SecureData

SecureRecovery for Windows

SecureRecovery for Windows

User Manual

SECURE DATA

TABLE OF CONTENTS

I GENERAL INFORMATION

1.1 Product Overview

SecureRecovery for Windows helps to recover files from logically damaged Windows and Mac OS X volumes.
Examples of logical damages are: deleted files, virus attack, file system corruption, re-formatted or re-partitioned drives.

1.2 Product Features

- SecureRecovery for Windows recovers data from Hard Disk Drives, Solid State Drives, and USB Flash Drives.
- Supported file systems: NTFS, FAT, ExFAT and HFS/HFS+.
- The software has a built-in quick diagnostic system that can determine drives' physical health and show whether it is safe or not to proceed with the recovery.
- The program uses a state of the art recovery engine that makes it one of the most successful and advanced data recovery software in the industry.
- SecureRecovery for Windows has a built-in previewer for most common office files and pictures that works even in Demo mode.

1.3 Product Limitations

SecureRecovery for Windows should not be installed on the same logical volume that is going to be recovered.

The software should not be used to save recovered files on the same logical volume that is going to be recovered.

The program cannot be used on drives with significant physical problems. It is not recommended to run any recovery software under these circumstances as it could worsen the driveâ€™s conditions and lead to the complete data loss.

SecureRecovery for Windows has a built-in diagnostic system that guides a user on whether it is safe to run recovery software.

1.4 System Requirements

SecureRecovery for Windows can be installed on any PC running Windows Server 2003, Server 2008, Server 2012, Windows XP/Vista/7/8/8.1/10.

The program requires local administrator privileges.

The PC running the product should have enough disk space to save restored files.

II INSTALLATION INSTRUCTIONS

ATTENTION: Do NOT install SecureRecovery for Windows on the same logical volume that is going to be recovered.

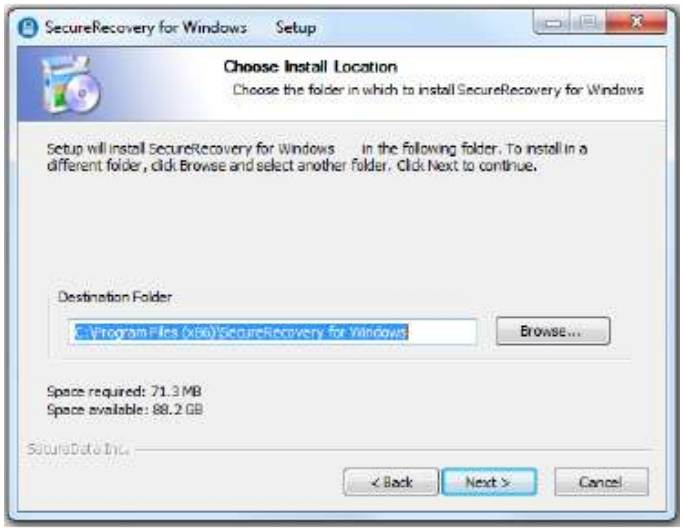
ATTENTION: Do NOT save recovered files on the same logical volume that is going to be recovered.
Neglecting these warning could lead to further data loss. Use another PC if necessary.

1. Run the SecureRecovery for Windows installer. Confirm request for local administrator privileges if necessary. Click the “Next” button on the first screen.

2. Read and accept License Agreement by clicking on the checkbox and then click “Next“.

3. Read the text and click to confirm that you have read and understood the warning. Click the “Next” button.

4. Confirm the installation location and click Next.

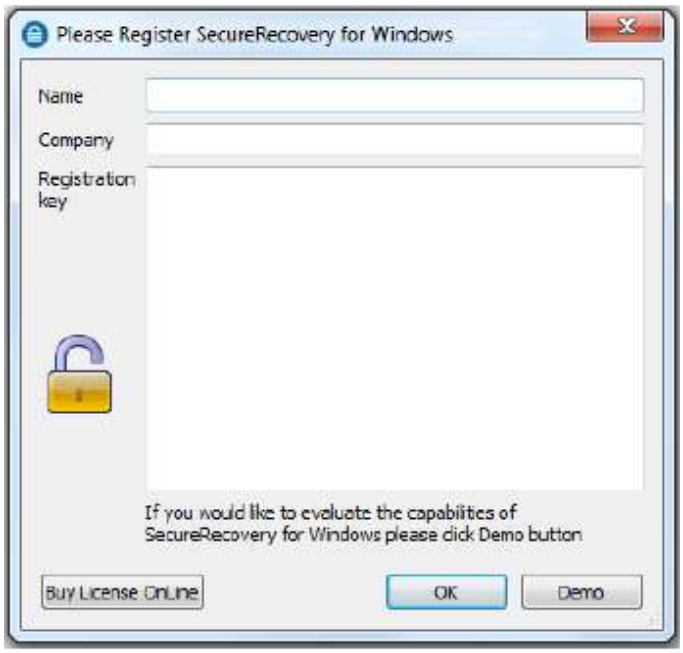


5. Confirm the installation location and click Next.

6. Click the “Finish” button to complete the installation process.

III SOFTWARE ACTIVATION

On the first run SecureRecovery for Windows will ask you to register the program.



You can buy a license and register the program right away, or you can run it in Demo mode unlimited number of times.

Demo mode is fully functional, including a preview of the recovered data. The ability to recover files in Demo mode may have limitations (i.e. the number and size of files that can be recovered). In order to remove limitations user must buy a license.

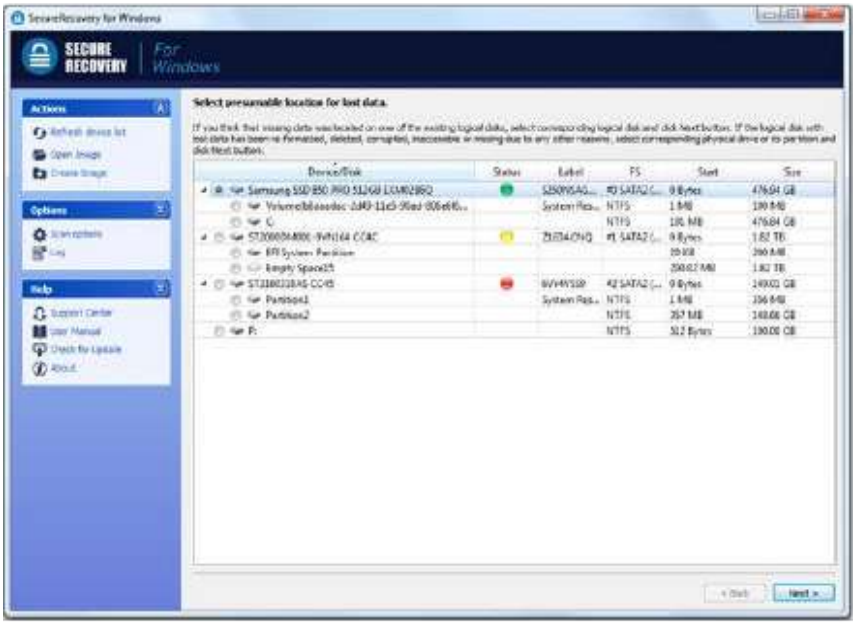
You can always buy a license later after checking the recovery results.

IV DATA RECOVERY PROCESS

4.1 Selecting Media for Recovery

4.1.1 Physical Drives and Volumes

SecureRecovery for Windows works with physical drives or logical volumes that reside on physical drives. The program also shows corresponding Windows device letters for each logical volume available to the system - note “C:” on the picture below.



