Active@ UNERASER

User Guide

LSOFT TECHNOLOGIES INC. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of LSOFT TECHNOLOGIES INC. to provide notification of such revision or change.

LSOFT TECHNOLOGIES INC. provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. LSOFT may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

All technical data and computer software is commercial in nature and developed solely at private expense. As the User, or Installer/Administrator of this software, you agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Contents

1. Overview

What Happened to my Data?

When data (file, partition, volume, etc...) is deleted from a hard drive, two systems are notified:

1. The system record in the File Table or Partition Table is removed (or marked as deleted)
2. Space where partition or file was located is labeled as 'unoccupied'. The data itself is not removed

In the event of an accidental deletion we strongly recommend that you perform the recovery operation as soon as possible. If any new partition or file is created instead on the same space and some information is written there, there is a chance that the writing process may allocate some data in this 'unoccupied space' thus damaging you data located on the disk and deleted previously.

Welcome to Active@ UNERASER

Active@ UNERASER is a powerful software utility, designed to restore accidentally deleted files, folders and partitions (volumes).

Active@ UNERASER can be installed on and run from USB Flash disk or bootable CD/DVD, so that the risk of overwriting your data is minimized.

Active@ UNERASER will help you to restore files, folders and partitions residing on hard drives formatted in any of the following file systems:

- Microsoft NTFS / NTFS5 / NTFS+EFS
- Microsoft FAT12 / FAT16 / FAT32 / exFAT
- Apple HFS+
- Linux Ext2 / Ext3 / Ext4
- FreeBSD Unix UFS

It works under all Windows family operating systems:

- Windows XP
- Windows Vista
- Windows Server 2003, 2008, 2008 RC2, 2012
- Windows 7
- Windows 8
- Windows PE (embedded Windows recovery environment loaded from CD-ROM or USB disk)

Active@ UNERASER supports:

- IDE, SATA, SSD, SCSI hard drives, External USBs, Floppy and USB Flash Media, Memory Cards
- Large-sized drives (more than 2TB)
- Detection and recovery of deleted and damaged partitions
- Unerase data on a file-by-file basis, and all volume data at once
- Saving scan results to the storage and re-opening them later on
- Correcting BOOT.INI if needed to keep the system bootable
- Fixing damaged MBR/GPT and deleting invalid partitions
- Automatic and Manual correction of Volume Boot Sectors
- Creating and working with Disk Images for data recovery purposes
- Integration with a Disk Viewer/Editor - to be able to inspect raw disk/partition/file data

New in version 6.0

- Support for recovery from FreeBSD UNIX UFS and Linux Ext4fs file systems

- Added an integrated Disk Editor (HEX Viewer) component being able to inspect disks and files on a low level (raw sectors)
- "In Place" and "Copy to Another Disk" partition recovery methods
- Convenient 'Go Back', 'Go Forward' and 'Go Up' navigation buttons and key combinations added
- Improvements in recovery kernel: faster scans, more files and partitions can be detected
- and more...

The free version can scan drives, detect deleted partitions and inspect files and folders there and unerase the only one file per session. To recover more files per recovery session you need to purchase a registration key and activate the software.

2. Using QuickScan to detect just deleted files and partitions

QuickScan searches for files, folders and partitions being just deleted. If you are looking for deleted files and folders, you must scan the existing drive (logical disk or volume) to detect files and folders being deleted. If you are looking for deleted partitions and volumes, you must scan unallocated space to detect the drive being deleted.

There are two methods for scanning: QuickScan and SuperScan.

QuickScan is a fast and basic scan. Partitions and files that have just been deleted most likely will be detected using this method (if no other partition has been created in unallocated space).

SuperScan is a much slower and thorough scan. It processes the whole hard drive surface detecting all possible deleted data. After running QuickScan, if you haven't found proper partition or files, try SuperScan. For more information on SuperScan, click the link at the bottom of this topic.

To run QuickScan:

- Open Active@ UNERASER and in the Local System Devices list under the particular Hard Disk Drive or USB Disk, select the Volume (Logical Disk) to be scanned for deleted files, or Unallocated Space to be scanned for deleted partitions
- Click QuickScan toolbar button
- You can also right-click the Unallocated Space or Volume and select QuickScan from the context menu, or click QuickScan from Action menu

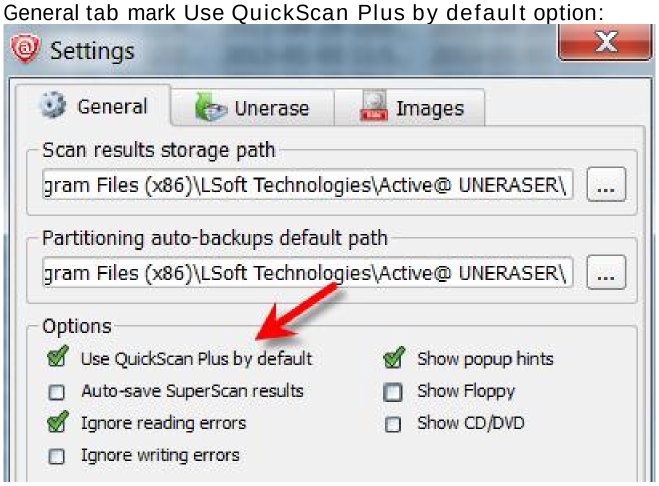
Disk scanning starts. To stop the scanning process for any reason, click Cancel button. After QuickScan is completed, you can inspect detected files and volumes, and recover your data.

QuickScan Plus

QuickScan Plus is an advanced version of QuickScan. It processes more unallocated space where deleted data assumed to be located, so it is a bit slower than QuickScan, however it detects more deleted files and folders. QuickScan Plus is still faster comparing to SuperScan (which processed all available disk space: unallocated and currently allocated).

After the regular QuickScan for the particular volume completed, toolbar button label and related menu items change to QuickScan Plus. This means that if you scan the same object one more time, some advanced features of QuickScan will be activated. It will take a bit more time, however it could detect more deleted files and folders. Advanced features include looking for files beyond the "live" system areas (current MFT area on NTFS, or directories tree on FAT). Moreover, for transactional file systems, like NTFS, Log File ($LogFile) and User Journal ($UsnJrnl$) are processed to get more information about recent transactions (deleting, renaming,...). This could be very useful when you quick-formatted your hard drive or USB flash disk.

To change default action for QuickScan button and menu item to use QuickScan Plus always, open Settings, and on the General tab mark Use QuickScan Plus by default option:



Settings

Scan results storage path

gram Files (x86)\LSoft Technologies\Active@ UNERASER\

Partitioning auto-backups default path

gram Files (x86)\LSoft Technologies\Active@ UNERASER\

Options

☑ Use QuickScan Plus by default

☐ Auto-save SuperScan results

☑ Ignore reading errors

☐ Ignore writing errors

☑ Show popup hints

☐ Show Floppy

☐ Show CD/DVD

Analyzing detected by QuickScan objects

You can tell the state of your files by the color of the icons:

Blue icon shows an existing file

Grey icon shows a deleted file

You can tell the state of your folders by the color of the icons:

Yellow icon shows an existing folder

Grey icon shows a deleted folder

You can tell the state of your partitions by the color of the icons:

Grey or Green icon shows an existing partition

Grey icon with Green box shows a deleted partition has a good integrity status and that can be safely recovered

Grey icon with Brown or Red box shows a deleted partition that can be recovered, however this partition might has been formatted before deletion or has some other damage

After you complete the drive scan, to locate your deleted partitions, just look under Unallocated Space nodes. If new partitions appear there - inspect them (click on icon) and verify their content browsing the files and folders.

You can inspect the content of the file by selecting the file and clicking Preview toolbar button, or executing Preview command from the context menu, or by pressing Alt+P key combination.

If you are looking for deleted files and folders, to locate them, you may search either manually, by opening folders in the tree, or automatically, using the search mode.

If you satisfied with results, select an object (file, folder or partition) proceed with a recovery (click Unerase toolbar button).

3. Use SuperScan to analyze deleted and severely damaged volumes

Use SuperScan when trying to recover a partition or volume that you know has been deleted or damaged. In other words, if you do not see a logical drive listed under a device node in the Local System Devices list, it is time to use SuperScan.

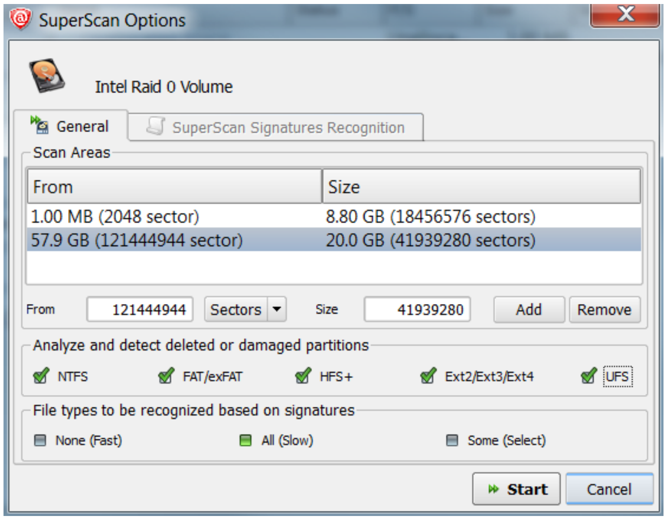
Another reason to use SuperScan is when the volume has been quick-formatted, or disk's surface has been heavily overwritten by other data, so you are not able to find your deleted data using QuickScan and Search procedures. SuperScan gives a chance to detect damaged file records as well as to reconstruct some known file types by signatures.

SuperScan processes the whole surface of the physical device searching for all possible logical drives (volumes) and partitions, whether they are existing, damaged or deleted. If a partition cannot be found, SuperScan keeps searching. SuperScan reads each disk sector and looks for not only the boot sector, but also tries to reconstruct the drive structure, based on residual clues to the drive's system structures that remain on the disk surface. This is a slow process, however it usually gives much better results than QuickScan.

When SuperScan finds file data and the deleted or damaged file is not fragmented, the SuperScan can detect files by matching template patterns to the found data. These files collected to Signature Files folder and can be recovered from there. Usually such files do not have name, date stamp and other file record information.

To run SuperScan:

1. In the Local System Devices list, select a physical device, or a volume that contains your data. It may be a Fixed Disk, USB external or Removable Disk, Memory Card, and even Floppy and CD/DVD-ROM
2. To open the SuperScan Options dialog, do one of the following:
   - Click SuperScan toolbar button:
   - Right-click the disk and choose SuperScan... from the context menu
   - Press Ctrl+Enter key combination



Intel Raid 0 Volume

Scan Areas

From	Size
1.00 MB (2048 sector)	8.80 GB (18456576 sectors)
57.9 GB (121444944 sector)	20.0 GB (41939280 sectors)

From 121444944 Sectors Size 41939280

Analyze and detect deleted or damaged partitions

☑ NTFS ☑ FAT/exFAT ☑ HFS+ ☑ Ext2/Ext3/Ext4 ☑ UFS

File types to be recognized based on signatures

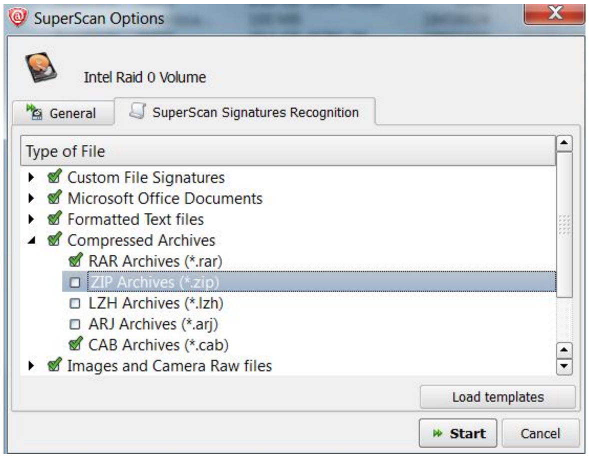
○ None (Fast) ● All (Slow) ○ Some (Select)

3. Fields From and Size contain currently selected object's geometry in sectors. You can switch geometry display to other units (Bytes, MB and GB) using drop down combo box. If you now click Start button - this area will be scanned by default

4. To select disk's area manually, type the starting sector number in the From field and the number of sectors in the Size field. If you need several areas to be scanned, define area parameters and click Add button, then type other area parameters and click Add again

5. In the Analyze and detect deleted or damaged partitions area, select the check boxes next to the partition types that you want to look for. Clear the check boxes next to the partitions that you do not want to look for. If you select all partition types, the scanning takes a longer time, however you may find more recoverable partitions

6. If a disk has been severely damaged and partitions and files are not found, you may turn on the File types to be recognized based on signatures option. Provided that the files are not fragmented, Active@ Scan technology would detect the file signatures and would try to reconstruct files of certain types. The detected files, when this option is turned on, will be placed into the Signature Files virtual folder and will have abstract filenames (because no file header could be detected, only file data), however their content can be valid. You may try to recover your documents or images from the Signature Files virtual folder later on. The None option means that no signatures recognition will be applied, it will speed up the SuperScan process, and less memory (RAM) will be consumed. The All option instructs SuperScan to recognize all possible supported signatures. The Some option lets you choose the file types you want to recognize based on signatures (including user-defined signatures being loaded from template file) and recover them later on:



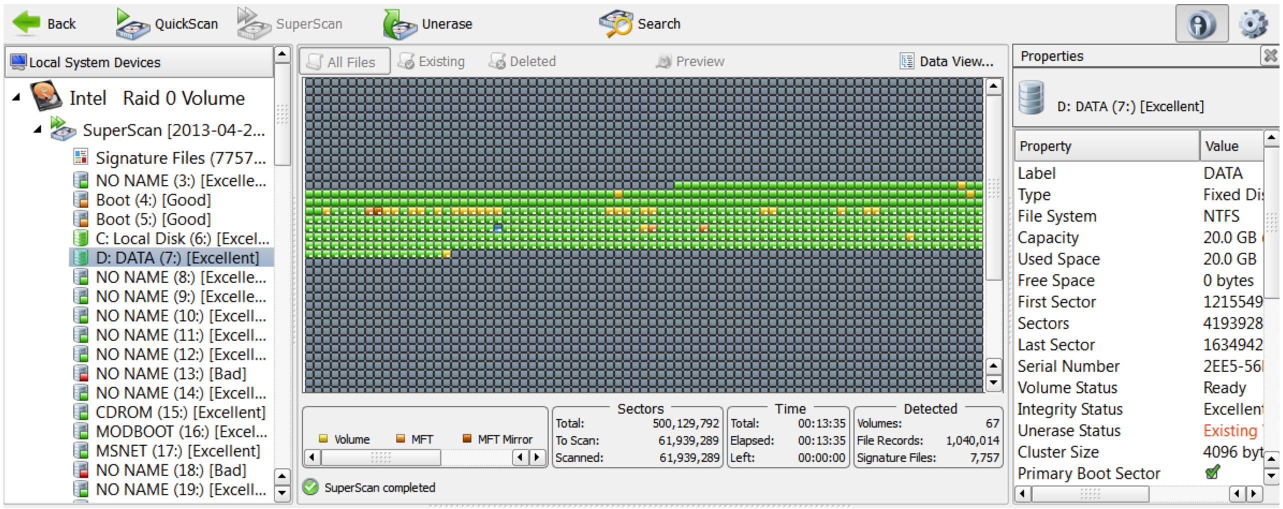
☑ Custom File Signatures
☑ Microsoft Office Documents
☑ Formatted Text files
☑ Compressed Archives
- ☑ RAR Archives (*.rar)
- □ ZIP Archives (*.zip)
- □ LZH Archives (*.lzh)
- □ ARJ Archives (*.arj)
- ☑ CAB Archives (*.cab)

☑ Images and Camera Raw files

7. Click Start button or press Enter to start SuperScan process

8. The statistics and progress bar appear underneath the scanning area. To stop the SuperScan at any time, click Pause red button at bottom, or choose Pause SuperScan from the context menu. If SuperScan has been paused, you may resume it by clicking Resume button at bottom or by choosing Resume SuperScan from the context menu. If you have saved paused SuperScan results, its state being saved as well, so you can resume SuperScan later on, after loading SuperScan results - even after re-boot, or on another machine having the same HDD/USB disk attached

9. For each SuperScan process a new virtual folder named SuperScan [YYYY-MM-DD HH:MM:SS] has been added under particular disk being scanned. The contents of this folder displayed in the tree view as well as in the Data View (right panel). You may treat SuperScan virtual folder and its contents the same way that you treat other device nodes in the list. You may follow the same steps to scan found volumes, then search for files and folders to be recovered.



Sectors		Time		Detected	
Total:	500,129,792	Total:	00:13:35	Volumes:	67
To Scan:	61,939,289	Elapsed:	00:13:35	File Records:	1,040,014
Scanned:	61,939,289	Left:	00:00:00	Signature Files:	7,757

SuperScan completed

Property	Value
Label	DATA
Type	Fixed Di
File System	NTFS
Capacity	20.0 GB
Used Space	20.0 GB
Free Space	0 bytes
First Sector	1215549
Sectors	4193928
Last Sector	1634942
Serial Number	2EE5-56
Volume Status	Ready
Integrity Status	Excellent
Unerase Status	Existing
Cluster Size	4096 byt
Primary Boot Sector	✓

Inspecting SuperScan results

SuperScan can be a long process. You can check the estimated run time displayed on the status panel at bottom of the Scanning Area. You can wait until SuperScan finishes, or you can inspect and manage found partitions (volumes) "on-the-fly":

- Click the volume in the tree (left panel) to highlight the volume position in the Scanning Area (right panel)
- Right-click the volume and choose Properties from the context menu - to check volume integrity and attributes being detected
- Double-click the volume, or choose QuickScan from the context menu - to scan the volume, browse its folders, view files and so on
- You can preview and recover your files from the found volume while SuperScan is still in progress
- After you have inspected the volume, if results are not satisfactory, you can hide the volume, by choosing Remove from the context menu
- To unhide all volumes being removed previously from the list, choose Show All Volumes from SuperScan node context menu

Note

After you run a SuperScan, you may notice a tab named Signature Files. This virtual folder contains file data that was detected based on templates of commonly used file types (*.JPG, *.DOC, etc...). Files in this folder have been renamed because no file header was detected. If the file data is un-fragmented, there is a good chance that SuperScan recovers the data in these files. If you haven't found your files during volumes inspection, try to recover similar file types from Signature Files folder. There could be a chance you find your data even if file record containing file name has been overwritten.

