Printed Documentation

目次

Stellar Forensic Toolkit

Stellar Forensic Toolkit v.12.5

User Guide

1. About Stellar Forensic Toolkit

The **Stellar Forensic Toolkit** is designed to recover, collect, preserve, and analyse digital data from your system or any external drive. It provides secure handling of evidence required for forensic investigations, legal proceedings, and in-depth forensic analysis.

The powerful scan engine of the software does a thorough scan of the selected storage device, shows a preview of files found during the scanning process and finally saves them to a specified destination. Separate options to recover documents, folders, mails or multimedia files from the storage media are also available.

In addition, the **Stellar Forensic Toolkit** enables users to **create new cases, load existing cases,** and **save scan results** to continue the recovery process at a later stage, ensuring flexibility and efficiency in forensic workflows.

Key Features:

1. **Case Creation from Forensic Images:** Supports logical and physical drives of .E01 and .DD images.
2. **E01 Image Types:** Create cases from Normal, Compressed, Fragmented, and Compressed-Fragmented images.
3. **DD (001) Image Types:** Create cases from Normal and Fragmented images.
4. **Supported Image Formats:** Load cases from .E01, .DD, .S01, .AFF, .BIN, .EX01, .IMG, AFF4-L, AFF-4, .TAR, and.ZIP formats.
    - **E01:** A common forensic image format used by EnCase. It not only stores a copy of the drive but also keeps extra details like case information, checksums, and compression.
    - **DD:** A raw copy of the drive created sector by sector. It's very simple, with no extra details or compression.
    - **S01:** Similar to E01, but it allows very large images to be split into smaller, more manageable parts.
    - **AFF:** Stands for Advanced Forensic Format. It can store both the drive image and important details (metadata), and it supports compression to save space.
    - **BIN:** A plain binary image of the drive. It's a direct copy without added information.
    - **EX01:** A newer version of E01, with better support for large drives, improved compression, and stronger protection.
    - **IMG:** A raw image format that makes an exact sector-by-sector copy of a drive or device.
    - **AFF4-L:** A modern version of AFF, designed to work with today's needs like very large data sets and even cloud storage.
    - **AFF-4:** A modern forensic format that stores multiple types of data (disk, memory, etc.) in one container and supports large-scale and cloud-based analysis.
    - **.TAR:** An archive format that combines multiple files into a single file without compression.

- **.ZIP:** A compressed archive format used to store and reduce the size of multiple files, with optional password protection.

5. **A**dded L01 support for Normal, Fragmented, Compressed, and Compressed Fragmented images.
6. **Case Settings and Evidence Form:** Added for better case management.
7. **Hash Validation:** Created images can be verified using MD5/SHA1/SHA256 hash values.
8. **Case Summary:** Includes source drive, evidence details, and acquisition/verification hash.
9. **Third-Party Compatibility:** All software (FTK Imager, UFS, FexImager, OS Forensic, Magnet, Belksoft, Oxygen Forensic) should be able to load our case image and scan the data.
10. **Reporting Enhancements:** Added log file summary, forensic report, and forensic recovery report.
11. **Forensic Report:** Includes source media details, evidence overview, hash details, and related information.
12. **Forensic Recovery Report:** Includes evidence overview, source media details, hash details, and a complete list of recovered files with EXIF info and preview.
13. **Edition Restriction:** Create Image and Recover from Image options not available in Forensic Edition.
14. **Tagging and Bookmarking:** Right-click to add Tags or Bookmarks; view and rename tags in the Tag View tab.
15. **Raw Recovery Reporting:** Forensic report generated automatically during raw recovery of a physical disk.
16. **Evidence Source Details in Reports:** Added when source is outside a case (e.g., Physical Disk, Logical Volume, RAID, VM, etc.).
17. **Media Metadata in Reports:** Camera details, PhotoDNA, and GPS info shown for JPEG, HEIC, PNG, and TIFF; previews supported for PNG, JPG, TIFF, BMP, and GIF.
18. **More Tools:** Shortcut for softwares such as Stellar Forensic for Backup Extractor, Stellar Forensic for iOS, Stellar Forensic for Android, Stellar Windows Password Recovery, Stellar Server Password Recovery, and Stellar Remote Forensic Imaging.

19. **Evidence Details Dialog:** Prompts during saving if details are missing (DD, IMG, BIN, RAID, Lost Partition, VM, etc.).
20. **Report Settings Control:** Option to enable/disable Evidence Details dialog (default: ON) and file preview in reports (default: OFF).
21. **EX01 Image Types:** Supports Normal, Fragmented, Compressed, and Compressed-Fragmented.
22. **EX01 Hash Validation:** Displays MD5 hash for .EX01 evidence files.
23. **EX01 Compatibility:** Supports images created in OpenText, EnCase and OSForensics.
24. **Cloud Image Support:** Added recovery for .AFF4-L images created by Magnet AXIOM.
25. **Recovery from Lost Drive/Unallocated Partition**: Recovers data from unallocated, uninitialized, unidentified and RAW partitions on a hard disk.
26. **Partition Recovery**: Recovers data from damaged, deleted, formatted, and lost partitions on any storage media device.
27. **Data Recovery from Physical Disk**: Recovers data from severely corrupted physical or removable disks.
28. **Raw Recovery Support**: Raw recovery of volumes and hard drives to search data based on signatures.
29. **RAID Recovery**: Seamless recovery for lost or inaccessible RAID hard drives. The software supports the creation of Virtual RAID to recover data.
30. **Virtual Machine Recovery**: Advanced recovery options for virtual machines, including support for Mac (APFS) and Linux volumes.
31. **Deep Scanning**: 'Deep Scan' does a comprehensive file signature-based search to maximize recovery in tough cases of data loss. Deep Scan is particularly useful for recovering the files that couldn't be found with normal scanning.
32. **Specific File Search**: Support to search a specific type of files in a logical drive/specific folder.
33. **Specific Folder Search**: Support to search a specific folder for lost & deleted data.
34. **Image Creation**: Supports the creation of image for hard disk and volumes for recovery.
35. **Preview Support**: Supports preview of files before recovery for most file types.
36. **Save and Resume Recovery Session**: Save and resume recovery option to recover data at a later stage without scanning the drive again.
37. **BitLocker Support**: Supports drives that are encrypted with BitLocker.
38. **File System Support**: Supports multiple file systems such as
    - Windows file systems - NTFS, FAT32, exFAT, and BTRFS.
    - CD/DVD file systems - CDFS, UDF, and HFS+.

- Linux file systems - EXT2, EXT3, and EXT4.
- Macintosh file systems - HFS, HFS+, and APFS.

39. **Simultaneous Scanning for File Systems:** Supports scanning of multiple file systems simultaneously and gives you the best possible scan results.
40. **Supported File Types**: Supports more than 300 file types by default. Also, supports adding and editing custom file types.
41. **Support for Multiple Drive Types**: Recovers data from desktop and laptop hard drives, external hard drives and pen drives, memory cards, SSD drives, SD cards, RAID servers, virtual machines, etc.
42. **Operating System**: Compatible with Windows 11, Windows 10, Windows 8.1, Windows 8, Windows Server 2022, Windows Server 2019, and Windows Server 2016.
43. **Theme** : Supports Vibrant, Dark, and Light themes for a customizable user experience
44. **Pause and Resume File System Scanning:** Support for pausing and resuming scans on NTFS, exFAT, FAT32, Linux, APFS, HFS+, and BTRFS file systems.
45. **ASUSTOR NAS RAID Recovery:** Supports recovery from RAID 5 and RAID 6 configurations on ASUSTOR NAS devices.
46. **Synology NAS Large File Recovery:** Efficient recovery of large files from Synology NAS systems.
47. **Multiple BTRFS Volume Support:** Enables the listing and scanning of multiple BTRFS volumes within a single pool (version 1 or higher).
48. **QNAP Static and Thick Volume Recovery:** Supports recovery of static and thick volumes on QNAP NAS devices.
49. **Bad Sector Skipping in Drive Imaging:** Option to skip bad sectors when creating a drive image, improving efficiency.

2. About the Guide

This user guide contains steps to assist you through various functions of **Stellar Forensic Toolkit**. Each function is explained in detail, in the corresponding sections.

The guide covers the following major topics:

This guide has the following features for easy navigation and understanding:

- Select a topic from the list of topics given on the left side navigation pane.
- There are Notes and Tips in some topics of this guide for better understanding and ease of work. These *Notes* and *Tips* are given in italics style.

3. Getting Started

3. Getting Started

3.1. Installation Procedure

Before installing the software, please ensure that your system meets the following minimum system requirements:

Minimum System Requirements:

- **Processor**: Intel compatible (x64)
- **Operating System**: Windows 11 / Windows 10 / Windows 8.1 / Windows 8 / Windows Server 2022 / Windows Server 2019 / Windows Server 2016 (Service Pack 1)
- **Memory**: 16 GB (recommended) 8 GB (minimum)
- **Hard Disk:** 250 MB for installation files

Steps to Install the Software:

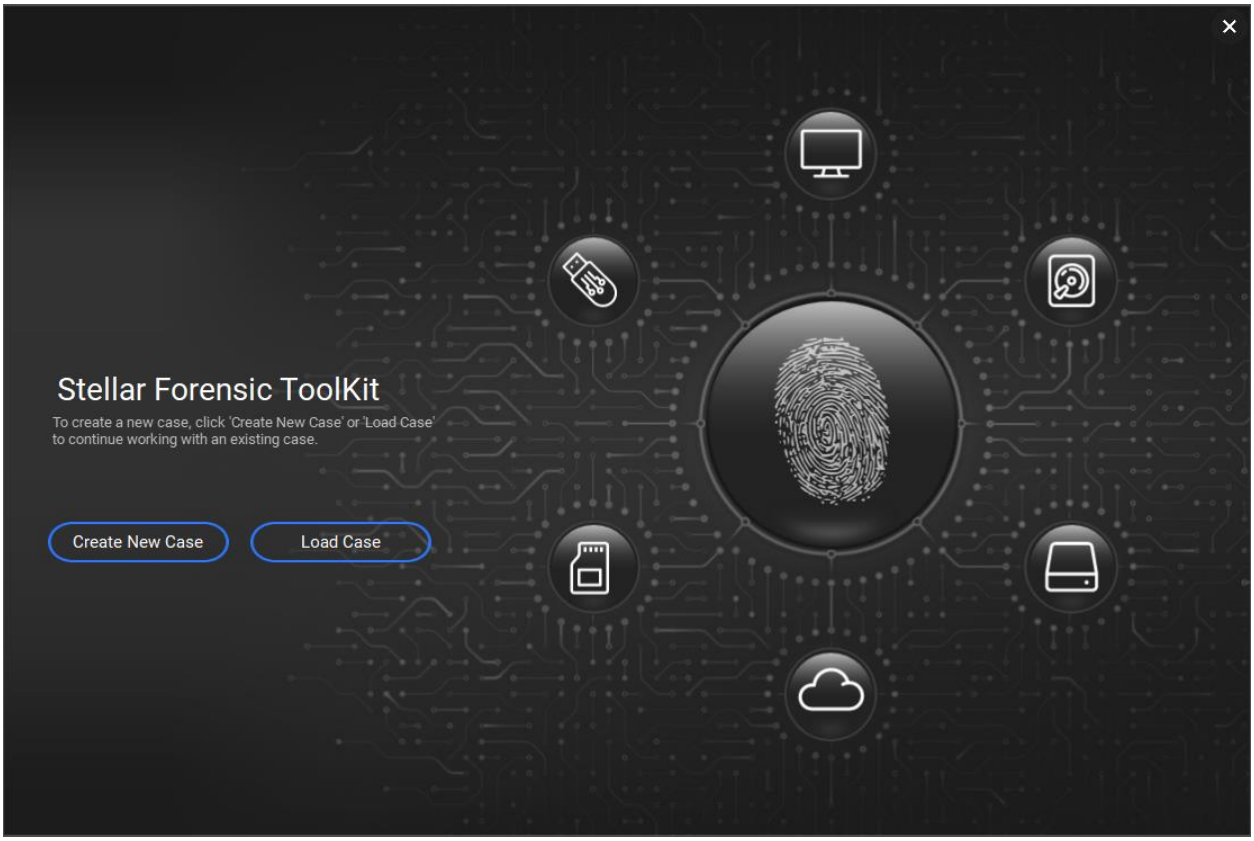
1. Double-click on **Setup Installer** to start the installation. **Select Setup Language** dialog box appears
2. From the drop-down list, select your language and click **OK**. **Setup - Stellar Forensic Tookit** window appears.
3. Click **Next**. **License Agreement** dialog box is displayed.
4. Choose **I accept the agreement option**. The **Next** button will be enabled. Click **Next**. **Select Destination Location** dialog box is displayed.
5. Click **Browse** to select the destination path where the setup files get stored. Click **Next**. **Select Start Menu** Folder dialog box is displayed.

6. Click **Browse** to provide a path for program's shortcuts. Click **Next**. **Select Additional Tasks** dialog box is displayed.
7. Select checkboxes as per your choice. Click **Next**. **Ready to Install** dialog box is displayed.
8. Review your selections. Click **Back** if you want to change them. Click **Install** to start the installation. The **Installing** window shows the installation process.
9. On completion of the installation process, Completing the **Stellar Forensic Tookit Setup Wizard** window is displayed. Click **Finish**.

3.2. Getting Familiar with User Interface

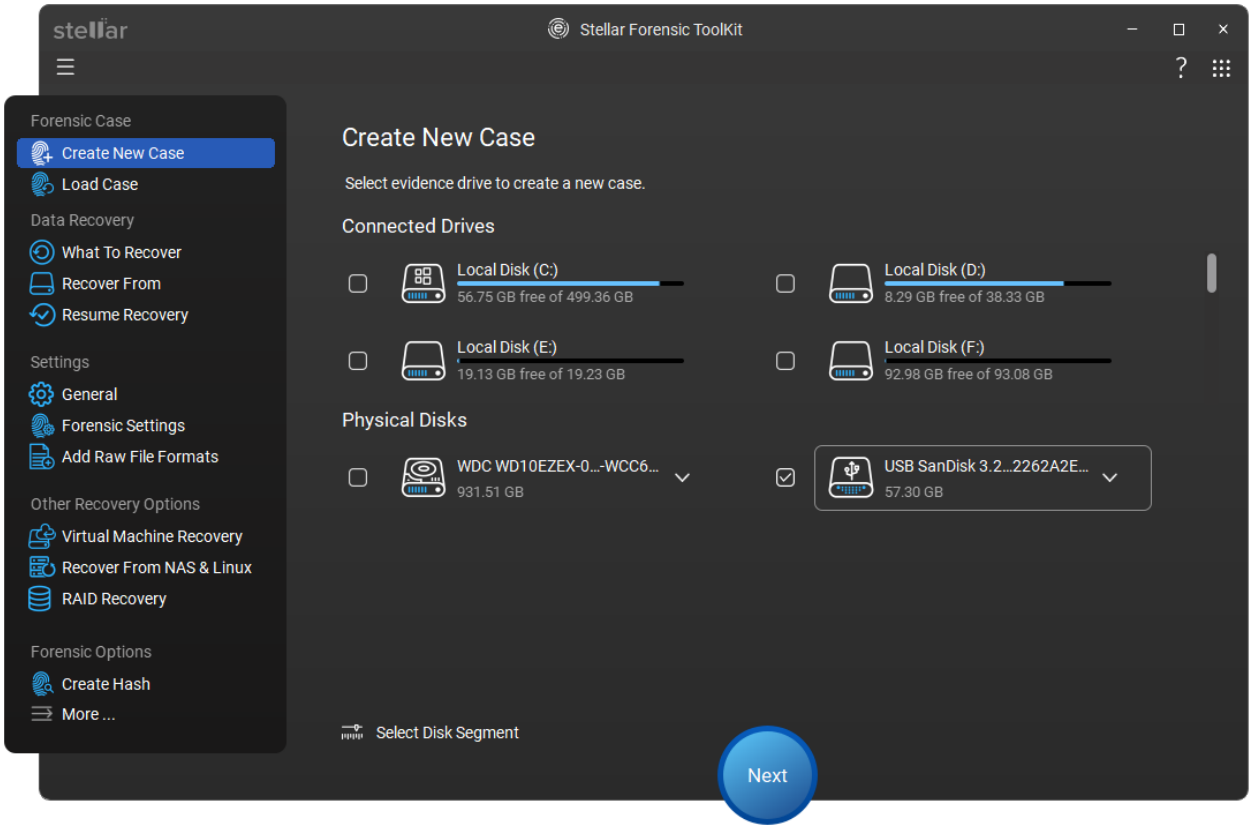
3.2. Getting Familiar with User Interface

The main user interface of **Stellar Forensic Toolkit** software is quite simple, easy to use and effective. On launching the software, below screen will be displayed.

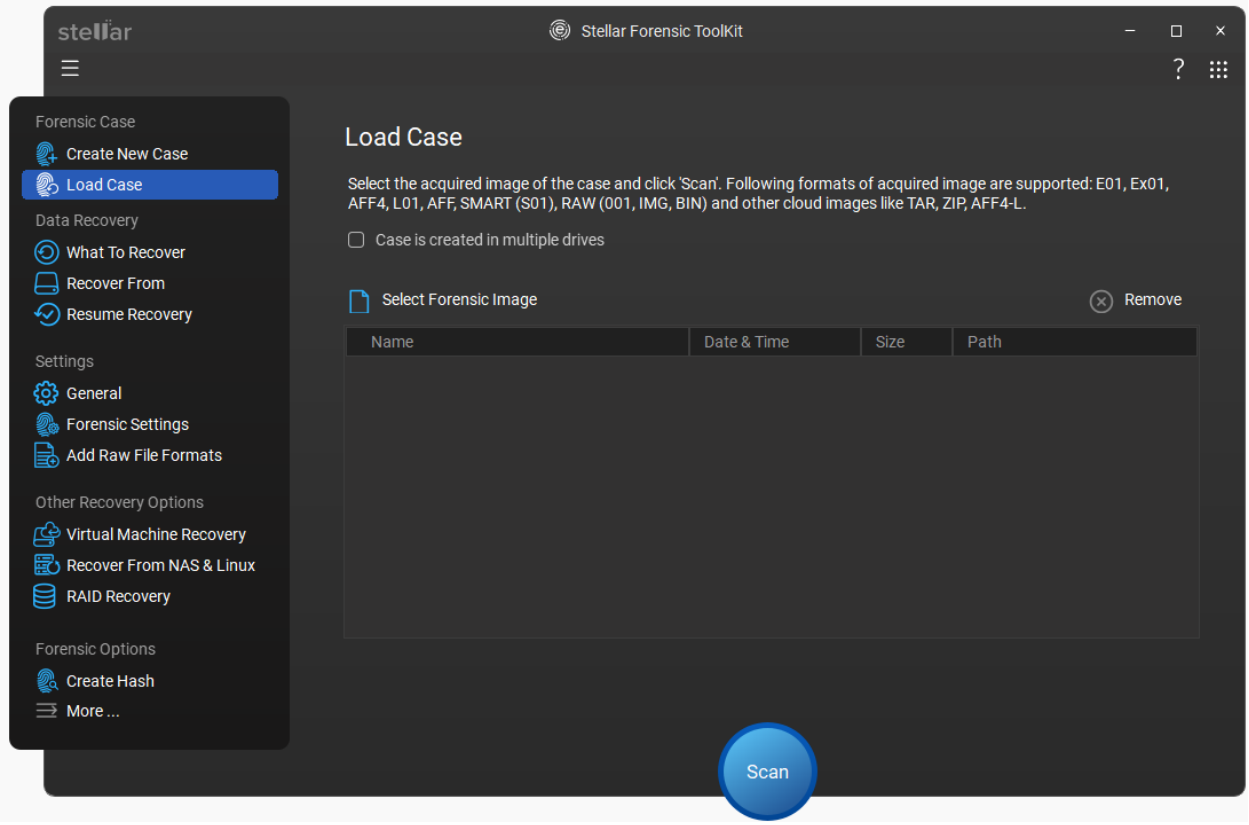


There will be two buttons available on the main screen, which are given below:

- **Create New Case:** Click this button to create a new case. The following screen will then appear.

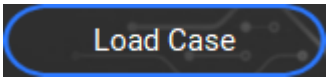
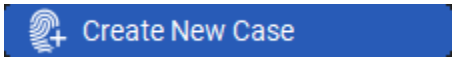


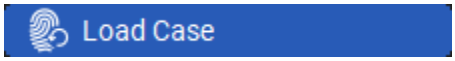
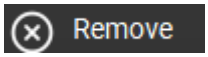
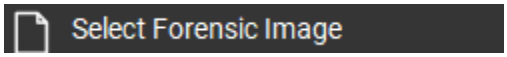
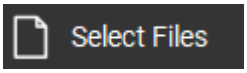
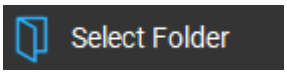
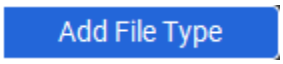
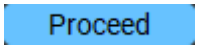
- **Load Case:** Click this button to load an existing case. The following screen will then appear.



3.2.1. Getting Familiar with Buttons

Some other general buttons/icons that you will encounter while using **Stellar Forensic Toolkit** are as follows:

	On the main screen, select this button to create a new case.
	On the main screen, select this button to load an existing case.
	From the left navigation menu, under **Forensic Case** section, select this button to create a new forensic case.

	From the left navigation menu, under **Forensic Case** section, select this button to load forensic case.
	From the left navigation menu, under **Settings** section, select this button to configure forensic settings.
	From the left navigation menu, under **Forensic Options** section, select this button to create hash.
	Click this button to remove the selected file from the list.
	Click this button to select a forensic image.
	Click this button to select the files.
	Click this button to select the folder.
	Click this button to add file type.
	Click this button to proceed to the next step in the process.
	Click this button to access additional tools related to **Stellar Forensic Toolkit**.
	Click this button to open user help guide.

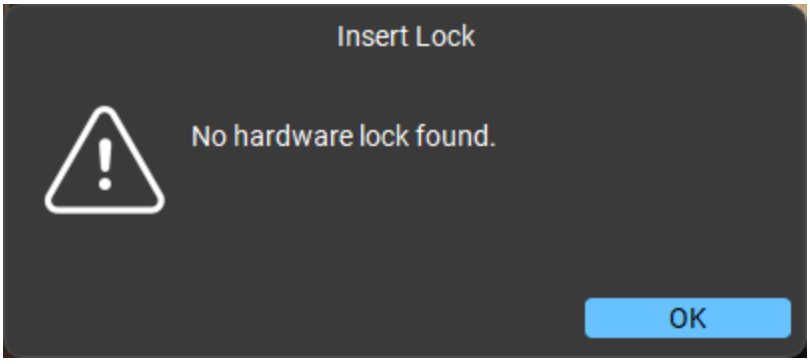
	Click this button to move to the next window.
	Click this button to proceed with the current operation.
	Click this button to mount a **Virtual Machine Image** disk for data recovery.
	Click this button to resume the scanning process.
	Click this button to recover the scanned data.
	Use this button to save the current case, file, or settings.

	Click this button to start the scanning process.
	Use the this button to confirm your action or selection.

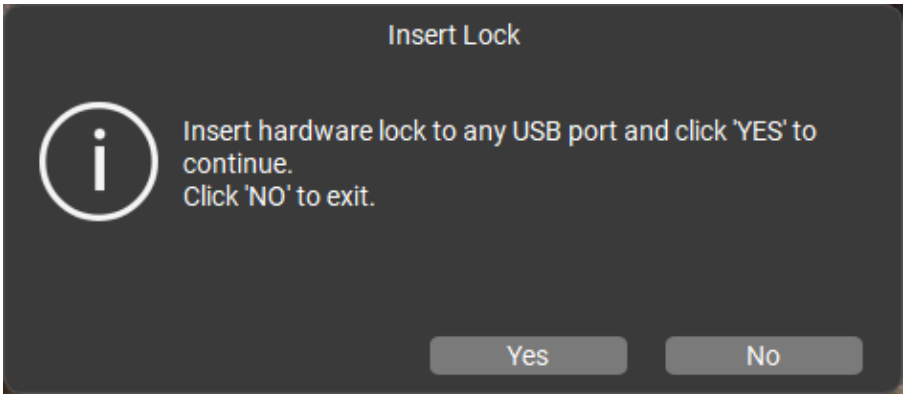
3.3. Starting the Software

To start the **Stellar Forensic Toolkit**, follow these steps:

1. Double-click on **Stellar Forensic Toolkit**.
2. **Insert Lock** dialog box appears on the screen with the message **"No harware lock found",** as shown below:



3. Click **OK**.
4. A below message appears on the screen prompting you to insert the hardware lock (Rockey) to any USB port of your computer. click **Yes** to continue and No for **Exit**.



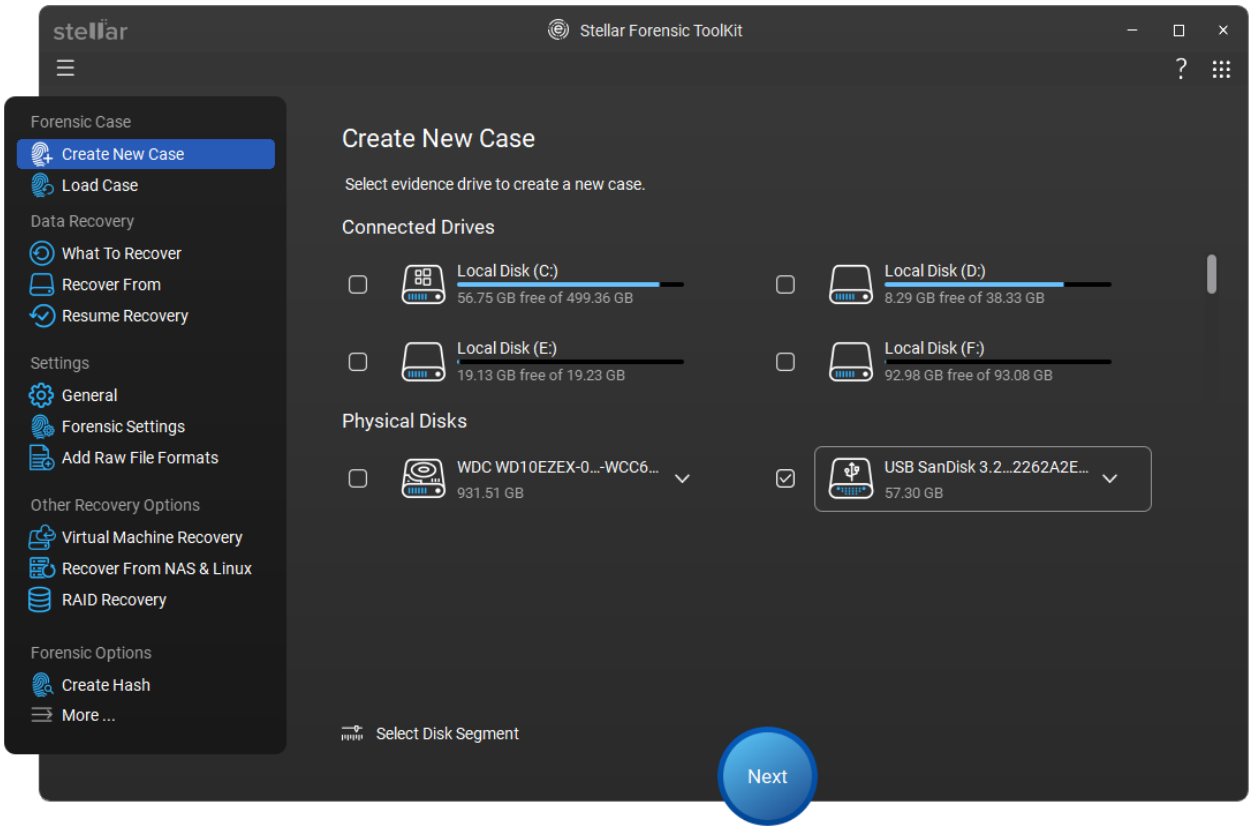
5. Insert the **Hardawre Lock (Rockey)** to any USB port of your computer to start the application.

4. How to

4. How to

Stellar Forensic Toolkit provides you options to Create New Case, Load Case and different options to recover your data. To recover data, you have to first scan the hard drive or volume. **Stellar Forensic Toolkit** has the option of scanning them as well. After scanning, you can preview the scanned results before recovery. You can also filter, find, and select the files you want to recover. You can then recover and save selected files to a destination folder of your choice.

With **Stellar Forensic Toolkit** you can perform specific operations. The software provides the following options:



Forensic Case

- **Create New Case:** Use this button to create a new forensic case.
- **Load Case:** Use this button to load forensic case.

Data Recovery

- **Recover Everything:** This option recovers all the data from a particular drive or location selected for recovery.
- **Customize Your Scan:** This option can recover office documents, emails, photos, audio, or videos, either separately or collectively, based on what you need.

The software also allows you to create new case and recover data by selecting any connected drive or a specific location on a drive or storage media connected to the system. Following selection options are provided by the software:

- **Connected Drives –** These include all the drives and external storage media connected to the system.
  There are specific **Icons**, **Symbols**, and **Bars** on volumes or partitions under Connected Drives. Refer to the below table for their details:

A. Drive Icons and Their Identification:

Icon	Identification

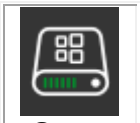
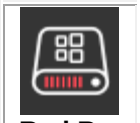
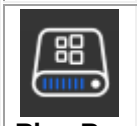
 **Lock Icon**	A **Lock icon** on a disk indicates drive is **BitLocker Encrypted**.
 **Minus Icon**	A **Minus Sign** icon on a disk indicates **Lost Drive/Unallocated** volume.
 **Warning Icon**	A **Warning** icon on a disk indicates **SMART** status of a disk or volume. This icon appears on a disk when the disk health status is changed from good to bad.
 **Question Mark Icon**	A **Question Mark** icon on a disk represents **Can't Find Drive** function. Use this function to recover data from lost partition.

B. Drive Symbol and Their Identification:

Symbol	Identification
 **Windows Symbol**	A **Windows Symbol** on a disk indicates the bootable volume of a hard disk.
 **No Symbol**	A **No Symbol** on a disk indicates **Existing Volume** of a connected drive.
 **Disk Symbol**	A **DiskSymbol** on a disk indicates a CD/DVD volume.
 **USB Symbol**	A **USB cable Symbol** on a disk indicates an external storage media or pendrive volume.

C. Drive Bar and Their Identification:

Bar	Identification

 **Green Bar**	**Green** color bars on a disk signify the good health status of a disk.
 **Red Bar**	**Red** color bars signify the bad health status of a disk.
 **Blue Bar**	**Blue** color bars signify that the **SMART** status is not supported in the drive.

Note: *A drive can be a combination of any* ***Icon*** *or* ***Bar****.*

- **Physical Disks –** It includes complete volumes of the system drive and external storage media connected to the system.
- **Common Locations –** It consists comman locations including Desktop, Documents, or choose location option.

You can also recover data from deleted and lost volumes of your computer's hard disk. Can't Find Drive option will list all volumes that have been deleted from your hard disk.

Working with Stellar Forensic Toolkit covers the following topics:

4.1. Create New Case

4.2. Load Case

4.3. Recover Data from Existing Volume

4.4. Recover Data from Lost Drive/Unallocated Partition

4.5. Recover Data from CD/DVD

4.6. Recover a Lost Partition

4.7. Recover Data from Physical Disks

4.8. Recover Data from Virtual Machine

4.9. Remote Recovery from NAS

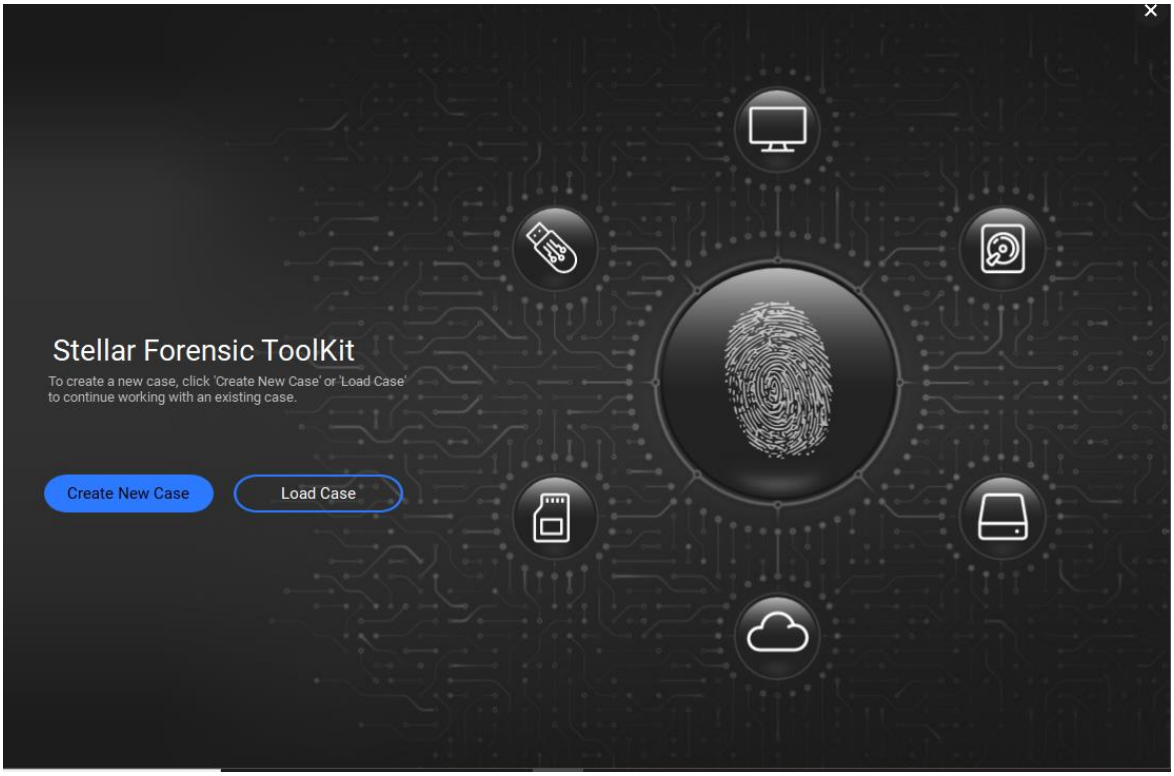
4.10. Remote Recovery from Linux System

4.1. Create New Case

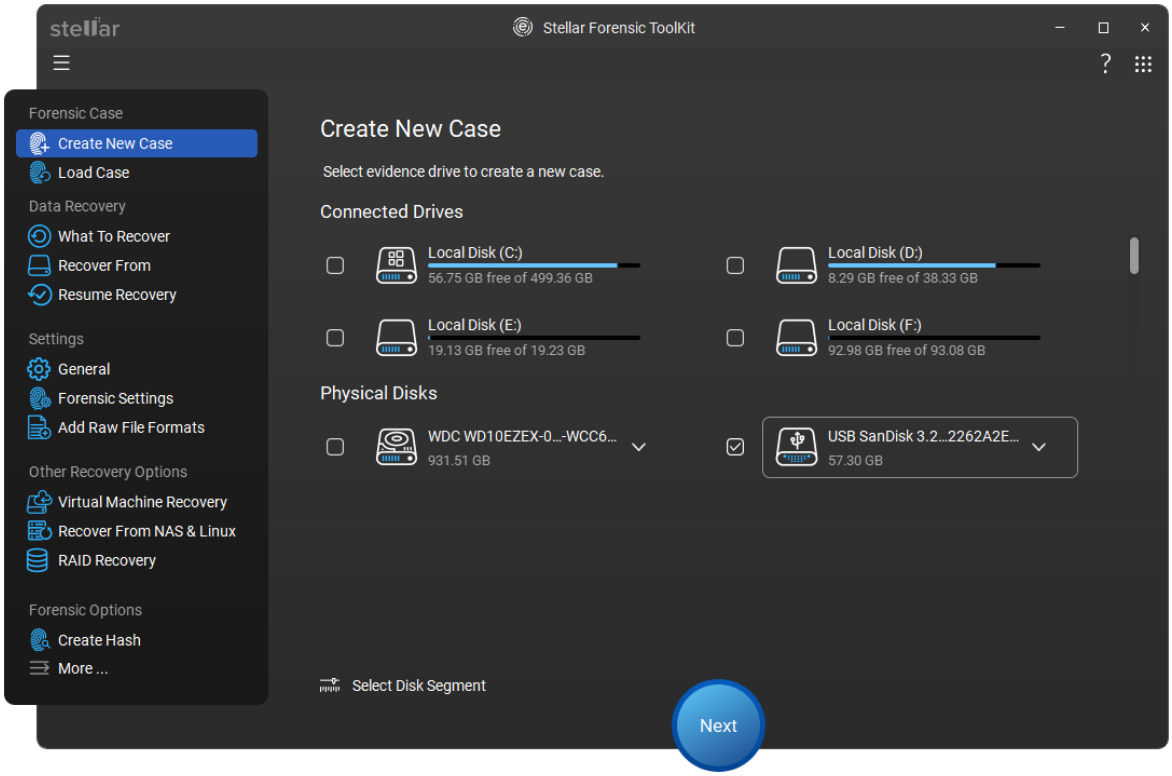
Stellar Forensic Toolkit provides you feature to create the case. You can select the any evidence drive to create a new case which includes image type, compression type, fragmented type, hash algorithm, case name etc.

Steps to Create a New Case

1. Launch **Stellar Forensic Toolkit.**
2. From the main screen, select **Create New Case** button.



3. **Create New Case** screen appears on the screen, as shown below:

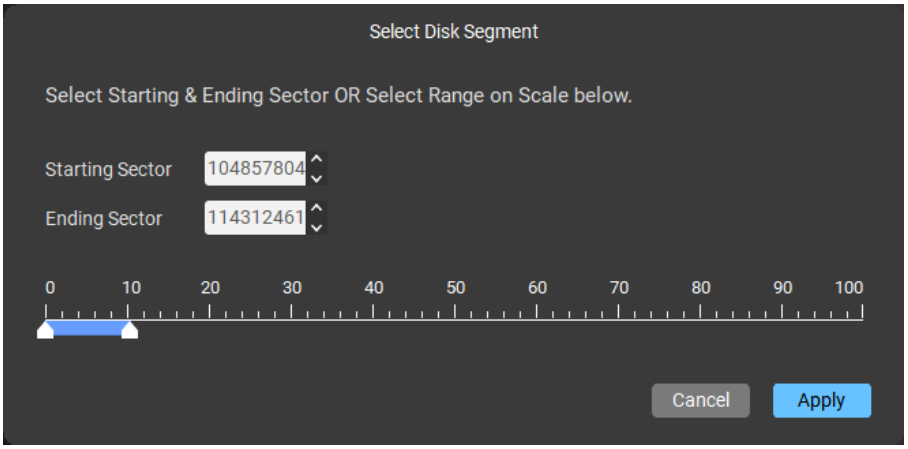


4. From the **Create New Case** screen, select the evidence drive or physical disk.

5. To create an image of the entire drive or partition click **Select Disk Segment** located at the bottom of the **Create New case** screen.

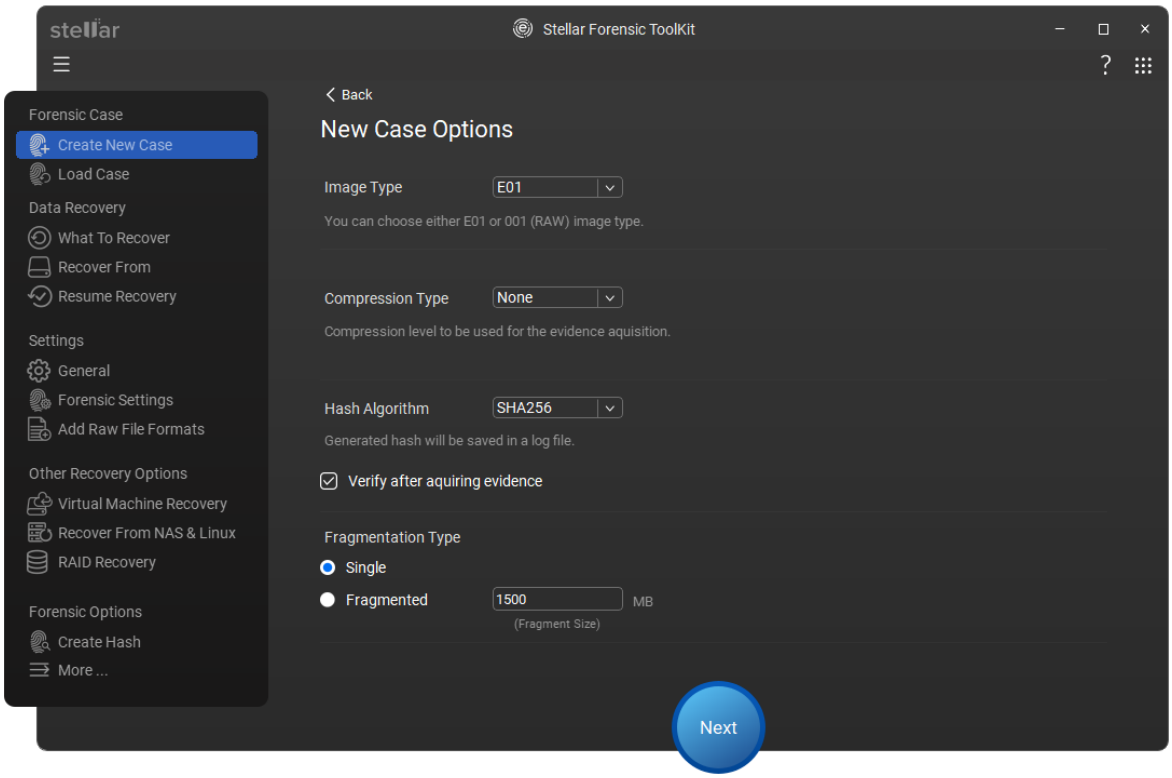
   Or

   To create an image of the selected region click on the **Select Disk Segment**. From the **Select Disk Image** screen, drag the sliders to define the starting and ending sectors of the image file. Click **Apply** button.



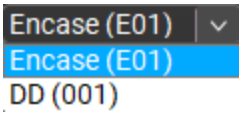
6. Click **Next** to contiue.

7. **New Case Options** screen appears, as shown below:



8. On the **New Case Options** screen, provide the following details:

- **Image Type:** Select the image type from the **Image Type** drop-down. You can choose either **EnCase (E01)** or **DD (001)** image type.



- **Compression Type:**

  Select the compression type such as, **Fast**, **Good** or **Best** from the **Compression Type** dropdown. Compression level to be used for the evidence aquistion.

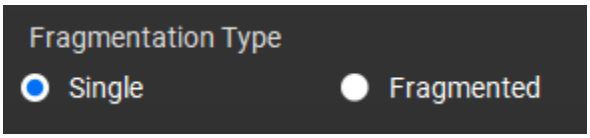
  - **Fast:** Creates the image quickly with minimal compression. The file size will be larger, but the process is faster.
  - **Good:** Provides a balance between speed and compression. The file size is moderate, and imaging speed is reasonable.
  - **Best**: Applies maximum compression to reduce file size. The process takes longer, but storage space is optimized.

- **Fragmentation Type and Fregment Size**

1. **Fragmentation Type:** Defines how large files are split into smaller parts (fragments) for storage or transfer.

You can select **Single** or **Fragmented** fragmentation type as per your requirement

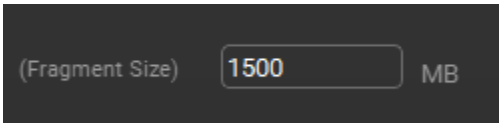
- **Single:** Saves the image as one complete file without splitting. To select this, click the **Single** radio button.
- **Fragmented:** Splits the image into multiple parts based on the selected fragment size. To select this, click the **Fragmented** radio button.



Note: *There are four combinations available for* ***EnCase*** *images and two for* ***DD (001)*** *images, based on compression and fragmentation options:*

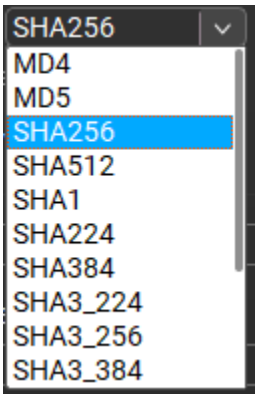
- ***EnCase:*** *Normal, Compressed, Normal Fragmented, and Compressed Fragmented*
- ***DD (001):*** *Normal and Normal Fragmented*

3. **Fregment Size:** Defines the size of each part when the **Fragmented** option is selected.



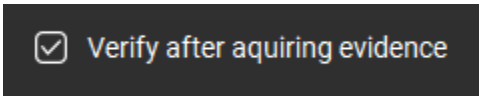
Note: *The minimum fragment size you can select is* ***500 MB****.*

- **Hash Algorithm:** Select the desired hash algorithm from the **Hash Algorithm** drop down.



Note: *Generated hash will be saved in a log file.*

- **Verify after aquiring evidence:** Select this option to verify the acquired evidence after the acquisition process.

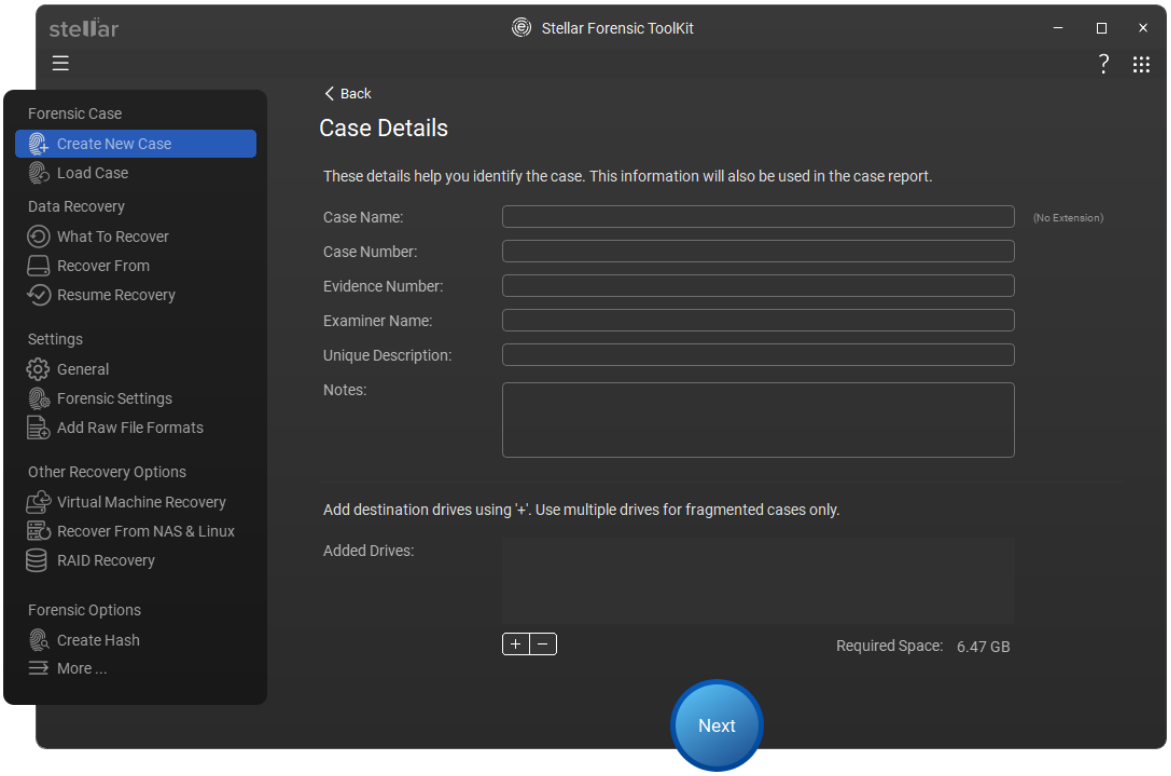


- Enter the **Case Name.**

- **Destination folder to save case**

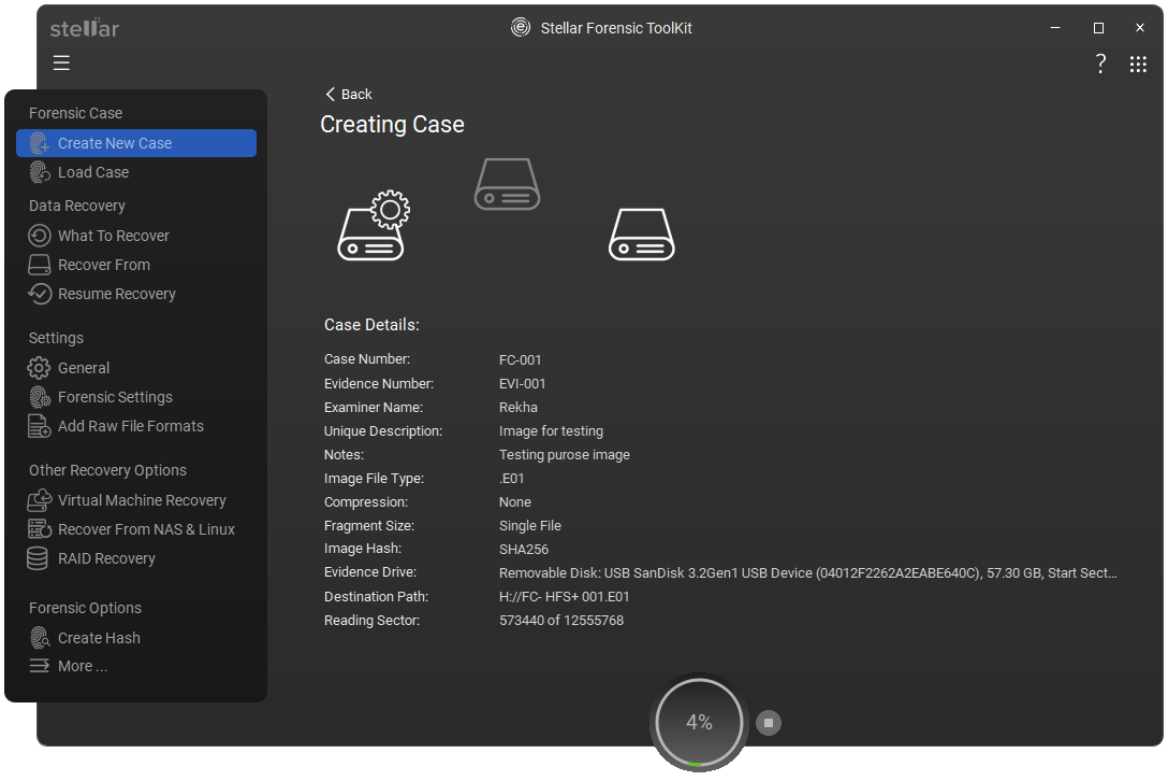
  Click the **Browse** button to select the destination folder where the case will be saved.

9. Click **Next** to proceed.
10. **Case Details** screen appears. Enter the following details:
    1. **Case Number:** A unique number assigned to the case.
    2. **Evidence Number:** A unique number for the specific piece of evidence
    3. **Examiner Name:** Name of the forensic examiner handling the case.
    4. **Unique Description:** A brief description of the evidence (e.g., device type, make, or model).
    5. **Notes**: Any additional remarks or relevant details related to the case or evidence.



Note: *All the above details are mandatory to fill. If any detail is missing, the process cannot proceed.*

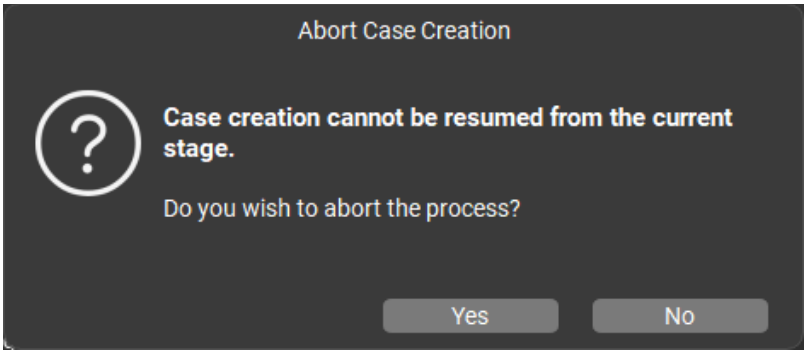
11. Click **Next** to continue.
12. **Creating Case** screen appears, displaying case details, as given below



Note: *If you want to stop the case creation process, follow these steps:*

*a. Click on **Stop** button located on the bottom of the screen.*

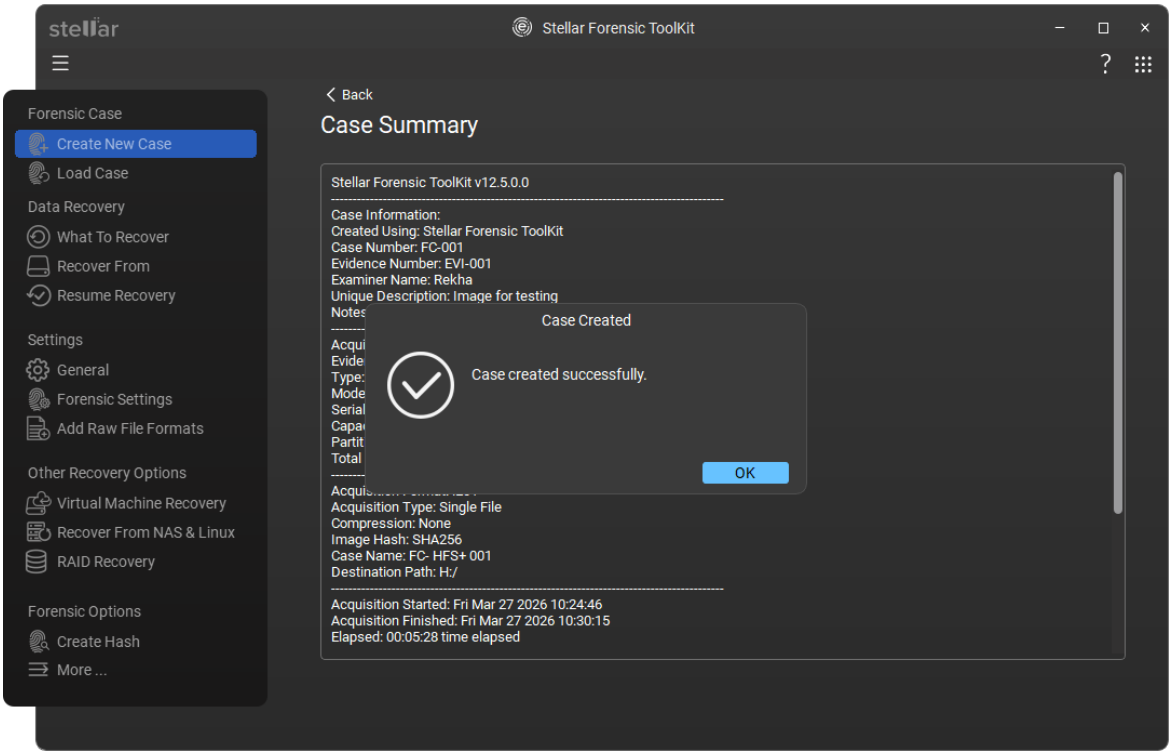
*b. **Abort Case Creation** dialog box appears on the screen .*



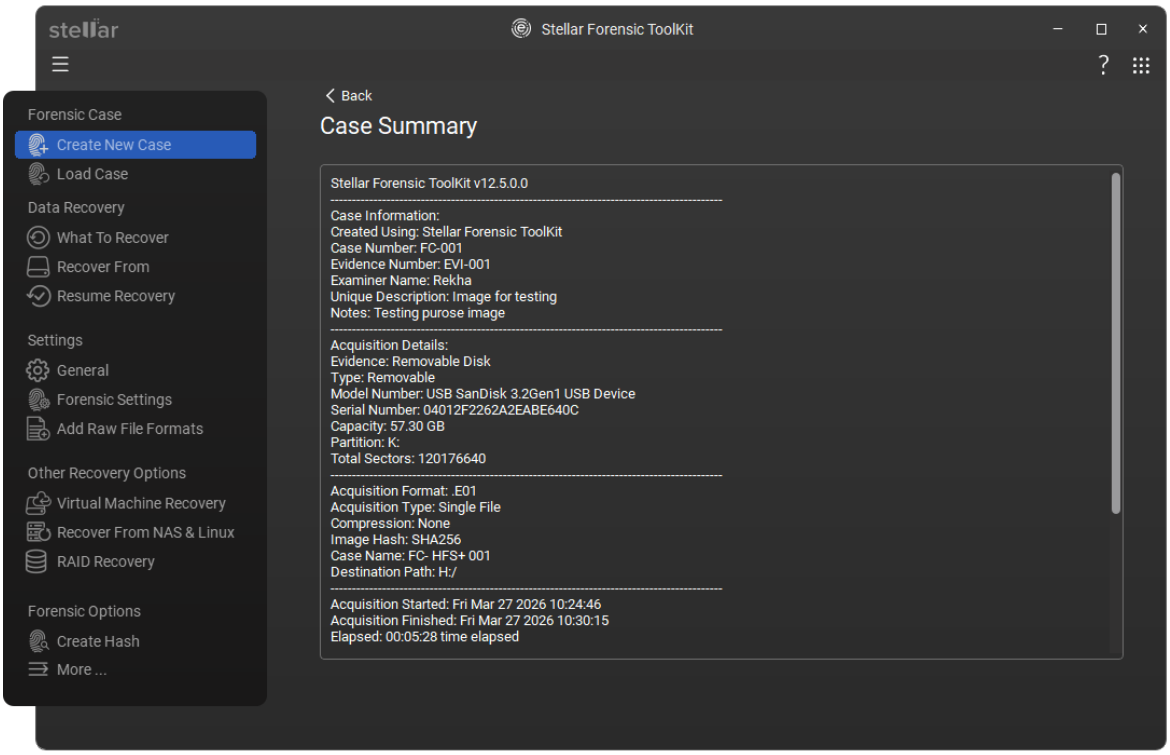
Important: *If you abort the case creation process, it cannot be resumed from the current stage.*

*c. Click **Yes** to proceed.*

13. **Case Created** dialog box appears on the screen.



14. Click **OK** to view **Case Summary.**

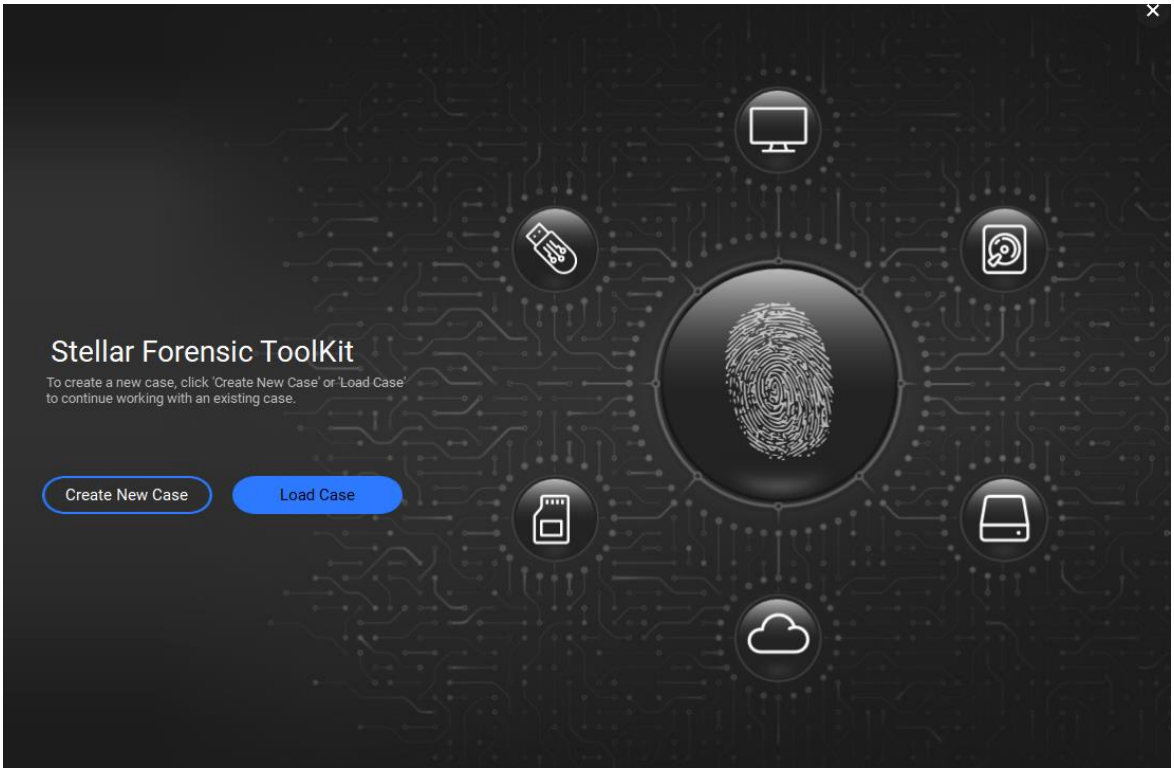


4.2. Load Case

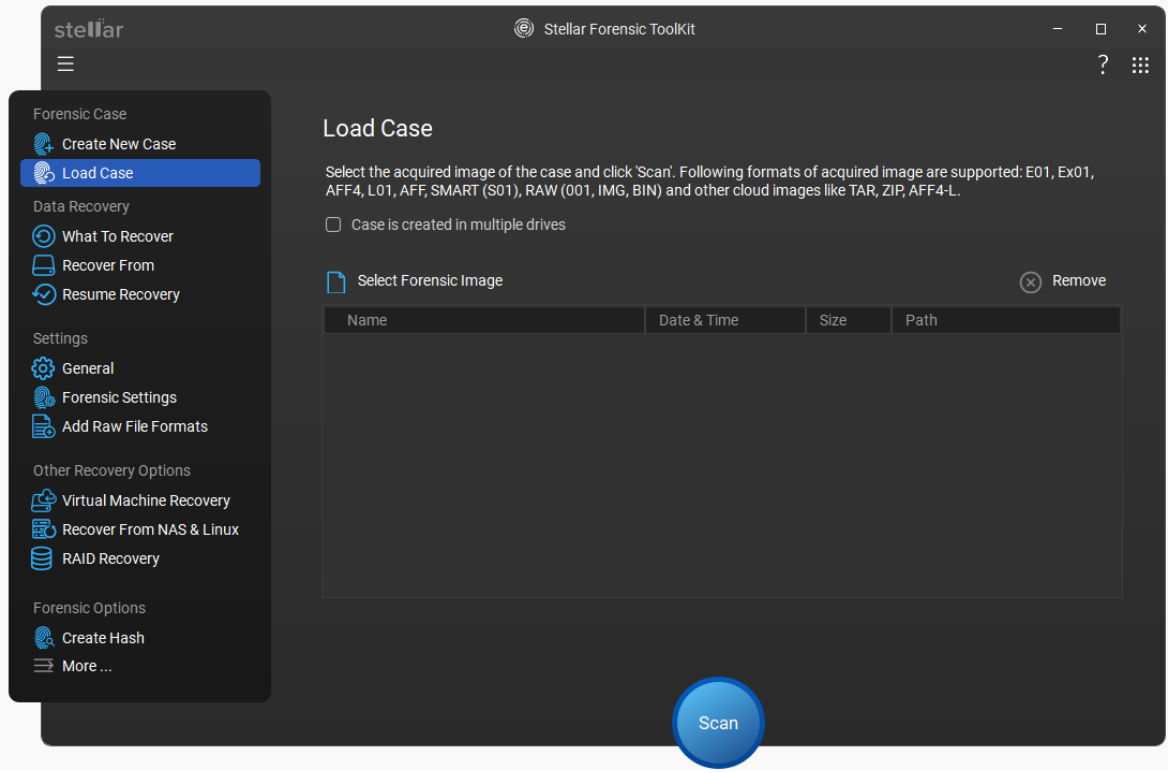
After creating the new case, you can load it, or if a case is already available, use this feature to scan and recover files.