- “Device/disk” column shows all detected physical drives and all logical volumes (partitions) that are found on physical drives.
- “Status” column shows physical drive “health” status.
- “Label” column contains physical drives serial numbers and logical volume labels/ names.
- “FS” column has physical drives bus interface numbers and detected File System for logical volumes.
- “Start” and “Size” columns contain information about sizes and start positions of all physical drives and logical volumes.

Select a drive or a volume for recovery by clicking on it.

- To recover deleted or lost files, it is recommended to start with selecting the logical volume where the files were located.
- If the drive was re-formatted, it is better to select the physical drive.

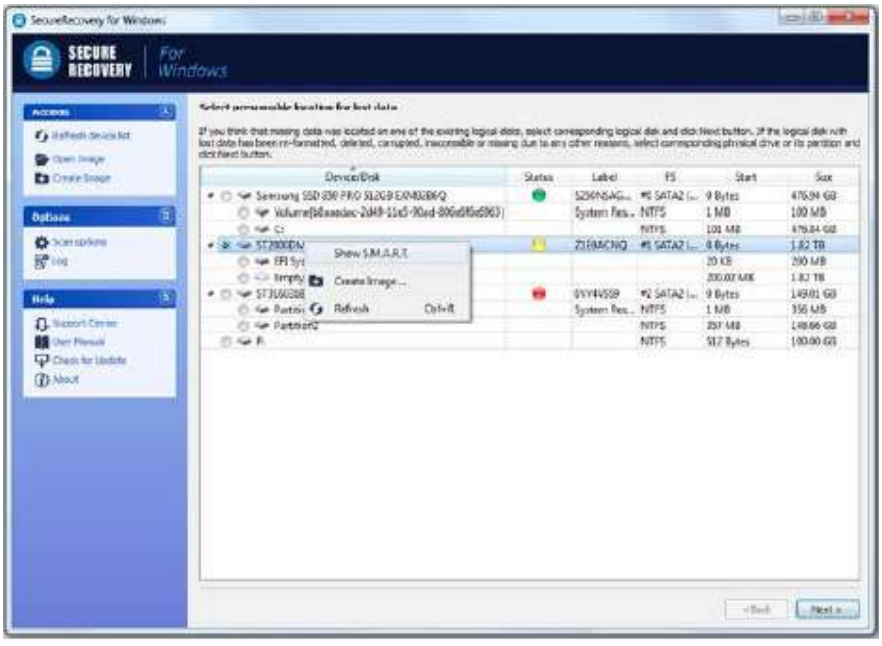
4.1.2 Media Status and S.M.A.R.T.

SecureRecovery for Windows has a built-in quick diagnostic system that can determine drives' physical health and warn if running recovery software is not recommended.

Quick diagnostic is based on physical drive S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology). The results of quick diagnostic are shown in the "Status" field.

Status Green	Represents fully functional physical drive. It is safe to run the program on this drive or any logical volume on this drive.
Status Yellow	Represents degraded physical drive. Run the recovery software with extreme caution. The program has additional diagnostic steps and would stop the process if the drive degrades further during the recovery process.
Status Red	Represents damaged physical drive. It is not safe to run any recovery software on such drive or any logical volume on it. Please send this drive for in-lab recovery by clicking on this link https://www.securedatarecovery.com/request-help

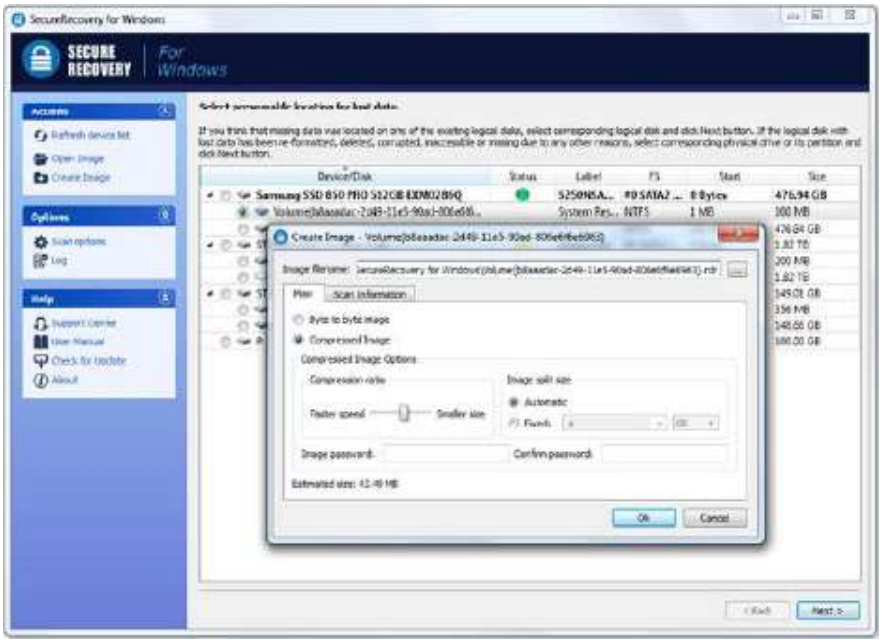
If you'd like to see detailed S.M.A.R.T. report - right click a physical drive and select Show S.M.A.R.T."



4.2 Creating and Using Disk Images

SecureRecovery for Windows allows user to create a binary image of any physical drive or logical volume and can later load that image and work with it as it would be a physical drive or logical volume.

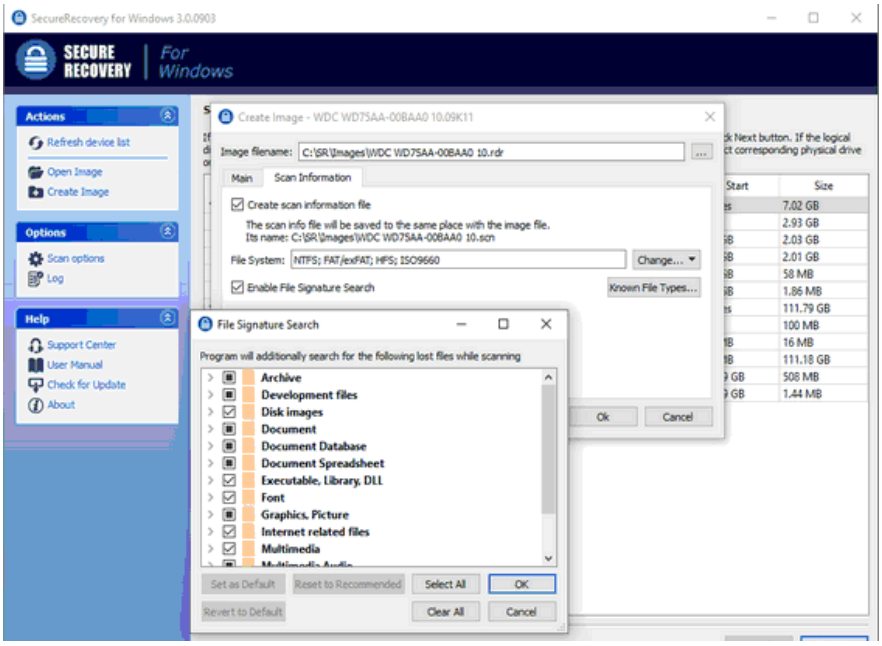
To create an image: click Create Image.



Select where you would like to save the image and click “OK”.

Please note that creating an image requires large amount of storage space - shown in “Estimated size”. Make sure you have enough free space available on your PC.

You may scan the disk while the image is being created.