Important

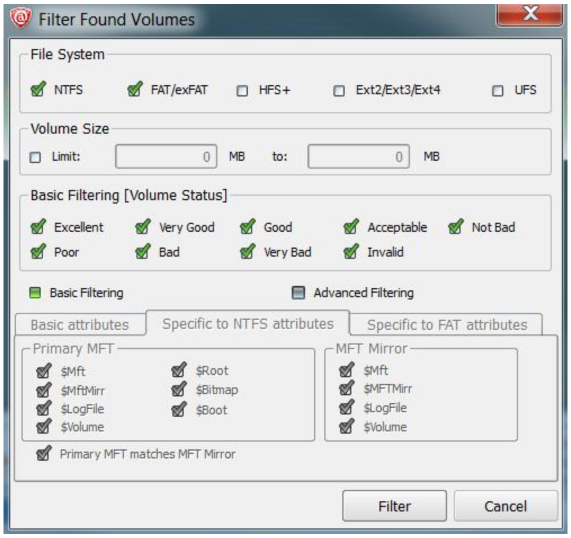
After you complete a SuperScan, you may find hundreds of partitions. Volumes having different locations and sizes, may have been created and then deleted at different times on the device being scanned. If you have virtual VMware workstation profiles (from VMware, Inc.) or VirtualPC profiles (from Microsoft Corp.), these files also contain partition information. Moreover, if remains of damaged disk structures not enough to define all necessary partition parameters, SuperScan uses complex algorithms to project the most probable parameters and instead of one partition could create 10-20 partitions having different sizes, offsets, cluster size and so on. This does not mean that SuperScan creates a lot of garbage. This means that among these projected partitions most likely will be the one you've lost, and most likely you'll be able to find and recover your data. So, if you cannot find your data on the volumes having Excellent or Good recovery status, it is still recommended that you wait until SuperScan finishes and then inspect all found volumes once again.

Filtering SuperScan results

To reduce the amount of work, you may use a filter so that you are working with a smaller set of data. After the SuperScan, all detected volumes are displayed. When you change the settings in the filter dialog box, you can display only selected types of volumes.

To filter SuperScan results:

1. After running SuperScan, select the virtual folder with the name SuperScan [date time stamp]
2. Right-click the node. From the context menu choose Filter... The Filter Found Volumes dialog box appears



Filter Found Volumes

File System

☑ NTFS ☑ FAT/exFAT □ HFS+ □ Ext2/Ext3/Ext4 □ UFS

Volume Size

□ Limit: 0 MB to: 0 MB

Basic Filtering [Volume Status]

☑ Excellent ☑ Very Good ☑ Good ☑ Acceptable ☑ Not Bad

☑ Poor ☑ Bad ☑ Very Bad ☑ Invalid

■ Basic Filtering □ Advanced Filtering

Basic attributes | Specific to NTFS attributes | Specific to FAT attributes

Primary MFT

☑ $Mft ☑ $Root

☑ $MftMirr ☑ $Bitmap

☑ $LogFile ☑ $Boot

☑ $Volume

MFT Mirror

☑ $Mft

☑ $MFTMirr

☑ $LogFile

☑ $Volume

☑ Primary MFT matches MFT Mirror

3. To select the types of file systems to display, in the File Systems area, clear the check box beside the types that you do not want to display. Only the selected types of file systems data will be displayed
4. To display only those partitions within a specified size limit, in the Volume Size area, indicate the minimum and maximum sized partitions in MegaBytes. Only those partitions within the specified range will be displayed
5. To use basic filtering parameters, click Basic Filtering. To select displayed partitions based on partition status, in the Basic Filtering [Volume Status] area, clear the check box next to each partition status number that you do not want to display. Only the selected status ratings will be displayed
6. To use advanced filtering parameters, click Advanced Filtering and use the bottom section:
    - To restrict displayed results for found boot sector's attributes (file system-independent), in the Basic Attributes area, select the check box beside all the types of data that you want to display
    - To restrict displayed results for NTFS-specific parameters, in the Specific to NTFS attributes area, select the check box beside all the types of data that you want to display
    - To restrict displayed results for FAT-specific parameters, in the Specific to FAT attributes area, select the check box beside all the types of data that you want to display
7. Click Filter to set up a filter for all volumes found by SuperScan

To remove a Filter and show all found volumes, execute Remove Filtering context menu command on the particular SuperScan node.

Searching SuperScan results to find files and folders

If, as a result of your SuperScan you find a large number of partitions, you may want to use a Search to help you locate specific files or folders. You may apply Search for the particular volume, or for all volumes found. There are options in the search dialog box that allow you to make the search go faster. For example, you may want to restrict the search so that only deleted files and folders appear in the results, or restrict files by size. By choosing strict conditions, you may be able to locate a specific file or folder faster.

Storing and loading SuperScan results

Depending on the size of the drive that you are scanning, it can take a long time to scan partitions. On large or damaged drives, it can take hours. If you have to exit Active@ UNERASER for any reason, it would take a long time to scan the partition again. So that you don't lose the information that you have scanned, you may save the SuperScan results to a file. When you open Active@ UNERASER, opening the saved results file takes much less time.

If you decide to stop the SuperScan process, it is easy to continue scanning from the point that you stopped. After SuperScan has stopped, you may save the SuperScan virtual folder results, exit and re-start the application, open SuperScan results and resume SuperScan from the last point. To continue scanning, select the SuperScan virtual folder and click Resume button on the right of the progress bar.

To save SuperScan results

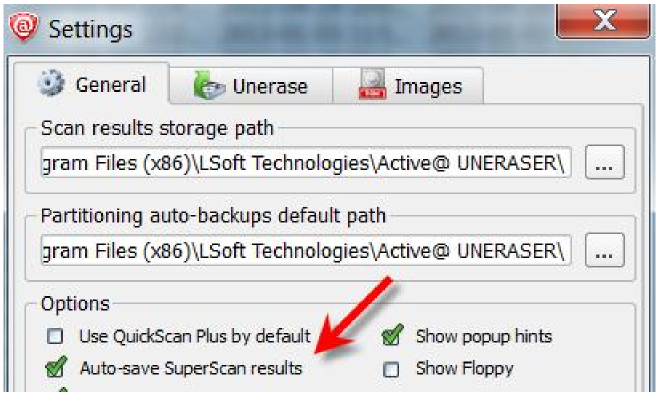
1. In the Local System Devices list, select the SuperScan virtual folder and do one of the following:
    - Right-click the device node. From the context menu click Save Scan Results...
    - From the File menu, choose Save Scan Results...
2. In the Save Scan Results dialog box, type a path or browse to a folder where the scan results file is to be stored
3. Click Save

To open SuperScan results

1. From the File menu click Open Scan Results...
2. In the Open Scan Results dialog box, browse to the file where you saved the scan results file
3. Click Open
4. In the Matched Devices dialog box confirm the device name (HDD/USB name) to apply SuperScan results for.

Note
Several devices might have the same name, for example, similar disks usually used in RAID arrays. In this case the order they appear in Matched Devices dialog matches the order devices appear in Local System Devices list. You may inspect your disks in Local System Devices list to know for sure which device to choose.

Important
SuperScan results can be saved automatically. You can configure this option and storage path in General tab of product Settings.



Scan results storage path: gram Files (x86)\LSoft Technologies\Active@ UNERASER\

Partitioning auto-backups default path: gram Files (x86)\LSoft Technologies\Active@ UNERASER\

Options
☐ Use QuickScan Plus by default
☑ Show popup hints
☑ Auto-save SuperScan results
☐ Show Floppy

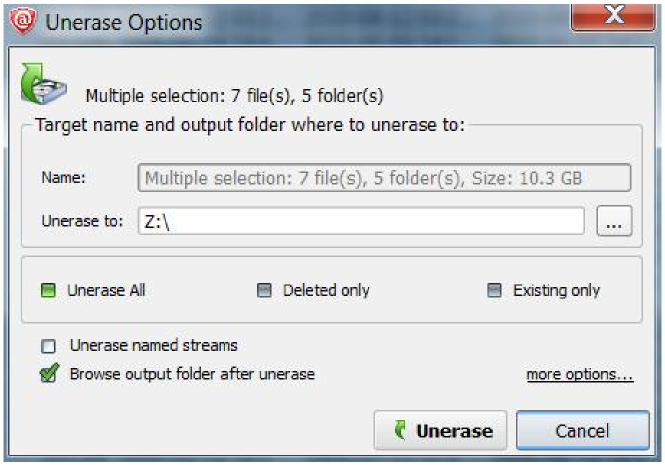
4. Unerase Deleted Files and Folders

You can distinguish deleted files and folders from existing ones by the icons:

- Blue and yellow icons show existing files and folders
- Grey icons show deleted files and folders

To restore a deleted file or folder:

1. In Active@ UNERASER, search for deleted files or search for file signatures and select the file or folder (or group of files and folders) to be recovered
2. Launch Unerase Options dialog using one of the following methods:
   - Click Unerase button on the toolbar:
   - Right-click the file or folder, and then choose Recover from the context menu
   - Press Ctrl+R key combination



Multiple selection: 7 file(s), 5 folder(s)

Target name and output folder where to unerase to:

Name: Multiple selection: 7 file(s), 5 folder(s), Size: 10.3 GB

Unerase to: Z:\

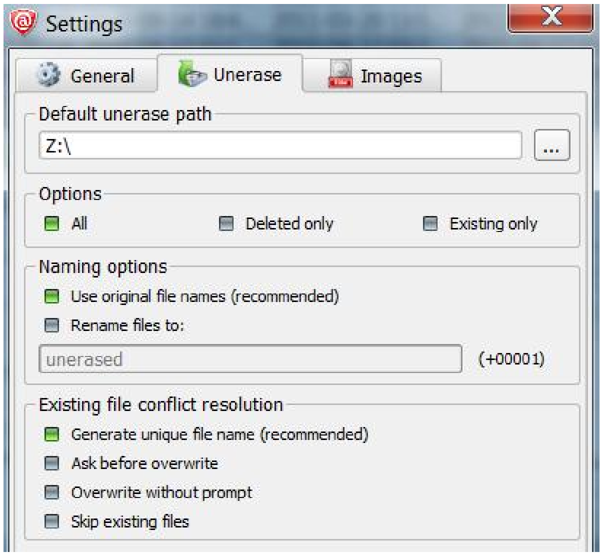
● Unerase All ○ Deleted only ○ Existing only

□ Unerase named streams

☑ Browse output folder after unerase

3. To give a name, you may use the name that appears in the Name field or you may type a different name. This option is only available if selected the only one file or folder
4. To recover the to a specified location, in the Unerase to field, you may type a different path or click the ellipsis button (...) and browse to a recovery folder location
5. If you selected several files or folders, you have an option of filtering them for the recovery process: to recover All selected files and folders, Deleted only or Existing only files and folders
6. You have an option of recovering named streams attached to a file on NTFS volume. This includes, for example, Music ratings and album info, Document Author and properties, and so on... These streams will only be recovered and attached to a file when recovering target is an NTFS volume (FAT/exFAT do not support named streams)
7. Option Browse output folder after recovery will open Windows Explorer and display the recovered items after recovery process is complete

8. Extended recovery configuration options are available when clicking more options... link at bottom:



Default unerase path

Z:\

Options

☑ All ☐ Deleted only ☐ Existing only

Naming options

☑ Use original file names (recommended)

☐ Rename files to:

unerased (+00001)

Existing file conflict resolution

☑ Generate unique file name (recommended)

☐ Ask before overwrite

☐ Overwrite without prompt

☐ Skip existing files

- Naming options: whether to use original file names, or to generate unique file names for each file being recovered

- Conflict resolution: what to do when file being recovered already exists in the target folder (name duplicate detected)

9. Click Unerase

After the recovery process is complete, make sure that the results are correct by verifying the contents of files. In some cases, a file cannot be reliably restored because its contents or a part of it has been overwritten.

Important

For the safety reasons, Active@ UNERASER warns you if you are trying to write the restored file back onto the same drive. When you write a file to the same drive that contains deleted or damaged data, you may overwrite data that belongs to other deleted files or folders, or you may overwrite part of the same file that you are trying to recover. Always restore files to another physical HDD, external USB, removable or network drive.

5. Unerase All Volume Data on a Deleted or Damaged Partition

There are scenarios when you do not want to recover your data on a file-by-file basis. You just want to restore all live (non-deleted) volume data (files and folders) at once.

Possible scenarios when this is applicable:

- USB Flash or Camera Memory Card is damaged or formatted
- Volume boot sector is damaged by virus or power surge and volume becomes not readable in Windows
- Partition or Volume has been deleted, or formatted accidentally
- RAID Disk Array crashed and needs to be re-build

There are two basic approaches for restoring volume data all at once:

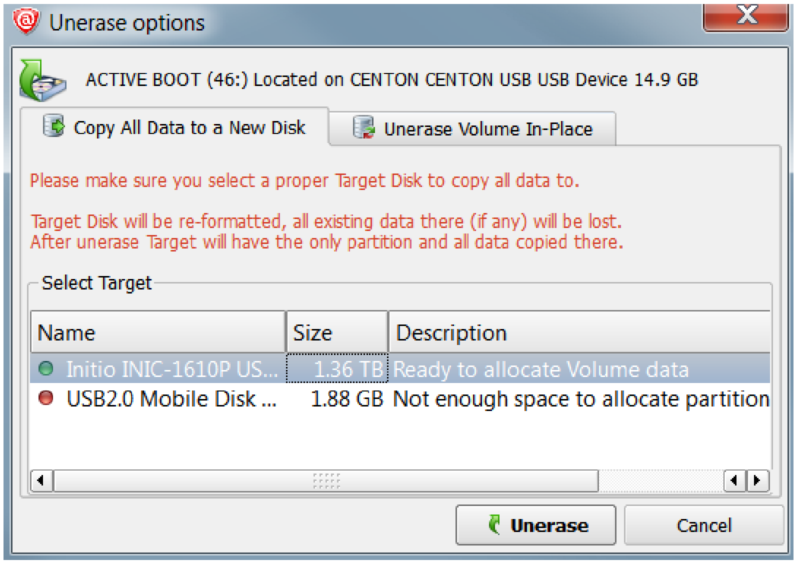
1. Copy all data to a new safe location (to another attached or external physical disk)
2. Physical recovery of the boot sector and partition table (in-place recovery)

Copying Volume Data to Another Location

This approach is the safest way to get all your data backed up to a new safe place, however this is a slowest way. You keep your original damaged disk (all data on it not touched), and just copy all your valuable information to a dedicated attached HDD/SDD, external USB HDD or Flash Disk. Copy process itself could take a long time, especially in case if you have terabytes of data (videos or photo archives).

To Copy All Volume Data to a New Disk:

1. In Active@ UNERASER, use QuickScan or SuperScan to detect deleted or damaged partition, verify its content and select the partition node.
2. To open the Unerase Options dialog box, use one of the following methods:
   - Click Unerase on the toolbar
   - Right-click the volume, and then choose Unerase from the context menu
   - Execute Unerase command from Action menu
   - Press Ctrl+R key combination



ACTIVE BOOT (46:) Located on CENTON CENTON USB USB Device 14.9 GB

Please make sure you select a proper Target Disk to copy all data to.

Target Disk will be re-formatted, all existing data there (if any) will be lost.
After unerase Target will have the only partition and all data copied there.

Select Target

Name	Size	Description
● Initio INIC-1610P US...	1.36 TB	Ready to allocate Volume data
● USB2.0 Mobile Disk ...	1.88 GB	Not enough space to allocate partition

3. Select a designated disk (having enough storage space) to copy all you data to. List box displays all available disks in the system, excluding physical disks where operating system is installed. You can plug-in more disks (or remove some them) and the software should detect and display them here immediately. Make sure you select a proper target disk, as long as before copying occurs it will be formatted (all existing data, if any, will be lost).
4. Click Unerase and wait while all volume data being copied.

After completion Windows Explorer should be launched and you can access and inspect your data at the new location.

Restoring a deleted/damaged volume in-place

This approach is the fastest way to return your volume "back to life" in place where it was resided originally, however this could be dangerous and non-guaranteed way. Recovery of partition information, volume boot sector and partition table usually takes couple seconds, however you need to be absolutely sure that you recover a proper volume, and recovery is successful only when file system itself has not been damaged previously.

This way works best when you just deleted a volume, realized the problem and immediately started recovery process. In this case not many data overwrite operations occurred within Windows environment, so most of your data structures are not being damaged.

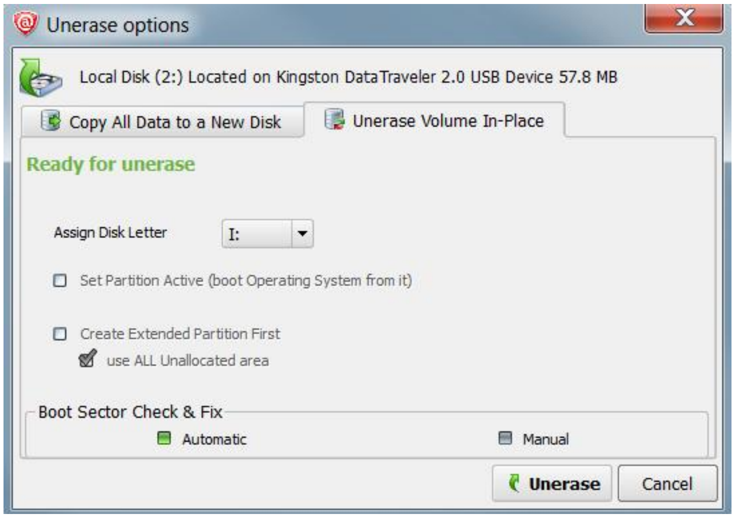
In case if you formatted the disk and installed a new OS, or copied some files to a newly formatted partition - you may still try this approach, however chances that some critical file system data structures has not been damaged are low, so most likely after recovery occurs Windows would not be able to access a logical disk and you will see something like: "Volume is not accessible or damaged" and "Do you want to format the volume?", and you'll need to delete this invalid partition and try another approach.