Steps the Load the case

1. Run **Stellar Forensic Toolkit**.
2. From the main screen, select **Load Case** button.

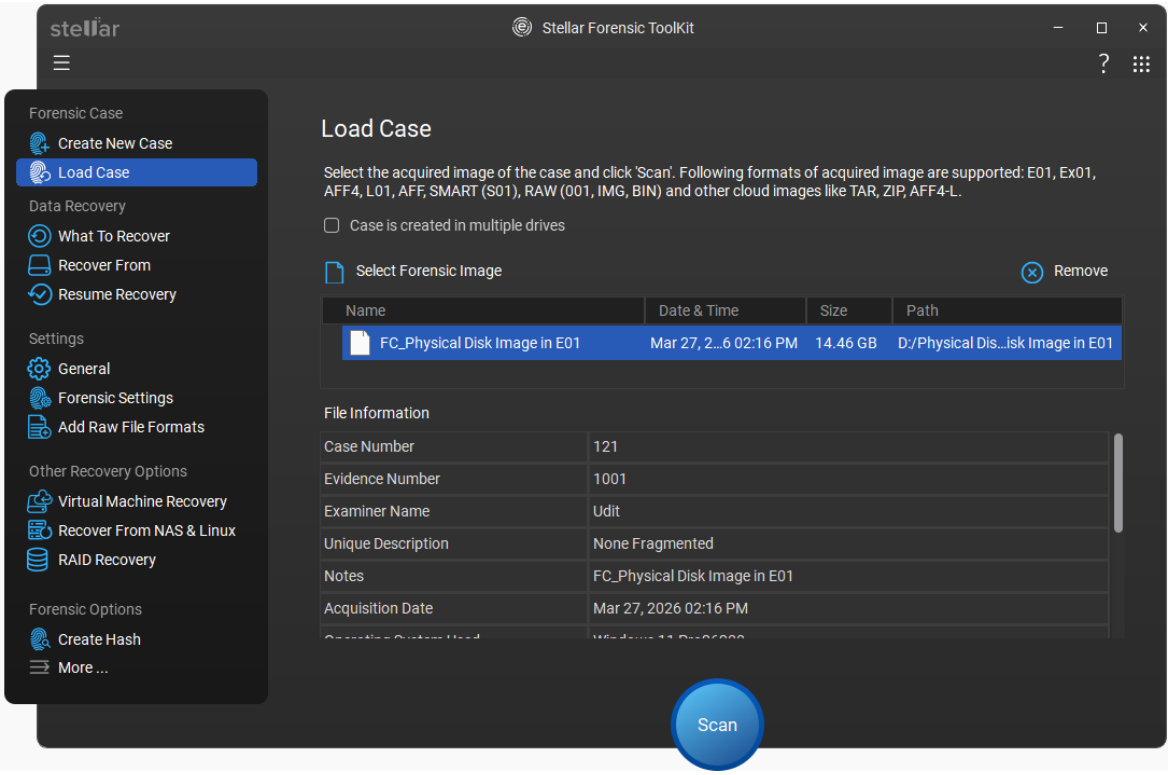


3. **Load Case** screen appears as given below.



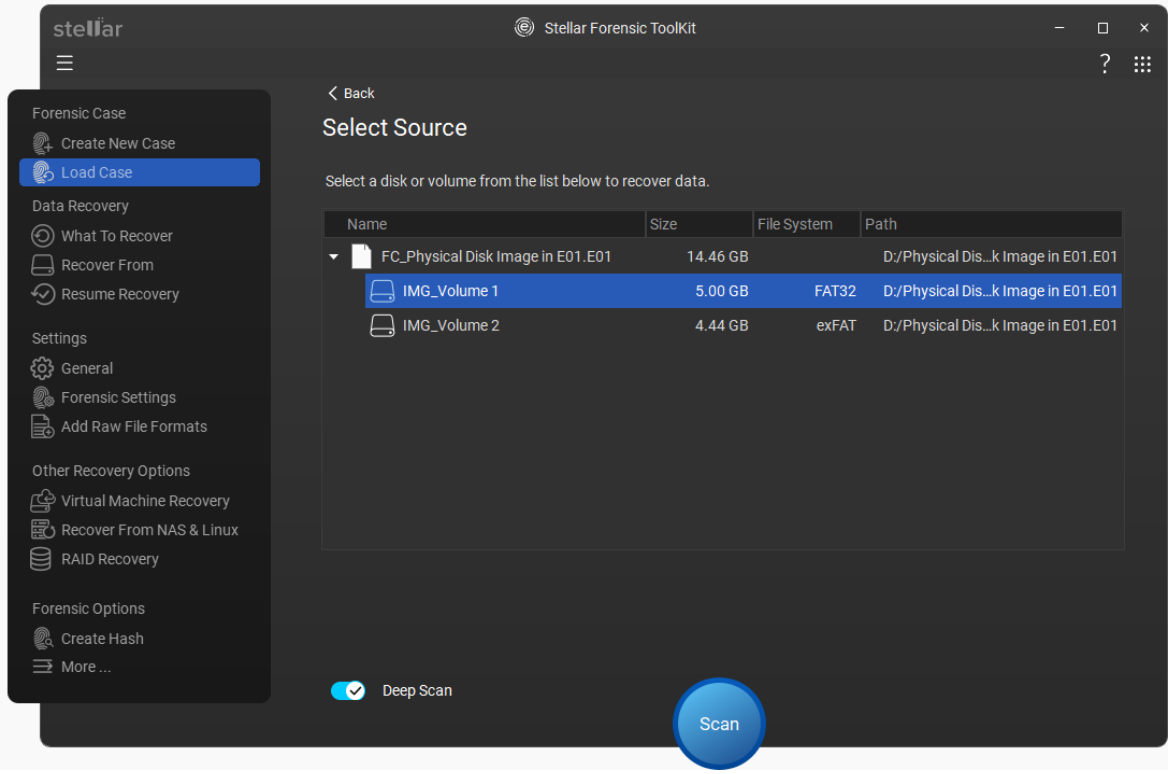
Note: *If you do not have a case, create a case first, then go to* ***Forensic Case*** *section in the left menu and click* ***Load Case****.*

4. Click on **Select Forensic Image** to choose the required image. The screen will display the case details, including name, creation date and time, size and path, along with case details such as case number, evidence number, examiner name, unique description, notes etc.



Note: *If you want to remove the selected disk from the list, click on* ***Remove*** *button.*

5. **Select Source** screen appears. Select a disk or volume you want to scan to start the recovery process. If you choose a volume, the scan begins immediately.

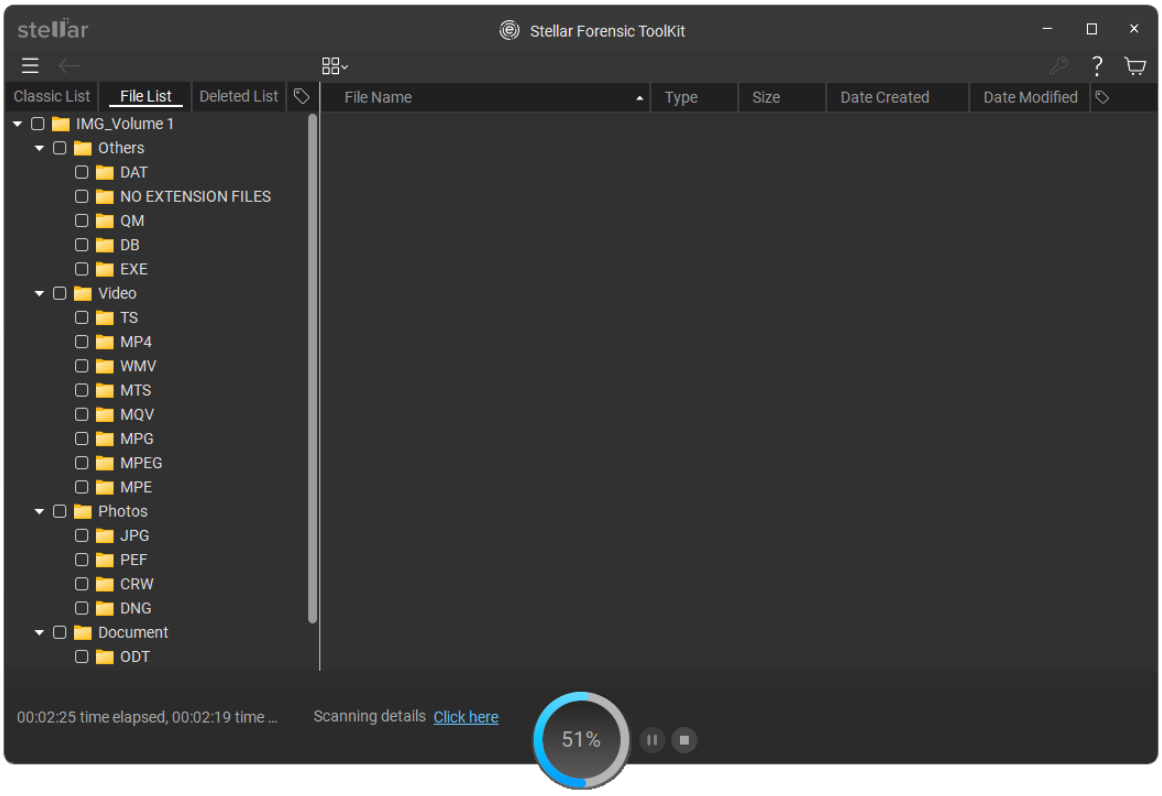


Note:

When you select the disk image, below radio buttons will be displayed on the screen.

- ***Scan for lost Paritions:*** *Select this radio button If you want to scan the lost partions. For more information, click here.*
- ***Raw Recovery on disk image:*** *Select this radio button If you want to proceed with the raw recovery process. For more information, click here.*

6. Click **Scan.**
7. A screen appears that shows the scanning process.

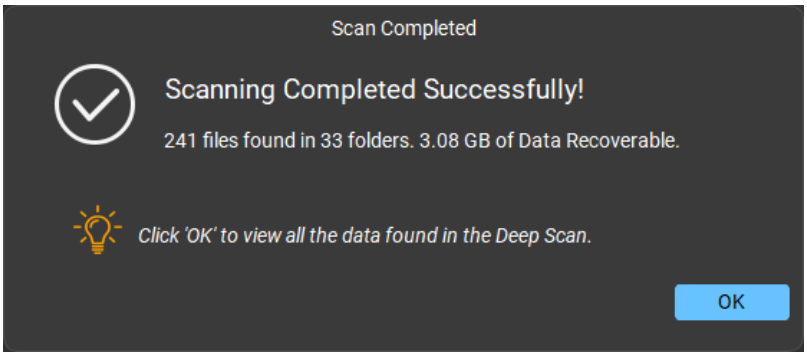


Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *Click* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the scanning process.*

Note: *You can also perform a deep scan after a quick scan by clicking the* ***'Click here'*** *link next to the* ***Deep scan*** *at the bottom of the screen.*

8. Once the scanning process completes, details of the files and folders found would be displayed in a **Scan Completed** dialog box as shown below:



9. **Click OK** button.

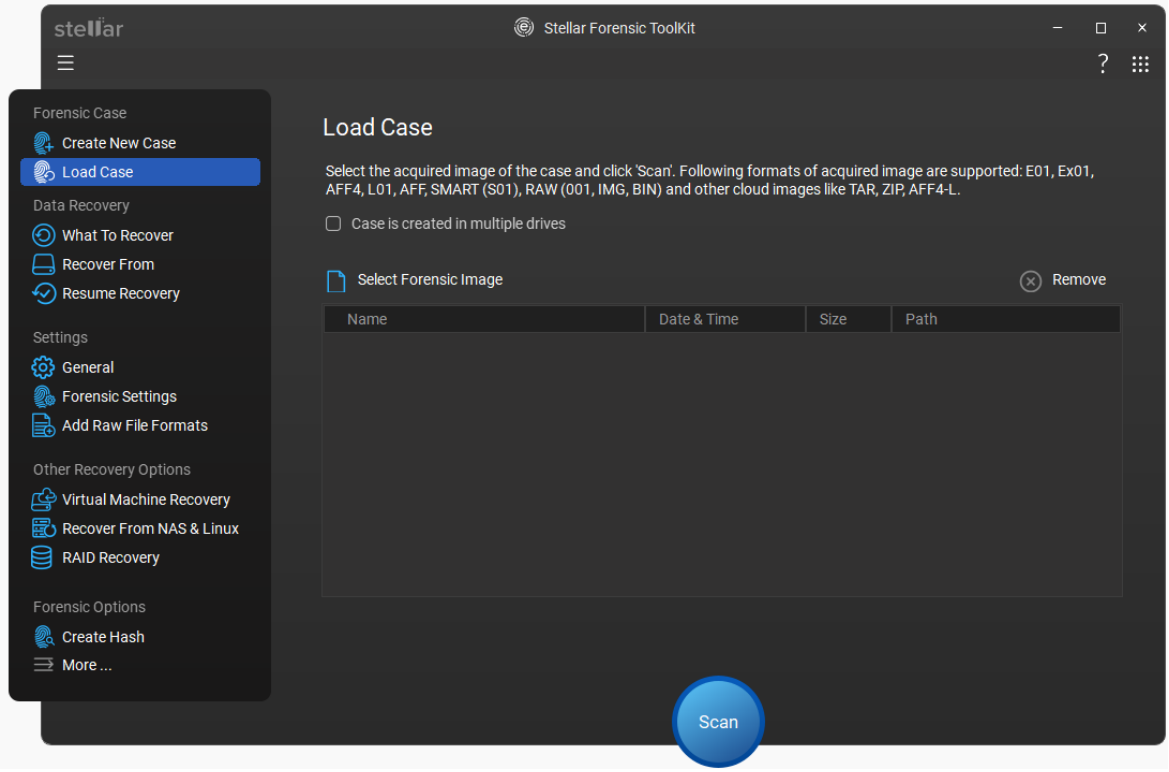
Note: *A forensic report is automatically generated and saved after the recovery process.*

10. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

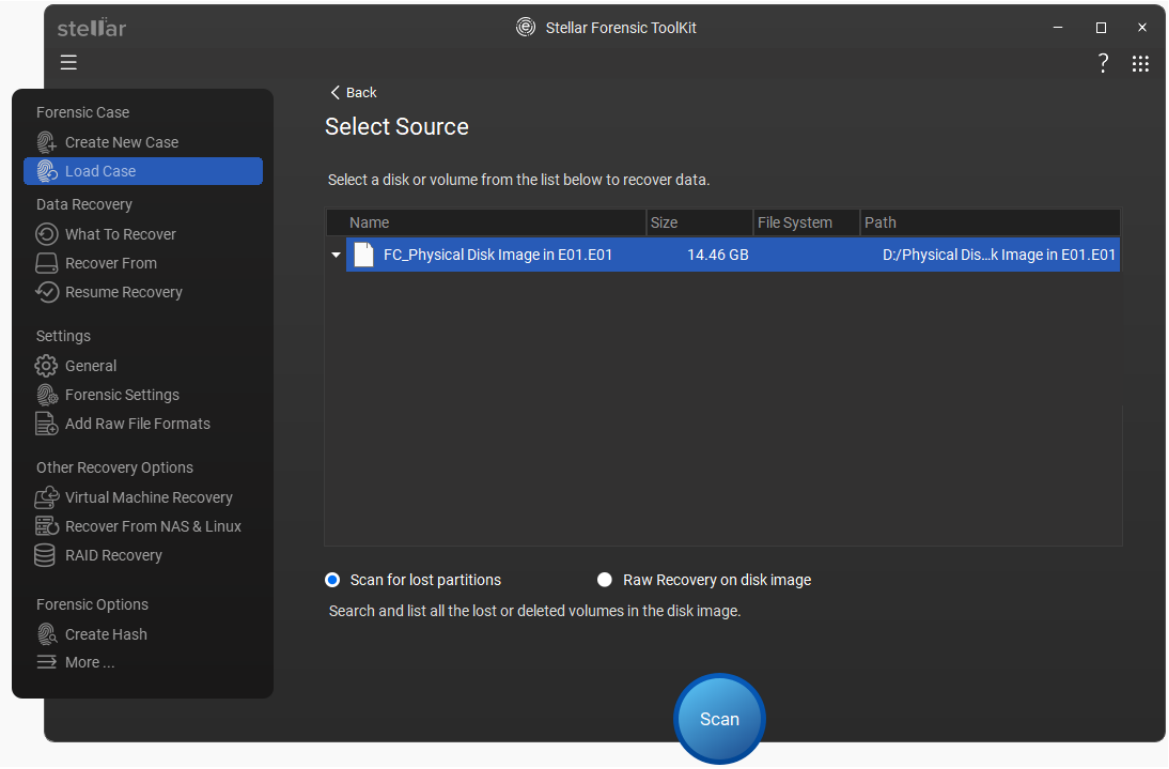
Note: *If you wish to save the scanned information and resume the recovery process at a later stage, see Saving the Scan Information.*

Scan for lost Paritions

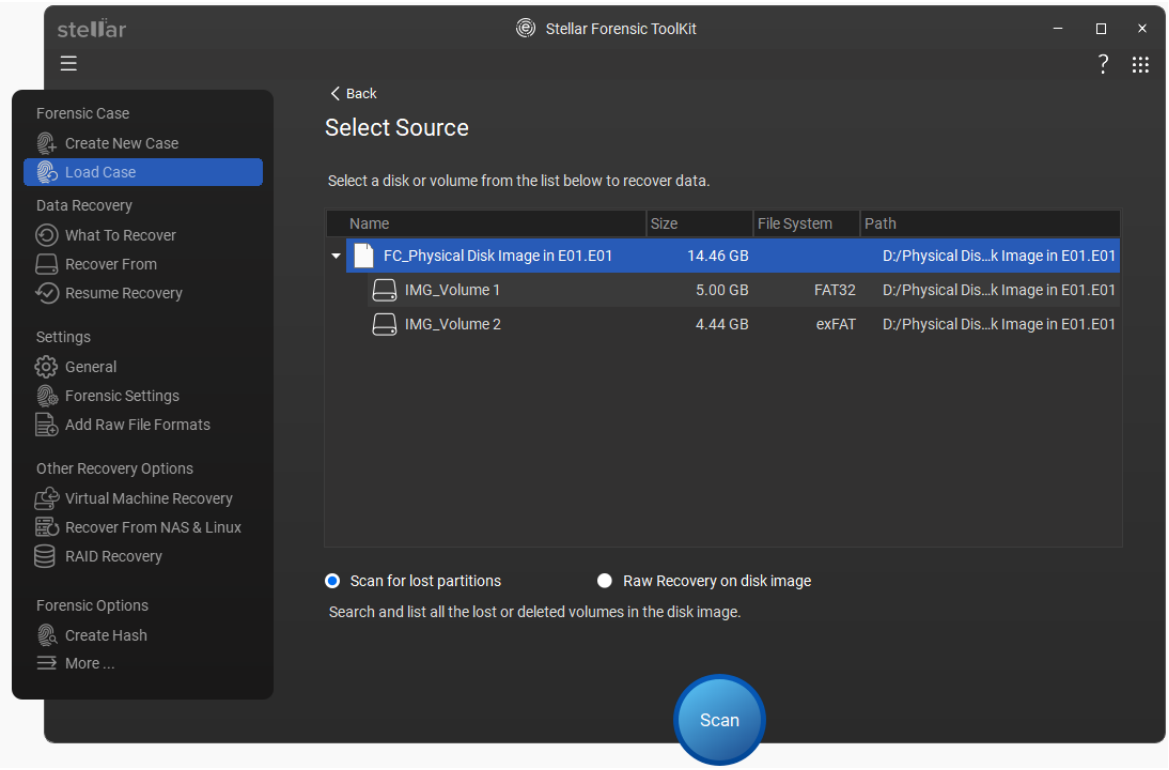
1. On the **Load Case** screen appears, click on **Select Forensic Image** to choose the required image, as given below:



2. The screen will display the image details, including name, creation date and time, size and path, along with case details such as case number, evidence number, examiner name, unique description, notes, etc.

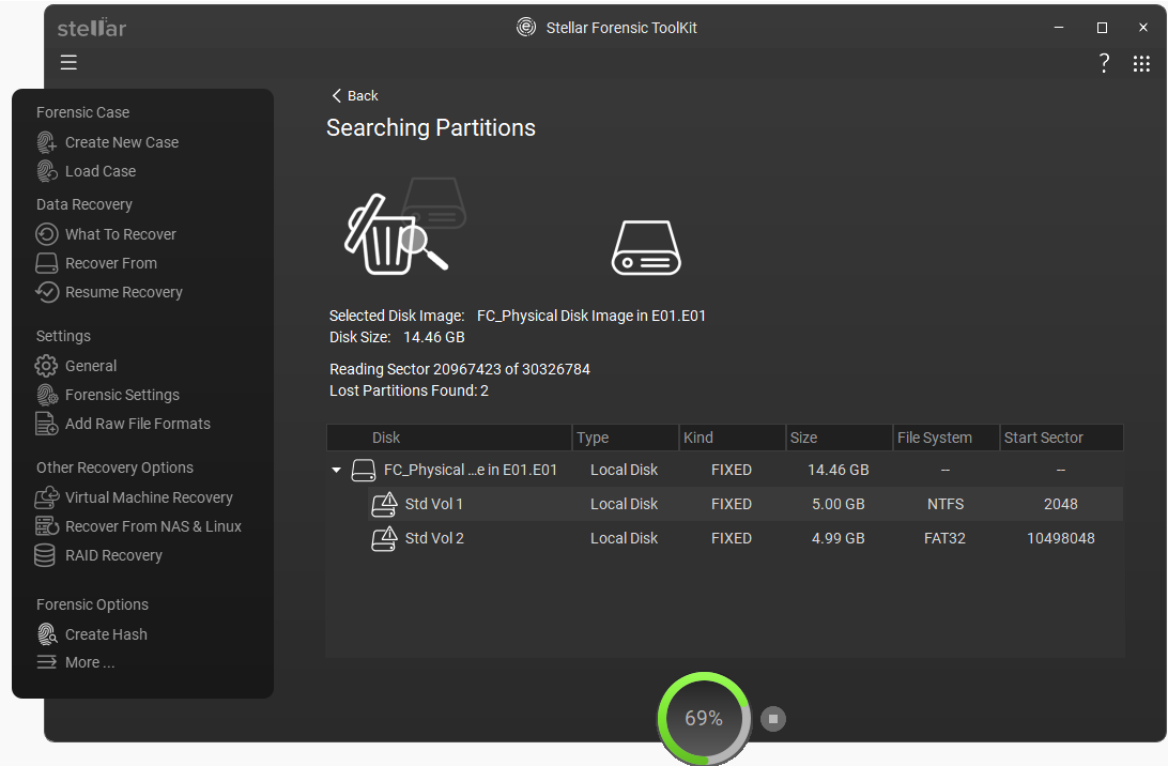


3. Select the disk image. When you select the disk image, two radio buttons such as **Scan for lost Paritions** and **Raw Recovery on disk image** will be displayed on the screen.

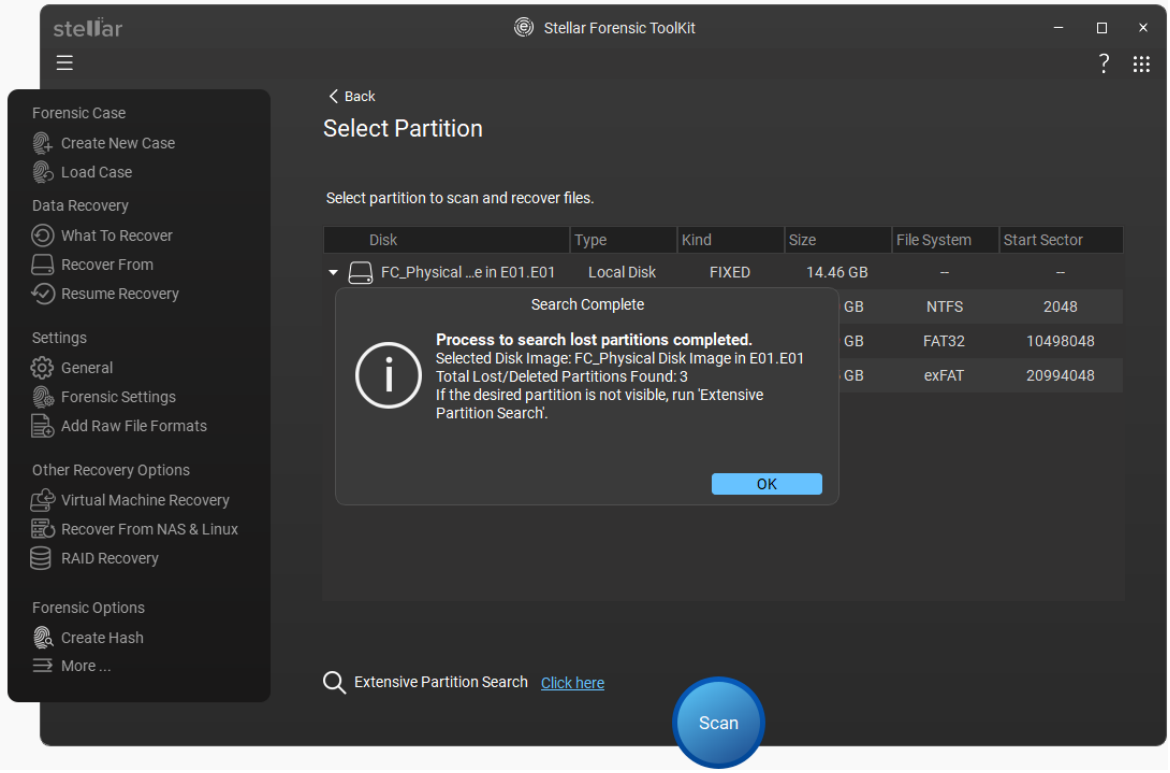


4. Select **Scan for lost Paritions** radio button and then click **Scan**.

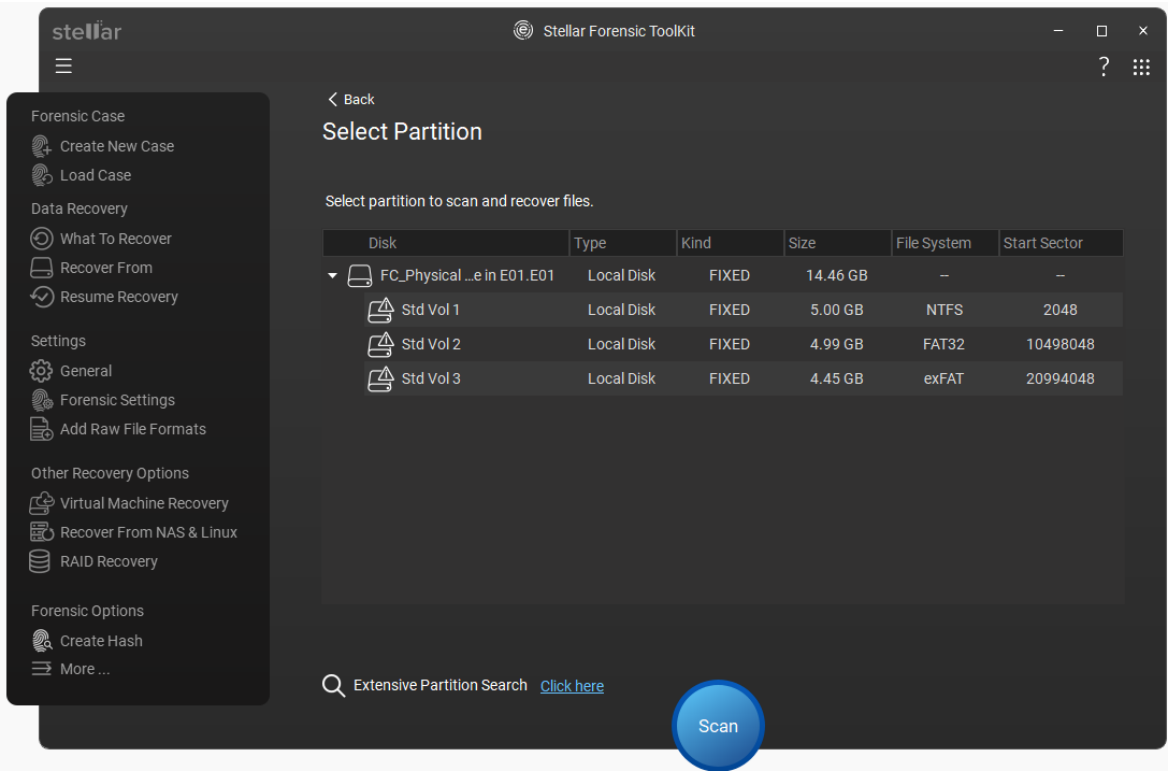
5. **Searching Partitions** window appears that provides the details of all lost partitions found in the selected disk.



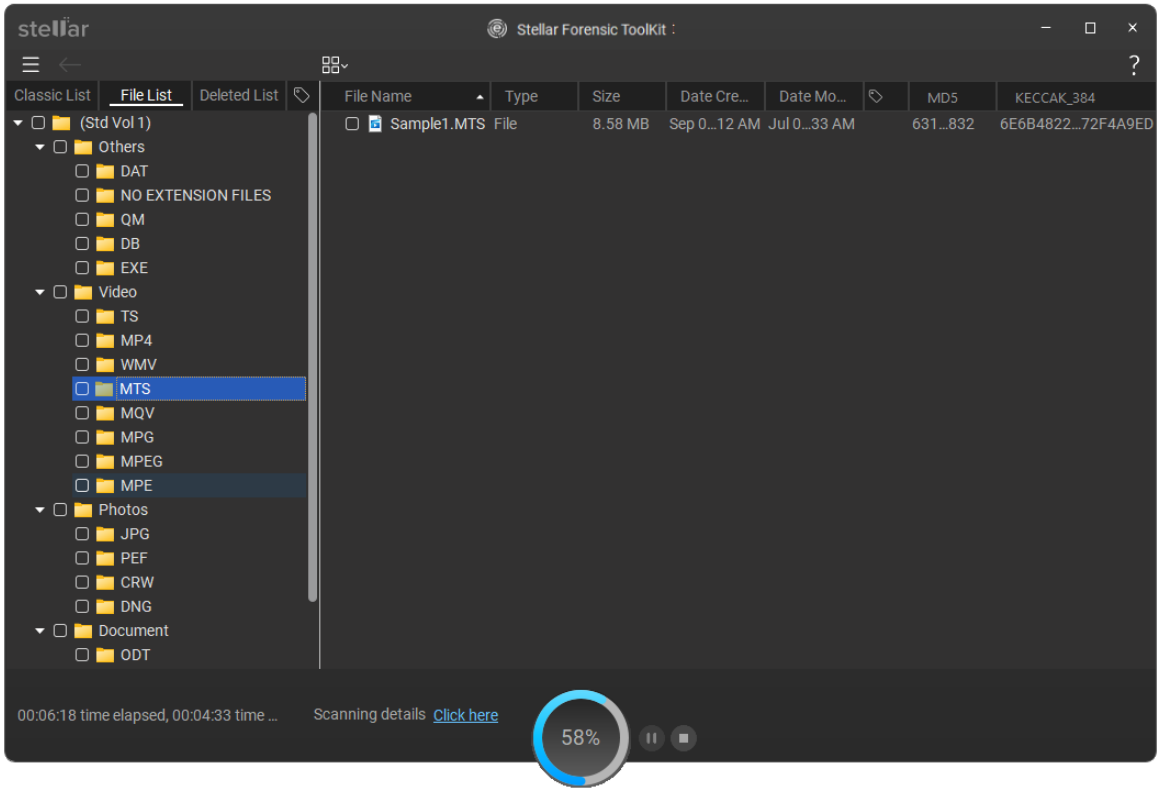
6. **Search Complete** dialog box appears, as given below:



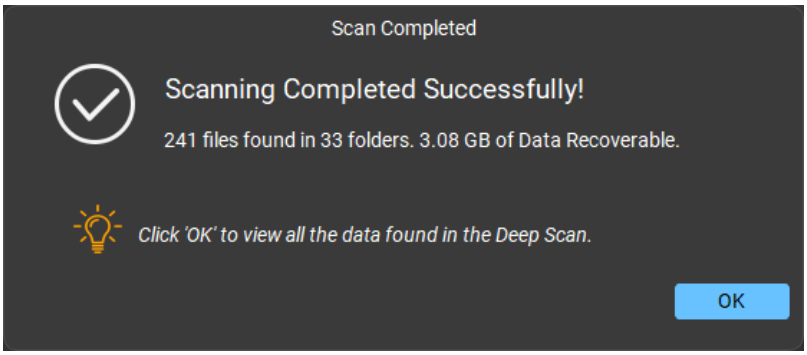
7. Click **OK** to continue.
8. All the partitions that are found will be listed in the **Select Partition** window, as shown below:



9. Click **Scan.**
10. A screen appears that shows the scanning process.



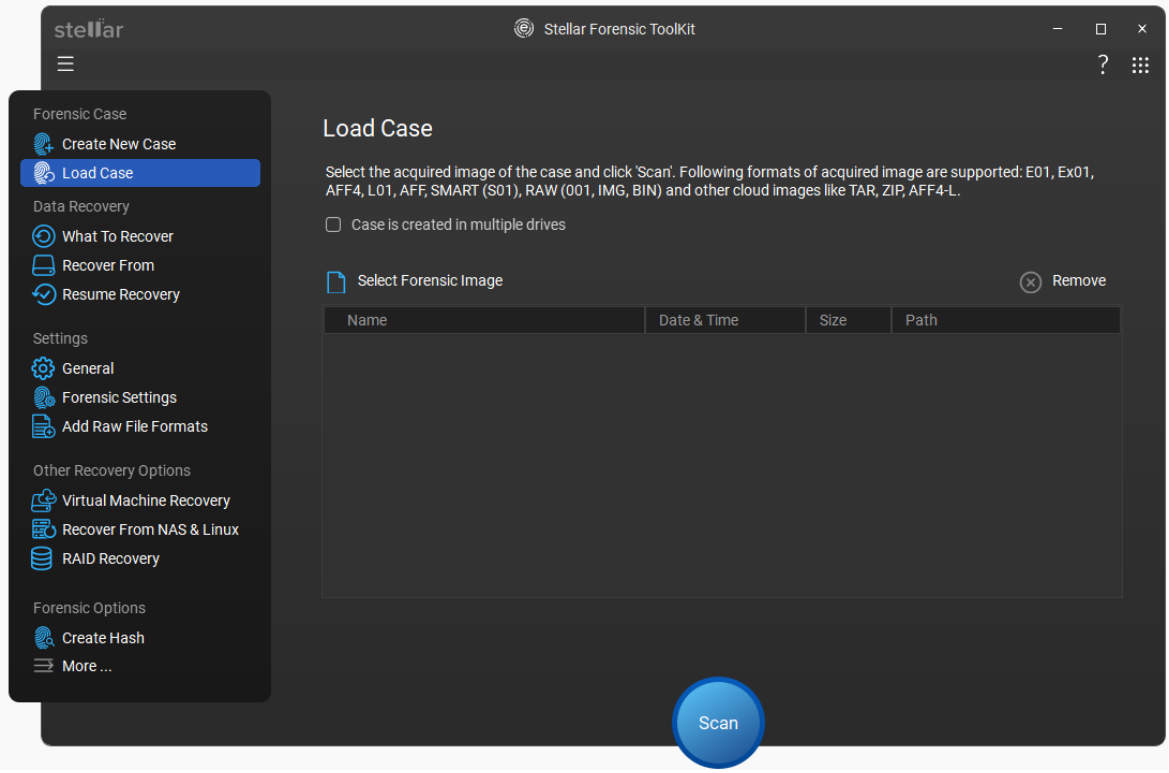
11. Once the scanning process completes, details of the files and folders found would be displayed in a Scan Completed dialog box as shown below:



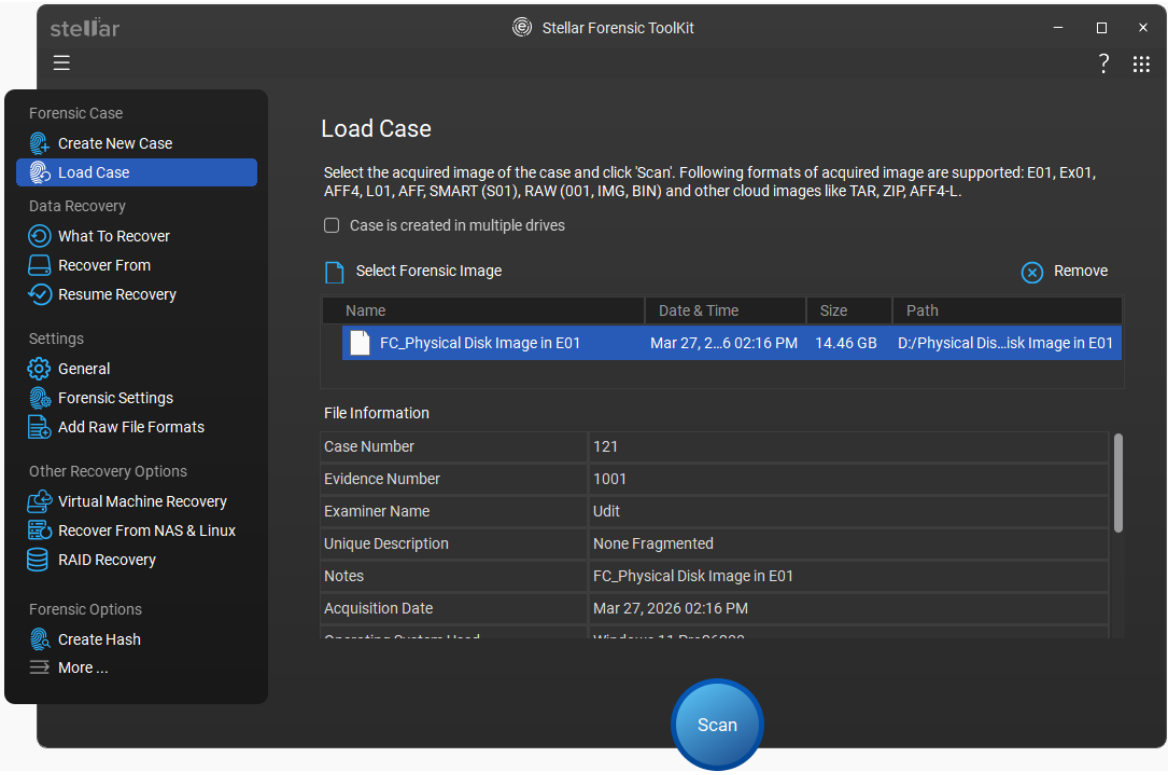
12. **Click OK** button.

Raw recovery on disk image

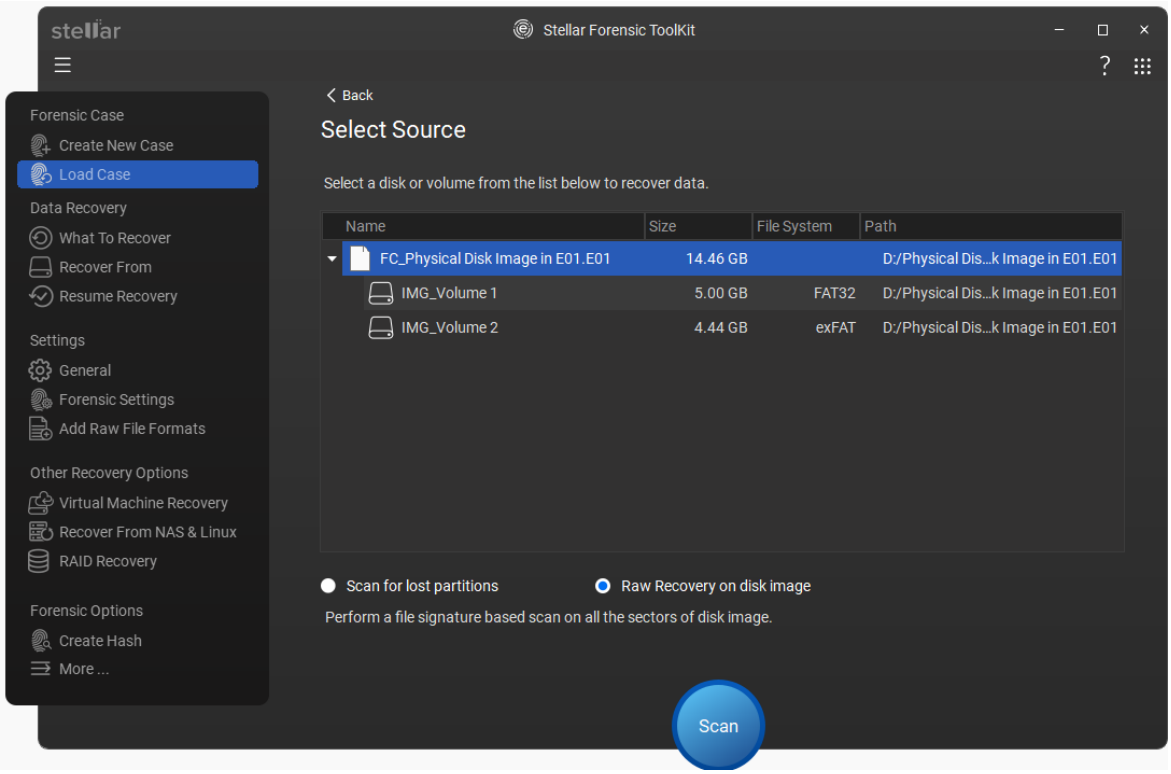
1. On the L**oad Case** screen appears, click on **Select Forensic Image** to choose the required image, as given below:



2. The screen will display the image details, including name, creation date and time, size and path, along with case details such as case number, evidence number, examiner name, unique description, notes, etc. Click **Scan**.

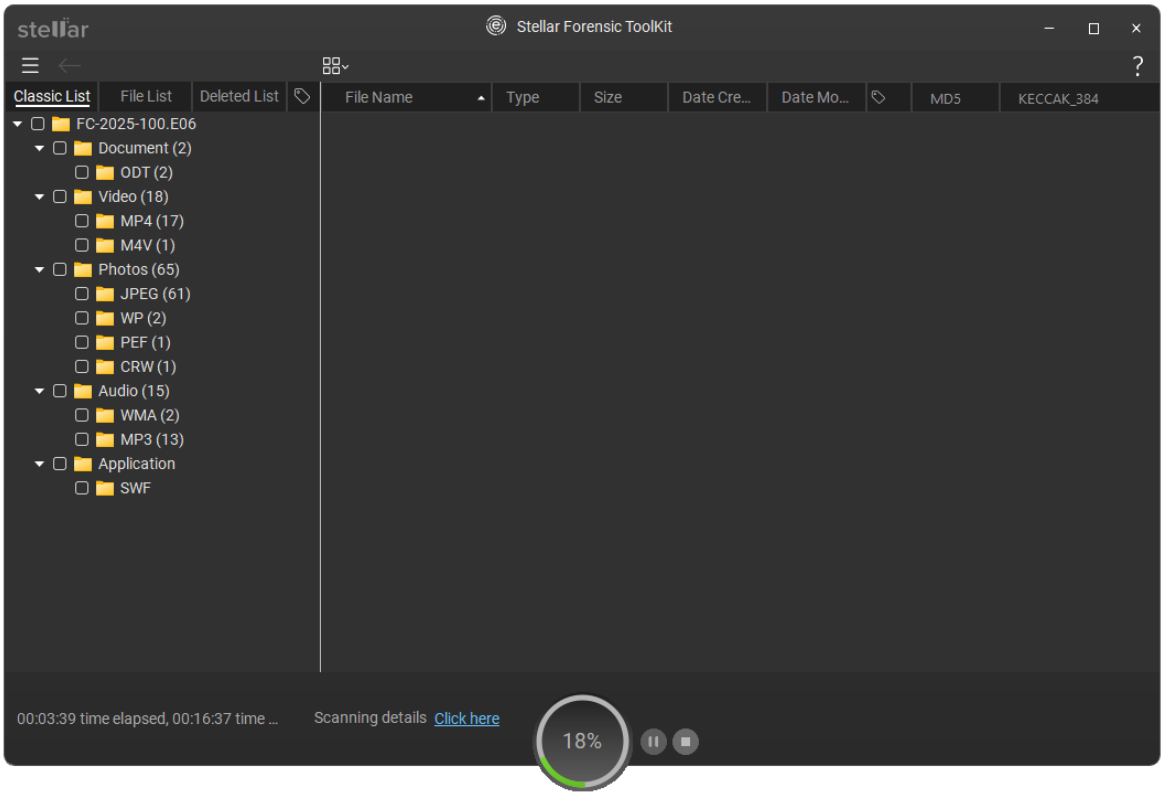


3. On the **Select Source** window, select the **disk** or **volume** from the list **and** then select **Raw Recovery on disk image** radio button.



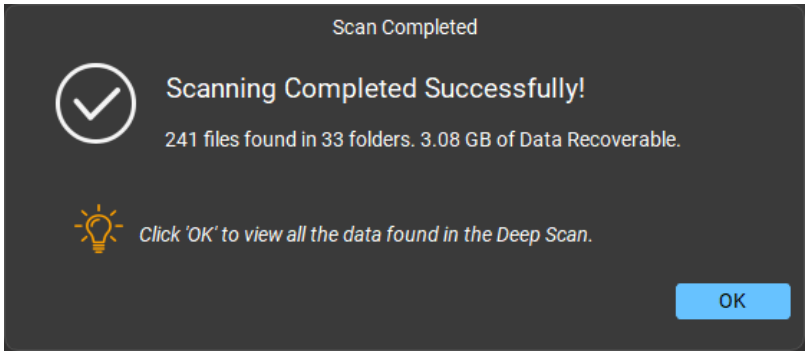
4. Click **Scan.**

5. A screen appears that shows the scanning process.



***Note:** During **Raw Recovery on a disk image**, only the **Classic List** tab will be enabled, while the **File List** and **Deleted List** tabs will remain disabled.*

6. Once the scanning process completes, details of the files and folders found would be displayed in a Scan Completed dialog box as shown below:



7. C**lick OK** button.

8. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

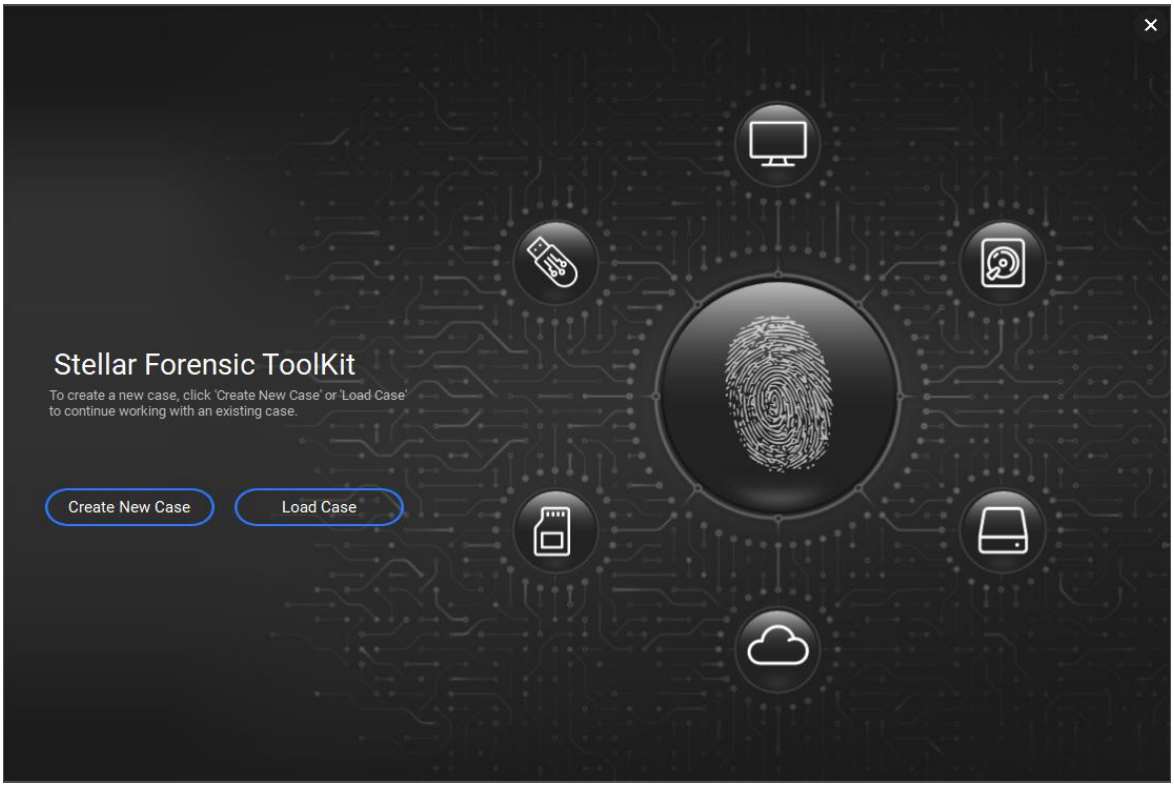
   Note: *If you wish to save the scanned information and resume the recovery process at a later stage, see Saving the Scan Information.*

4.3. Recover Data from Existing Volume

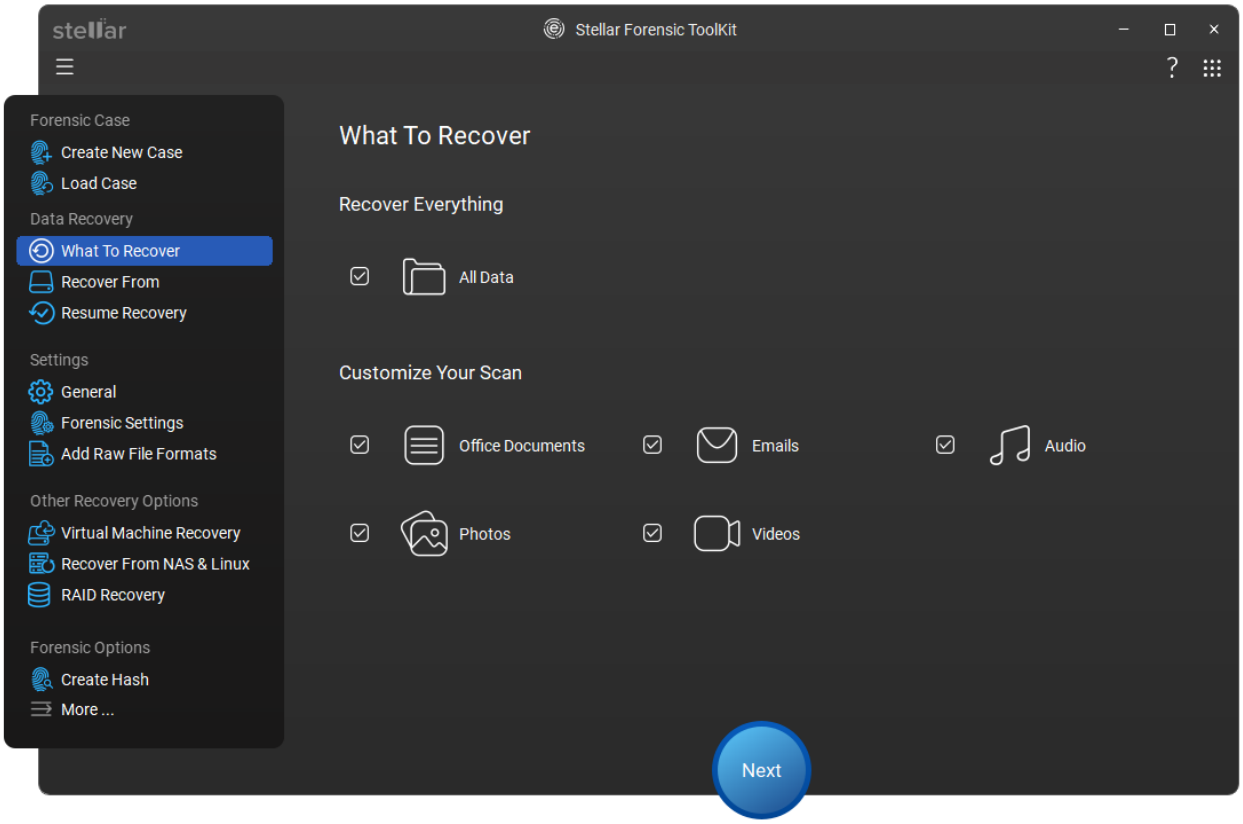
With **Stellar Forensic Toolkit** you can recover your deleted or lost data from the hard drive or external storage media connected to the system. Almost all data of the volume can be found by performing recovery on selected volume or removable media. NTFS, FAT 32, exFAT, Ext2, Ext3, Ext4, Linux, HFS, HFS+, APFS, and BTRFS file systems are supported by the application.

To Scan Existing Volume:

1. Run **Stellar Forensic Toolkit**.
2. From the main screen, select **Create New Case** or **Load Case** button.

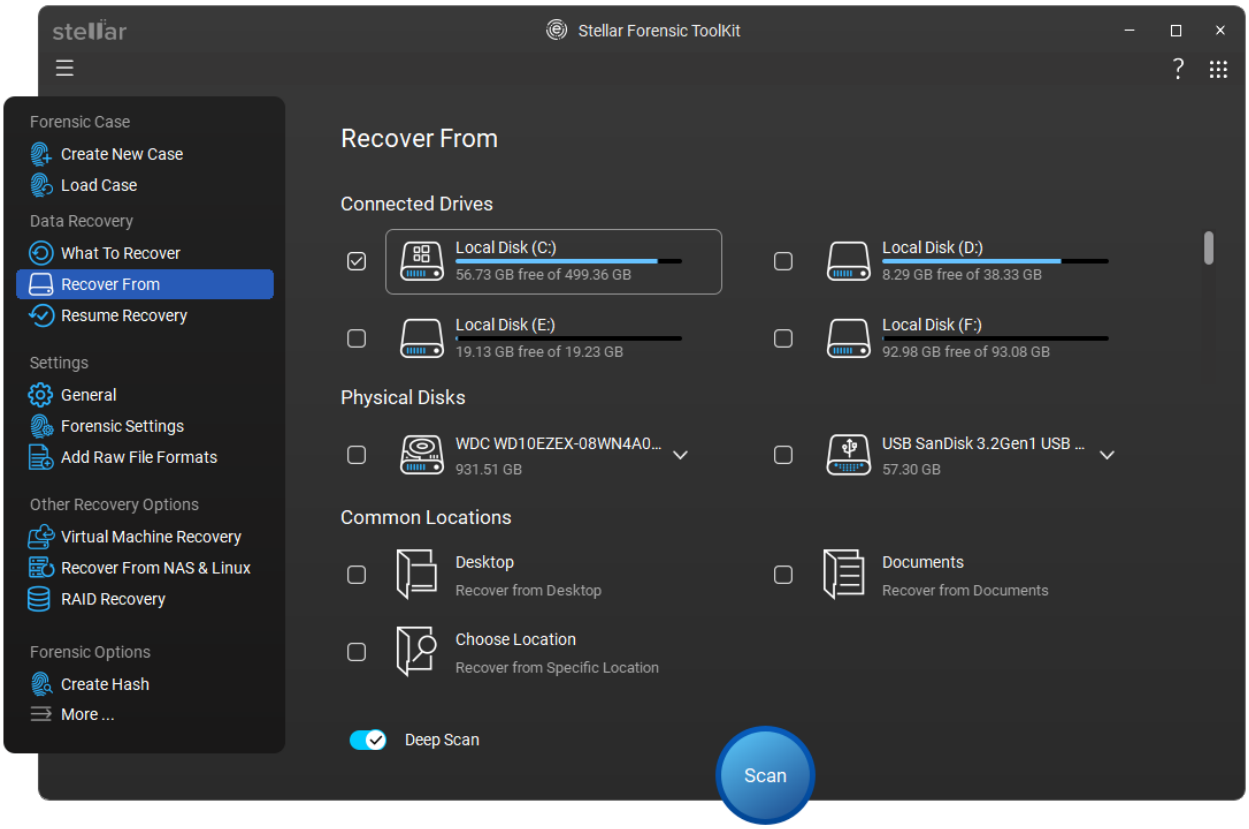


3. From the left navigation menu, go to **Data Recovery** section and click on **What To Recover** . Then, select the type of data i.e. **All Data** or **Office Documents, Emails, Audio, Photos and Videos**, you want to recover.



4. Click **Next**.

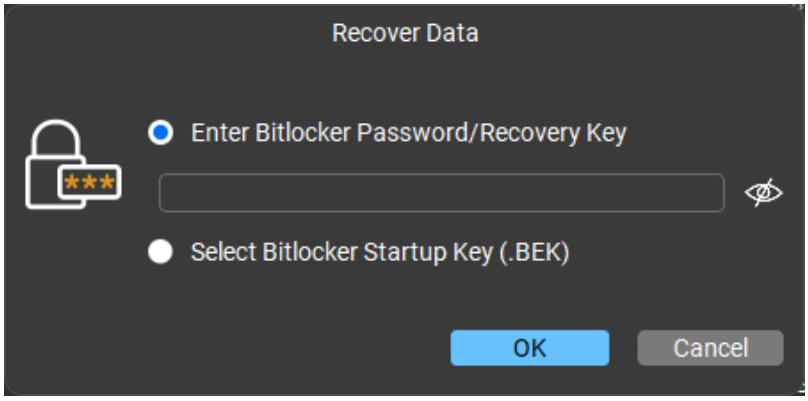
5. From **Recover From** screen, select the existing volume under the **Connected Drives** option from which you want to recover your data.