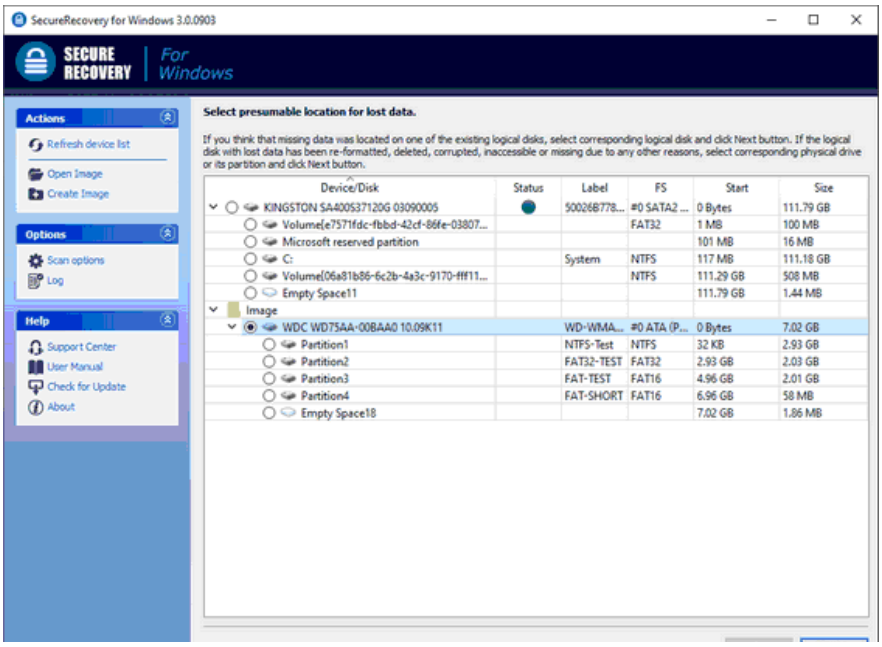


You may also specify file signatures to search for.

ATTENTION: NEVER save an image file on the same logical volume that would be recovered. Neglecting this warning could lead to further data loss.

To load previously created image click Open Image, select the image file and click **Open**.

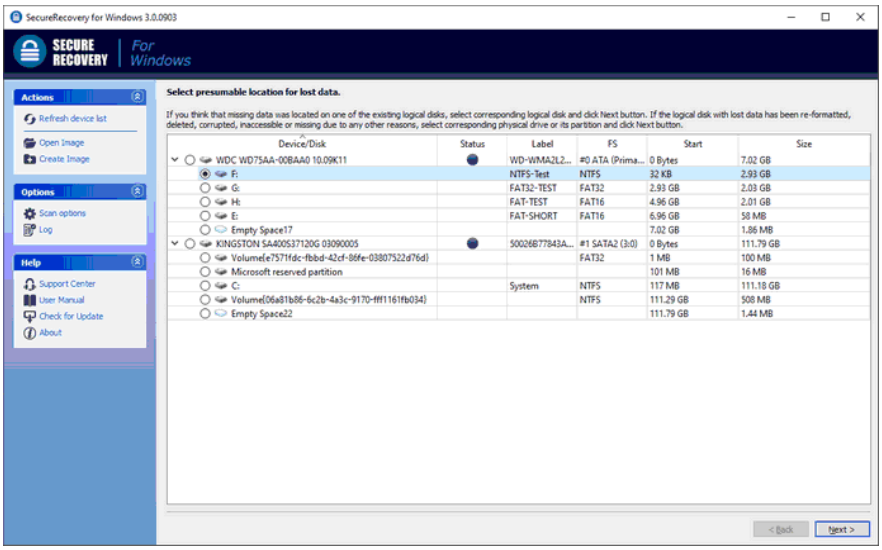
An opened image would look like just another disk or volume.



4.3 Recovering Lost Data from Existing Logical Volumes

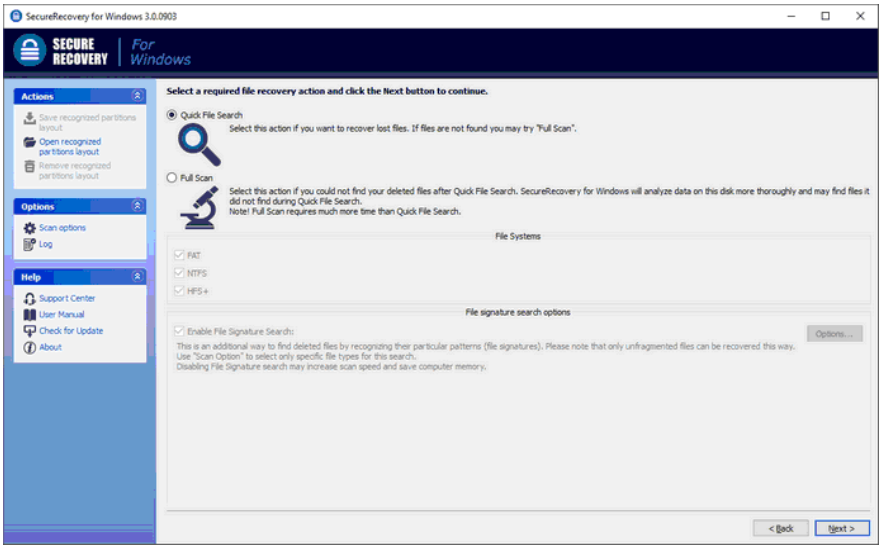
This section describes the recovery process when data loss occurred on the existing volume (i.e. deletion, missing files or corruption to the folder structure).

In this situation the logical volume and file system type will be recognized by SecureRecovery for Windows and the volume will be shown in the Device/Disk column. It may or may not have a logical letter assigned (i.e. C:).



Select the volume and click the Next button.

The Software will present 2 options - Quick File Search or Full Scan.



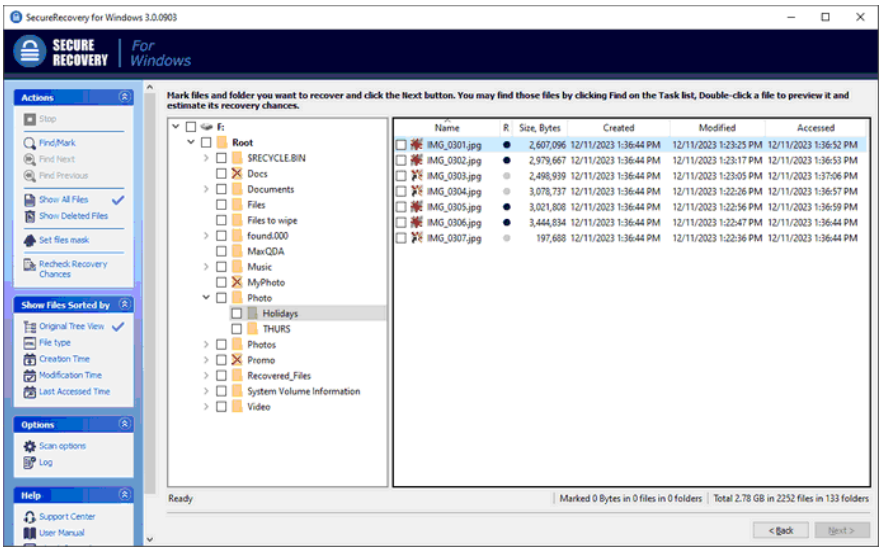
4.3.1 Quick File Search

Quick File Search is the default option and is always recommended for the first attempt. It scans media in certain areas for existing file system data structures. The result is usually quick and sufficient for finding recently deleted, lost, or corrupted files.

To apply Quick File Search option, make sure the appropriate option is selected and click Next.

