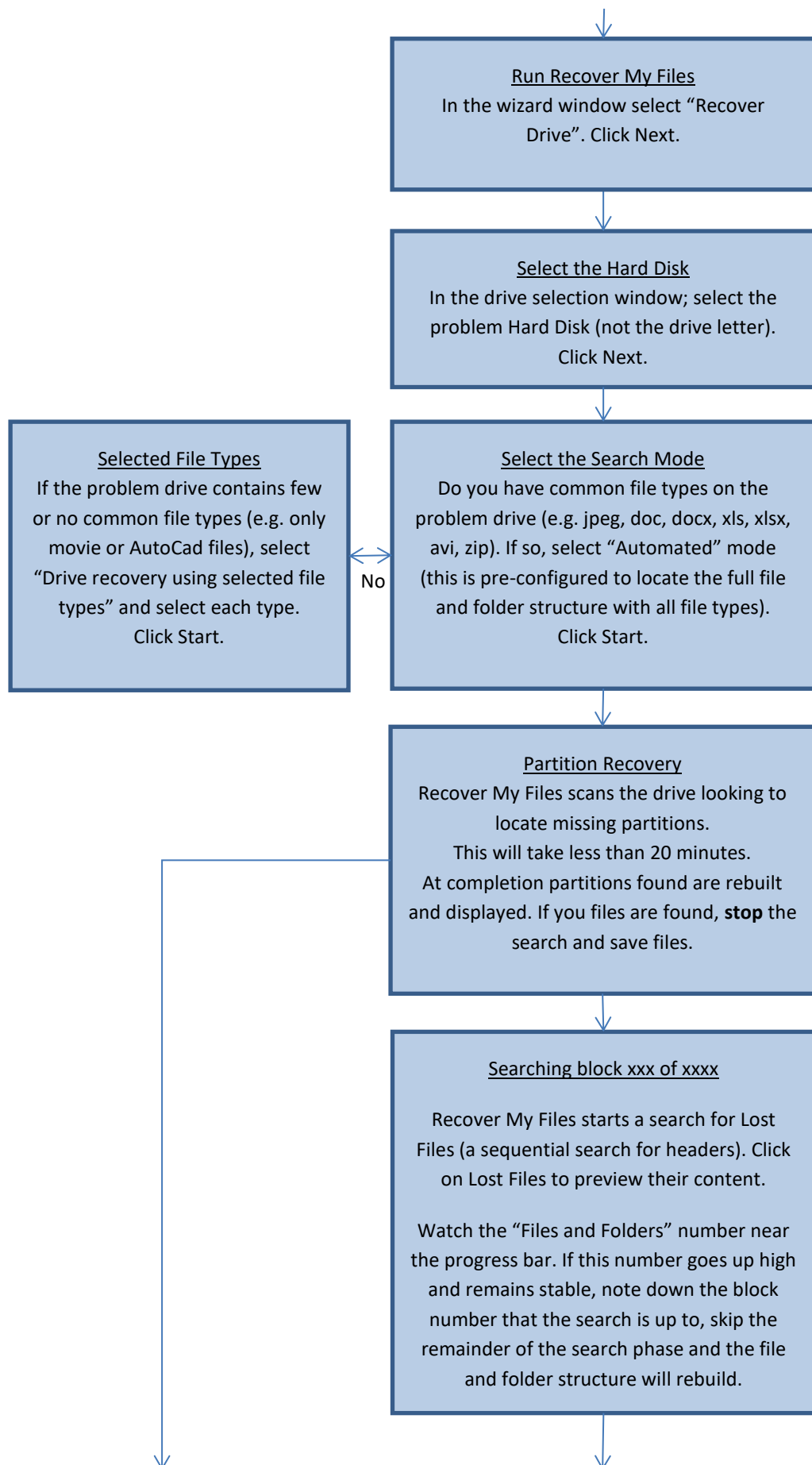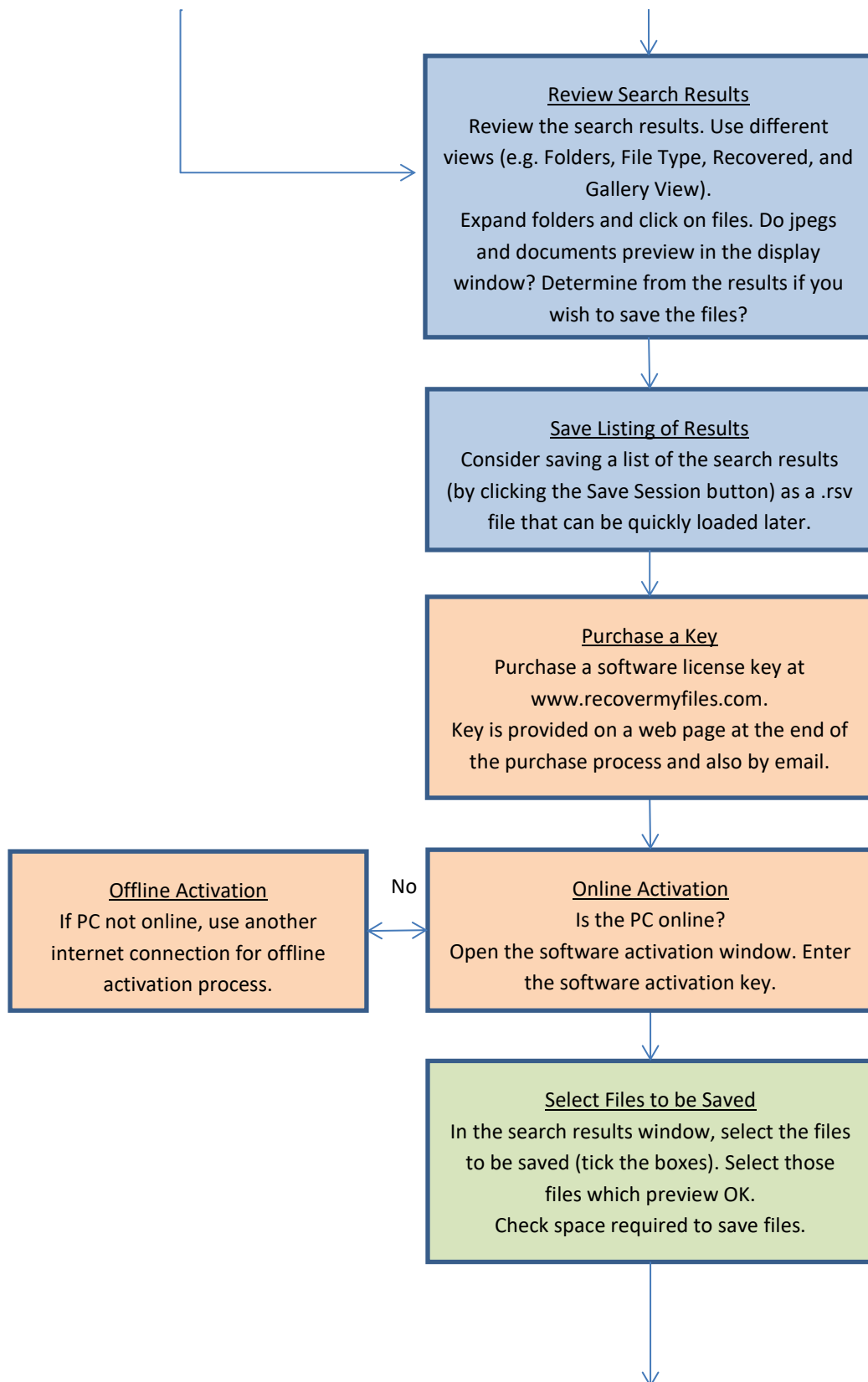
Chapter 9 - Recover a Drive

In This Chapter

9.1   RECOVER DRIVE - QUICK START GUIDE

START

Formatted, Unallocated, RAW, Windows
reset, Windows reinstall, corrupt drive

STOP
Loud clicking or grinding noise?
STOP! There is possible physical
damage. Power down the drive
and seek assistance from a
hardware data recovery service.

No

Check for hardware fault
Does the drive sound normal?

Check Drive Status
Does the drive have power?
Can you hear the drive spinning?
Check power and connection
cables. If the drive is in a USB case,
consider removing the drive and
trying another case or a direct
connection to your PC.

No

Check Drive Status
Is the "Disk" listed in Windows > Disk
Management?
(Right click on "Computer > Manage > Disk
Management)

Minimize Disk Usage
Minimize the use of the problem hard disk.
Do NOT write to or format the drive
If the disk is your current C: drive, consider
connecting the drive to another computer as
a secondary drive to run the recovery.

Review Your PC Power Settings
Change PC power settings to "High
Performance" for data recovery
(see Chapter 7).

Download Recover My Files
Download and install Recover My Files.
Preferably install on a different hard disk.
(see Chapter 3)

Run Recover My Files
In the wizard window select "Recover Drive". Click Next.

Select the Hard Disk
In the drive selection window; select the problem Hard Disk (not the drive letter). Click Next.

Selected File Types
If the problem drive contains few or no common file types (e.g. only movie or AutoCad files), select "Drive recovery using selected file types" and select each type. Click Start.

No

Select the Search Mode
Do you have common file types on the problem drive (e.g. jpeg, doc, docx, xls, xlsx, avi, zip). If so, select "Automated" mode (this is pre-configured to locate the full file and folder structure with all file types). Click Start.

Partition Recovery
Recover My Files scans the drive looking to locate missing partitions.
This will take less than 20 minutes.
At completion partitions found are rebuilt and displayed. If you files are found, **stop** the search and save files.

Searching block xxx of xxxx

Recover My Files starts a search for Lost Files (a sequential search for headers). Click on Lost Files to preview their content.

Watch the "Files and Folders" number near the progress bar. If this number goes up high and remains stable, note down the block number that the search is up to, skip the remainder of the search phase and the file and folder structure will rebuild.

Review Search Results
Review the search results. Use different views (e.g. Folders, File Type, Recovered, and Gallery View).
Expand folders and click on files. Do jpegs and documents preview in the display window? Determine from the results if you wish to save the files?

Save Listing of Results
Consider saving a list of the search results (by clicking the Save Session button) as a .rsv file that can be quickly loaded later.

Purchase a Key
Purchase a software license key at www.recovermyfiles.com.
Key is provided on a web page at the end of the purchase process and also by email.

Offline Activation
If PC not online, use another internet connection for offline activation process.

No

Online Activation
Is the PC online?
Open the software activation window. Enter the software activation key.

Select Files to be Saved
In the search results window, select the files to be saved (tick the boxes). Select those files which preview OK.
Check space required to save files.

Save Files
Press save files button and select the destination drive. Files must be saved to a different drive.
Click OK to start the save process.

Review the Saved Files
Check the destination drive to ensure that the files have saved correctly. Open and test files with their creating applications (e.g. Word, XLS).

Files are recovered
Once you have confirmed that your data has been successfully recovered, assess what you now wish to do with the problem drive. E.g. Use Windows to copy the recovered files back onto it, or replace the problem hard drive with a new drive.

9.2   WHEN TO USE RECOVER DRIVE

The "**Recover Drive**" option is best used when:

- a drive has been **formatted**;

- a drive has been **formatted and Windows reinstalled**;

- a **Windows recovery** or **system restore** has resulted in a fresh installation of Windows and the previous user created files are missing;

- a **drive letter** has **gone missing**;

- the drive is **unallocated** or **RAW** in Windows Disk Management and no files can be read;

- Or some other problem has affected the entire contents of the drive.

The Recover Drive search will recover the missing file and folder structure with all file types.
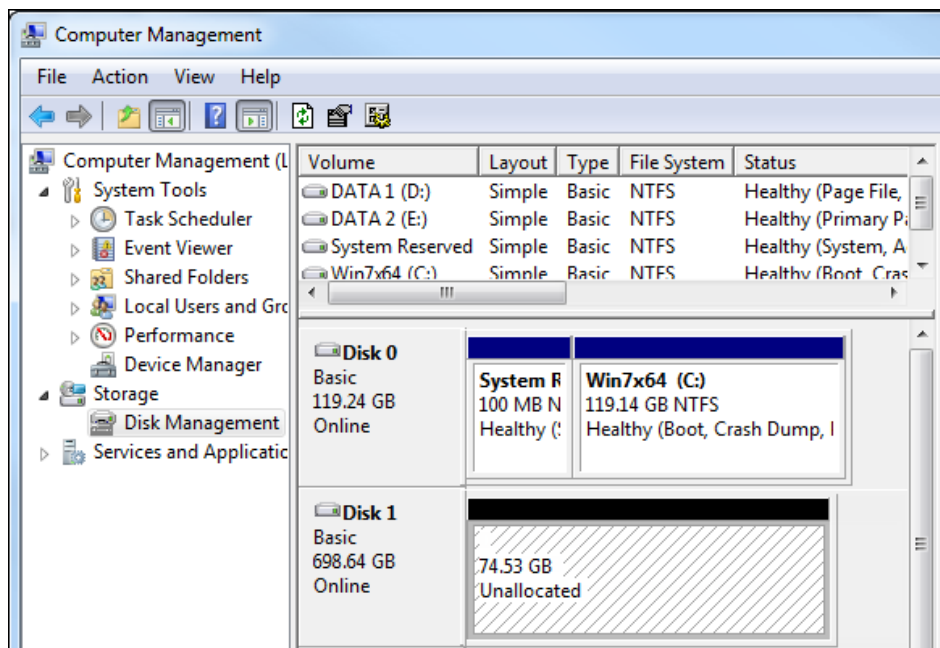
9.3   BEFORE YOU BEGIN

Is the drive physically OK?

Check that your problem drive is mechanically functional. If it is making a loud grinding or clicking noise then it is likely that it has suffered physical damage. It should be powered off immediately and assistance sought from a hardware data recovery service.

Check the status of the drive in Windows Disk Management (in Windows 7, right click on My Computer > Manage > Disk Management). At a minimum you should see the physical disk listed:

Figure 55, Windows Disk Management, showing an "unallocated" Disk 1

Consider the best way to connect the drive to run the recovery
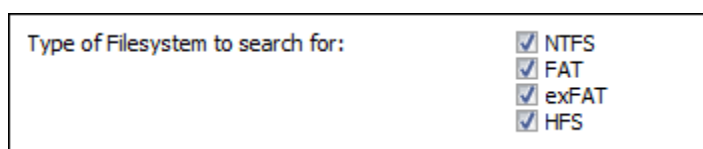
Avoid writing any new data to the drive. If it is your current C: (e.g. you have reinstalled or re-set Windows) you may consider connecting the drive to another PC as a secondary drive and then using that computer to run the search (making it less likely that new data will be written to it).

In critical situations, you may also consider taking a disk image (a sector by sector copy of the entire disk) and working on the image rather than the original drive. See Chapter 14 for more information.

Do you know what type of file-system you are trying to recover?

If you know the type of file-system that you are trying to recover, e.g. NTFS, FAT, exFAT, HFS, EXT, you can specify this in program options before your run the search. This can increase search speed and also simplify search results by not including unwanted data. Select **Options** > **Search** and specify the File-system type (⚠ Only change this option if you are sure of the file-system type to be recovered).

Figure 56, Options > Search, Setting the type of file-systems to recover

Review your PC power settings

When running a Recover Drive search it can be advantageous to boost your PC power settings so that problems are not encountered with drives powering down during the recovery or the save process. See Chapter 7 for more information.

9.4   RUNNING THE RECOVER DRIVE SEARCH

To **recover a drive**:

1. Run Recover My Files. In the wizard, click the "**Recover Drive**" icon (if the Wizard
    screen is not open, click the Start icon in the toolbar) and click the **Next** button ;

2. For a **Recover Drive** search, select the Hard Disk rather than a drive letter (Only
    search a drive letter if you problem drive contained multiple partitions, e.g. drives
    E:, F:, G: and the problem relates to only one of the drive letters). In the drive
    selection window, **highlight a Hard Disk** to search and click the **Next** button.