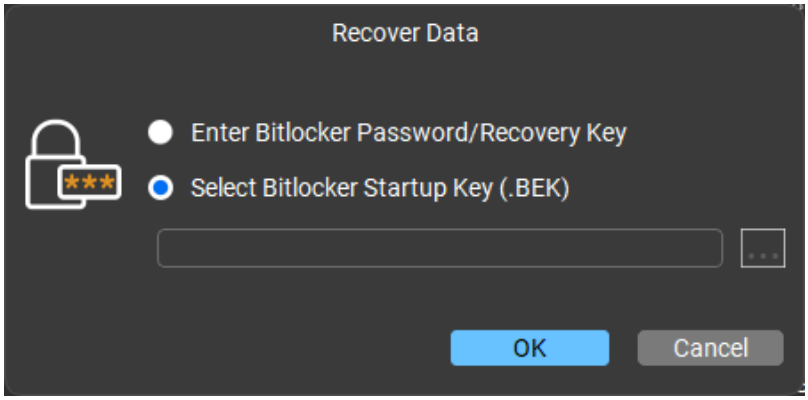
Note: *To run a Quick Scan, turn off the* ***Deep Scan*** *option located at the bottom of the screen.*

Note*: If you are scanning a drive that is encrypted using* ***BitLocker****, you will be prompted to either enter the* ***Bitlocker password/Recovery Key*** *or Select a* ***Bitlocker Startup Key (.BEK file)****. Use any one of the following steps, to initiate the scan process:*

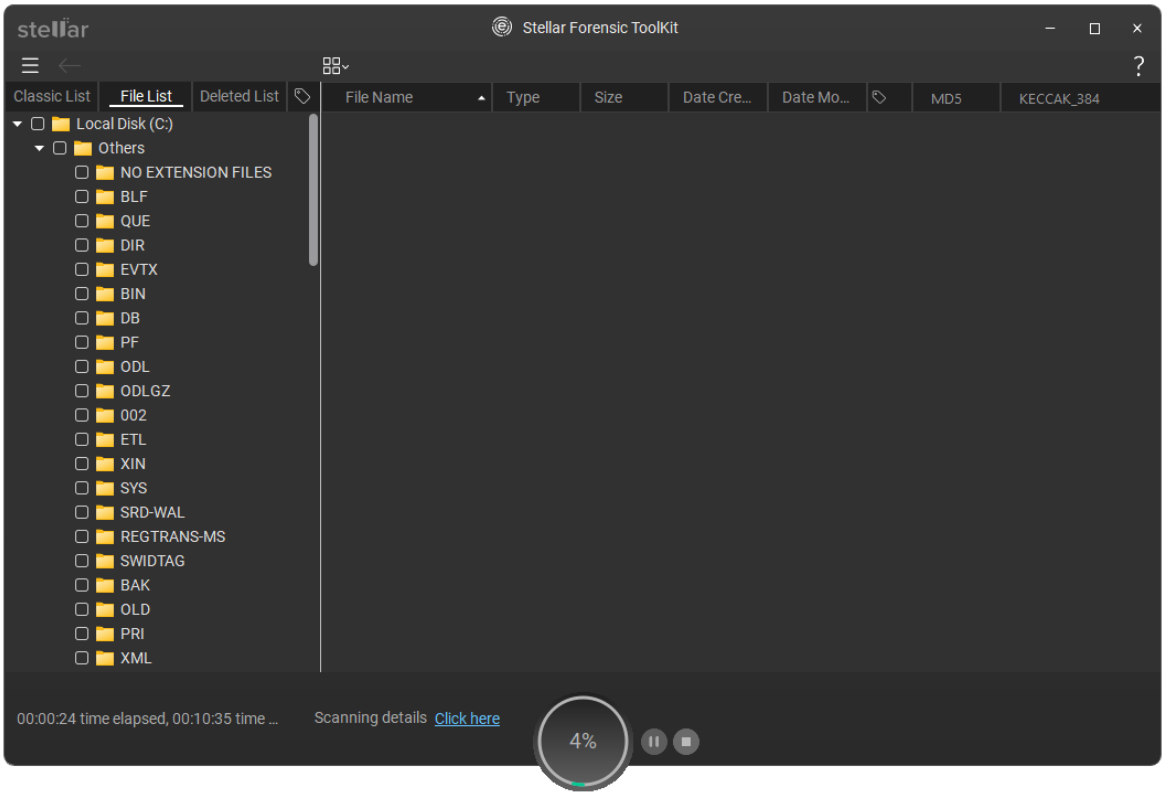
- *Enter the* ***Bitlocker password/Recovery Key*** *in the text box given and click* ***OK****.*



- *Alternatively, choose Select **Bitlocker Startup Key (.BEK)** radio button. Click*  *to browse and select the .BEK file and click **OK**.*



6. Click **Scan**. A screen appears that shows the scanning process.



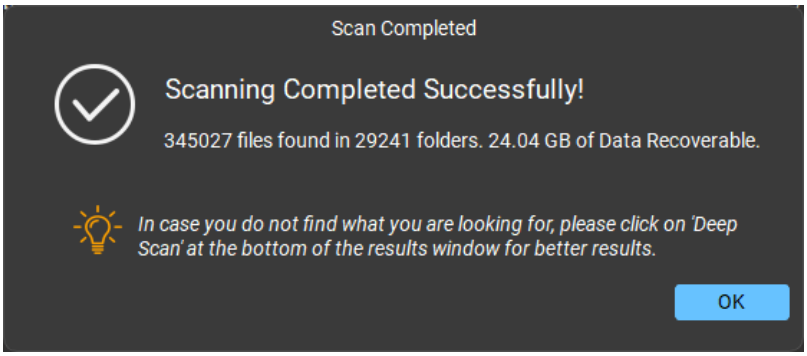
***Note:** To view the scanning details, click the **Click here** link next to the **Scanning details** at the bottom of the screen. To save the scan information once the scanning process is completed, click here.*

***Note:** To stop or resume the scanning process, click **Stop** or **Pause/ Resume** button located at the bottom of the screen.*

Note: *To resume recovery using the saved scan information, click* ***here****.*

Note: *If the quick scan does not find all the lost or deleted files, you can perform a* ***Deep scan*** *to search for more files. To do this, click the '****Click here****' link next to* ***Deep Scan*** *at the bottom of the screen once the scanning is completed.*

7. Once the scanning process is completed, details of the files and folders found are displayed in a dialog box as shown below:



8. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

Note*: If you wish to save the scanned information and resume the recovery process at a later stage, see Save the Scan Information.*

4.4. Recover Data from Lost Drive/Unallocated Partition

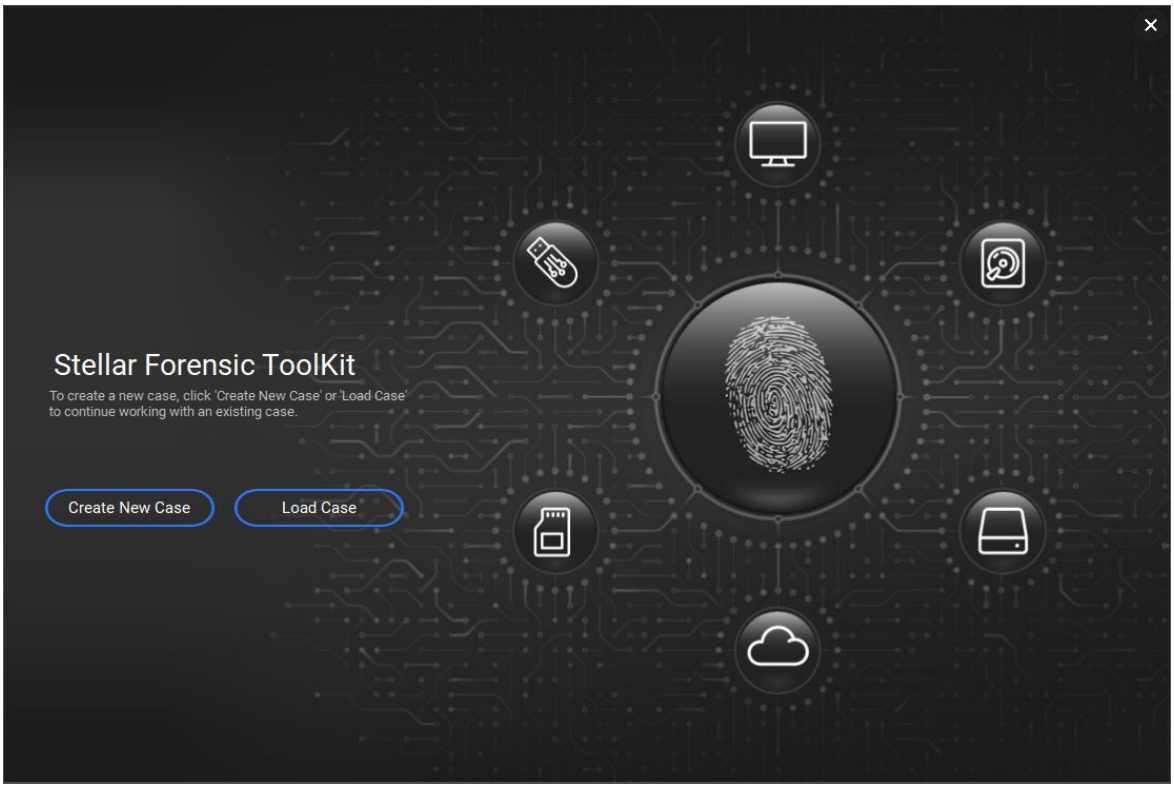
Stellar Forensic Toolkit allows you to locate and recover data from the **Lost Drive/Unallocated Partition** from a connected hard drive. Partition becomes **unallocated/RAW** when a drive letter is not assigned, a partition is accidentally deleted, or a file system is damaged or corrupted. The unallocated partition is not listed under the drives on the PC therefore you cannot access any file from this partition.

With using **Stellar Forensic Toolkit** you can recover your lost data from unallocated space and access your files and folders easily. This function works on **Raw Recovery** to recover the lost data from unallocated partition.

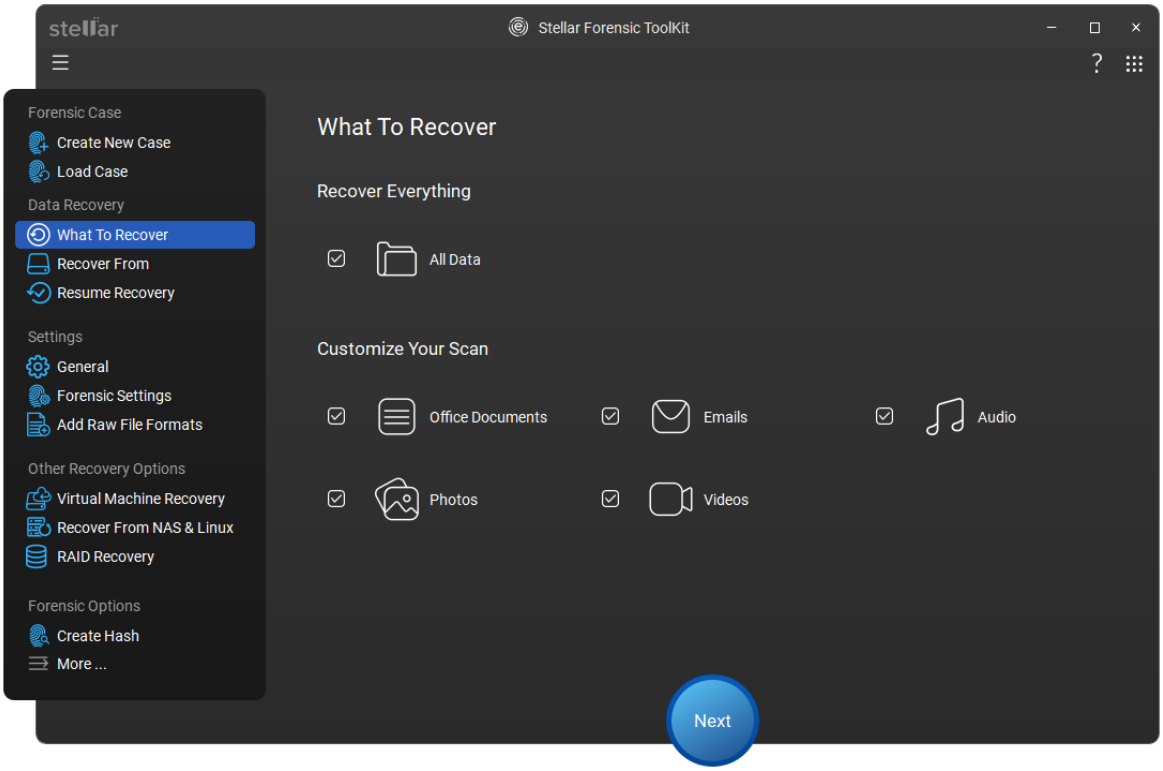
Steps to recover data from Lost Drive:

1. Run **Stellar Forensic Toolkit.**

2. From the main screen, select **Create New Case** or **Load Case** button.

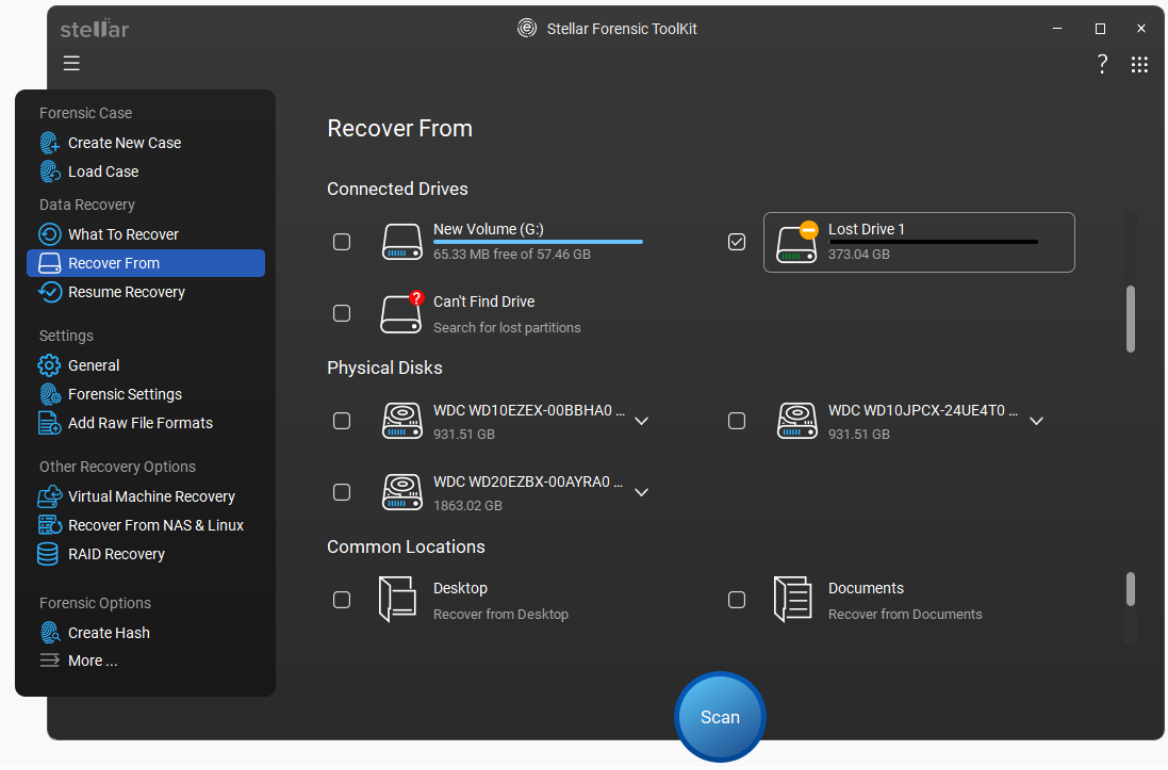


3. From the left navigation menu, go to **Data Recovery** section and click on **What To Recover**. Then, select the type of data i.e. **All Data** or **Office Documents, Emails, Audio, Photos** and **Videos**, you want to recover.



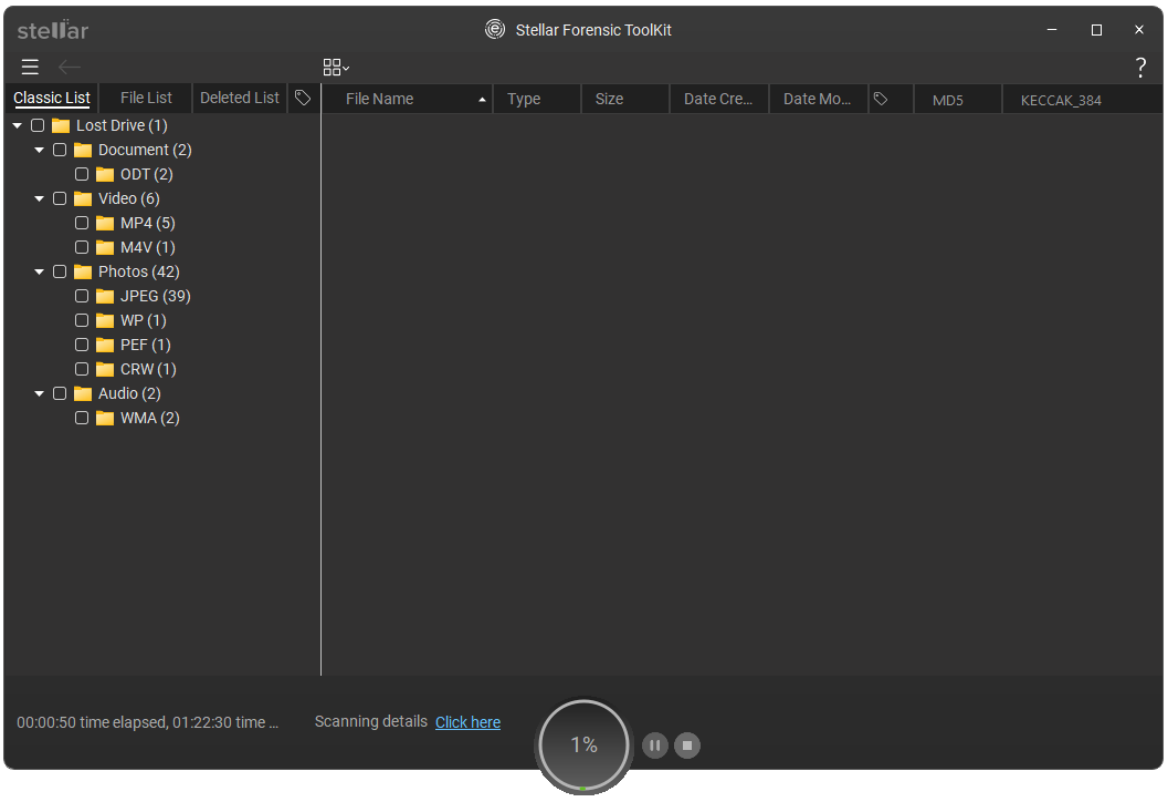
4. Click **Next**.

5. On **Recover From** screen, select **Lost Drive** from the **Connected Drives** section.



Note: *When there are multiple unallocated spaces on a hard disk, it will appear under* ***Connected Drives*** *as* ***Lost Drive 1****,* ***Lost Drive 2*** *and so on. You can select only one* ***Lost Drive*** *at a time for recovery.*

6. Click **Scan**. A screen appears that shows the scanning process.



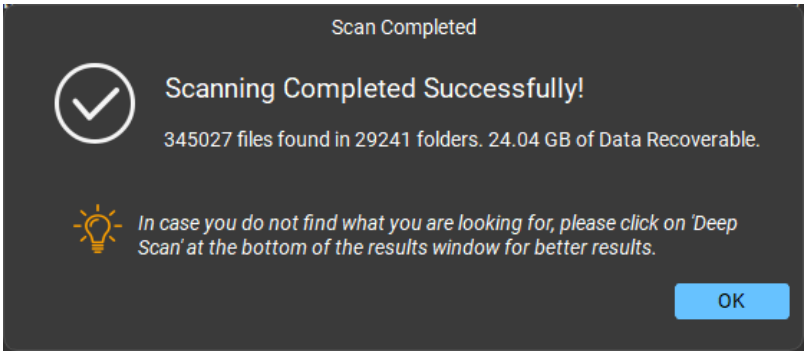
Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *Click* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the scanning process.*

Note: *To resume recovery using the saved scan information, click here.*

Note: *You can also initiate the deep scan process, once the scan of the selected hard drive volume is complete, click the* ***"Click Here"*** *next to* ***Deep Scan*** *at the bottom of the screen.*

7. Once the scanning process is completed, details of the **files** and **folders** found are displayed in a dialog box as shown below:



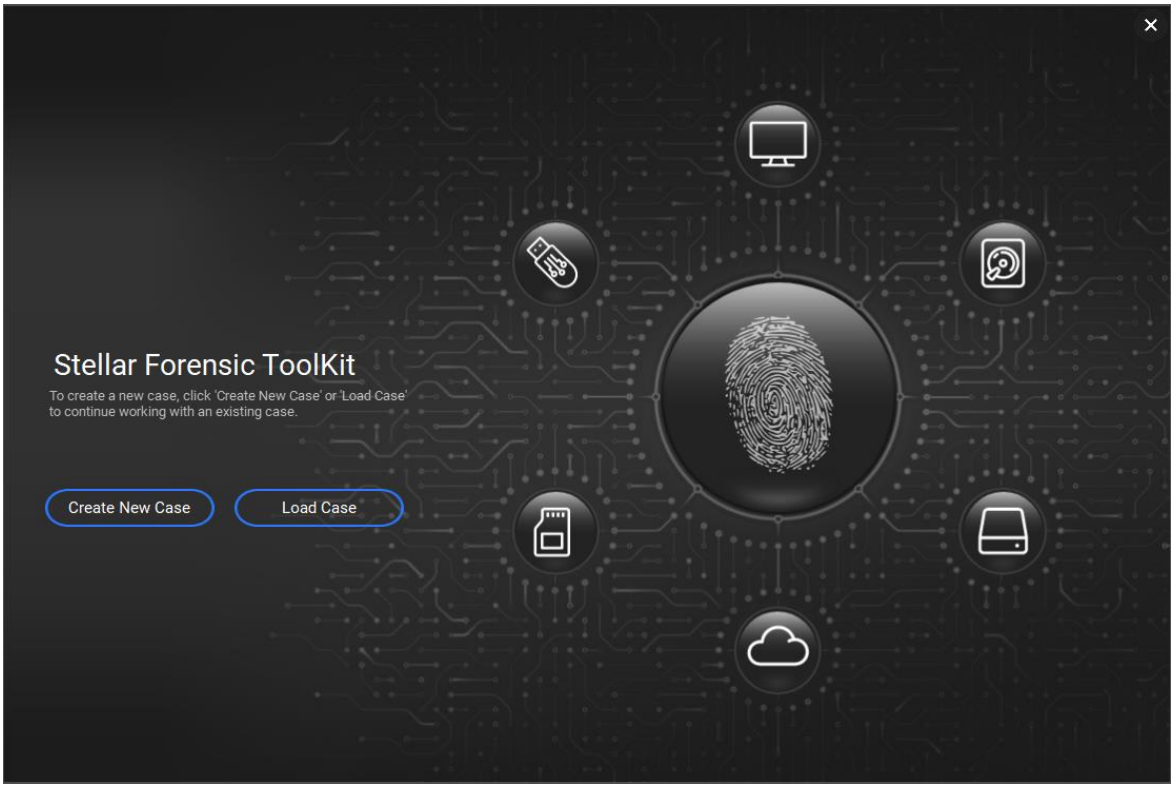
8. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

4.5. Recover Data from CD/DVD

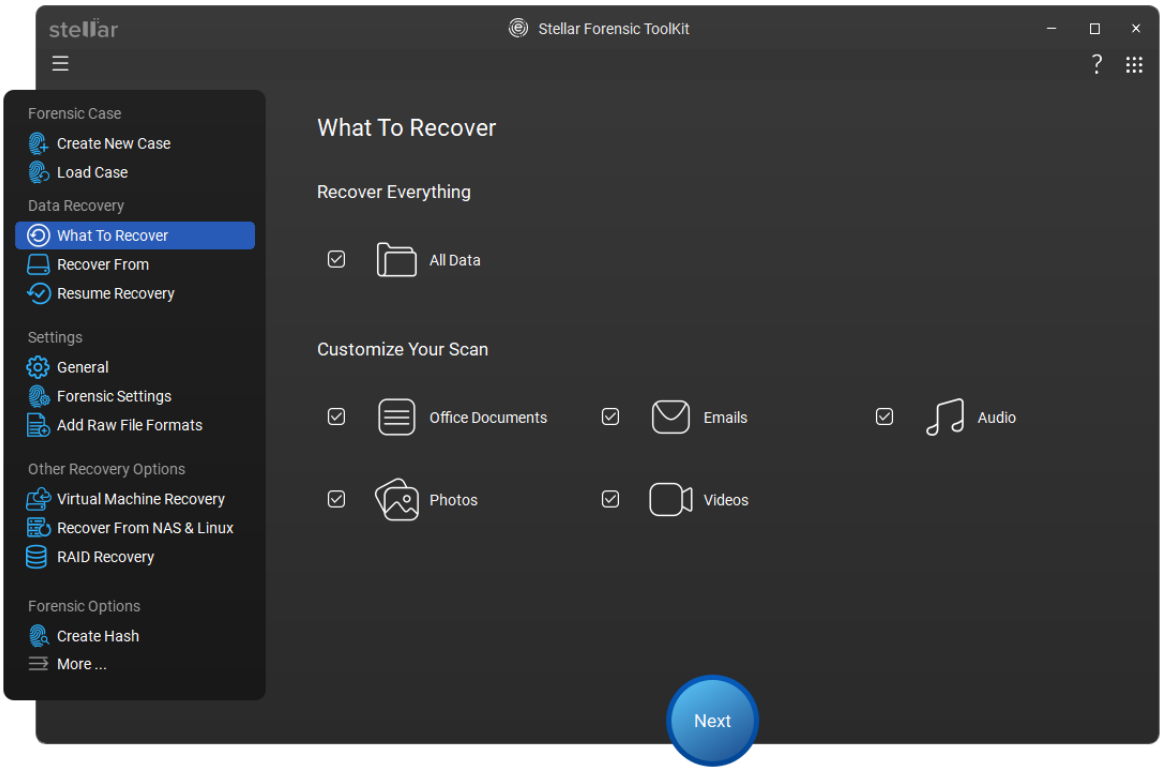
A CD/DVD disk might become unreadable or corrupt due to a number of factors, such as heat, dust, scratches on the disk. **Stellar Forensic Toolkit** can recover data from damaged CD-ROM, CD-RW, DVD and DVD-RW discs. **Stellar Forensic Toolkit** supports recovery from corrupt optical media disks burnt on Windows, Linux, UNIX, and Macintosh systems. The application performs a scan on the selected optical media for recovery.

To scan CD/DVD:

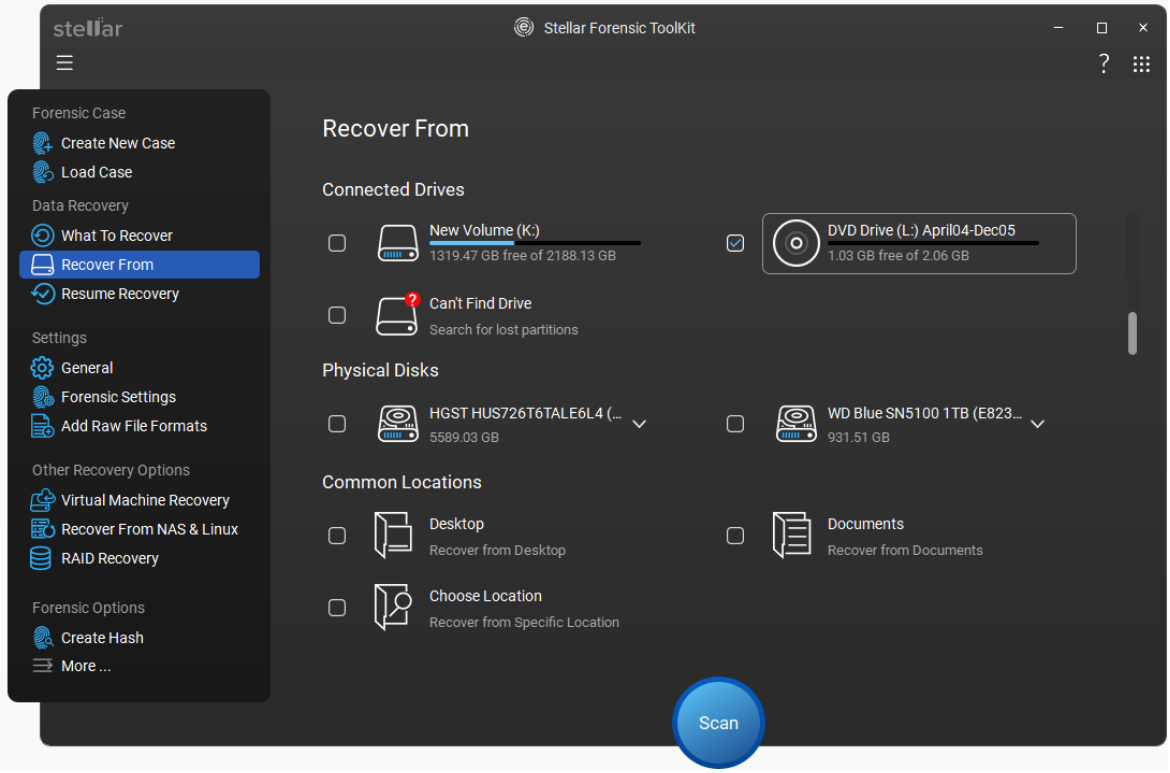
1. Run **Stellar Forensic Toolkit**.
2. From the main screen, select **Create New Case** or **Load Case** button.



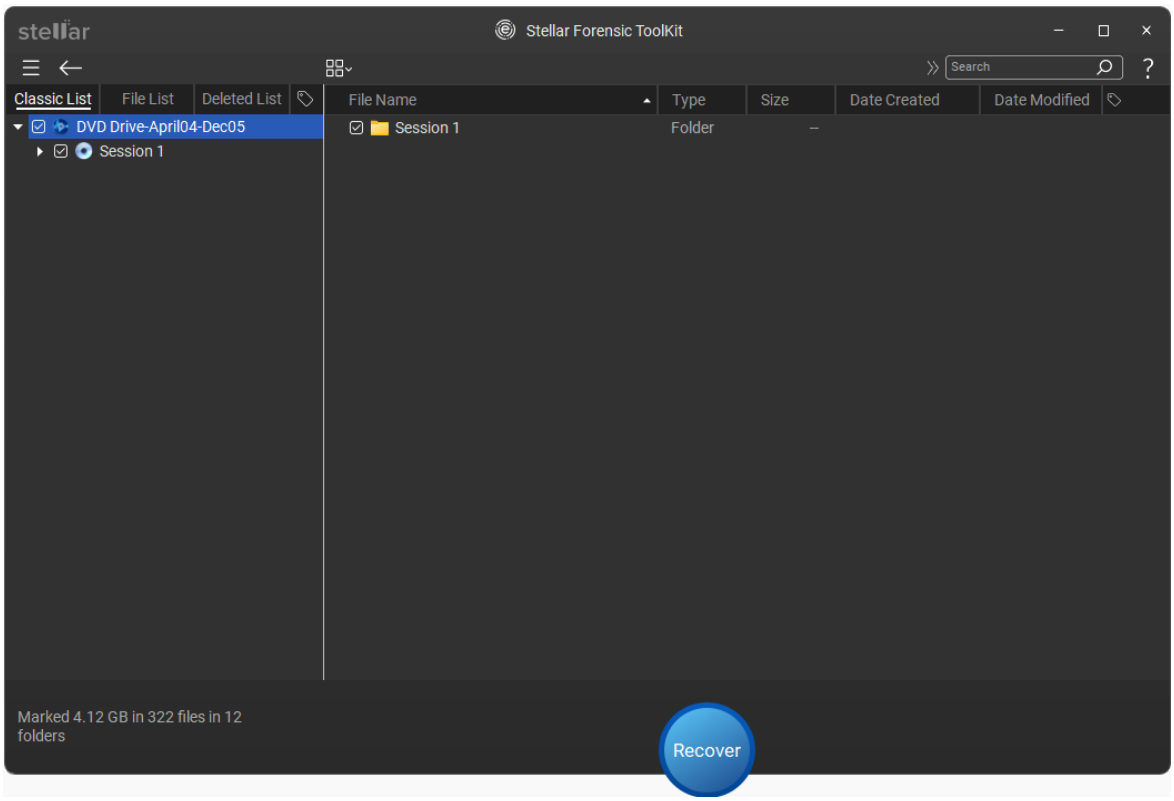
3. From the left navigation menu, go to **Data Recovery** section and click on **What To Recover** . Then, select the type of data i.e. **All Data** or **Office Documents, Emails, Audio, Photos and Videos**, you want to recover.



4. Click **Next**.
5. From **Recover From** screen, select the connected CD/DVD drive from **Connected Drives**.



6. Click **Scan**. A screen appears that shows the scanning process.

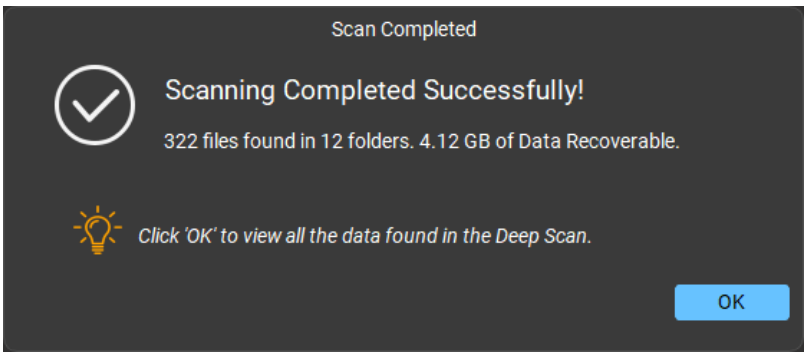


Note: *To view the scanning details, click the* ***Click here*** *link at the bottom of the screen.*

Note: *Click* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the scanning process.*

Note: *You can also initiate the deep scan process, once the scan of the selected hard drive volume is complete, click the* ***"Click Here"*** *next to* ***"Deep Scan"*** *at the bottom of the screen.*

7. Once the scanning process is completed, details of the **files** and **folders** found are displayed in a dialog box as shown below:



8. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

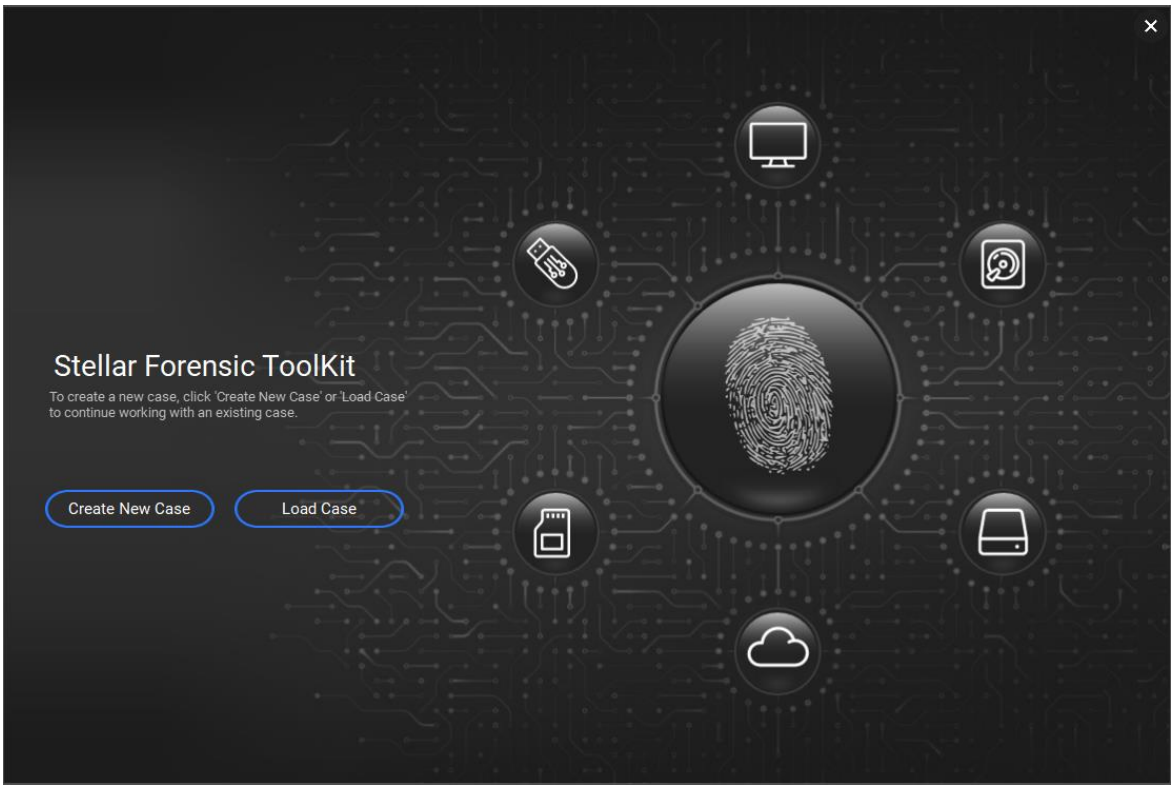
Note: *You can select only one CD/DVD at a time for recovery.*

4.6. Recover a Lost Partition

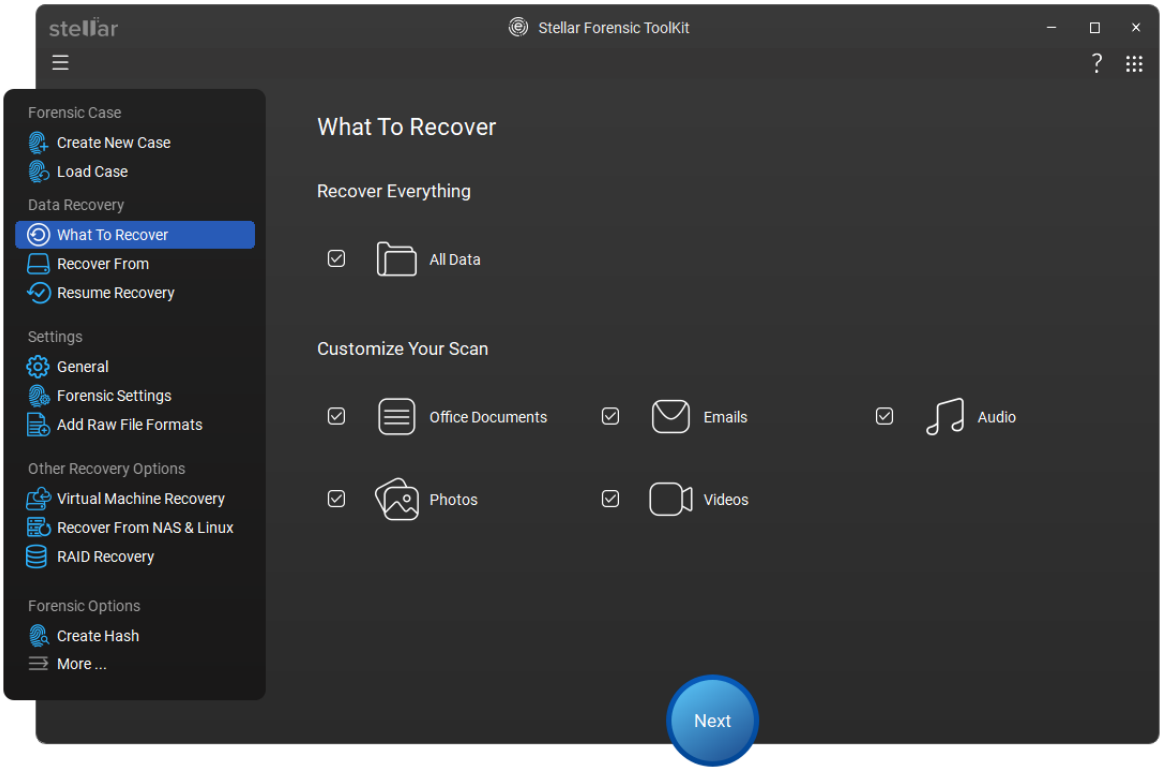
Stellar Forensic Toolkit allows you to search and recover data from lost and deleted partitions of a hard disk. You should use this option to recover data from an accidentally deleted partition. This option will search and list all the deleted and lost partitions in the hard disk along with existing volumes.

To recover lost partition:

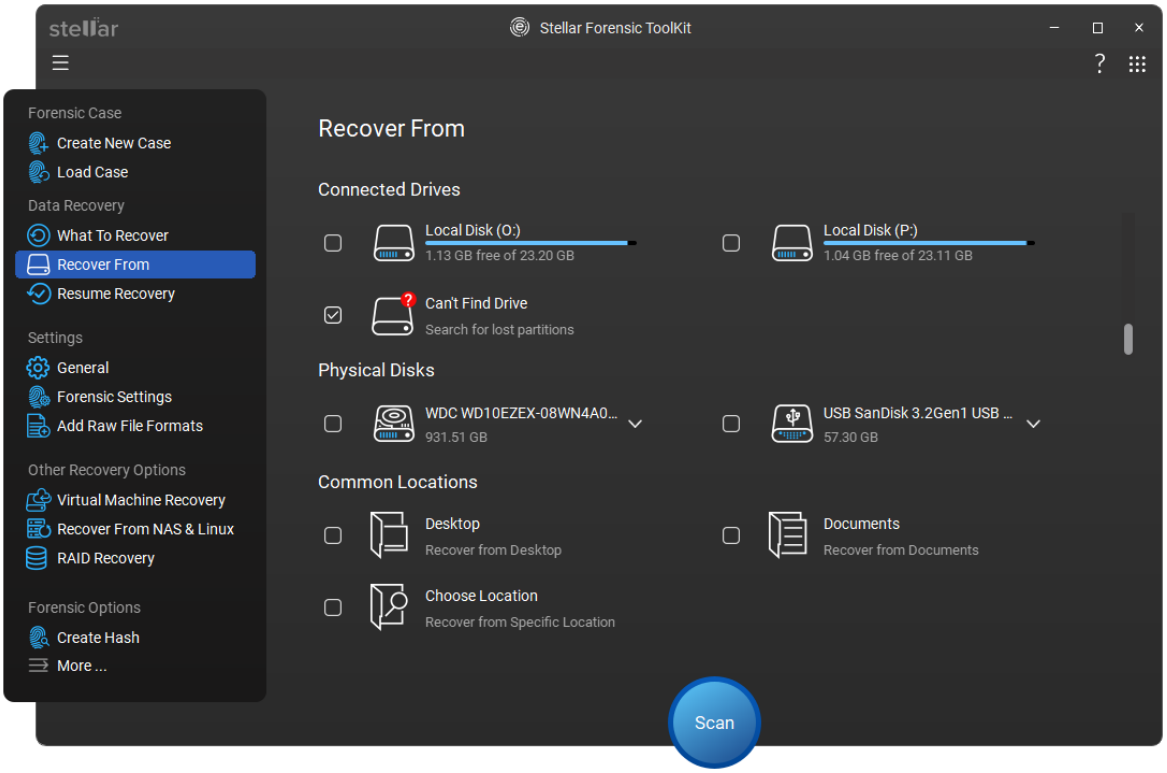
1. Run **Stellar Forensic Toolkit**.
2. From the main screen, select **Create New Case** or **Load Case** button.



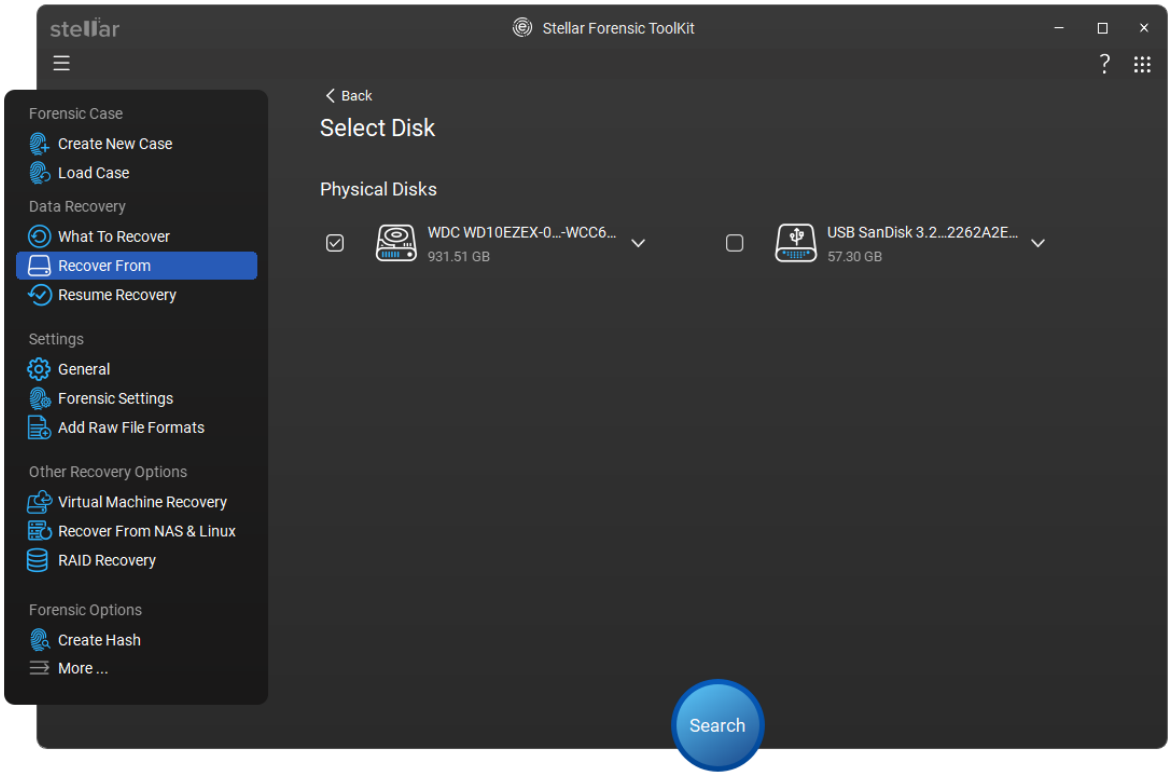
3. From the left navigation menu, go to **Data Recovery** section and click on **What To Recover**. Then, select the type of data i.e. **All Data** or **Office Documents, Emails, Audio, Photos** and **Videos**, you want to recover.



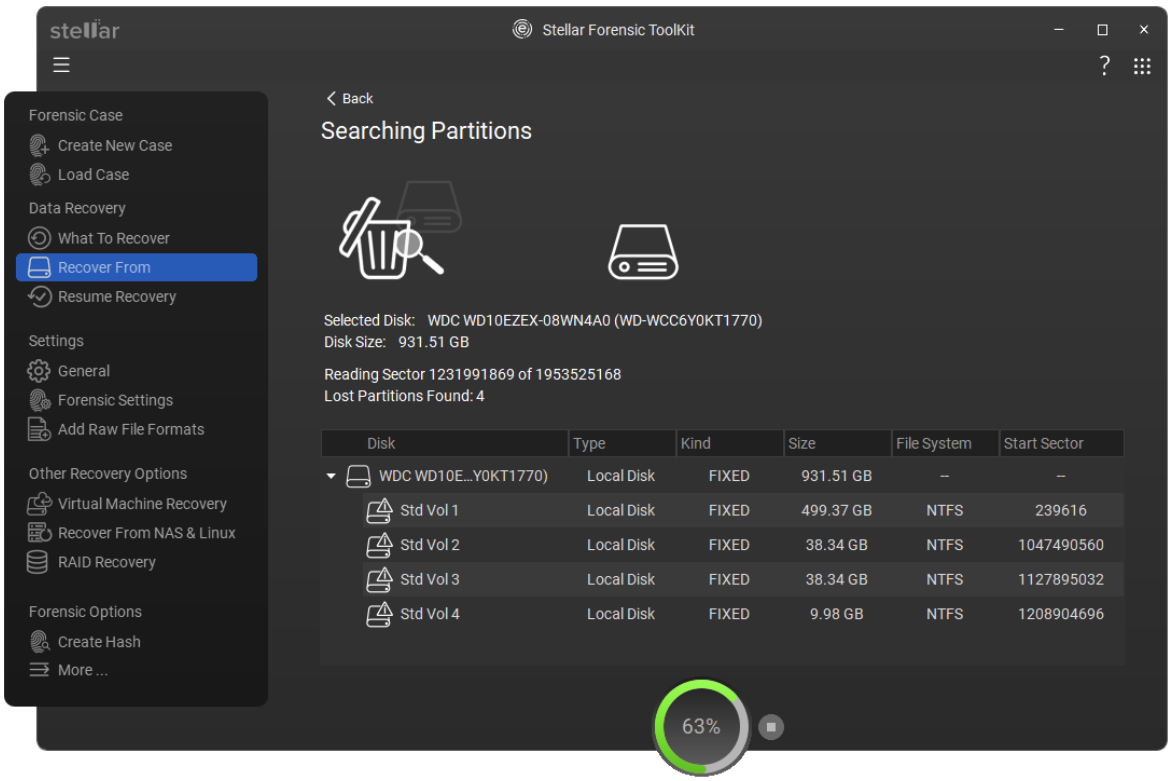
4. Click **Next**.
5. From **Recover From** screen, select **Can't Find Drive** from **Connected Drives**.



6. Click **Scan**. The following screen is displayed.

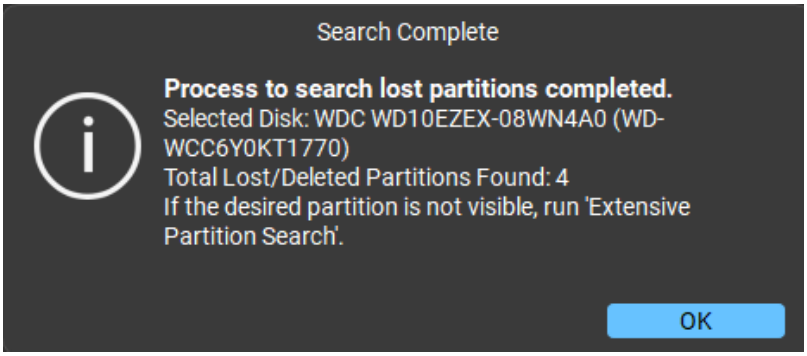


7. In the **Select Disk** window, all connected hard drives are displayed under the **Physical Disks** section, along with detailed information about each drive. From this window, choose a hard drive you want to scan for lost partitions and click **Search**. A scan for lost or deleted partitions will be performed in the selected disk or drive.

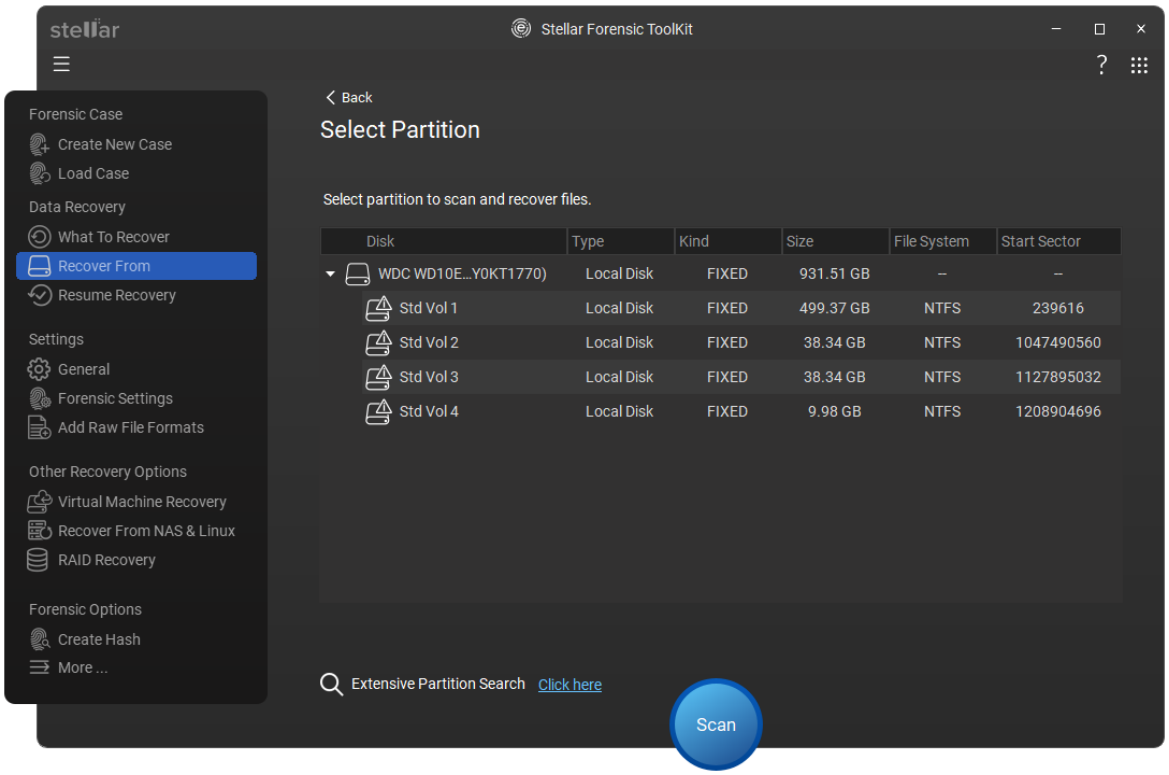


8. **Searching Partitions** window appears that provides the details of all lost partitions found in the selected disk.

9. **Search Complete** dialog box will appear showing the number of partitions found in the selected disk. Click **OK**.

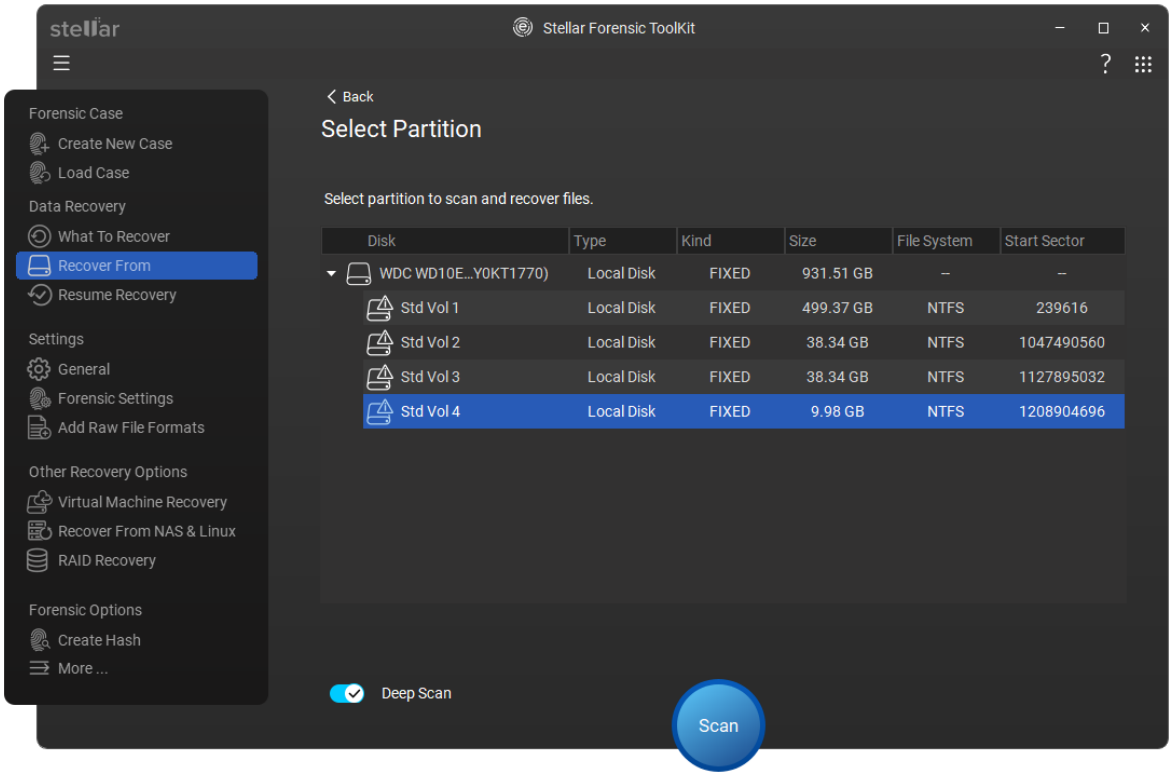


10. All the partitions that are found will be listed in the **Select Partition** window under **Select partition to scan and recover files** section as shown below:



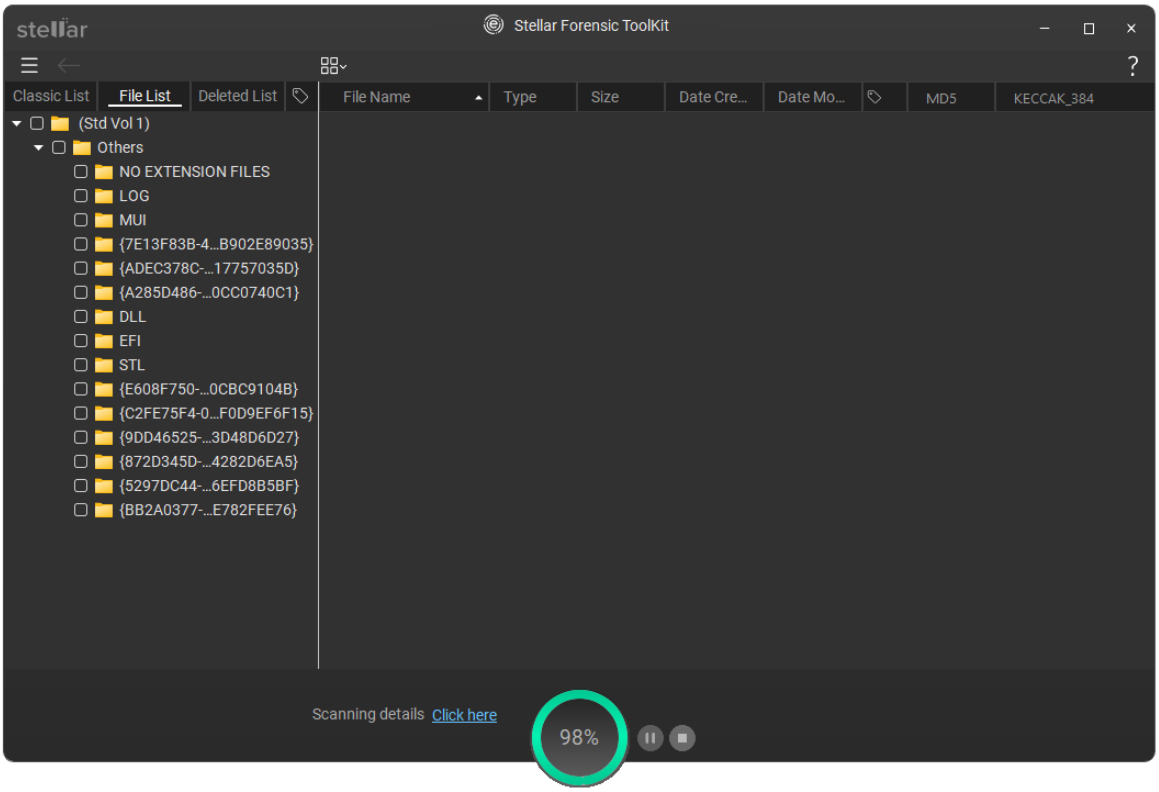
Note: *If the desired partition is not visible, click on* ***Click here*** *link next to the* ***Extensive Partition Search*** *given at the bottom of the screen. Click on disk to enable the* ***Extensive Partition Search.***

11. From the list of partitions found, select any desired partition.



Note: *Once you select the desired partition,* ***Deep Scan*** *option becomes available.*

12. Click **Scan** to continue with the recovery process.

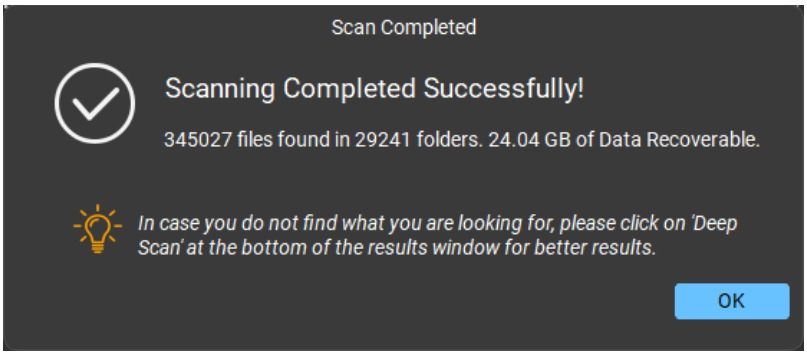


Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *Click* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the scanning process.*

Note: *You can also perform a deep scan after a quick scan by clicking the* ***'Click here'*** *link next to the* ***Deep scan*** *at the bottom of the screen.*

13. Once the scanning process completes, details of the **files** and **folders** found would be displayed in a **Scan Completed** dialog box as shown below:



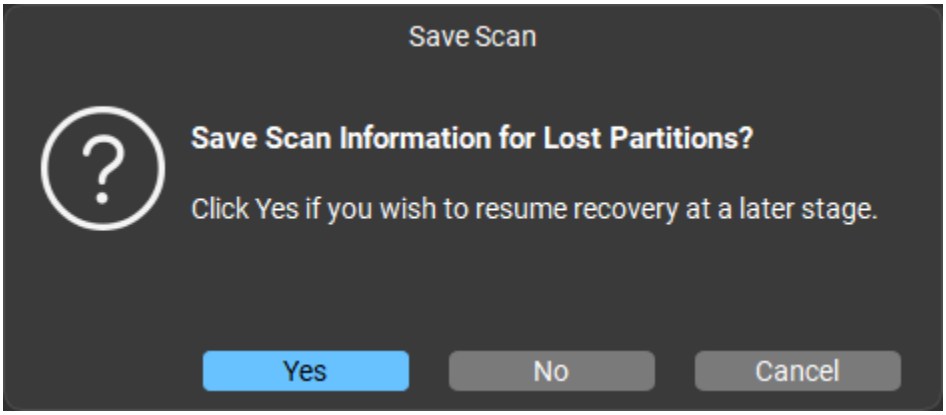
14. Click **OK** button.

15. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

Note: *If you wish to save the scanned information and resume the recovery process at a later stage, see Save the Scan Information.*

Steps to Save the Scan Information for Lost/Deleted Volumes:

1. In **Select Partition** window, click  **Back** button or close the software.
2. **Save Scan** dialog box will appears. Click **Yes**.