The software will then run a scan.

Once the scan is completed, the software will move to the next step where all the found files and folders will be presented.



SecureRecovery for Windows shows its estimates of chances for successful file recovery in the Rec column.

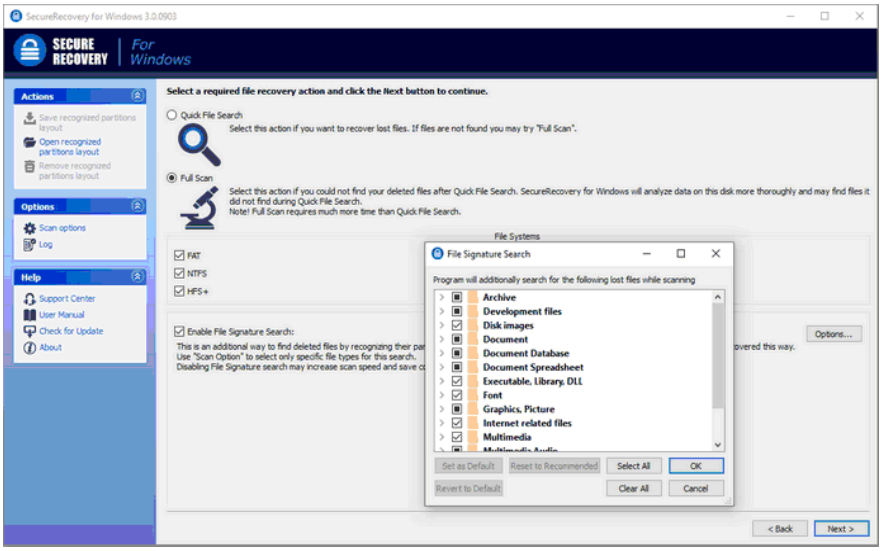
At this step, user can check if the lost data has been found. The files of many common types (like DOC, PDF, JPG and similar) can be opened in preview mode and selected for further recovery (extraction).

Section **Working with Found Data** addresses the details of previewing and recovering found files.

4.3.2 Full Scan

Full Scan is used when the Quick File Search option is unable to find lost data. Full Scan reads and analyses the data through the entire volume, which may take an extended amount of time (multiple hours) depending on the volume size.

This mode allows the software to pick up lost fragments of the existing, older, or overwritten file systems residing on the volume, which might have been missed by Quick File Search algorithm. To enable the Full Scan option, select the corresponding mode, then enable or disable check-boxes for specific file systems expected to exist on the logical volume.



Selecting Full Scan also unlocks the File Signature Search capabilities. This option allows the software to find files with no regards to the existing or missing file system.

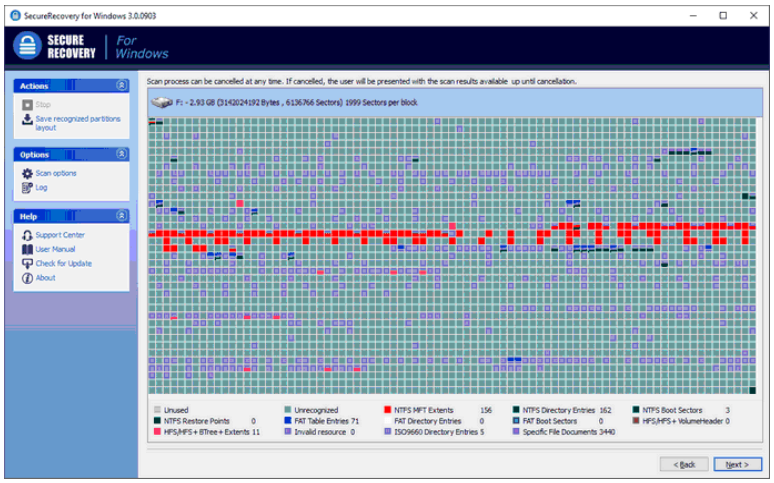
This option has limitations:

1. It does not recover folders structure and original file names;
2. It can only recover first part of fragmented files;
3. It does not recover files of the types unknown to the software.

To enable this option, make sure that Enable File Signature Search checkbox is ON. Specific file types can be selected in the File Signature Search dialog by clicking the Options button.

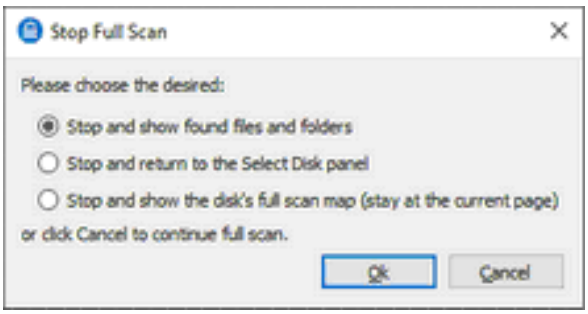
Once the selections for File Types and File Systems are done, click the Next button, and

the software will advance to the scan.



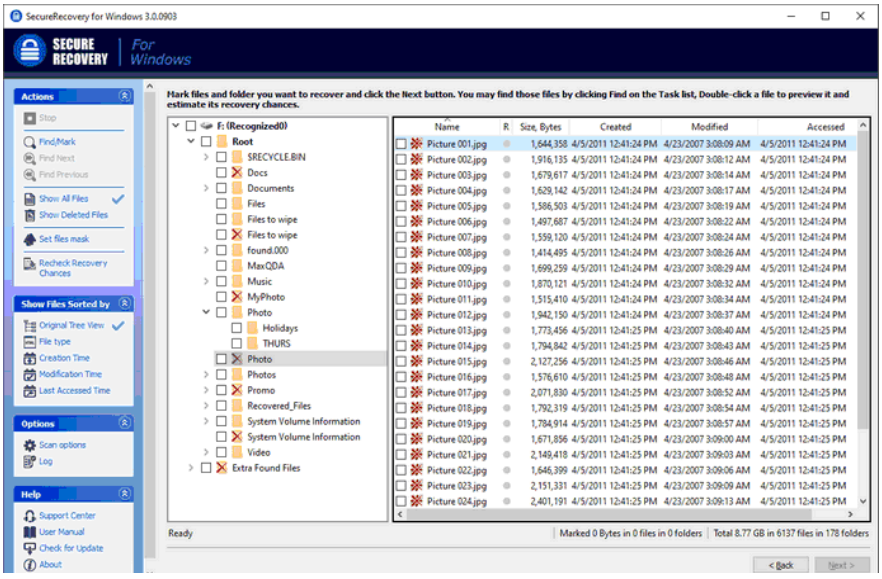
Scan process can be interrupted at any time by pressing the Stop button. From there, user will have options to show found data, return to the previous step, remain on the current step or continue scanning.

Once the scan is finished or interrupted with the option to show found data, the software will advance to the next step and the results of the scan will be shown. At this point user



will be able to search, select, and recover found files.

You may save and load scan information.