Figure 57, Drive selection screen, showing "Hard Drive 3" which has lost its drive letter
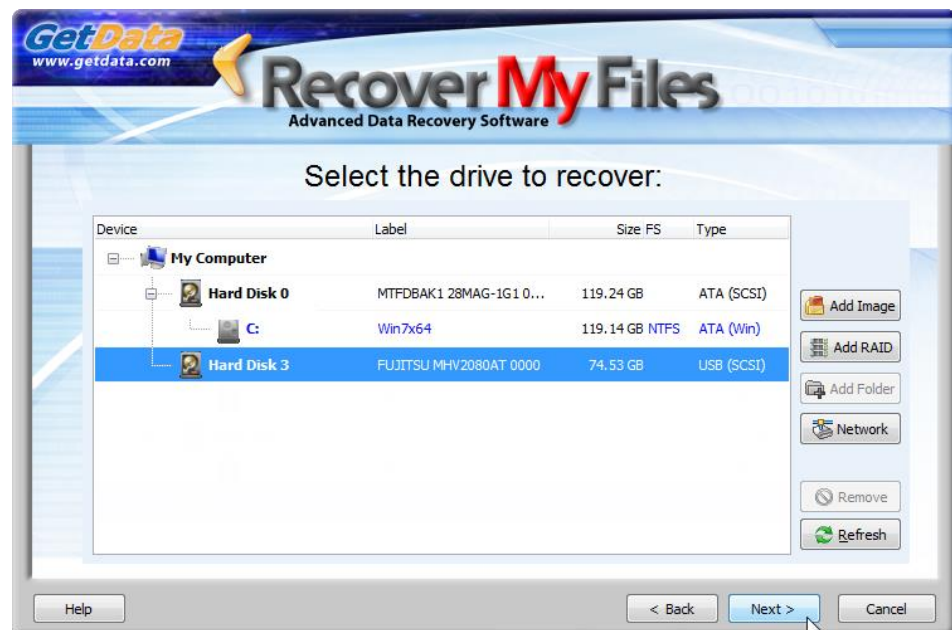
The Device Selection window includes the following information:

> **Label:** Physical drives are listed with their Windows device number.
> Logical drives display the drive label (if no label is present then "{no
> label}" is used).
>
> **Size:** The size column contains the size of the physical or logical device. Note
> that the actual size of the drive is usually smaller than what the drive is
> labeled. Drive manufactures usually round up the drive capacity, so a
> 453.99 GB drive in this screen may be sold as 500GB.

> **FS:** The File-system on the drive, e.g. FAT, NTFS or HFS;
>
> **Type:** Describes the way in which the drive is connected to the computer.

⚠ Drive not listed: See 11.1 - Troubleshooting drive selection.

⚠ Working with image files: See 14.3 - Recovering data from an image file.

3. The **drive recovery options** windows asks the user to select between an automatic or manual recovery:

Figure 58, Drive recovery options

The selection in this window configures the search for **lost files.** Lost files are found by a sequential search of the drives unique file signatures (learn more about lost files at the beginning of this manual in Data Recovery Fundamentals). Lost files assist Recover My Files to locate and rebuild the folder and file structure. The options are:

- **Automatic drive recovery**

    An "Automatic Drive Recovery" uses pre-selected common file types (Avi, EXE, iTunes, Jpeg, xls, xlsx, doc, docx and Zip).

- **Drive recovery using selected file types**

    A "Drive recovery using selected file types" allows the user to manually select the file types to assist in locating the missing file and folder structure. It is suggested that you only use this option:

    o   If the problem drive does NOT contain some of the pre-selected common file types (described in the "Automatic" option above). For example, if

the problem drive contained only HTML files, it is best to manually select the HTML file type; or

o The drive contains common file types, but you are specifically looking for additional file types not in the common list, such as .qbb or .dwg. In this case you would manually select the common file types and add the additional.

The benefit of manually adding a file type is that in addition to helping locate the file-system records, you are simultaneously searching for the lost files by type. If the original file and folder structure cannot be recovered (it may be overwritten or corrupt), you may still recover file content as a lost file.

The disadvantage of a adding many file types is that each addition type requires additional processing time and it will slow down the search. We suggest that you do not select more than 10 file types at any time.

4. Once the required selection has been made, press the **Start** button to begin the search.

9.5 SEARCH PROGRESS

A Recover Drive search runs in phases. The search phase is identified by text above the progress bar. The phases in the search will be dependent on any search options set (e.g. Options > Advanced > Run a Lost Files search only). The following **describes a Recover Drive search with default options**.

PHASE 1 OF 5: SEARCHING FOR KNOWN PARTITIONS

Phase 1 of the Recover Drive search identifies the **configuration of the existing drive**. Recover My Files examines the MBR (Master Boot Record) and other system files to determine the type of file-system currently installed and the drive parameters. Phase 1 is very fast and is complete within a few seconds.

PHASE 2 OF 5: PARTITION RECOVERY

Phase 2 of a Drive Recovery attempts to **locate missing partitions**. Recover My Files performs two separate passes down the drive looking for partition tables. Typically this part of the search will take less than 20 minutes. Partitions located are rebuilt in the next phase.

PHASE 3 OF 5: REBUILDING PARTITIONS

Partitions located in phase 2 are **rebuilt and displayed in the search results screen** in phase 3. They are created using the naming convention:

 [Partition Type] Partition @ [Starting block number] [Drive label]

An example of a recovered FAT partition is shown in Figure 59 below:

Figure 59, FAT partition located in Stage 1 of a Recover Drive search

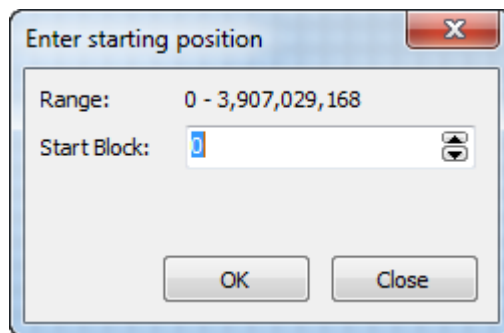Once added, a recovered partition can be browsed even as the search continues. Click the ⊞ icon to expand the search results. Use the different data views and sort and filter functions (see Chapter 6 for more information) to determine if the missing files have been located.

⚠ If relevant files and folders are located in a partition the remaining search phases can be skipped and files saved.

PHASE 4 OF 5: SEARCHING FOR "FILES AND FOLDERS" AND "LOST FILES"

Phase 4 of the Recover Drive, "**Scanning block xxx of xxx …**" is a sequential search for "Files and Folders" and "Lost Files".

Figure 60, Recover Drive, phase 4 of 5

Lost Files

As Lost files are found by file signature they are added to the "Lost Files" folder in the results screen and are immediately available to be previewed. Their preview confirms that Recover My Files is successfully reading the drive. However the value of lost files is limited because although they contain file content, they do not have their original file name. Their principal use is to assist to locate Files and Folders (described below).

Files and Folders

Scanning for Files and Folders and Lost files over a large drive can be a long process:

Knowing when to best stop this phase can save many hours.

"Files and Folders" are recreated from individual file-system records (e.g. FAT or MFT records). File-system records for a drive which has lost a single partition are **usually**

clustered at the start of the drive, i.e. within the first 30,000,000 blocks. In most drive recoveries, the complete file and folder structure will be found early in the search (within the **first 40 minutes**). Once the file-system records have been located, the file and folder structure can be rebuilt and all files can be located without the need to scan the entire drive.

To **rebuild file and folder** structure:

1. Watch the "**Files and Folders: xxxxx**" number near the progress bar. When file-system records are found this number will rise sharply (each item is an individual file or folder) and then remain stable;

2. Note down the approximate block number that the search is up to (a subsequent search can be started from this position if required) and press the Skip button:

   The following window will appear:

3. Click OK and skip to phase 5.

9.5.1   PHASE 5 OF 5: REBUILDING "RECOVERED PARTITIONS"

Phase 5 of the search is the rebuild of the file and folder structure. Depending on the number and complexity of file-system records located, this phase of the search may take up to 45 minutes. It is not possible to skip this final phase.

Results are added as Recovered Partitions in the following format:

Recovered [File-system type] Partition @ [starting block]

As shown in Figure 61 below:

Figure 61, Recover Drive search results showing Recovered FAT and NTFS partitions
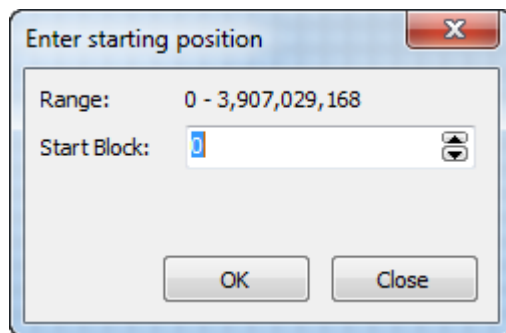
Click the ⊞ icon to expand the search results. Use the different data views and sort and filter functions (see Chapter 6 for more information) to determine if the missing files have been located.

9.5.2   RUNNING A RECOVER DRIVE SEARCH FROM A SPECIFIC BLOCK

If the recovered partition does not contain your missing files it is possible to continue the search from the block at which the previous search was stopped.

1. Select Options > Advanced > and select "Prompt for start block", and "Run a lost files search only". Start a Recover Drive search and proceed through the wizard steps. Start the search and when prompted, enter the starting block;

9.6   RECOVERING FILES FROM BITLOCKER DRIVES
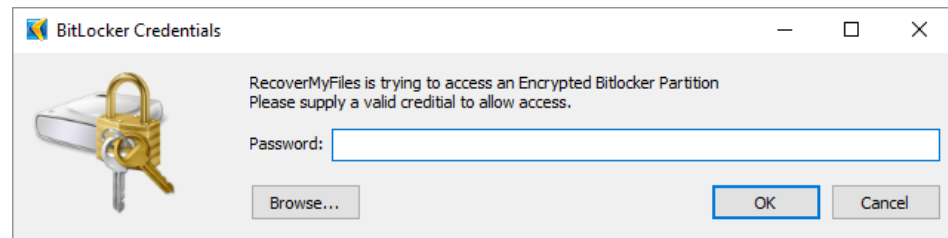
Recover My Files v6 supports the recovery of **BitLocker** drives. BitLocker is a full disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes.

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** when prompted with the
following authentication window:

Figure 62, BitLocker credentials window

The **BitLocker** protected partition will then be added to the folders tree.

Chapter 10 - Saving Files

In This Chapter

10.1 VALIDATING A SUCCESSFUL RECOVERY

The principle way to validate a successful recovery is to preview missing files in the search results window. Use the different data views with sort and filter functions (see 6.4) to locate relevant files. Click on documents and graphics to preview their content in the display view, as shown in Figure 63 below:

Figure 63, Preview of a delete jpg

10.1.1 VALIDATE EXTENSIONS

A "Validate Extensions" test is a post search tool to test search results for valid or invalid content. It is a comparison between a recovered files extension (as given in the filename) and file signature (read from the data in the file header). It is based on the assertion that a file extension should match the file signature.

To run a validate extensions test;

> At the completions of a search, select "**Validate Extensions**" from the **Recover My Files drop down menu**;
>
> Or, select the **Validate** button on the program toolbar:

This opens the following screen:

The tool creates and populates the "Valid Extension" column in file view, as shown below:

Figure 64, Valid extension column

The following rules are applied:

- If **file extension matches the signature**, the file extension is written in **green** to indicate a **valid** file.
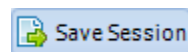
- If **file extension and signature do not match**, and the **signature is known**, the signature extension is written in **blue** to indicate a valid file of **another type**;

- If the file extension is in the list of known signatures, but does not match a signature, the entry is **Invalid Data**.

- If the extension is unknown, the entry is **Unknown Type.**

In the example above, a text filter on the valid extension column for "jpg" will return only jpg files.
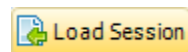
⚠ Not able to preview files: see 11.3.

10.2 SAVE AND LOAD A LISTING OF SEARCH RESULTS

When Recover My Files is closed, or a new search is started, any existing search results are cleared from memory. In order to recreate the existing search results, it is necessary to run a new search. To avoid this, it is possible to save a listing of existing search results as an .rsv file so that they can be quickly reloaded at a later time.

| Save Session | To save a listing of search results, click the Save Session button and save a [search name].rsv file. |
| Load Session | To load a list of search results at a later time, ensure that the problem hard drive is connected, select the Load Search button and load the relevant .rsv file. |

It is important to remember that you are saving a listing of the search results only. If the content of the drive subsequently changes (i.e. new data is written to the drive), this may overwrite and destroy deleted files and the saved search results may no longer be valid. If you plan to reload the search at a later time, minimize the use of the drive in the interim.

10.3 SAVING RECOVERED FILES

10.3.1 WHAT SHOULD I SAVE?

Recover My Files is designed to get back your created photos, documents, music etc. Select and save the files that are most important to you. Remember;

- There is no point saving gigabytes of Windows System files that will be worthless to you and it will just slow the saving process down;

- Rather than trying to recover and save software programs, it is better to reinstall software programs from the original drives or installation files to be sure of the integrity of their registry settings etc.;

- Start by saving only a small sample of files. Once you have saved them, go to the drive on which the files are saved and open them with their creating

application (e.g. Word) to make sure they are complete. Once you are satisfied with the test, save a larger batch of files.

The files **must** be saved to another drive. It is NOT possible to save the files directly to the drive from which they are being recovered (this would result in new data being written to the drive and overwriting and destroying yet to be saved files). You can save files to another drive letter on the same drive, a separate hard drive, a USB, thumb/pen drive, or a network drive.
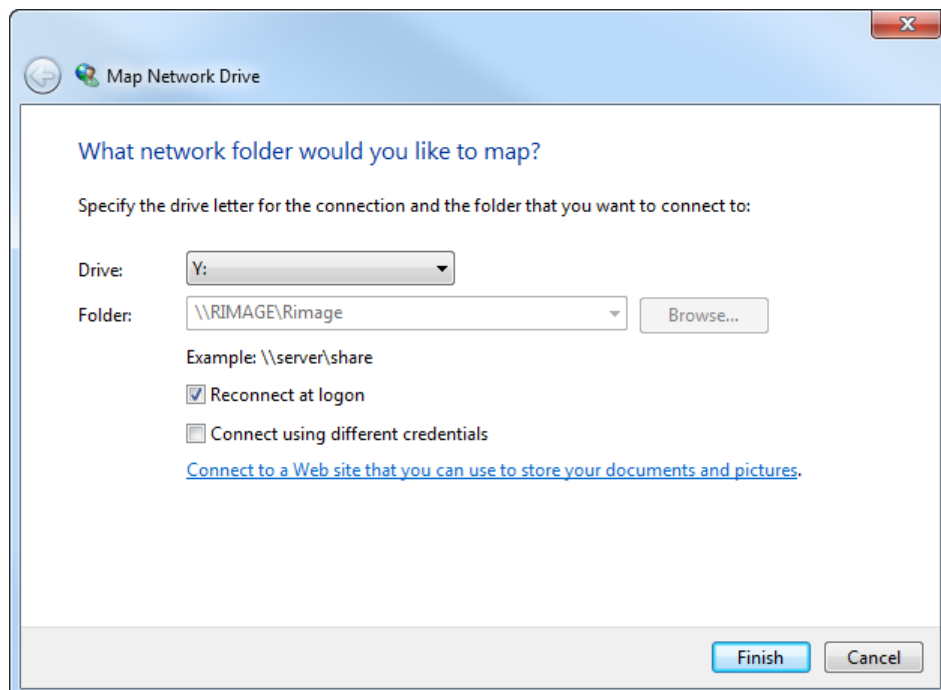
The recommended option is that files be saved to an external USB drive. They are inexpensive, large capacity and can be easily connected to most computers.

Saving to a Network Drive

To save to a network drive a folder on the remote computer must be mapped as a drive letter on the computer running the recovery. To map a Network drive in Windows 7:

1. Open **Windows Explorer**;

2. Click on the **Network** icon and then click the desired computer (login to the remote PC if prompted);

3. **Right click** on the desired folder on the remote computer and select "**Map Network Drive...**" from the drop down menu. The following window will appear:

Figure 65, Mapping a network drive in Windows 7

4. Click **Finish**. The drive letter should now be mapped to your computer. You should now see the drive appear as a drive letter in Windows Explorer, as shown below.

Figure 66, Mapped drive letter in Windows Explorer

10.3.3 BEST POWER SETTINGS

When preparing to save files it can be prudent to ensure that your computer power settings are adequately set to avoid any of the devices powering down during the save process. It is relevant if you are saving from a device which has lost its drive letter as Windows may not be able to adequately detect the device to keep it awake over an extended period. To set powers settings, follow the instructions in Chapter 7 - Best Power Settings.

10.3.4 HOW TO SELECT FILES TO BE SAVED

To select a **file** to be saved, in the search results screen place a tick in the box next to the file:

    ☑   User selected file;

    ▣   A folder in which not all files inside that folder (or its sub-folders) have been selected.

To select a **Folder** to be saved, place a tick in the box next to the folder, and all files within the sub folders will automatically be selected.

To select a **group of files** to be saved, hold down the SHIFT or CTRL key, highlight the files with your mouse, and then press the SPACE BAR to turn the selection ticks on (or off).

Gallery view currently only allows the selection of single files.

10.3.5 HOW MUCH SPACE DO I NEED?

In the bottom border of the main program screen you can see how many folders and files have been selected and the total size.