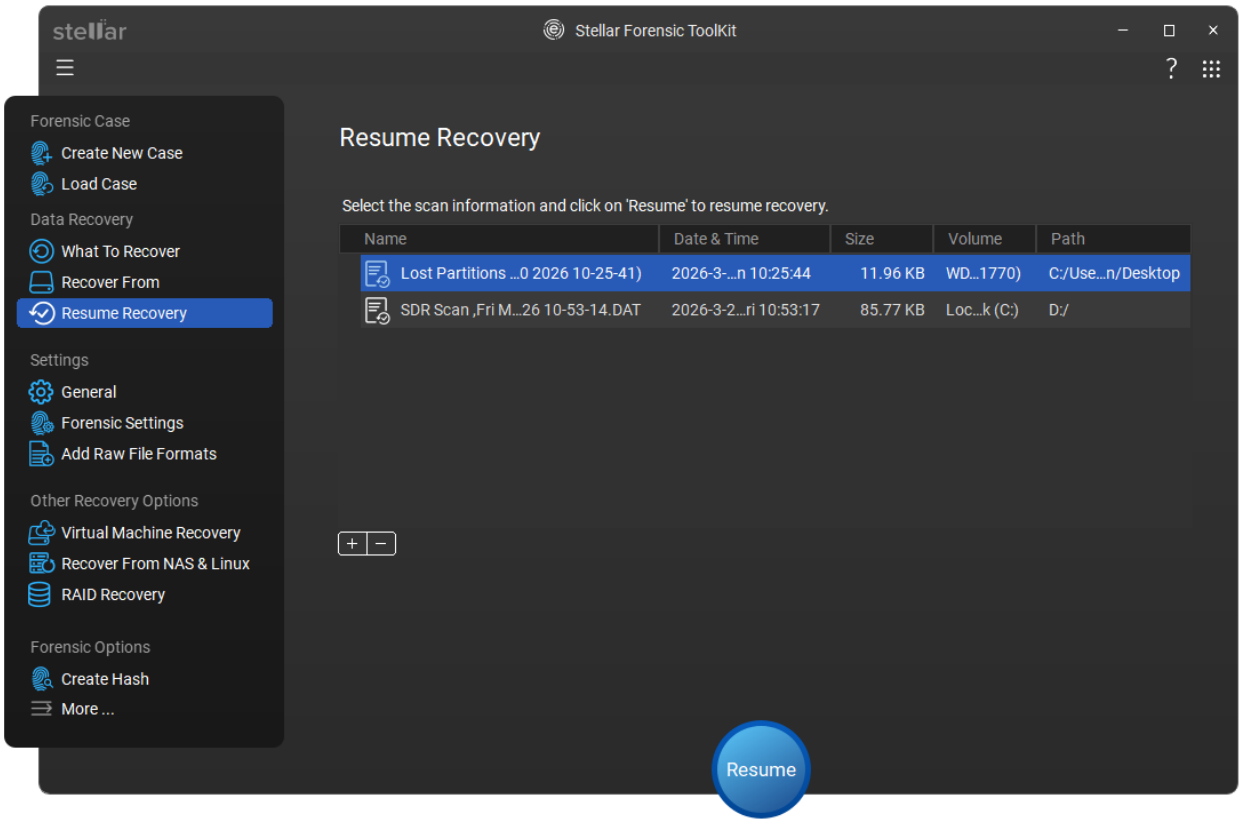


3. In the **Save Scan** dialog box, specify the location where you want to save the image file. Type the name of the image file in the **File name** text box. Click **Save** button.
4. **Scan saved** dialog box appears with a message **"Lost Partitions Scan Information is saved successfully".** Click **OK**.

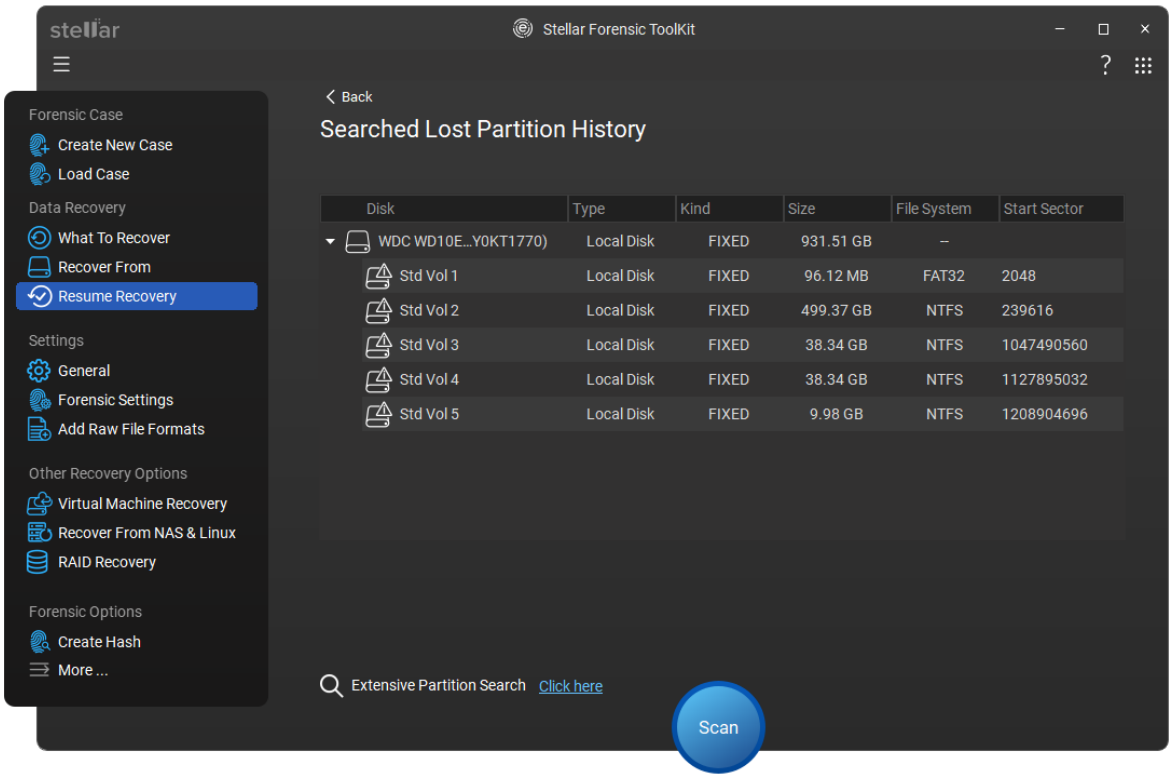
Steps to Load the Previously Saved Scan Information for Lost Volumes:

This option is used to resume the recovery process from a saved scan information file.

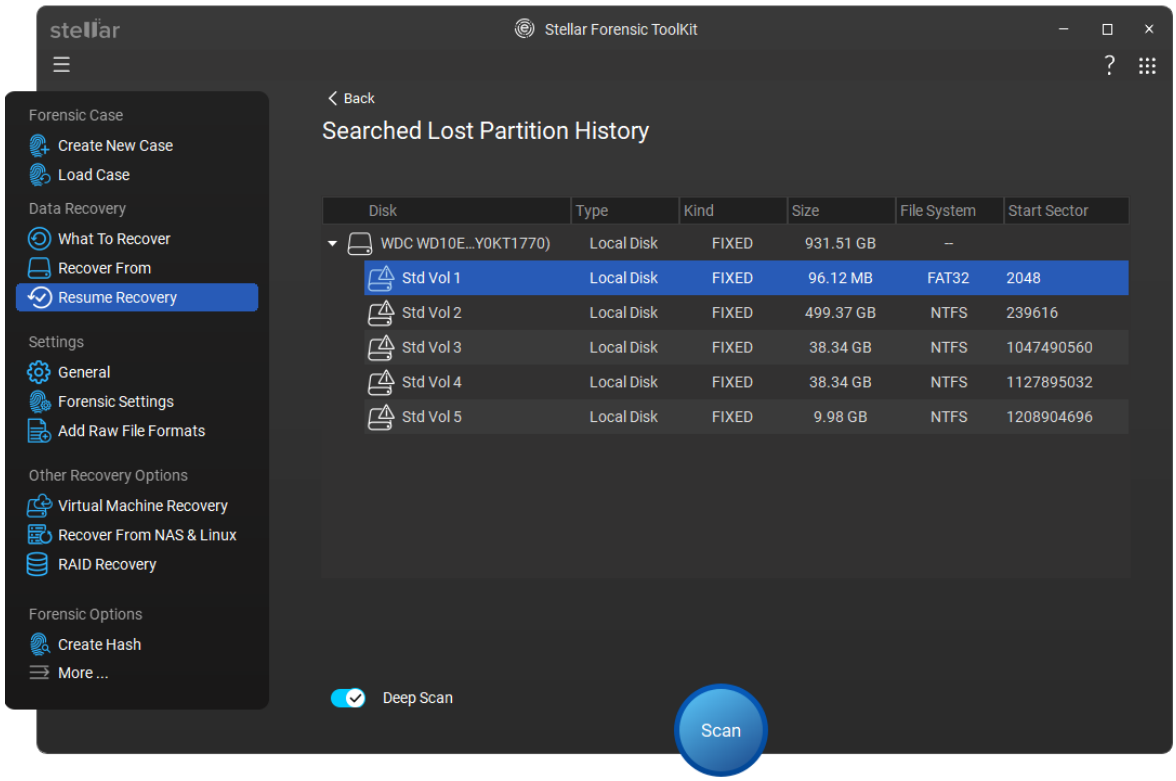
1. Run **Stellar Forensic Toolkit software**.
2. Click  **Resume Recovery** icon and select the previously saved **Scan Information**.
3. A **Resume Recovery** window will appear which displays a list of saved scan information files existing in the system.



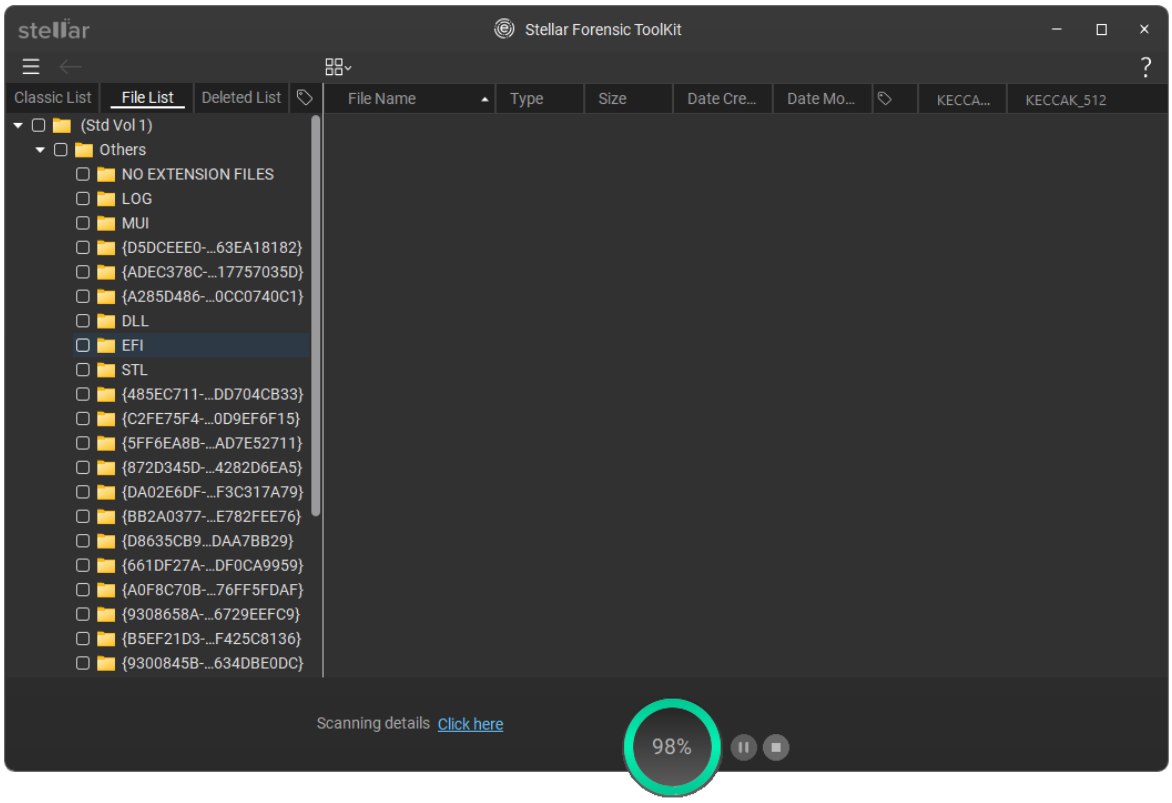
4. If the file you need is not in the list, click the **Add** button and select the file.
5. Click **Open**.
6. The file you added gets displayed in the **Resume Recovery** window. Click **Remove** button if you want to remove the save scan file.
7. Select the required **Lost Volume** and click **Resume** button.
8. Clicking on the **Resume** button will display results for **Searched Lost Partition History** window is displayed.



9. Select the required **Lost Partition.**



9. Click **Scan** to start the scanning process.

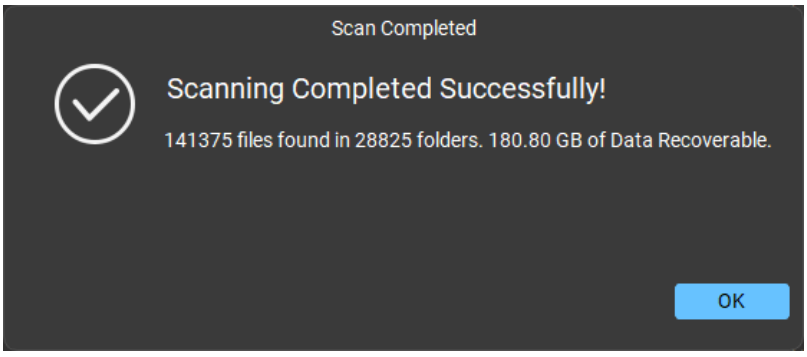


Note: *You can turn on the* ***Deep Scan*** *toggle if you want to perform a comprehensive scan of the selected volume.*

Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *Click on* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the process.*

10. After the scan process is completed, details of the **files** and **folders** found are displayed.

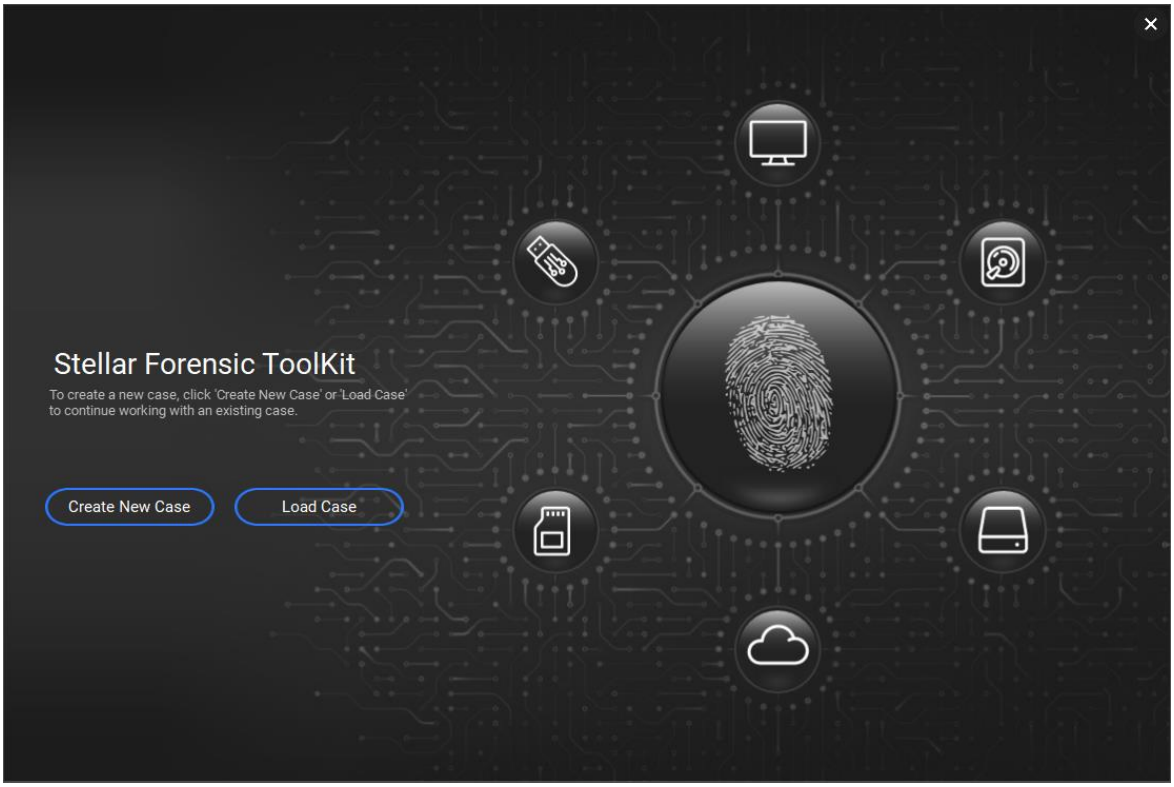


4.7. Recover Data from Physical Disks

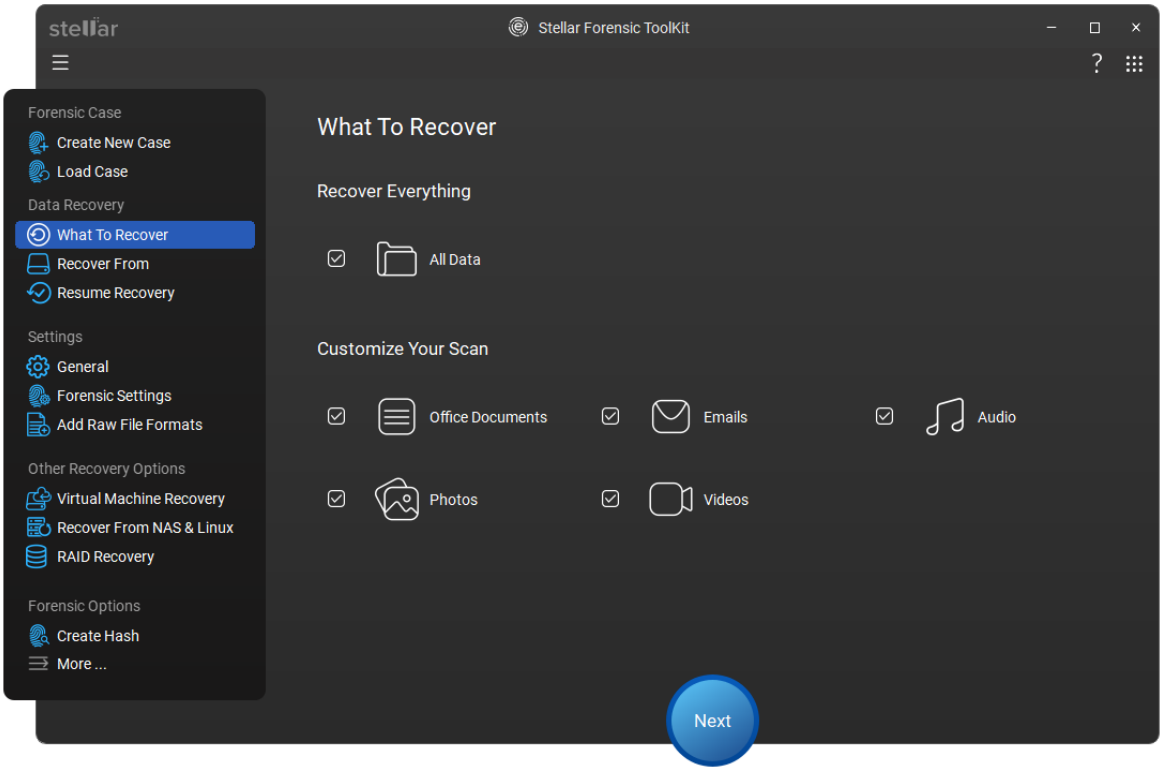
Sometimes you can't recover your data by using the quick scan, deep scan and can't find drive options. It happens because of severe corruption or partition damage in the physical/removable disk. In this scenario, **Stellar Forensic Toolkit** allows you to recover your data by using the **Physical Disks** option. This option supports both internal and external hard drives. **Physical Disks** feature works with Raw Recovery to retrieve the highly corrupted data and has better chances of recovery.

Steps To Scan Physical Disk:

1. Run **Stellar Forensic Toolkit.**
2. From the main screen, select **Create New Case** or **Load Case** button.

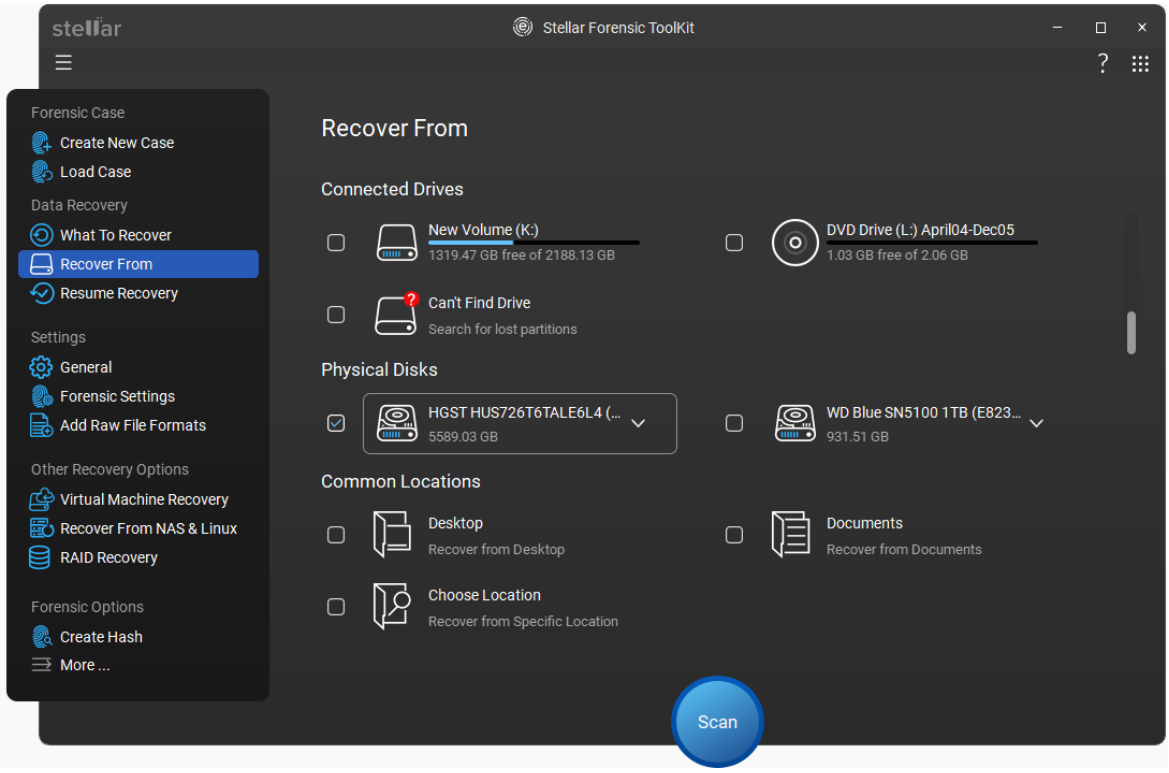


3. From the left navigation menu, go to **Data Recovery** section and click on **What To Recover**. Then, select the type of data i.e. **All Data** or **Office Documents, Emails, Audio, Photos** and **Videos**, you want to recover.

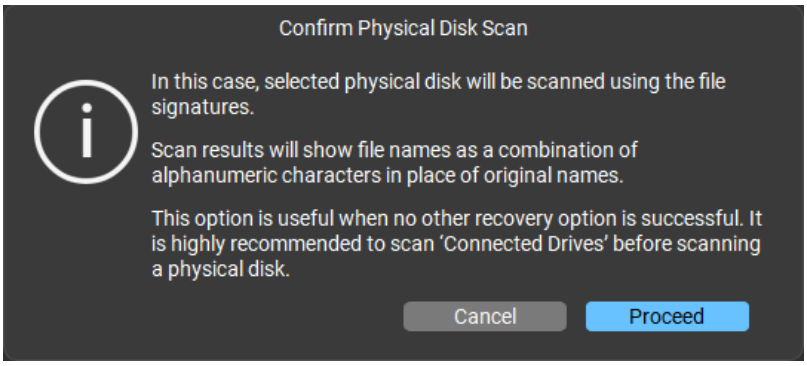


4. Click **Next**.

5. From **Recover From** screen, select the disk you want to recover from **Physical Disks**.

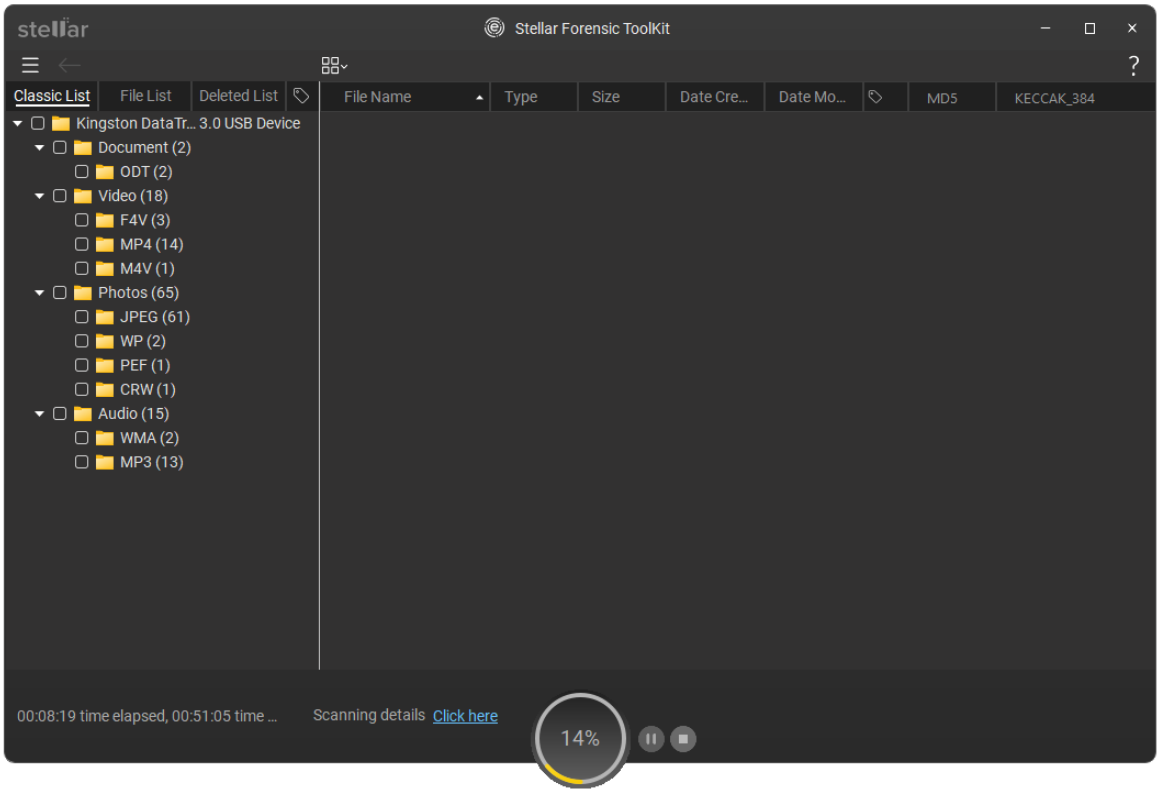


6. The **Confirm Physical Disk Scan** dialog box appears, as shown below:



7. Click **Proceed** to start the scanning process.

8. A screen appears that shows the scanning process.

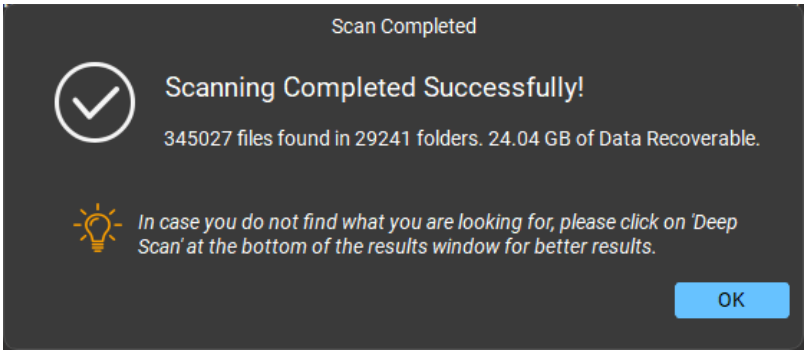


Note: *You can click the* ***Stop, Pause,*** *or* ***Resume*** *buttons to control the scanning process at any point.*

Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *You can also perform a deep scan after a quick scan by clicking the* ***'Click here'*** *link next to the* ***Deep scan*** *at the bottom of the screen.*

9. Once the scanning process is completed, details of the **files** and **folders** found are displayed in a dialog box as shown below:



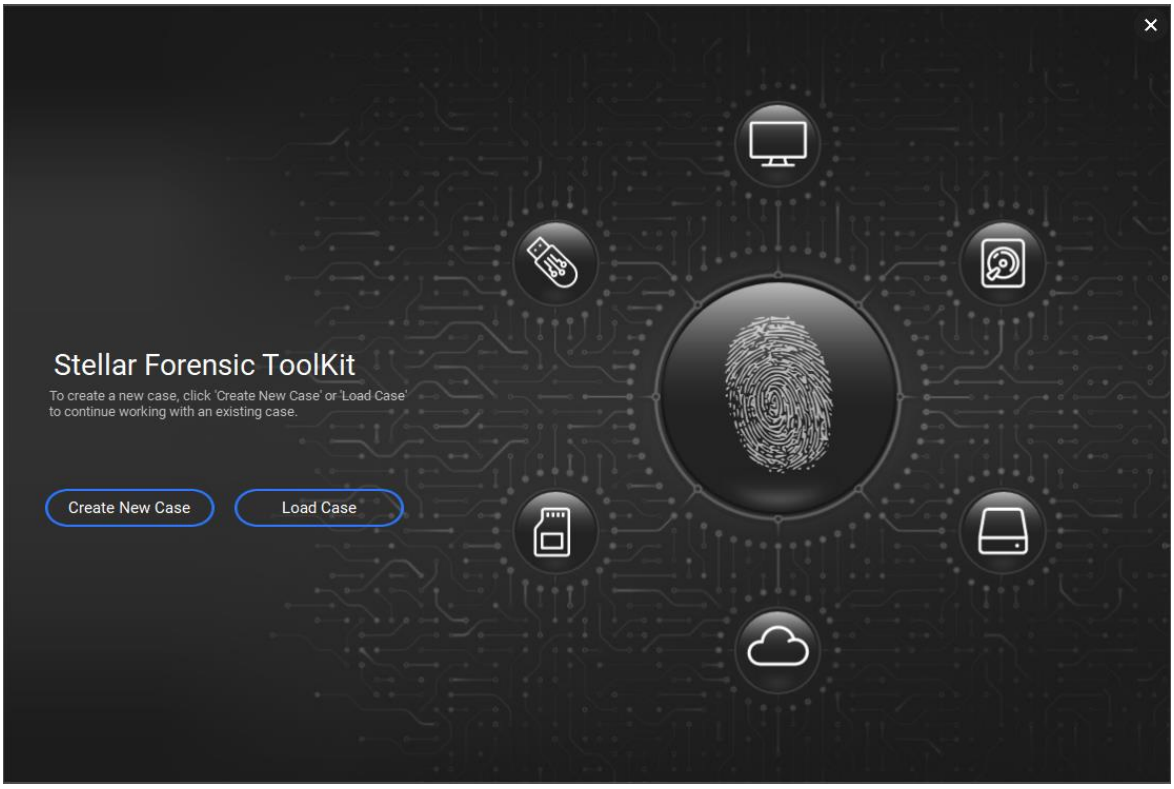
10. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

4.8. Recover Data from Virtual Machine

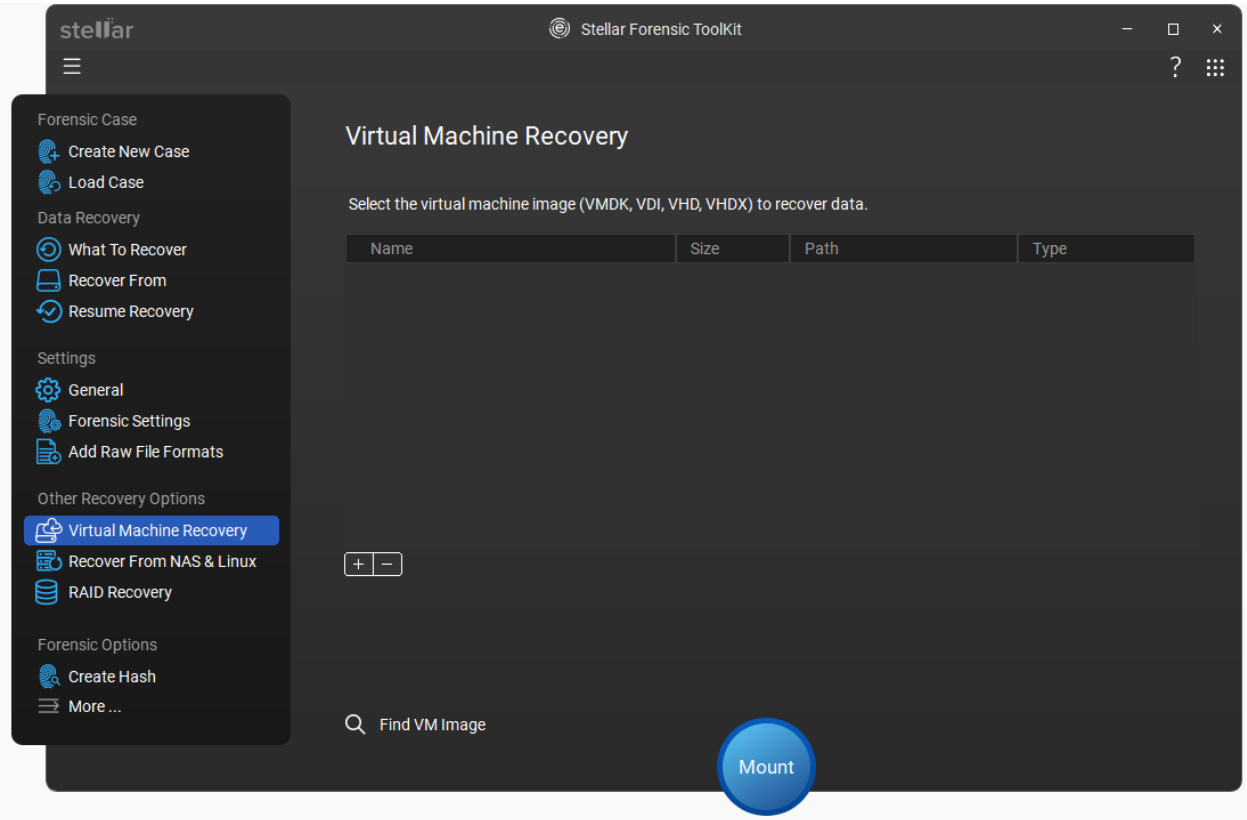
A virtual machine is used to create a virtualized environment that behaves like a separate computer system. This virtual computer system when created stores data in the form of images. **Stellar Forensic Toolkit** supports recovery from these virtual machine images for VMDK, VDI, VHD and VHDX formats.

To recover data from Virtual Machine image:

1. Run **Stellar Forensic Toolkit**.
2. From the main screen, select **Create New Case** or **Load Case** button.

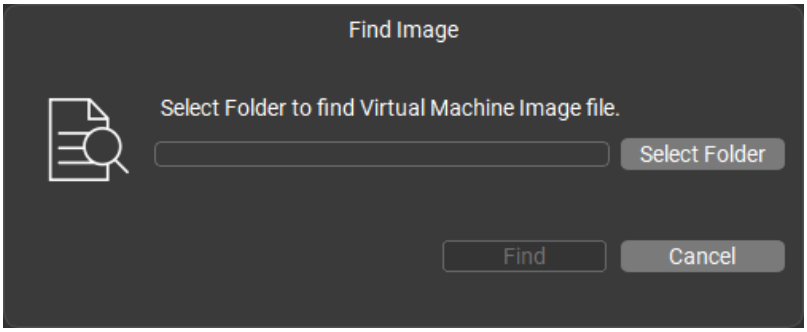


3. From the side panel, under the **Other Recovery Options**, click on  **Virtual Machine Recovery** option.

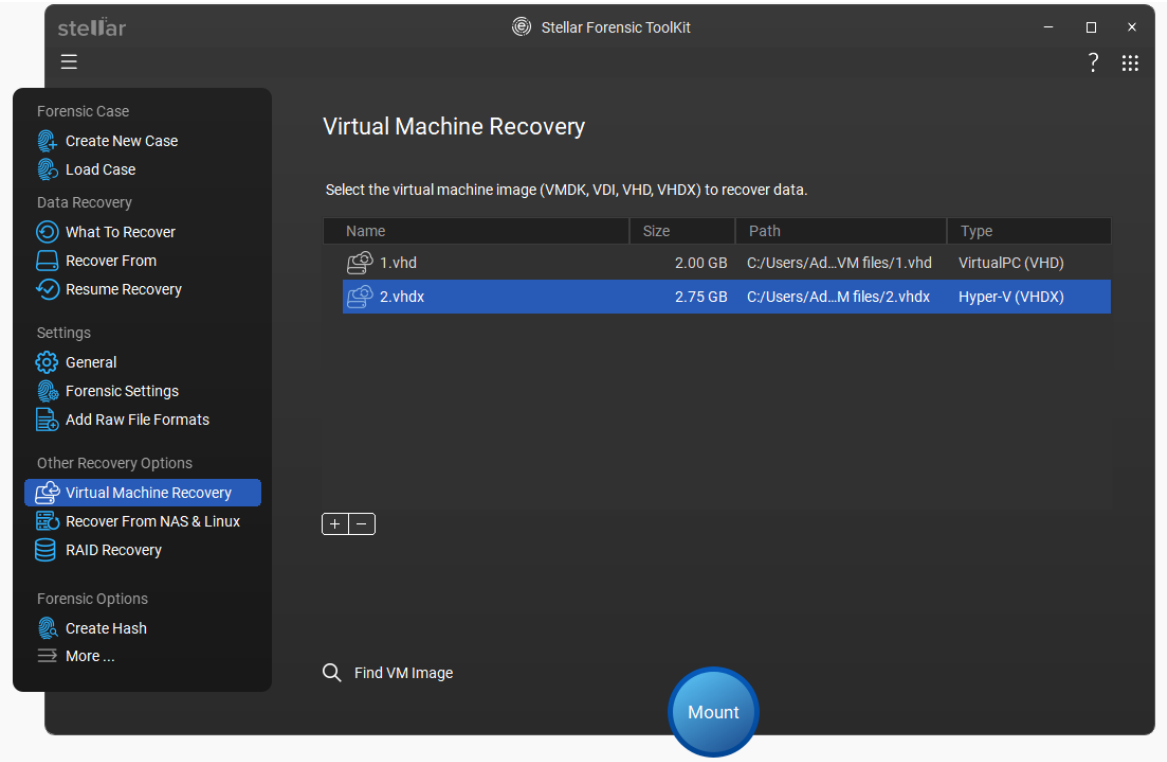


4. From the **Virtual Machine Recovery** screen, click on **Find VM Image** button at the bottom of the screen to find VM Image(s).

5. **Find Image** dialog box appears. Click the **Select Folder** button to find the virtual machine image file, then click **Find** to proceed.



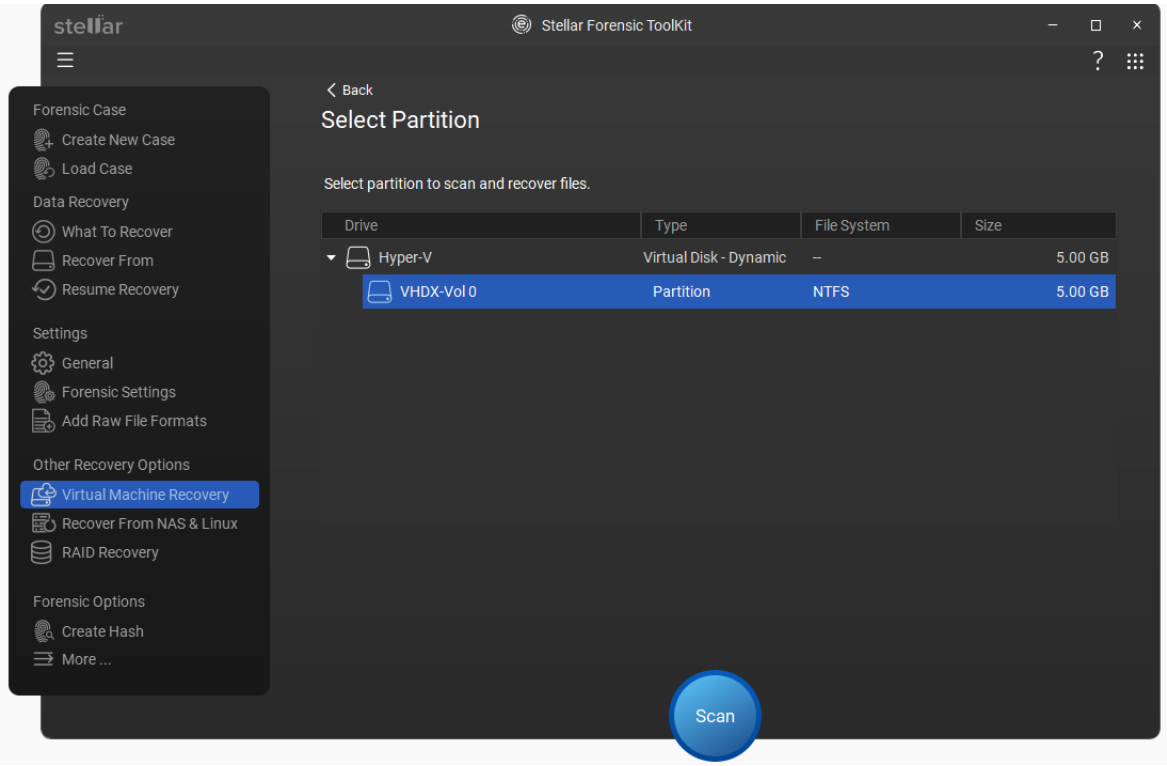
6. It will list the VM Image(s) as shown below with its respective size, path, and type. Select the image from which you want to recover data and click **Mount**.



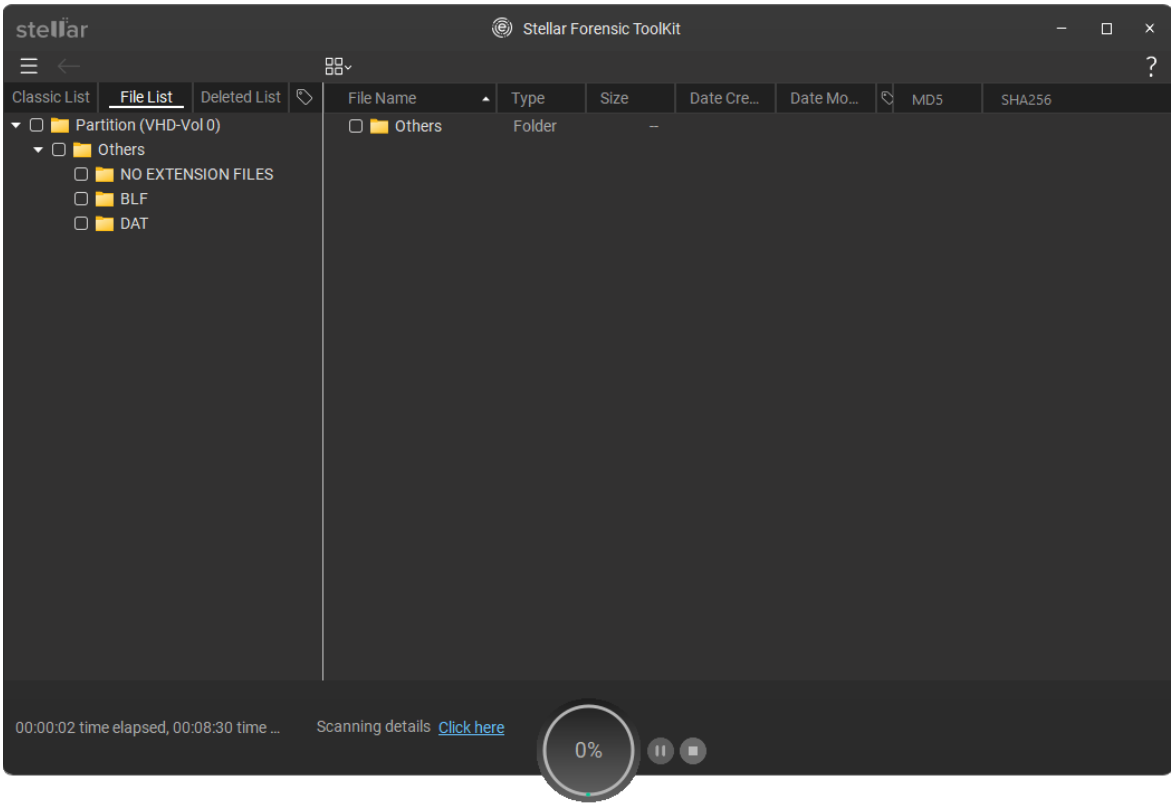
Note:

- *You can also add a particular Image file using* **+** ***Add*** *icon and remove a particular image file listed using* **−** ***Remove*** *icon.*
- *The Virtual Machine Recovery supported formats are* ***VMDK***, ***VDI***, ***VHD***, *and* ***VHDX***.
- *You can select only one image file at a time for recovery.*

7. **Select Partition** screen appears listing all the volumes found in the selected virtual machine image file. Select the volume you wish to scan and click **Scan** to start the recovery process.



8. A screen appears that shows the scanning process.

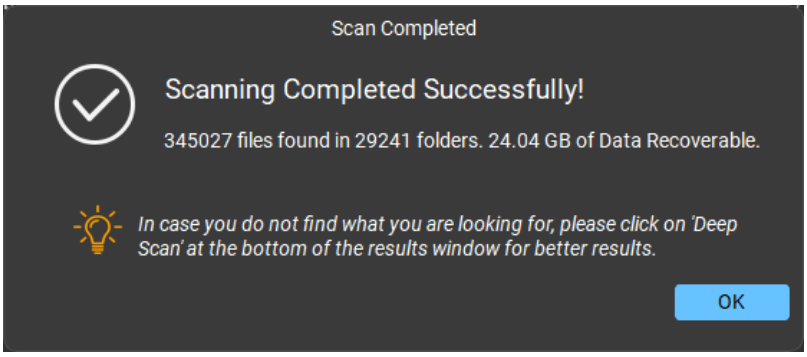


Note: *To view the scanning details, click the* ***Click here*** *link next to the* ***Scanning details*** *at the bottom of the screen.*

Note: *Click* ***Stop*** *or* ***Pause/Resume*** *button to stop or resume the scanning process.*

Note: *You can also initiate the deep scan process, once the scan of the selected hard drive volume is complete, click the* ***"Click Here"*** *next to* ***"Deep Scan"*** *at the bottom of the screen.*

9. Once the scanning process is completed, details of the **files** and **folders** found are displayed in a dialog box as shown below:



Note: *To mount a virtual machine of VHD/VHDX file in* ***Stellar Forensic Toolkit****, make sure that the VHD/VHDX image file is not mounted in your Windows OS. To unmount VHD/VHDX file in Windows, go to the New Volume/drive in Windows Explorer, right-click and select* ***Eject****.*

10. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

Note: *If you wish to save the scanned information and resume the recovery process at a later stage, see Save the Scan Information.*

4.9. Remote Recovery from NAS

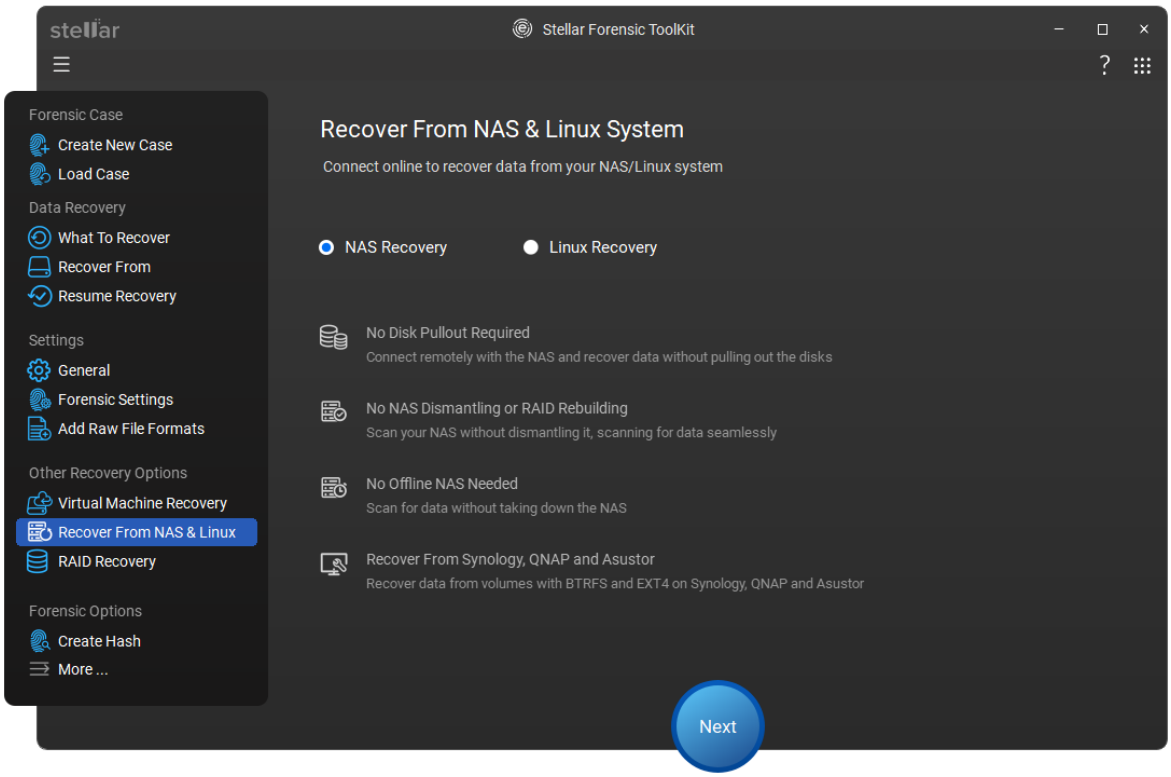
4.9. Remote Recovery from NAS

Stellar Forensic Toolkit allows you to recover lost or deleted data from **NAS (Network Attached Storage)** systems remotely. This feature eliminates the need to remove disks from NAS server. You can scan the NAS volumes over network while the device is online.

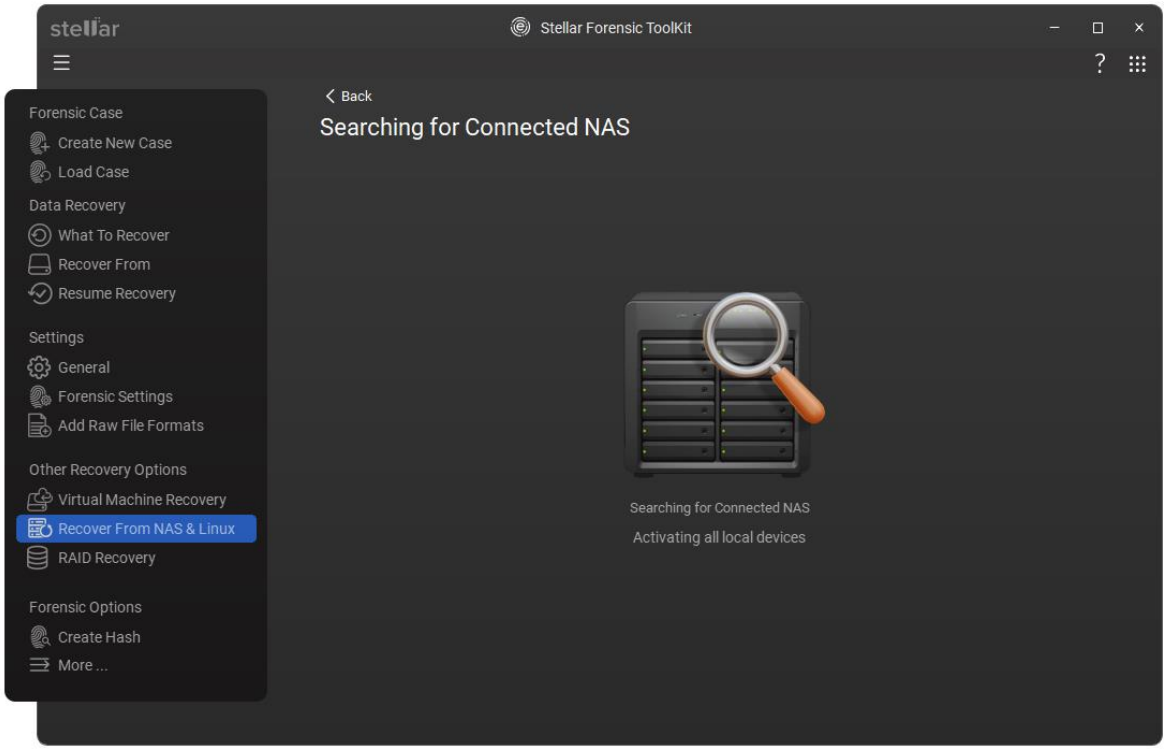
Note: *The software can only connect to the NAS device if both the system and NAS are on same* ***Local Area Network (LAN)****.*

Steps to recover data from NAS remotely:

1. Start Stellar Forensic Toolkit.
2. From the left navigation menu, Navigate to **Other Recovery Options.**
3. From **Other Recovery Options** section**,** select **Recover From NAS & Linux** option.
4. On **Recover From NAS & Linux System** screen, select **NAS Recovery** radio button and select **Next**.

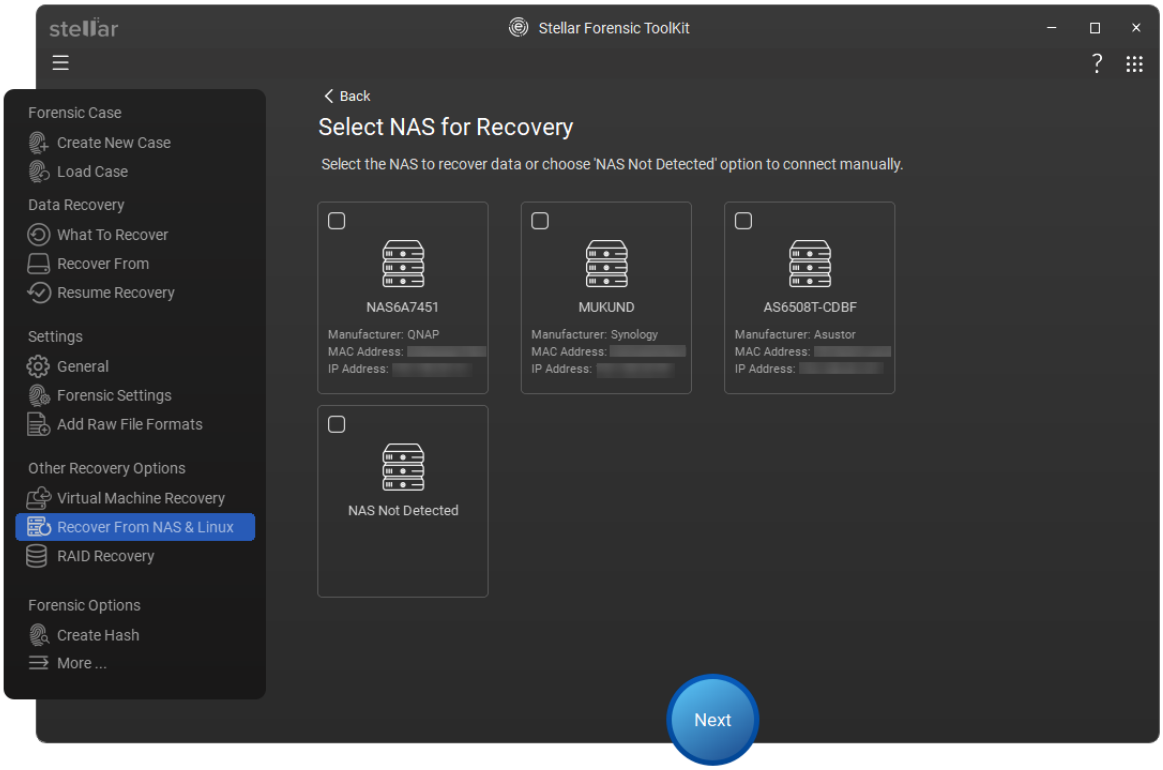


5. The software starts **Searching for Connected NAS** devices in your local network.



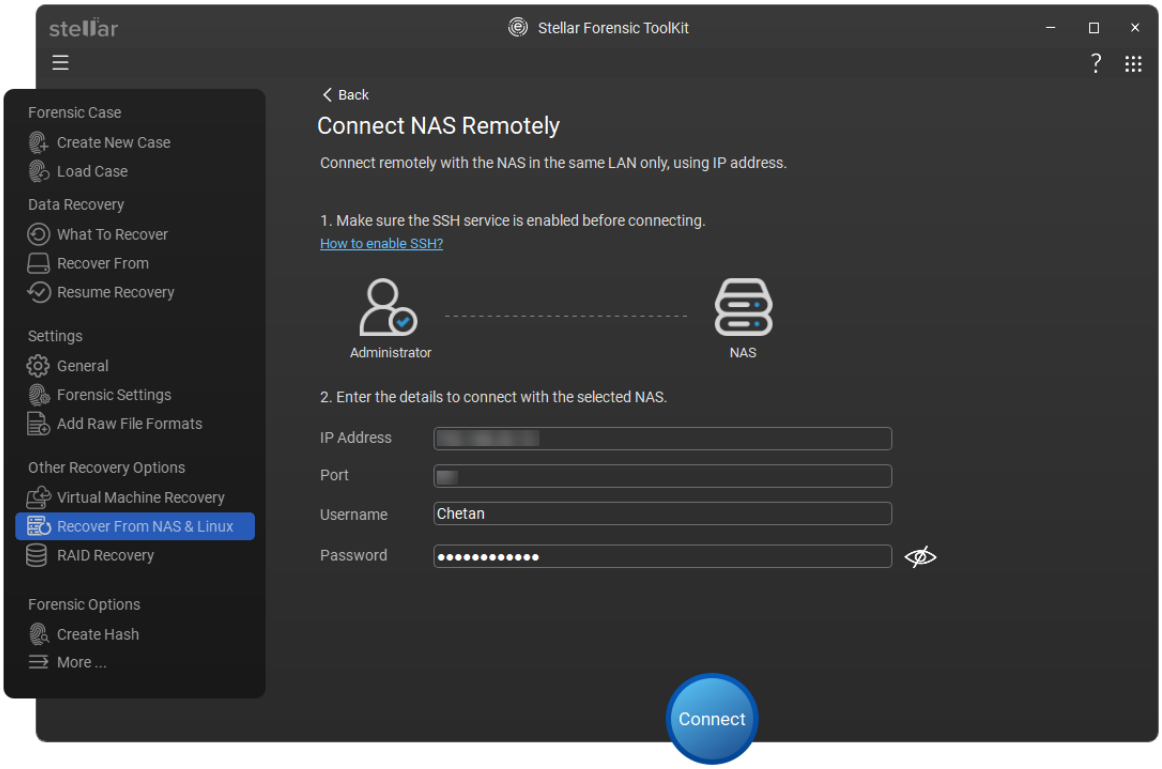
6. All detected NAS devices are listed on the **Select NAS for Recovery** screen.

    - Select the NAS device you want to scan and click **Next**.
    - If your NAS deivce is not listed, select **NAS Not Detected** to connect manually. For more information about next steps, select here.



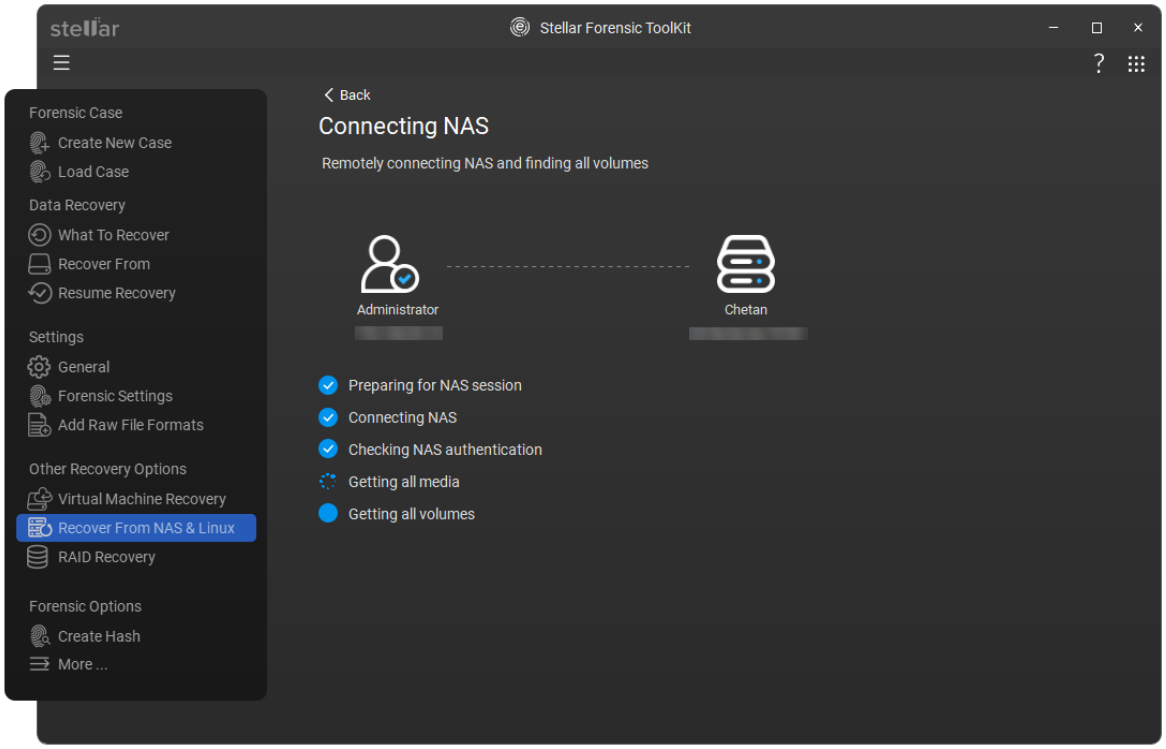
7. On **Connect NAS Remotely** screen, enter the following details:

   - **IP Address:** The software automatically fetches the IP address of selected NAS. You can also enter it manually if required.
   - **Port:** Enter the port number (Default is 22).
   - **Username and Password:** Enter administrator credentials for NAS.

