

## ***Overview of a Drive's Architecture***

In simple terms all drives (FAT, NTFS, CDFS etc) are divided into three primary sections: Drive Information, File Information, and Data.

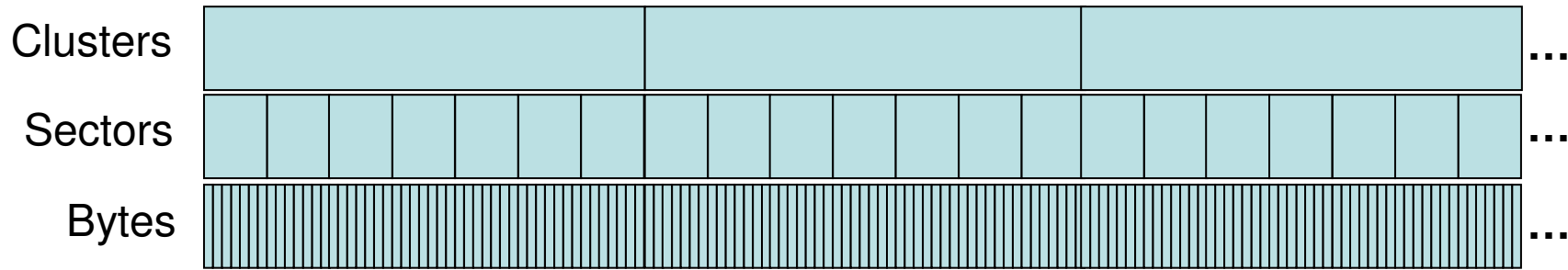


The **Drive Information** section provides information on how the drive is organised. This includes such information as: its name, sector size, cluster size, location of the other areas.

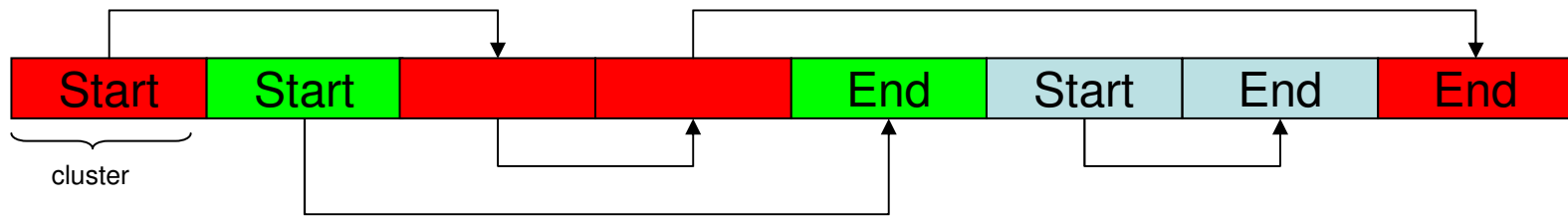
The **File Information** section provides information on the files and directories that exist on the drive and includes information such as: its name, size, clusters used.

The **Data** section contains the raw pieces of data that each file consists of.

The drive is split into sections called clusters. A cluster contains a fixed number of sectors (defined in the Drive Information), and a sector contains a fixed number of bytes.

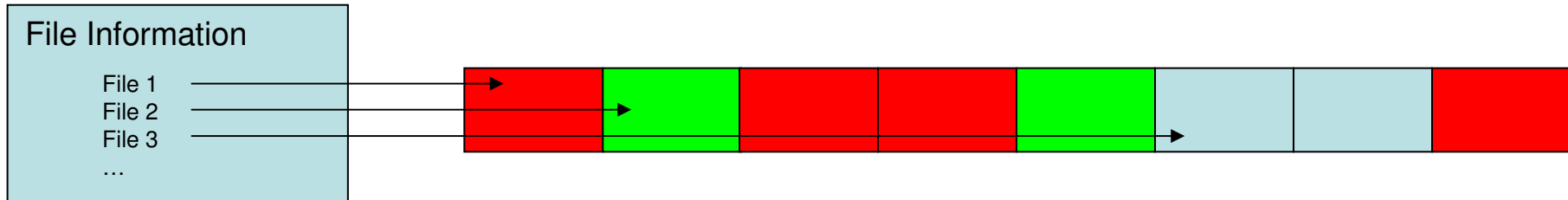


In simple terms, files consist of one or more clusters of data. It helps to think of a file as a *chain* of clusters. Sometimes the clusters are contiguous (together in one block) and sometimes they are fragmented (spread over several blocks)