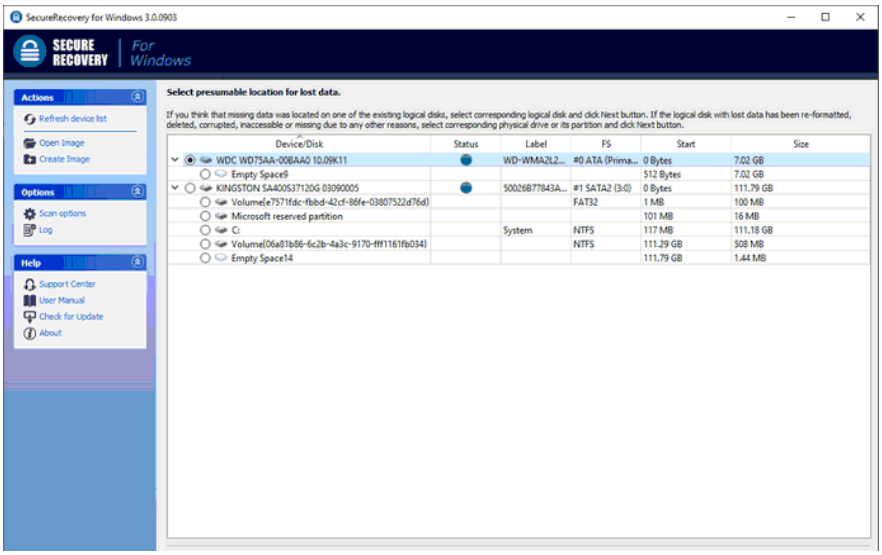


Section **Working with Found Data** addresses the details of previewing and recovering found files.

4.4 Recovering Lost Files from Deleted/Corrupted Logical Volumes

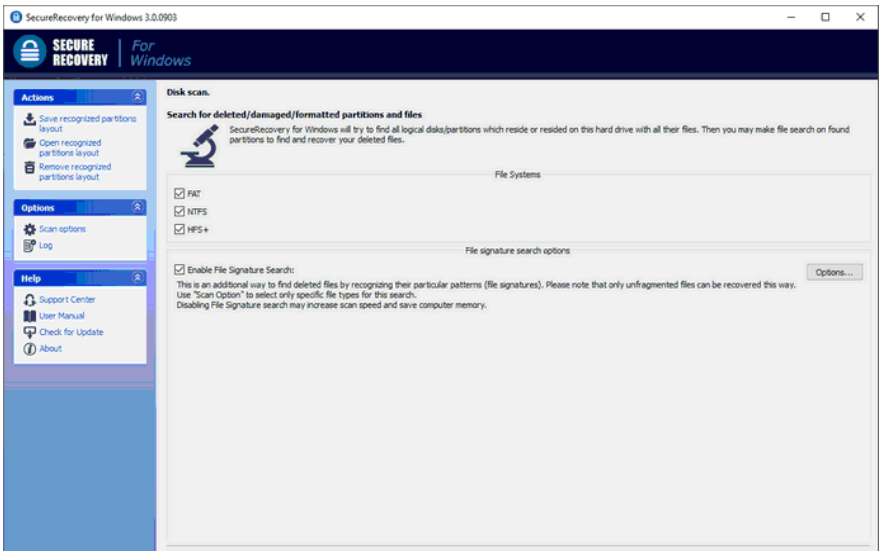
Some of the data loss scenarios can cause damage to logical volumes. Examples include: volume deletion, partial overwriting, re-partitioning of the drives, re-formatting of logical volumes and similar issues. These types of situation would look like an inability to detect the file system or missing logical volumes (partitions).

SecureRecovery for Windows is unable to detect any volumes on the physical drive.



For these types of data loss scenarios the software uses a specific mode called Disk Scan. Disk Scan can be applied to the entire physical drive or to the partition or logical volume with an unknown or missing file system.

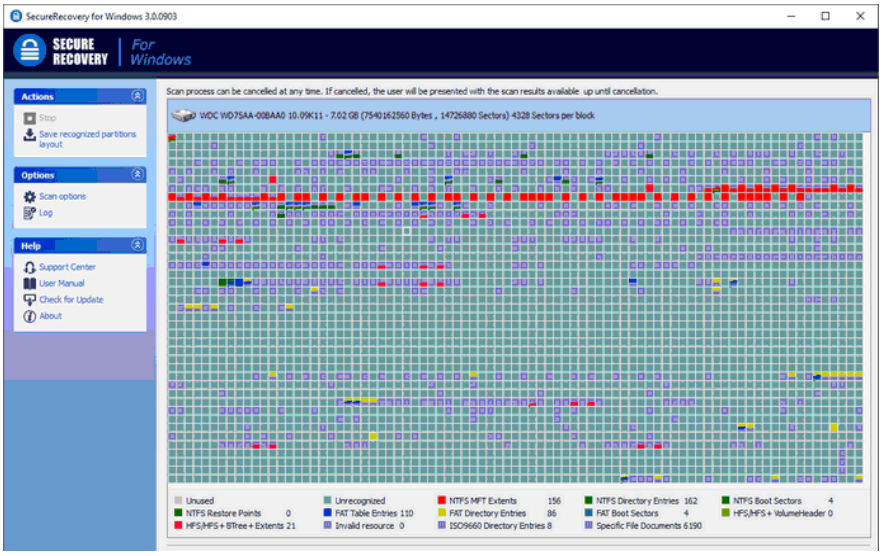
Select Disk or Volume and click the Next button to advance to the next step.



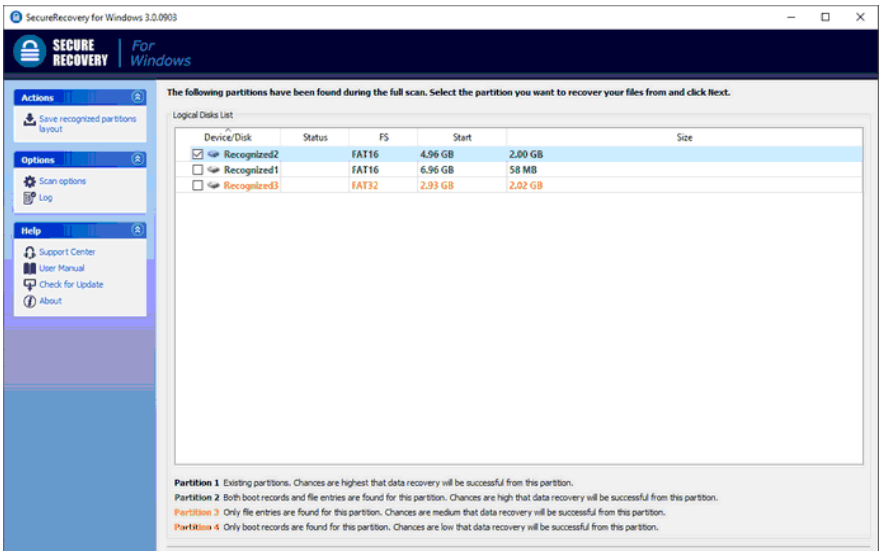
On Disk Scan screen user can make a selection of the file system types to search for.

There is also an option to run File Signature Search at the same time. File Signature Search was described in the **Full Scan** section.

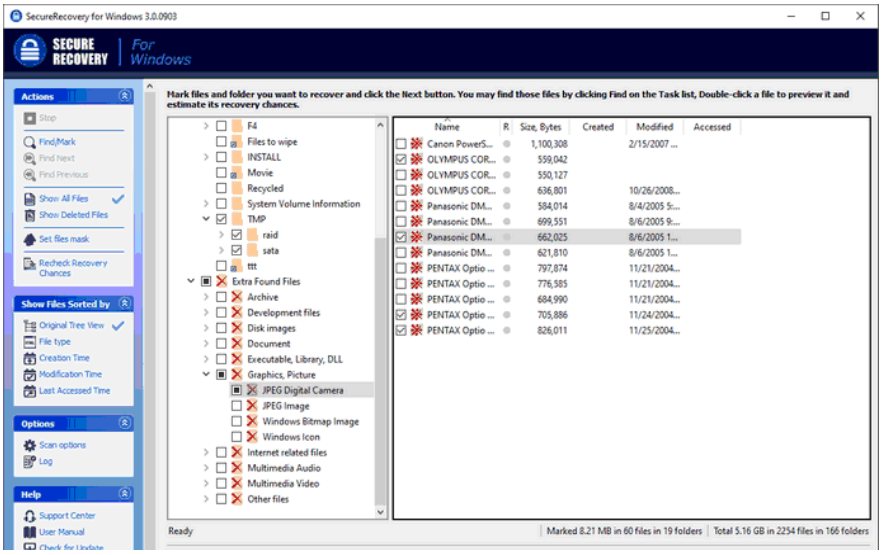
Click the Next button to start the scan.