To evaluate your chances for successful physical recovery (in-place recovery), take a look at the icon besides the found volume. You can distinguish deleted partitions from existing ones by the icons:

- Grey icon shows an existing partition or drive visible in Windows Explorer
- Green icon shows live drive in SuperScan results (having drive letter)
- Grey icon with Green mark shows a deleted partition with Excellent integrity status, which means the chances for successful recovery in-place are good
- Grey icon with Brown mark shows a deleted partition with Acceptable integrity status, which means that there are chances for successful recovery in-place
- Grey icon with Red mark shows a deleted partition with Poor integrity status, however this partition might has been formatted before deletion or has some other damage, so there are minimal chances of successful volume recovery in-place

To restore a deleted volume in-place:

1. In Active@ UNERASER, use QuickScan or SuperScan to detect deleted partition, verify its content and select the deleted partition node.
2. To open the Unerase Options dialog box, use one of the following methods:
   - Click Unerase on the toolbar
   - Right-click the volume, and then choose Unerase from the context menu
   - Execute Unerase command from Action menu
   - Press Ctrl+R key combination
3. Go to Unerase Volume In-Place tab and check recovery options



Local Disk (2:) Located on Kingston DataTraveler 2.0 USB Device 57.8 MB

Ready for unerase

Assign Disk Letter I:

□ Set Partition Active (boot Operating System from it)

□ Create Extended Partition First

☑ use ALL Unallocated area

Boot Sector Check & Fix

🟩 Automatic

▨ Manual

4. To assign a partition to be recovered non-default disk letter, you may choose one of available letters from the drop-down box

5. To mark a partition to be recovered as an Active , you may check the related check box. Be careful ! If you mark as an Active a partition that does not have system files on it for the booting process - your computer might not boot properly. So mark it as an Active only when you sure 100% percent that partition being recovered had an Active status before deletion

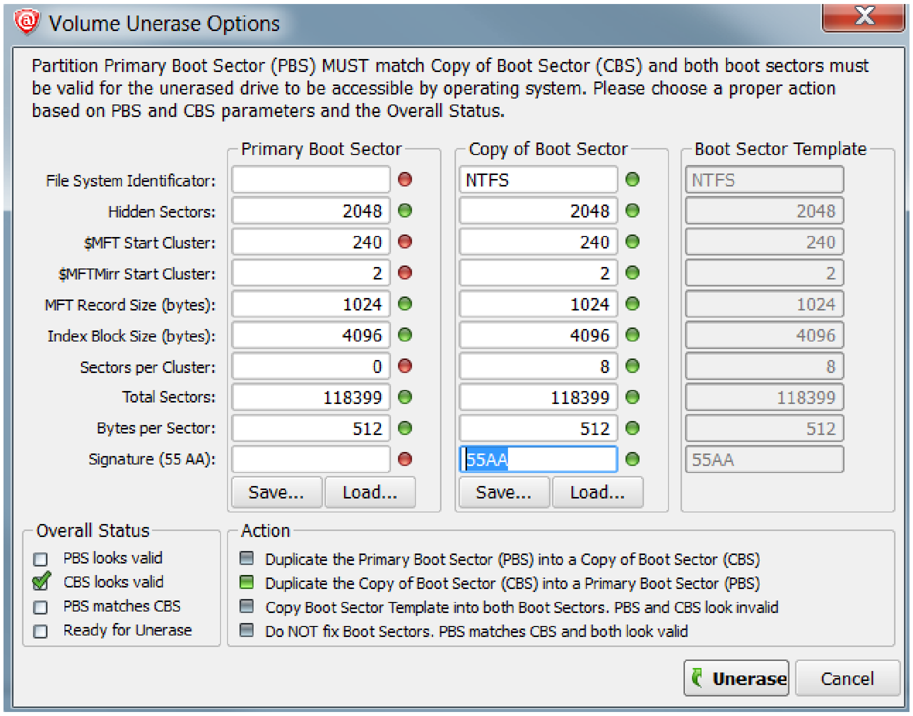
6. In some cases partition being recovered seems to be not a Primary type, but the Logical Disk in the Extended partition. In this case Create Extended Partition First options will be available, if no Extended partition exists on the disk. Keep it turned on if you want to create Extended partition container first, then to place your recovered partition inside. If option use ALL Unallocated area is turned off - Extended partition (container) will have the same size as partition being recovered, otherwise Extended partition (container) would occupy all unallocated space on the disk

7. You have an option to perform either Automatic or Manual check and fix of the Volume Boot Sector. If you are not familiar with disk low-level structures, use Automatic mode. If you know a lot about sectors, clusters, FAT, MFT, etc.. you can choose Manual mode to check the parameters manually and to select the most appropriate action

8. Click Unerase

After the recovery process is complete, a confirmation message pops up. Make sure that the results are correct by verifying the contents of the recovered partition in the Windows Explorer. Recovered partition should appear there after you refresh its content.

Manual mode for Volume Boot Sector Recovery



Volume Unerase Options

Partition Primary Boot Sector (PBS) MUST match Copy of Boot Sector (CBS) and both boot sectors must be valid for the unerased drive to be accessible by operating system. Please choose a proper action based on PBS and CBS parameters and the Overall Status.

	Primary Boot Sector		Copy of Boot Sector		Boot Sector Template
File System Identificator:		🔴	NTFS	🟢	NTFS
Hidden Sectors:	2048	🟢	2048	🟢	2048
$MFT Start Cluster:	240	🔴	240	🟢	240
$MFTMirr Start Cluster:	2	🔴	2	🟢	2
MFT Record Size (bytes):	1024	🟢	1024	🟢	1024
Index Block Size (bytes):	4096	🟢	4096	🟢	4096
Sectors per Cluster:	0	🔴	8	🟢	8
Total Sectors:	118399	🟢	118399	🟢	118399
Bytes per Sector:	512	🟢	512	🟢	512
Signature (55 AA):		🔴	55AA	🟢	55AA

Overall Status

□ PBS looks valid
☑ CBS looks valid
□ PBS matches CBS
□ Ready for Unerase

Action

□ Duplicate the Primary Boot Sector (PBS) into a Copy of Boot Sector (CBS)
🟩 Duplicate the Copy of Boot Sector (CBS) into a Primary Boot Sector (PBS)
□ Copy Boot Sector Template into both Boot Sectors. PBS and CBS look invalid
□ Do NOT fix Boot Sectors. PBS matches CBS and both look valid

If you've chosen Manual mode for the Boot Sector Check & Fix, dialog like above appears.

You can:

- Verify the parameters of the Primary and Copy of Boot Sector located on the disk. Parameters that look like invalid are marked with a red mark. Boot Sector Template column is formed programmatically and contains the most appropriate parameters for the partition found
- Save to the file raw Primary Boot Sector or Copy of Boot Sector to be able to analyze these raw values in Hex Editor or third party software, or restore them back if recovery is unsuccessful
- Load from the file raw Primary Boot Sector or Copy of Boot Sector to restore them back after unsuccessful recovery
- See the Overall Status of Partition Boot Sectors (their validity and match)
- Choose an Action to execute for the Boot Sectors while partition recovery:

1. Duplicate Primary Boot Sector into a Copy of Boot Sector - if you are sure that Primary Boot Sector is valid, but Copy is not
2. Duplicate Copy of Boot Sector into a Primary Boot Sector - if you are sure that Copy of Boot Sector is valid, but Primary is not
3. Copy Boot Sector Template into both Boot Sectors - if both Primary and Copy of Boot Sector look invalid
4. Do NOT fix Boot Sectors - if both Boot Sectors look valid and match each other and the Boot Sector Template values.

In the example above, even you are not a specialist - you can notice that Primary Boot Sector contains missed information (i.e. damaged), the red marks appear next to the fields, so the most appropriate action is to Duplicate Copy of a Boot Sector into a Primary Boot Sector.

Important

Unerase command for a deleted volume has been automatically logged to the partitioning backup file, and you can always rollback you changes later on.

Note

Unerase in place for a deleted partition function is available in commercial (purchased) version only.

6. Search for Deleted Files and Folders

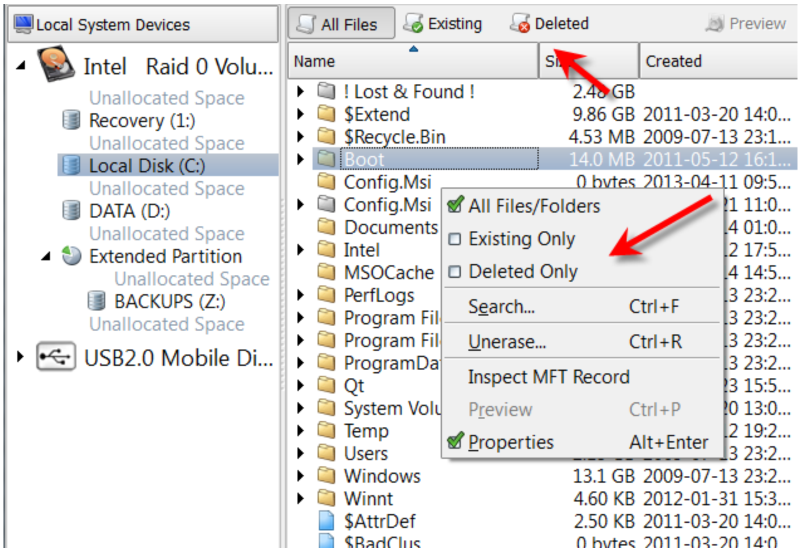
Search procedure can be helpful when you've completed QuickScan for the particular volumes and you are not able to locate your files, or you cannot assume the location.

Advice

Before using any recovery software, including Active@ UNERASER, check the Recycle Bin to see if the deleted file or folder is there. If it is, use the standard Windows Restore command to recover your data from there. If you cannot find the file or folder you are looking for in the Recycle Bin, continue with search and recovery procedures.

To locate specific files and folders:

1. Launch an Active@ UNERASER and select a volume that supposedly contains deleted files
2. Try direct listing: If you know exactly where the deleted files or folders are located, you can use the volume scan procedure. After the drive has been scanned, manually navigate to the folder path the same way as you would in Windows Explorer. If you cannot find the file or folder, open a tree node named !Lost & Found! If the parent folder of the deleted file has been deleted as well, it is very likely the deleted item will be placed in this virtual folder. If you are still unable to locate your data, proceed to the next step
3. Try filtering: For the particular volume (or even folder) you can setup a filter to display deleted only or existing only files and folders:
   - To display only deleted files, right-click the view and choose Deleted only from the context menu. You can also click Deleted toolbar button in Filter section
   - To display only existing files, right-click the view and choose Existing only from the context menu. You can also click Existing toolbar button in Filter section
   - To clear the filter, right-click the view and choose All Files/Folders from the context menu. You can also click All Files toolbar button in Filter section



Name	Si	Created
! Lost & Found !	2.48 GB	
$Extend	9.86 GB	2011-03-20 14:0...
$Recycle.Bin	4.53 MB	2009-07-13 23:1...
Boot	14.0 MB	2011-05-12 16:1...
Config.Msi	0 bytes	2013-04-11 09:5...
Config.Msi		1 11:0...
Documents		4 01:0...
Intel		2 17:5...
MSOCache		4 14:5...
PerfLogs		3 23:2...
Program Fil		3 23:2...
Program Fil		3 23:2...
ProgramDa		3 23:2...
Qt		3 15:5...
System Volu		0 13:0...
Temp		2 19:2...
Users		3 23:2...
Windows	13.1 GB	2009-07-13 23:2...
Winnt	4.60 KB	2012-01-31 15:3...
$AttrDef	2.50 KB	2011-03-20 14:0...
$BadClus	0 bytes	2011-03-20 14:0

4. Try Search mode: If you are not certain where the deleted file or folder was located before it was deleted, select a drive or folder and click Search on the toolbar, or right-click the drive or folder and choose Search in the context menu, or select a volume and press Ctrl+F. Do the following in the Search dialog box:

   a. To find a file by name, enter the file name in the Find what field. Search will look for files that match the name. You may enter part of the file name and use an asterisk (*) to represent the rest of the name. Regular expressions are supported (RegExp)

   b. To search by file type, choose a file type from the File type drop-down list

   c. To exclude existing files and folders from the search results, mark the Deleted option

   d. To exclude deleted files and folders from the search results, mark Non-deleted option

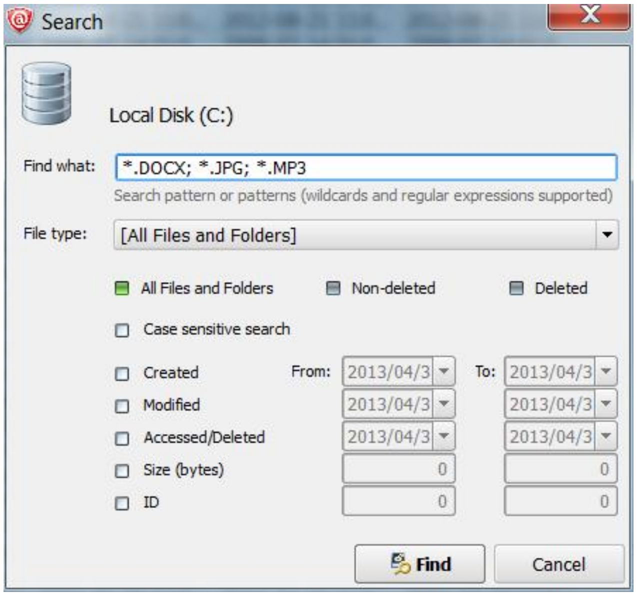
   e. To use case sensitive search, clear the Case insensitive search check box

   f. To search for a file based on a date, select the Created, Modified or Accessed [Deleted] check boxes and enter a From and To date range

   g. To search for a file based on the size of the file, select the Size check box and enter a From and To size range

   h. To search for a file identifier, select the ID check box and enter a From and To identifier range

   i. Click Find to start Search process



Search

Local Disk (C:)

Find what: *.DOCX; *.JPG; *.MP3

Search pattern or patterns (wildcards and regular expressions supported)

File type: [All Files and Folders]

● All Files and Folders ● Non-deleted ● Deleted

□ Case sensitive search

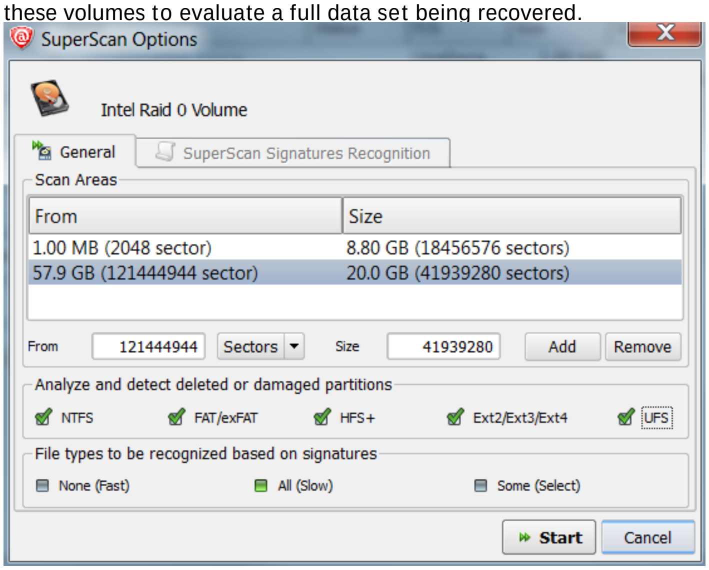
	From:	To:
□ Created	2013/04/3	2013/04/3
□ Modified	2013/04/3	2013/04/3
□ Accessed/Deleted	2013/04/3	2013/04/3
□ Size (bytes)	0	0
□ ID	0	0

   j. After the Search is complete, examine the Search Results virtual folder. This is a flat list of all items satisfying your criteria. You can sort Search results on any column (name, size, date, ID...), check properties of items, preview and recover files and folders.

5. Try SuperScan: If no files were found, use the SuperScan to thoroughly scan the HDD/SSD/USB surface to reconstruct all possible data entries. This is relatively slow process, however it brings maximum results:

   1. SuperScan detects and reconstructs many volumes presumably existed on scanned disk area. It can detect FAT/FAT32/exFAT, NTFS, Apple HFS+, Linux Ext2/Ext3/Ext4fs, Unix UFS file systems. Inspect

these volumes to evaluate a full data set being recovered.



Scan Areas

From	Size
1.00 MB (2048 sector)	8.80 GB (18456576 sectors)
57.9 GB (121444944 sector)	20.0 GB (41939280 sectors)

From 121444944 Sectors Size 41939280

Analyze and detect deleted or damaged partitions

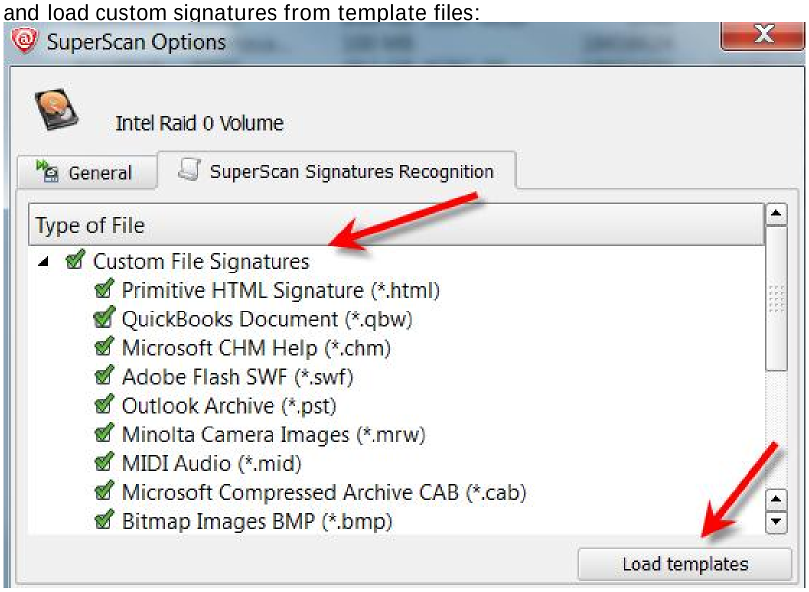
☑ NTFS ☑ FAT/exFAT ☑ HFS+ ☑ Ext2/Ext3/Ext4 ☑ UFS

File types to be recognized based on signatures

□ None (Fast) ■ All (Slow) □ Some (Select)

2. SuperScan inspects existing volumes more deeply, for example, if you formatted the volume, QuickScan displays no files on it, however SuperScan most likely will detect formatted data structures and will reconstruct previous data tree.