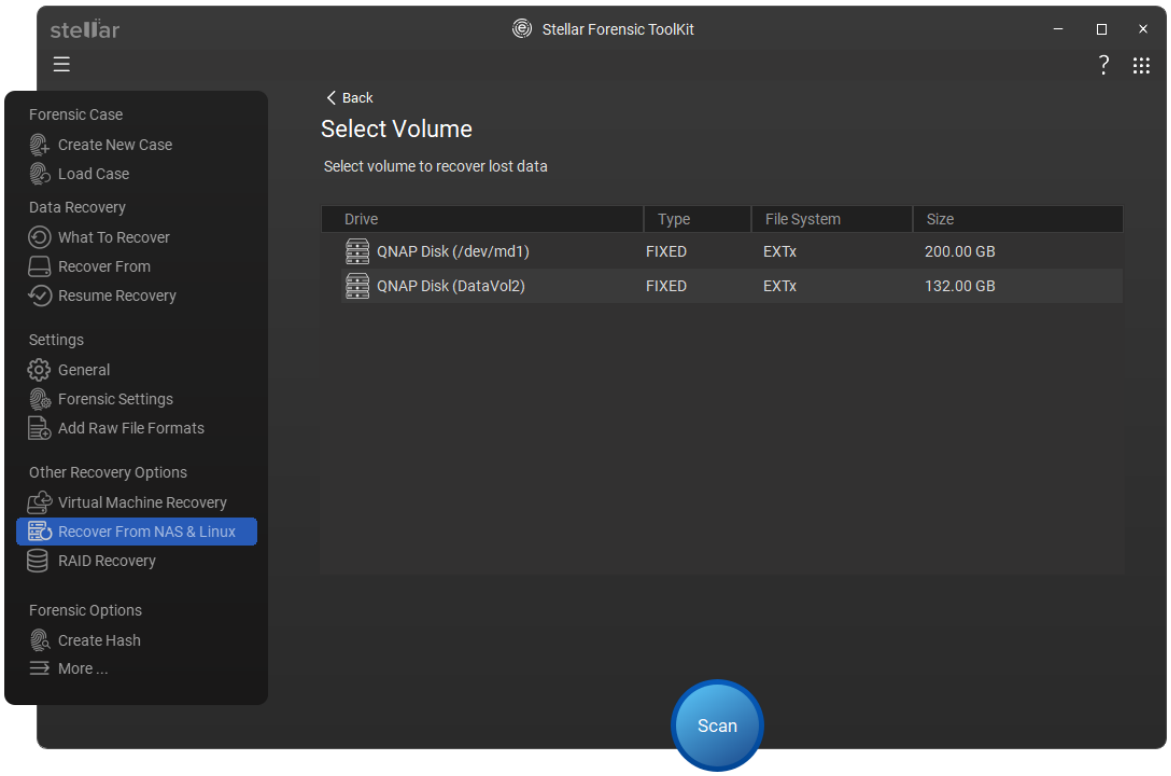


Note: *Make sure the SSH service is active on your NAS device. If you need help, click* ***'How to enable SSH?'*** *for more instructions.*

8. Select **Connect**. The software establishes a remote connection and identifies all volumes.

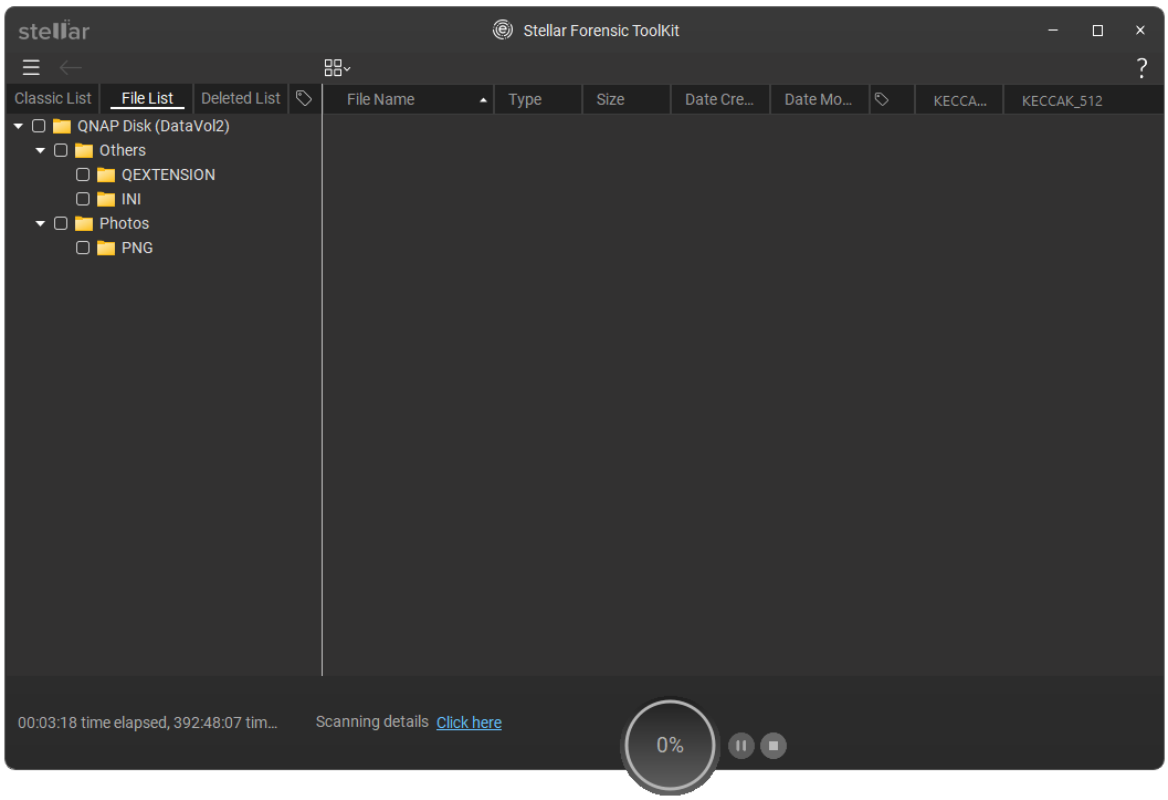


9. From **Select Volume** screen, select the volume from which you want to recover data.



Note: *You can enable* ***Deep Scan*** *at the bottom if you want a more thorough search for lost partitions or data.*

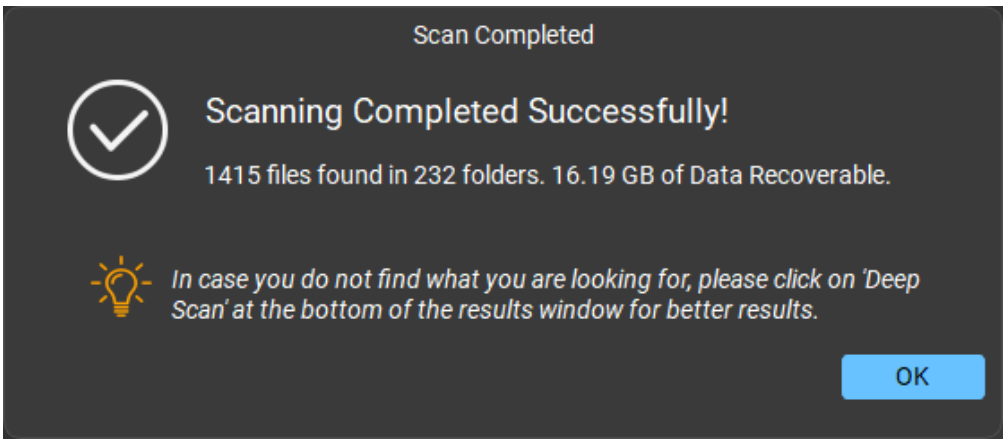
10. Select **Scan**. The software begins the scanning process and shows the progress.



Notes:

- *To view detailed scan information, select **Click here** link near the scanning details. To save the scan information after the scan completes, select here.*
- *To stop, pause or resume the scan, select **Stop** or **Pause/Resume** button.*
- *To continue recovery later using saved scan information, select here.*

11. After the scan completes, application displays the list of files and folders found.

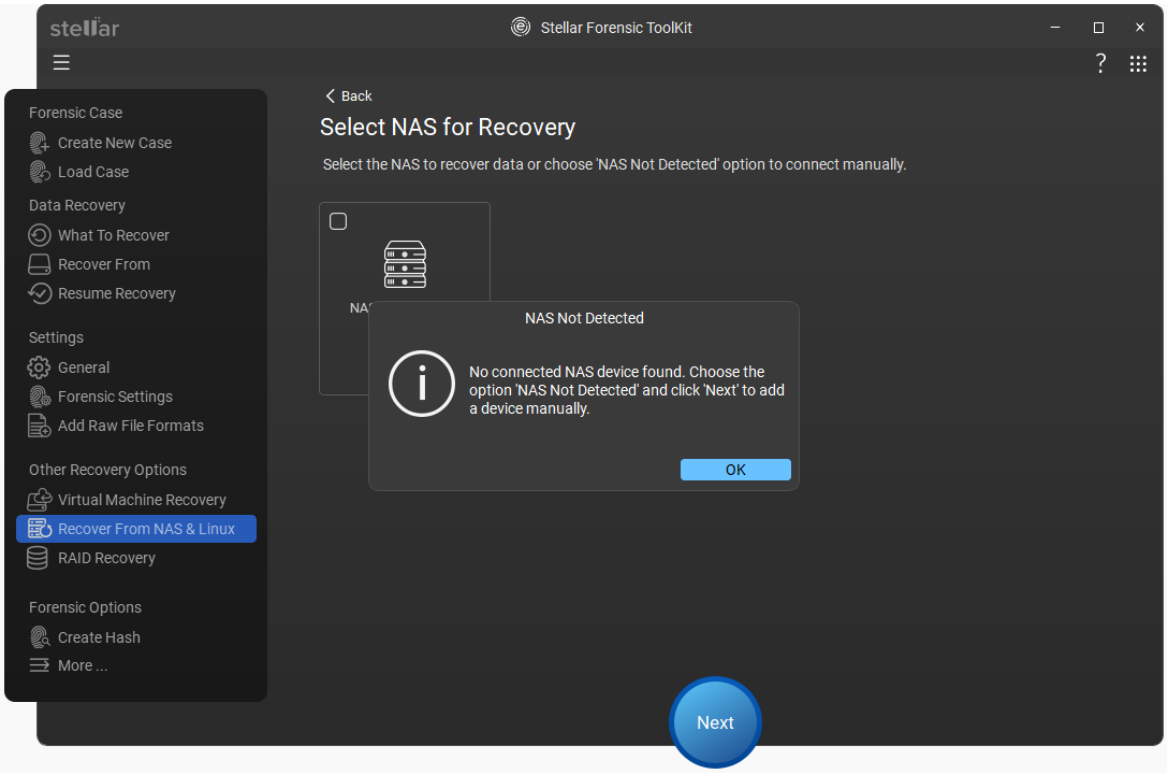


12. To preview and save the recovered files, see Preview the Scan Results and Save the Recovered Files.

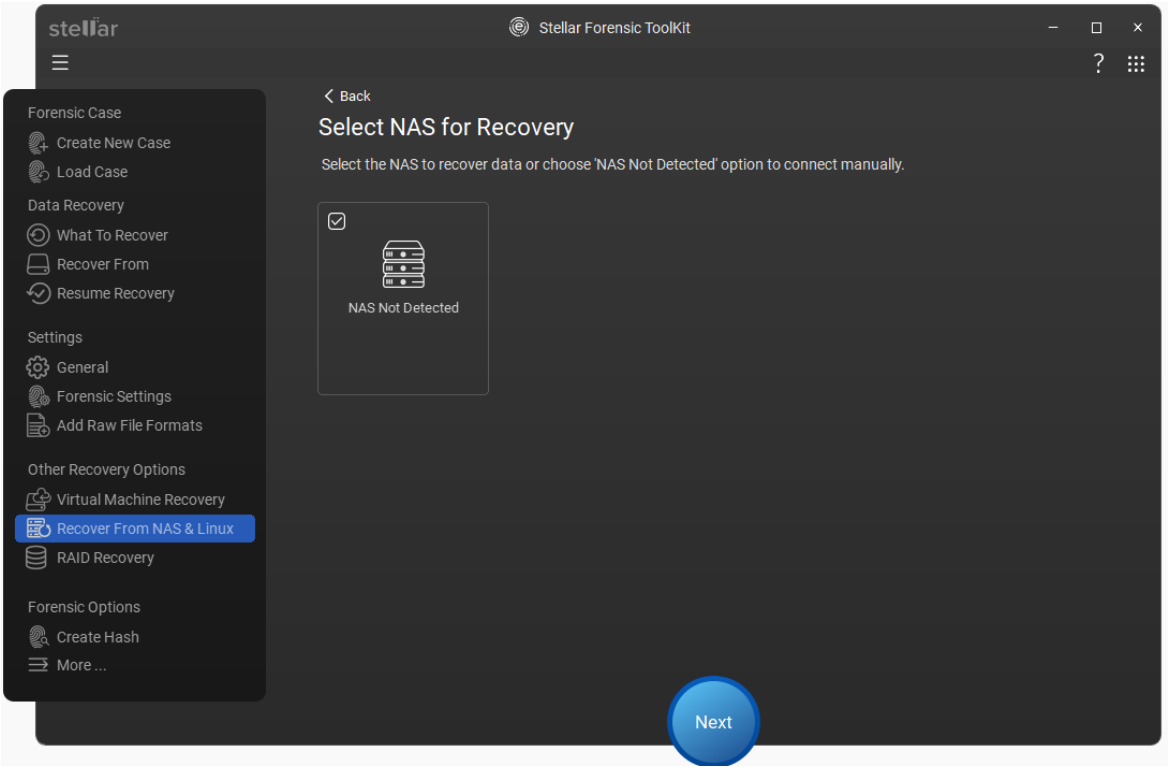
NAS Not Detected:

If the software does not find your NAS device automatically, a **"NAS Not Detected**" dialog box appears. You can then add the device manually.

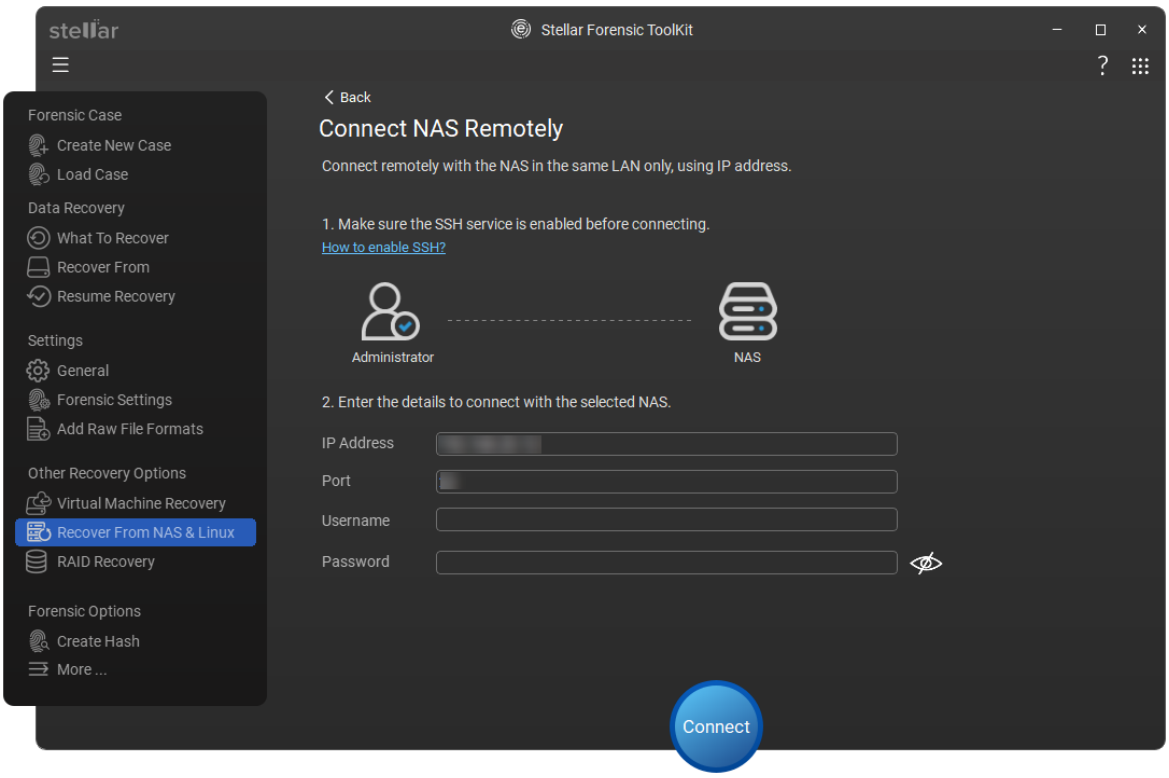
1. On **NAS Not Detected** dialog box, select **OK**.



2. On the **Select NAS for Recovery** screen, select the **NAS Not Detected** checkbox and select **Next**.

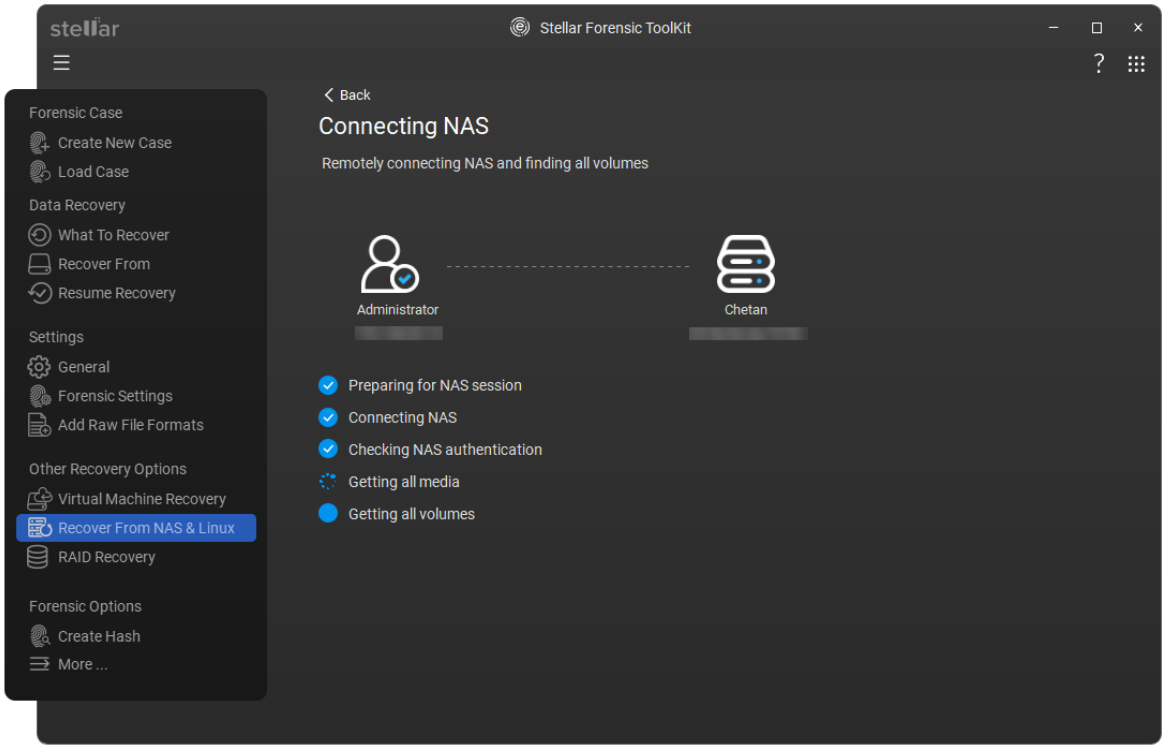


3. The **Connect NAS Remotely** screen appears. Perform the following:
    - **IP Address:** Type the IP address of your NAS device.
    - **Port:** Type the port number (Default is 22).
    - **Username and Password:** Type the administrator credentials for the NAS.

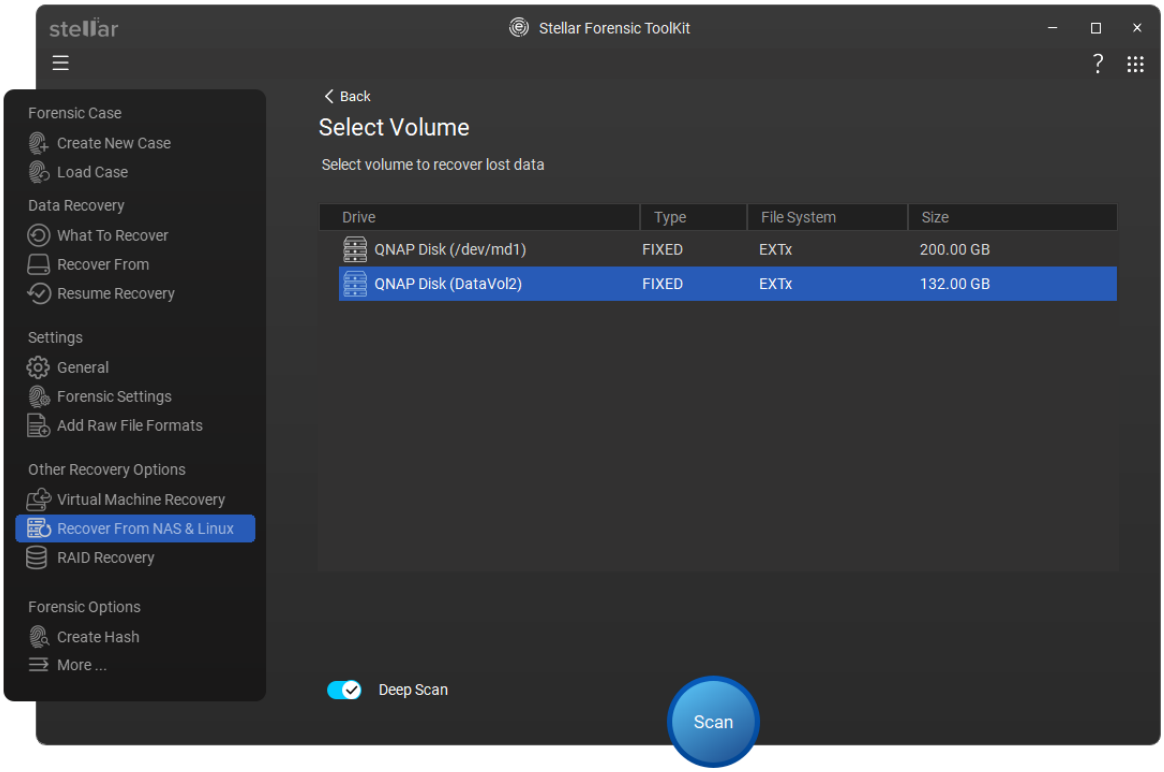


Note: *Make sure the SSH service is active on your NAS device. If you need help, click* ***'How to enable SSH?'*** *for more instructions.*

4. Select **Connect**. The software establishes a remote connection and identifies all volumes.

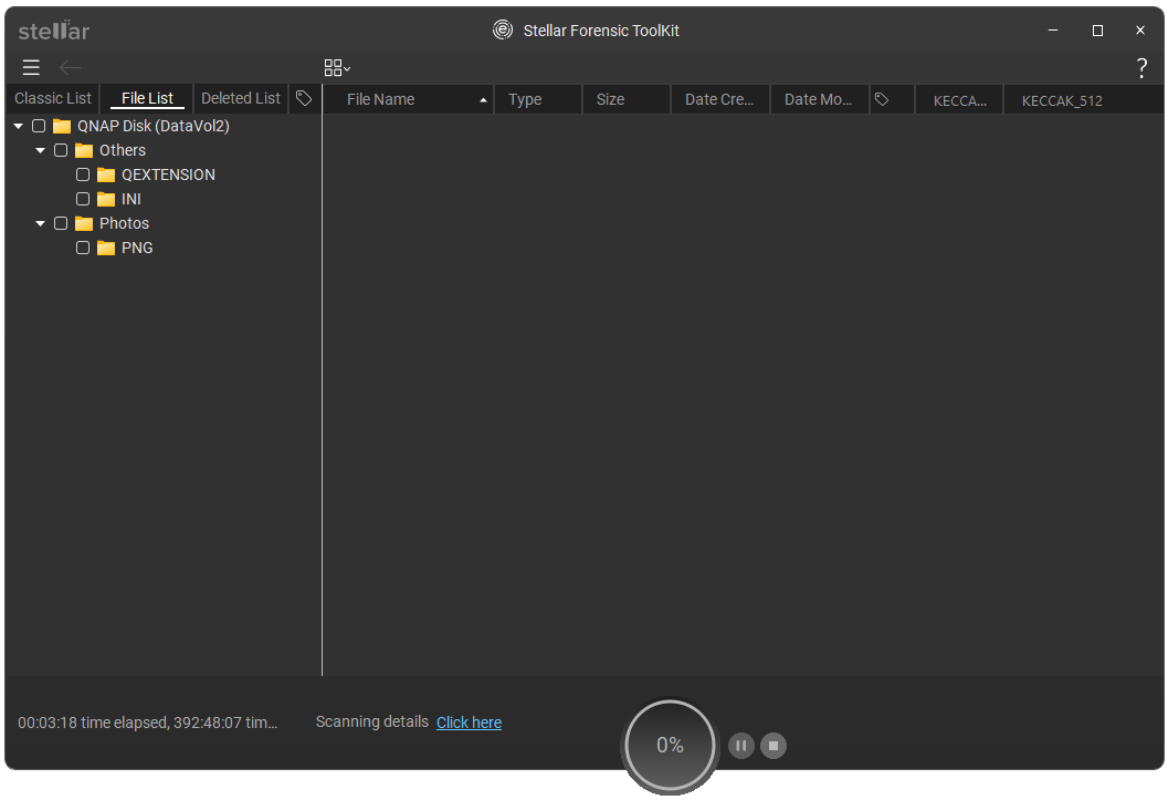


5. From **Select Volume** screen, select the volume from which you want to recover data.



Note: *You can enable* ***Deep Scan*** *at the bottom if you want a more thorough search for lost partitions or data.*

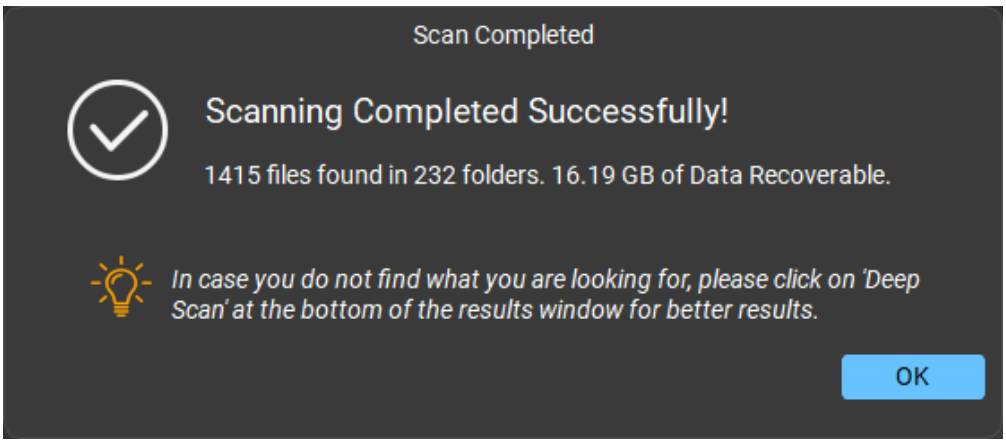
6. Select **Scan**. The software begins the scanning process and shows the progress.



Notes:

- *To view detailed scan information, select **Click here** link near the scanning details. To save the scan information after the scan completes, select here.*
- *To stop, pause or resume the scan, select **Stop** or **Pause/Resume** button.*
- *To continue recovery later using saved scan information, select here.*

7. After the scan completes, application displays the list of files and folders found.



8. To preview and save the recovered files, see Preview Scan Results and Save the Recovered Files.

4.9.1. Configure and Enable SSH

SSH allows secure remote access to NAS system. You can use SSH for troubleshooting, advanced configuration, and system recovery.

Before you start, make sure:

- You have administrator access.
- The NAS is powered ON.
- You are logged in to the web management interface.

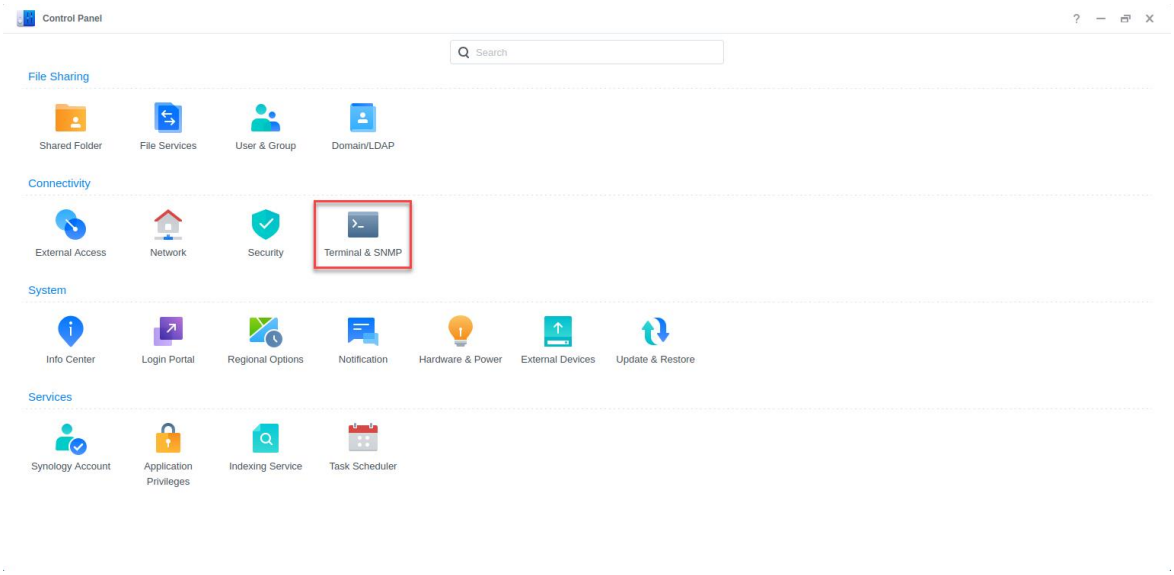
Notes:

- *If your device is a **QNAP** or an **Asustor NAS**, search the phrase "How to enable SSH?" on Internet, or contact the device manufacturer for support.*
- *These steps apply to a **Synology NAS** device.*

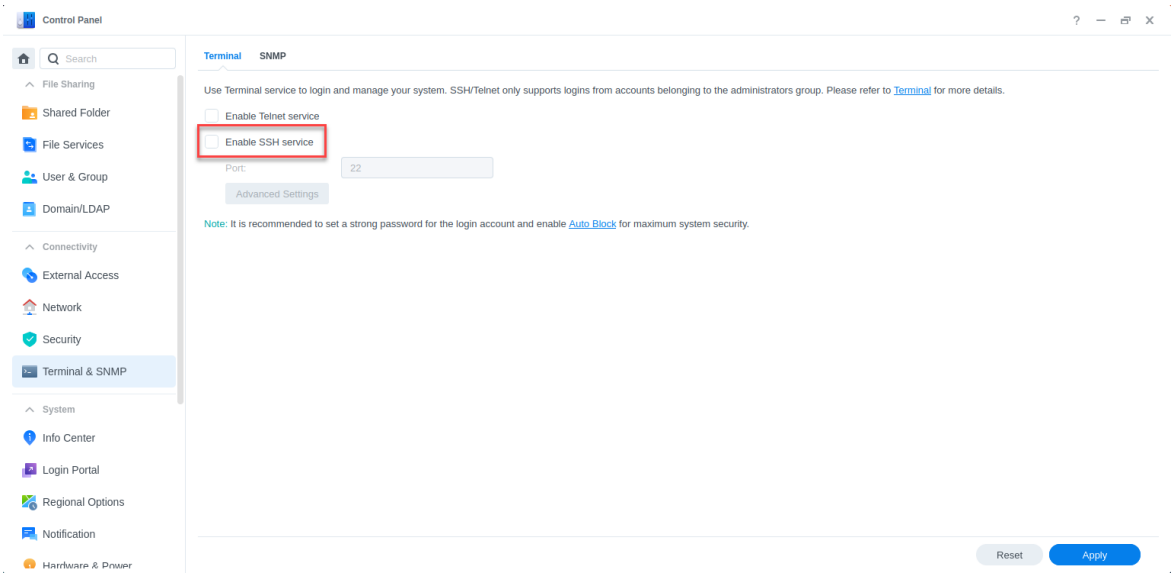
Steps to Enable SSH:

1. Login to NAS web interface. Select **Control Panel** on the desktop.

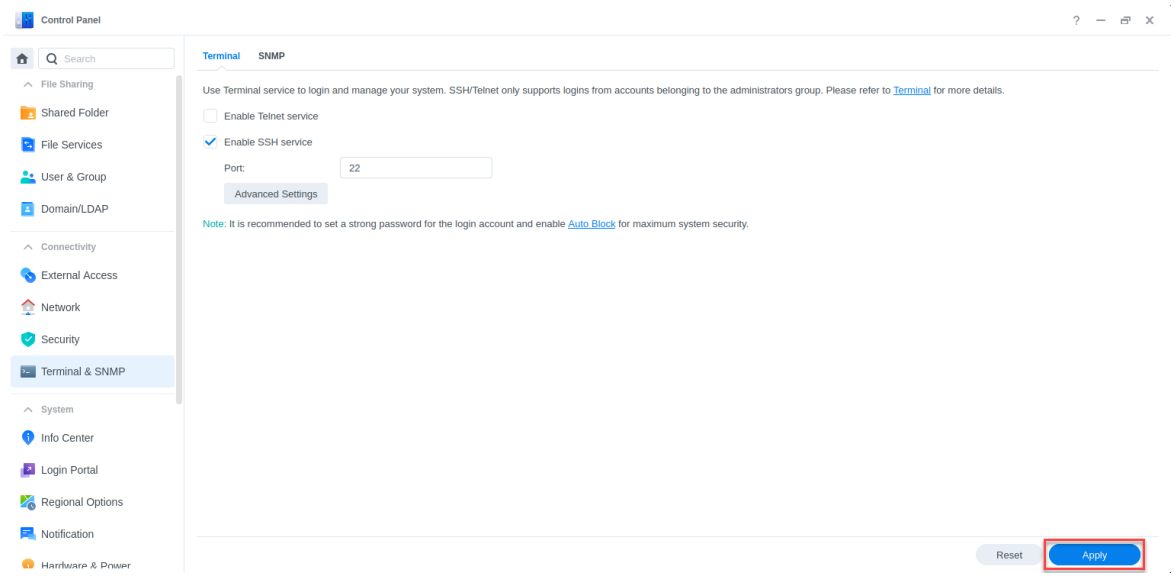
2. In Control Panel, select **Terminal & SNMP**. The system displays Terminal settings page.



3. Under Terminal section, select **Enable SSH service**.



4. Select **Apply**. The System enables SSH services.



4.10. Remote Recovery from Linux System

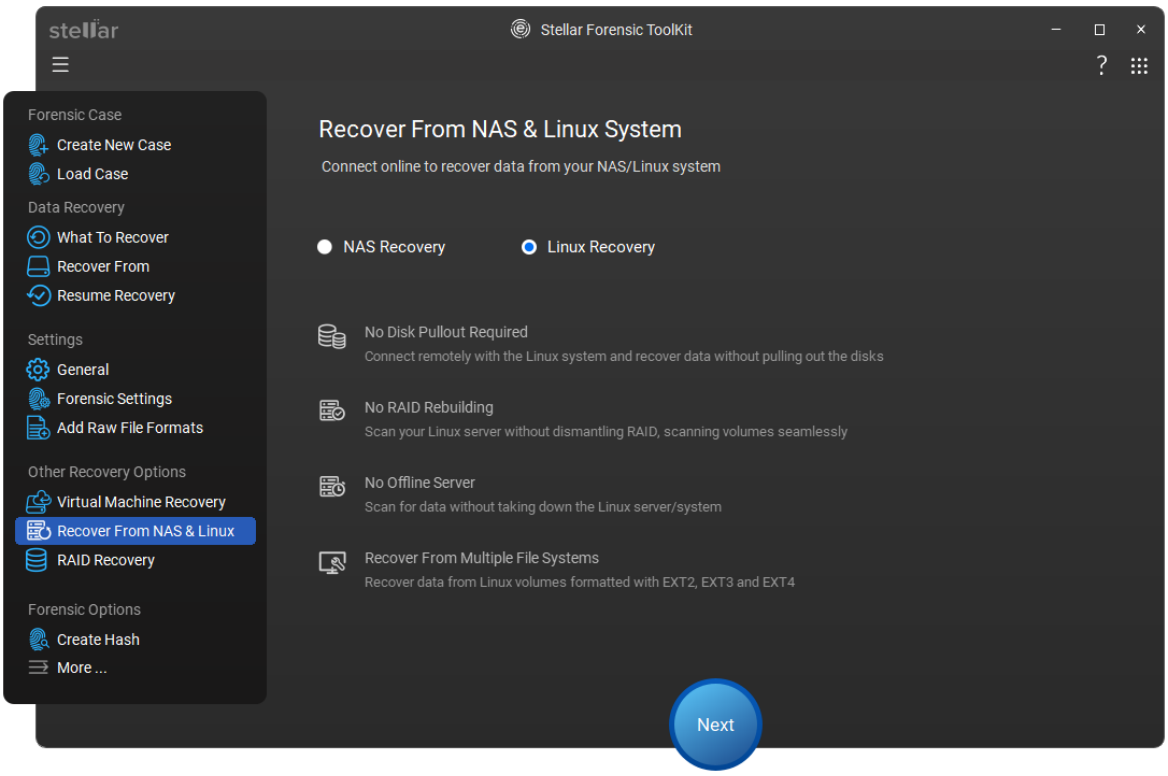
4.10. Remote Recovery from Linux System

Stellar Forensic Toolkit allows you to recover lost data from a Linux computer over a network. This feature connects to a remote Linux system and scans its volumes without removing the hard drives.

Note: *The software can only connect to Linux system if both computers are on same* ***Local Area Network (LAN)****.*

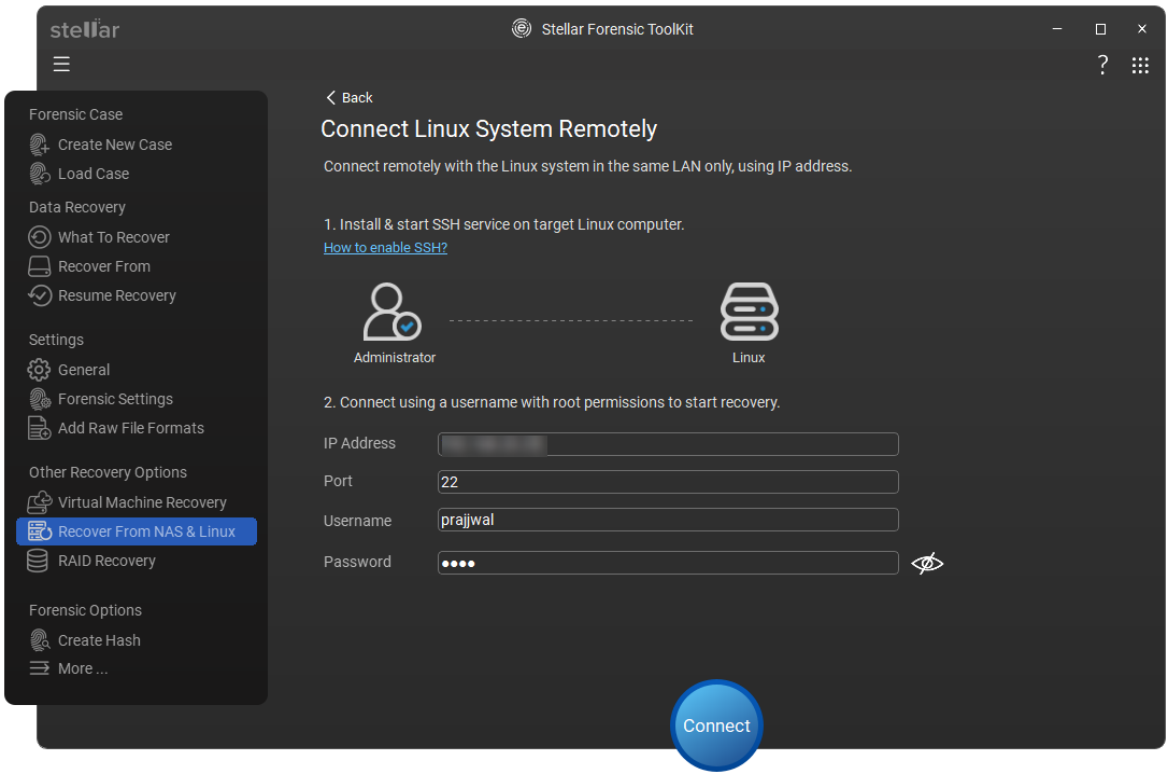
Steps to recover data from Linux system remotely:

1. Start Stellar Forensic Toolkit.
2. From the left navigation menu, Navigate to **Other Recovery Options.**
3. **From Other Recovery Options** section**,** select **Recover From NAS & Linux** option.
4. On **Recover From NAS & Linux System** screen, select **Linux Recovery** radio button and select **Next**.



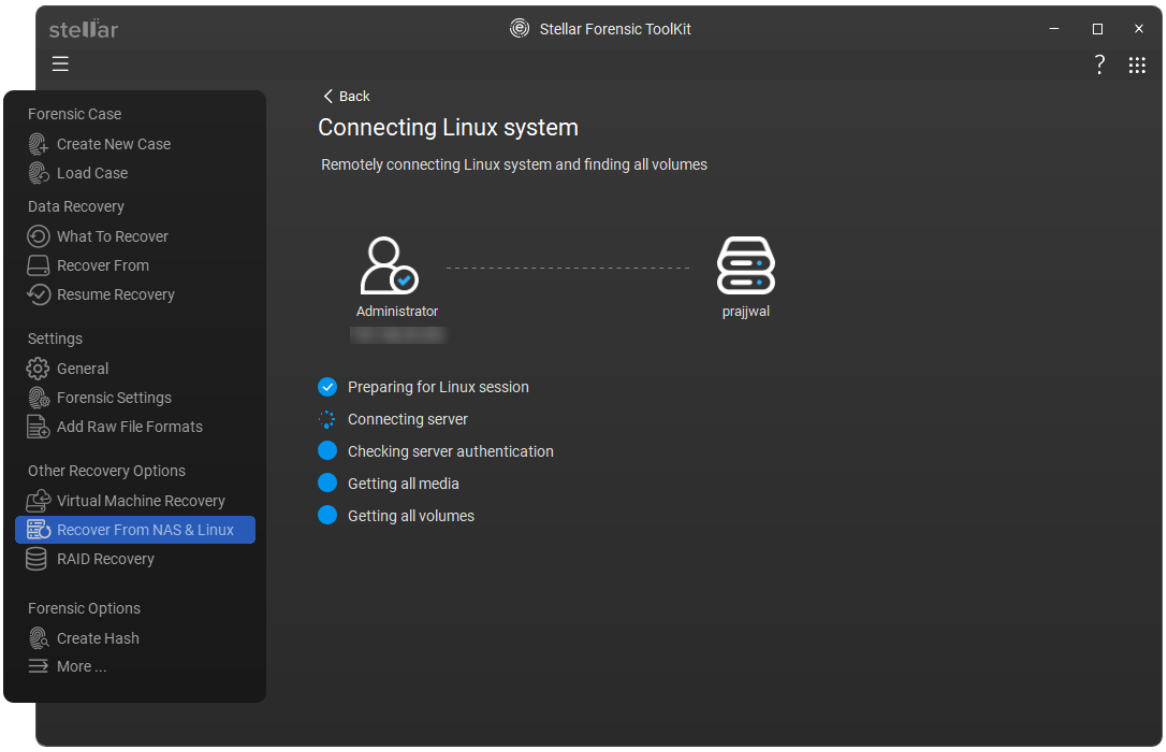
5. The **Connect Linux System Remotely** screen appears. Perform the following:

    - **IP Address:** Type the IP address of the Linux computer.
    - **Port:** Type the port number (Default is 22).
    - **Username and Password:** Type the administrator (root) credentials to allow access.

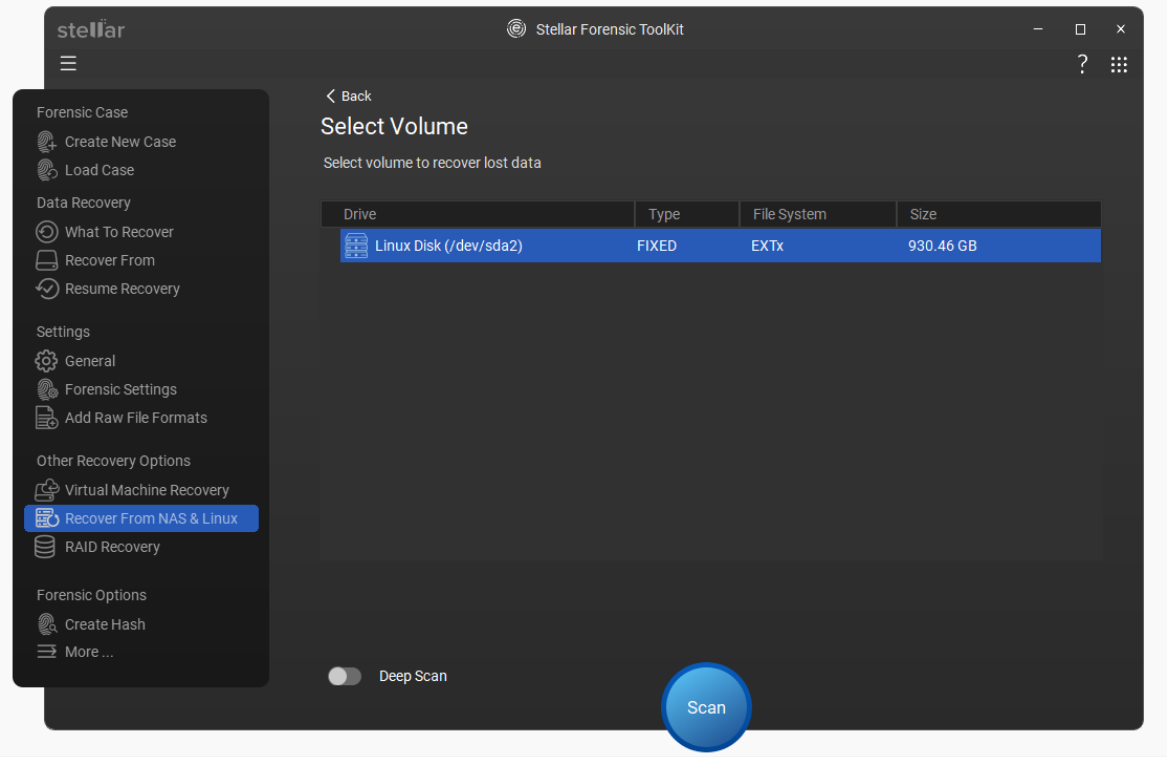


Note: *Make sure the SSH service is active on your NAS device. If you need help, click* ***'How to enable SSH?'*** *for more instructions.*

6. Select **Connect**. The software starts connecting and finding all volumes on the Linux system.

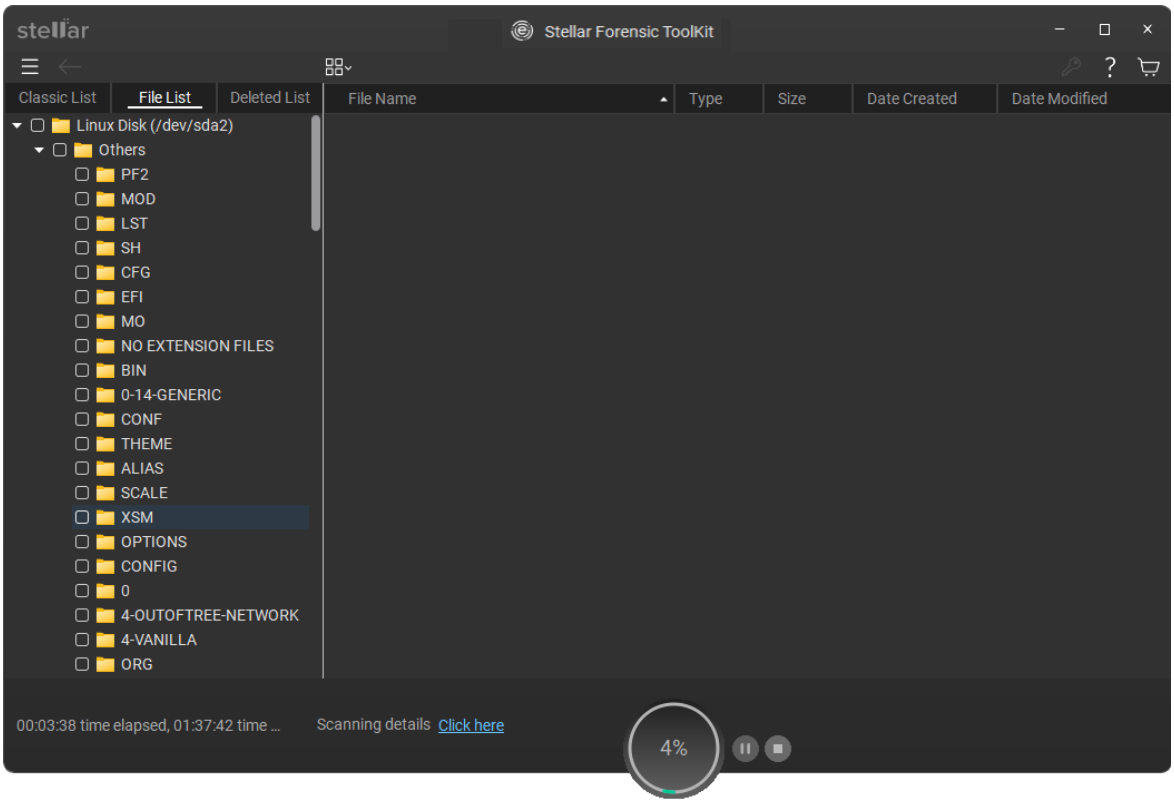


7. On the **Select Volume** screen, select the volume you want to scan for lost data.



Note: *You can enable* ***Deep Scan*** *at the bottom for a more thorough search.*

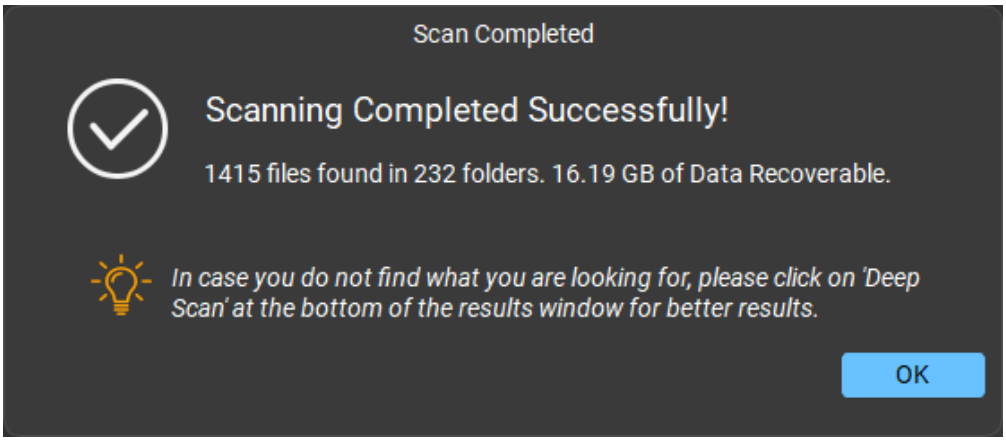
8. Select **Scan**. The software begins scanning process and shows the progress.



Notes:

- *To view detailed scan information, select **Click here** link near the scanning details. To save the scan information after the scan completes, select here.*
- *To stop, pause or resume the scan, select **Stop** or **Pause/Resume** button.*
- *To continue recovery later using saved scan information, select here.*

9. After the scan completes, application displays the list of files and folders found.



10. To preview and save the recovered files, see Preview Scan Results and Saving the Recovered Files.

4.10.1. Install and Enable SSH

SSH provides secure remote access to the NAS system from a Linux machine. It can be used for troubleshooting, advanced configuration, and system recovery.

Before you start, make sure:

- You have administrator (or sudo) privileges on the NAS.
- You know the IP address of NAS.
- You are logged in to a Linux system with terminal access.

Steps to Install & Enable SSH:

1. Open the **Terminal** application.
2. In Terminal, type following command:

```
sudo apt install openssh-server
```

3. Press **Enter.**
4. This will install the package and Enable the SSH.

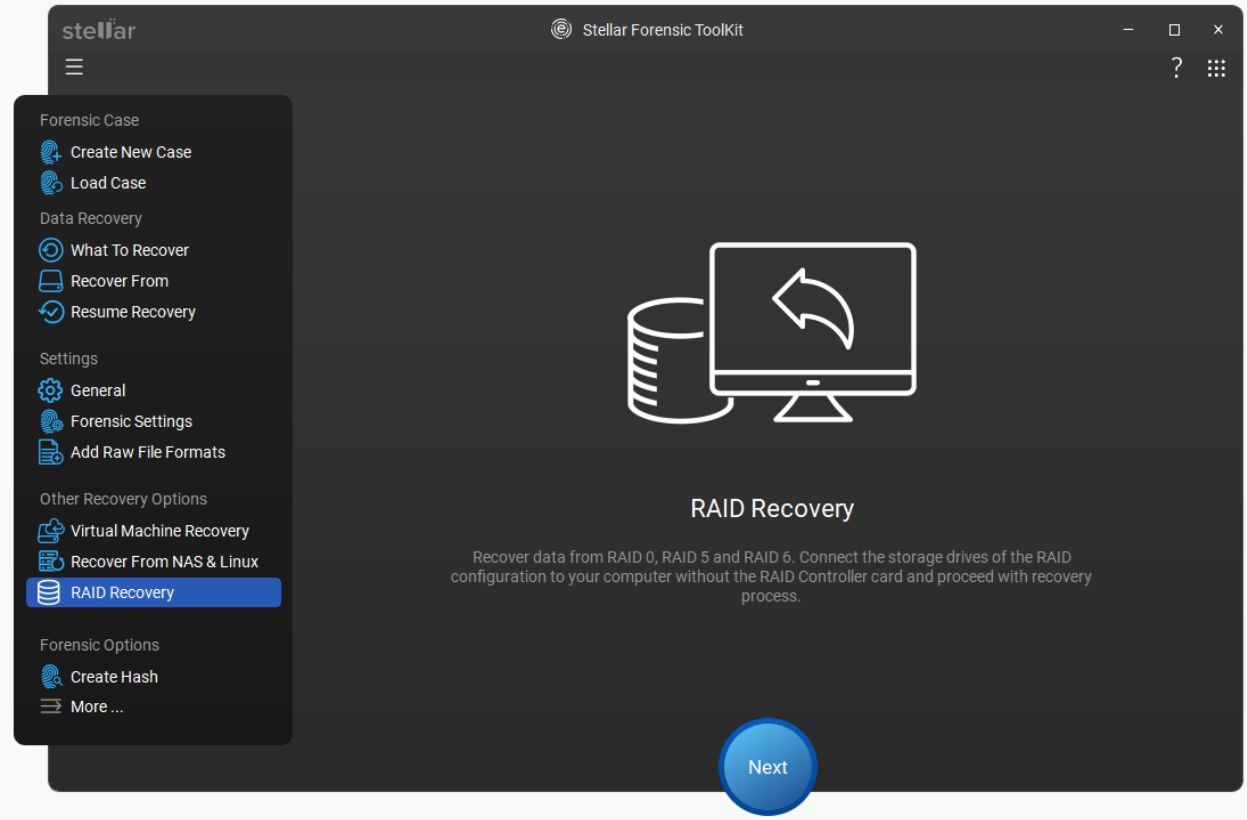
4.11. Work with RAID

4.11 Work with RAID

RAID, or Redundant Array of Independent Disks is a storage device made up of multiple disks. A **RAID**, connected to a system, is shown as one logical disk unit in the operating system. **RAID** is a way of storing the same data at multiple places (hard disks) to improve data access, data safety, performance, fault tolerance, and to increase the mean time between failures.

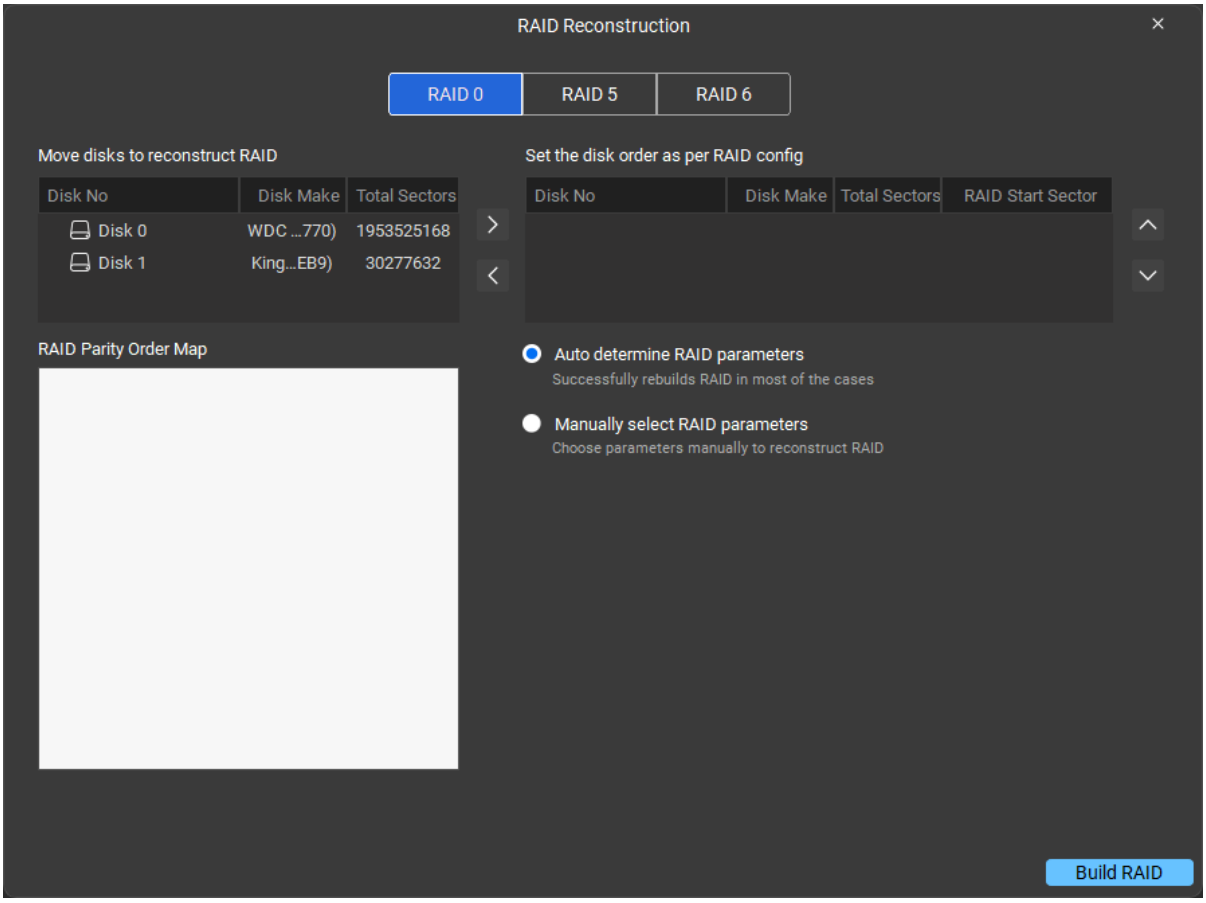
Stellar Forensic Toolkit supports data recovery from three **RAID** levels – **RAID 0, RAID 5**, and **RAID 6**.