Once the scan is complete, the software automatically switches to the next step showing recognized volumes and file systems.



Once the scan is complete Select the necessary partition and click the Next button.



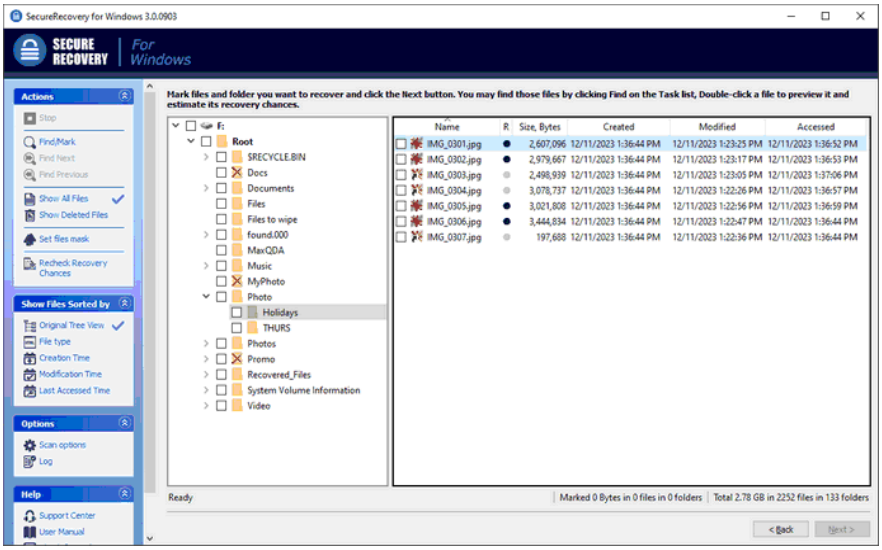
From this point the process transforms to **Recovering Lost Data from Existing Logical Volumes**. Select the Volume, then click the Next button and proceed with recovering data.

4.5 Working with Found Data

At the final step of Data Recovery Process the found files are presented in a tree-view, similar to a regular file system layout. In most cases, the tree would replicate the original folder structure that existed on the media.

Tree navigation is similar to Windows Explorer.

The list in the right section can also be sorted by columns (file size and three timestamps).

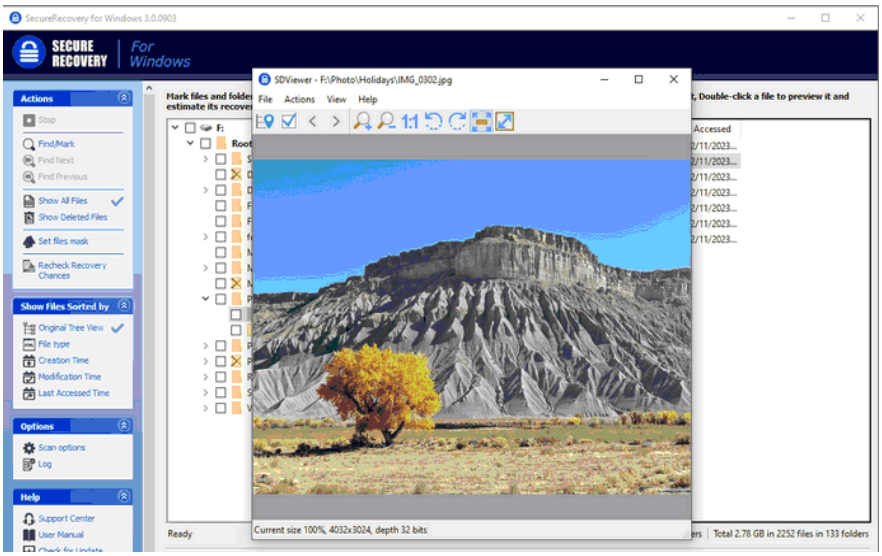


SecureRecovery for Windows shows its estimates of chances for successful file recovery in the Rec column.

4.5.1 Previewing

SecureRecovery for Windows allows the user to preview the most common file types before extraction. To open the preview window - double-click the file.

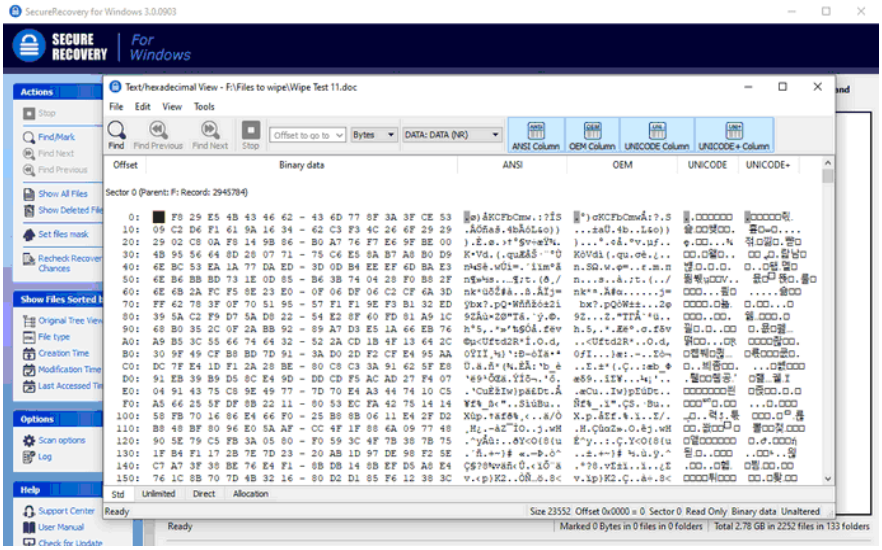
The software currently supports previewing for many file types, including images, video formats, MS Office / OpenOffice / LibreOffice files, and PDF files.



The picture can be rotate, zoomed in/out by, and marked for recovery.

If SecureRecovery for Windows does not support preview for a specific file type, or the file content is corrupted, the default preview window would be displayed instead.

This window shows the file content in binary (hexadecimal) and text (both ASCII and Unicode) forms.



4.5.2 Searching, Masking and Sorting

SecureRecovery for Windows has a powerful set of features to sort and group found files, search for the specific files and folders, and hide unnecessary data.

4.5.2.1 Sorting and Grouping the Recovery Results

The highlighted middle section of toolbar is responsible for sorting the recovery results.

There are 5 different options available: Original Tree View, File Type, Creation Time, Modification Time, and Last Access Time.

Original Tree View sorting mode replicates the original folder structure that existed on the media and shows it under the Root section.

Folders and files marked by red X have existed on the file system before, but they were deleted, lost or corrupted at some point of time.