Figure 67, Volume of selected files
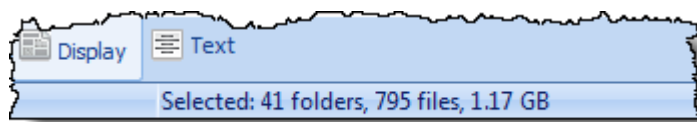
10.3.6 SAVING

It is recommended that files be saved into a new folder. Use Windows Explorer to create a new folder on the drive on which you are going to save the files. In the example below, this folder is called "Search 1 Results".
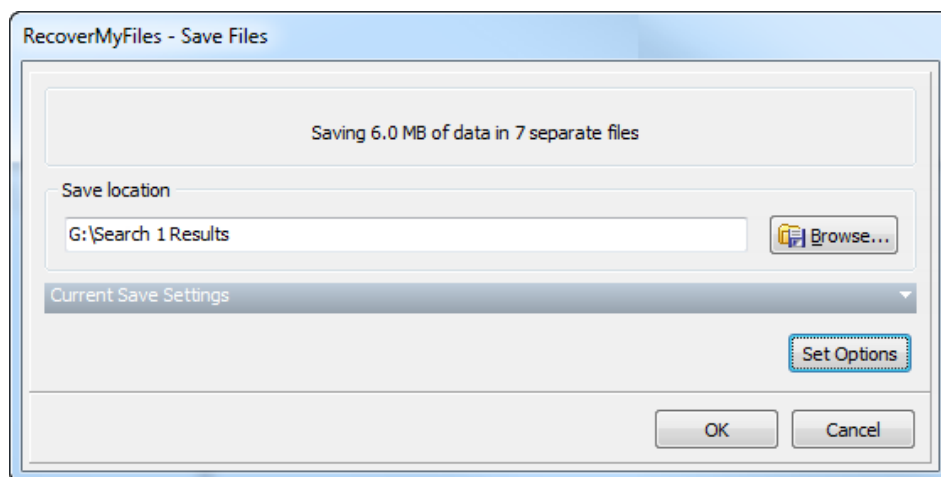
Once files have been selected (described above), press the **Save Files** button (or the Save menu item in the "Recover My Files" drop down menu:

(Note: The drop down arrow next to the Save button gives access to "Save As". If this option is selected Recover My Files will prompt for a new file name for each file saved):

The following window will appear prompting for the save location. Click the Browse button to locate and select the folder in which to save the files.

Figure 68, Selecting the save location

Click the **Set Options** button to configure advanced saving options: See Save Options - 12.3.

Click **OK** to begin the save process:
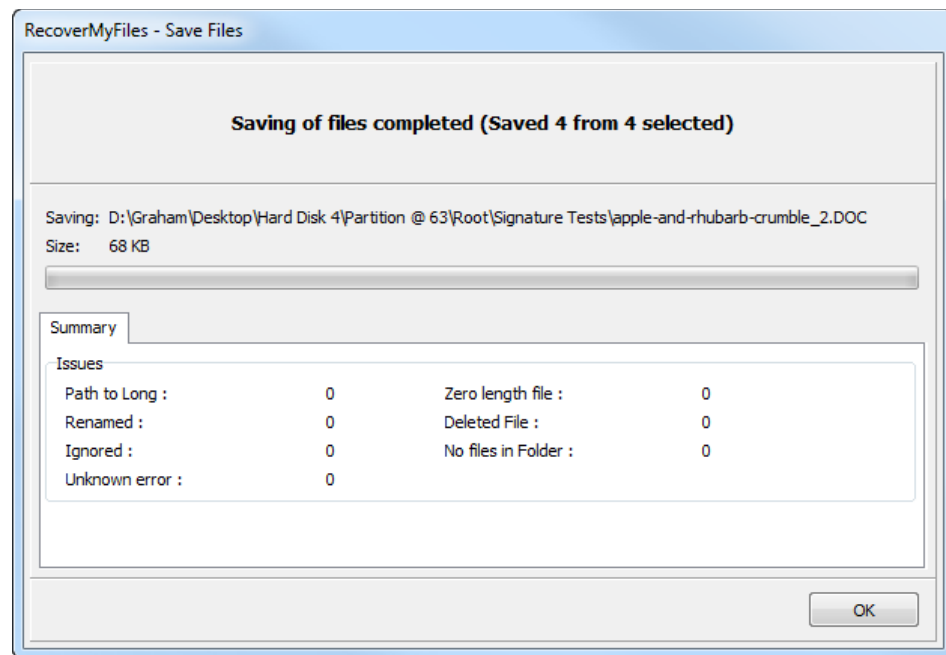
10.3.7 WHAT WILL THE FILES LOOK LIKE WHEN THEY ARE SAVED?

With default save options set, the saved files will have the same folder and file structure that appears in the "Folder" window. The first level saved folder is the device name (i.e. for a Recover Files search it will be a drive letter, e.g. "C", and for a Recover Drive search it will be the name of the device searched, e.g. "Hard Disk 1").

10.3.8 WHAT HAPPENS AFTER I SAVE THE FILES?

As a file is saved, the tick is removed from the selection box. The file stays in the search results window. Re-select the file and repeat the process if you wish to save a second copy.

Once the files have been saved, use Windows Explorer to go to the drive on which the files are saved and open them with their creating application, e.g. Microsoft Word, to make sure they open correctly.

Never write new data to the problem drive until you are sure that you have recovered all data that you need. Writing new data to the drive will change its content and may overwrite and destroy deleted or missing files so that a new search with Recover My Files will no longer find them.

Once the files have been saved and tested, use Windows to move or copy them to the required location. If you are running a drive recovery, consider replacing a problem drive rather than re-using it.

Now is a good time to make a copy of the files as a secure backup!

⚠ **Troubleshooting:** The saved files do not open. See 11.4.

Chapter 11 - Troubleshooting

In This Chapter

11.1 TROUBLESHOOTING DRIVE SELECTION

Important: If you hear an unusual **clicking or grinding noise** coming from a hard drive it is an indication that it has physical damage. Power down the drive immediately and seek assistance from a hardware recovery service.

If the physical **hard drive is not listed:**

> Check for basic connection issues (cables / power etc.). Can you hear the drive spinning? Is the drive light on?

> Check Windows Drive Management (right click on My Computer > Manage > Drive Management) to ensure the device is being correctly recognized.

> Look for the correct drive based on the physical drive size. Note that drive manufacturers usually round-up drive size, so a 480GB drive in Windows Drive Management may be labeled on the drive as 500GB.

> If the hard drive is not correctly recognized by your PC, Recover My Files will not be able to search the drive. You may consider a different type of connection to solve this problem, e.g. try a different USB case, or a direct connection to the PC. Contact technical support for further assistance. If trying different connection options, press the "**Refresh"** button in the drive selection window to refresh and redisplay the available drives to search.

The **drive letter of the problem drive is not listed:**

> If the drive letter of the problem drive is not listed, select and search the hard disk

My **digital camera is not listed as a drive:**

> Some digital cameras have a proprietary connection to your computer which Recover My Files cannot recognize as a drive letter. In this case you will need to use a digital camera card reader, an inexpensive device into which your digital camera memory card is inserted and then connected to your PC (usually via a USB connection).

My **iPod Touch or iPhone is not listed as a drive:**

> The iPod Touch and iPhone have proprietary protection which prevents software from gaining access to the drive letters. Recover My Files is not able to search these devices. Other apple devices do not have this issue.

11.2 SEARCH SPEED

Knowing when to stop a search

In most data loss situations Recover My Files is capable of getting back all files within 2 hours (and often in much less time). The greatest time savings can be achieved by knowing when to stop a search.

The longest search component of Recover My Files is the sequential search of a hard drive for "Lost" files (by file signature). However, it is rarely necessary to let this search run over the entire drive. Refer to 8.4.2 (File Recovery) and 0 (Drive Recovery) for more information on stopping the search.

General Speed Issues

If you are experiencing a slow search speed, check the following:

- Ensure that you are using the **best available equipment**. Data recovery is a resource intensive process and a slow CPU speed will lengthen the search.

- If you are recovering from an external USB drive, **USB2 is the minimum** speed requirement.

- **Bad sectors** on the problem drive can slow down a search. If the problem drive has bad sectors and is unstable, consider a hardware data recovery service. If you wish to proceed with the software option:

    o Consider taking a disk image of the drive (see Chapter 14 – Drive Imaging), or

    o Process the drive in sections (avoiding bad sectors) by using the Options > Advanced "prompt for start block" option (learn more in chapter 12.4).
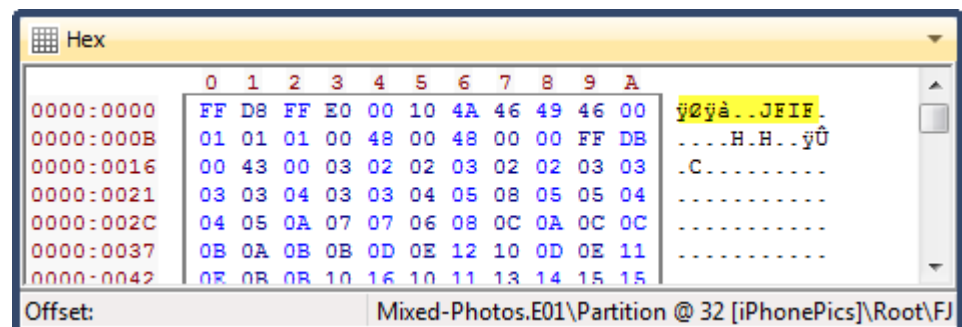
    Ensure that your **PC power settings** are configured to maintain maximum power settings throughout the search so that power to a problem drive is not lost. See Chapter 7 for more information.

11.3 FILES DO NOT PREVIEW IN SEARCH RESULTS SCREEN

Files which do not preview

Not all file types will preview in the Recover My Files display window. If you are not able to preview a file, switch to Text or Hex view to determine if the file has a valid header and recognizable content. The example in Figure 69 below shows a JPEG file in HEX view with a valid JPG header. In this instance, the only way to determine if the file is valid is to save the file and try and open it.
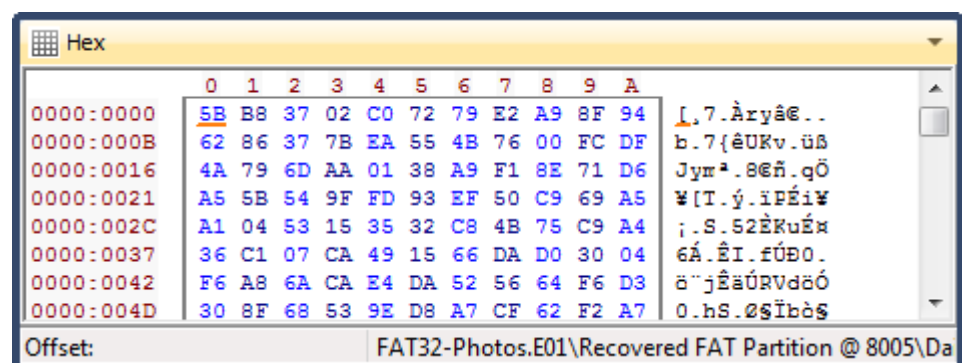
Figure 69, Hex view of a JPG file showing a valid JPG header

Corrupt files

It is not unusual in a data recovery that some files may be corrupt. The principal reason for this is that new data has been written to the drive since the data loss and the content of the missing file has been overwritten and destroyed. It is also possible that a corrupt partition no longer points to the correct location on the drive for a file. Corrupt files present with random data, as seen in Figure 70 below:

Figure 70, Hex view of a corrupt JPG file

Corrupt files can rarely be repaired. If possible, do not save these files. They can be identified by running the Validate Extension tool described in 10.1.1.

A hardware issue

A hardware issue during a search can break the connection between the search results and the problem drive. For example, a drive may lose power after the

completion of the search. In this case, all previewed files will show now data, as seen in Figure 71 below:

Figure 71, Hex view of a file showing blank data
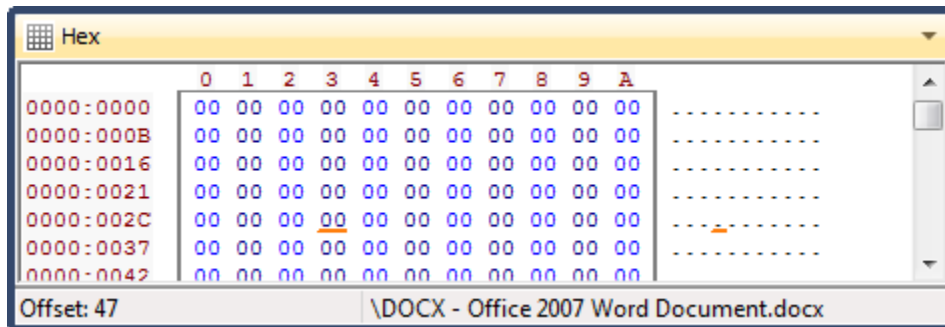
To recover from this problem:

1. Save a listing of the search results to a .rsv using the Save Session button in the program toolbar;

2. Close Recover My Files;

3. Listen to the drive to determine if it has power and is spinning (If an unusual grinding or clicking noise can be heard, power down immediately and seek assistance from a hardware data recovery service). Check the status of the drive in Windows > Disk Management.

4. If the problem drive is a USB, disconnect the drive and power the drive down and up. If the drive is a non USB, consider a reboot of the computer;

5. Double-check computer power settings (see Chapter 7) to ensure that is not a power related issue;

6. Reconnect the problem drive,

7. restart Recover My Files and load the search results using the "Load Session" button in the toolbar;

8. Click individual files in the search results screen to identify if the files preview.

11.4 SAVED FILES DO NOT OPEN

Were you able to preview the file in the search results screen?

Corrupt files which did not preview in the search results screen are unlikely to open once saved. The Validate Extension tool described in 10.1.1 is an automated method of identifying corrupt files and excluding them from the save process.

Conversely, if a file did preview in the search results screen, but does not open once saved, it is an indication of an error during the save process.

Does the file contain valid data?

Open the saved file and view the raw data to determine its content. To do this for small files, change the file extension to .txt and open in notepad. For larger files, download and use a hex editor.

In some instances a storage device may power down (or go flat) during the save process. This may cause Recover My Files to save blank files. If this is the case, follow the instructions provided in 11.3 above.

The file contains data but will not open

If the saved file contains data, but does not open, it is likely that it is partially or totally corrupt. Examine the header and content of the file to determine if it has a recognizable file header or read able content. Try an alternate method to open the file. For example:

- **Photos**: Irfanview (www.irfanview.com) is a free graphics viewer which is good at opening corrupt image files;

- **Doc Files:** Word Repair (www.wordrepair.com) is a free Word repair utility that can extract text from damaged .doc files

- **PST Files:** Recover My Email (www.recover-my-email.com) is a tool for reading corrupt Microsoft Outlook .PST files.

If problems persist with corrupt files, please contact technical support.

Chapter 12 - Options

In This Chapter

12.1 DISPLAY OPTIONS

Click on the "Options" button in the toolbar of the main program screen to set program options:
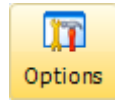
Default options can be reset at any time by selecting the "Reset to Defaults" button.

Figure 72, Options - Display tab
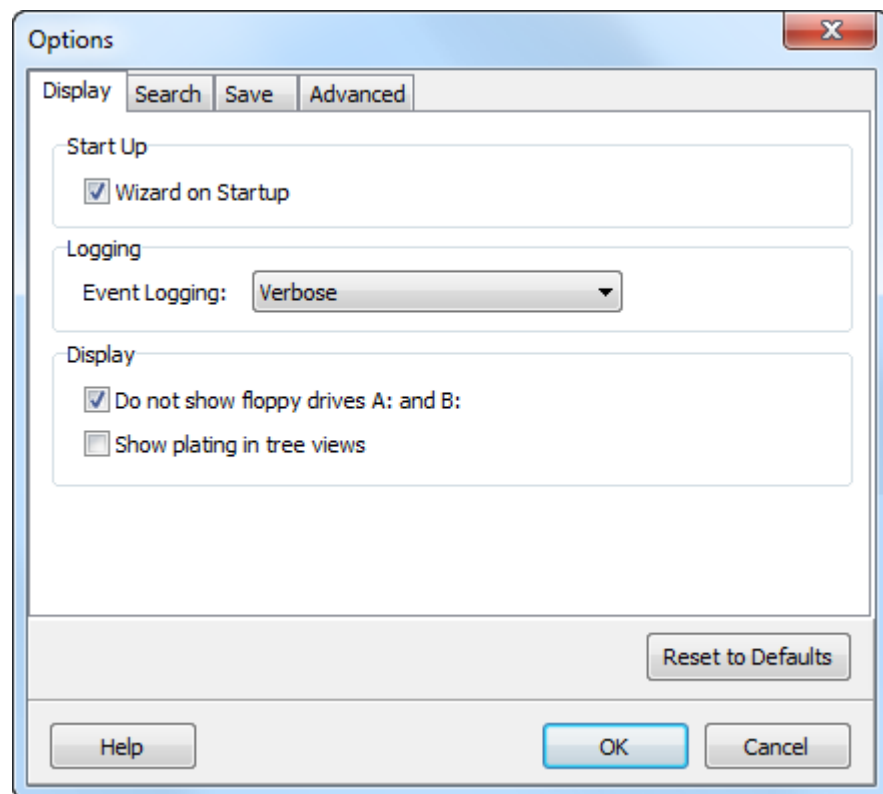
Wizard on Startup

This option controls whether the search wizard window opens automatically when the program starts.