3. SuperScan has an option of detecting deleted files by their signatures. More than 60 predefined file signatures have been implemented internally (MP3, JPG, DOC, ZIP, etc..) and there is an option to create and load custom signatures from template files:



Type of File

- ☑ Custom File Signatures
  - ☑ Primitive HTML Signature (*.html)
  - ☑ QuickBooks Document (*.qbw)
  - ☑ Microsoft CHM Help (*.chm)
  - ☑ Adobe Flash SWF (*.swf)
  - ☑ Outlook Archive (*.pst)
  - ☑ Minolta Camera Images (*.mrw)
  - ☑ MIDI Audio (*.mid)
  - ☑ Microsoft Compressed Archive CAB (*.cab)
  - ☑ Bitmap Images BMP (*.bmp)

If you have completed of all the steps listed above and your files and folders still cannot be found, it is likely that the drive space formerly occupied by your files has been completely overwritten with other data. If this is the case, there are no recovery tools that can help you. This can happen when a lot of writing operations occur on the drive, for example during a software installation. As well, Windows operating system will sometimes create temporary files for different processes. If the process involves a lot of data and many temporary files are written, your deleted files may have been destroyed.

Important

When you are using a search pattern in Search, it is the same pattern recognized when searching in Microsoft Windows. The asterisk symbol (*) in the pattern means, that at this place can be zero, or any number of any symbols.

Examples:

```
*           - All files on the drive or in the folder
*.TXT       - All files with "TXT" extension
My*.*       - All files starting with "My"
MyFile.txt - Search for the file named "MyFile.txt"
```

Note

You can distinguish deleted files and folders from existing files and folders by the icons:

- Blue or yellow icon point to an existing file and folder
- Grey icon points to a deleted file and folder

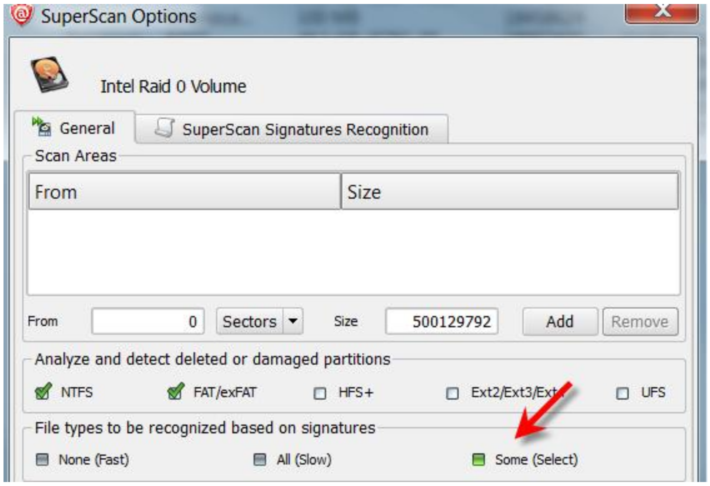
7. Search for Standard File Signatures and Define Custom Signatures

In case if recovery software is unable to detect deleted files after QuickScan or SuperScan (for example, when directory area keeping file headers is wiped out or overwritten by other data), the only chance to recover files is to search for file signatures. In this case un-fragmented files can still be detected and recovered.

Active@ UNERASER comes with more than sixty predefined (internally programmed, very fast) file signatures to be analyzed and detected while SuperScan is in progress (MS Office Documents, Photo Camera Image formats, ZIP/RAR Archives, Music & Video MP3/MP4, etc..). For expert users there is advanced programming language which allows to define custom file signatures for UNERASER to search for specific data formats.

To search for standard file signatures:

1. Start Active@ UNERASER and choose a disk or volume to be inspected (place a cursor on it)
2. Launch SuperScan dialog box and define SuperScan options
3. Select All or Some file signatures to be recognized:



SuperScan Options

Intel Raid 0 Volume

General | SuperScan Signatures Recognition

Scan Areas

From	Size

From: 0 Sectors   Size: 500129792

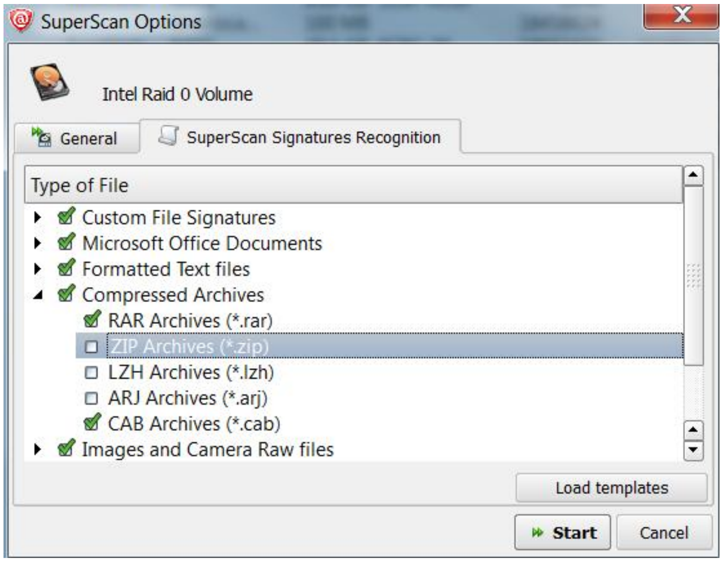
Analyze and detect deleted or damaged partitions

☑ NTFS ☑ FAT/exFAT □ HFS+ □ Ext2/Ext3/Ext4 □ UFS

File types to be recognized based on signatures

○ None (Fast) ○ All (Slow) ● Some (Select)

4. On a SuperScan Signatures Recognition tab verify signatures to be processed:



- ☑ Custom File Signatures
- ☑ Microsoft Office Documents
- ☑ Formatted Text files
- ☑ Compressed Archives
  - ☑ RAR Archives (*.rar)
  - □ ZIP Archives (*.zip)
  - □ LZH Archives (*.lzh)
  - □ ARJ Archives (*.arj)
  - ☑ CAB Archives (*.cab)
- ☑ Images and Camera Raw files

5. Click Start button and wait until something is recognized
6. Inspect specific groups in Signatures folder for files being detected
7. Preview and recover files (if detected) from specified groups

Custom File Signatures

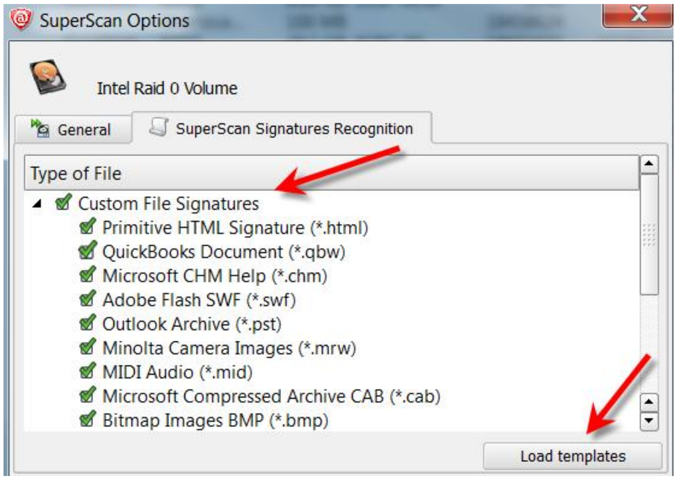
Sometimes advanced users need to detect more specific file formats, not being described in standard set of file signatures.

Active@ UNERASER offers advanced tools to define user's templates for signatures to be analyzed. Signatures can be described using extended definition language which complies with RegExp (Regular Expressions). See language definition and syntax below.

To create and use a custom file signatures:

1. Create a text file containing one or multiple signatures definition (using syntax and examples below)
2. Launch Active@ UNERASER, select disk or volume to be inspected, and click SuperScan button
3. In SuperScan options, File types to be recognized based on signatures area, choose Some (Select)
4. Load created text file contents into Signatures Tree
   - Click Load Templates... button
   - Select created text file containing signatures definition

- Find custom signatures in Signatures Tree and make sure that they are selected



SuperScan Options

Intel Raid 0 Volume

General | SuperScan Signatures Recognition

Type of File

- ☑ Custom File Signatures
  - ☑ Primitive HTML Signature (*.html)
  - ☑ QuickBooks Document (*.qbw)
  - ☑ Microsoft CHM Help (*.chm)
  - ☑ Adobe Flash SWF (*.swf)
  - ☑ Outlook Archive (*.pst)
  - ☑ Minolta Camera Images (*.mrw)
  - ☑ MIDI Audio (*.mid)
  - ☑ Microsoft Compressed Archive CAB (*.cab)
  - ☑ Bitmap Images BMP (*.bmp)

5. Click Scan button to execute SuperScan

6. Inspect specific groups in Signatures Files panel for files being detected

7. Preview and recover files (if detected) from specified groups

Signatures definition language and examples:

```
; ==========================================================================================================
;                                        Signature Templates Usage
; ==========================================================================================================
; Empty lines and lines starting with semicolon are ignored
; Sections order and lines order in sections are not important
; Letter case is not important (excepting RegExp fields)
; ----------------------------------------------------------------------------------------------------------
; Section TEMPLATES - required and contains fields numbering from one
;        - TEMPLATE### - points to the section where signature template is described (numbered from one)
;
; ----------------------------------------------------------------------------------------------------------
; Section Template Header - required and contains fields:
;      - BEGIN - required. Points to the section describing begin of the signature file
;      - FOOTER - non required. Points to the section describing end of the signature file
;      - MAX_SIZE - non required. Maximum file size to force file-end, if no file-end signature is detected. By
default it is 64Kb.
;      - GROUP - non required. If missed - template goes to User Defined templates group by default
;      - DESCRIPTION - non required. This is a descriptive name of user template being displayed on a screen
;      - EXTENSION - non required. This is a file extension to be assigned and displayed
;      - SCRIPT - non required. Refers to the section where size of the file being calculated
; ----------------------------------------------------------------------------------------------------------
;       Note: If field SCRIPT is present, then field FOOTER is ignored
;
; ----------------------------------------------------------------------------------------------------------
; Section describing file beginning (required), contains fields of the same type:
;
;     <signature> = <offset_start> | <offset_end>
;
;     signature      - expression (regular or RegExp-compatible). Expression max length is 1024 bytes.
;     offset_start   - acceptable minimal signature offset from the beginning of the file
;     offset_end     - acceptable maximum signature offset from the beginning of the file
;
;     If there are several fields listed in signature beginning, logical AND operation applied to confirm file
start.
;
;-----------------------------------------------------------------------------------------------------------
; Section calculating file size (not required), contains operators of four types:
;     <result> = <command> (<argument>, <argument>)
;     <result> = <argument>
;     IF (<argument< <condition> <argument>) GOTO <label>
;     GOTO <label>
;
; <commands> : READ, ENDIAN, SUM, SUB, MUL, DIV, SHR, SHL, AND, OR and XOR
;     Most of commands are the same as in assembler programming language, except:
;     READ - first argument - data type (size) to be read, second - offset from the beginning of the file
;     ENDIAN - first argument - data type (size), second - expression, which byte order will be swapped
;     First argument for commands READ and ENDIAN must be one of reserved data types: BYTE, WORD, DWORD, QWORD
; <argument> : can be either a named variable or a constant
; <result>   : can be the only named variable
; <condition>: can be one of : <  <=  ==  >=  >  !=   (meaning is the same as in C++)
; <label>    : consists of label name followed by colon and it can precede any operator
;
; Label named EXIT has been reserved and instructs to complete the calculations
; Named variable SIZE has been reserved and keeps the file size
; Constants can be in Decimal form, Binary (followed by 'b'), Octal ('o'), and Hexadecimal ('h') or can be a text
string
;
; -----------------------------------------------------------------------------------------------------------
; Section describing file end (not required), contains fields of the same type:
;
;     <signature> [= <bytes_to_append>]
;
;     signature       - expression (regular or RegExp-compatible). Expression max length is 1024 bytes.
;     bytes_to_append - not required. How many bytes to append to the file after the signature is found
;
;     If there are several fields listed in signature, logical OR operation applied to define file end.


; ===========================================================================================================
;                                                Examples
; ===========================================================================================================

[TEMPLATES]
TEMPLATE1 = PRIMITIVE_HTML
TEMPLATE2 = PRIMITIVE_JPG
TEMPLATE3 = QBW_HEADER
TEMPLATE4 = CHM_HEADER
TEMPLATE5 = SWF_HEADER
TEMPLATE6 = PST_HEADER
TEMPLATE7 = MRW_HEADER
TEMPLATE8 = MID_HEADER
TEMPLATE9 = CAB_HEADER
TEMPLATE10 = BMP_HEADER
TEMPLATE11 = DJV_HEADER


[PRIMITIVE_HTML]
DESCRIPTION = Primitive HTML Signature
EXTENSION = html
BEGIN=HTML_BEGIN
FOOTER=HTML_FOOTER
MAX_SIZE = 655360


[HTML_BEGIN]
<html = 0 | 512
<head = 0 | 1024

[HTML_FOOTER]
</html> = 2

[PRIMITIVE_JPG]
BEGIN=BEGIN.TEST.JPG
GROUP = Images and Camera RAW files
DESCRIPTION = Primitive JPG files
FOOTER=FOOTER-.TEST.JPG
EXTENSION = test.jpg
MAX_SIZE = 3221225472
[BEGIN.TEST.JPG]
\xFF\xD8\xFF = 0 | 0

[FOOTER-.TEST.JPG]
\xFF\xD9

[DJV_HEADER]
DESCRIPTION=DjVu Document
EXTENSION=djvu
BEGIN=DJV_BEGIN
SCRIPT=DJV_SCRIPT

[DJV_BEGIN]
AT&TFORM=0|0

[DJV_SCRIPT]
                size = read(dword, 8)
                size = endian(dword, size)
                size = sum(size, 12)

[QBW_HEADER]
DESCRIPTION=QuickBooks Document
```

```
EXTENSION=qbw
BEGIN=QBW_BEGIN
SCRIPT=QBW_SCRIPT

[QBW_BEGIN]
MAUI=96|96

[QBW_SCRIPT]
                data = read(dword, 36)
                temp = read(dword, 52)
                if (temp <= data) goto exit
                size = sum(temp, 1)
                size = shl(size, 10)

[CHM_HEADER]
DESCRIPTION=Microsoft CHM Help
EXTENSION=chm
BEGIN=CHM_BEGIN
SCRIPT=CHM_SCRIPT

[CHM_BEGIN]
ITSF=0|0

[CHM_SCRIPT]
                version = read(dword, 4)
                if (version == 0) goto exit
                header = read(dword, 8)
                if (header <= 1Ch) goto exit
                temp = read(qword, header)
                if (temp != 1FEh) goto exit
                temp = sum(header, 8)
                size = read(qword, temp)
                temp = sum(header, 10h)
                if (size > temp) goto exit
                size = 0

[SWF_HEADER]
DESCRIPTION=Adobe Flash SWF
EXTENSION=swf
BEGIN=SWF_BEGIN
SCRIPT=SWF_SCRIPT

[SWF_BEGIN]
FWS=0|0

[SWF_SCRIPT]
                data = read(byte, 3)
                if (data <= 10h) goto exit
                size = read(dword, 4)
                if (size <= 8) goto exit
                size = 0

[PST_HEADER]
DESCRIPTION=Outlook Archive
EXTENSION=pst
BEGIN=PST_BEGIN
SCRIPT=PST_SCRIPT

[PST_BEGIN]
!BDN=0|0

[PST_SCRIPT]
                data = read(byte, 10)
                if (data == 0Eh) goto valid
                if (data != 17h) goto exit
                size = read(dword, 184)
                goto exit
valid:
                size = read(dword, 168)

[MRW_HEADER]
DESCRIPTION=Minolta Camera Images
EXTENSION=mrw
BEGIN=MRW_BEGIN
SCRIPT=MRW_SCRIPT

[MRW_BEGIN]
\x00MRM=0|0

[MRW_SCRIPT]
                data = read(dword, 4)
                if (data == 0) goto exit
                width = read(word, 24)
                if (width == 0) goto exit
                width = endian(word, width)
                height = read(word, 26)
                if (height == 0) goto exit
                height = endian(word, height)
                pixel = read(byte, 32)
                if (pixel == 0) goto exit
                pixel = mul(pixel, width)
                pixel = mul(pixel, height)
                pixel = div(pixel, 8)
                size = endian(dword, data)
                size = sum(size, pixel)
                size = sum(size, 8)

[MID_HEADER]
DESCRIPTION=MIDI Audio
EXTENSION=mid
BEGIN=MID_BEGIN
SCRIPT=MID_SCRIPT

[MID_BEGIN]
MThd=0|0

[MID_SCRIPT]
next:
                temp = read(dword, size)
                if (temp == "MThd") goto valid
                if (temp != "MTrk") goto exit
valid:
                size = sum(size, 4)
                temp = read(dword, size)
                size = sum(size, 4)
                temp = endian(dword, temp)
                size = sum(size, temp)
                goto next

[CAB_HEADER]
DESCRIPTION=Microsoft Compressed Archive CAB
EXTENSION=cab
BEGIN=CAB_BEGIN
SCRIPT=CAB_SCRIPT

[CAB_BEGIN]
MSCF=0|0

[CAB_SCRIPT]
                version = read(word, 24)
                if (version != 103h) goto exit
                folders = read(word, 26)
                folders = mul(folders, 8)
                folders = sum(folders, 36)
                files = read(word, 28)
                files = mul(files, 16)
                files = sum(files, folders)
                temp = read(dword, 16)
                if (temp < folders) goto exit
                temp = read(dword, 8)
                if (temp <= files) goto exit
                flags = read(word, 30)
                flags = and(flags, 4)
                if (flags == 0) goto skip
                flags = read(dword, 36)
                if (flags != 20) goto skip
                flags = read(dword, 44)
                if (flags < temp) goto skip
                size = flags
                temp = read(dword, 48)
skip:
                size = sum(temp, size)

[BMP_HEADER]
DESCRIPTION=Bitmap Images BMP
EXTENSION=bmp
BEGIN=BMP_BEGIN
SCRIPT=BMP_SCRIPT

[BMP_BEGIN]
BM=0|0

[BMP_SCRIPT]
                width = read(dword, 12h)
                if (width == 0) goto exit
                height = read(dword, 16h)
                if (height == 0) goto exit
                pixel = read(word, 1ch)
                if (pixel == 1) goto valid
                if (pixel == 4) goto valid
                if (pixel == 8) goto valid
                if (pixel == 16) goto valid
                if (pixel == 24) goto valid
                if (pixel != 32) goto exit
valid:
                pixel = mul(pixel, width)
                pixel = mul(pixel, height)
                pixel = div(pixel, 1000b)
                rastr_size = read(dword, 22h)
                if (rastr_size < pixel) goto exit
                rastr_offset = read(dword, 0Ah)
                if (rastr_offset < 38) goto exit
                rastr_offset = sum(rastr_offset, rastr_size)
                size = read(dword, 2)
                if (size >= rastr_offset) goto exit
                size = 0
```

Important

Regular Expressions can be used while defining signature headers and footers. Please check RegExp syntax on a web, for example here.