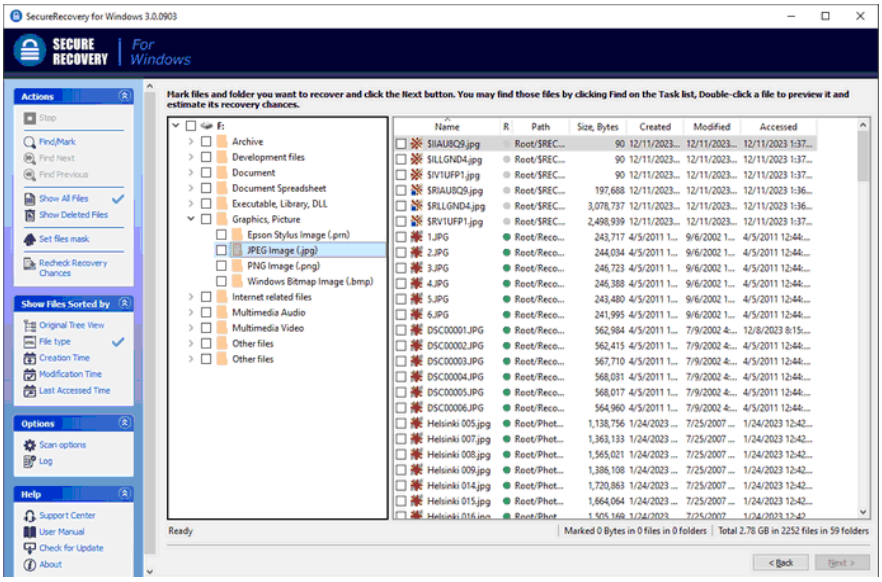
Extra Found Files section contains folders, which lost their names and parent folders, therefore they cannot be put into the Root tree above. The contents of those folders usually have the original file names and sub-folder structure intact.

Extra Found Files section also shows results of File Signature Search if this option was selected for Full Scan mode. The results are grouped by file type.

Please note that some file types (like JPG pictures) might have their timestamps and camera info preserved.

The second sorting mode is **File Type**.

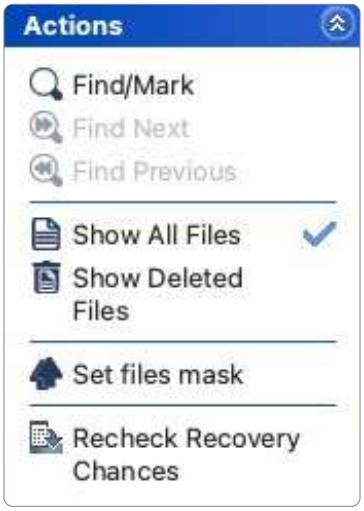
In this mode all found files from the media are grouped and organized by type.



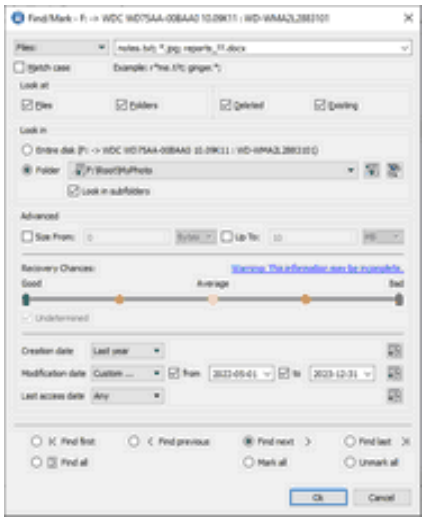
The last three sorting modes (**Creation Time**, **Modification Time**, and **Last Access Time**) use file timestamps to group all found files by a year, month, and date of their creation, modification, or last access respectively.

4.5.2.2 Searching Through the Recovery Results

SecureRecovery for Windows allows the user to search for specific files and optionally select them for further extraction. Click the Find/Mark menu item to open the corresponding dialog window.



All Files mode means that the search uses all available files while applying additional criteria from the dialog window.



You may specify how to treat specified strings. Please note that SecureRecovery stores previously entered search strings.	
All Files and Folders	If this option is selected, SecureRecovery applies Advanced Options to all files.
File Extensions	If this option is selected, SecureRecovery treats specified strings as file extensions
Files and Folders	If this option is selected, SecureRecovery treats specified strings as file names. Use ? for one unspecified character and * for an unlimited number of them to specify file masks.
Regular Expressions	If this option is selected, SecureRecovery treats specified strings as regular expressions
Match case	If this check box is selected, SecureRecovery makes a case-sensitive search
Look at	
Files	If this check box is selected, SecureRecovery includes files into a search.
Folders	If this check box is selected, SecureRecovery includes folders into a search. Disables when the Mark/Unmark All option is selected.
Deleted files	If this check box is selected, SecureRecovery makes a search among deleted files/folders.
Existing files	If this check box is selected, SecureRecovery makes a search among existing files/folders. Specifies where SecureRecovery searches for, and marks, files. It can look for them on the Entire partition, or in/from a certain folder.
Look in	If several partitions are opened in one tab, the places will be: All opened partitions, Selected partition, or in/from a certain folder. You may specify the starting folder for the search.
Advanced options	If this check box is selected, SecureRecovery will use the advanced options.
Size from/up to	Specifies file size limits.

Bad sectors	Specifies whether there are bad sectors in the files. Not known: it's unclear if there are bad sectors in the files.
Recovery Chances	Specifies files with certain recovery chances.
Date	Specifies file date boundaries. Dates for Modified, Created, and Last Accessed timestamps may be set separately.
	The Set for all button sets the specified data for all fields.
Find/?Mark options	Specify what SecureRecovery does with the found files. The Find first/previous/next/last options. SecureRecovery stops at the first/previous/next/last file that matches the specified search criteria. Find all files. SecureRecovery searches for all files that matches the specified search criteria.. The search results appear in the Find Results panel. Mark/Unmark All. SecureRecovery marks/unmarks all files that match the search criteria. When these options are selected, SecureRecovery marks/unmarks files only, not folders, regardless of what Look at: Folders specifies. Please note, that when performing a new find and mark/unmark task, SecureRecovery does not takes into consideration the previous marked/unmarked state of files. For example, if you first mark all doc files, and then all txt files, all doc files remain marked, too. To unmark them, you should specify doc once again and select Unmark files.

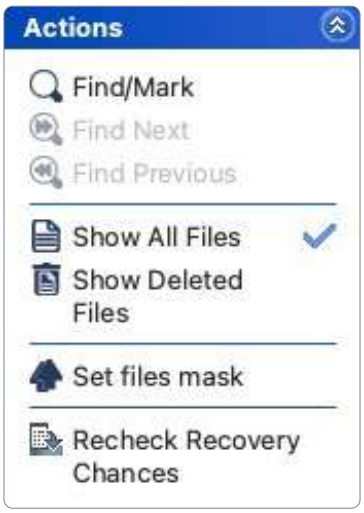
To repeat the search,

*Click Find Next or Find Previous

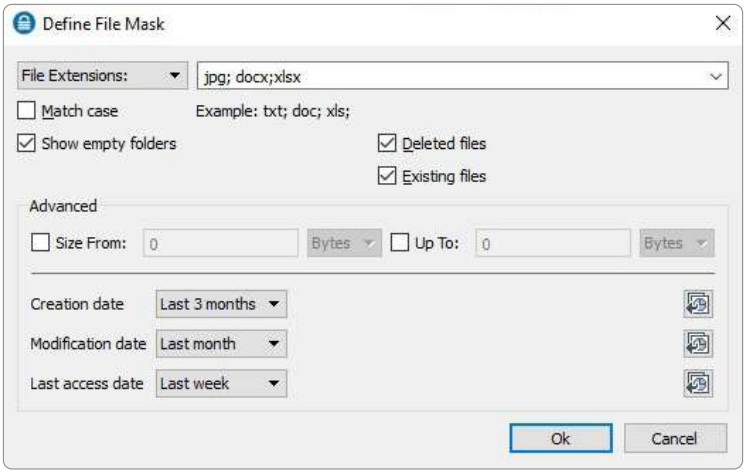
4.5.2.3 Masking the Recovery Results

Masking allows showing only the files with specific parameters, while hiding everything else.