Event Logging

This option controls the level of logging during processing. It is recommended that it be set at "None" or "Verbose" to maintain search speed. Do not use "Debug" or "Technical" unless instructed by GetData support staff.

Ignore floppy drives A: and B:

This option controls whether floppy drives connected to the computer are shown in the drive selection wizard window.

12.1.1 SHOW PLATING IN TREE VIEWS

One of the most powerful features of Tree view is the "show branch plate". When the show branch plate is turned on, all files beneath that plate are displayed as a single list in List view. For example, this action can be used to display the contents of a folder and all of its sub folders and files.

To turn the branch plate on:

1. Click Options > General > Display > **Show plating option in tree views**

2. Click the **plate icon next** to the required folder (the plate will turn orange). The content of the folder and its subfolders will be displayed in the list view:

Figure 73, The "Animals" folder is plated, showing its content in list view, and the content of its sub folders
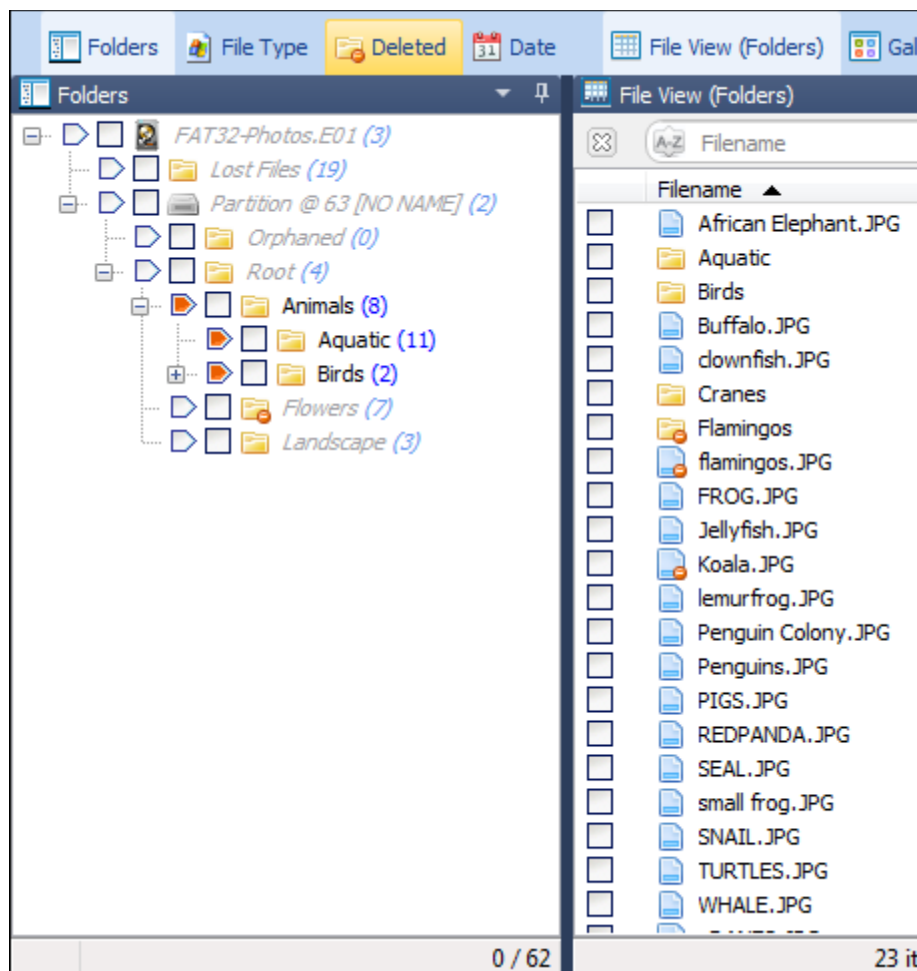
Plated folders are displayed in **normal font**. The non-plated folders are in **grey italic**.

To **plate multiple branches**;
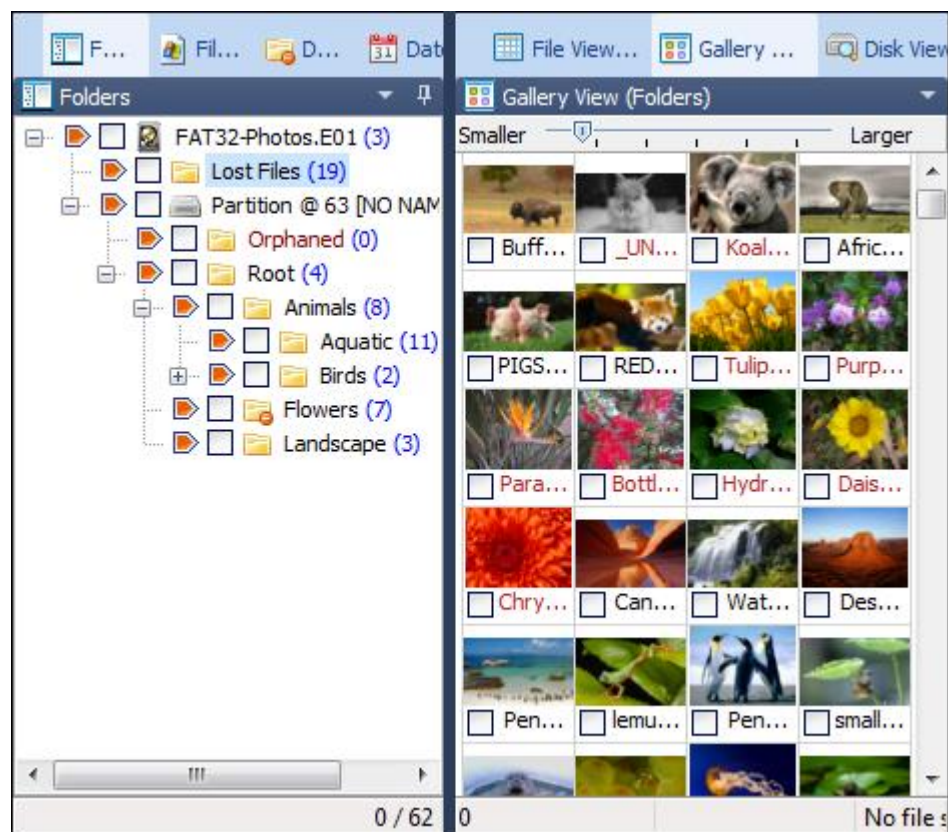
1. Click the **first required plate** with the mouse;

2. Hold down the **CTRL** key and click **the other required plates**.

Figure 74, Plating of multiple branches
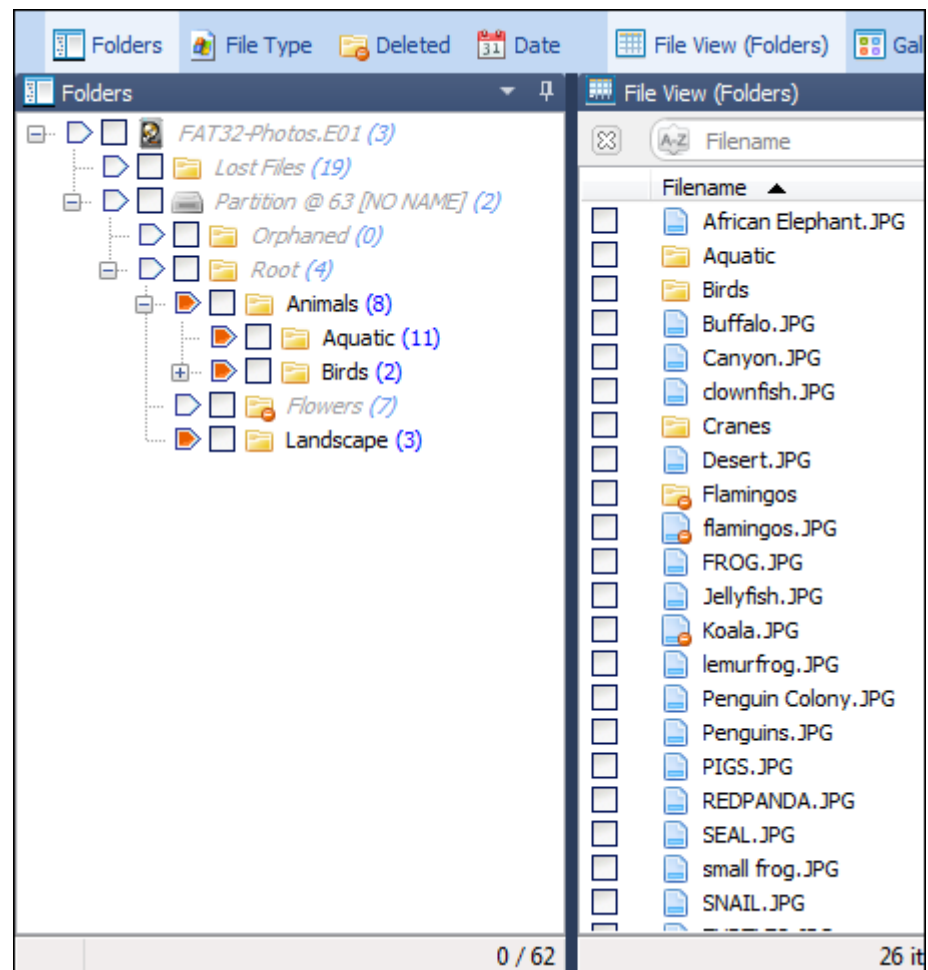
A useful application of the branch plate is to Gallery view all pictures on the drive. To do this, select the branch plate for the Root folder, Partition, or drive, and then switch to Gallery view (as shown in Figure 75 below):

Figure 75, Plated folders with Gallery view

12.2 SEARCH OPTIONS

Figure 76, Options - Search tab
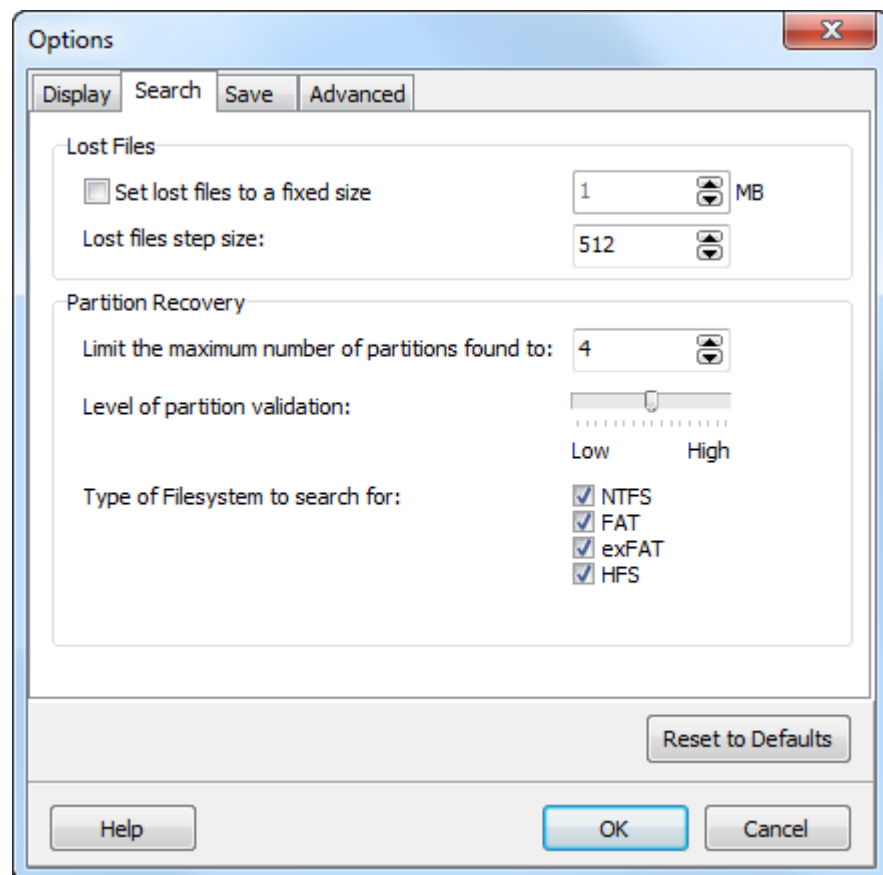
Lost Files

Lost Files are located by a sequential search of the drive looking for headers of selected file types. (See Data Recovery Fundamentals at the start of this manual for more information).

Set lost files to a fixed size

When a file header is located, calculations are performed to locate the end of the file. If the file end is not found it is assigned a default file size according to that file type. The size of lost files can be forced to a fixed size using this option.

Lost file step size

The step size control how the Lost File search sequentially steps down the drive looking for headers of selected file types. The default option is 512 bytes (sector by sector). Only change this option if you know the allocation size of the drive being searched.

Partition Recovery

Limit the maximum number of partitions fount to:

This setting puts a limit on the number of recovered partitions displayed in search results screen. Each found partition is given a validity score, with the highest validity partitions added to the search results screen until this limit is reached. It is recommended that this setting be left at the default option.

Level of partition validation

This option controls the amount of processing to determine the validity of a recovered partition:

- A high setting is more likely to show valid partitions only. It will however increase processing time and may exclude some corrupt partitions from which files may have been recovered.

- A low setting is likely to show all partitions, but some may contain invalid data.

It is recommended that this option be left at a balanced setting.

Type of File-system to search for

In a Recover Drive search, this option controls the types of File-systems that will be searched for. If the File-system that is trying to be recovered is known, the search speed can be improved by selecting only that File-system in the list. It can also make search results clearer by not recovering any unwanted partition types and presenting them in the search results.

12.3 SAVE OPTIONS

Figure 77, Options - Save tab
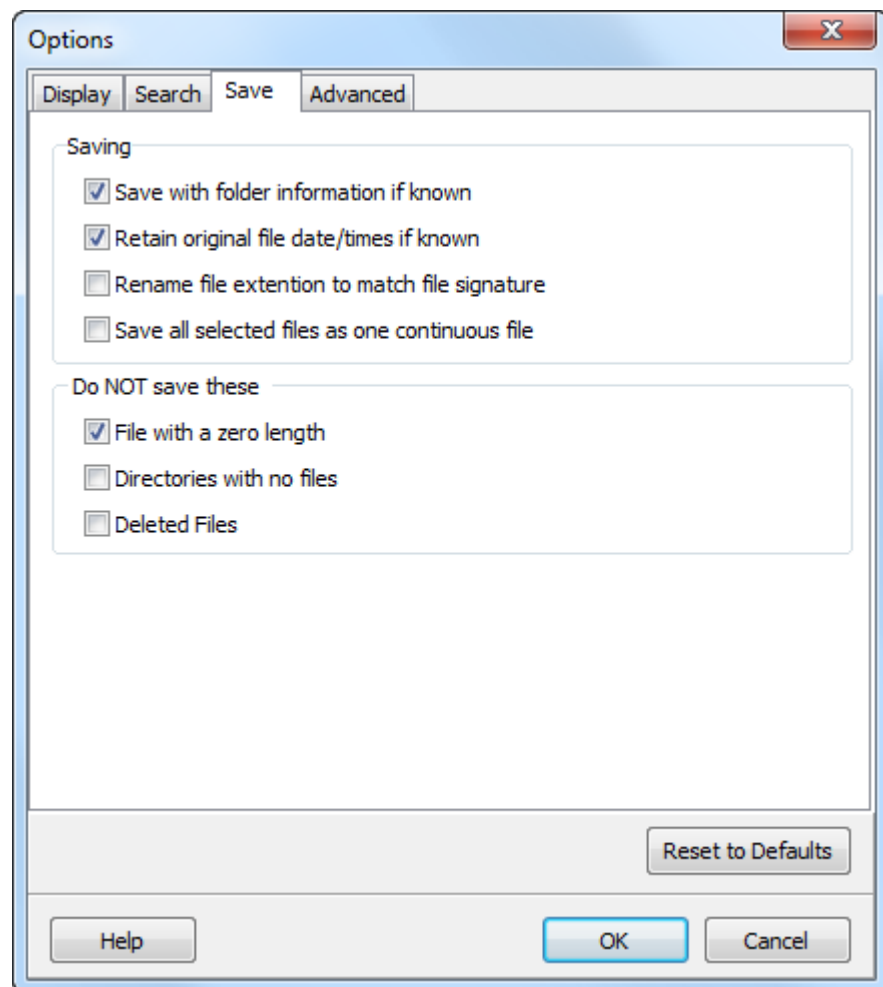
Save with folder information if known

Files are saved with the file and folder structure shown in the Folder data view. If this option is deselected, files will be saved into a single folder only.