8. Preview File (Check Recovery Status)

In order to recover files or folders, you must scan the drive or partition and then search for damaged or deleted files or folders. If you have found some damaged or deleted files and you are not sure whether or not a file is safe for recovery or you are not sure whether or not the file data has been overwritten on the drive, you may preview the content of file before recovery occurs.

For Preview mode to be available, File Preview component needs to be selected when you are installing the software. If File Preview has not been installed, Preview command will be greyed out and inaccessible.

If the file data has been overwritten on the drive, it is not likely that the file can be previewed. If this is the case, you will see a warning message, and file will be previewed in Hex format. If you plan to purchase the commercial version of Active@ UNERASER, you may want to preview file contents to help you determine whether or not the contents are valuable using the FREE version of the software. If you can preview file contents, it is likely that you can recover the file.

Preview file contents using the built-in preview module works with the following image files: *.bmp, *.wbmp, *.dib, *.gif, *.jpg, *.jpeg, *.pcx, *.ico, *.tif, *.tiff, *.png, *.wmf.

Other document types can be previewed using an external viewer like Microsoft Word or using the built-in Hex/Text viewer. If you want to preview a file named MyDoc.DOC you must have an application installed that is able to open *.DOC files. The file will be rendered and previewed using this application. If you do NOT have an application installed that is able to open *.DOC files, the file will be previewed in the default built-in Hex/Text viewer.

For example, if you have Microsoft Office installed, most likely you will be able to preview office document types: *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.vsd, *.mpp, *.rpt.

Important

Avoid previewing large files! In order to preview a file's contents, the file needs to be recovered and placed in temporary storage. The built-in or external preview utility reads this temporary file. If you have enough RAM, the temporary file is kept in volatile memory. If you do not have enough RAM, a temporary file could be written onto the drive that contains damaged or deleted files and there is a chance that you may overwrite your original deleted data.

To preview file contents and check recovery status:

1. In Active@ UNERASER, search for deleted files and folders and select the file.
2. To launch Preview module, use one of the following methods:
    - Click Preview toolbar button:

- Right-click the file, and choose Preview from the context menu
- Double-click the file
- Press Enter or Ctrl+P key combination

3. A Preview window appears with the first page of your document.

Note

You cannot preview encrypted files and files having size more than 10MB.

9. Rollback, Backup and Restore Disk Partitioning Info

Disk Partitioning Information is an MBR/GPT, Partition Table and Volume Boot Sectors for each existing partition on the disk.

You might ask, "Why should I backup Partitioning Info?"

Here is the answer: If you something goes wrong while attempting to recover the partition (for example you recovered wrong partition), you will be able to restore original partitioning structure for the drive being repaired.

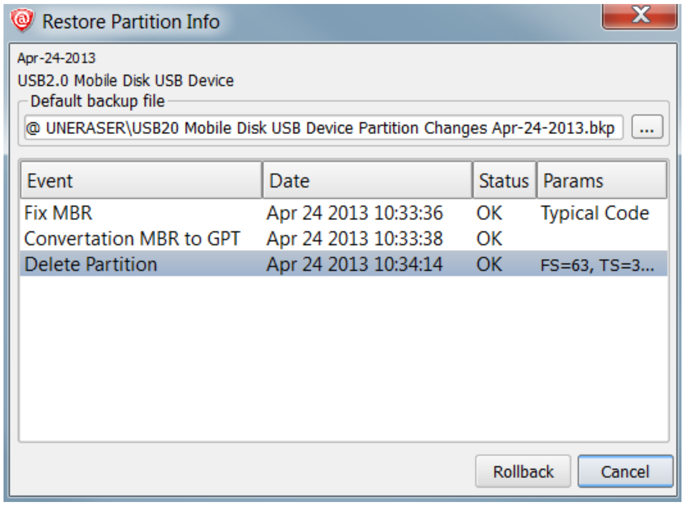
Automatic Partitioning Backups

When you are trying to resolve your partitioning problem in place, you usually execute such commands of Active@ UNERASER as Create/Fix Partitioning, Convert Partition Style, Fix Boot Sector, Delete Invalid Partition and Recover Partition (in place). Every command execution has been automatically logged the partitioning backup file. If something goes wrong (you recovered not a proper partition, you accidentally removed a valid partition...) you always have a chance to rollback your last changes to the system.

Backups are stored for each physical device at the location Partitioning auto-backups default path in Settings.

To rollback partitioning changes:

1. Start Active@ UNERASER and select a physical device that you want to rollback changes for
2. From Partition menu click Rollback Partition Changes... command
3. Select a backup file, or confirm the backup file default location
4. Select a restore point to rollback to. If you executed several commands, these commands listed from top to bottom, and you can select a particular place to revert to
5. Click Rollback
6. Rollback process starts, you can check the results in log



Apr-24-2013
USB2.0 Mobile Disk USB Device
Default backup file
@ UNERASER\USB20 Mobile Disk USB Device Partition Changes Apr-24-2013.bkp

Event	Date	Status	Params
Fix MBR	Apr 24 2013 10:33:36	OK	Typical Code
Convertation MBR to GPT	Apr 24 2013 10:33:38	OK	
Delete Partition	Apr 24 2013 10:34:14	OK	FS=63, TS=3...

Important

To be able to rollback partitioning to the any particular restore point, we recommend you to use the only standard functions of Active@ UNERASER, and avoid using other tools, like Windows Disk Manager (to remove partitions, initialize disk, etc..)

To backup Disk Partitioning Info:

1. Start Active@ UNERASER and select a physical device (HDD, USB, Memory Card...) that you want to create a backup for
2. From Partition menu click Backup Partitioning Info... command
3. Select a file name and location where to store backup
4. Click Save

To restore Disk Partitioning Info from the backup:

1. Start Active@ UNERASER and select a physical device that you want to restore backup for
2. From Partition menu click Restore Partitioning Info... command
3. Select a backup file
4. Click Open
5. Restoration process starts, you can check the results in log

Important

Existing disk partitioning structure will be overwritten on the disk where you restore Disk Partitioning Info backup file to.

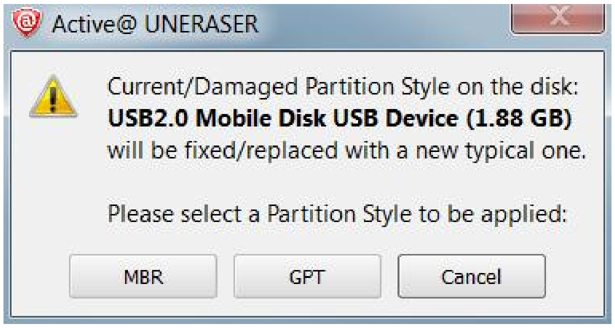
10. Fix damaged MBR/GPT and use Disk Partitioning Tools

Fixing MBR/GPT

If partition table looks OK for the disk you are recovering physically (you see all volumes in the Explorer Tree), but your computer still does not boot from this disk, it is possible that Master Boot Record (MBR) is damaged by virus or overwritten. You can try to use Fix Partitioning command to replace existing MBR with the one from the set of templates (the typical one).

To fix damaged Master Boot Record (MBR) or GUID Partition Table (GPT):

1. Select the disk in you want to fix MBR/GPT for (place cursor on it)
2. In the main window, from the Partition menu, choose Create/Fix Partitioning...
3. In confirmation dialog make sure that a proper disk is selected for MBR fixing
4. Click either MBR or GPT (depending on a partitioning style you like) to confirm the command and wait while list of disks is being refreshed:



Current/Damaged Partition Style on the disk:
USB2.0 Mobile Disk USB Device (1.88 GB)
will be fixed/replaced with a new typical one.

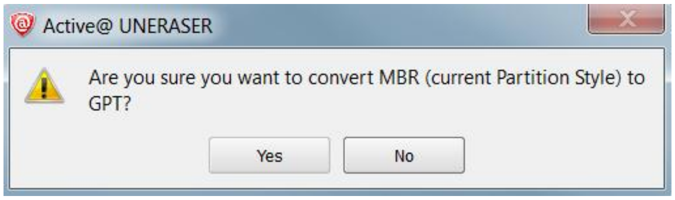
Please select a Partition Style to be applied:

Converting Partition Style

If you want to change "old" MBR style to a "new" one (GPT) to be able having more than four primary partitions or for some other reasons, you can easily do it with Active@ UNERASER. The same applied if you want to return from a "modern" GPT to "obsolete" MBR (but most compatible), for example, to work with disk under Windows 95/98/ME environments.

To convert partition style:

1. Select the physical disk which partitioning style will be converted (place cursor on it)
2. In the main window, from the Partition menu, choose Convert Partition Style...
3. In confirmation dialog make sure that a proper partitioning style will be applied
4. Click Yes to confirm the command and wait while list of disks is being refreshed:



Active@ UNERASER

Are you sure you want to convert MBR (current Partition Style) to GPT?

Deleting Invalid Partition

If you know for sure that partition on the disk is NOT valid (damaged, or created by mistake instead of deleted one, or recovered not properly) you can delete the existing partition first and then try to search and recover other partitions.

This is also the only option when you found deleted partition using QuickScan or SuperScan, and you know for sure that it is valid, but you are unable to recover it in place due to overlapping with others existing partitions. You are to detect the invalid partition first, delete it and then to recover the only partition you are interested in.

To delete invalid partition:

1. Verify that existing partition you want to delete is actually invalid partition (Windows Explorer is not displaying it properly, or unable to access it and suggests to format it, or displays a garbage instead of your files)
2. Select the partition to be deleted (place cursor on it)
3. In the main window, from the Partition menu, choose Delete Invalid Partition
4. In confirmation dialog make sure that a proper partition is selected for deletion
5. Click Yes to confirm the command and wait while list of disks is being refreshed

Note

You can delete the only existing partition (Primary or Extended) and you cannot delete the System partition (Active one or having Windows installed) . If you need to delete the Extended partition, make sure that it is empty (no logical drives left in it). If logical drives exist in Extended partition, you are to delete them first, then to delete Extended partition itself.

Important

Create/Fix Partitioning and Delete Invalid Partition commands for the hardware device has been automatically logged to the partitioning backup file, and you can always rollback you changes later on.

Note

Create/Fix Partitioning function is available in commercial (purchased) version only.

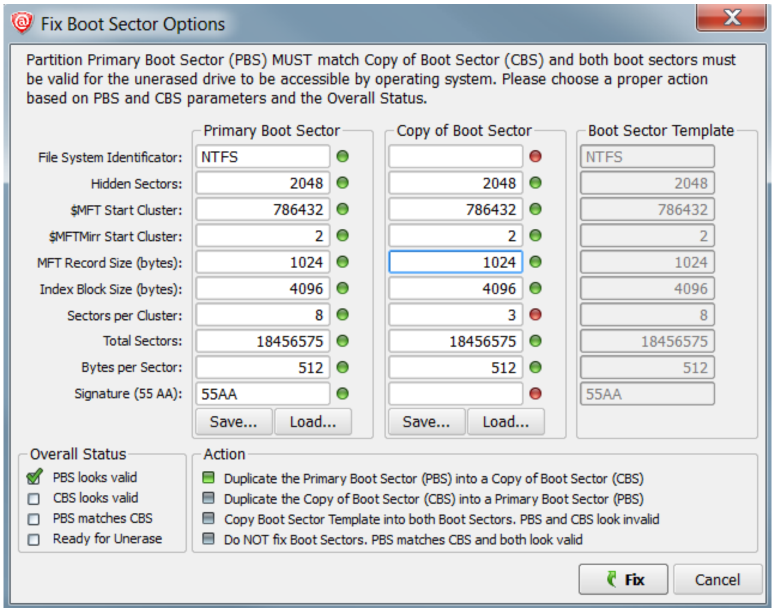
11. Fix Damaged Partition/Volume Boot Sector

Fixing Boot Sector

If volume looks OK for the disk you are recovering (you see all volumes in the Explorer Tree), but Windows still does not recognize a volume, or says "Volume is inaccessible" , it is possible that Partition Boot Sector (or Copy of Boot Sector) is damaged by virus or overwritten. You can try to use Fix Boot Sector command to replace Primary Boot Sector with its Copy (or backward), or both of them from the set of templates (typical boot sector). The idea is the same as for the Manual Volume Recovery Mode.

To fix damaged Partition (Volume) Boot Sector:

1. Select the volume (logical disk) you want to fix Boot Sector for (place cursor on it)
2. In the main window, from the Partition menu, choose Fix Boot Sector... or execute the same command from the context menu
3. In the dialog compare boot sector values, change them if needed, and select an action to execute. Details...
4. Click Fix to confirm the command and wait while list of disks is being refreshed



Fix Boot Sector Options

Partition Primary Boot Sector (PBS) MUST match Copy of Boot Sector (CBS) and both boot sectors must be valid for the unerased drive to be accessible by operating system. Please choose a proper action based on PBS and CBS parameters and the Overall Status.

	Primary Boot Sector		Copy of Boot Sector		Boot Sector Template
File System Identificator:	NTFS	🟢		🔴	NTFS
Hidden Sectors:	2048	🟢	2048	🟢	2048
$MFT Start Cluster:	786432	🟢	786432	🟢	786432
$MFTMirr Start Cluster:	2	🟢	2	🟢	2
MFT Record Size (bytes):	1024	🟢	1024	🟢	1024
Index Block Size (bytes):	4096	🟢	4096	🟢	4096
Sectors per Cluster:	8	🟢	3	🔴	8
Total Sectors:	18456575	🟢	18456575	🟢	18456575
Bytes per Sector:	512	🟢	512	🟢	512
Signature (55 AA):	55AA	🟢		🔴	55AA

Overall Status

☑ PBS looks valid
□ CBS looks valid
□ PBS matches CBS
□ Ready for Unerase

Action

🟩 Duplicate the Primary Boot Sector (PBS) into a Copy of Boot Sector (CBS)
■ Duplicate the Copy of Boot Sector (CBS) into a Primary Boot Sector (PBS)
■ Copy Boot Sector Template into both Boot Sectors. PBS and CBS look invalid
■ Do NOT fix Boot Sectors. PBS matches CBS and both look valid

Important

Fix Boot Sector command for the hardware device has been automatically logged to the partitioning backup file, and you can always rollback you changes later on.

Note

Fix Boot Sector function is available in commercial (purchased) version only.

12. Re-create Deleted or Damaged Disk Array (RAID) Virtually

There are many reasons for a Redundant Array of Independent Disks (RAID) system to fail (RAID controller failures, software RAID emulator errors, etc.). Active@ UNERASER provides an easy way to assemble array disks together and make damaged or deleted data accessible.

You can combine together a disk that was previously used as a part of a RAID system in a temporal (virtual) disk array. With this virtual configuration, you are able to perform all drive file recovery manipulations as though it is regular drive. You can even to create a Disk Image for the whole RAID and store it to the safe location.

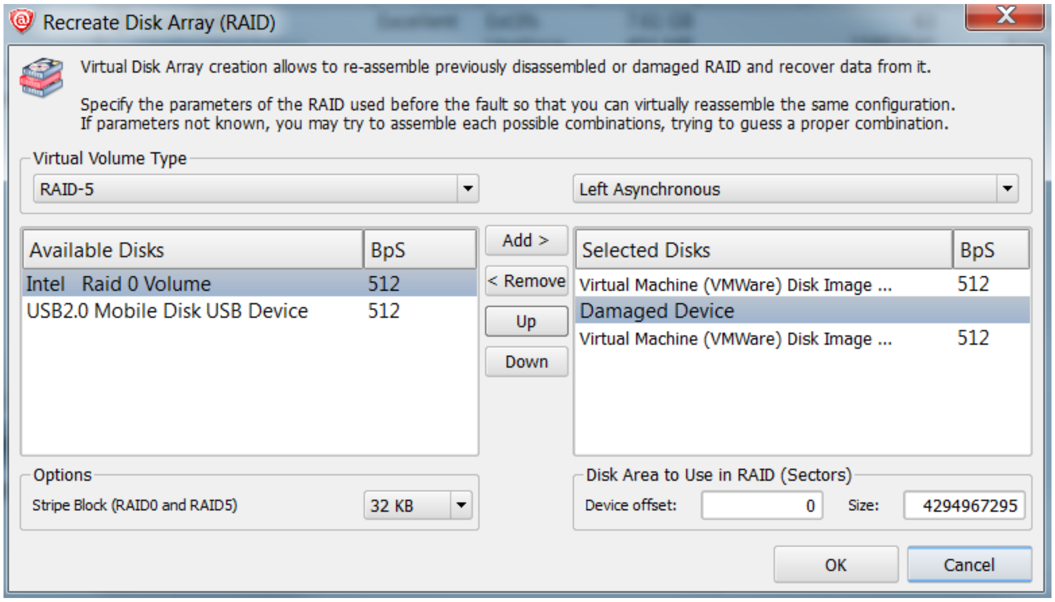
It is important that you specify the parameters of the RAID system that you know existed before the fault so that you can virtually reassemble the same system.