RAID Reconstruction - Main User Interface screen



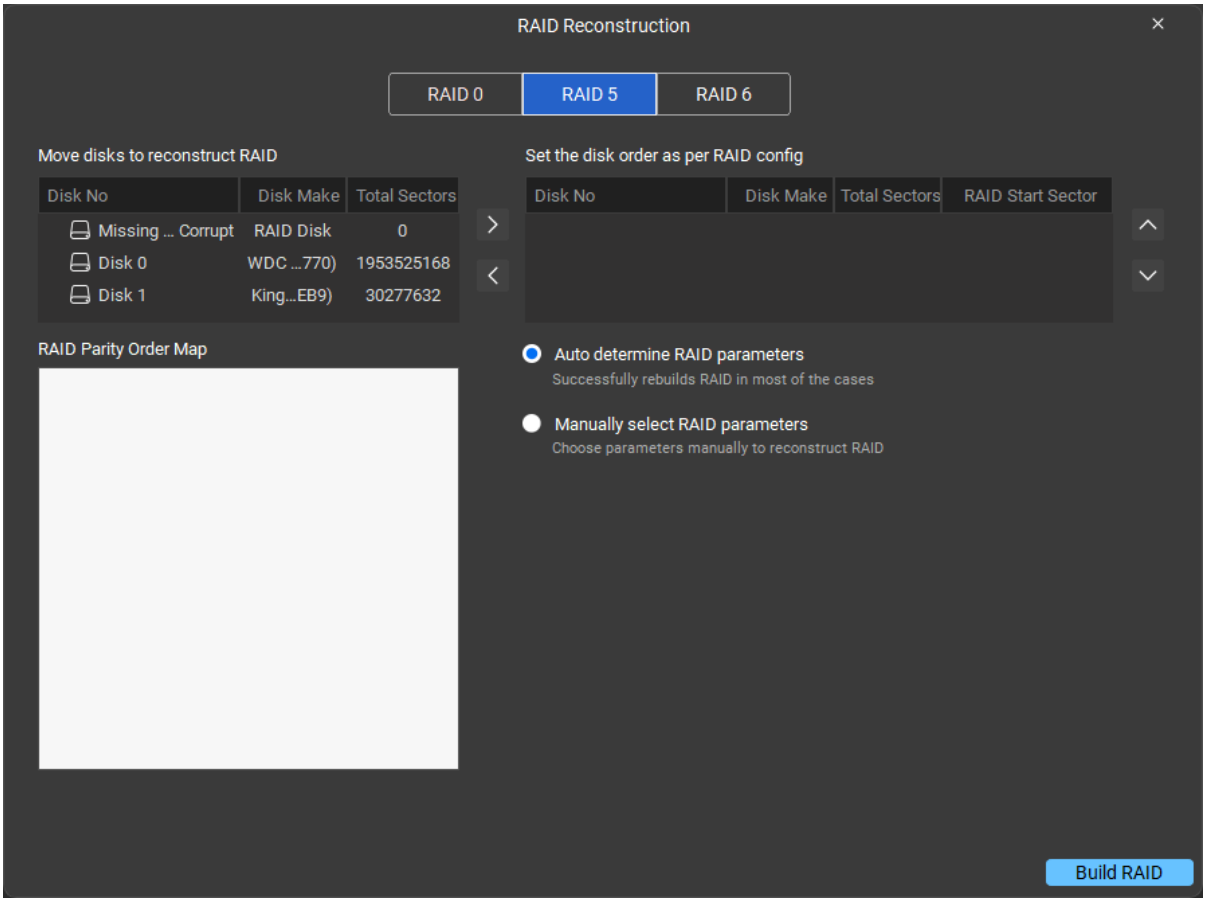
RAID Reconstruction - RAID 0 Screen

RAID 0 is the first level of **RAID** technology that uses block-level striping without parity or mirroring and has no (or zero) redundancy. **RAID 0** improves performance and storage but has no fault tolerance. Any drive failure will lead to total data loss and the chances of failure increases with an increase in the number of hard disks.



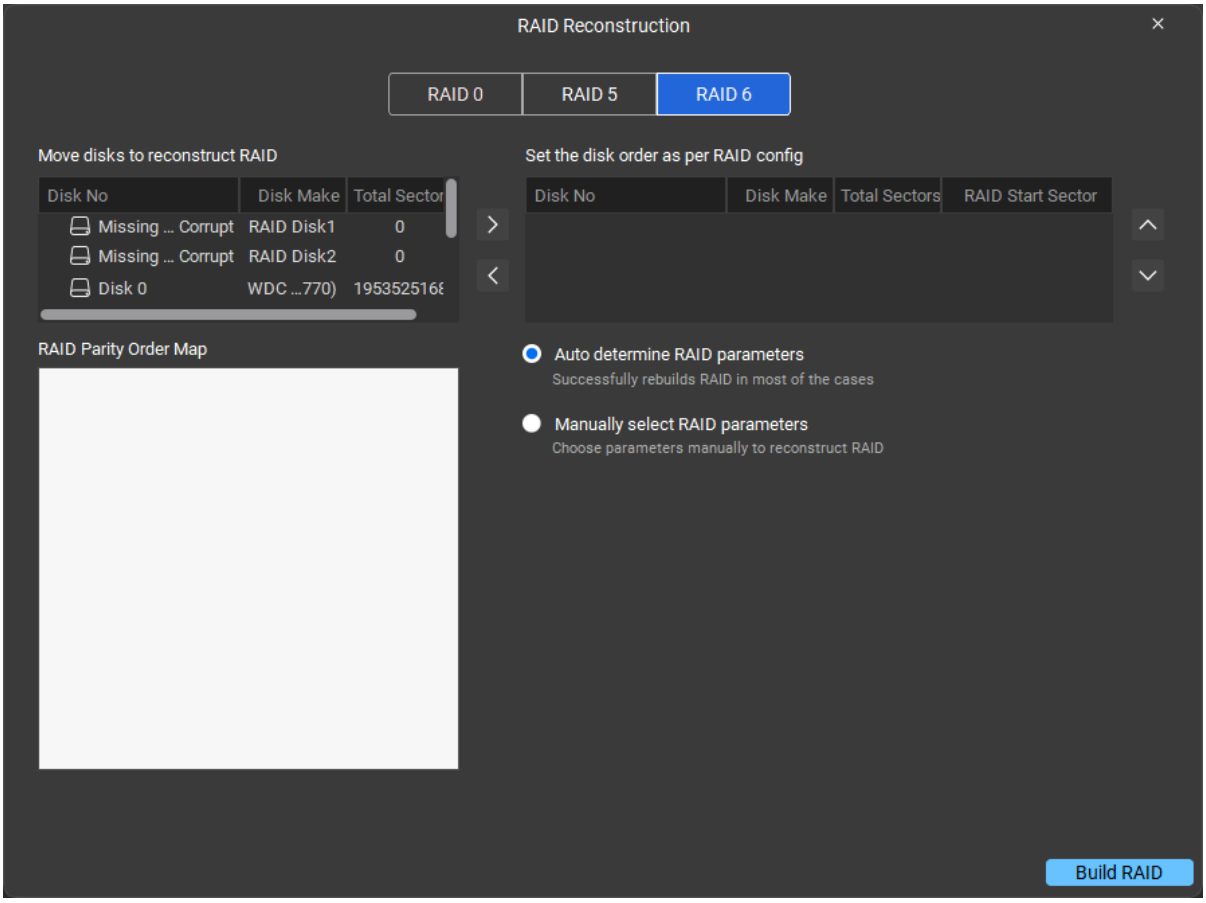
RAID Reconstruction - RAID 5 Screen

RAID 5 is another level of **RAID** technology, which uses distributed parity and distributed data technique. This level requires at least three hard disks and a single disk failure does not lead to total data loss.



RAID Reconstruction - RAID 6 Screen

RAID 6 level uses block-level striping with double distributed parity. This level requires a minimum of four disks and it can tolerate up to two hard disk failures. This **RAID** level technology is intended for high-availability systems and makes larger **RAID** groups more practical.



In this section, you will learn, how tol

4.11.1. Build RAID When Parameters are Unknown

4.11.2. Build RAID When Parameters are Known

4.11.3.Scan RAID Volumes

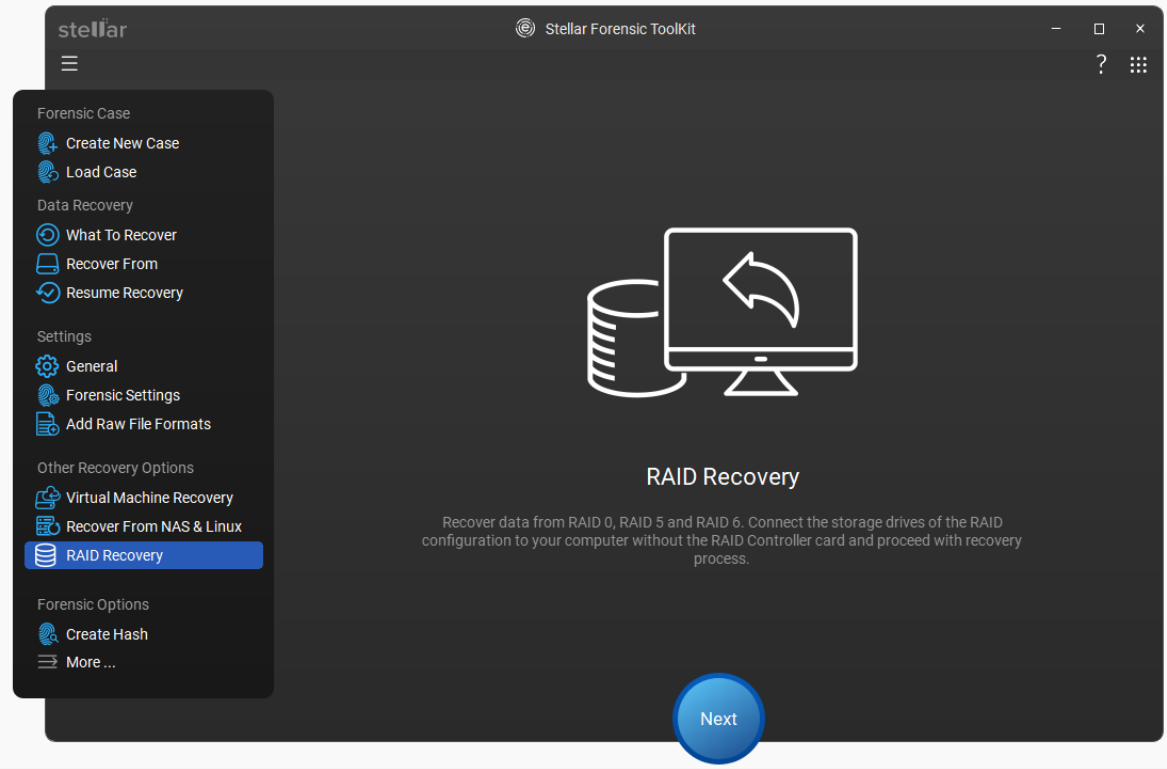
4.11.1. Build RAID When Parameters are Unknown

To build **RAID** using **Stellar Forensic Toolkit**, the user must preferably know the disk order, start sector of **RAID** in each disk, stripe/block size, parity repetition/delay, and parity order. If any **RAID** parameters are unknown, the user can select the **"Auto determine RAID parameters"** provided in the recovery window. This option automatically configures the optimal **RAID** settings for quick recovery, rebuilding the **RAID** in most cases while minimizing data loss and reducing manual intervention.

To build RAID when parameters are unknown:

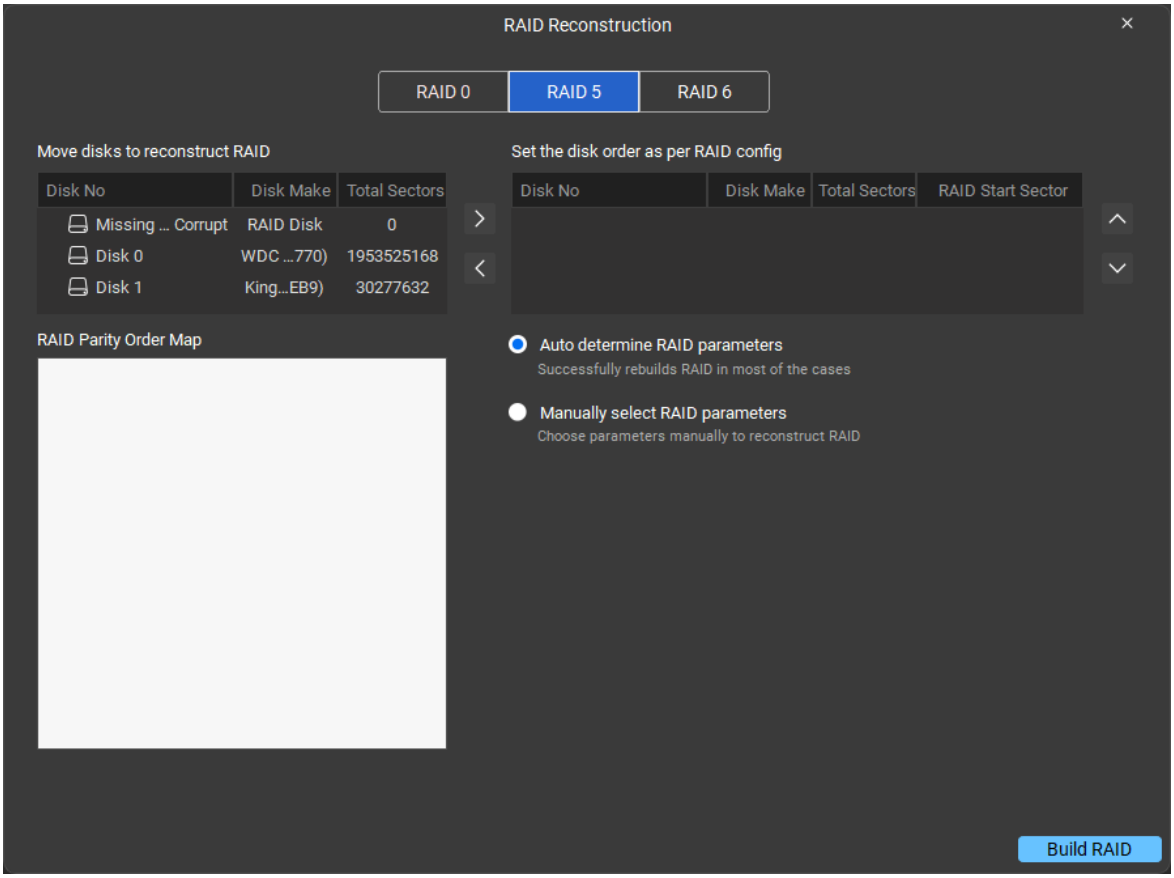
1. Run **Stellar Forensic Toolkit**.

2. From the side panel, under **Other Recovery Options**, select **RAID** Recovery.



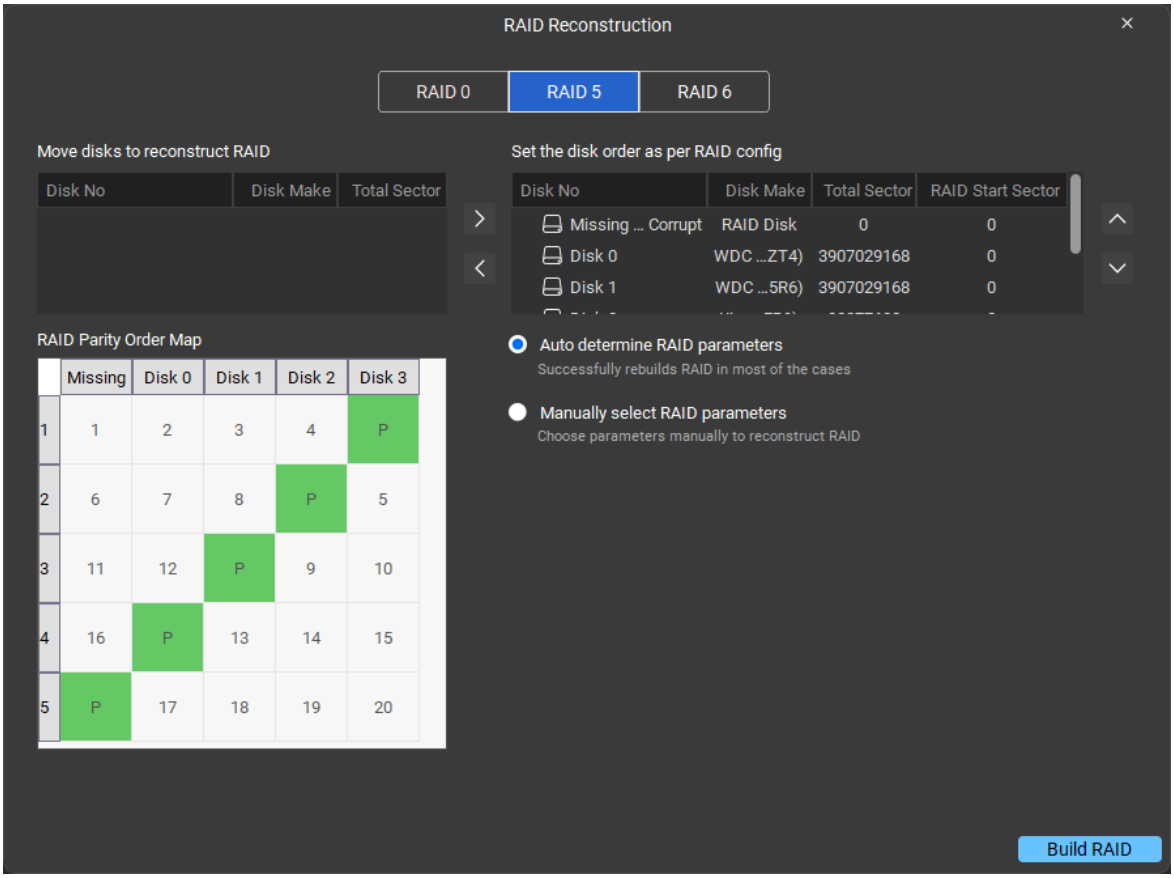
3. Click **Next**.

4. The **RAID Reconstruction** window is displayed. All the **RAID** drives and a missing drive are shown in **'Move disks to Reconstruct RAID'** section.



***Note: RAID 5** is selected by default because it's the most common setup for data protection with parity. **RAID 0** is not selected as it offers no redundancy (backup), and **RAID 6** is less commonly used. You can manually change the **RAID** level to **RAID 0** or **RAID 6** if needed.*

5. In the '**Move disks to Reconstruct RAID**' section, click on a **RAID hard disk** and then click  Repeat this till all the **RAID** disks are shown in the '**Set the disk order as per RAID config**' section.



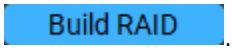
6. In **Set the disk order as per RAID config** section, click on a **hard disk** and then click  or  to change its order. Repeat this till all the drives are set in the correct order. Double click the block under **RAID start sector** to type the starting sector.

   Note: *Ensure at least 3 disks are selected to build the **RAID**. Add a 'Missing' disk to replace any failed disk.*

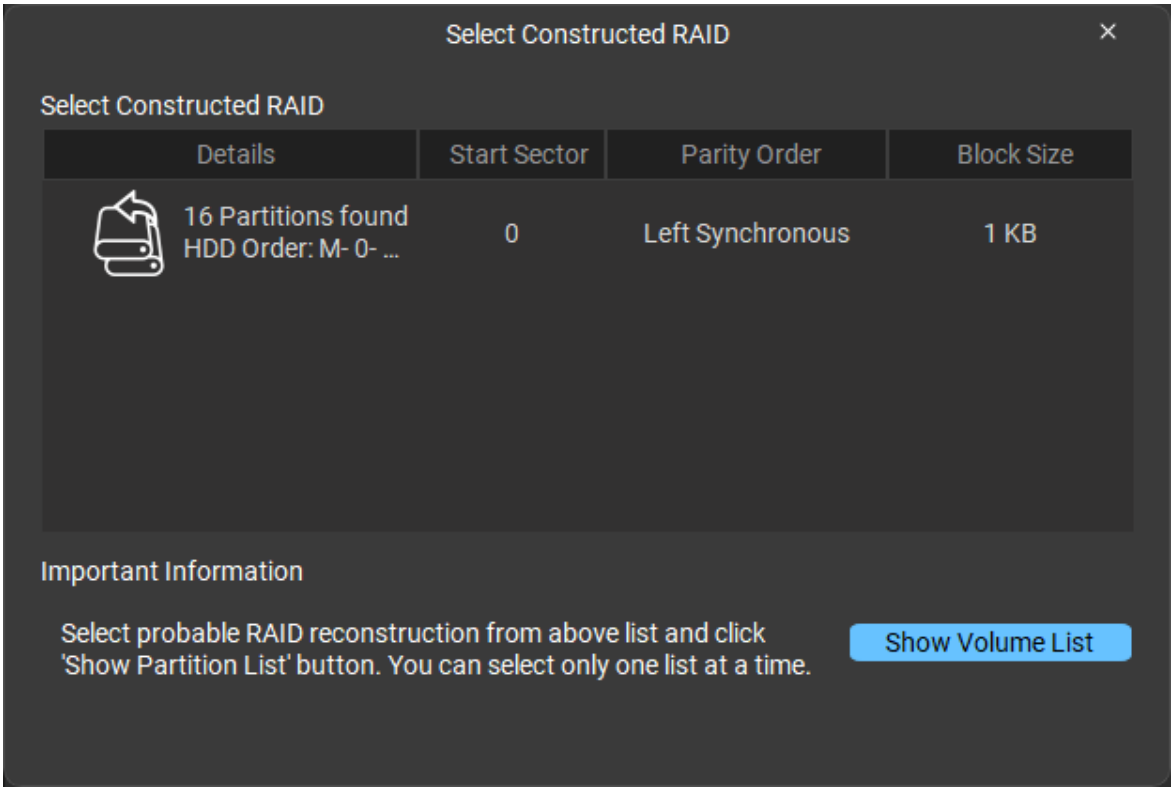
7. If you're unsure of the parameters, select the "**Auto determine RAID parameters**" radio button. This option automatically configures the optimal **RAID** settings for quick recovery, rebuilding the **RAID** in most cases while minimizing data loss and reducing manual intervention.

   Note: *When you select **Raid 0**, you need to select at least 2 disks to build **RAID**.*

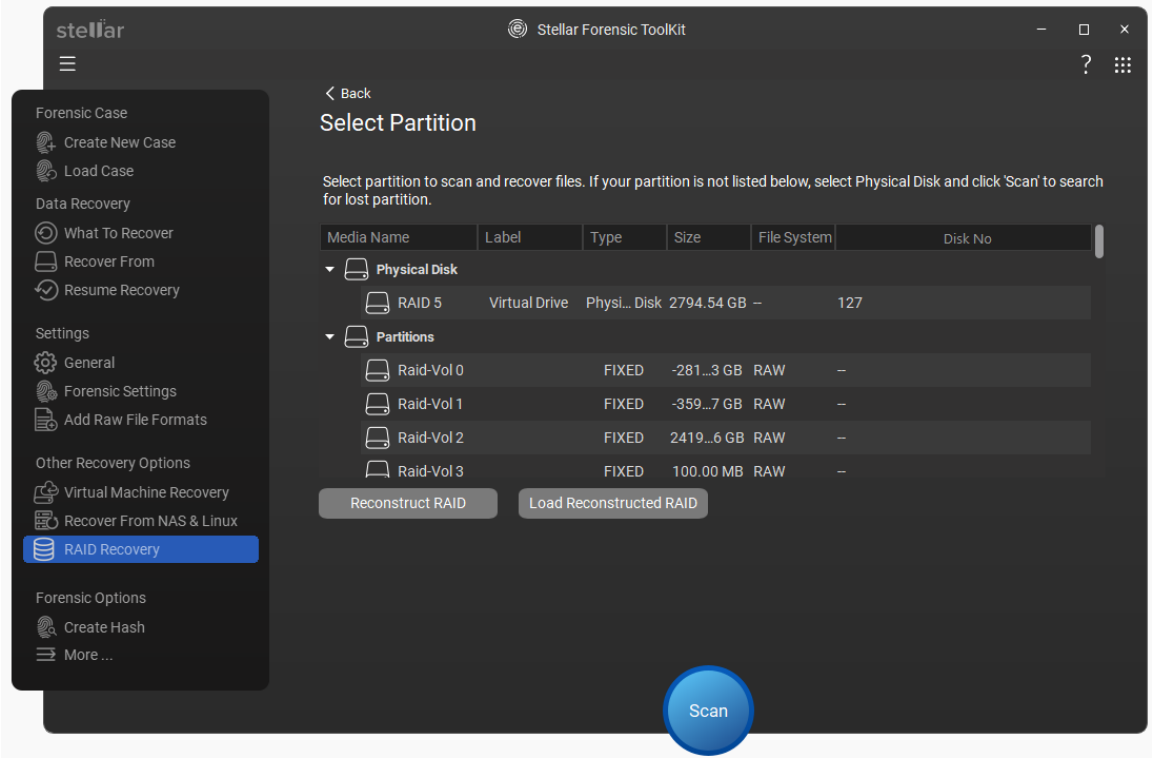
   Note: *When you select **Raid 6**, you need to select at least 4 disks to build RAID. And, add a '**Missing disk'** to replace a failed disk.*

8. Click  . The recovered **RAID** is shown.

9. If you have used the "**Auto determine RAID parameters**" option for one or more of the **RAID parameters**, a list of probable **RAIDs** are constructed and shown in a list. **RAID** information is also shown. Select one of the **RAIDs** according to its score and click the **Show Volume List** button.



10. **RAID** volumes are shown on the **Select Partition** screen.



Note: *If the desired partition is not listed in the list, select physical disk and click* ***Scan*** *to search for lost partition.*

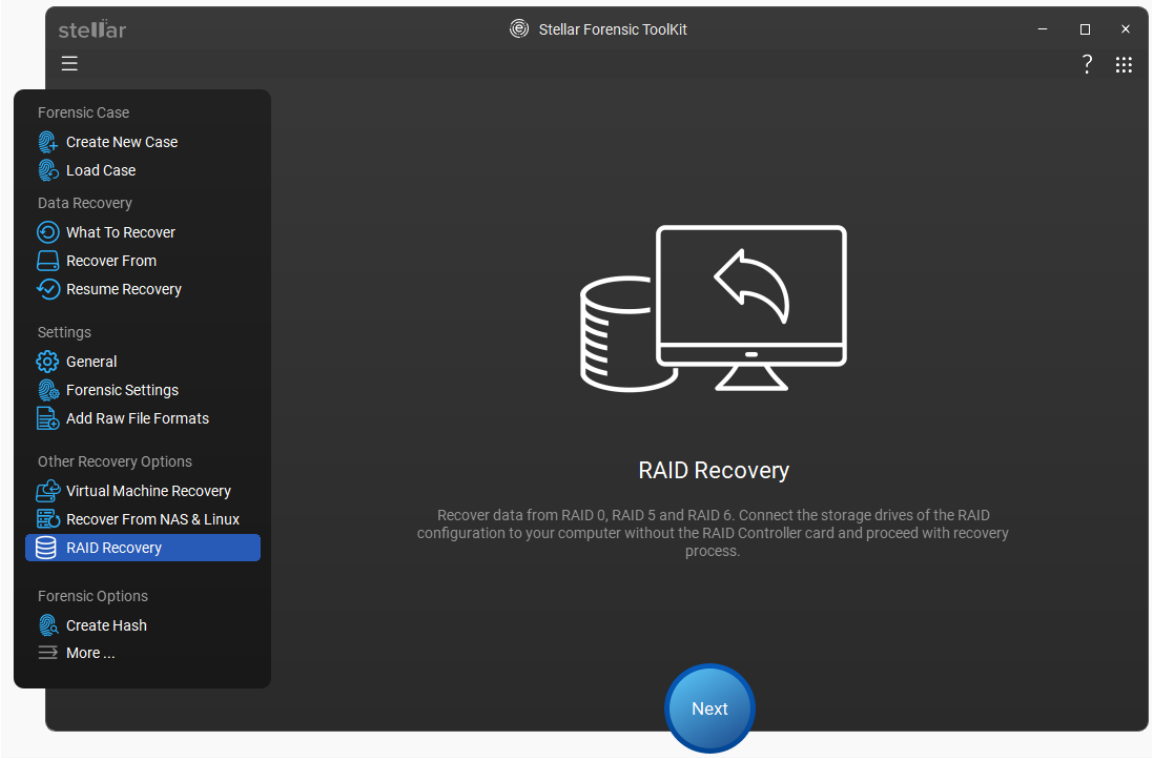
11. Click the **Reconstruct RAID** button to perform construction once again, or click **Load Constructed RAID** button to select another constructed **RAID** from the list of probable **RAIDs**.

4.11.2. Build RAID When Parameters are Known

To build **RAID** using **Stellar Forensic Toolkit**, you must preferably know the disk order, start sector of **RAID** in each disk, stripe/block size, parity repetition/delay, and parity order. Multiple possible **RAIDs** are constructed according to the combination of parameter options that you provide. User has to choose from any one of them. After the **RAID** is rebuilt, you can perform scanning and recovery operations on the **RAID** volumes.

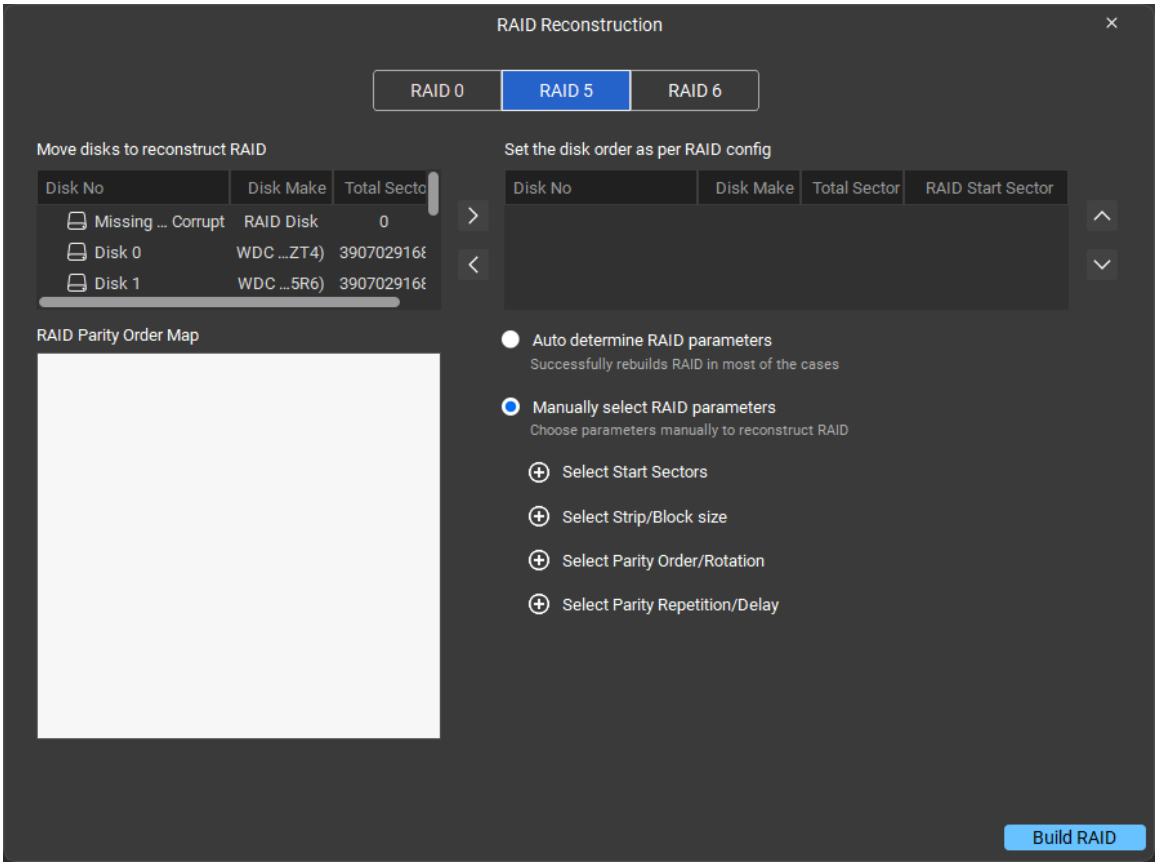
To build RAID when parameters are known:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Other Recovery Options**, select **RAID Recovery**.

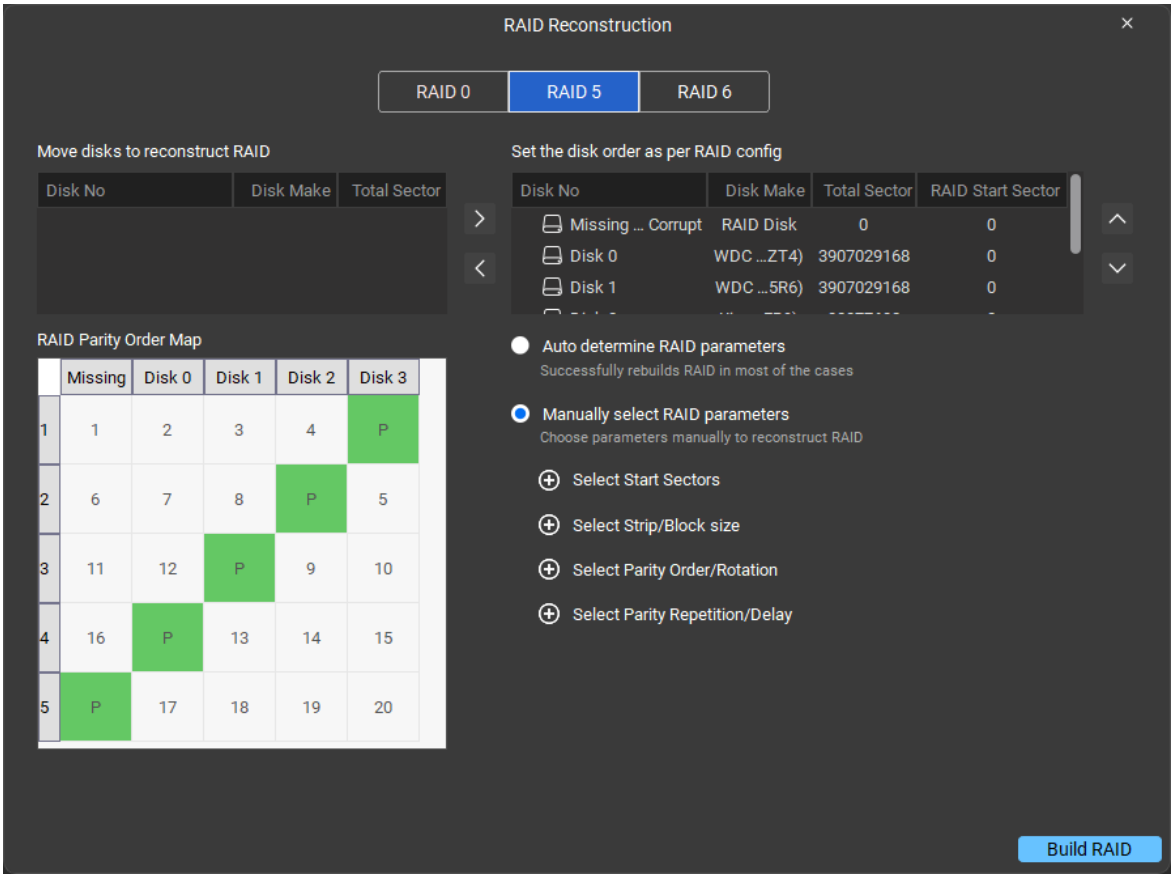


3. Click **Next**.

4. The **RAID Reconstruction** window is displayed. All the **RAID** drives and a missing drive are shown in '**Move disks to reconstruct RAID**' section.



5. In the '**Move disks to reconstruct RAID**' section, click on a **RAID hard disk** and then click . Repeat this till all the **RAID** disks are shown in the **Set the disk order as per RAID config** section.



6. In the **Set the disk order as per RAID config** section, move hard drives up/down for disk order, click on a hard disk and then click  or  to change its order. Repeat this till all the drives are in the correct order. Double click the **block** under **RAID Start Sector** to type the starting sector.

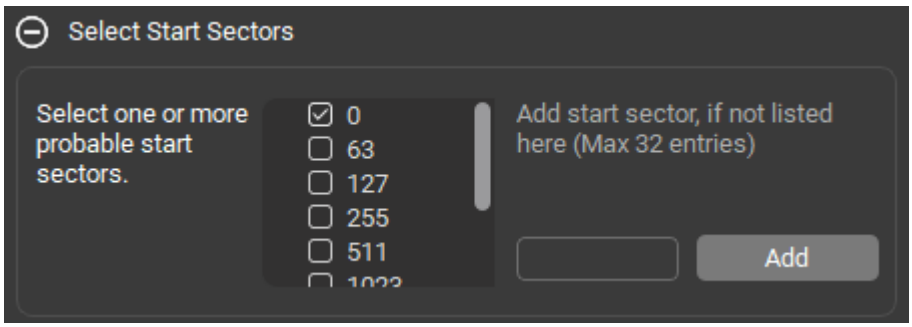
7. Select the **RAID parameters:** Choose between **Auto determine RAID parameters** and **Manually select RAID parameters**.

    i. **Auto determine RAID parameters:** Auto-determining **RAID** parameters automatically identifies and configures the optimal **RAID** settings, ensuring quick recovery. It successfully rebuilds the **RAID** in most cases, minimizing data loss and manual intervention. If any of the **RAID** parameters are unknown, the user can select the "**Auto determine RAID parameters**" option in the recovery window. Click "Auto-determine RAID parameters" to learn how to use it.

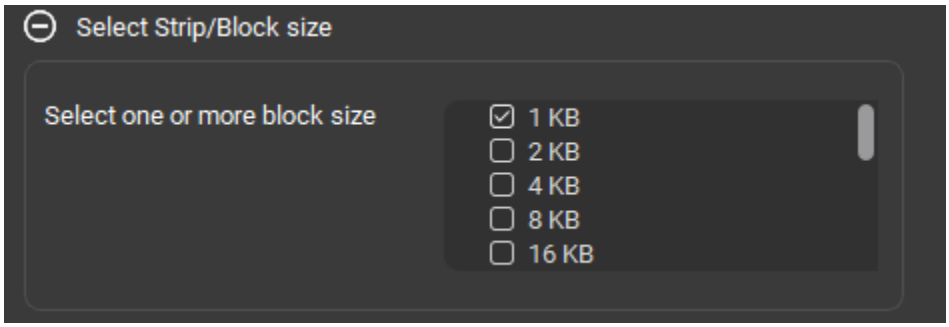
    ii. **Manually select RAID parameters:** Manually selecting **RAID** parameters allows users to define settings like **Select start sectors**, **Strip Size / Block size**, **Parity Order / Roatation**, and **Parity Repetition / Delay** or when automatic detection fails.

    To choose parameters manually, select following parameters:

a. Expand the **Select Start Sector** icon to view and choose from available start sectors. You can then select one or more probable start sectors for the reconstruction process. Click the **Add** button to manually enter a start sector if it's not listed, with a maximum of **32 entries** allowed.

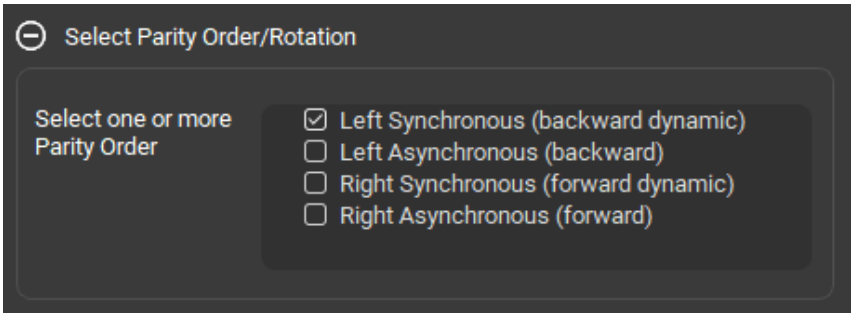


b. Expand the **Strip/Block Size** to view and select the desired **strip/block size**. You can choose one or more block sizes as needed.

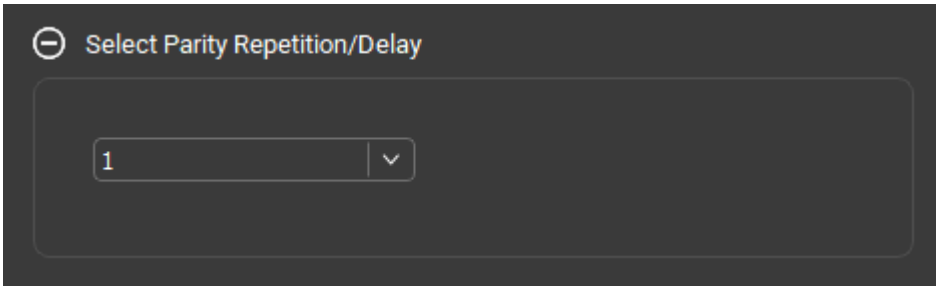


c. Expand the **Select Parity Order/Rotation** icon**.**

- Select one or more parity orders by selecting the boxes from the four available options:
  - **Left Synchronous (Backward Dynamic)**
  - **Left Asynchronous (Backward)**
  - **Right Synchronous (Forward Dynamic)**
  - **Right Asynchronous (Forward)**

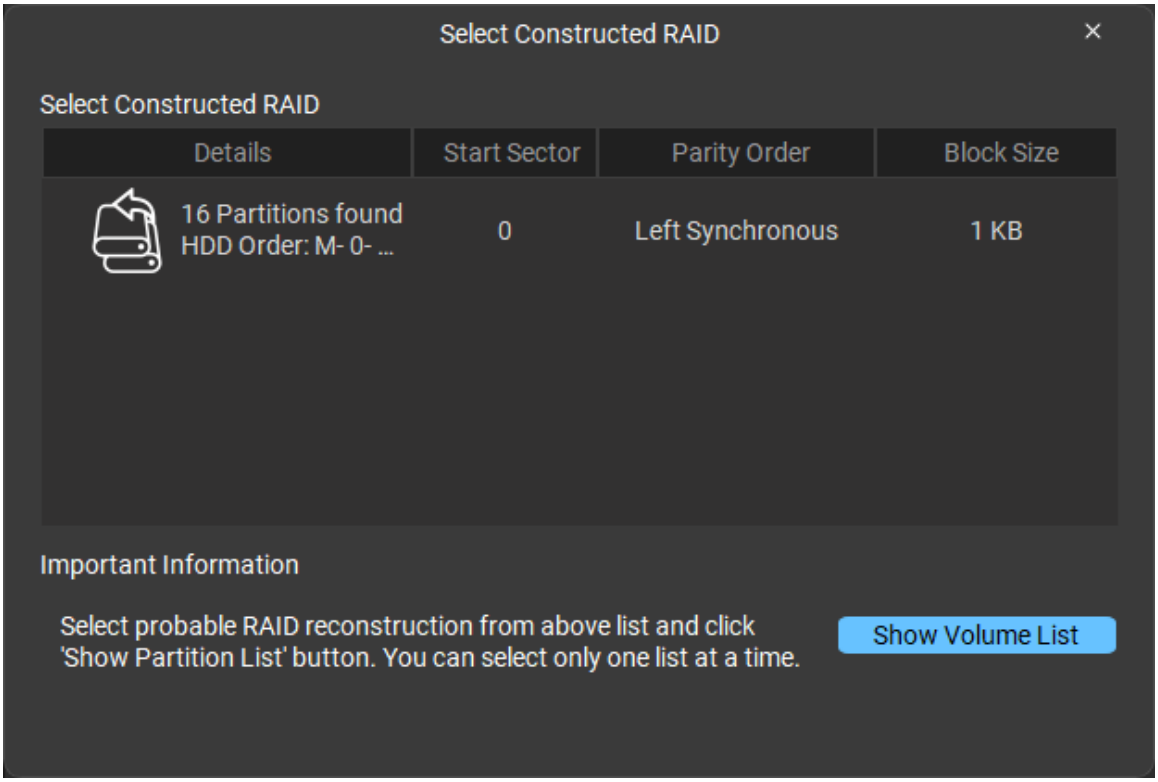


d. Expand the  **Select Parity Repetition/Delay** icon to choose up to a maximum of **32 entries** from the dropdown menu.

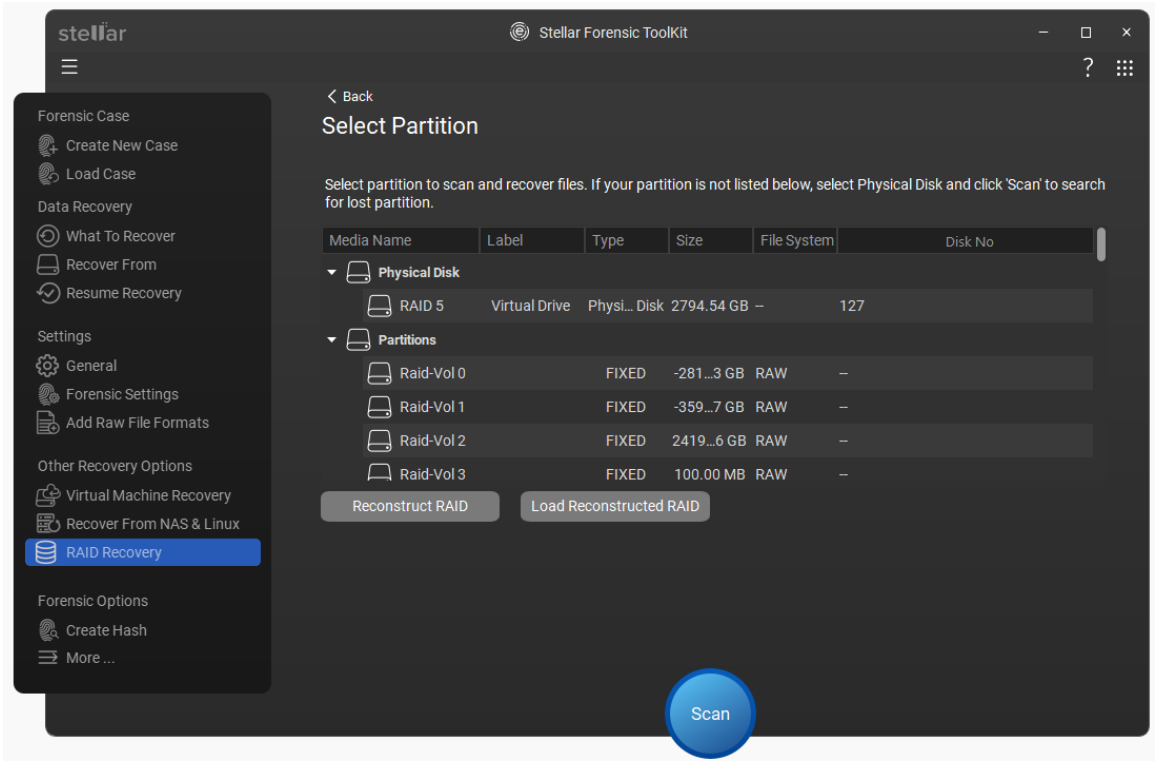


Note: *In **RAID 0**, you have only two options available: **Start Sectors** and **Strip/Block size**. In **RAID 6**, you get all the options available in **RAID 5**, along with an additional option to select **RAID 6 Type**.*

8. Click Build RAID. A single **RAID** is shown. Select it and click the **Show Volume List** button to continue recovery. The found volume and the **RAID** are shown under the **RAID Recovery** button on the main screen.



9. If **Stellar Forensic Toolkit** is not able to build a **RAID** and no volume is found, select physical disk and click **Scan** to search the lost partition.



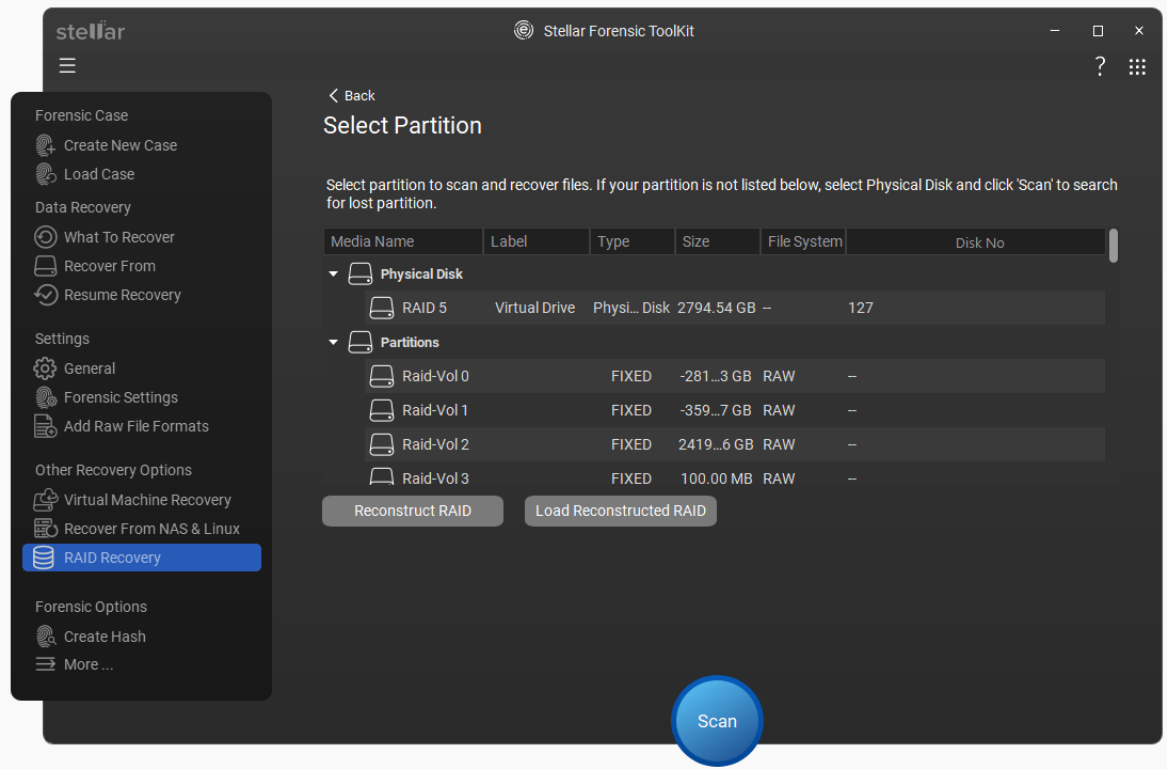
10. Click the **Reconstruct RAID** button to perform construction from once again, or click **Load Constructed RAID** button to select another constructed **RAID** from the list of probable **RAIDs**.

4.11.3. Scan RAID Volumes

After you have built a **RAID**, all **RAID** volumes will be displayed in the **RAID Recovery** screen. You have to scan a **RAID** volume to recover data in that volume. You can select only one volume at a time for scanning. Almost all the data in the files and folders will be found by performing recovery on the selected volume or removable media. **FAT**, **NTFS** and **exFAT** file systems are supported by the software.

To scan RAID volumes:

1. After you built **RAID**, **RAID volumes** are displayed in the **Select Partition** screen.
2. Select the volume to be recovered and click **Scan**.



3. Recover your data using the options given below:

- Recovering Data from Existing Volume: You can recover your deleted or lost data from the hard drive or external storage media connected to the system

- Performing a Deep Scan: In case, your desired file is not included in the list of files detected, you can opt for Deep Scan to perform a comprehensive scan of the selected drive or location.

  Note: *The option to save scan information is not available for RAID Recovery.*

4.12. Preview Scan Results

4.12. Preview Scan Results

Sellar Forensic Toolkit shows the files and folders present in the scanned physical volume or the removable media. All files and folders that are found in the scanned volume or removable media are shown in a two-pane structure. The two panes are the left and right pane.

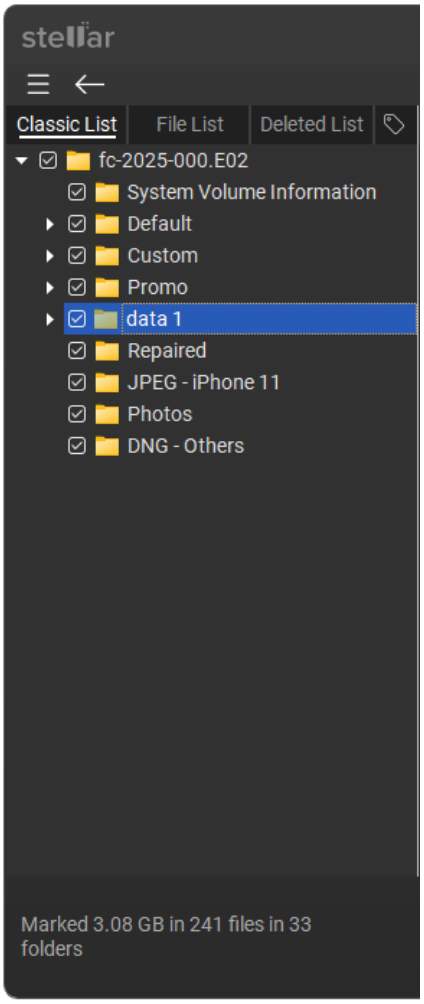
- In the left-pane, a tree structure according to folders is created.
- Right pane, all files and folders that are in the selected folder in the tree view are listed.

Change the Scan Result View:

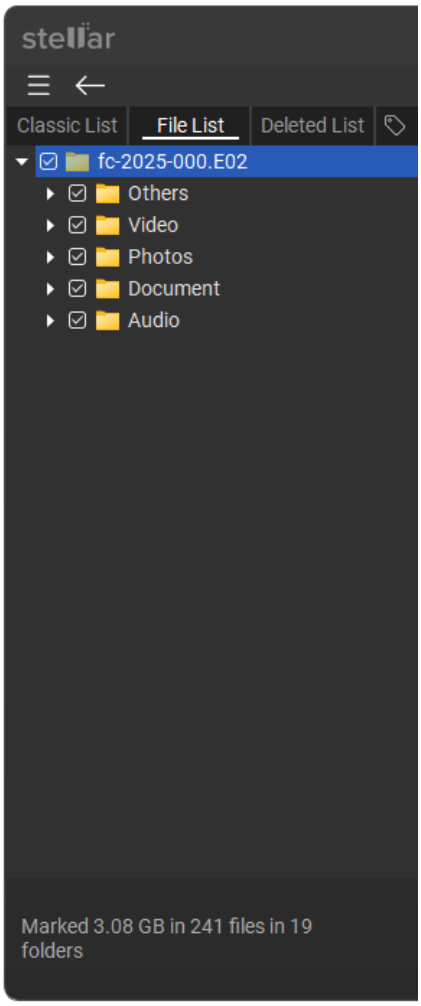
Stellar Forensic Toolkit provides the following four types of previews to view lost or deleted files/folders before recovering them:

- Classic list
- File list
- Deleted list
- Tag List

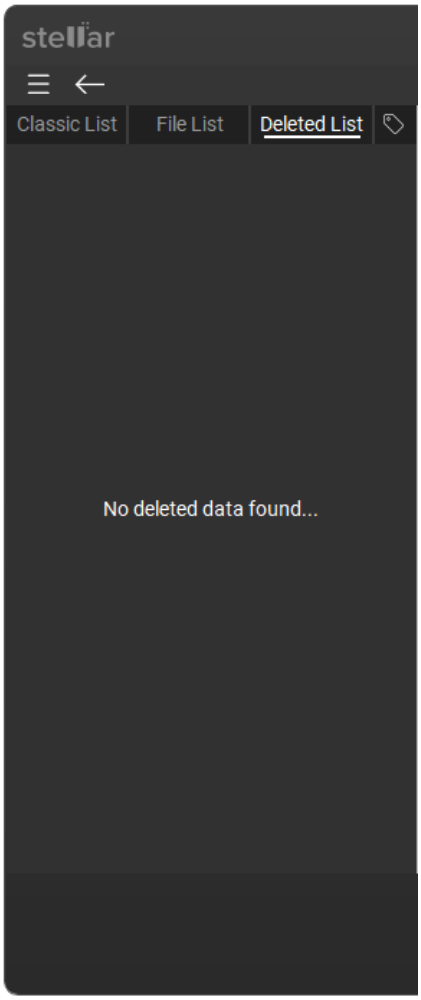
1. **Classic List:** In this view, files/folders are listed as they are found in the hard disk. To see the **Classic List** preview, click the **Classic List** tab in the **preview window**.



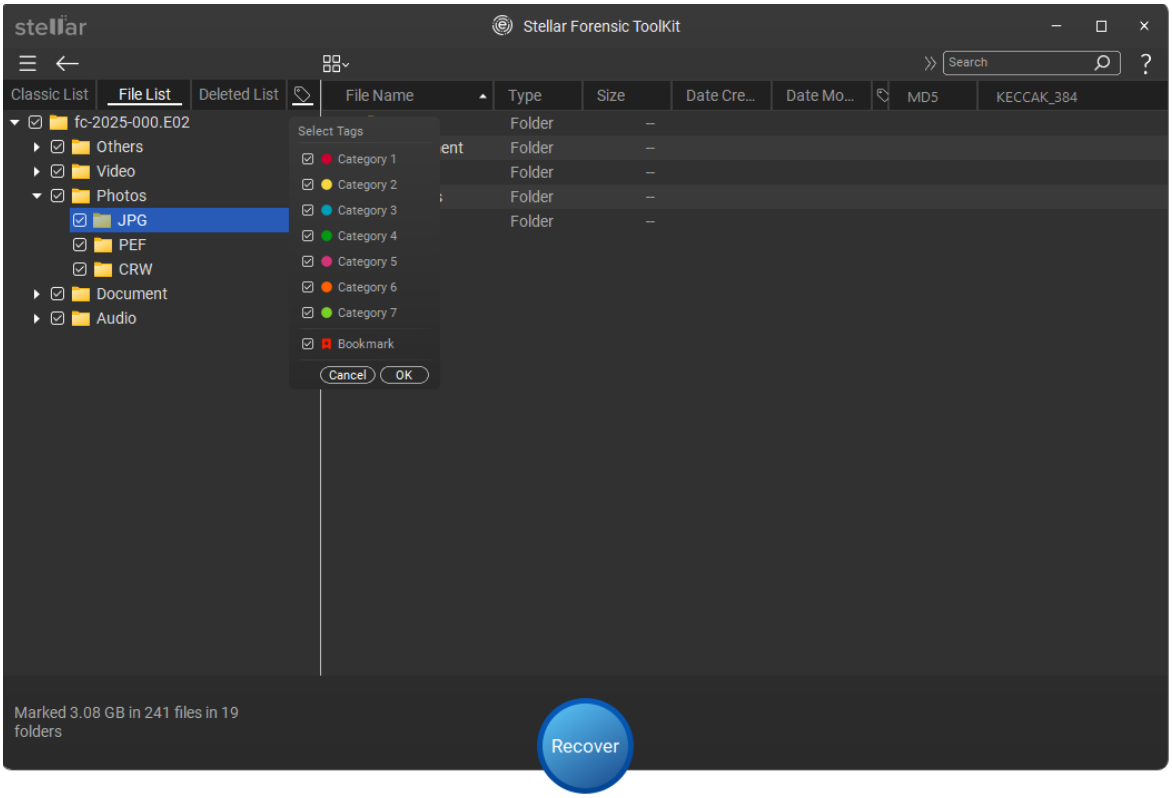
2. **File List:** In this view, files/folders are listed according to their type such as **Document**, **Audio**, **Video**, **Archive**, etc. To see the **File List** preview, click the **File List** tab in the **preview window**.



3. **Deleted List:** You can see the list of deleted and raw files in this preview. Click the **Deleted List** tab. A dialog box prompts as shown.



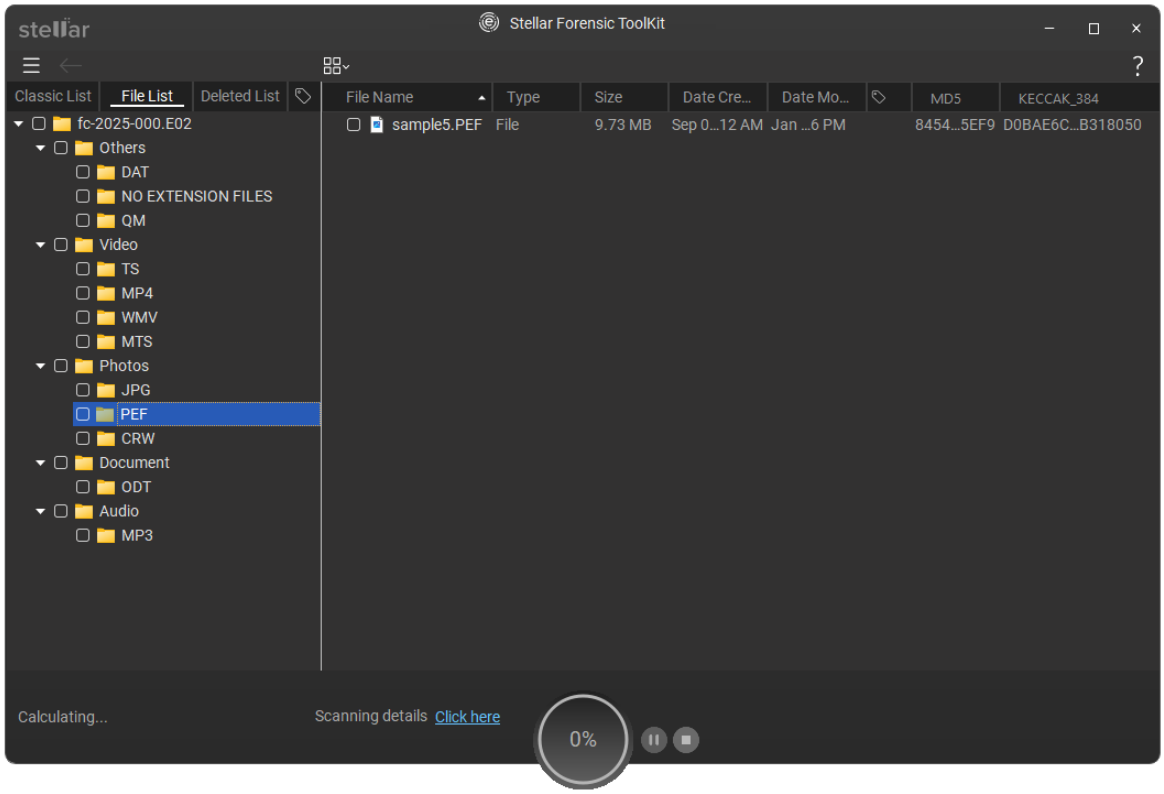
4. **Tag List:** You can select tags by checking the category checkbox corresponding to the category color. For more Information, click here.