Retain original file date/times if known

If this option is set the saved files will have the file date and times shown in the data views of the results screen. If this option is not selected, saved files will show the date and times when the save took place.

Rename file extension to match file signature

If this option is selected a file that has an extension which does not match the file signature (the header) will be renamed when saved. (See "Determine file type" in the "Search" options above).

Do NOT save these

Files with a zero length

If this option is set files with a 0kb length will not be saved.

Directories with no files
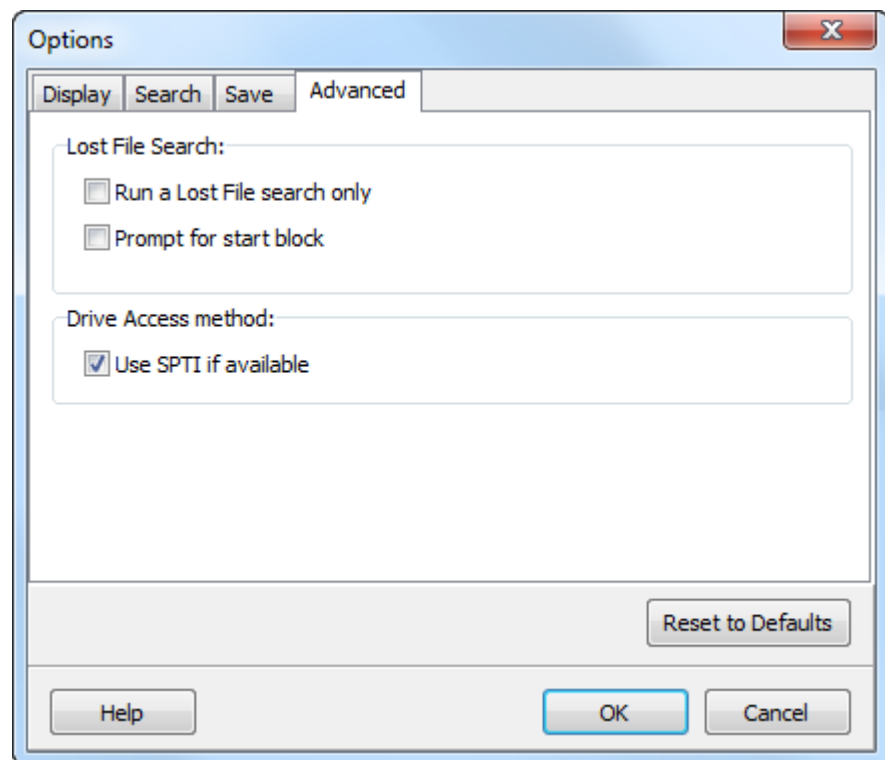
If this option is set empty folders will not be saved.

Deleted files

If this option is set, deleted files are not saved (i.e. files marked in the "Is Deleted" column as "Yes"). This option is usually set in a Drive Recover when the user wants to recover the file and folder structure from a drive but does not require any of the deleted files contained within that file-system.

12.4 ADVANCED OPTIONS

Figure 78, Options - Advanced tab

Run a Lost Files search only (do not read existing File-system)

When this option is selected, Recover My Files will search only for Lost Files (a sequential search of the drive for the file headers of the selected file types - Learn more about Lost Files in Data Recovery Fundamentals at the start of this manual).

Prompt for start sector

A Lost File search can be specified to start at any block on the drive. This option can be used to:

- Process large drives in segments, rather than a search of an entire drive in one pass. For example, the drive can be divided into quarters and four separate searches run over each quarter of the drive.

- Skip bad sections of a drive. For example, if a drive is known to have bad sectors at a certain point, a search can be stopped prior to this point and then a new search started after this point.

- To seek out the starting point of a partition. For example, if an unallocated hard disk had two equal partitions the search could be started just prior to the middle of the disk to quickly locate the second partition.

When the "Prompt for start block" option is selected, the following window will appear when a search for lost files commences:
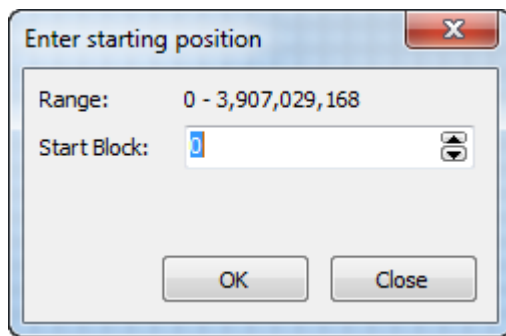
Enter the starting position and click ok. The search will commence from the block entered.

Use SPTI if available

- SPTI (SCSI pass through Interface) is an API, allowing Microsoft Windows applications (starting with NT/2000) to work with SCSI-devices. It is recommended that this option is selected.

Reset to Default

Clicking the reset to defaults option is a global reset for Display, Search, Save and Advanced.

Chapter 13 - RAID recovery

In This Chapter

13.1 RAID - INTRODUCTION

Recover My Files supports the analysis of the following types of RAID:

JBOD

JBOD (Just a Bunch of Drives) 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.

RAID 0

A RAID 0 (also known as a stripe set or striped volume) splits data evenly across two or more drives (striped) with no redundancy. RAID 0 is normally used to increase performance, as the two or more drives can write or read a file concurrently.

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

RAID 5

A RAID 5 uses block-level striping with parity data distributed across all member drives. 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.

13.2 PREPARATION

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

Successful RAID setup in Recover My Files 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 drives make up the RAID?

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

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

13.3 SEARCHING A FUNCTIONING RAID

If a hardware or software RAID is recognized correctly b a PC and is visible by the Windows operating system, the drive can be searched normally by following the instructions for a Recover Files (Chapter 8) or Recover Drive (Chapter 9) search.

13.4 REBUILDING A BROKEN RAID

If the RAID is not functional, it can be rebuilt in Recover My Files and searched. A RAID can be constructed from:

- Physical disks;

- Disk image Files; or,

- A combination of both physical drives and disk image files.

To add a RAID drive to a search:

1. Start a search and select the required search mode, **Recover Files** or **Recover Drive**. Click **Next**;

2. In the Device Selection window, click on the [Add RAID] button. This opens the RAID configuration window.

Figure 80, RAID configuration

13.4.1 HARDWARE RAID

Enter the known hardware RAID parameters into the configuration window. If you do NOT know the parameters, Recover My Files will attempt to identify the way in which the hardware RAID was configured. To do this:

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

2. Click the **Add Drive** or **Add Image** button to add the physical drives and/or image files in the correct sequence. If the correct sequence is unknown, add them in the order that is believed 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;

4. Click **OK** to add the configured RAID to the drive selection window. The RAID can then be selected and searched like any other device.

Note that the 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
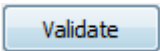
by adding the image to the case to determine if individual files can be accessed and previewed. If the Find Layout button did not return a suggested configuration, or, the suggested configuration did not result in a successful recovery;
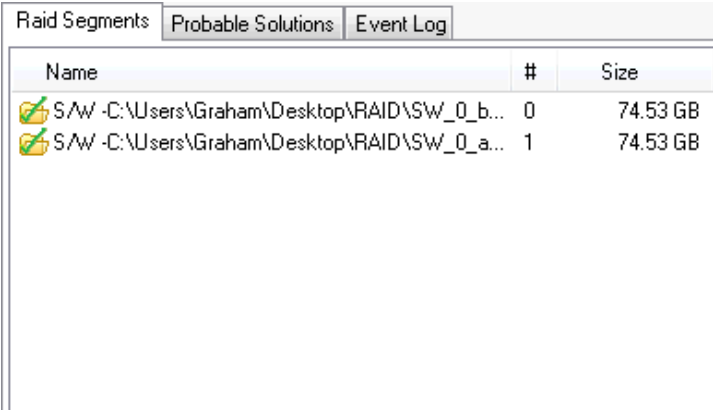
- Click on the "Probable Solutions" tab to view suggested configurations for the RAID;

- change the "stripe size", RAID Options and drive sequence as suggested;

- click the "Test Layout" button to test the modified configuration; and,

- add the RAID drive and run a new search.

Repeat this process until a search result preview indicates that the RAID is correctly configured.

13.4.2 SOFTWARE RAID

To add a software RAID:

1. In the RAID configuration window, set the "Type" of RAID to "software";

2. Press [Validate] to confirm a valid software RAID. A valid software RAID will show with green ticks on the added drives (or image files):

Raid Segments	Probable Solutions	Event Log		
Name			#	Size
S/W -C:\Users\Graham\Desktop\RAID\SW_0_b...			0	74.53 GB
S/W -C:\Users\Graham\Desktop\RAID\SW_0_a...			1	74.53 GB

If validation fails, change the drive order using the 🔼 buttons.

3. Click **OK** to add the configured RAID to the drive selection window. The RAID can then be selected and searched like any other device.

Chapter 14 - Disk Imaging

In This Chapter

14.1 GETDATA'S FORENSIC IMAGER

Included in the Recover My Files installation folder is the stand alone drive imaging program "**Forensic Imager**". Forensic Imager is a Windows based program that will acquire a sector copy ("image") of a drive into one of the following common forensic file formats:

- DD /RAW (Linux "Drive Dump")

- AFF (Advanced Forensic Format)

- E01 (EnCase®) [Version 6.xx format]

14.2 RUNNING FORENSIC IMAGER

Forensic Imager is run from the Recover My Files drop down menu by selecting the "Disk Imager" option:

Figure 81, Recover My Files drop down menu
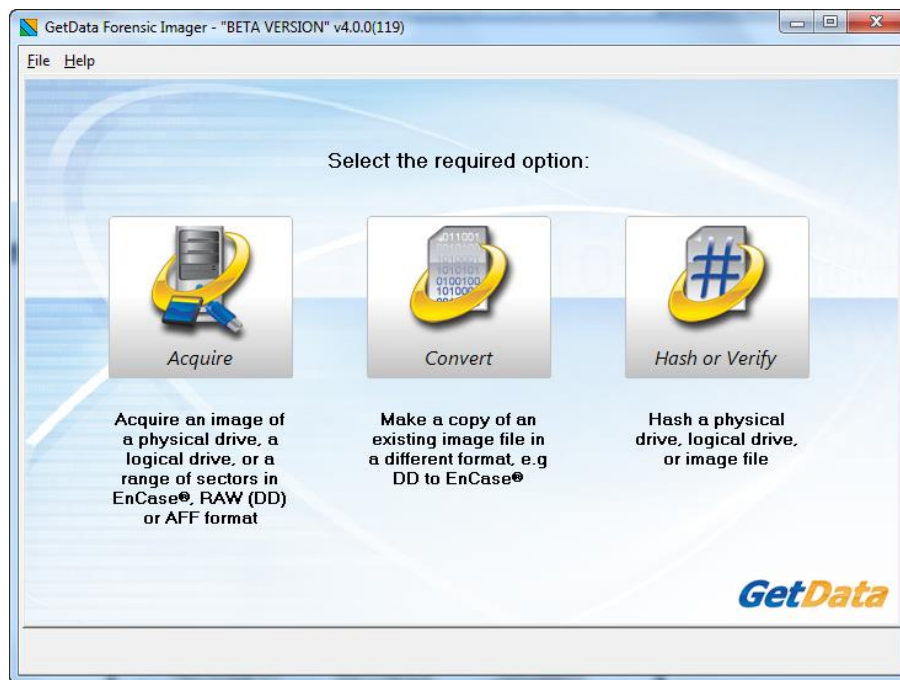
Or by selecting the Disk Imager shortcut from the "Windows Start > All Programs > Recover My Files v6 > Disk Imager" shortcut.

When Forensic Imager is run the wizard presents 3 options:

Acquire: The acquire option is used to take a forensic image (an exact copy) of the target media into an image file on the investigators workstation;

Convert: The convert option is used to copy an existing image file from one image format to another, e.g. DD to E01;

Hash or verify The hash or verify option is used to calculate a hash value for a device or an existing image file.

As shown in Figure 82 below:

Figure 82, Forensic Imager

When "Acquire" or "Convert" is selected, the subsequent work flow is:

1. Select source;

2. Select destination options;

3. Create the image;

4. Display and save event log.

When "Hash or Verify" is selected, the subsequent work flow is:

1. Select source;

2. Verify;

3. Display and save event log.

The workflow is discussed in more detail below:
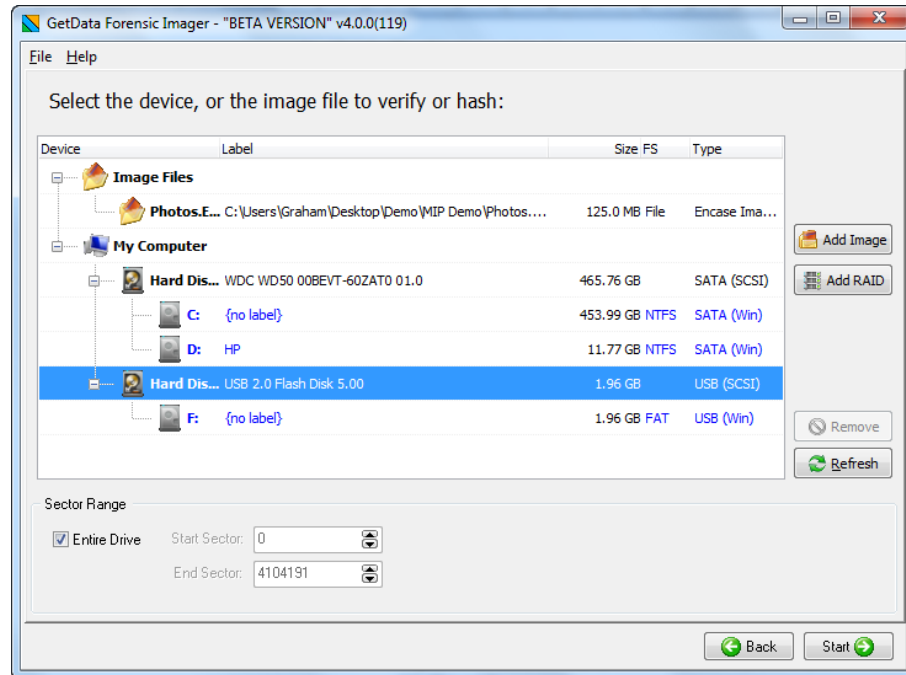
1. SELECTING THE SOURCE

When the "Acquire", "Convert" or "Hash or Verify" button is selected, the source selection screen is displayed enabling selection of the source media:

- When "**Acquire**" is selected, the source window shows the available physical devices (hard drives, USB drives, camera cards, etc.) and logical devices (partitions or volumes on the physical devices, e.g. "C:" drive) attached to the forensic workstation.

- When "**Convert**" is selected, the source window allows the selection of the source image file. Click the "Add Image" button to add the required image file to the selection list.

- When the "**Hash or Verify**" button is selected, the source window allows the selection of either a physical or logical drive, or an image file.

Figure 83, Forensic Imager - selecting the source device (Hash or Verify option shown)

The device selection window includes the following information:

Label: Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used). Image files show the path to the image.

Size: The size column contains the size of the physical or logical device, or the size of the image file. Note that the actual size of the drive is usually smaller than what the drive is labeled. Drive manufacturers usually round up the drive capacity, so a 453.99 GB drive in this screen may be sold as 500GB.

FS: The File-system on the drive, e.g. FAT, NTFS or HFS;

Type: Describes the way in which the drive is connected to the computer. An image file will show the type of image (e.g. EnCase or RAW).

Acquisition of physical vs. logical device

In most situations, pending compliance with any overriding case specific legal requirements, an investigator is most likely to select and image a physical device. Imaging the physical device gives access to the content of the entire media, for example, the space between partitions. Carrier, 2005, observes: *"The rule of thumb is to acquire*

data at the lowest layer that we think there will be evidence. For most cases, an investigator will acquire every sector of a drive". (2 p. 48)

In specific circumstances, an investigator may need to acquire a range of sectors from the device. In this case, start and end sector information in entered in the sector range fields at the bottom of the source selection window.

To select the source:

1. **Highlight** the required **device** or **image file** using the mouse;

2. Click the "**Next**" button to proceed to the destination window.

2. SELECTING THE DESTINATION

The image destination screen, shown in Figure 84 below, is where the parameters for the image file are set, including type, compression, name, location etc.