It is also important to list the disks in the correct order when making a virtual disk array. In most cases, the correct order is unknown. The only way to discover the correct order is to try all available combinations until you reach the one that works. If you are dealing with only two disks, it is simple. You have only two ways to arrange the order. If there are three disks, you must try a maximum of six combinations. If there are four disks, 24 combinations, and so on...

Each time you try a combination, write down the order you are trying, click OK and check the results by trying to access and scan the newly-created virtual RAID that is added to the list of Local System Devices. If you don't see your data or if there was an error during virtual array creation, mark this one as a failure and try another order of disks in array.

To create a Virtual Disk Array (RAID):

1. To open Recreate Disk Array (RAID) dialog, in the Action menu, choose Recreate RAID (Virtually)...



Recreate Disk Array (RAID)

Virtual Disk Array creation allows to re-assemble previously disassembled or damaged RAID and recover data from it.

Specify the parameters of the RAID used before the fault so that you can virtually reassemble the same configuration.
If parameters not known, you may try to assemble each possible combinations, trying to guess a proper combination.

Virtual Volume Type: RAID-5 | Left Asynchronous

Available Disks	BpS
Intel Raid 0 Volume	512
USB2.0 Mobile Disk USB Device	512

Selected Disks	BpS
Virtual Machine (VMWare) Disk Image ...	512
Damaged Device	
Virtual Machine (VMWare) Disk Image ...	512

Options
Stripe Block (RAID0 and RAID5): 32 KB

Disk Area to Use in RAID (Sectors)
Device offset: 0 Size: 4294967295

2. To choose a supported RAID type, in the Virtual Volume Type area, choose one of the following:

- Stripe Array (RAID-0) - Data located in stripes (blocks of size 32KB, 64KB, 128KB, etc.) distributed between two or more drives
- Mirror Array (RAID-1) - Data on two disks is identical - provides complete data duplication (or mirroring)
- RAID-5 Array - Data located in stripes distributed between two or more drives with parity control
- Span Array - Data located contiguously on one disk then on another disk, and so on...

3. To select disks from a list to create a virtual disk array:

   a. In the Available Disks list, select a device (or disk image)

   b. To add it to the Selected Disks list, click Add

   c. Repeat steps a. and b. for every disk in the original array. If one of the disks is physically damaged and not accessible, and if you have selected RAID-0 or RAID-5 in step 2, from the Available Disks list add Damaged Device instead of the named damaged disk

d. To change the order of disks in the Selected Disks list, select a disk name and click Up or Down to change its position in the list

4. To indicate the size of the stripe block, in the Options area, type the size of the block in kilobytes in the Stripe Block (RAID0 and RAID5) field. This is applicable only to RAID-0 and RAID-5 arrays. Standard values are 32Kb, 64Kb, 128Kb, 256Kb. If you are not sure, try each size until you get the correct one

5. To indicate the offset and the size of the device, measured in sectors (each sector is 512 bytes), in the Disk Area to Use in RAID (Sectors) area, type the values in the Device offset and Size fields. In most cases, the default values are acceptable. Some RAID controllers use only part of the disk surface. For example HighPoint 370 uses the first 100 sectors on the first drive for its own system information. In this case you would specify the offset as 100 sectors

6. Click OK to start Virtual Disk Array reassembly process

7. In the Local System Devices list, a new Virtual Disk Array device node appears. You may treat this new node and its contents the same way that you treat other device nodes in the list.

You may follow the standard steps to scan the Virtual Disk Array node, then search for files and folders to be recovered. You may also create a Disk Image of the whole Virtual Disk Array to work with it later on.

Note

When dealing with Span Arrays, you may get the size of a Damaged Disk a couple of ways:

- Go to the hard drive manufacturer's web site and look for the model.
- Look for the device geometry label on the top of the physical drive. If you find it (it is not always there) you can multiply the parameters C*H*S (Cylinders * Heads *Sectors per Track) to get the number of sectors. For example, Samsung SW0212A has the following: CYL 4092, HD 16, SEC 63, 2.1GB. Multiply 4,092*16*63 to get 4,124,736 sectors. To calculate the disk size, multiply 4,124,736*512 = 2,111,864,832bytes = 2.1GB. We just confirmed the size 2.1GB. The size is marked on drive label and that proves that our calculations are correct.

Important

When dealing with RAID5 Arrays, if the most frequently used Left Asynchronous type does not work for you, you may try some several different types of building array:

- Left Asynchronous (the most frequently used in hardware RAIDs)
- Left Synchronous (used in the most software RAIDs, based on LDM)
- Right Synchronous
- Right Asynchronous

You may consult your RAID controller manufacturer to determine the proper RAID5 type being used in hardware.

13. Create and Work with a Disk Image

A Disk Image is a mirror copy of your entire logical drive or physical device stored as set of files. It may be a good idea to create a Disk Image for a drive, if you have enough space on another drive.

You might ask, "Why should I create a Disk Image on a drive that holds my data?"

Here is the answer: If you do something wrong while attempting to recover the partition, you will be able to recover files and folders from the Disk Image that you have wisely created.

Disk Image (Active@ Image format) consists of configuration file (with an extension .DIM) and set of file chunks having extensions .000, .001, .002 ... By default Active@ UNERASER tries to create one file (chunk) for the whole volume/device, however, in case if target location is FAT/FAT32, it may not be possible due to file system limitations. In this particular case disk image split to several chunks and each file has a size of 2Gb. Chunks content can be RAW or RAW-Compressed, depending on settings.

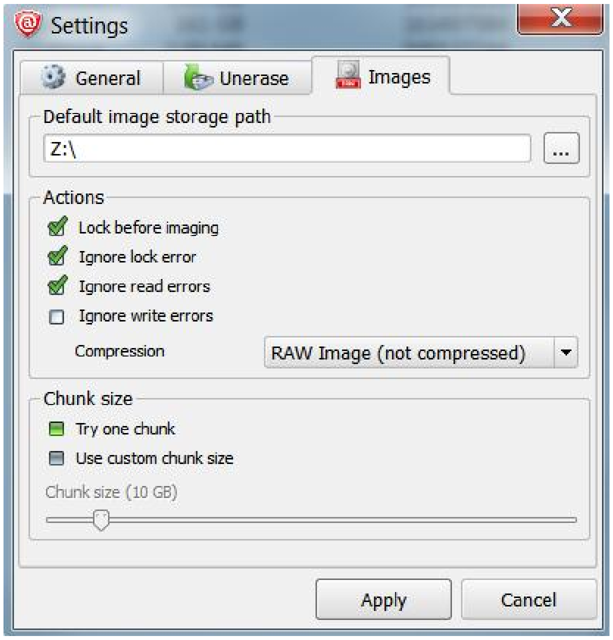
To create a Disk Image:

1. Start Active@ UNERASER and select a drive or physical device that you want to create an image for
2. To open the Create Disk Image dialog box, do one of the following:
   - Select the item and click Create Image menu item from File menu or press Ctrl+I key combination
   - Right-click the selected item, and choose Create Image on the context menu
3. In the Save In drop-down list, select another physical device or to another logical drive
4. Browse to the folder where you want to save the Disk Image
5. To give the Disk Image file a different name, type one in the File Name field
6. Click Save

Watch the progress and wait while drive's contents are copied to the new location. You may cancel the process of image creation anytime by clicking Stop.

Disk image creation default options:

To change a default disk image storage path, compression methods, splitting to chunks and some other options, open Settings, go to Images tab and customize default disk image creation options:



Default image storage path: Z:\

Actions

☑ Lock before imaging

☑ Ignore lock error

☑ Ignore read errors

☐ Ignore write errors

Compression: RAW Image (not compressed)

Chunk size

● Try one chunk

○ Use custom chunk size

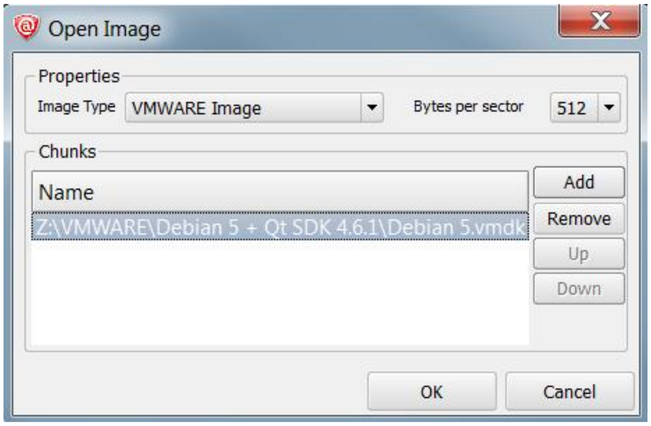
Chunk size (10 GB)

Important

You must always create a Disk Image on a drive other than the source drive. Do not try to save a Disk Image of a drive onto itself.

To open and work with a Disk Image:

1. Start Active@ UNERASER
2. To invoke the Open Image dialog, do one of the following:
   - Press Ctrl+O key combination
   - In the File menu, choose Open Image...
3. Use drop-down list box at bottom to specify disk image type: Active@ Image, Any RAW image, VMWare or VirtualPC Disk image
4. Locate and select disk image file you want to open. Click Open
5. Confirm Disk Image Type, Bytes per Sector and chunks, specified in configuration file:



Open Image

Properties

Image Type: VMWARE Image

Bytes per sector: 512

Chunks

Name
Z:\VMWARE\Debian 5 + Qt SDK 4.6.1\Debian 5.vmdk

6. If there are no configuration file, you can add chunks and change their order manually, using buttons at the right side
7. Click OK to complete configuration and read disk image structures

The opened disk image appears in the Local System Devices list.

You may treat the opened Disk Image node and its content the same way that you treat other device nodes in the list. You may follow the same steps to scan the volume and then search for files and folders to be recovered. Or you can use opened Disk Images as devices for creating RAID Virtual Arrays.

Active@ UNERASER can open:

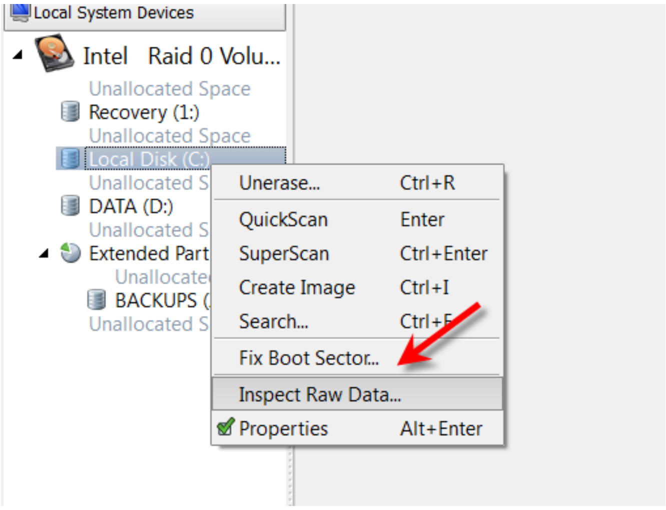
- RAW and RAW-Compressed disk images (Active@ Image format: *.DIM)
- RAW disk images created by third party software (WinHex, etc...)
- Disk Images (RAW format) composed from several chunks
- VMWARE (*.vmdk) and VirtualPC (*.vhd) Disk Images

Note

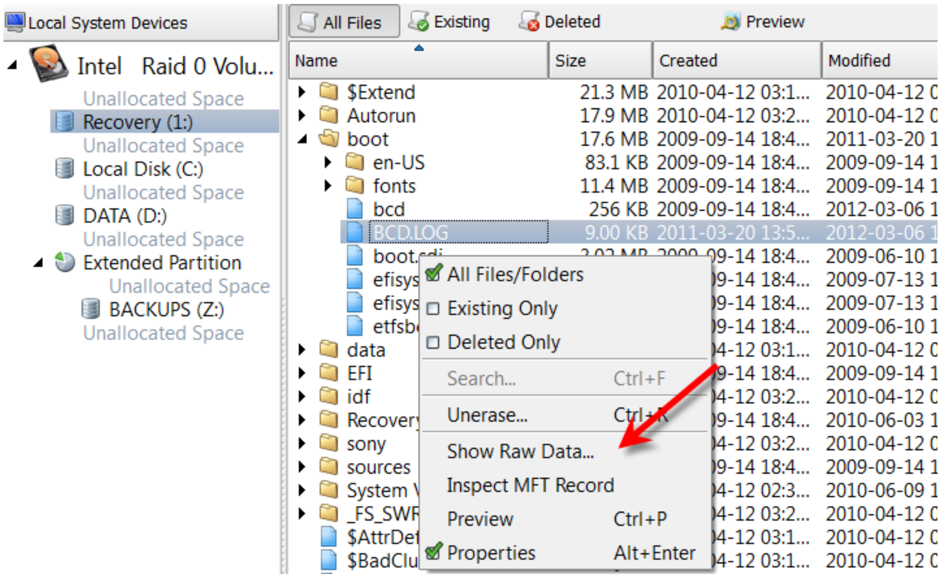
If you've created raw disk image using other third-party utilities (like copying sectors from WinHex) you are still able to open it! Just choose Any Raw Image disk image type in the Open File standard dialog and you will see all files on the disk. Select the required one.

14. Inspect disk data with integrated Disk Editor

Advanced users and IT professionals may require inspecting raw disk structures before actual recovery occurs - to evaluate damage to the data and recovery chances. For these purposes Disk Editor (Hex Viewer) supplied as a separate application and is accessible from recovery panel. Launch it from the context menu for the object to be inspected (hard disk, volume, file data):



For FAT/FAT32 & NTFS volumes inspection of headers of file records is available, for example Disk Editor is launched and "NTFS MFT file record" template is applied for binary data automatically:

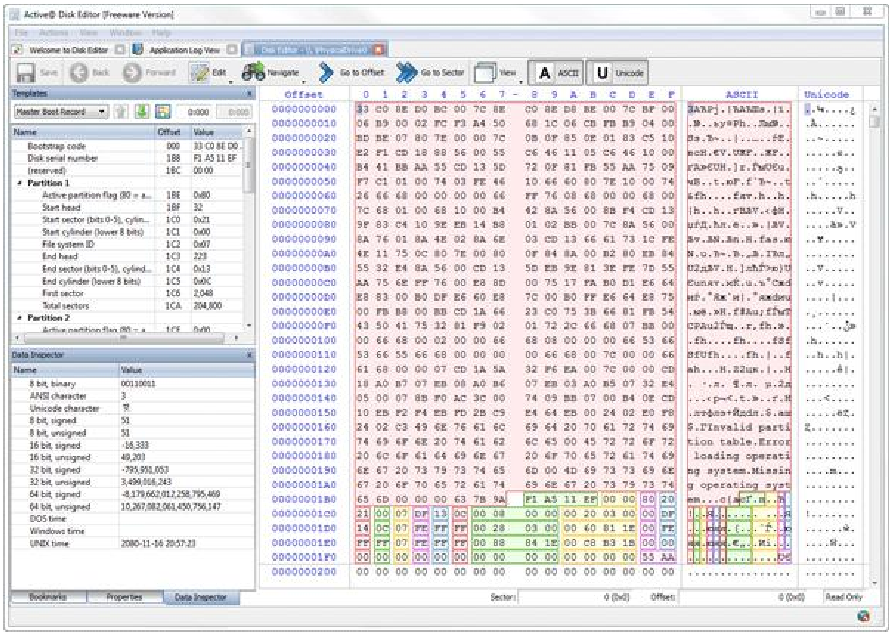


Name	Size	Created	Modified
$Extend	21.3 MB	2010-04-12 03:1...	2010-04-12 0
Autorun	17.9 MB	2010-04-12 03:2...	2010-04-12 0
boot	17.6 MB	2009-09-14 18:4...	2011-03-20 1
en-US	83.1 KB	2009-09-14 18:4...	2009-09-14 1
fonts	11.4 MB	2009-09-14 18:4...	2009-09-14 1
bcd	256 KB	2009-09-14 18:4...	2012-03-06 1
BCD.LOG	9.00 KB	2011-03-20 13:5...	2012-03-06 1
boot.sdi	3.02 MB	2009-09-14 18:4...	2009-06-10 1
efisys		09-14 18:4...	2009-07-13 1
efisys		09-14 18:4...	2009-07-13 1
etfsb		09-14 18:4...	2009-06-10 1
data		04-12 03:1...	2010-04-12 0
EFI		09-14 18:4...	2009-09-14 1
idf		04-12 03:2...	2010-04-12 0
Recovery		09-14 18:4...	2010-06-03 1
sony		04-12 03:2...	2010-04-12 0
sources		09-14 18:4...	2009-09-14 1
System V		04-12 02:3...	2010-06-09 1
_FS_SWR		04-12 03:2...	2010-04-12 0
$AttrDef		04-12 03:1...	2010-04-12 0
$BadClu		04-12 03:1...	2010-04-12 0

Active@ Disk Editor basics

Active@ Disk Editor uses a simple, low-level disk viewer which displays information in binary and text modes at the same time. You can use this view to analyze the contents of data storage structure elements such as:

- Hard disk drives
- SSD & USB Disks
- Partitions & Volumes
- Files



Name	Offset	Value
Bootstrap code	000	33 C0 8E D0 ...
Disk serial number	1B8	F1 A5 11 EF
(reserved)	1BC	00 00
Partition 1		
Active partition flag (80 = a...	1BE	0x80
Start head	1BF	32
Start sector (bits 0-5), cylin...	1C0	0x21
Start cylinder (lower 8 bits)	1C1	0x00
File system ID	1C2	0x07
End head	1C3	223
End sector (bits 0-5), cylind...	1C4	0x13
End cylinder (lower 8 bits)	1C5	0x0C
First sector	1C6	2,048
Total sectors	1CA	204,800
Partition 2		
Active partition flag (80 = a	1CE	0x00