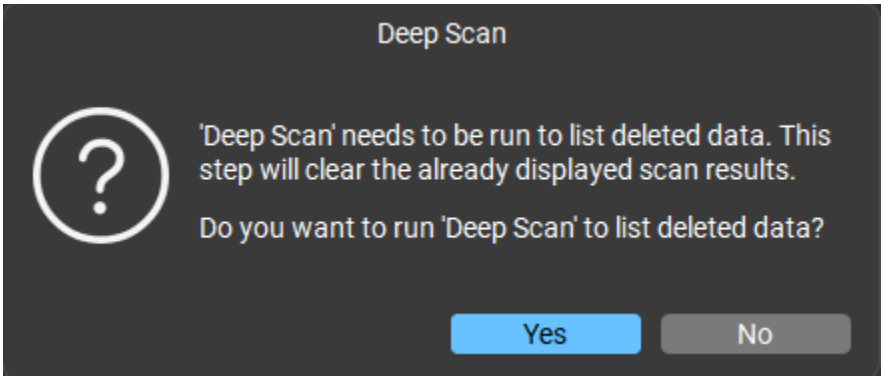
Stellar Forensic Toolkit will list the specific files in the preview window.

Note: *In the* ***demo*** *version of the product, you cannot see the preview of files having* ***size greater than 10 MB****. In the* ***full*** *version of the product, you cannot see the preview of files having size* ***greater than 100 MB****.*

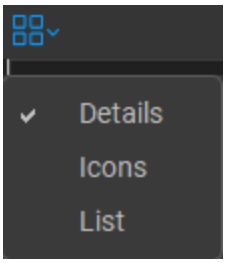
5. After the scanning process is completed, all the files are listed in a **tree view**, as shown below:



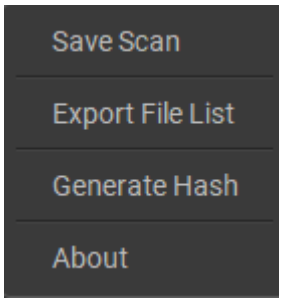
Note: *If you stop the quick scan or it doesn't complete, the* ***Deleted List*** *tab shows no data. To list deleted data, you need to perform a* ***Deep Scan****, which will clear the already displayed scan results.*



Note: *You can also switch between* ***Details***, ***Icon*** *and* ***List*** *view by clicking the*  *at the top of the screen.*

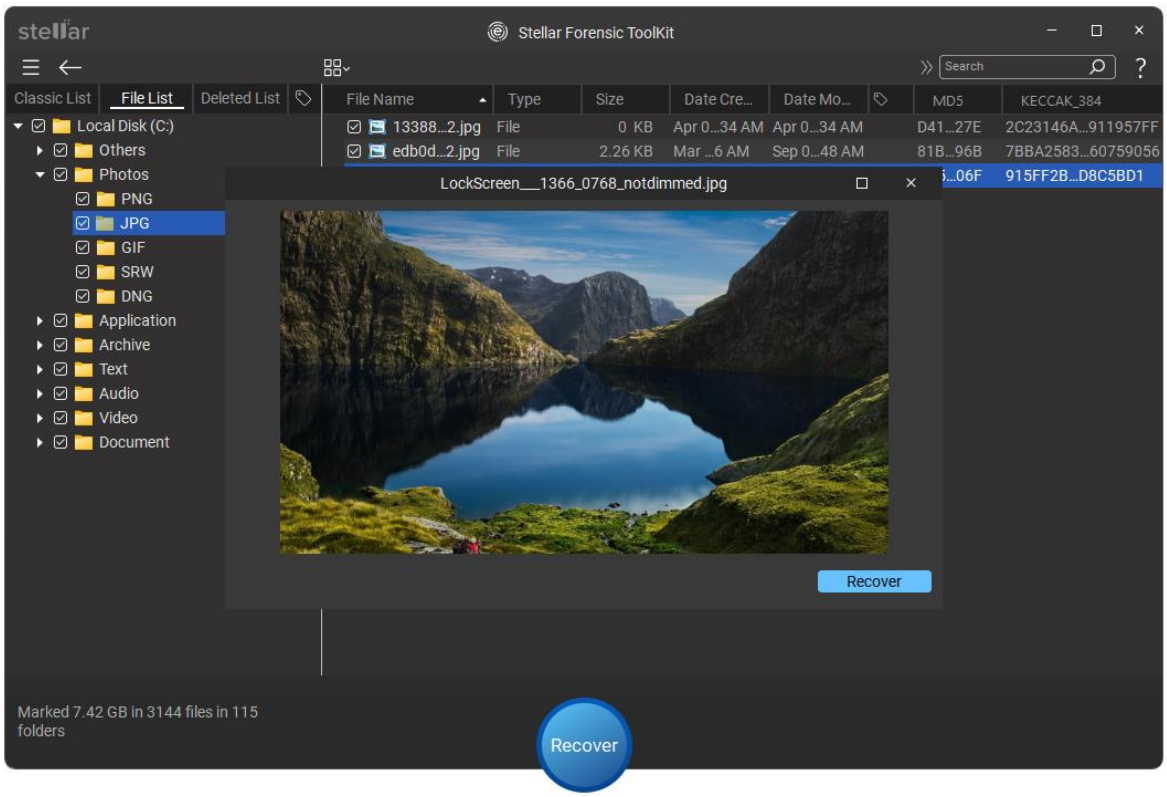


6. Click on the tab in the left pane to view your data in **Classic List**, File List or Deleted List. You can also export and save the mentioned file lists at your preferred location in html format using the **Export File List** button provided in the **More options** button.



Steps to Preview the files:

1. Expand the tree structure and click the desired folder in the left pane.
2. Double-click the file in the right pane that you want to preview.
3. A new window opens with the preview of the selected file.

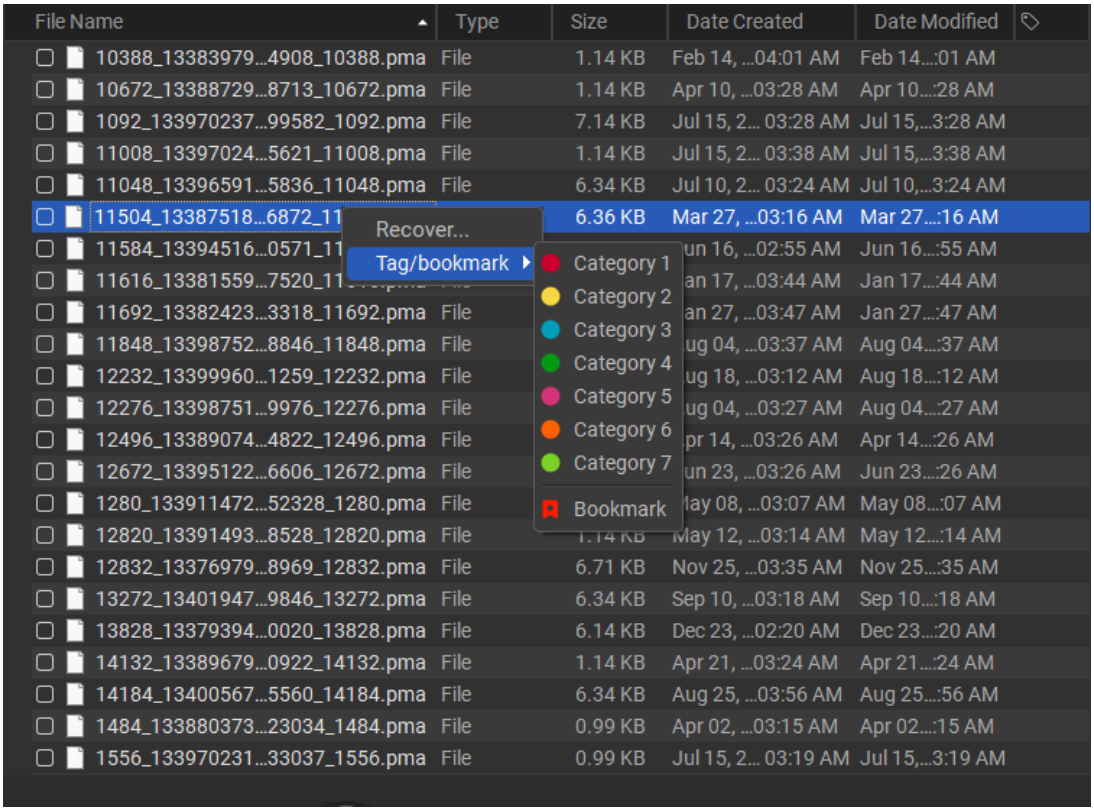


Note: *If you can't find your desired file/folder in the list of scanned and detected files, you can choose* ***Deep Scan*** *option to perform a comprehensive scan of the selected drive.*

How to Tag/Bookmark the File/Items

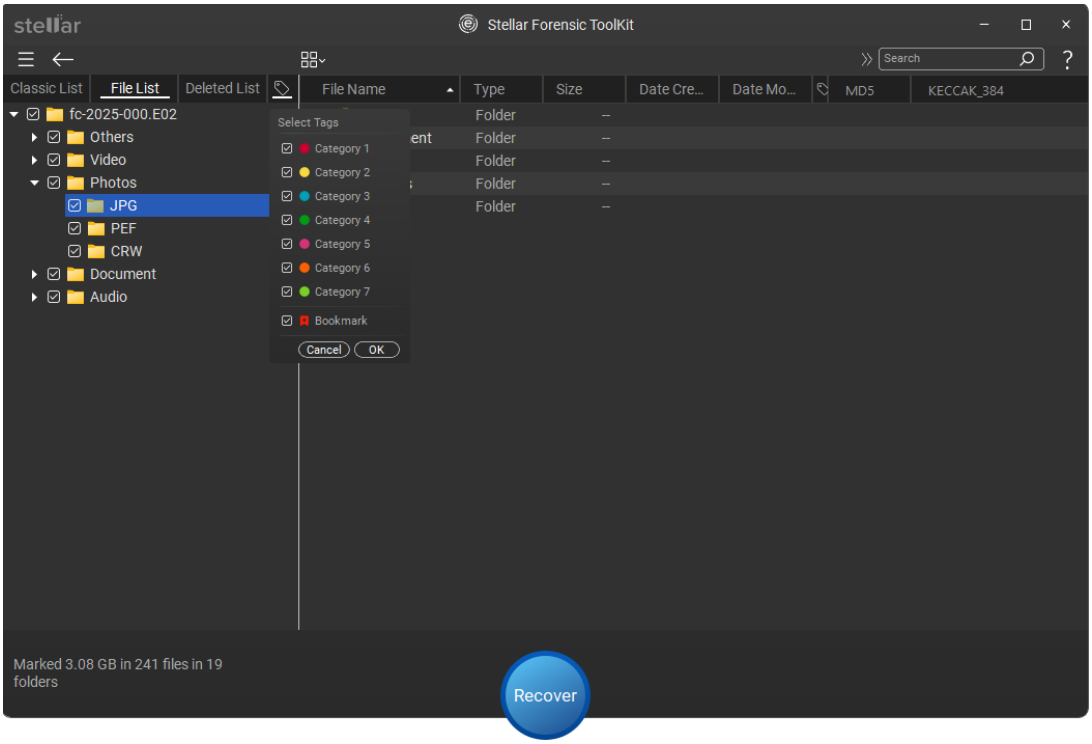
To tag a file/items, follow these steps:

1. While scanning, right-click on the desired file/items.
2. A dropdown menu appears with two options: **Recover** and **Tag/Bookmark**.
3. Select the **Tag/Bookmark** option.
4. From the **Tag/Bookmark** menu, choose the desired category or bookmark.

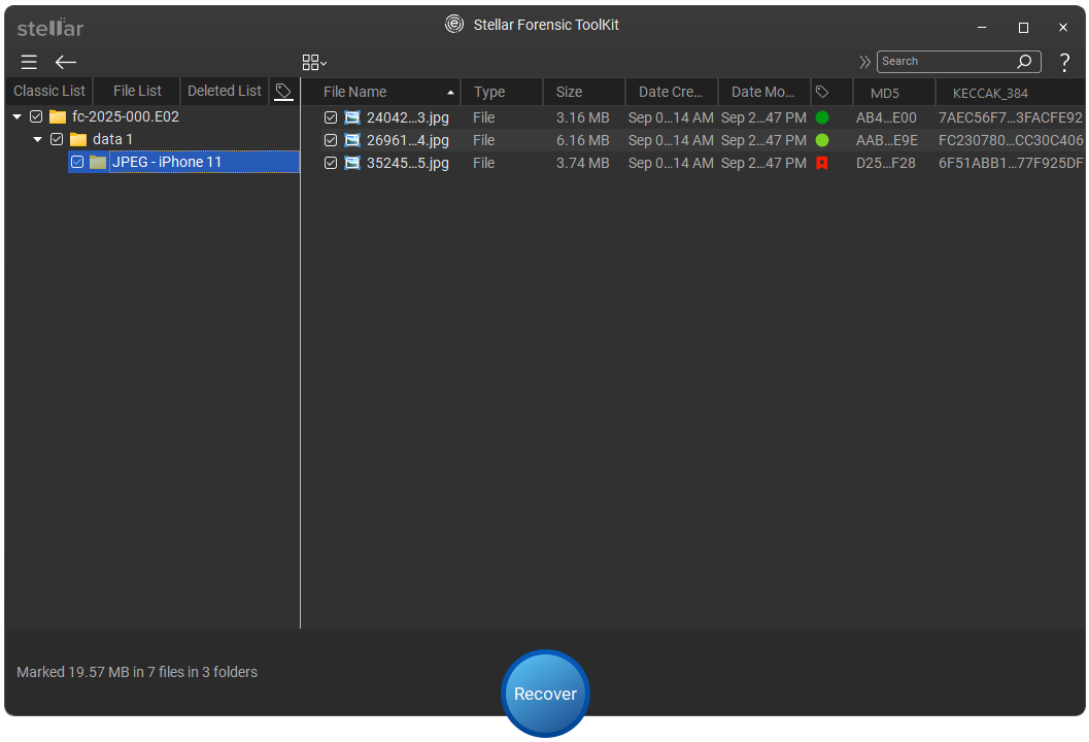


Note: *You can only tag the any file only during the scanning process.*

5. To view the tags files/items after scanning, naviagte to the **Tag** tab in the left pane of the scanning result window.



6. Select the desired catagory and click **OK** to view the tag list.



Note: *To know how to set the catagory for tagging, click here.*

4.12.1. Supported File Formats for Preview

Stellar Forensic Toolkit can preview the types of files listed on this page. If a file type isn't listed, you can still recover it using the software.

However, if the file type is listed and you're having trouble previewing the file, it might be because the file is severely corrupted and partially recovered, or it might be too big to be previewed (more than 500 MB). In that case, it is recommended to save the file and check using the file's default software.

File types that preview:

Photo/Raw File Formats:

JPEG, TIFF, TIF, PNG, BMP, GIF, NEF, CR2, CR3, CRW, ORF, SR2, K25, KDC, DCR, RAF, MRW, PEF, ARW, DNG, ERF, NRW, MOS, RAW, X3F, EIP, IIQ, SRW and BAY.

Video Formats:

WMV, AVI, MPEG, MPG, ASF, MOV, MP4, 3GP, 3G2, MTS, DIVX, FLV, M4V, VOB, MKV, WEBM, HDMOV, MXF, OGM, M1V, M2TS, M2T, DV, F4V, SVI, TOD, OGV, MPV, AVCHD, MP2, MPE, M2V, WM, AMV, MP4V, 3GP2, 3GPP, 3GPP2, QT, HDV, F4P, TS, PS, DVCPRO and DVCPROHD.

Audio Formats:

WMA, WAV, MP3, MIDI, MID, AAC, AIF, AIFF, AMR, AU, CAF, DSS, M4A, OGG, RA, RM, M4R, M4B, AIFC, F4A, M4P, F4B, OGA, OGX, SND, MPA, MPE, M3U, FLAC, ADT, ADTS and CDA.

Document Formats:

DOC, DOCX, DOT, DOTX, XLS, XLSX, PPT, PPTX, PPTM, POT, POTX, POTM, PPSX, PPS, ODP, PDF, XLA, XLAM, XLT, XLSM, XLSB, XLTX, XLTM, ODT, ODS, DOCM, DOTM and DOT.

Archive Formats:

Zip and RAR.

Text/Application Formats:

JSP, ASPX, PHP, MHT, HTML, MHTML, TXT, C, CPP, H, PLIST and Apple Mail EMLX/EML.

4.13. Save the Recovered Files

4.13. Save the Recovered Files

Stellar Forensic Toolkit can recover all the data on the selected volume. You can recover all the files and folders listed in the tree view and save them at a location of your choice.

Steps to Recover Data:

1. From the **tree view**, select the files and folders you want to recover. You can change the tree view to **Classic List, File List, and Deleted List** if you want to recover the files of a specific type only. Also, you can change the tree view to **Deleted List** if you want to recover your deleted data.

   Note: *See Preview the Scan Results for more information on view type.*

   To search for specific files:

   - Click on the **Search** button, it will expand to 

search bar.
   - Type the desired file name in the search text box and press **Enter**.
   - Click the **Search** to find more files with the same text as entered in the 

search text box.

   To Recover all the files:

   - Check the root node in the left pane and then click **Recover**.

   To Recover an individual folder:

   - Click the desired folder in the left pane. It will list all the files within the selected folder in the right pane.
   - Check the folder in the left pane or desired files of the folder in the right pane. Click **Recover**.

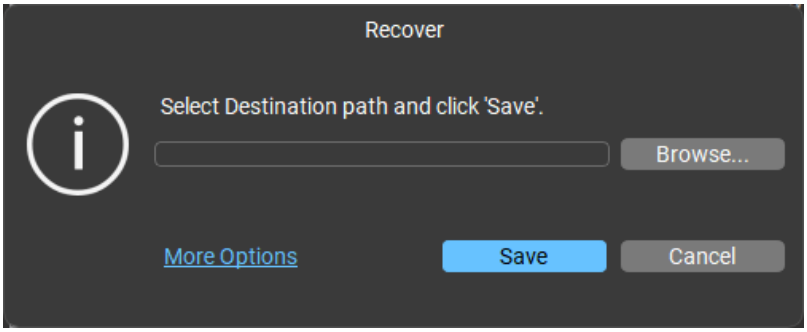
   To recover an individual file:

   - Right-click on the file in the right pane and select **Recover** option.

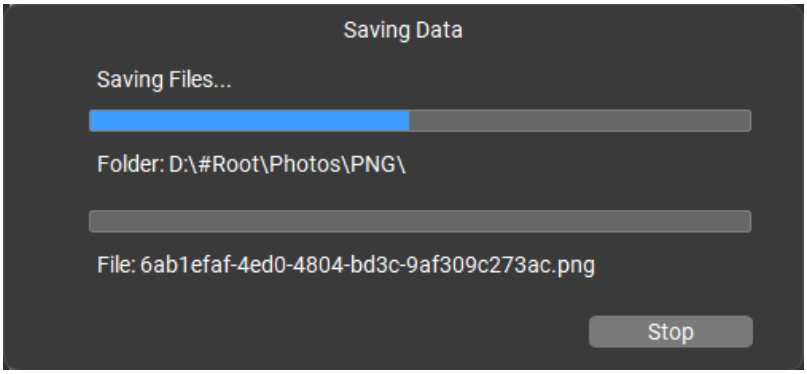
   To recover files of specific type:

   - Click on **File List** tab. Check the type of files you wish to recover.
   - Click **Recover**.

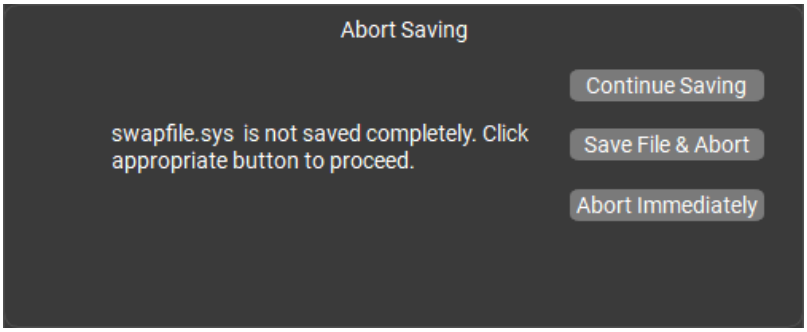
2. A **Recover** dialog box is displayed. Click **Browse** button to select desired destination to save the data.



3. Click **Save** to start the saving process. If the destination files have the same names, then you can overwrite, rename or skip.



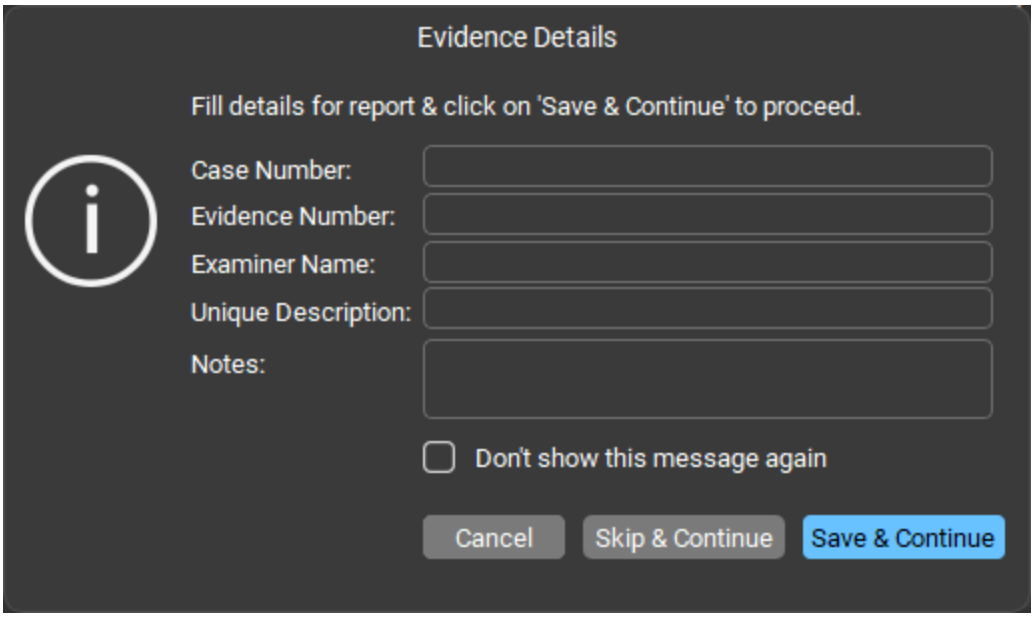
Note: *if you abort the saving process, click on the* ***Stop*** *button, the* ***Abort Saving*** *dialog box appears on the screen with the following options:*



- ***Continue Saving:*** *Select this option to continue with the saving process.*
- ***Save File & Abort:*** *Select this option to abort and save file.*
- ***Abort Immediately:*** *Select this option to abort immediately the saving process.*

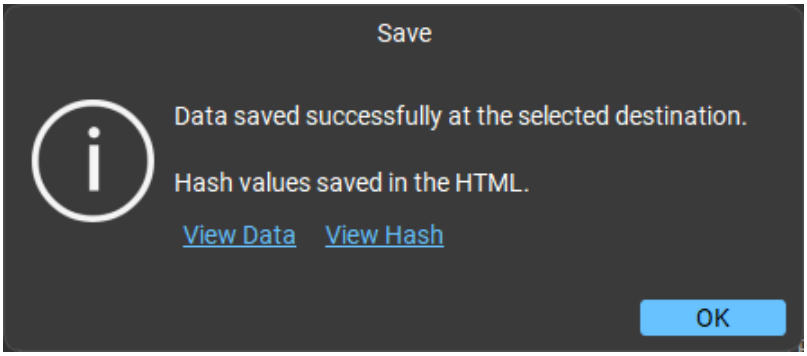
Note: *If you are saving the raw image formats, the* ***Evidence Details*** *dialog box appears, where you need to enter details such as* ***Case Number***, ***Evidence Number***, ***Examiner Name***, ***Unique Description***, *and* ***Notes***. *Click* ***Save & Continue***.

Important: *To view this dialog box while saving the raw image formats, you need to select the* ***Prompt for evidence details if unavailable before report save*** *checkbox in* ***Report Options*** ***of the Forensic Settings.***



Note: *If you do not want to view* ***Evidence Details*** *dialog box while saving, check the* ***Don't show this message again*** *checkbox.*

4. The selected files will be recovered and saved at the specified location. Navigate to the destination to view files.



Note: *To view the saved data, click the* ***View Data*** *link. To view the hash value, click the* ***View Hash*** *link.*

Note: *A forensic report is automatically generated and saved after the recovery process.*

4.13.1. More Options

Stellar Forensic Toolkit lets you configure the recovery options while saving the files. With **More Options**, you can

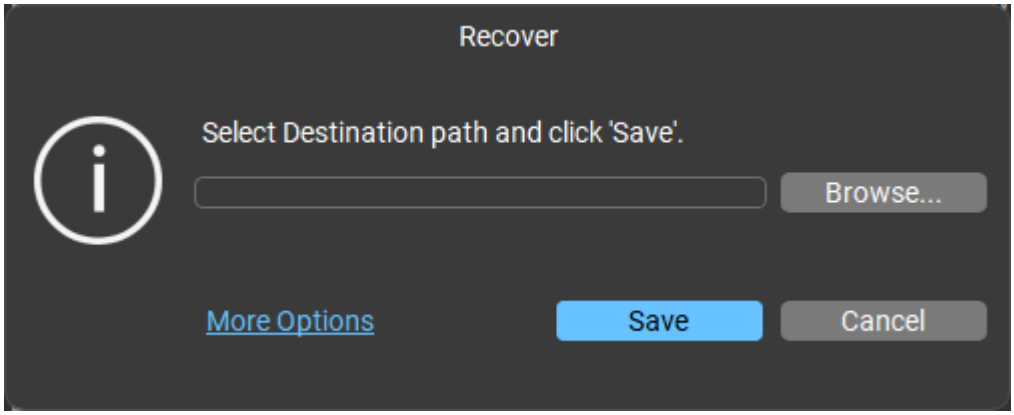
- Apply Compression
- Change Recovery Option
- Specify file filters

Apply Compression

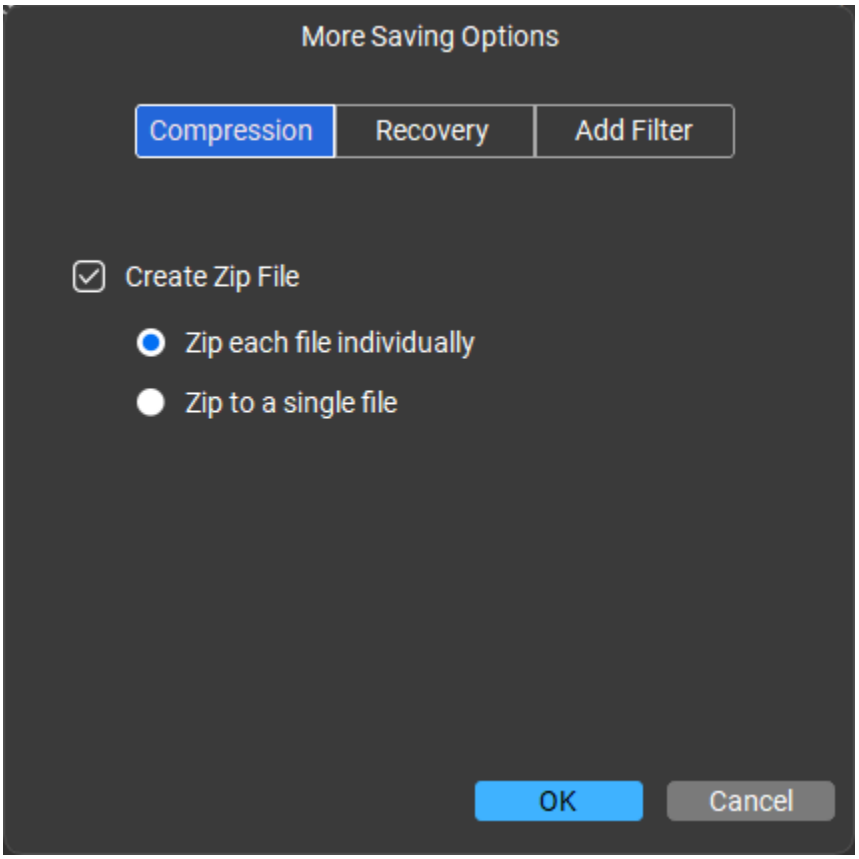
You can save recovered files in compressed zip folders. However, compression can be applied only if recovered files are being saved to a local disk or drive.

To apply compression:

1. In the **Recover** dialog box, click **More Options**.



2. The **More Saving Options** dialog box appears with the **Compression** option selected by default.



3. Select the **Create zip** file check box. Select:

- **Zip each file individually:** This option saves all selected files in their corresponding zip folder.
- **Zip to a single file**: This option saves all recovered files in a single zip folder.

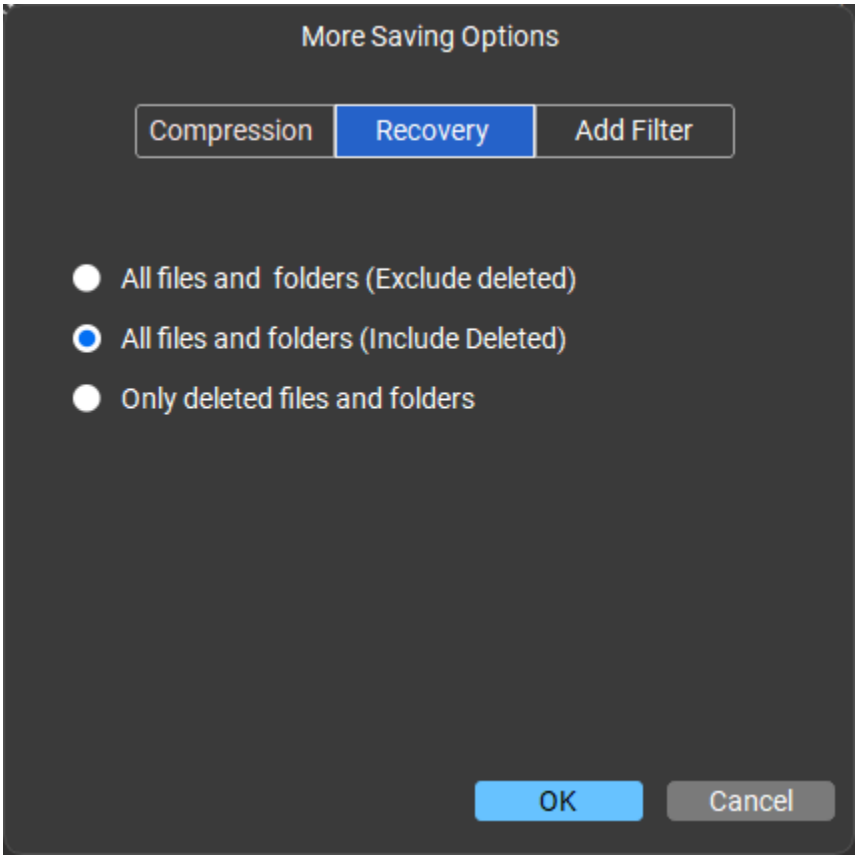
4. Click **OK**.

Change Recovery Option

This section is shown when all the files and folders are selected for recovery. You can choose to exclude or include the deleted files while recovery.

To change the recovery option:

1. From the **More Saving Options** dialog box, select **Recovery** option.



2. Select any one of the following options:

- **All files & folders (Exclude deleted):** Choose this option to exclude the deleted files while recovering the selected files and folders.
- **All files & folders (Include deleted):** Choose this option to include the deleted files and folders while recovering the selected files and folders.
- **Only deleted files & folders:** Choose this option to recover only deleted files and folders.

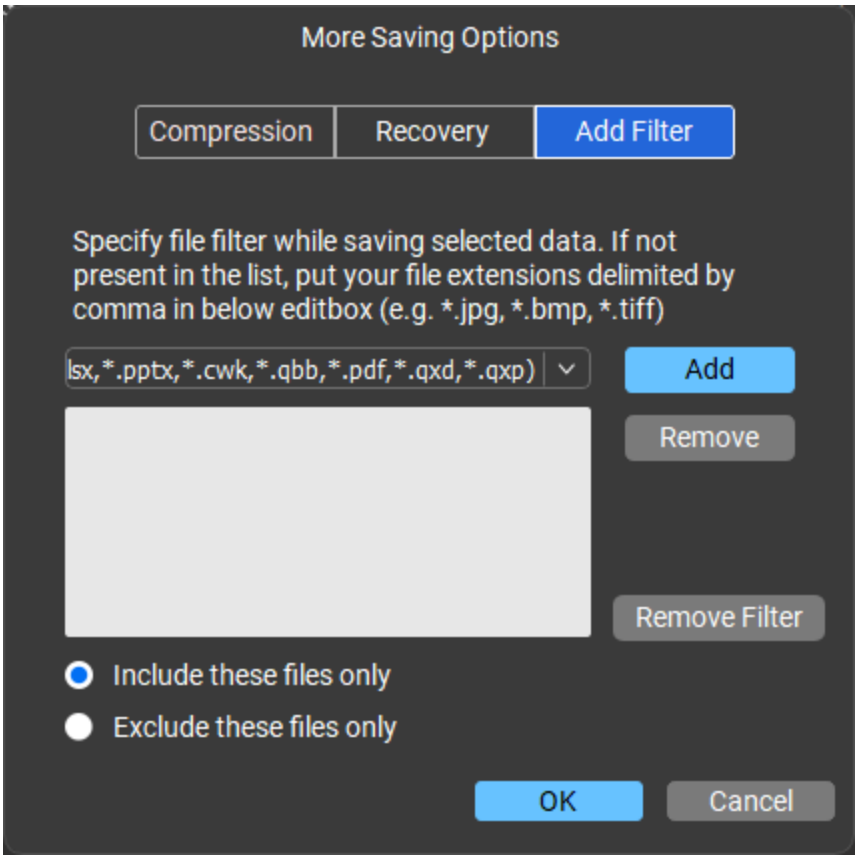
3. Click **OK**.

Specify Filters

You can add a filter according to your requirement.

To apply filter:

1. From the **More Saving Options**, dialog box select **Add Filter** option.



2. Select a group of file types from the drop down box and click **Add** button, to include it in the list.
3. To remove any extension from the list select the extension and click **Remove** button.
4. To remove the filter from the list select **Remove Filter** button.
5. Select **Include these files only** to include the listed file types during recovery or **Exclude these files only** to leave the listed file types during recovery.
6. Click **OK**.

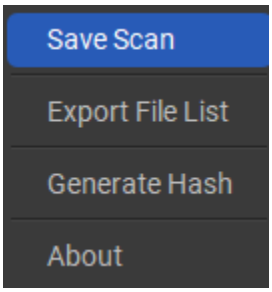
4.14. Save the Scan Information

You can save scan result of any scanning process as DAT file. You can save scan result of a complete or incomplete recovery process.

Saving scan information saves your time. You can resume recovery by selecting the DAT file without scanning the drive again.

To save scan information:

1. In the **'Scan Results'** window, click the **More Options** and select **Save Scan**.



Tip: *The software prompts you to save the scan information when you click on* ***Back*** *button or you try to close the software. You can also save the scan information using the prompt.*

2. In '**Save scan information**' dialog box, Select the location where the file should be saved. Type the name of the file in the **File name** text box and click **Save**.

For information about resuming the recovery session, see resume scan information.

Note: *Scan Information file will be saved with DAT extension.*

Note: *If you stopped a scanning process, you can save scan information up to that point. However, you should perform complete scan, and then save scan result.*

Tip: *It is recommended that you should save 'scan information file' and 'hard disk image' at different locations with a proper name such that you can easily retrieve the required DAT file.*

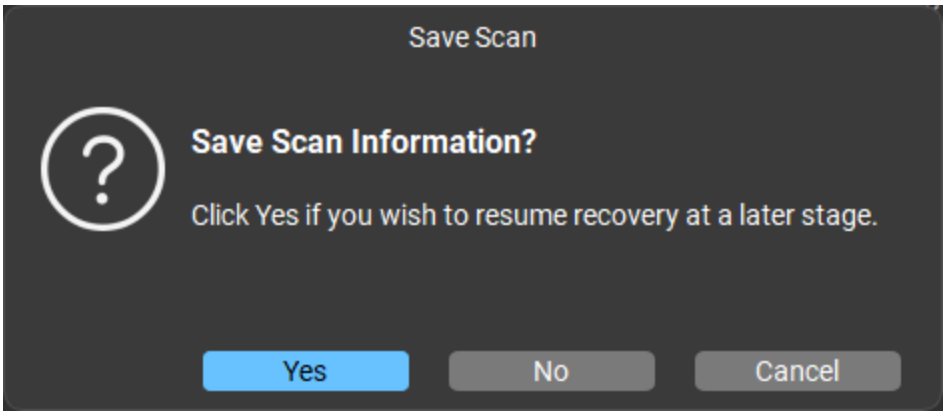
Save Scan Information:

Scan Information file, saved as a DAT file, contains scan details. You save it during any complete or incomplete recovery process and use it to resume recovery later. You can recover more files later from the same drive using the saved DAT file.

A scan information file saves time by not scanning the same files again. It shows all files and folders from the scan. If no files are saved, you can use the DAT file to resume recovery later.

Steps to Save Scan Information:

1. In the **Scan Results** window. Click **Back** button or close the application.
2. The software prompts you to save the scan information. Click **Yes**.

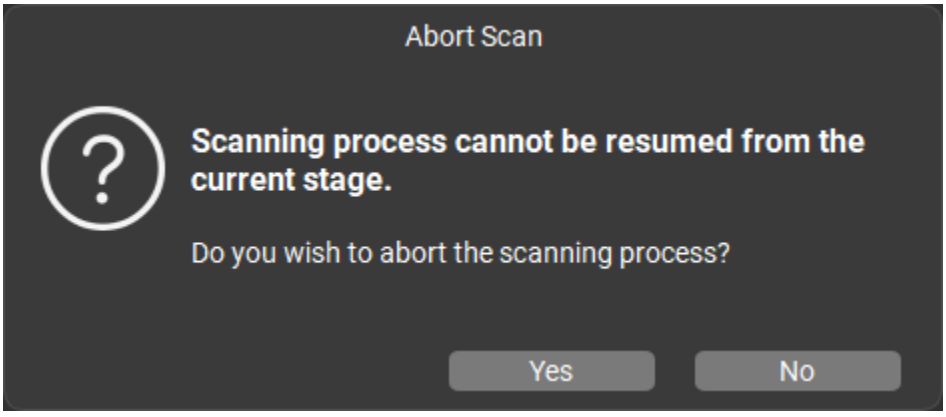


3. In '**Save scan information**' dialog box, specify the location where you want to save the file. Type the name of the file in the **Save As** text box. Click **Save**.
4. Scan Information file will be saved.

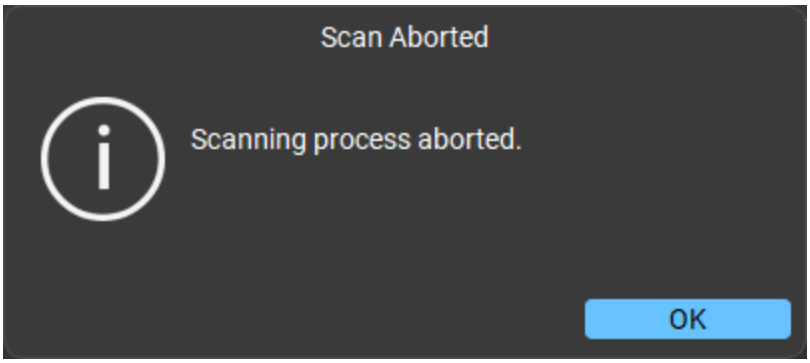
Steps to Save Your File When the Scan Stops During the Process

If you stop a scanning process, you can save the scan information up to that point. However, you should perform a complete scan and then save the scan result.

1. While scanning, click the **Stop** button in the **Scan Results** window.
2. **Abort Scan** dialog box appears with the message, as shown below:

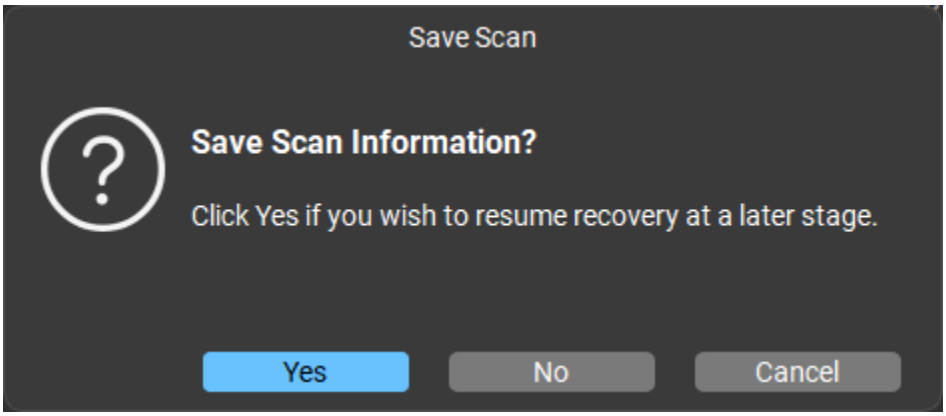


3. Click **Yes** to abort the scanning process. **Scan Aborted** dialog box appears. Click **OK**.



Tip: *It is recommended that you should save 'scan information file' and 'hard disk image' at different locations with a proper name so that you can easily retrieve the required file.*

4. Click **Back** button or close the software. **Save Scan** dialog box appears.
5. Click **Yes** to continue the saving process.

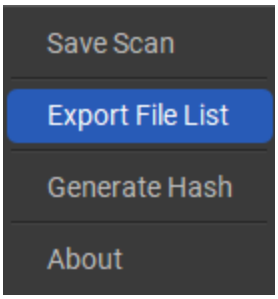


6. **Save scan information** dialog box appears, specify the location where you want to save the file. Type the name of the file in the **Save As** text box. Click **Save**.
7. Scan Information file will be saved.
8. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

Steps to export file list:

You can also export and save the file lists at your preferred location in html format using the **Export File List** button provided in the **More options** option.

1. In the **'Scan Results'** window, click the **More Options** and select **Export File List.**

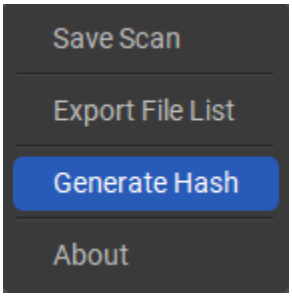


2. In **Save File List** dialog box, Select the location where the file should be saved. Type the name of the file in the **File name** text box and click **Save**.

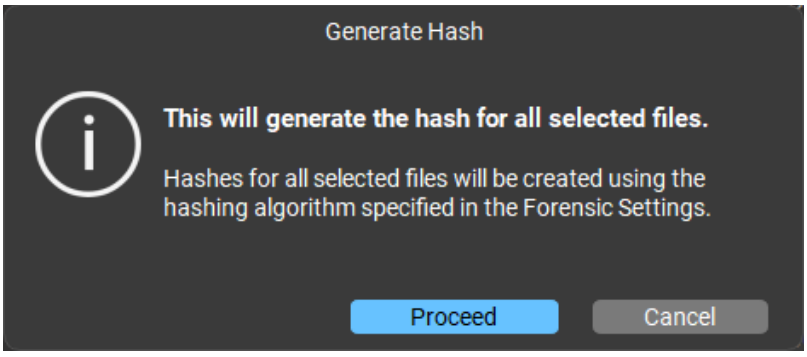
Generate Hash

1. Select the file which you want to generate the hash.

2. In the **'Scan Results'** window, click the **More Options** and select **Save Scan**.



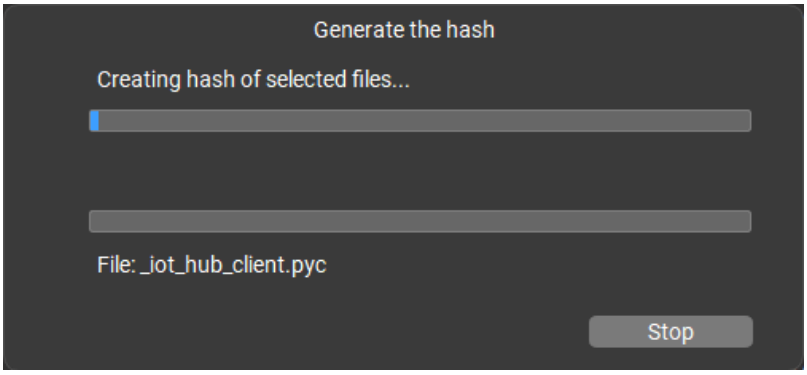
3. **Generate Hash** dialog box appears on the screen as shown below:



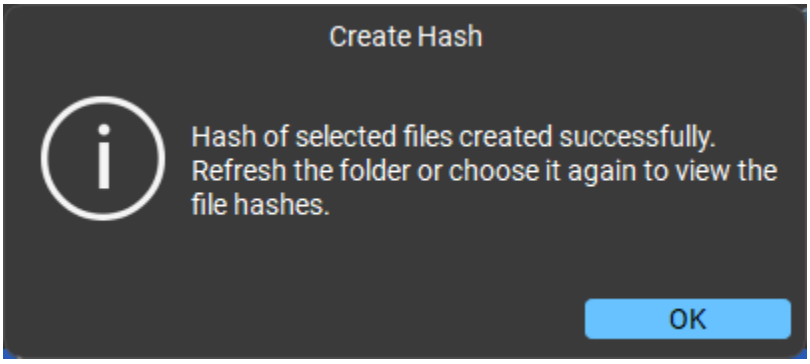
Note: *To generate the hash alogorithm, select the required algorithm from* ***Forensic settings****.*

4. Click **Proceed**.

5. Hash Generating process starts as shown below:



6. **Create Hash** dialog box appears with the message **"Hash of selected files created successfully. Refresh the folder or choose it again to view the file hashes."**



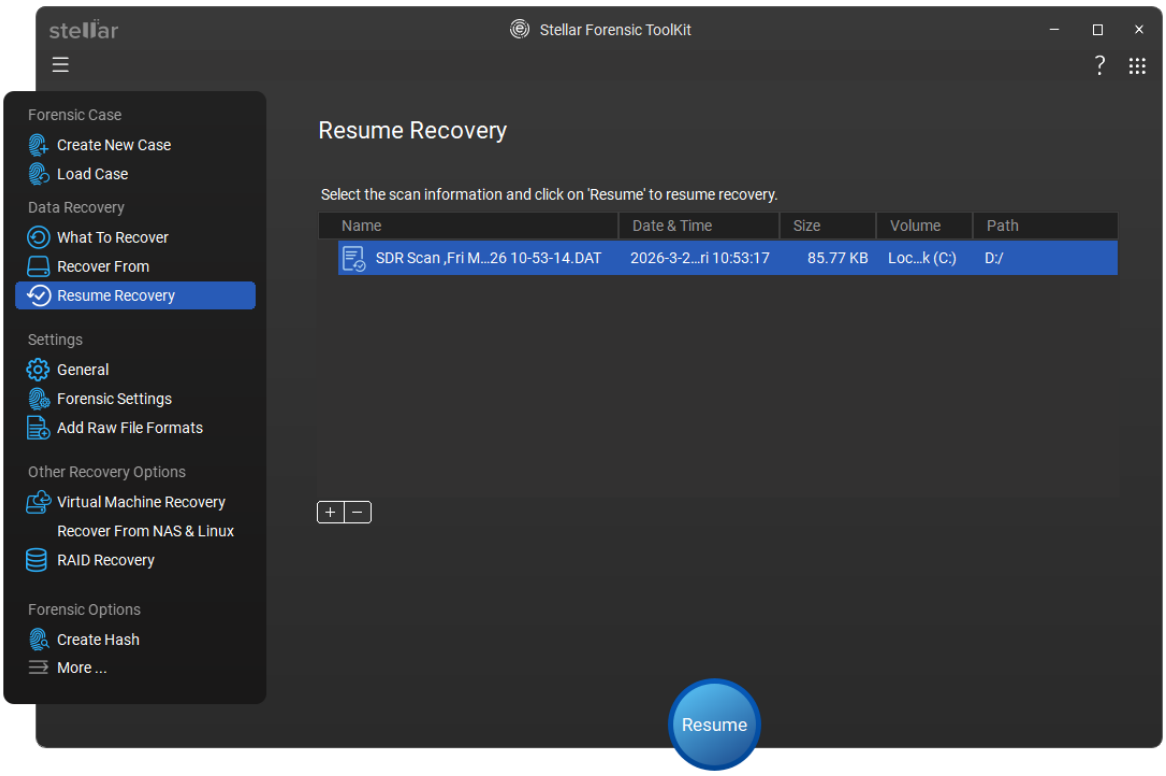
7. Click **OK**.

4.15. Resume Scan Information

Resume Recovery allows you to restart a recovery process using a saved DAT file. This eliminates the need to rescan, as all previously scanned files and folders will be displayed, enabling you to pick up the recovery from where it was left off.

To Use Resume Recovery Scan Information File:

1. Run **Stellar Forensic Toolkit.**
2. From the side panel, under **Data Recovery**, select **Resume Recovery** option.
3. A **Resume Recovery** window appears with a list of saved scan information file existing in the system.
4. Select your desired saved scan file you wish to resume by clicking on it.

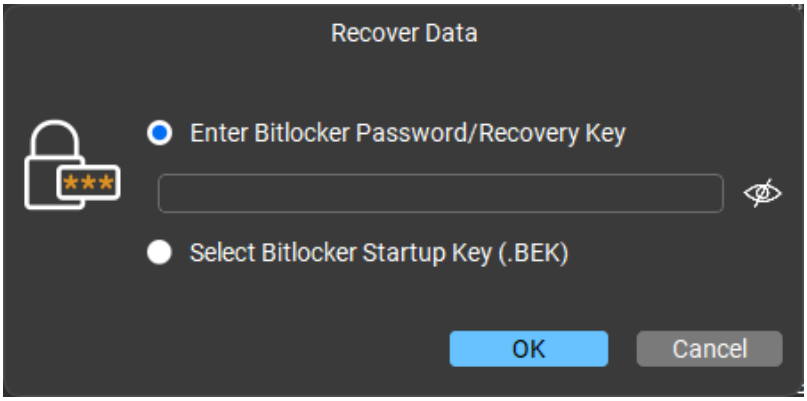


Note: *In case the file you desire is not in the list, click* + ***Add*** *button and select the desired file*

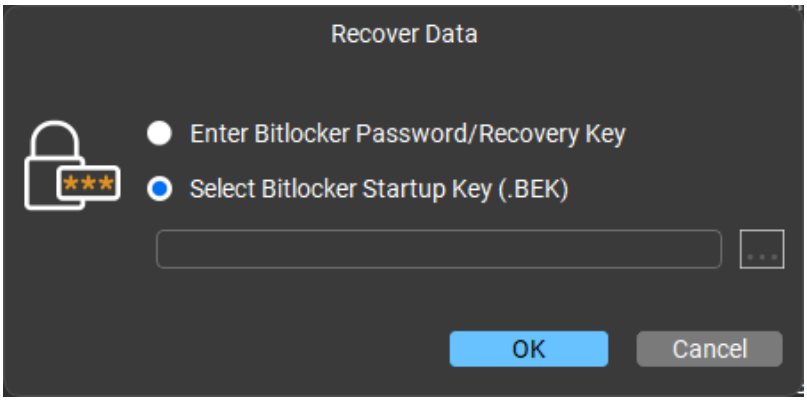
5. Your added file is displayed in the resume recovery window. Click − **Remove** button if you want to remove the listed saved scan file.
6. Click **Resume** button.

Note: *If you are scanning a drive that is encrypted using* ***BitLocker****, you will be prompted to either enter the* ***Bitlocker password/Recovery*** *Key or Select a* ***Bitlocker Startup Key (.BEK file)****. Use any one of the following steps, to initiate the scan process:*

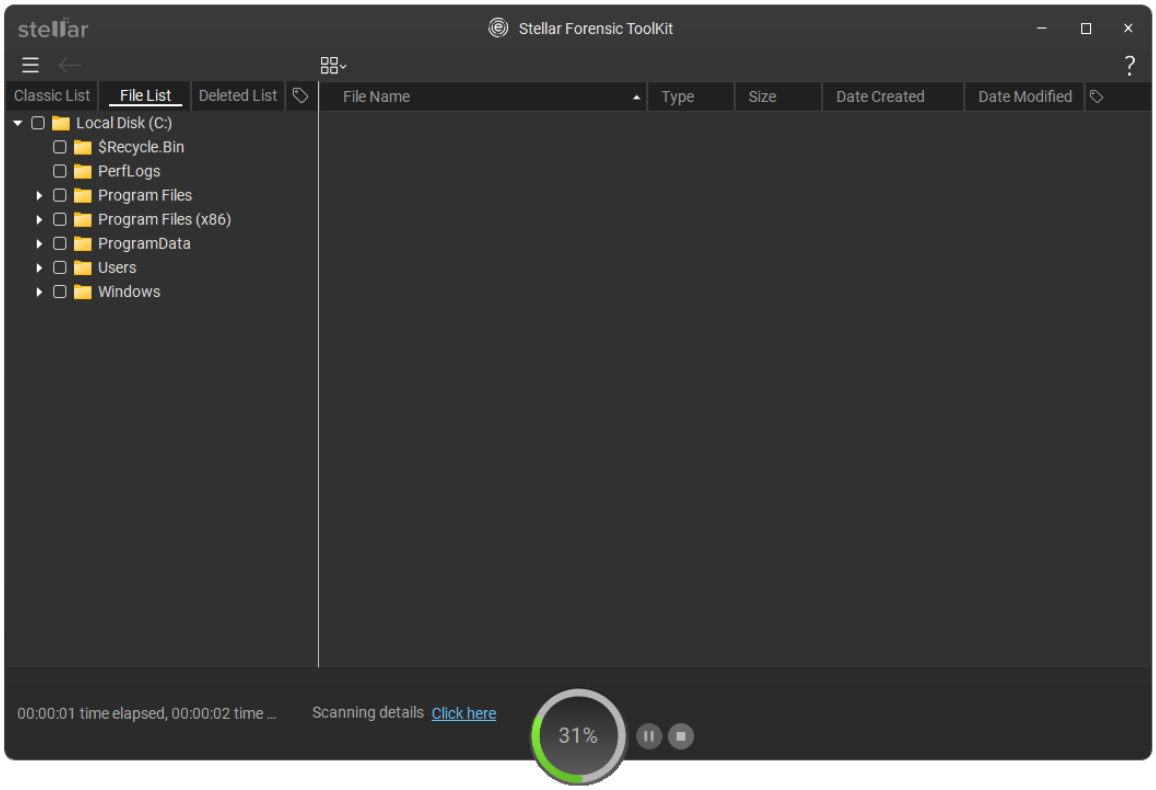
- *Enter the* ***Bitlocker password/Recovery Key*** *in the text box given and click* ***OK****.*



- *Alternatively, choose Select **Bitlocker Startup Key (.BEK)** radio button. Click to*  ***browse** and select the **.BEK** file and click OK.*



7. A screen appears that shows the scanning process.



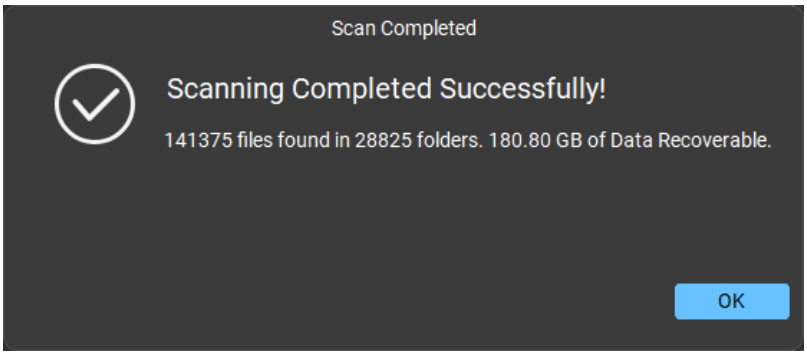
Note: *You can select only one file at a time to start the process of scanning.*

Note: *To view the scanning details, click on* ***Click here*** *link at the bottom of the screen.*

Note: *Click on* ***Stop*** *or* ***Pause/ Resume*** *button to stop or resume the scanning process.*

Note: *You can also perform a deep scan after a quick scan by clicking the* ***'Click here'*** *link next to the deep scan at the bottom of the screen.*

8. Once the scanning process completes, details of the **files** and **folders** found would be displayed in a dialog box as shown below:



9. For information on how to preview and recover the scanned data, see Preview Scan Results and Save the Recovered Files.

4.16. Configure Settings

4.16. Configure Settings

In **Stellar Forensic Toolkit**, you can configure various settings, such as **General Settings**, **Forensic Settings**, and **Add Raw File Formats**. For more details, navigate to the links below:

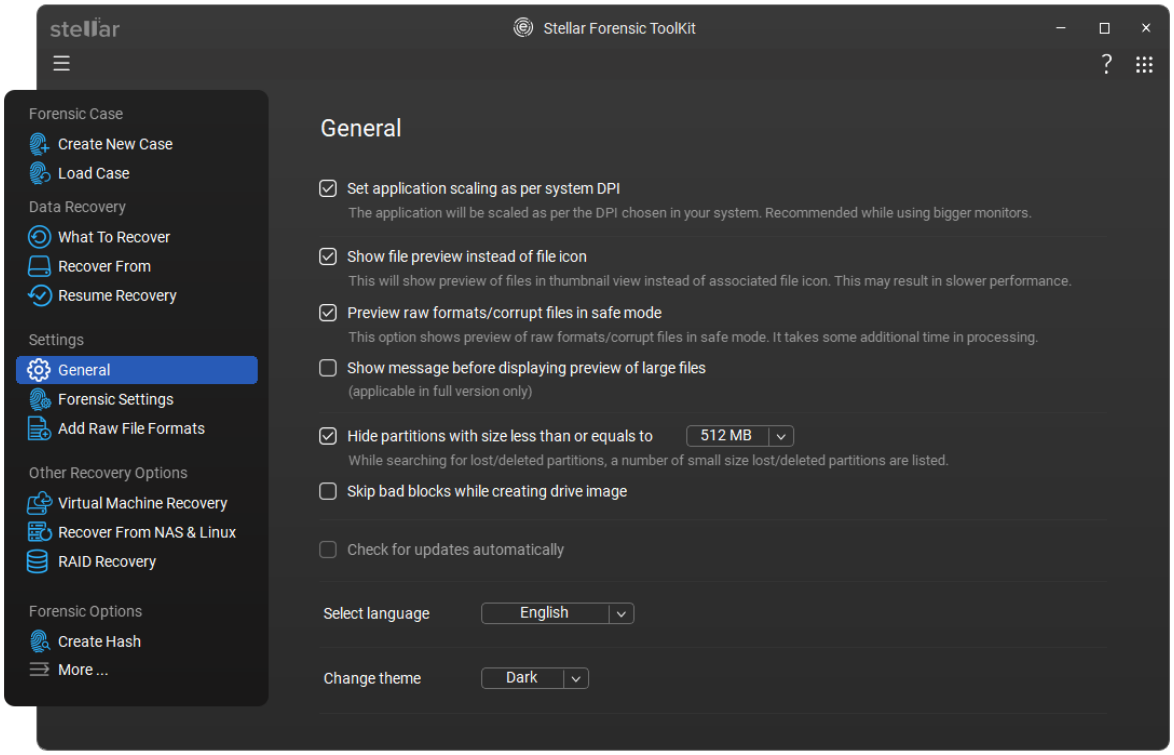
4.16.1. Configure General Settings

4.16.1. Configure General Settings

General Settings can be configured to run **Stellar Forensic Toolkit** according to personal requirement. This option make this software exceptional and easy to operate.

To Configure General Settings:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **General**  option.
3. **General** window appears. Using this you can configure following settings:



- To set the application scaling according to the system DPI, select the **Set application scaling as per system DPI** checkbox.
- Select the **Show file preview instead of file icon** check box to preview the thumbnail view instead of the associated file icon.
- To preview raw formats/corrupt files in safe mode select the **preview raw formats/corrupt files in safe mode** check box.
- To display a message before showing the preview of a large file, check the **Show message before displaying preview of large file** checkbox. This option is only available in the full version.
- Select the **Hide partitions with size less than or equal to** checkbox and choose a size from the drop-down menu to filter out small lost or deleted partitions during the search.
- Select the checkbox **Skip bad blocks while creating drive image** if you wish the software to skip bad blocks while creating drive image.
- Select the checkbox **'Check for updates automatically'** to get notified about new updates. However, this option does not work in the offline variant.