Figure 84, Setting destination options
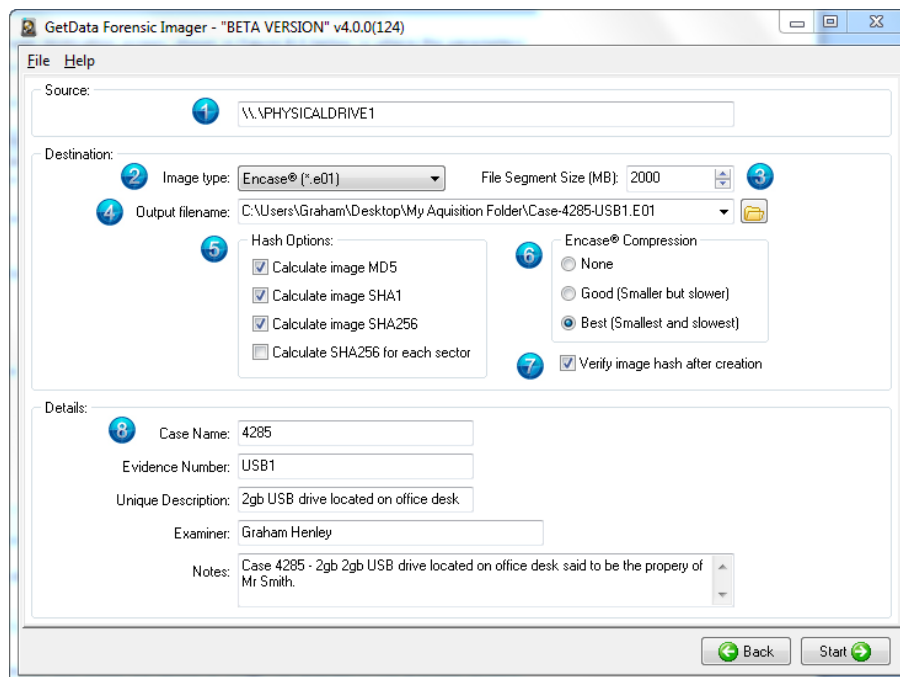
1. SOURCE

The source field shows the device or image file selected in the previous window. This source field cannot be edited here. Select the back button if a change to the source is required.

2. IMAGE TYPE

The investigator has the choice of creating the forensic image in one of the following forensic file formats:

DD / RAW:

The DD / RAW format originates from the UNIX command line environment. DD /RAW images are created from blocks of data read from the input source and written directly into the image file. The simplicity of a DD image makes it possible to compare the imaged data to the source, but the format lacks some of the features found in more modern formats, including error correction and compression.

Advanced Forensic Format (AFF):

AFF is "an extensible open format for the storage of drive images and related forensic metadata. It was developed by Simson Garfinkel and Basis Technology". (3). Refer to http://afflib.org/ for further information.

 EnCase®.E01

The EnCase® E01 evidence file format was created by Guidance Software Inc. It is widely accepted in the forensic community as the imaging standard. Further information is available at www.guidancesoftware.com. The structure of the EnCase®.E01 format allows for case and validation information (CRC and MD5) to be stored within the image file. The structure of the EnCase® file format is shown below:

Figure 85, EnCase® header
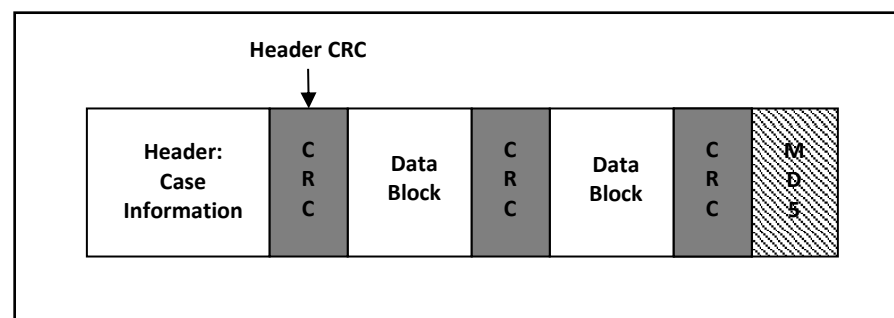
Source: (4)

3. FILE SEGMENT SIZE

Sets the segment size of the created forensic image file:

This setting enables the forensic image file to be broken into segments of a specific size. Setting an image segment size is primary used when the forensic image files will later be stored on fixed length media such as CD or DVD.

For the EnCase®.E01 image format, Forensic Imager uses the EnCase® v6 standard and is not limited to a 2 GB segment size. However, if an investigator plans to use larger file segments they should give consideration to the limitations (RAM etc.) of the systems on which the image files will be processed.

4. OUTPUT FILENAME

Sets the destination path and file name for the image file:

The output file name is the name of the forensic image file that will be written to the investigators forensic workstation. Click on the folder icon to browse for the destination folder.

5. HASH OPTIONS

Calculates an MD5 and/or SHA256 acquisition hash of the imaged data:

A hash value is a mathematical calculation that is used for identification, verification, and authentication of file data. A hash calculated by Forensic Imager during the acquisition of a device (the "acquisition hash") enables the investigator, by recalculating the hash at a later time (the "verification hash"), to confirm the authenticity of the image file, i.e. that the file has not changed. Any change to the acquired image will result in a change to the hash value.

Calculation of HASH values during the acquisition process requires CPU time and will increase the duration of an acquisition. However, it is recommended, in line with accepted best forensic practice, that an acquisition hash is always included when acquiring data of potential evidentiary value. It is also recommended that the investigator regularly recalculate the verification hash during the investigation to confirm the authenticity of the image.

Forensic Imager has three independent hash calculation options, MD5, SHA1 and SHA256. The investigator should select the hash option/s which best suits:

MD5 (Message-Digest algorithm 5):

> MD5 is a widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). It is a 128-bit hash value that uniquely identifies a file or stream of data. It has been extensively used in computer forensics since the late 1990's.

> In 1996 cryptanalytic research identified a weakness in the MD5 algorithm. In 2008 the United States Computer Emergency Readiness Team (USCERT) released vulnerability Note VU#836068 stating that the MD5 hash:

> *"…should be considered cryptographically broken and unsuitable for further use".* (5).

SHA1

> In 1995 the Federal Information Processing Standards published the SHA1 hash specification which was adopted in favor of MD5 by some forensic tools. However, in February of 2005 it was announced that a theoretical weakness had been identified in SHA1, which suggests its use in this field may be short lived. *(6) (7)*

SHA-256:

> From 2011, SHA-256 is expected to become the new hash verification standard in computer forensics. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the National Security Agency (NSA), and published by the USA National Institute of Standards and Technology.

For more detailed information on hashing and how the strength of a hash value applies to the forensic investigator suggested reading includes: *"The Hash Algorithm Dilemma– Hash Value Collisions", Lewis, 2009, Forensic Magazine, www.foreniscmag.com.*

Sector Hashing

The fourth option in the hash section is "**Calculate SHA-256 for each sector**". When this option is selected a separate SHA-256 hash for each individual sector of the target device is created and stored in a file in the same folder as the iamge file.

Like the more commonly used "file hash", a sector hash can be used to:

- Reduce the volume of a data set by excluding known and trusted sectors from the case. For example, the hash of a blank sector can be used as the identifier to eliminate the need to search all blank sectors in the case; or

- Locate fragments of known files. For example, an investigator may search for a fragment of a known document or image file and positively identify the existence (or partial existence) of that file on a drive even if only one sector of that file remains on the drive.

For more information on sector hashing, refer to Yoginder Singh Dandass; Nathan Joseph Necaise; Sherry Reede Thomas, *An Empirical Analysis of Drive Sector Hashes for File carving*, Journal of Digital Forensic Practice, Volume 2, Number 2, 2008, 95-104.

6. ENCASE® COMPRESSION

Sets the compression level for the EnCase® forensic image file

The EnCase®.E01 file format supports compression of the image file during the acquisition process. Compressing a forensic image file during the acquisition process takes longer, but the file size of the forensic image on the investigators workstation will be smaller. The amount of compression achieved will depend upon the data being imaged. For example, with already compressed data such as music or video, little additional compression will be achieved.

AFF and DD/RAW image formats do not support compression.

7. VERIFY IMAGE HASH AFTER CREATION

During the acquisition of a device the "source" hash (MD5 and/or SHA1 and/or SHA256 as per the investigator selection) is calculated as the data is read from the source drive. Once the acquisition is complete, the source hash is reported in the event log in the format:

Source MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

For EnCase®.E01 files the MD5 acquisition hash is embedded within the header of the image file.

When the "Verify image hash after creation" box is selected, at the completion of writing the image file Forensic Imager reads the file from the forensic workstation and recalculates the hash. The verification hash is reported in the event log in the format:

Verify MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

At the conclusion of the verification process a comparison is made between the source and verification hash. An exact image of the source drive to the image file should result in a "match":

MD5 acquisition and verification hash: Match

Should the acquisition and verification hash not match, it is an indication that a problem has occurred and the device should be re-acquired.
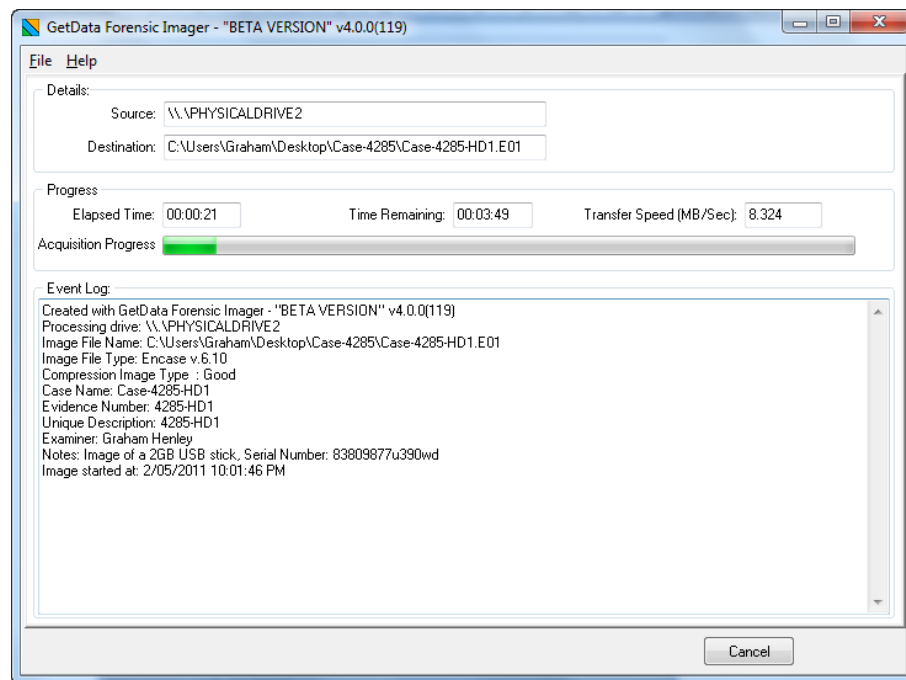
8. DETAILS

For EnCase®.E01 files, information entered into the "Details" files are written into the image file header and stored with the image. DD/RAW and AFF files do not store this information as part of the image, however they are still required to be entered as for all formats the information is included in the Forensic Imager event log.

3. PROGRESS

The progress screen displays source information (the drive being acquired) and destination information (location where the forensic image files is being written). Progress information, including elapsed time, time remaining and transfer speed is displayed. The progress window is shown in Figure 6-8 below:

Figure 86, Forensic Imager Progress screen

The event log provides feedback to the investigator during the image process.

4. LOG FILE

The event log for each acquisition is automatically saved to the same folder as the image file/s. A typical event log contains the following type of information:

Created with GetData Forensic Imager - v4.0.0(124)
Processing drive: \\.\PHYSICALDRIVE1
Image File Name: C:\Users\Graham\Desktop\My Acquisition Folder\Case-4285-USB1.E01
Image File Type: Encase v.6.10
Compression Image Type : Best
Case Name: 4285
Evidence Number: USB1
Unique Description: 2gb USB drive located on office desk
Examiner: Graham Henley
Notes: Case 4285 - 2gb USB drive
Image started at: 4/05/2011 11:45:50 PM
Image finished at: 4/05/2011 11:50:25 PM
Elapsed time: 00:04:34
GUID: {D6BF98CA-F3EA-4BBD-88A9-C5E5B07D8600}
Actual Source MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA
Source SHA1Hash: d11d009c71c089dfcdb3dabad4c4014078c15183
Source SHA256Hash:
3370edc5662703534d3ad539d49bcc7f0ca86f559b7faa3c4dc7f7290056d039
Verify MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA
Verify SHA1Hash: d11d009c71c089dfcdb3dabad4c4014078c15183
Verify SHA256Hash:
3370edc5662703534d3ad539d49bcc7f0ca86f559b7faa3c4dc7f7290056d039

Acquisition completed!
MD5 acquisition and verification hash: Match
SHA1 acquisition and verification hash: Match
SHA256 acquisition and verification hash: Match

14.2.1 BAD SECTORS AND ERROR REPORTING

Drive errors can occur during the image process due to a problem with the entire drive or a problem isolated to specific sectors. If a bad sector is identified, Forensic Imager writes 0's for the data that cannot be read and logs the location of bad sectors in the event log as they are found.

14.3 RECOVERING DATA FROM AN IMAGE FILE

Disk images can be created in any version of Recover My Files.

⚠ However, the ability to read a disk image file in Recover My files is limited to the evaluation version and **Professional & Technician licenses**. The add image button will not appear when Recover My Files is activated with a Standard license key (see 4.2.4 for a comparison of license features).

To recover data from an image file:
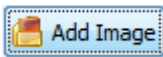
1. Run Recover My Files and select the **Recover Files** or **Recover Drive** search. Click **Next**.

2. In the drive selection window, click the [Add Image] button. Navigate to the location of the image file on your computer and **select the image** and click the **Open** button.

3. The selected image file will then be added to the drive selection window under the "Image Files" section, as shown below in Figure 65, Drive selection window showing an added image file. (To add additional image files to this list, repeat the process or to remove image files, highlight the file and use the Remove button):

Figure 87, Drive selection window showing an added image file
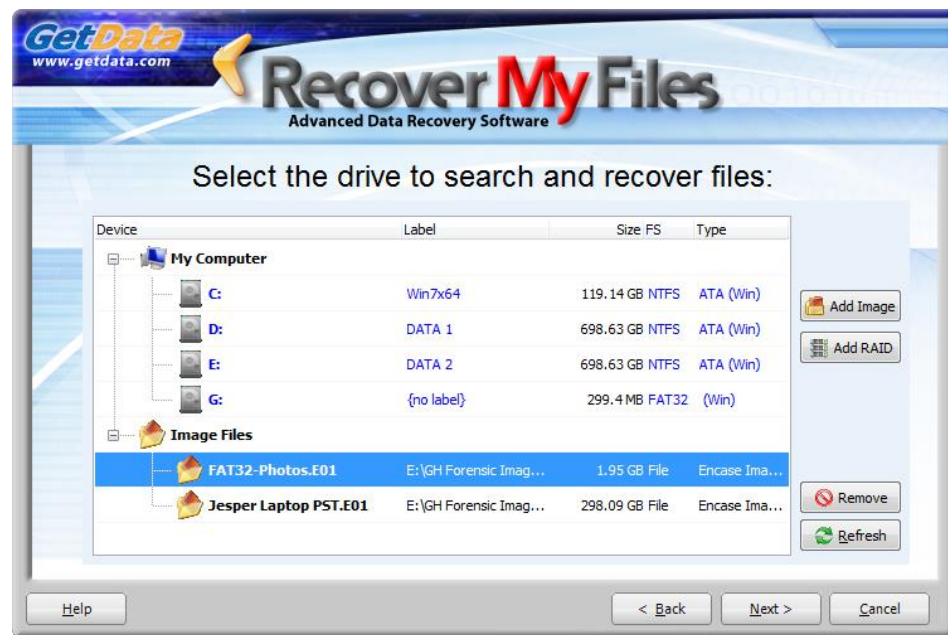
4. Highlight the required image from which data is to be recovered and press the **Next** button.

5. Continue with the data recovery as per the instructions: Chapter 8 – Recover Files, and Chapter 9 – Recover a Drive.

Chapter 15 - Customizing the Interface

In This Chapter

15.1 CUSTOMIZING THE INTERFACE

⚠️ Customizing the interface is a **Professional & Technician license** feature. Interface customization options are available in evaluation mode. However they will not appear when Recover My Files is activated with a Standard license key (see 4.2.4 for a comparison of license features).