Name	Value
8 bit, binary	00110011
ANSI character	3
Unicode character	쌳
8 bit, signed	51
8 bit, unsigned	51
16 bit, signed	-16,333
16 bit, unsigned	49,203
32 bit, signed	-795,951,053
32 bit, unsigned	3,499,016,243
64 bit, signed	-8,179,662,012,258,795,469
64 bit, unsigned	10,267,082,061,450,756,147
DOS time	
Windows time	
UNIX time	2080-11-16 20:57:23

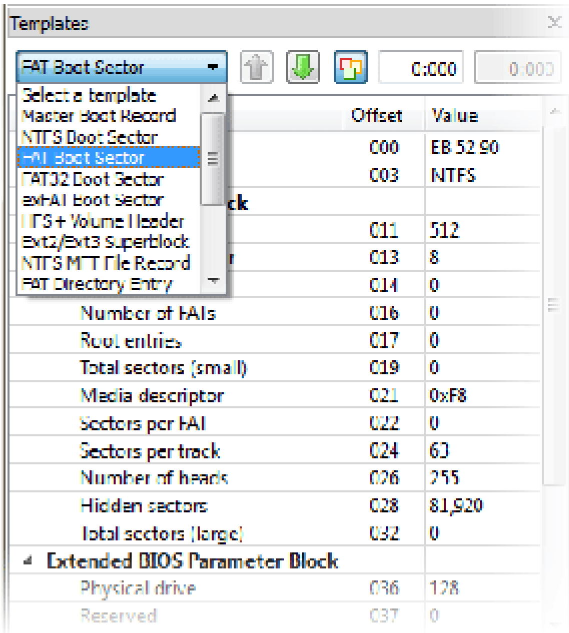
```
  Offset      0  1  2  3  4  5  6  7 -  8  9  A  B  C  D  E  F
0000000000   33 C0 8E D0 BC 00 7C 8E   C0 8E D8 BE 00 7C BF 00
0000000010   06 B9 00 02 FC F3 A4 50   68 1C 06 CB FB B9 04 00
0000000020   BD BE 07 80 7E 00 00 7C   0B 0F 85 0E 01 83 C5 10
0000000030   E2 F1 CD 18 88 56 00 55   C6 46 11 05 C6 46 10 00
0000000040   B4 41 BB AA 55 CD 13 5D   72 0F 81 FB 55 AA 75 09
0000000050   F7 C1 01 00 74 03 FE 46   10 66 60 80 7E 10 00 74
0000000060   26 66 68 00 00 00 00 66   FF 76 08 68 00 00 68 00
0000000070   7C 68 01 00 68 10 00 B4   42 8A 56 00 8B F4 CD 13
0000000080   9F 83 C4 10 9E EB 14 B8   01 02 BB 00 7C 8A 56 00
0000000090   8A 76 01 8A 4E 02 8A 6E   03 CD 13 66 61 73 1C FE
00000000A0   4E 11 75 0C 80 7E 00 80   0F 84 8A 00 B2 80 EB 84
00000000B0   55 32 E4 8A 56 00 CD 13   5D EB 9E 81 3E FE 7D 55
00000000C0   AA 75 6E FF 76 00 E8 8D   00 75 17 FA B0 D1 E6 64
00000000D0   E8 83 00 B0 DF E6 60 E8   7C 00 B0 FF E6 64 E8 75
00000000E0   00 FB B8 00 BB CD 1A 66   23 C0 75 3B 66 81 FB 54
00000000F0   43 50 41 75 32 81 F9 02   01 72 2C 66 68 07 BB 00
0000000100   00 66 68 00 02 00 00 66   68 08 00 00 00 66 53 66
0000000110   53 66 55 66 68 00 00 00   00 66 68 00 7C 00 00 66
0000000120   61 68 00 00 07 CD 1A 5A   32 F6 EA 00 7C 00 00 CD
0000000130   18 A0 B7 07 EB 08 A0 B6   07 EB 03 A0 B5 07 32 E4
0000000140   05 00 07 8B F0 AC 3C 00   74 09 BB 07 00 B4 0E CD
0000000150   10 EB F2 F4 EB FD 2B C9   E4 64 EB 00 24 02 E0 F8
0000000160   24 02 C3 49 6E 76 61 6C   69 64 20 70 61 72 74 69
0000000170   74 69 6F 6E 20 74 61 62   6C 65 00 45 72 72 6F 72
0000000180   20 6C 6F 61 64 69 6E 67   20 6F 70 65 72 61 74 69
0000000190   6E 67 20 73 79 73 74 65   6D 00 4D 69 73 73 69 6E
00000001A0   67 20 6F 70 65 72 61 74   69 6E 67 20 73 79 73 74
00000001B0   65 6D 00 00 00 63 7B 9A   F1 A5 11 EF 00 00 80 20
00000001C0   21 00 07 DF 13 0C 00 08   00 00 00 20 03 00 00 DF
00000001D0   14 0C 07 FE FF FF 00 28   03 00 00 60 81 1E 00 FE
00000001E0   FF FF 07 FE FF FF 00 88   84 1E 00 C8 B3 18 00 00
00000001F0   00 00 00 00 00 00 00 00   00 00 00 00 00 00 55 AA
0000000200   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
```

The Main Features:

- Enhanced template view
- Detailed MFT record information
- Side-by-side Compare and Edit
- Fields coloring with data in tooltips
- Extensive exFAT support
- Fast navigation points
- Filling selection with a pattern
- Unicode support
- Quick Disk Info
- Bookmarks
- Data Inspector

Enhanced template view

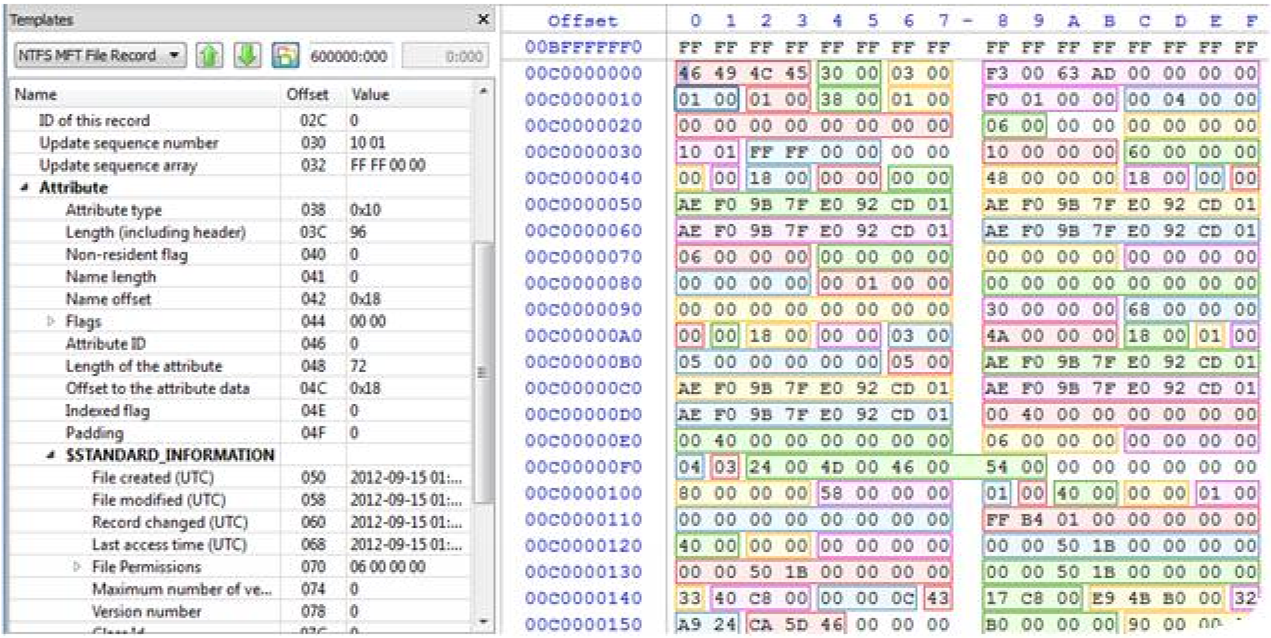
Template view shows parsed records of the most important areas on disk, allowing easily interpretation and editing. When you navigate to a point of interest, a proper template is selected automatically. The following templates are supported: MBR, NTFS boot sector, FAT boot sector, FAT32 boot sector, exFAT boot sector, HFS+ Volume header, Ext2/Ext3 superblock, NTFS MFT file record, FAT directory entry, exFAT directory entry, LDM structures. As you edit data in Hex, ASCII or Unicode pane or in Templates window, modified data is fully synchronized between views. After each modification a template view is recalculated giving you an up-to-date interpretation of data.



	Offset	Value
	C00	EB 52 90
	C03	NTFS
ck		
	C11	512
	C13	8
	C14	0
Number of FATs	C16	0
Root entries	C17	0
Total sectors (small)	C19	0
Media descriptor	C21	0xF8
Sectors per FAT	C22	0
Sectors per track	C24	63
Number of heads	C26	255
Hidden sectors	C28	81,920
Total sectors (large)	C32	0
Extended BIOS Parameter Block		
Physical drive	C36	128
Reserved	C37	0

Detailed MFT record information

MFT file record template shows data in great detalization level using multiple levels. You can examine a standard header, all attributes and attribute data of the record. The attributes interpreted are: $STANDARD_INFORMATION, $ATTRIBUTE_LIST, $FILE_NAME, $OBJECT_ID, $SECURITY_DESCRIPTOR, $VOLUME_NAME, $VOLUME_INFORMATION, $DATA, $INDEX_ROOT, $INDEX_ALLOCATION, $BITMAP, $REPARSE_POINT, $EA_INFORMATION, $EA, $LOGGED_UTILITY_STREAM.

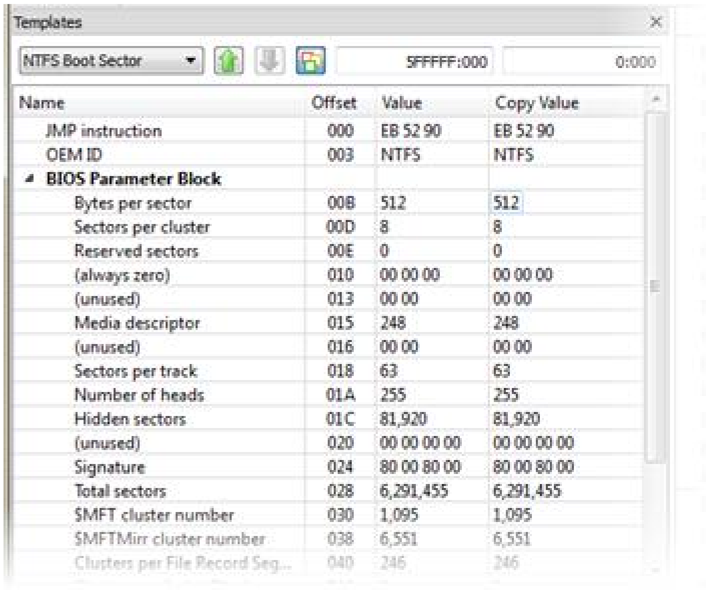


Name	Offset	Value
ID of this record	02C	0
Update sequence number	030	10 01
Update sequence array	032	FF FF 00 00
Attribute		
Attribute type	038	0x10
Length (including header)	03C	96
Non-resident flag	040	0
Name length	041	0
Name offset	042	0x18
Flags	044	00 00
Attribute ID	046	0
Length of the attribute	048	72
Offset to the attribute data	04C	0x18
Indexed flag	04E	0
Padding	04F	0
$STANDARD_INFORMATION		
File created (UTC)	050	2012-09-15 01:...
File modified (UTC)	058	2012-09-15 01:...
Record changed (UTC)	060	2012-09-15 01:...
Last access time (UTC)	068	2012-09-15 01:...
File Permissions	070	06 00 00 00
Maximum number of ve...	074	0
Version number	078	0

```
  Offset      0  1  2  3  4  5  6  7 -  8  9  A  B  C  D  E  F
00BFFFFFF0   FF FF FF FF FF FF FF FF   FF FF FF FF FF FF FF FF
00C0000000   46 49 4C 45 30 00 03 00   F3 00 63 AD 00 00 00 00
00C0000010   01 00 01 00 38 00 01 00   F0 01 00 00 00 04 00 00
00C0000020   00 00 00 00 00 00 00 00   06 00 00 00 00 00 00 00
00C0000030   10 01 FF FF 00 00 00 00   10 00 00 00 60 00 00 00
00C0000040   00 00 18 00 00 00 00 00   48 00 00 00 18 00 00 00
00C0000050   AE F0 9B 7F E0 92 CD 01   AE F0 9B 7F E0 92 CD 01
00C0000060   AE F0 9B 7F E0 92 CD 01   AE F0 9B 7F E0 92 CD 01
00C0000070   06 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00C0000080   00 00 00 00 00 01 00 00   00 00 00 00 00 00 00 00
00C0000090   00 00 00 00 00 00 00 00   30 00 00 00 68 00 00 00
00C00000A0   00 00 18 00 00 00 03 00   4A 00 00 00 18 00 01 00
00C00000B0   05 00 00 00 00 00 05 00   AE F0 9B 7F E0 92 CD 01
00C00000C0   AE F0 9B 7F E0 92 CD 01   AE F0 9B 7F E0 92 CD 01
00C00000D0   AE F0 9B 7F E0 92 CD 01   00 40 00 00 00 00 00 00
00C00000E0   00 40 00 00 00 00 00 00   06 00 00 00 00 00 00 00
00C00000F0   04 03 24 00 4D 00 46 00   54 00 00 00 00 00 00 00
00C0000100   80 00 00 00 58 00 00 00   01 00 40 00 00 00 01 00
00C0000110   00 00 00 00 00 00 00 00   FF B4 01 00 00 00 00 00
00C0000120   40 00 00 00 00 00 00 00   00 00 50 1B 00 00 00 00
00C0000130   00 00 50 1B 00 00 00 00   00 00 50 1B 00 00 00 00
00C0000140   33 40 C8 00 00 00 0C 43   17 C8 00 E9 4B B0 00 32
00C0000150   A9 24 CA 5D 46 00 00 00   B0 00 00 00 90 00 00
```

Side-by-side Compare and Edit

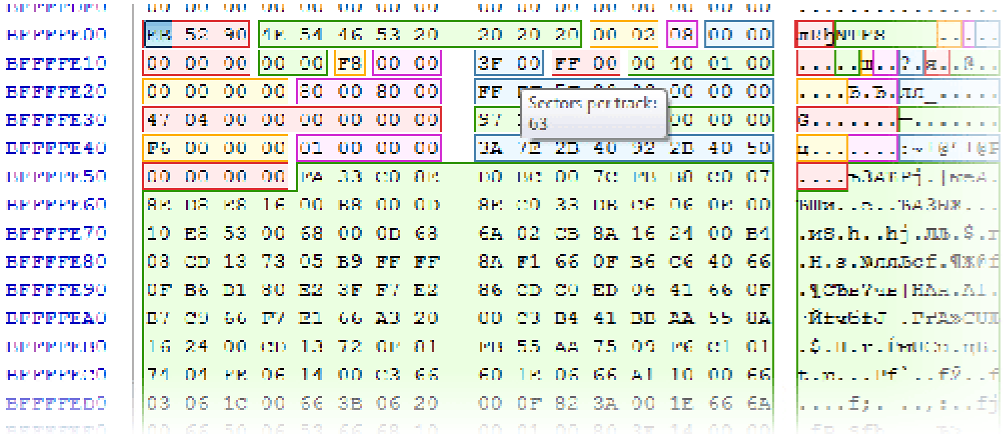
Some records like boot sectors have their copies. Templates view automatically detects records supporting copies and shows both main and copy values allowing to compare them. You can arbitrary set an offset of main record and its copy.



Name	Offset	Value	Copy Value
JMP instruction	000	EB 52 90	EB 52 90
OEM ID	003	NTFS	NTFS
BIOS Parameter Block			
Bytes per sector	00B	512	512
Sectors per cluster	00D	8	8
Reserved sectors	00E	0	0
(always zero)	010	00 00 00	00 00 00
(unused)	013	00 00	00 00
Media descriptor	015	248	248
(unused)	016	00 00	00 00
Sectors per track	018	63	63
Number of heads	01A	255	255
Hidden sectors	01C	81,920	81,920
(unused)	020	00 00 00 00	00 00 00 00
Signature	024	80 00 80 00	80 00 80 00
Total sectors	028	6,291,455	6,291,455
$MFT cluster number	030	1,095	1,095
$MFTMirr cluster number	038	6,551	6,551
Clusters per File Record Seg...	040	246	246

Fields coloring with data in tooltips

Individual template fields are colored in hexadecimal pane giving a quick overview of all data. As you travel along fields in Templates window, the current field is highlighted in Hex pane. Hover mouse over a colored field to get a tooltip with additional information.