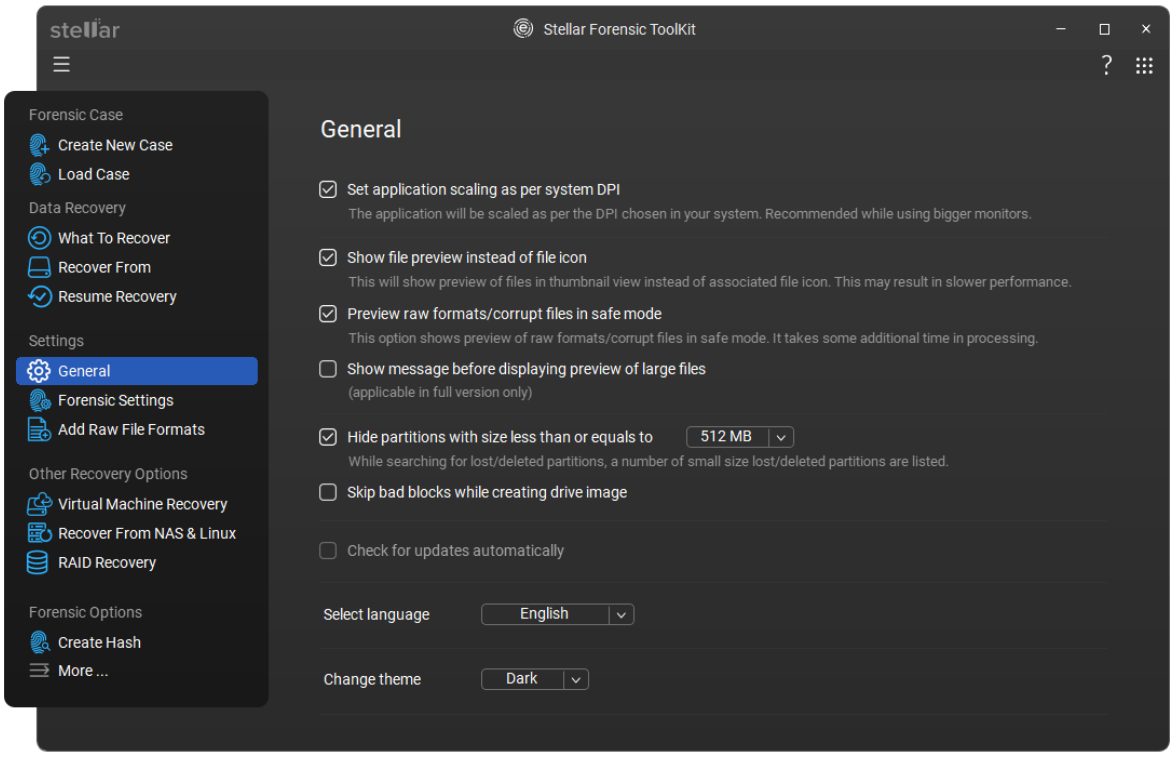
- To change the software language, select your preferred language. In the offline variant, the default language is **English**.
- To change the product theme, select your preferred **theme (Vibrant, Dark, Light)** from the **Change product theme** dropdown.

4.16.1.1. Preview Settings

Preview option allows you to apply settings for preview window of the application.

To apply preview settings:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **General** option.
3. **General** window appears. Select the **Preview raw formats/corrupt files in safe mode** checkbox to preview files during the scanning process based on your preference.



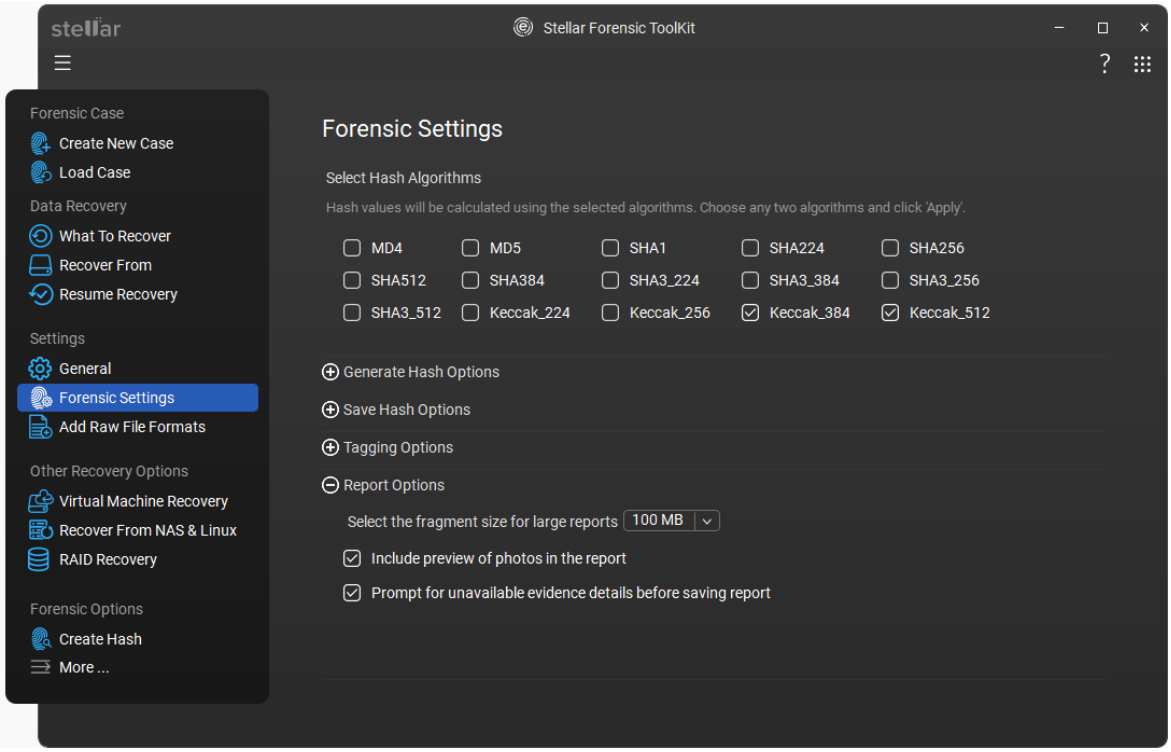
Note: *This option enables the preview of raw format or corrupt files in safe mode, which may take additional time for processing.*

4.16.2. Configure Forensic Settings

Forensic Settings can be configured to run **Stellar Forensic Toolkit** according to your requirement. This option make this software exceptional and easy to operate.

Steps to Configure Forensic Settings

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **Forensic Settings**  option.
3. **Forensic Settings** window appears, as shown below:



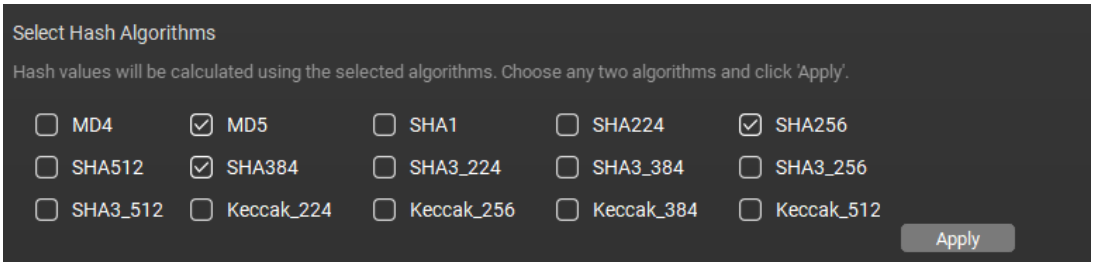
4. In the **Forensic Settings** window, configure the following settings.

Forensic Settings window divided into five sections, which are given below:

- Select Hash Algorithms
- Generate hash Options
- Save Hash Options
- Tagging Options
- Report options

Select Hash Algorithms:

Use this option to select the hash algoritms. Hash value will be calculated using the selected algoritms. To select a hash algorithms, check the box next to the desired algorithm and click **Apply**.



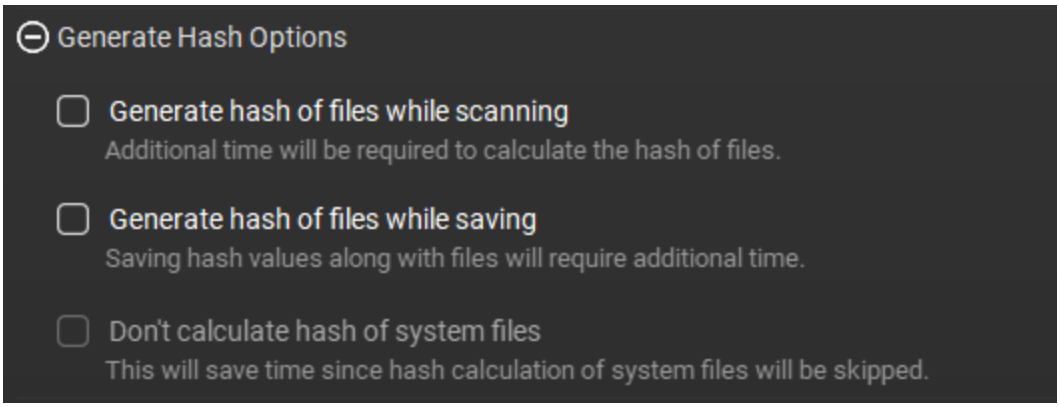
Note: *You can select up to two algorithms at a time.*

Generate Hash Options:

Use this option to generate hash options. To generate hash options, expand the **Generate Hash Options** and then check the box next to the desired hash options.

You can generate three types of hash options, which are given below:

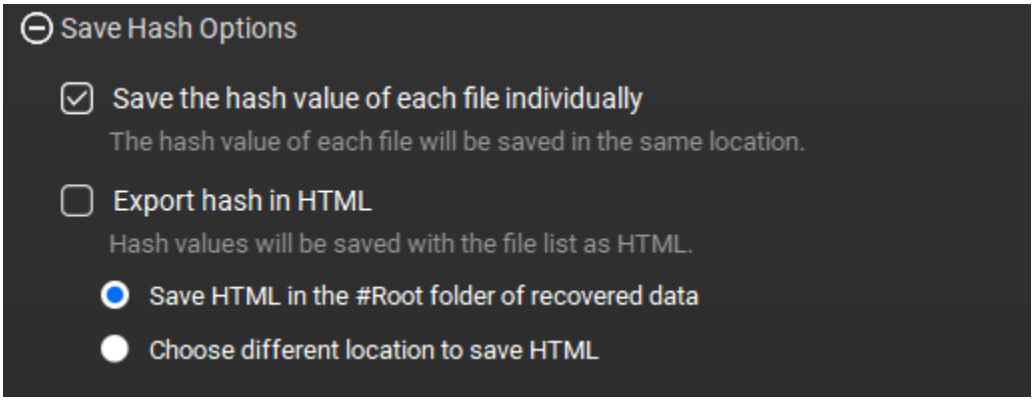
- **Generate hash of files while scanning:** Select this option if you want to generate hash values during the scanning process. Make sure that this may take additional time as the hash of each file will be calculated.
- **Generate hash of files while saving:** Select this option if you want to generate hash values while saving the files. Saving hash values along with files may require extra time.
- **Don't calculate hash of system files:** Select this option if you want to skip hash calculation for system files. This will save time as the hashing process for system files will be excluded.



Note: *The* ***Don't calculate hash of system files*** *option works with both* ***Generate hash of files while scanning*** *and* ***Generate hash of files while saving****. However, if you select* ***Generate Hash of Files while Scanning****, the option to* ***Generate hash of file while scanning*** *will be disabled, and vice versa.*

Save Hash Options:

Use this option to save hash options. To save hash options, expand the **Save Hash Options** and then check the box next to the desired save hash options.



You can save hash values in two ways, which are given below:

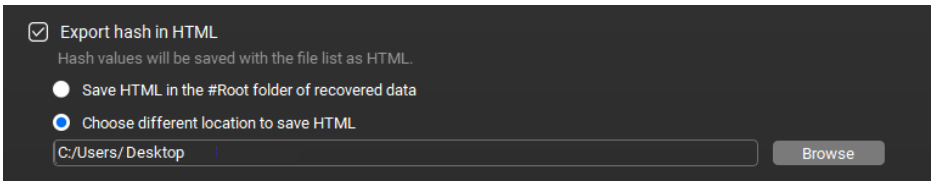
- **Save the hash value of each file individually:** Select this option to save the hash value of each file separately. The hash values will be stored in the same location as the files.
- **Export Hash in HTML:** Select this option to export hash values in an HTML file. The HTML file will contain the list of files along with their corresponding hash values.

You can save the HTML file in the following locations, which are given below:

a. **Save HTML in the #Root folder of recovered data:** Select this radio button to save the HTML file containing hash values directly in the root folder where the recovered data is stored.

b. **Choose different location to save HTML:** Select this radio button if you want to save the HTML file at a custom location of your choice instead of the root folder.

To choose the different file location, select the **Choose different location to save HTML** radio button then click on **Browse** button to save the HTML in different location.



.

Tagging Options

In **Stellar Forensic Toolkit,** the tagging option helps you to make the investigation process more organized and efficient. Basically, tagging is like adding labels to evidence**,** making large volumes of forensic data easier to manage, analyze, and report.

You can use the **tagging option** by choosing the specific color for each category in various scenarios, few examples are given below:

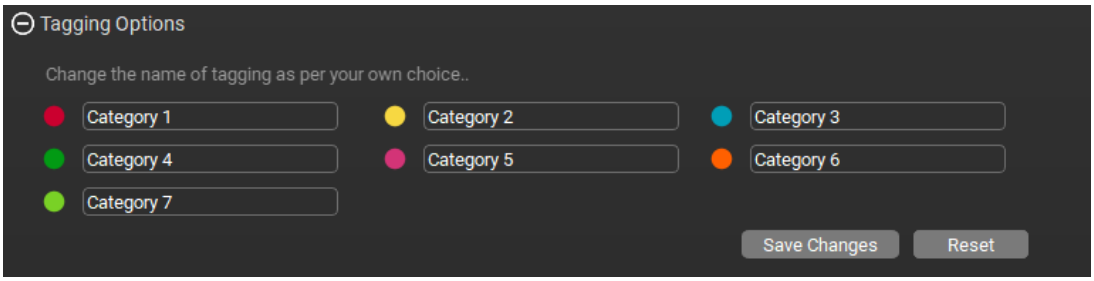
- Marking important evidence for quick reference.
- Categorizing data into groups like suspicious, irrelevant, confidential, deleted, etc.
- Filtering or searching by tags to instantly retrieve related evidence.
- Supporting team investigations by allowing multiple investigators to see which items are already reviewed, flagged, or require further attention.

Example color usage:

- **Red:** Suspicious or critical evidence
- **Green:** Safe or verified data
- **Yellow**: Needs review or further analysis
- **Blue:** Informational or reference-only data

You can change the name of tag as per your choice. To change the name of the tag, follow the below steps:

i. Enter the name of the category in the text box corresponding to the specific color.



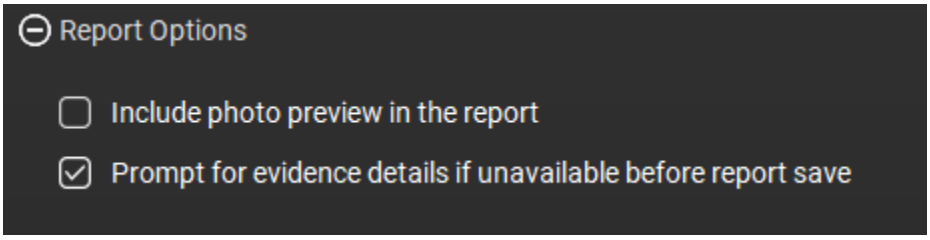
ii. Click on **Save Changes**.

Note: *If you want to reset the category, click on the* ***Reset*** *button.*

Report Options

This section helps you to configure the report settings, which are given below:

- **Include photo preview in the report:** Select this option to include photo in the report.
- **Prompt for evidence details if unavailable before report save:** Select this checkbox to prompt the details before saving the report. This option can be used with the raw image formats, where the option to enter evidence details is not available.



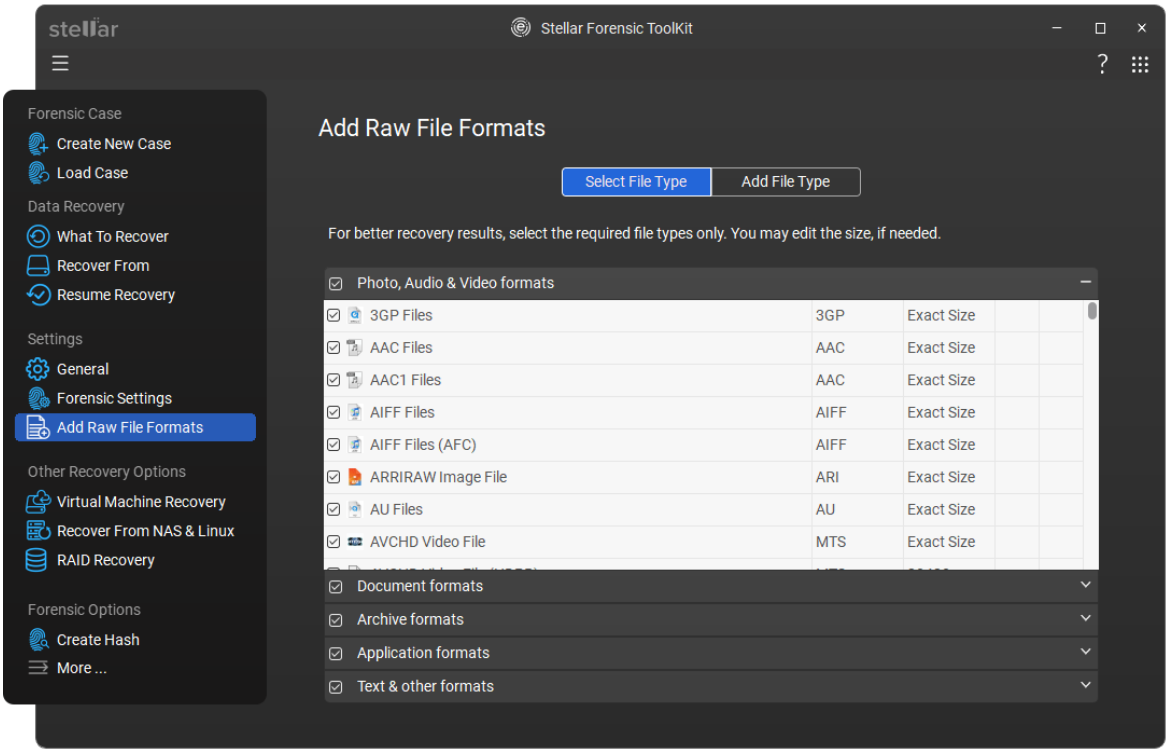
4.16.3. Select Raw File Formats

4.16.3. Select Raw File Formats

File types give information about the type of file such as video, audio and its extension. You can select file types while performing signature search such that, scanning process should search only for the specified file types. Various file types are listed in the file list option of **Stellar Forensic Toolkit**. You can select the required file types for their recovery.

To select file type:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **Add Raw File Formats** option.
3. A list of all the supported file formats is shown, as given below:



4. A list of all supported file formats is shown. Select the file types you want to recover using the check box in front of the file type.

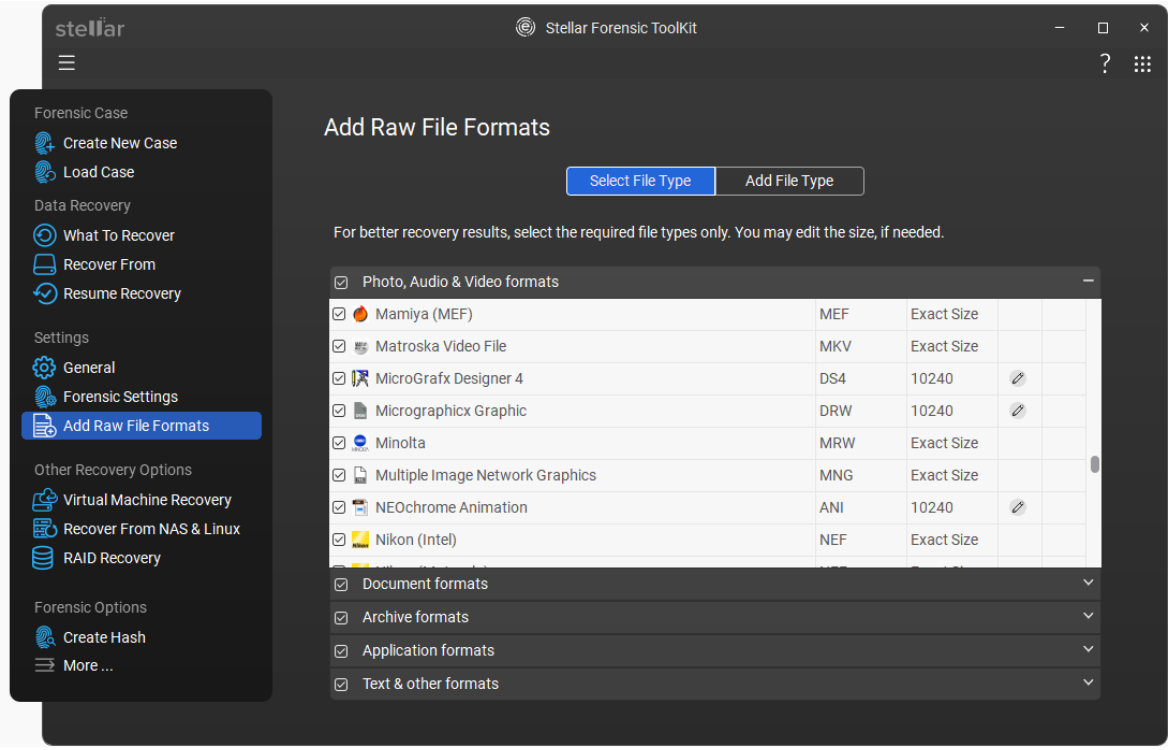
Tip: *It is recommended that you select* ***All Data*** *in* ***Select What To Recover*** *screen (Main User Interface) while selecting file formats in the* ***File List****. This is helpful to avoid any file type conflicts. For example, a conflict will happen if you have not selected* ***Multimedia Files*** *from* ***Select What To Recover*** *screen but have selected the multimedia file formats from* ***File List****. In this case, even though the files are selected in* ***File List****, these files will not be included in recovery as* ***Multimedia Files*** *are disabled from the Main User Interface.*

4.16.3.1. Edit File Formats

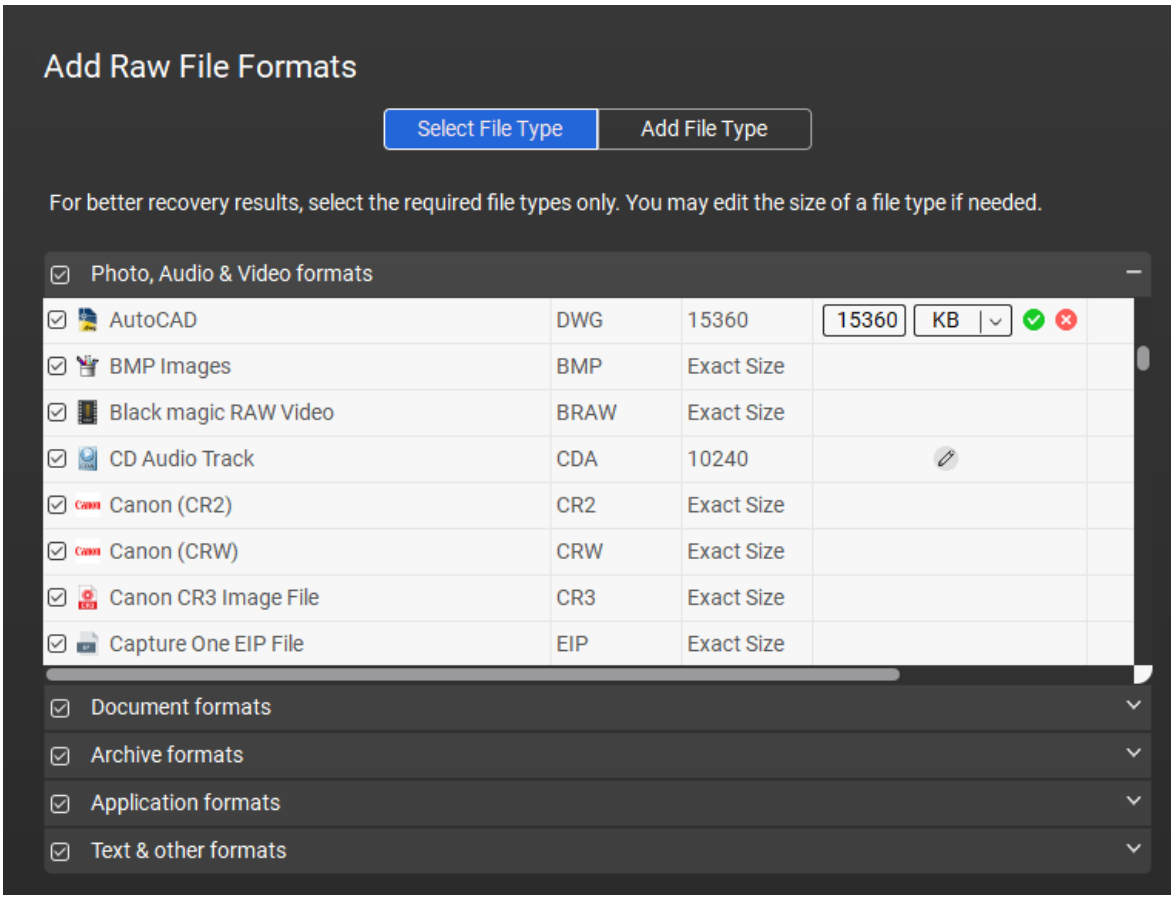
You can also edit an existing file type or newly added file type. You can change every setting of the file type.

To change size of supported file types/remove added file types:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **Add Raw File Formats** option.
3. Under **Select File Type** tab, select the desired file type from the list.



4. Click the Edit icon to edit the file size.



5. Enter the desired new size for the file, then choose the file size unit (KB or MB).

6. Click  to update the file size.

Note: *To cancel editing the file size, click*  .

4.16.4. Add File Formats

Stellar Forensic Toolkit allows you to add additional file types apart from those already mentioned in **File Lists**. Using **Add File Type** option, you can add a new file type to facilitate the recovery process.

Add File Type

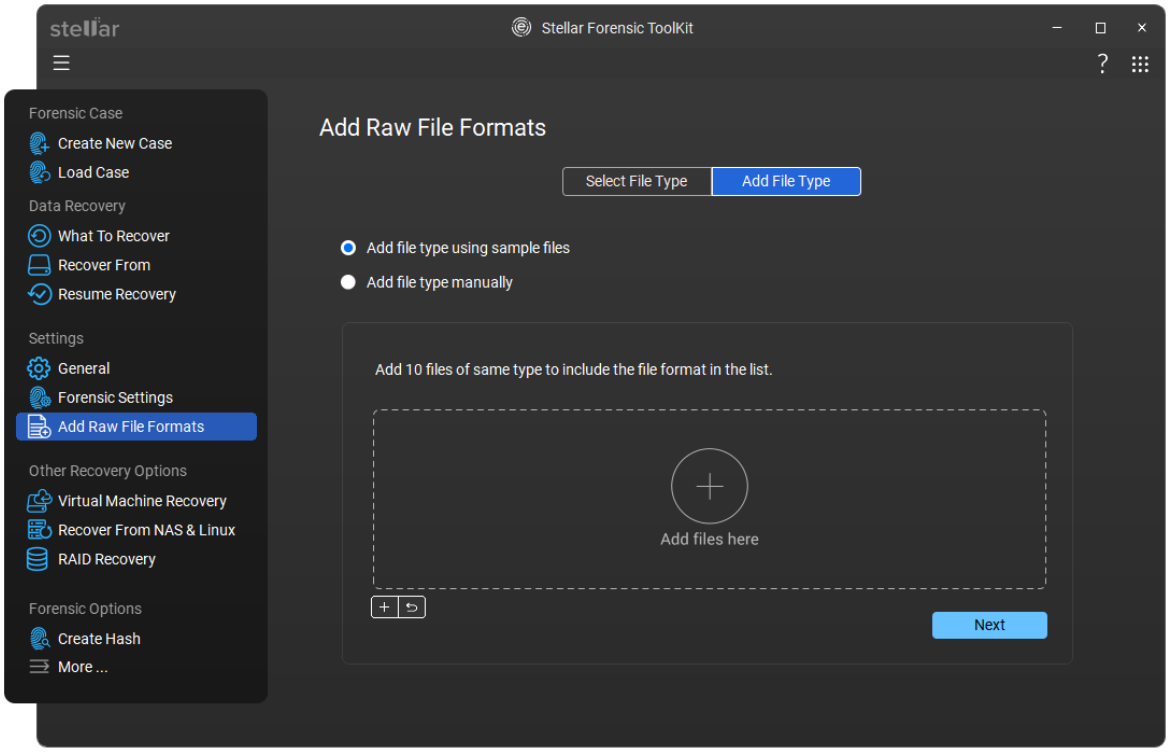
You can add new file types to the predefined list of supported file types in **Stellar Forensic Toolkit** using **Add File Type** functionality in **Add Raw File Formats** screen.

You can add file type either

- **Automatically**
- **Manually**

To add File Type automatically:

1. Run **Stellar Forensic Toolkit**.
2. From the side panel, under **Settings**, select **Add Raw File Formats** option.



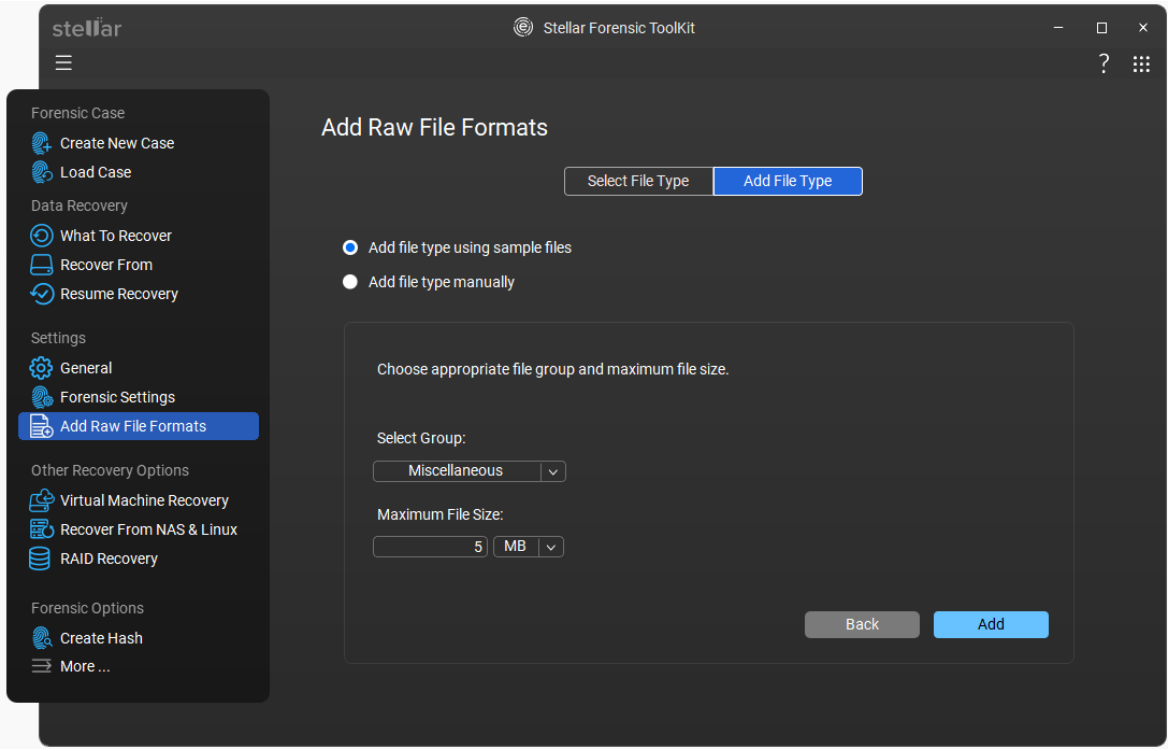
3. Click **Add File Type** button from **Add Raw File Formats** window.
4. Select the radio-button **Add file type using sample files**.
5. Click on **Add files here** box to browse to the location of file type you want to add.

   Note: *Alternatively, you can click* **+** ***Add*** *button to browse to the location of file type you want to add.*

   Note: *Click* **↩** ***Reset*** *button if you wish to remove all the added files at once.*

   Note: *You need to add at least* ***10 or more samples / files*** *of the same type to include it in the list of supported file types.*

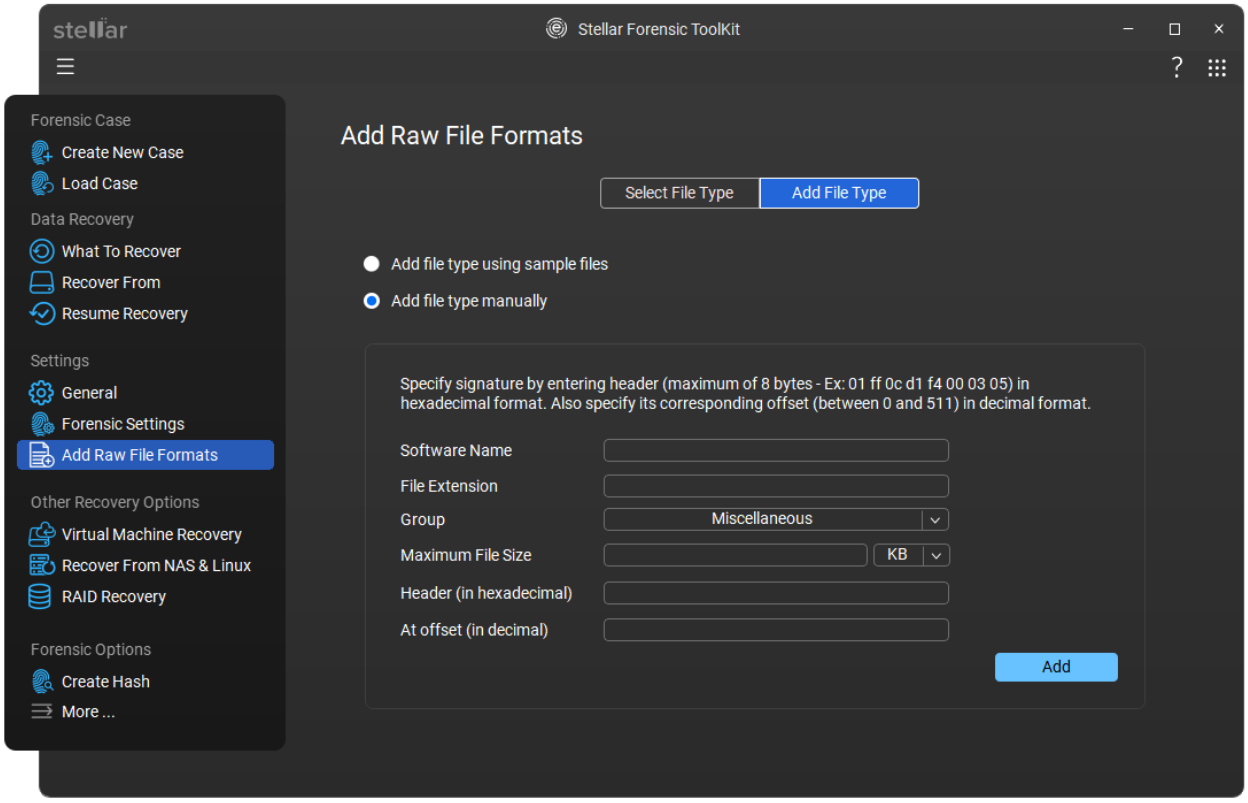
6. The names of added files with the same format will be listed in the box. Click **Next.**
7. Choose the appropriate file group from the **Select Group** drop down.
8. Specify the **maximum file size** in the text box, then select the unit (KB or MB).



9. Click the **Add** button.

To add file type manually:

1. Run **Stellar Forensic Toolkit.**
2. From the side panel, under **Settings**, select **Add Raw File Formats** option.



3. Click **Add File Type** tab.
4. Select the radio-button **Add file type manually**.

- Specify **Software Name**.
- Specify **File Extension**.
- Select **Group** from the drop down list.
- Specify **Max File** Size in KB and MB.
- Specify **Header** in hexadecimal.
- Specify At **Offset** in decimal.

5. Click **Add** button.

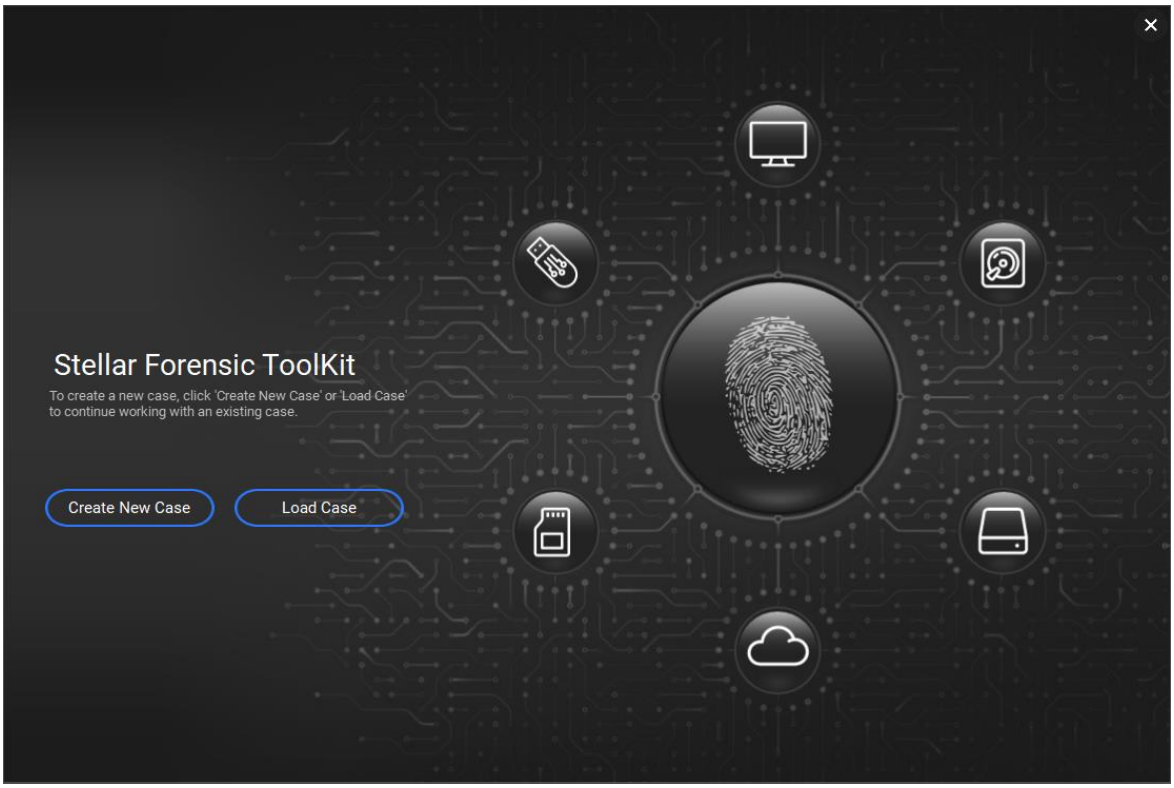
4.17. Create Hash

Stellar Forensic Toolkit gives you option to create the hash of the acquired evidence. This ensures data integrity by generating a unique digital fingerprint for the evidence file. The hash value can later be used to verify that the evidence has not been altered or tampered with.

Steps to create the Hash

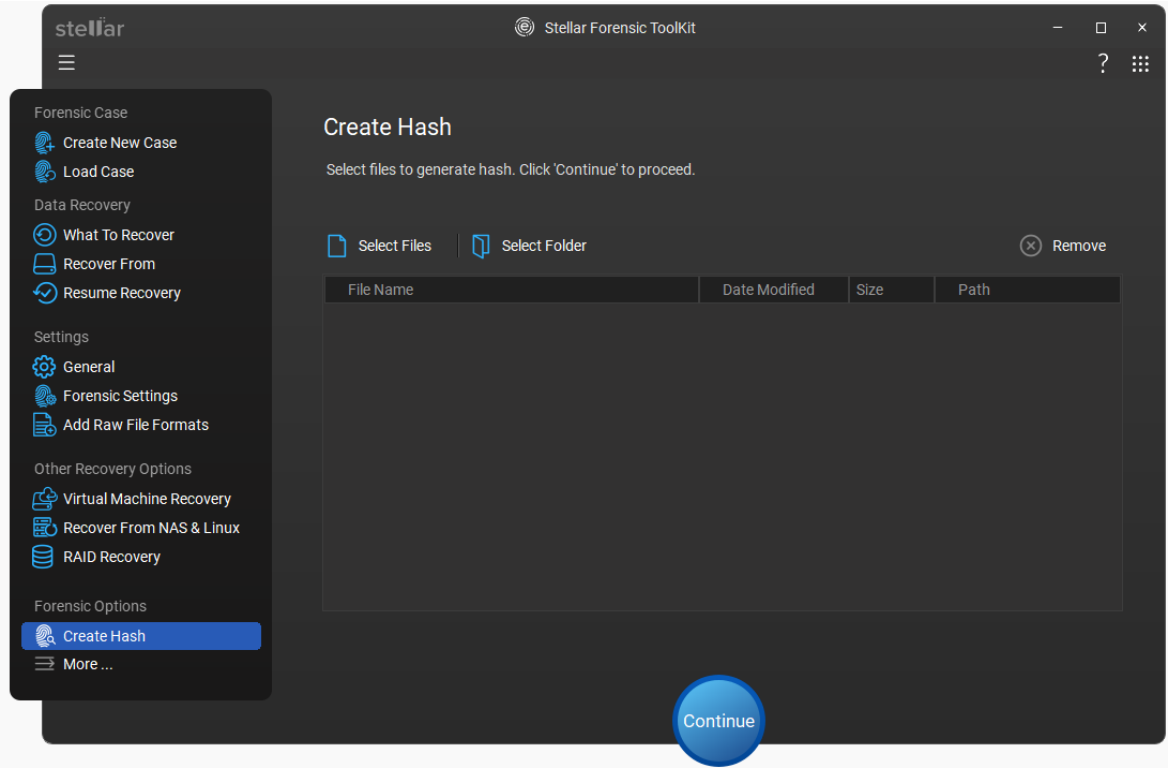
1. **Run Stellar Forensic** Toolkit.

2. From the main screen, select **Create New Case** or **Load Case** button.



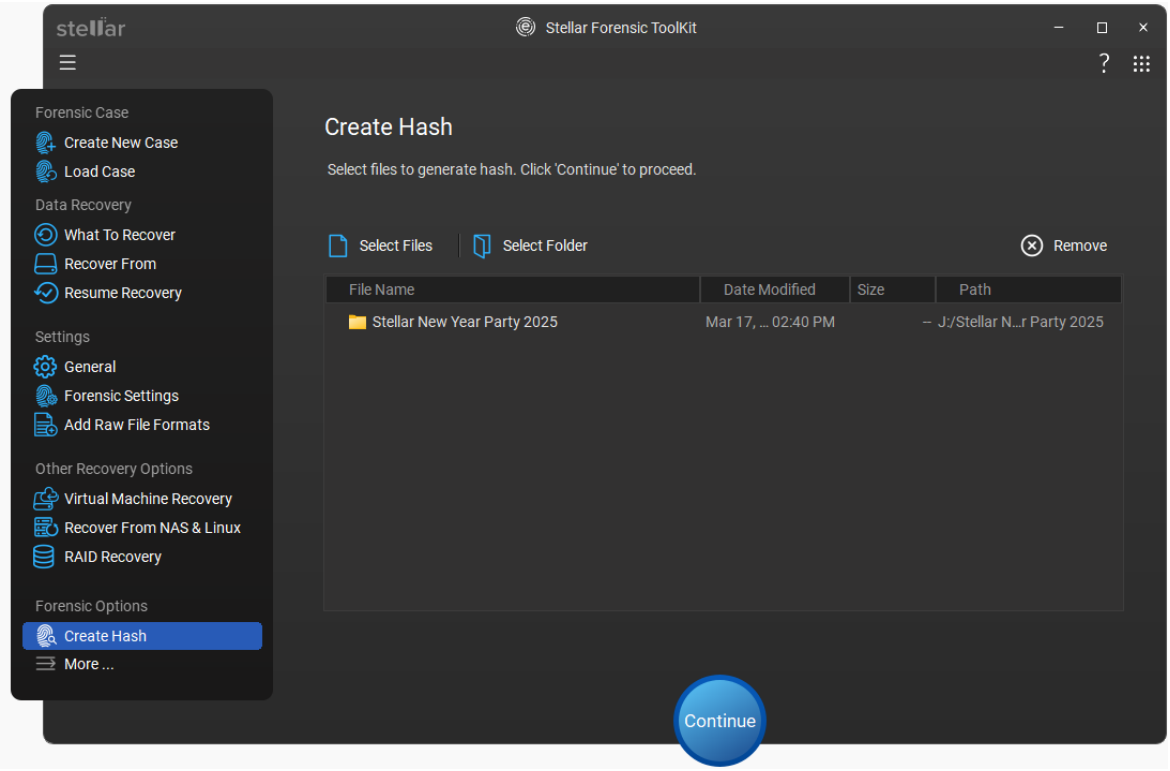
3. From the left navigation menu, go to **Forensic Options** section and click on **Create Hash**.

4. **Create Hash** window appears on the screen, as given below:

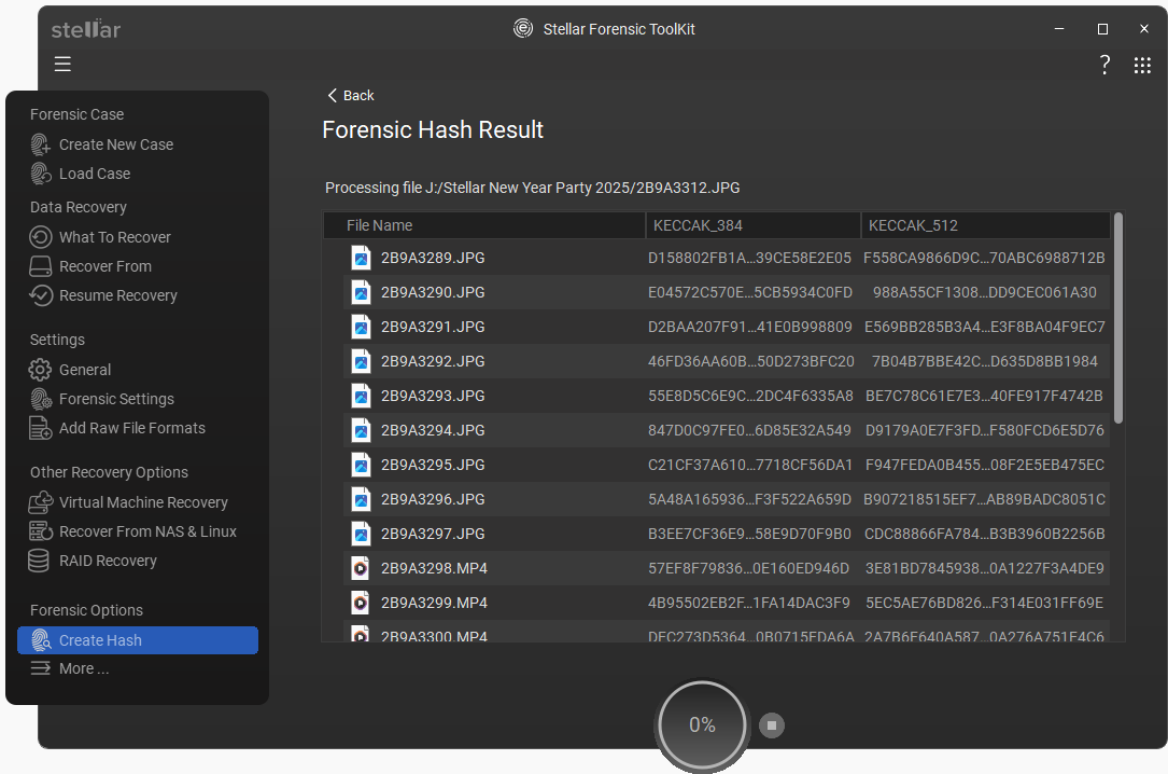


5. In the **Create Hash** window, there are two options available to select the files: **Select Files** and **Select Folder**.

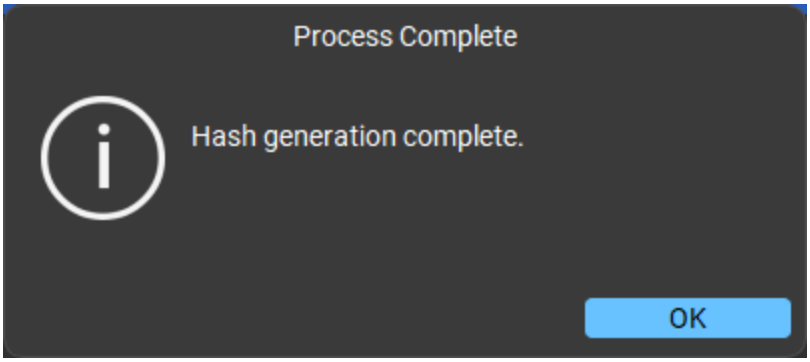
    - **Select File:** Use this option if you want to choose the required file.
    - **Select Folder:** Use this option if you want to choose the required folder.



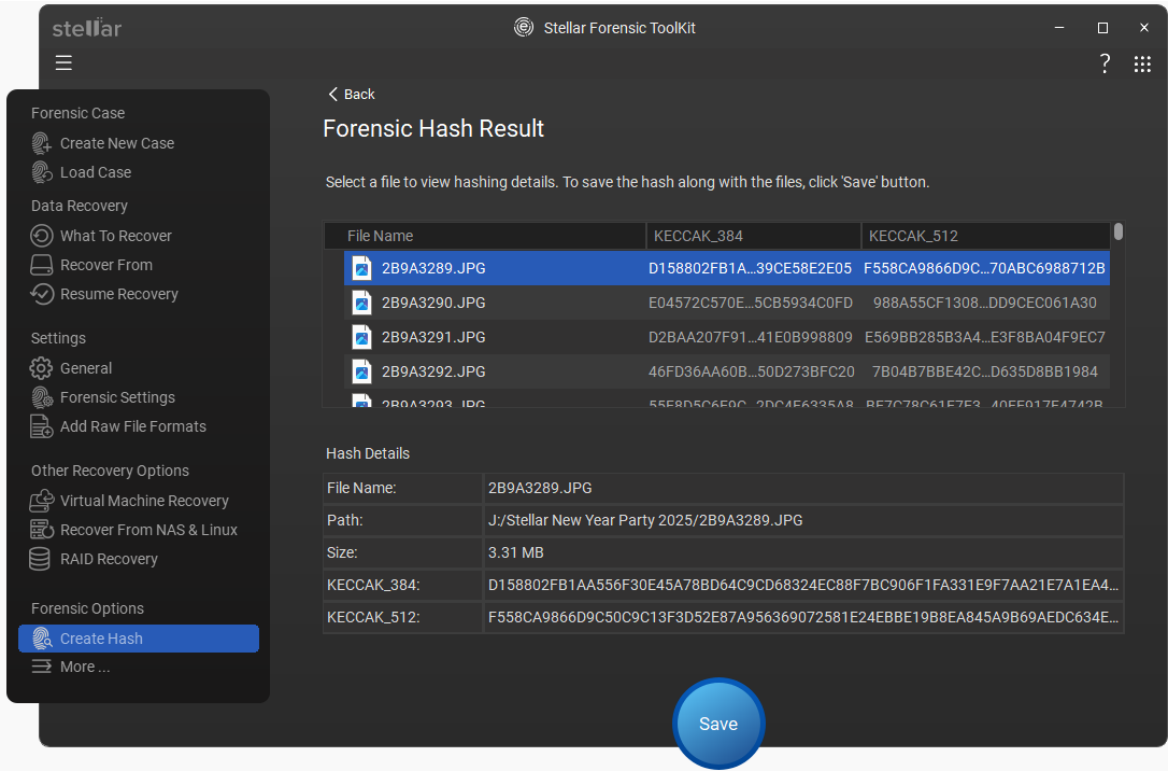
6. **Forensic Hash Result** screen will appear, displaying scanning deatils as given below:



7. **Process Complete** dialog box appears, displaying the message **"Hash generation complete".** Click **OK.**

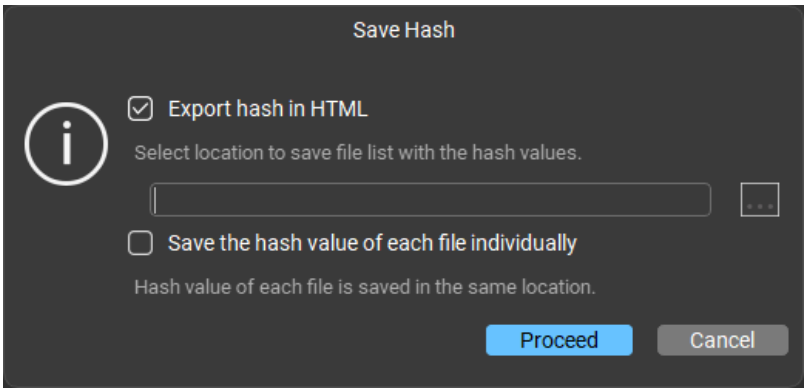


8. **Forensic Health Result** window appears, displaying file name with match algorithm such as **MD5** and **SHA256** along with Hash Deatils.



9. Click on **Save** button.

10. **Save Hash** dialog box pops up on the screen, as given below:



11. In the **Save Hash** dilog box, there are two check boxes: **Export hash in HTML** and **Save the hash value of each file individually**. You can select the check boxes individually or together as per your requirement.

    - **Export hash in HTML:** Use this check box If you want to export the hash in HTML.

    To export the hash in HTML, follow these steps:

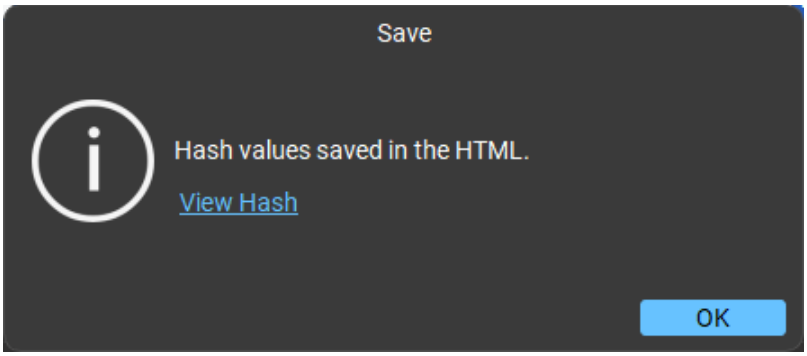
    a. Select the **Export hash in HTML** check box.

    b. Click on the **Browse** button to select the location to save the file list with hash values.

    - **Save the hash valueof each file individually:** Use this option if you want to save the hash value of each file individually at the same location.

12. Click **Proceed** to continue.

13. **Save** dilaog box appears, displaying the message **"Hash Values saved in the HTML"**.



14. To view the hash**,** click **View Hash** link in the **Save** dialog box. Click **OK**.

5. Frequently Asked Questions (FAQs)

1. **Can I use Stellar Forensic Toolkit without internet?**

   Yes, you can use it offline. All core functions like case creation, scanning, recovery, and reporting work without an internet connection.

2. **Which forensic image formats are supported for case creation?**

   The toolkit supports case creation from .E01 and .DD (001) image formats, as well as images created by other forensic software.

3. **What image types are supported for .E01 and .DD (001) cases?**

   - **E01:** Normal, Compressed, Fragmented, and Compressed-Fragmented
   - **DD (001):** Normal and Fragmented

4. **Can only audio, video, documents and photos be recovered by this software?**

   No, the software can recover all the files and folders in the selected volume. **Stellar Forensic Toolkit** can preview the types of files listed on Supported File Formats for Preview section of this manual. However, if a file type isn't listed, you can still recover it using the software.

5. **Can I verify created images for authenticity?**

   Yes. Created images can be verified using **MD5, SHA1, or SHA256 hash validation** to ensure data integrity.

6. **What reports are generated by the toolkit?**

   Three types of reports are available:

   - **Log File Summary**
   - **Forensic Case Creation Report** (includes media details, evidence overview, hash info)
   - **Forensic Case Recovery Report** (includes evidence overview, hash info, recovered files list with EXIF info and preview)

7. **Can I recover a specific file with help of this software?**

   Yes, to recover a specific file you can right-click on that particular file while preview the scanned files and select **Recover** button.

8. **What is the function of the Evidence Details dialog box?**

The Evidence Details dialog prompts during saving if evidence details are missing (e.g., DD, IMG, BIN, RAID, VM, etc.). This can be enabled or disabled from report settings (default: ON).

9. **I have deleted a volume. Can I recover the files in it?**

   Yes, choose the Recover a Lost Partition option in the application to find the lost or deleted volumes. Then continue with the scan option to recover data from the deleted volumes.

10. **What is quick scan and deep scan?**

    Quick scan is a faster scanning option. If the files are not recovered still, then you can use deep scan. Performing Deep scan is a bit slower but results are better than quick scan.

11. **How much time Stellar Forensic Toolkit will take to recover data?**

    The recovery time depends upon the size of the hard disk or volume. If the process is running that means that software is still scanning the deleted files and you have to wait for recovery process to complete. Once the process is complete you can save the recovered file at any selected location.

12. **Can I recover data from my exFAT partition?**

    Yes, you can recover data from exFAT partition. **Stellar Forensic Toolkit** supports NTFS, FAT32, exFAT, Ext2, Ext3, Ext4, HFS, HFS+, APFS, and BTRFS file systems.

13. **How to find only a particular file type and recover them?**

    You can search for a specific file in the preview window or from **File Type List** tab check the **File Types** category folders as per your choice. The files of the selected '**file types folders**' will be listed in the file list pane. Select the files and click Recover. The files are saved at the selected destination.

14. **How can I recover only deleted data?**

    There are two methods with which you can recover only the deleted data:

    - Using the **Deleted List** tab in the preview window: After scanning, the software shows preview of all the data that can be recovered. To recover only the deleted data, select the files from the **Deleted List** tab of the preview window. See Preview Scanned Results for more details.
    - Using **More Options**: The software provides an option to filter only the deleted files and folders while saving. See '**Change Recovery Option'** in More Options for more details.

15. **Can the software recover only images from a removable storage device?**

Yes, you can recover only photos from removable devices like pen drive, memory card, etc. Select *Photos* option from **Select What to Recover** screen to search the files according to your criteria.

16. **Can a recover data from a Virtual Machine using** Stellar Forensic Toolkit**?**

Yes, **Stellar Forensic Toolkit** supports the recovery of data from Virtual Machine Images. VMDK, VDI, VHD, and VHDX formats are supported. See Recover Data from Virtual Machine for more details.

17. **What is an Unallocated/RAW partition?**

A free space on the disk which doesn't belong to any partition or file system is act as an **Unallocated/RAW** space on a hard disk. This space is not listed under the drives on the PC therefore you cannot access any file or folder from this space. To access files and folders of Unallocated/RAW partitions use **Stellar Forensic Toolkit** software.

18. When a drive space becomes Unallocated/RAW?

A drive space becomes Unallocated/RAW in the following cases:

- Accidentally deleted a hard disk partition.
- A drive letter is not assigned to the partition.
- Damaged or Corrupted file system.
- An uninitialized partition of a hard disk.
- Changed partition map when a screen prompts from operating system.

19. **Can I recover data from an Unallocated/RAW partition?**

Yes, you can recover your lost or corrupted data from an **Unallocated/RAW** partition with using **Stellar Forensic Toolkit** software easily. This software helps you to find your **Unallocated/RAW** partition on a connected drive and recover lost data from it. See "Recover Data from Lost Drive/Unallocated Partition" for more details.

20. How to recover highly corrupted data when it is not even visible in the lost drive?

Severely corrupted data that can't be recovered with quick scan, deep scan, and can't find drive options; can be recovered by using **Physical Disks** option of **Stellar Forensic Toolkit** software. See "Recover Data from Physical Disks" for more information.

6. About Stellar

Stellar is a global Data Care organization offering DIY solutions for Data Recovery, Email Repair and Conversion, File and Database Repair, and Data Erasure. **Stellar**® solution portfolio comprises 100+ proprietary software tools widely used by enterprises, IT service providers, and individuals in 190+ countries. The company has presence in the USA, Europe, and Asia.

Data Recovery	**Email Repair and Conversion**
DIY tools to recover the data, including documents, photos, videos, etc., lost due to deletion, formatting, corruption, missing partition, crashed system, etc. Recovers from internal and external hard drives, portable storage, RAID, and virtual drives. *Stellar Data Recovery - Windows* *Stellar Data Recovery - Mac* *Stellar Photo Recovery* Know More >>>	Advanced tools to repair corrupted EDB, PST, OLM, and other email files and recover the mail items. Also, convert the email files of Exchange, Outlook, Apple Mail, HCL Notes (formerly IBM Notes), etc., and extract the complete mailbox data. *Stellar Repair for Exchange* *Stellar Repair for Outlook* *Stellar Converter for EDB* *Stellar Converter for OST* Know More >>>

File and Database Repair	**Data Erasure**
Powerful software to repair the corrupted database files of MS SQL, MySQL, Access, SQL Anywhere, QuickBooks, and more. Also, comprises DIY tools to repair the corrupted images and videos taken from all types of cameras. *Stellar Repair for MS SQL* *Stellar Repair for Video*	Secure and certified software for permanent wiping of laptops and desktops, loose drives, server storage, and mobile devices. The tools protect data privacy through failsafe erasure and guarantee compliance with regulatory norms. *BitRaser Drive Eraser* *BitRaser File Eraser*

Know More >>>	Know More >>>