The Recover My Files v6 user interface is highly **customizable** and has been designed to maximize the benefits of using a multi monitor computer setup .Data views in Tree, List and Display panes can be detached to operate as stand-alone windows, or moved and re-attached to another pane. Custom layouts can be saved and reloaded on demand. An example is shown below:

Figure 88, Customized interface with detached gallery view and display and hex view sharing the bottom pane

Note that GUI customization feature is license key dependent:

Evaluation mode: Data views are locked when the program is first run. When unlocked, all interface customize options are available.

Standard license: Customization options are disabled. The Recover My Files interface is locked in its default setting.

Professional license: All interface customize options are available.

Technician license: All interface customize options are available.

15.1.1 ACCESSING THE CUSTOMIZATION MENU

To access the interface customization menu, click on the ▼ icon in any data view. The following menu appears:

Figure 89, Data view customization menu
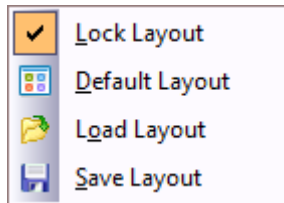
Lock Layout

When ticked, this option locks the layout in its current position (except windows that are currently detached). Its purpose is to stop the accidental detach / movement of a data views.

Default Layout

Selecting the default layout menu item returns the Recover My Files interface back to its default position, i.e. default tree pane data views left, list pane data views top and display pane data views bottom.

Load Layout

The load layout option enables the user to select an XML file containing a previously saved layout. The default open location is the Recover My Files installation folder.

Save Layout

The save layout option saves the current interface position into an XML file. The default save location is the Recover My Files v6 installation folder.

15.1.2 UNDOCKING AND DOCKING DATA VIEWS

To undock a data view:

1. In any data view, click on the ▼ icon and ensure that the "Lock Layout" option is off;

2. Click on the data view tab or title bar, old down the mouse and drag it away from its position, as shown in **Figure 90** below:
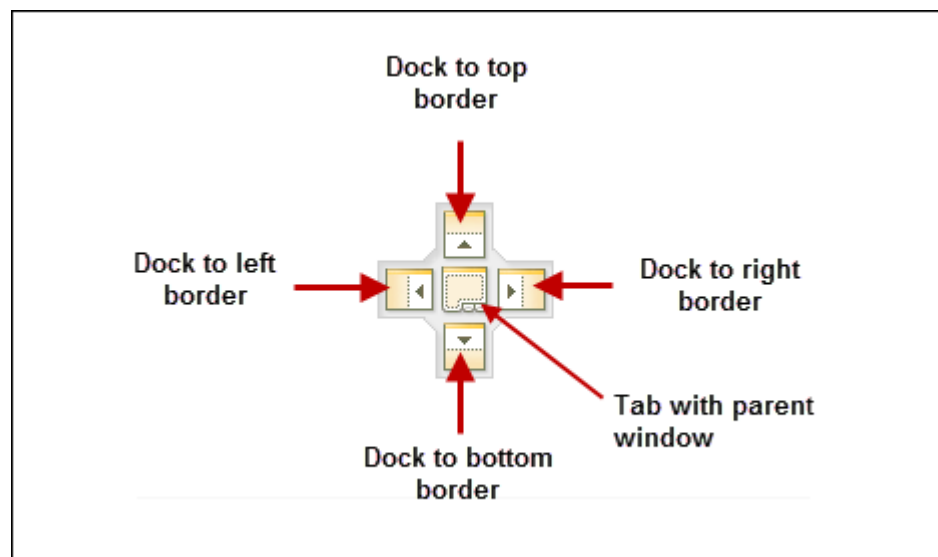
Figure 90, Undocking a view using drag and drop
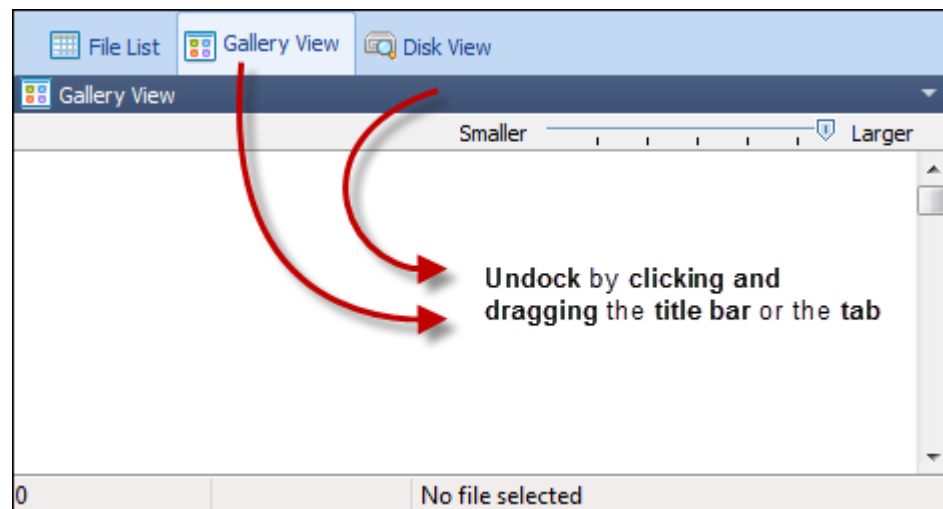
To **dock a data view**:

- Click on the data view title bar and **drag and drop** it next to **other data view tabs**; or,

- Drag and drop the data view over the **a dock arrow** as detailed below:

Figure 91, Dock positioning arrows

Chapter 16 - Legal

In This Chapter

16.1 THIS MANUAL

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

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

16.2 COPYRIGHT

This manual 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 manual 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®.

16.3 LICENSE AGREEMENT

GetData Pty Ltd ("GetData") is the developer of the software. Permission to use the software 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. GetData shall have the right to check license details at any time in any reasonable manner.

A license of the software permits you to use one copy of the Software on a single computer or, in the event that you have purchased multiple licenses, to install the Software concurrently on multiple computers equivalent to the number of licenses that you have purchased.

You are not permitted to share the product activation information provided to you for this Software with other users. Doing so will entitle GetData to immediately terminate this Agreement.

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.

GetData may from time to time revise or update the software and shall make such revisions or updates available subject to payment of the applicable license fee. Support for the Software is provided via its web sites.

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

16.4 DISCLAIMER

The software available for down loading through Internet sites and published by GetData 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.

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.

Appendix 1 - Technical Support

APPENDIX 1 - TECHNICAL SUPPORT

GetData Pty Ltd has its headquarters in Sydney Australia.

16.4.1 SUPPORT

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

Video Tutorials: http://www.recovermyfiles.com/data-recovery-videos.php

Email Support: support@getdata.com

Phone Support: USA: (866) 723-7329 callback service

Or;

Sydney, Australia: +61 2 82086053
Hours: Australian Eastern Time, 9am - 5:30pm Mon - Fri

16.4.2 SECURE POST

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

16.4.3 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 to Fri
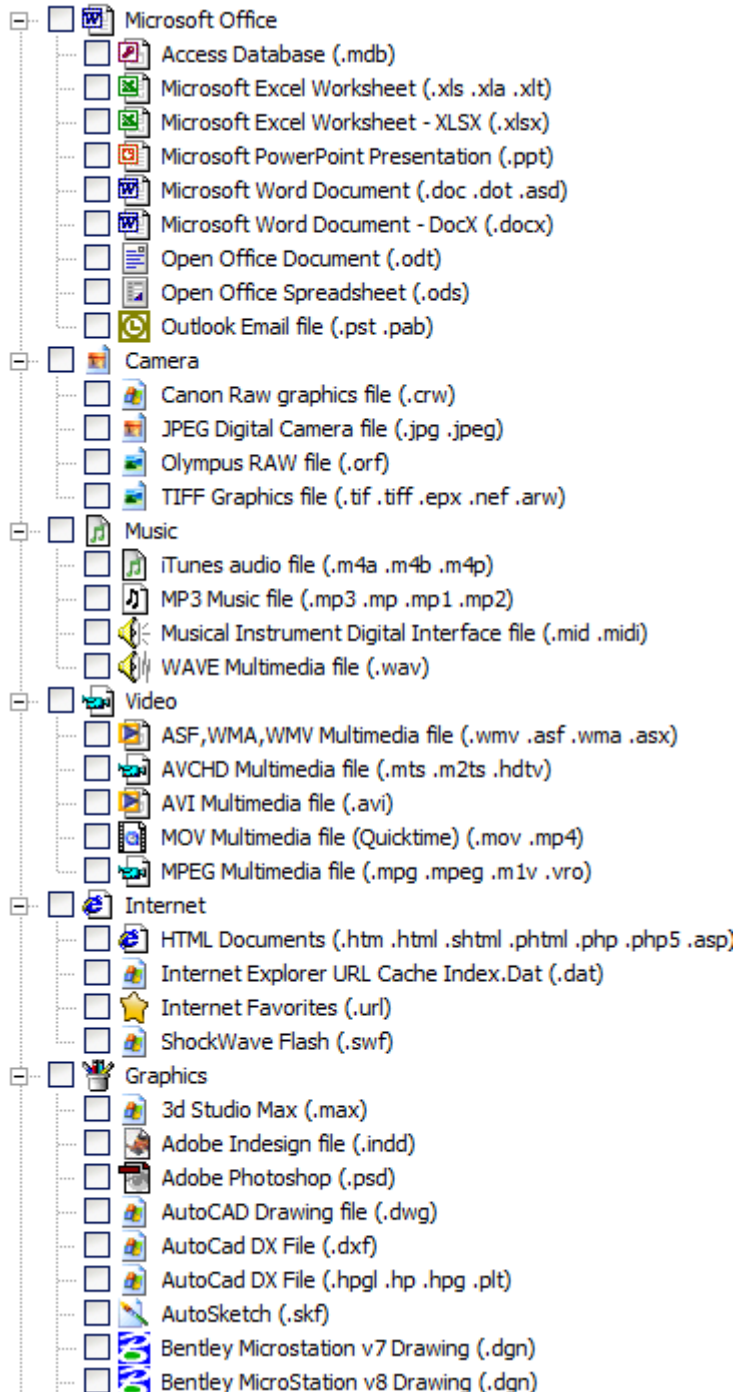
Appendix 2 - File Carving

The following file types are supported by Recover My Files file carving engine:

- Microsoft Office
  - Access Database (.mdb)
  - Microsoft Excel Worksheet (.xls .xla .xlt)
  - Microsoft Excel Worksheet - XLSX (.xlsx)
  - Microsoft PowerPoint Presentation (.ppt)
  - Microsoft Word Document (.doc .dot .asd)
  - Microsoft Word Document - DocX (.docx)
  - Open Office Document (.odt)
  - Open Office Spreadsheet (.ods)
  - Outlook Email file (.pst .pab)
- Camera
  - Canon Raw graphics file (.crw)
  - JPEG Digital Camera file (.jpg .jpeg)
  - Olympus RAW file (.orf)
  - TIFF Graphics file (.tif .tiff .epx .nef .arw)
- Music
  - iTunes audio file (.m4a .m4b .m4p)
  - MP3 Music file (.mp3 .mp .mp1 .mp2)
  - Musical Instrument Digital Interface file (.mid .midi)
  - WAVE Multimedia file (.wav)
- Video
  - ASF,WMA,WMV Multimedia file (.wmv .asf .wma .asx)
  - AVCHD Multimedia file (.mts .m2ts .hdtv)
  - AVI Multimedia file (.avi)
  - MOV Multimedia file (Quicktime) (.mov .mp4)
  - MPEG Multimedia file (.mpg .mpeg .m1v .vro)
- Internet
  - HTML Documents (.htm .html .shtml .phtml .php .php5 .asp)
  - Internet Explorer URL Cache Index.Dat (.dat)
  - Internet Favorites (.url)
  - ShockWave Flash (.swf)
- Graphics
  - 3d Studio Max (.max)
  - Adobe Indesign file (.indd)
  - Adobe Photoshop (.psd)
  - AutoCAD Drawing file (.dwg)
  - AutoCad DX File (.dxf)
  - AutoCad DX File (.hpgl .hp .hpg .plt)
  - AutoSketch (.skf)
  - Bentley Microstation v7 Drawing (.dgn)
  - Bentley MicroStation v8 Drawing (.dgn)

- Bitmap (.bmp)
- COREL Draw file (.cdr)
- DesignCAD file (.dcd)
- Encapsulated Postscript file (.eps)
- Enhanced Metafile (.emf)
- FormZ Document (.fmz .fzb)
- Freehand 10 (.fh10 .fh11)
- Freehand 7 to 9 (.fh9 .fh7 .fh8)
- Fuji Camera Raw (.raf)
- GIF graphics file (.gif)
- GIS ShapeFiles (.shp)
- GUE Map file (.gue .gmp)
- ICO File (.ico)
- JPEG 2000 (.jp2)
- JPEG Digital Camera file (.jpg .jpeg)
- Lightwave object (.lwo)
- Lightwave scene (.lws)
- MapSource 1 file (.gdb)
- Maya 3D file (.mb)
- Microsoft Photodraw (.mix)
- Microsoft Visio Drawing (.vsd .vss .vst)
- Paintbrush file (.pcx .scr)
- PaintShop Pro (.psp)
- PaperPort (.max)
- PNG Graphics file (.png)
- Portable Graphics Map (.ppm .pgm .pbm)
- PrintMaster (.hcr .biz)
- QuarkXPress file (.qxp .qxd .qxb .qxl .qpt)
- QuickCAD (.cad)
- ShockWave Flash (.swf)
- Sigma X3F Raw (.x3f)
- SmartDraw file (.sdr .sdt)
- SwishMax (.swi)
- Thumbnail file (.db)
- TurboCAD for Windows (.tcw)
- Windows Metafile (.wmf)
- XARA Graphic file (.xar)
- Documents
  - Adobe PageMaker (.pmd .p65)
  - Adobe Premier Project (.ppj)
  - Avery DesignPro (.zdp)
  - Casio Disk Title (.ctw)
  - CoolPage (.cpg)
  - Corel Presentation File (.shw)
  - Crystal Reports (.rpt)
  - Diablo2 Save (.d2s)
  - Electronic Publication (.epub)
  - Etax file (.efx)
  - Family TreeMaker (.ftw)
  - FamilySearch file (.paf)
  - Final Draft (.fdr .fdt)
  - Final Fantasy 7 (.ff7)

- Fudemane (.fwa)
- Fudeou (.fzd)
- Generic Email (.mht)
- Hangul Document (.hwp)
- HotDocs (.hfd)
- Ichitaro Document (.jtd)
- InteractWeb Reports (.rpt)
- Label Mighty (.jlb)
- Lotus 123 (.wk3 .wk1 .wk2 .wk4 .wks .fm3 .wb1 .123)
- Lotus WordPro file (.lwp)
- Mapsource 2 file (.mps)
- Microsoft Excel Worksheet (.xls .xla .xlt)
- Microsoft Excel Worksheet - XLSX (.xlsx)
- Microsoft OneNote file (.one)
- Microsoft PowerPoint Presentation (.ppt)
- Microsoft Project (.mpp)
- Microsoft Publisher Document (.pub .puz)
- Microsoft Visio Drawing (.vsd .vss .vst)
- Microsoft Word Document (.doc .dot .asd)
- Microsoft Word Document - DocX (.docx)
- Microsoft Write/WordPad (.wri)
- Mime File (.mht)
- Mime File (.mht)
- MS Works 4 Document (.wps)
- MS Works Spreadsheet (.wks)
- NASCAR Racing 2003 (.sim)
- OLE Document (eg. MS Office) (.)
- Open Office Document (.odt)
- Open Office Spreadsheet (.ods)
- PDF document (.pdf .ai)
- QuattroPro 7 File (.qpw)
- Rich Text Document (.rtf)
- SureThing CD Labeler (.dsn .std)
- VI data (.vi)
- WordPerfect 6 to 10 (.wpd .wcm .wpt)
- WordPerfect Documents and Graphics v8 (.wpg)
- XML Documents (.xml .xsl .svg .xms .nib .opf .ncx)
- Archives
  - 7ZIP (.7z .7zip)
  - Cabinet compression file (.cab)
  - GZIP compression file (.gz .gzip)
  - ISO 9660 - CD-ROM File System (.iso .iso9660)
  - LZH compression file (.lzh)
  - Miliki Super Compression (.qcf)
  - MS Backup File (.bkf)
  - RAR compression file (.rar)
  - Restrospect File (.rfb .rdb)
  - TAR archive file (.tar)
  - Zip compression file (.zip .jar .afz)
- Multimedia
  - 3GPP Multimedia file (Quicktime) (.3gp .3g2 .3gpp .3gp2 .mp
  - Adaptive MultiRate Audio (.amr)
  - ASF,WMA,WMV Multimedia file (.wmv .asf .wma .asx)