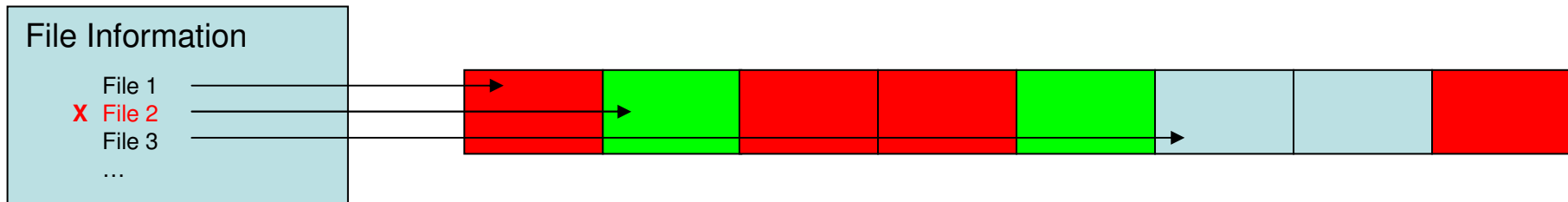


Key	<b>File 1</b>	Fragmented
	<b>File 2</b>	Fragmented
	<b>File 3</b>	Contiguous

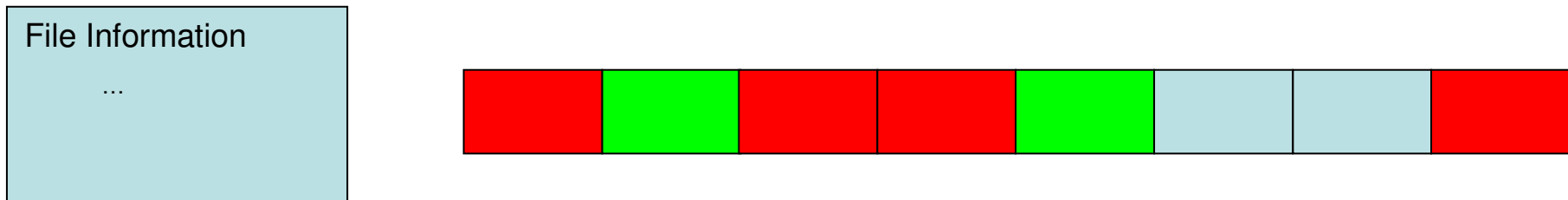
Information about a file's cluster chain is held in the File Information area of the drive.



When a file is deleted, the file's data is left untouched and the file's entry in the File Information area is left intact with the data clusters being marked as re-usable.



When a drive is formatted the Drive and File Information areas are erased and rewritten. All references to the data are removed. However, the Data itself may be left untouched.



## ***What's the difference between an Undelete Scan and a Low-Level Scan?***

### **Undelete Scan**

#### **Overview**

This scan reads the drive's Drive and File Information areas and uses the information found to identify deleted files and to determine their cluster-chains.

By using the Drive's File Information area, it is:

- Able to obtain a file's name and also the directory structure in which the file was originally found.
- Able to return only those files marked as deleted by being able to tell the difference between deleted and non-deleted files.
- Fast, because it only accesses the parts of the drive it requires.

#### **When should you use it?**

It is best to use the Undelete Scan:

- When you have accidentally deleted a file
- As your first attempt to recover a files
- When you need the filename and/or directory

# Low Level Scan

## Overview

This scan relies on the fact that files begin with a consistent sequence of bytes to identify the file type, called a File Header. i.e. All files of type .drs begin with the byte sequence: 'DRS-FILE'.

This scan ignores the drive's File Information area and reads the complete drive as a continuous sequence of bytes. Whilst reading the drive, it looks for the pre-defined File Headers that indicate the beginning of a known file type.

As the scan doesn't reference the File Information area, it has no reference as to the what the data on the drive "means". This has some consequences:

- It cannot determine filenames or directories. Because of this it simply names the files: File1, File2, File3...
- A file's data cannot be fragmented – it can only recover files whose data occurs in a single block.
- It is also slower than the Undelete Scan because it has to scan the entire drive from beginning to end.

## **When should I use it ?**

It may seem that the Low Level Scan isn't very useful when compared to the Undelete Scan so why would you use it?

The main circumstances when you would use the Low Level scan are:

- The drive has been formatted. (Formatting will erase the File Information but not necessarily the Data).
- The drive has become corrupt.
- The Undelete Scan didn't find the file(s) you were looking for. (The File Information may be corrupt but the Data still ok.)

### **Tip**

Because the Low Level scan can only look for particular file headers, you will get the best results by specifying exactly which file types you are looking for.

Don't be tempted to select all of the file types as it makes the scan much slower.

## Summary

### Undelete

Advantages	Disadvantages
<ul style="list-style-type: none"><li>• Can identify filenames and directories.</li><li>• Can find fragmented files.</li><li>• Fast – it only accesses the drive data for the files it finds.</li><li>• Doesn't need to know about file types.</li></ul>	<ul style="list-style-type: none"><li>• If the File Information is missing or badly damaged (i.e. the drive becomes corrupt or formatted) then it will not find anything.</li></ul>

### Low Level

Advantages	Disadvantages
<ul style="list-style-type: none"><li>• Can find files even if the drive's File Information has become corrupted.</li><li>• Can often find files even if the drive has been formatted.</li></ul>	<ul style="list-style-type: none"><li>• Cannot determine filenames or directories.</li><li>• Cannot recover fragmented files.</li><li>• Slow – it has to read the whole drive.</li><li>• It must know the File Headers in advance.</li></ul>

## **What does the “Show Images” checkbox do?**

There is an option with the Undelete Scan to “Show Images”. If checked, this will show you a thumbnail of jpg, wmf, emf, and bmp images.

However, as the Undelete Scan returns filenames and directories you may not need to see them.

Unchecking the “Show Images” checkbox makes the scan much faster and uses much less of your computer’s memory.

When an image (jpg, bmp, emf and wmf) is displayed as a thumbnail in Media Investigator, it automatically checks whether or not the file is OK. If Media Investigator finds a problem with a file then that file is removed from the recovery list.

When “Show Images” is unchecked this check does not occur.

This can result in a different number of files being returned when scanning the same drive with “Show Images” checked and unchecked.