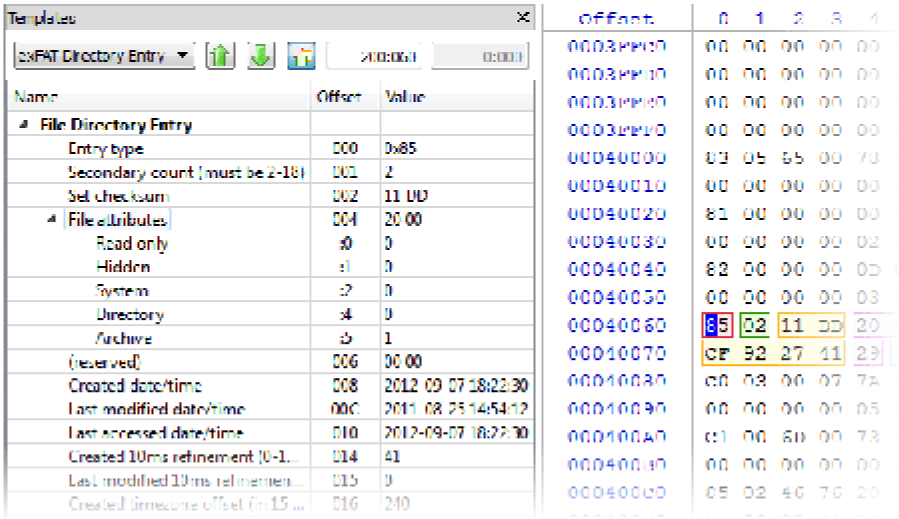


```
BFFFFE00  EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00
BFFFFE10  00 00 00 00 00 F8 00 00  3F 00 FF 00 00 10 01 00
BFFFFE20  00 00 00 00 80 00 80 00  FF FF                00 00 00
BFFFFE30  47 04 00 00 00 00 00 00  97 1                 00 00 00
BFFFFE40  F6 00 00 00 01 00 00 00  3A 72 2D 40 92 2D 40 50
BFFFFE50  00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07
BFFFFE60  8E D8 E8 16 00 B8 00 0D  8E C0 33 DB C6 06 0E 00
BFFFFE70  10 E8 53 00 68 00 0D 68  6A 02 CB 8A 16 24 00 B4
BFFFFE80  08 CD 13 73 05 B9 FF FF  8A F1 66 0F B6 C6 40 66
BFFFFE90  0F B6 D1 80 E2 3F F7 E2  86 CD C0 ED 06 41 66 0F
BFFFFEA0  B7 C9 66 F7 E1 66 A3 20  00 C3 B4 41 BB AA 55 8A
BFFFFEB0  16 24 00 CD 13 72 0F 81  FB 55 AA 75 09 F6 C1 01
BFFFFEC0  74 04 FE 06 14 00 C3 66  60 1E 06 66 A1 10 00 66
BFFFFED0  03 06 1C 00 66 3B 06 20  00 0F 82 3A 00 1E 66 6A
```

Sectors per track:
63

Extensive exFAT support

exFAT boot sector as well as all types of exFAT directory entries are supported giving you a detailed information on different exFAT structures. Move template offset up/down feature allows easily navigate between records.



Templates

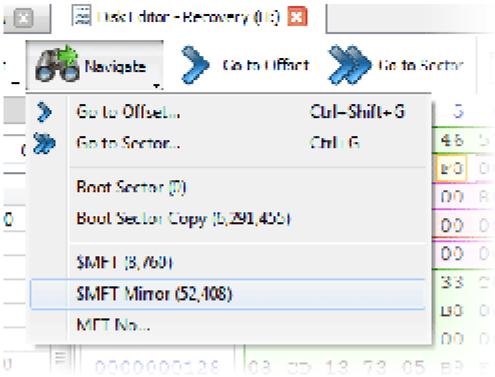
exFAT Directory Entry ▾ | 40000060 | 0:0000

Name	Offset	Value
File Directory Entry		
Entry type	000	0x85
Secondary count (must be 2-18)	001	2
Set checksum	002	11 DD
File attributes	004	20 00
Read only	:0	0
Hidden	:1	0
System	:2	0
Directory	:4	0
Archive	:5	1
(reserved)	006	00 00
Created date/time	008	2012-09-07 18:22:30
Last modified date/time	00C	2011-08-25 14:54:12
Last accessed date/time	010	2012-09-07 18:22:30
Created 10ms refinement (0-1...	014	41
Last modified 10ms refinemen...	015	0
Created timezone offset (in 15 ...	016	240

```
Offset     0  1  2  3  4
0003FFC0  00 00 00 00 00
0003FFD0  00 00 00 00 00
0003FFE0  00 00 00 00 00
0003FFF0  00 00 00 00 00
00040000  83 05 65 00 70
00040010  00 00 00 00 00
00040020  81 00 00 00 00
00040030  00 00 00 00 02
00040040  82 00 00 00 0D
00040050  00 00 00 00 03
00040060  85 02 11 DD 20
00040070  CF 92 27 41 23
00040080  C0 03 00 07 7A
00040090  00 00 00 00 05
000400A0  C1 00 60 00 73
000400B0  00 00 00 00 00
000400C0  05 02 40 76 20
```

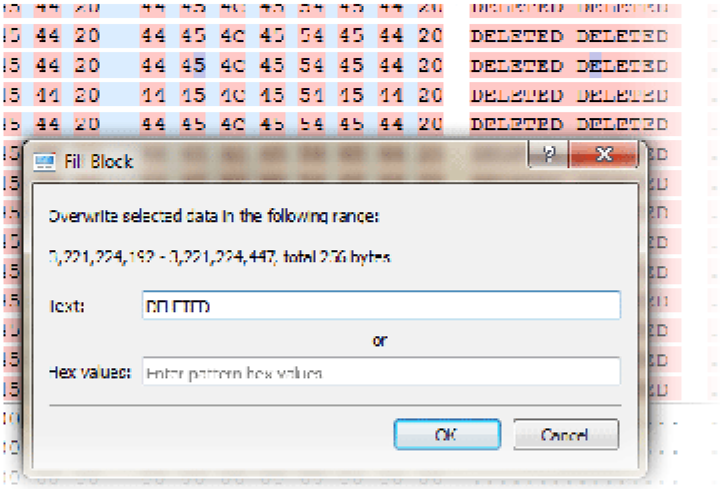
Fast navigation points

You don't need to guess what is the sector of root directory on FAT volume is or where is $MFT record on NTFS partition located. Simply use fast navigation points set up in the menu. When Disk Editor opens an object, the most important areas are detected and automatically added to the list. They include boot sectors, FAT tables, root directory, $MFT and $MFT Mirror and others.



Filling selection with a pattern

It might be handy to fill an area on the disk with particular data. Besides simply zeroing an area by providing 00 as hexadecimal value you can specify any hexadecimal or text pattern for better flexibility.



Fill Block

Overwrite selected data in the following range:

3,221,224,192 - 3,221,224,447, total 256 bytes

Text: DELETED

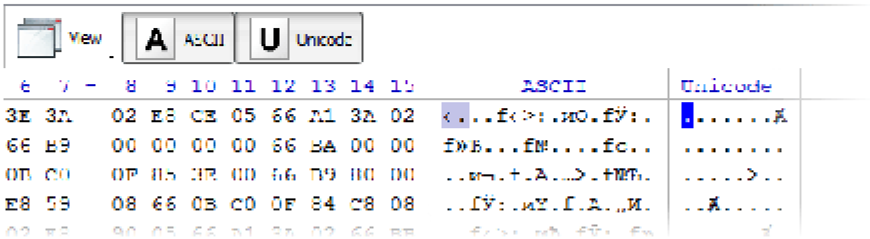
or

Hex values: Enter pattern hex values

```
45 44 20  44 45 4C 45 54 45 44 20  DELETED DELETED
45 44 20  44 45 4C 45 54 45 44 20  DELETED DELETED
45 44 20  44 45 4C 45 54 45 44 20  DELETED DELETED
45 44 20  44 45 4C 45 54 45 44 20  DELETED DELETED
```

Unicode support

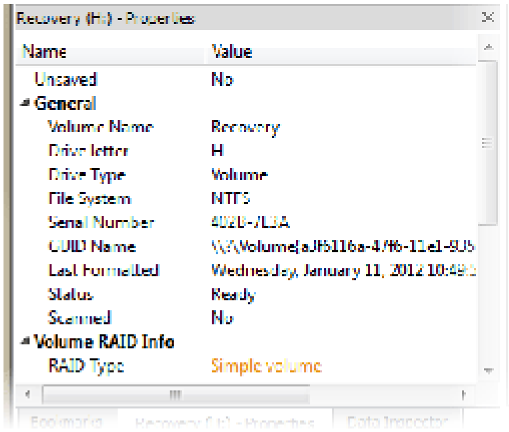
Work with hexadecimal, ASCII or Unicode representation of data. Editing data in Unicode pane allows to enter extended characters directly while ASCII and Hexadecimal panes gives you control over individual bytes.



```
 6  7 -  8  9 10 11 12 13 14 15         ASCII          Unicode
3E 3A   02 E8 CE 05 66 A1 3A 02   <...f<>:.MO.fЎ:.    ........Ä
66 B9   00 00 00 00 66 BA 00 00   f¹Б...fM....fc..    ........
0B C0   0F 85 3E 00 66 D9 00 00   ..Ђ¬.+.A...>.fЩЂ.   ......>..
E8 59   08 66 0B C0 0F 84 C8 08   ..ГЎ:.MY.Г.A..„И.   ..Ä.....
```

Quick Disk Info

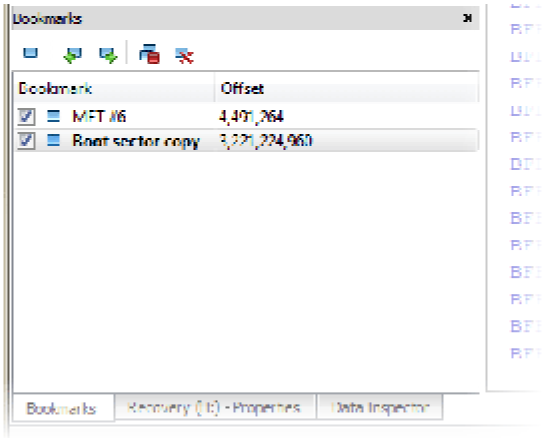
Properties window gives a concise overview of disk or partition opened in Disk Editor. If unwanted this information can be hidden to save screen space.


Recovery (H:) - Properties

Name	Value
Unsaved	No
General	
Volume Name	Recovery
Drive letter	H
Drive Type	Volume
File System	NTFS
Serial Number	402B-7E3A
GUID Name	\\?\Volume{a0f6116a-4746-11e1-905
Last Formatted	Wednesday, January 11, 2012 10:49:2
Status	Ready
Scanned	No
Volume RAID Info	
RAID Type	Simple volume

Bookmarks

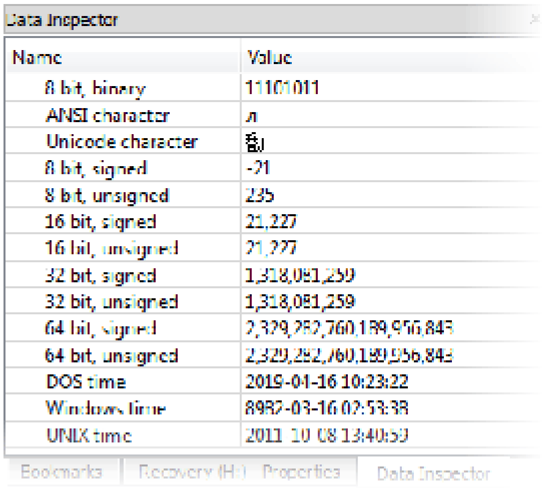
When analyzing large amounts of data don't get lost when navigating between different points. Easily bookmark locations by keyboard shortcuts and cycle through them. If you need even more flexibility, you can give any bookmark a name and navigate between them using a bookmark window.


Bookmarks

Bookmark	Offset
☑ MFT #6	4,401,264
☑ Boot sector copy	3,221,224,960

Data Inspector

As you move a cursor along, data under cursor is automatically interpreted and shown in Data Inspector in different formats. You can see them as one to four byte numbers as well as time and other useful structures.



Name	Value
8 bit, binary	11101011
ANSI character	л
Unicode character	勫
8 bit, signed	-21
8 bit, unsigned	235
16 bit, signed	21,227
16 bit, unsigned	21,227
32 bit, signed	1,318,081,259
32 bit, unsigned	1,318,081,259
64 bit, signed	2,329,282,760,189,956,843
64 bit, unsigned	2,329,282,760,189,956,843
DOS time	2019-04-16 10:23:22
Windows time	8982-03-16 02:53:38
UNIX time	2011-10-08 13:40:59

15. Activate Software with a Registration Key

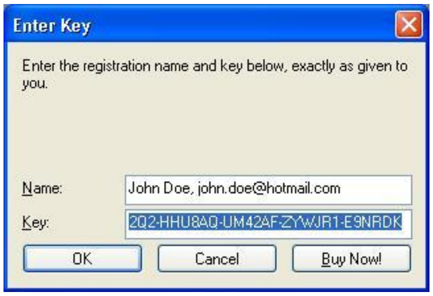
After you have downloaded the FREE version - that can detect deleted partitions and files is able to recover the only one file per session - to get full functionality, you need to activate it with a registration key.

To activate the FREE version, you do not need to re-install software. You do not have to re-scan hard drives to detect deleted partitions and files. All you have to do is to enter the registration key and continue working with the software registered in your name. You may purchase a registration key from our web site or from many third-party re-sellers.

When typing the Name information, be careful to spell the name and e-mail exactly the way you specified them while purchasing the registration key. Any variation will cause product activation and registration to fail.

You can activate and register FREE software in one of two ways:

1. In the main window, from the Help menu, choose Enter Registration Key... The Enter Key dialog box appears.



Enter the registration name and key below, exactly as given to you.

Name: John Doe, john.doe@hotmail.com

Key: 2Q2-HHU8AQ-UM42AF-ZYWJR1-E9NRDK

a. If you have not purchased your registration key yet, click Buy Now! to go to our web site and purchase it online.

b. In the Name field, type your Name for a Personal License or type your company name for a Corporate License.

c. In the Key field, type your registration key, or you may copy your registration key and paste it in this field.

d. Click OK.

2. If you are using the FREE version, it can detect deleted partitions and files. You can inspect and verify its content. If you try to recover a partition or more than one file per session, the FREE version limitation dialog box appears.

   a. If you have not purchased your registration key yet, click Buy Online to go to our web site and purchase it online.

   b. If you have purchased your registration key, click Enter Key. The Enter Key dialog box appears. Follow instructions in number 1, above.

After you have activated and registered the product successfully, you may continue with recovery of the partition and files being detected previously.

16. Glossary of Terms

boot record

- See boot sector.

boot sector

- The boot sector continues the process of loading the operating system into computer memory. It can be either the MBR (see MBR, below) or the partition boot sector (see partition boot sector, below).

cluster

- A group of disk sectors that contain file data. It is the smallest allocation unit for storing a file. For example, if the file size is 100 bytes and the cluster size is 4096 bytes, the file system reserves one cluster, or 4096 bytes for file data.

data striping

- Spreading blocks of data from files across multiple disk drives. Quicker read and write performance is a result.

device node

- In the Local System Devices list, a physical device containing logical drives.

disk mirroring

- Identical data is written to two disks simultaneously. Used when access to data at all times is critical.

FAT

- File Allocation Table. An area that contains the records of every other file data and directory in a FAT-formatted hard disk drive. The operating system needs this information to access the files and define the data cluster's chain. There are FAT32, FAT16 and FAT versions.

file

- A collection of data with a file name and file attributes, like size.. Almost all information stored in a computer must be in a file.

folder

- An object that can contain a group of files. Folders are used to organize information. In DOS and UNIX, folders are called directories or root areas.

HDD

- Hard disk drive.

log file

- A file that lists all events that have occurred. For example, Active@ File Recovery writes a log file entry for every request made to the program and every event that happens as a result. You can see the log at the bottom of the main screen.

logical drive

- A partition is a logical drive because it does not affect the physical hard disk other than the defined space that it occupies, yet it behaves like a separate disk drive.

MBR

- The Master Boot Record (MBR) is a small program that is executed when the computer is first turned on. Typically, the MBR can be found on the first sector of a disk. The MBR first reads the disk's partition table to determine which partition is used to load the operating system. The MBR then transfers control to this partition's "boot sector" to continue the process. Loading the operating system is called "booting" the computer.

MFT

- Master File Table. A file that contains the records of every other file and directory in an NTFS-formatted hard disk drive. The operating system needs this information to access the files.

Named Streams

- NTFS supports multiple data streams where the stream name identifies a new data attribute on the file. A handle can be opened to each data stream. A data stream, then, is a unique set of file attributes. Streams have separate opportunistic locks, file locks, and sizes, but common permissions.

NTFS

- NT File System. NTFS was created to provide a more reliable operating system, compared to the FAT file system.

partition

- A section of memory or hard disk isolated for a specific purpose. Each partition can behave like a separate disk drive.

partition boot sector

- On NTFS or FAT file systems, the partition boot sector is a small program that is executed when the operating system tries to access a particular partition. On personal computers, the Master Boot Record uses the partition boot sector on the system partition to determine file system type, cluster size, etc. and to load the operating system kernel files. Partition boot sector is the first sector of the partition.

partition status

- SuperScan gives each partition a rating depending on how likely it is to recover data on the partition. Statuses rated from Excellent to Very Bad.

physical device

- A piece of hardware that is attached to your computer by screws or wires. A hard disk drive is a physical device. It is also referred to as a physical drive.

RAID-0

- Provides data striping but no redundancy. This method provides quick performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost.

RAID-1

- Writes identical data to two separate disks. Level 1 provides quick read performance and the same write performance as single disks.

RAID-5

- Provides data striping at the byte level and also stripe error correction information. This results in excellent performance and good fault tolerance. Level 5 is one of the most popular implementations of RAID.

root area (and root folder)

- An object that can contain a group of files in a FAT file system. In other words, a directory or folder. The root folder is the top-level folder that has no parent and can have children. A logical drive can have only one root folder. Its name is usually '.' (dot).

sector

- The smallest unit that can be accessed on a disk. Tracks are concentric circles around the disk and the sectors are segments within each circle.

signature files

- File types are recognized by specific patterns that may serve as a reference for file recovery. When a file header is damaged, the type of file may be determined by examining patterns in the damaged file and comparing these patterns to known file type templates.

span array

- A series of dynamic drives linked together to make one contiguous spanned volume.

templates

- File types are recognized by specific patterns that may serve as a reference for file recovery. When a file header is damaged, the type of file may be determined by examining patterns in the damaged file and comparing these patterns to known file type templates. This same pattern-matching process can be applied to deleted or damaged partitions. Using FAT or NTFS templates, recovery software can assume that a particular sector is a FAT or NTFS boot sector because parts of it match a known pattern.

volume

- A fixed amount of storage on a hard disk. A physical device may contain a number of volumes. It is also possible for a single volume to span a number of physical devices.