- Audio Interchange file format (.aif .aiff)
- CakeWalk Pro (.cwp)
- Digital Speech File (.dss)
- Digital Voice File (.dvf)
- Finale Music file (.mus .fan)
- Flash (.fla)
- Fruity Loops file (.flp)
- Jet Voice File (.sc4)
- Kaydara FBX Binary (.fbx)
- Logic Audio (.lso)
- Ogg Vorbis/Media (.ogg .ogm .oga .ogv .ogx)
- RealAudio file (.ra .ram .rm)
- Reason (.rns)
- RIFF Multimedia file (.rif .riff .avi .cdr .npr .wav .rmid)
- Sibelius Music file (.sib .lib)
- WAVE Multimedia file (.wav)
- Email
  - Exchange Server Database (.edb)
  - Lotus Notes (.nsf)
  - Outlook Address file (.wab)
  - Outlook Email file (.pst .pab)
  - Outlook Express Email file (.dbx)
  - Outlook MSG (.msg)
  - Yahoo Messenger (.dat)
- Databases and Financials
  - Access Database (.mdb)
  - Access Project (.adp)
  - Ancestry Family Tree (.aft)
  - CanTax T1 Personal (.p00 .p96 .p97 .p98 .p99 .p01 .p02 .p
  - CanTax T2 Corporate (.c00 .c96 .c97 .c98 .c99 .c01 .c02 .c
  - DBase-FoxPro Database file (.dbf .scx .dbc)
  - EndNote (.enl)
  - FileMaker (.fp7 .fp3 .fp5 .fp8 .fp9)
  - FoxPro Executable (.fxp)
  - Interbase Backup (.gbk)
  - Interbase Database (.gdb)
  - Lacerte Tax (.mdx)
  - Lacerte Tax Individual (.id9 .id0 .sd0 .sd9 .pd0 .pd9 .fd0 .f
  - MicroSim PCBoard Log Of Forward Engineering Change Orde
  - Microsoft Money (.mny)
  - MS Works 4 Database (.wdb)
  - MS-SQL Server Database (.mdf)
  - MS-SQL Server Log (.ldf)
  - MYOB Data (.dat .prm .pls)
  - Omnis Database file (.df1 .lbr .ohf .lbs)
  - Quickbooks Backup file (.qbb)
  - Quickbooks QBW file (.qbw)
  - Quicken QDF file (.qdf)
  - QuickTax file (.q04 .q99 .q00 .q01 .q02 .q03)
  - SAS ASCII Data File (.sas)
  - SAS Binary Data file (.sas7bdat .sd2)
  - SPSS (.sav)
  - TaxAct (.ta5)

- ☐ TaxCut file (2000-3) (.t00 .t01 .t02 .t03)
- ☐ TurboTax file (.tax)
- ☐ Text (NB: Slows Search)
  - ☐ Text (Shift JIS) Documents (.jis)
  - ☐ Text (UTF-16) Documents (.txt)
  - ☐ Text (UTF-8) Documents (.txt)
  - ☐ Text Documents (.txt)
- ☐ Other
  - ☐ EXE/DLL file (.exe .sys .dll)
  - ☐ Help (.hlp)
  - ☐ TrueType Font file (.ttf)
  - ☐ Windows Link (.lnk)

Appendix 3 - References

APPENDIX 3 - REFERENCES

1. **Magic number (programming).** *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Magic_number_(programming).

2. Carrier, Brian. *File System Forensic Analysis.* s.l. : Addison Wesley Professional, 2005.

3. **Forensiks Wiki. Forensics Wiki.** *AFF.* [Online] [Cited: Mar 29, 2011.] http://www.forensicswiki.org/wiki/AFF.

4. Bunting, Steve and Wei, William. *The Official EnCE EnCase Certified Examiner Study Guide.* Indianaplois IN : Wiley Publishing, Inc., 2006.

5. United States Computer Emergency Readiness Team. US-CERT Vulnerability Note VU#836068. *US-CERT: United States Computer Emergency Readiness Team.* [Online] [Cited: March 5, 2011.] http://www.kb.cert.org/vuls/id/836068.

6. Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu. *Collision Search Attacks on SHA1.* 2005.

7. Merritt, Rick. Chinese researchers compromise SHA-1 hashing algorithm. *EE Times.* [Online] 2 16, 2005. [Cited: May 4, 2100.] http://www.eetimes.com/electronics-news/4051745/Chinese-researchers-compromise-SHA-1-hashing-algorithm.

8. Injosoft AB. ASCII Code - The extended ASCII table. *http://www.injosoft.se/.* [Online] http://www.ascii-code.com/.

9. Microsoft MSDN. *http://msdn.microsoft.com/en-us/library.* [Online] http://msdn.microsoft.com/en-us/library/cc231989%28PROT.13%29.aspx.

10. *Hidden Disk Areas: HPA and DCO.* Gupta, Mayank R., Hoeschele, Michael D. and Rogers, Marcus K. Fall 2006, Volume 5, Issue 1, International Journal of Digital Evidence.

11. *Automated mapping of large binary objects using primitive fragment type classification.* Conti, Gregory, et al. 2010, Digital Investigation, Vol. 7S, pp. S3-S12.

12. *Fileprints: Identifying file types by n-gram analysis.* W. Li, K. Wang, S. Stolfo and B. Herzog. West Point, NY : s.n., June, 2005. 6th IEEE Information Assurance Workshop.

13. Wikipedia. Regular Expression. [Online] en.wikipedia.org/wiki?Regular_expression.

14. Microsoft. Windows registry information for advanced users. *Article ID: 256986 - Revision: 12.3.* [Online] February 4, 2008. [Cited: August 19, 2011.] http://support.microsoft.com/kb/256986.

15. Wikipedia. Windows Registry. *Wikipedia - List of standard registry value types.* [Online] [Cited: December 27, 2011.] http://en.wikipedia.org/wiki/Windows_Registry.

16. *The Windows Registry as a forensic resource.* Carvey, Harlan. 3, September 2005, Pages 201-205 , Digital Investigation, Vol. 2, pp. 201-205.

17. Access Data Inc. Registry Quick Find Chart. *Access Data.* [Online] 2005. [Cited: August 19, 2011.] http://accessdata.com/media/en_us/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf.

18. *Time and date issues in forensic computing--a case study.* Boyd, Chris and Foster, Pete. 1, February 2004, Digital Investigation, Vol. 1, pp. 18-23.

19. Jones, Keith J, Bejtlich, Richard and Rose, Curtis W. *Real Digital Forensics Computer Security and Incident Response.* s.l. : Addison-Wesley, 2006.

20. Mederios, Jason. *NTFS Forensics: A Programmers View of Raw Filesystem Data Extraction.* s.l. : Grayscale Research, 2008.

21. Russon, Richard. Linux NTFS Project: NTFS Documentation. *Sourceforge.net.* [Online] 1996 - 2004. [Cited: March 16, 2011.] http://sourceforge.net/projects/linux-ntfs/files/NTFS%20Documentation/.

22. MBR is damaged - www.NTFS.com. *NTFS.com.* [Online] http://www.ntfs.com/mbr-damaged.htm.

23. Microsoft. *Microsoft Extensible Firmware Initiative FAT32 File System Specification. FAT: General Overview of On-Disk Format.* s.l. : Microsoft, 2000.

24. Stoffregen, Paul. Understanding FAT32 Filesystems. *PJRC.* [Online] Feb 24, 2005. [Cited: March 18, 2011.] http://www.pjrc.com/tech/8051/ide/fat32.html.

25. Microsoft. Detailed Explanation of FAT Boot Sector. *support.microsoft.com.* [Online] Article ID: 140418 - Last Review: December 6, 2003 - Revision: 3.0, December 6, 2003. http://support.microsoft.com/kb/140418.

26. —. Windows and GPT FAQ. *Microsoft Developers Netword (MSDN).* [Online] July 2008. http://msdn.microsoft.com/en-us/windows/hardware/gg463525.aspx.

27. —. Basic Storage Versus Dynamic Storage in Windows XP. *Microsoft Support.* [Online] December 1, 2007. [Cited: March 23, 2011.] http://support.microsoft.com/kb/314343.

28. National Institute of Standards and Technology. CFTT Project Overview. *Compuer Forensics Tool Testing Program.* [Online] [Cited: March 28, 2011.] http://www.cftt.nist.gov/disk_imaging.htm.

29. Wikipedia - Host Protected Area. *http://en.wikipedia.org/wiki/Host_protected_area.* [Online] [Cited: Mar 29, 3011.] http://en.wikipedia.org/wiki/Host_protected_area.

30. Apple Computer, Inc. Technical Note TN2166 - Secrets of the GPT. *developer.apple.com.* [Online] 11 6, 2006. [Cited: April 5, 2011.] http://developer.apple.com/library/mac/#technotes/tn2166/_index.html .

31. Apple Inc. *Inside Macintosh: Files.* Reading, Massachusetts : Addison-Wesley, August 1992.

32. Apple, Inc. HFS Plus Volume Format - Technical Note TN1150. *developer.apple.com.* [Online] March 5, 2004. [Cited: April 6, 2011.] http://developer.apple.com/library/mac/#technotes/tn/tn1150.html.

33. Wikipedia: Extent (file systems). Extent (file systems). *Wikipedia: Extent (file systems).* [Online] [Cited: 4 6, 2011.] http://en.wikipedia.org/wiki/Extent_(file_systems).

34. Aomei Technology, Co., Ltd. What is a Dynamic Disk? *Dynamic Disk.* [Online] 2009. [Cited: April 13, 2011.] http://www.dynamic-disk.com/what-is-dynamic-disk.html.

35. Lewis, Don L. The Hash Algorithm Dilemma–Hash Value Collisions. *Forensic Magazine.* [Online] 2009. [Cited: May 2011, 4.] http://www.forensicmag.com/article/hash-algorithm-dilemma%E2%80%93hash-value-collisions?page=0,0.

36. *An Empirical Analysis of Disk Sector Hashes for Data Carving.* Yoginder Singh Dandass, Nathan Joseph Necaise, Sherry Reede Thomas. 2008, Journal of Digital Forenic Practice, Vol. 2, pp. 95-104.

37. Inc., Guidance Software. *EnCase Forensic Version 6.10 User Manual.* s.l. : Guidance Software, 2008.

Appendix 4 - Definitions

APPENDIX 4 - DEFINITIONS

Alternate Data Stream (ADS)	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. Recover My Files shows ADSs with a blue file icon with an "A" character.
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) (8).
Cluster	A cluster is the smallest logical unit of drive 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.
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.
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"

and it is returned and displayed in Recover My Files as a "carved". 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.
Drive Slack	The area between the end of a partition and the end of the drive. It is usually considered to be blank, but can hold remnants of previous drive configurations or could be used to purposely hide data.
Drive view	A graphical representation in Recover My Files of sectors on the examined device. Drive view can be used to: • Examine the content of the data in a specific sector/s; • Quickly navigate to a desired sector position on the device; • Obtain a graphical overview of the file types which make up the drive and where they are position on the examined media; • Identify the location and fragmentation of individual files.
DST	Daylight Savings Time
E01	A forensic file format used to create drive image files. Developed by Guidance Software (http://www.guidancesoftware.com/)
Explorer View	File display technology written by GetData and used in the Recover My Files Display view to show the contents of more than 300 different file types.
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 carve	File carving (also known as file carving or carving) is the process of searching for files based on a known content, rather than relying of file-system

metadata. This usually involves searching for a known header and footer of a specific file type.

Recover My Files has built in code to data carve for more than 300 file types.

File Signature	The header component of a file which has unique identifiers that assigns it to a type, e.g. a jpeg. Most common file types have a signature set by the International Organization for Standardization (ISO). Identifying a file by its signature is a more accurate method of assessment that using the file extension, which can easily be altered.
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.
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).
Flag	In Recover My Files a flag is used to mark a file as relevant. It is a colored box (flag) that is applied to a List view when the "Flag" column is displayed. Eight colored flags are available for use. Flags are applied by highlighting and artifact and double clicking the opaque flag color in the flag column, or by using the right click "Add Flag" menu.
Folder	See Root Directory
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 drive so that it's written in non-contiguous clusters.
Free Space	Free space is often used to describe unallocated clusters, the available drive storage space that is not allocated to file storage by a volume. Free space can however also refer to the unused area of a drive not taken up by
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 algorithm in use is 128-bit MD5. |

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.
INFO2	Windows automatically keeps an index of what files were deleted including the date and time of the deletion. The index is held in a hidden file in the Recycle Bin called INFO2.
	When the Recycle Bin is emptied, the INFO2 file is deleted. Recovery and analysis of deleted INFO2 files can provide important information about files that were once located on the computer.
LFN (also see SFN)	Long File Name refers to file or folder on a FAT file-system which has a name greater than 8 characters and 3 for the file extension (or one which contains special characters). The storage of the additional file name information makes it necessary for Windows to create an additional LFN directory entry (or entries) to hold the extra information.
Link Files (LNK)	Link files (.lnk) are Microsoft Windows shortcut files. Link files have their own metadata and can provide valuable information about files stored on the computer.
Logical Evidence File	Logical Evidence Files (or Logical images Files) are images of selected files, rather than the traditional image of a volume or physical drive. 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.
Logical Sector (LS)	
Lost (file)	Files located by "file carving" with Recover My Files are displayed as "Lost_[fileytpe].xxx.

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".* (9))
Metadata	Metadata is often referred to as "data about data". Windows metadata includes a files create, last accessed and modified dates, as shown in *File* List view of Recover My Files. File metadata includes information such as camera make and model in a JPEG, or author name in Microsoft Word.
Mount Image Pro (MIP)	A computer forensics software tool written and sold by GetData (www.mountimage.com) which enable the mounting of forensic image files as a drive letter on a Windows computer system.
MRU	Most Recently Used (MRU) is a term used to describe a list of the most recently opened files by an application. Many Windows applications store MRU lists as a way of allowing fast and consistent access to most recently used files. Most MRU lists are stored in the Windows registry.
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.
Pane	An area of the Recover My Files module. The Recover My Files module is broken down into three panes, Folder Tree, *File* List view and File Display. A pane can contain multiple different windows, such a Hex view, Text view, Drive view, *Console* etc.
Partition	A part of a hard drive that can have an independent file-system.
Physical sector (PS)	
RAID	Redundant Array of Independent Drives.
RAM	Random Access Memory, where programs are loaded and computer code is executed. The content of RAM is lost when the computer is turned off.
RAM Slack	RAM slack is the data between the end of the logical file and the rest of that sector. For example, a sector is written as a block of 512 bytes, so if the last

sector contains only 100 bytes, the remaining 412 bytes is padded with RAM slack. In older Operating Systems, e.g. Windows 95, RAM slack could contain data from RAM unrelated to the content of the file. In more recent Operating Systems, RAM slack is filled with zeros.

Recover My Files	Data Recovery Software authored and sold by GetData at www.recovermyfiles.com
Registry	The Windows Registry is a hierarchical database that stores configuration settings and options for the Microsoft Windows operating systems. For the computer forensics examiner it can be a wealth of information on all aspects of the computer and its use, including hardware, applications, and user configuration.
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 root of a tree, from which the trunk and branches arise). The root folder is the same as click on the drive letter in Windows Explorer, e.g. being located in folder "C:\". 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 drive. A sector on a hard drive 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).
SFN (see also LFN)	Short File Name refers to a file or a folder on a FAT file-system that has a file name that can be stored in the 8.3 file name format (8 name characters with 3 characters for the extension). The name and metadata for a SFN file can be stored within a standard FAT directory entry.
Slack	See File Slack, Drive Slack, FAT Slack
Steganography	Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity (Definition from: http://en.wikipedia.org/wiki/Steganography)
Unallocated Clusters	Unallocated clusters (also referred to as unallocated space or free space) are the available drive 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.

Appendix 5 - Icon Key

Recover My Files icons sorted by Category:

Icon	Category	Description
	Date	File date
	Device	A physical device, e.g. a hard drive
	Device	A logical device, e.g. C: drive.
	File	A deleted file
	File	A FAT "dot" directory entry
	File	A FAT "double dot" directory entry
	File	A system file
	File	An active file
	Folder	A deleted folder
	Deleted items	Categorize deleted items - File-system > Folder Tree > Category view
	Folder	An active folder
	Free space	Free space in partition (Space inside a partition which is not in use)
	Free space	Free space on drive (Space on the physical drive which is not in use)
	Image	A forensic image file
	Image folder	Select an image from a folder
	Image library	Add or select an image from the library
	Navigation	An expandable branch (folder structure)
	Navigation	Active branch plate
	Navigation	Inactive branch plate
	Partition	A partition
	Partition	An active partition
	Unallocated	Unallocated clusters on FATxx volume
	Unallocated	Unallocated clusters on NTFS volume

Appendix 6 - Index

APPENDIX 7 - INDEX