The first option is to select between All Files and Deleted Files only, which can be used directly from the toolbar.



The Mask dialog box will appear



You may specify options for All Files, File Extensions, Files, and Regular Expressions	
Match case	If this check box is selected, SecureRecovery makes a case-sensitive search.
Show empty folders	If this check box is selected, SecureRecovery will show folders with no files inthem.

Deleted files	If this check box is selected, SecureRecovery makes a search among deleted files/folders.
Existing files	If this check box is selected, SecureRecovery makes a search among existing files/folders.
Use advanced options	If this check box is selected, SecureRecovery will use the advanced options, even when they are hidden.
Advanced Options	
Size from/up to	Specifies file size limits.
Bad sectors	Specifies whether there are bad sectors in the files. Not known: it's unclear if there are bad sectors in the files.
Runtime image	Specifies whether the files have already been included into the runtime image.
Date	Specifies file date boundaries. Dates for Modified, Created, and Last Accessed timestamps may be set separately.
	The **Set for all** button sets the specified data for all fields.

4.5.3 Selecting Files and Recovering

Before extracting the recovered data - the desired files and folders need to be selected and marked first.

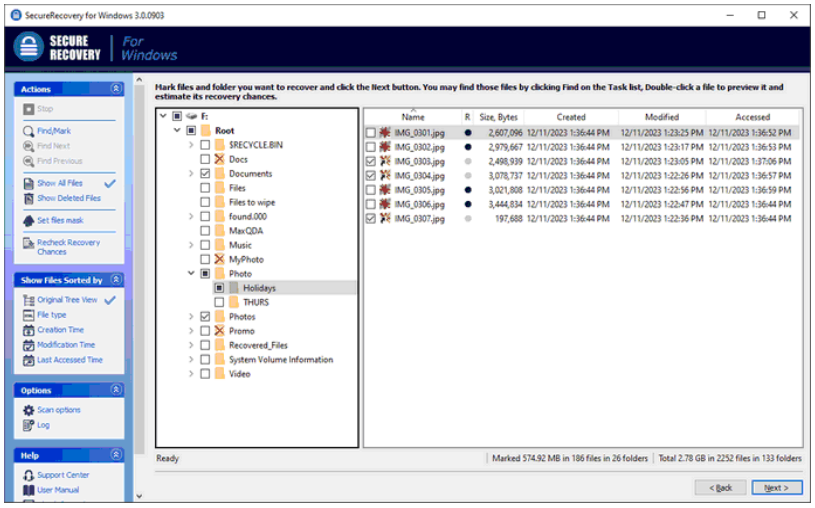
Files can be marked by clicking on a checkbox to the left of a file or folder name.

Using checkbox at the very top of the tree would select the whole tree - i.e. everything visible.

A checkmark near a folder name indicates that the full folder content is marked.

If folder has only some files/subfolders selected, the symbol becomes square (example - folder Logs below).

The counters located at the bottom show the total amount of data available (after masking), and how much from it is currently marked.



File marking can also be combined with File masking. Start with applying the file mask and hiding the unnecessary files/folders, and then use the marking for visible objects.

The second way to mark the specific files is to use Find/Mark dialog. Apply the desired criteria first, then select Mark matched files option.

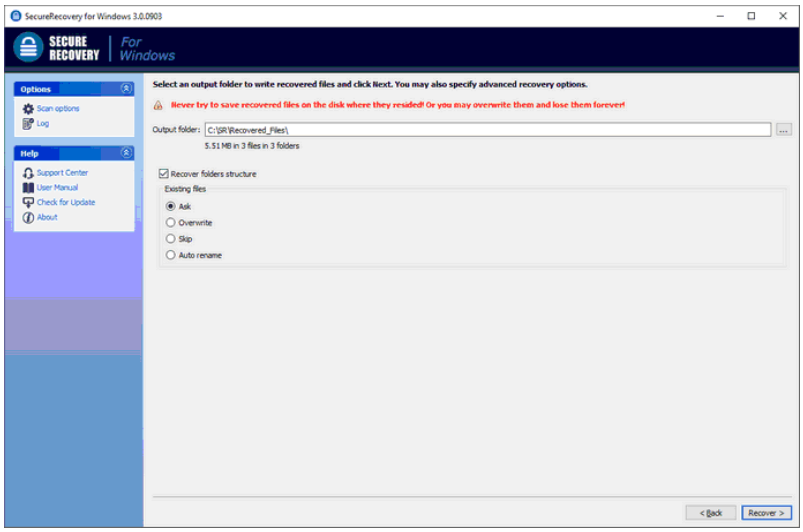
As a result, only the specified files will be marked. SecureRecovery for Windows allows the user to select a continuous range of files/folders on the right side of the window using the standard combination of SHIFT key and a mouse pointer.

After all necessary files are marked, click the Next button to start data extraction.

In Demo mode the ability to recover files may have limitations (i.e. the number and size of files that can be recovered). But the software can be registered with the valid license at this step by clicking on About link on the toolbar.

There's also an option to preserve the original folder structure, or restore all files into a single folder with no subfolders.

The Existing Files option allows selecting the software behavior in case of duplicated files: ask for confirmation every time, overwrite all duplicates, skip all, and rename all.



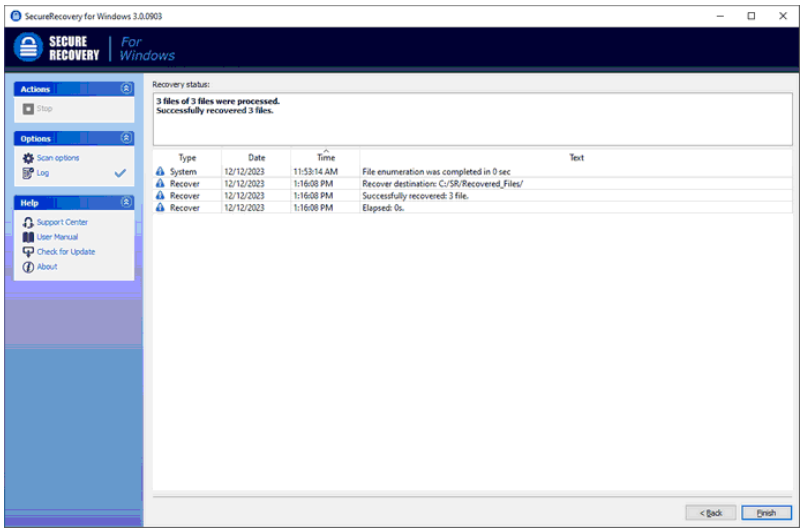
Please read the warning note (in red) carefully: restoring recovered data to the original media may destroy the files and should not be attempted. Always use another drive or flash device.

Clicking on the Recover > button starts the data extraction process.

It is possible to stop the extraction at any time by clicking the Stop button.

The pop-up dialog allows the user to abort the extraction process, skip the currently extracting file (continue after), and continue extraction.

If the extraction is finished or aborted, the summary will be displayed.



Please note that Log option on the toolbar can be switched on/off at any time during the data extraction to show the specific events, warnings, and errors, or hide them.

V CONTACT INFORMATION AND TECHNICAL SUPPORT

SecureRecovery for MacOS Support	https://www.securedata.com/contact
In-lab Data Recovery inquires:	https://www.securedatarecovery.com/request-help