Axcient

x360Recover
Recovery Toolkit

axcient.com

Updated: Jan 2021

Customer Support

At Axcient, we want to help you quickly resolve your technical issues and value your input to build products that incorporate your suggestions.

If you need assistance with set-up or any other technical questions or issues, please open a ticket with our Technical Support team or call:

- 720-204-4500, and select 2 for technical support, then 1 for Replibit, which includes x360Recover, or
- 800-352-0248 and select 2 for technical support, then 1 for Replibit, which includes x360Recover.

For known problem resolutions, open a browser and navigate to:

Knowledgebase:
https://support.axcient.com/hc/en-us/categories/115000502027-Axcient-x360Recover

Table of Contents

Overview of Features

The x360Recover Recovery Toolkit is a Linux Live CD containing a wealth of tools and utilities for performing system recovery, diagnostics, troubleshooting, and general digital forensics.

Note: The Recovery Toolkit supports both legacy MBR and modern UEFI system architecture.

This utility contains:

x360Recover Bare Metal Restore Wizard: Recover protected systems from a Replibit Appliance or Vault, or an exported virtual disk image directly back onto your replacement hardware. Protected systems may be recovered onto either physical or virtual machine hardware.

Replibit Driver Injector: Inject critical device drivers into an offline Windows operating system to allow it to boot properly after it has been recovered to dissimilar hardware.

Also included are tools for:

- disk partition recovery and editing
- filesystem repair
- antivirus scanning
- offline Windows registry editing
- disk cloning and imaging.
- Hardware inventory
- Disk usage profiling
- Many more

Getting Started

The x360Recover Recovery Toolkit is built on Linux, and contains a comprehensive set of utilities that should please even the most experienced Linux users. For those less familiar with Linux, the disc has been designed to look and feel as much like Windows as possible, and typical Windows users should have little difficulty navigating the GUI environment. Some of the most common applications have shortcuts located on the desktop, and the application menu behaves similarly to the Windows Start menu.

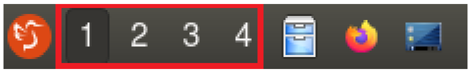
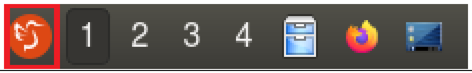
On the desktop, you will find the following items:

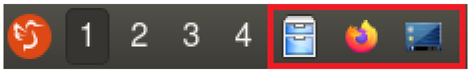
- Boot Repair – Repair most common boot start issues affecting Linux or Windows
- Computer – Browse local and network files similar to Windows Explorer
- Disk Manager – Manages the mounting and dismounting of system disks
- Driver Injector – Offline driver installer for use when recovering to dissimilar hardware
- GParted – Graphical Partition Management utility
- QTerminal – Access the Linux command shell for advanced users
- Recovery Wizard – Recover systems from a Replibit Appliance or Vault
- Remote Support – Link to Axcient ScreenConnect Portal

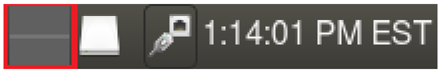
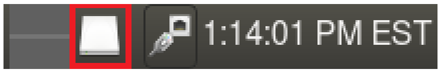
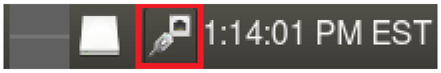
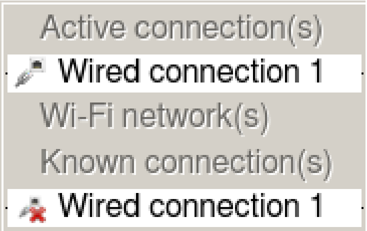
The Taskbar

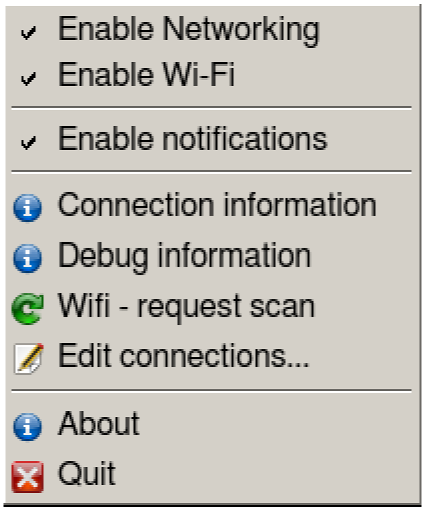
The system taskbar is located at the bottom of the desktop. This operates similarly to the Windows taskbar.

The system Taskbar contains:

Desktop Selector  	The Desktop Selector buttons allow you to toggle between four virtual desktops. After opening your Application windows, you can click on the selector buttons as shown, and easily alternate between them by clicking on each selector, 1-4.
Launcher Menu  	The Launcher Menu is similar to Windows Start menu. To open, click on the button in the bottom left corner as shown.

	Use the Launcher menu to navigate a list of installed applications as you do similarly in Windows.
Quick Launch Bar  	The Quick Launch bar contains icons for quickly launching the File Browser or Firefox web browser, as well as 'Show Desktop' for your convenience.

Task Tray	The bottom right of the screen contains the Task Tray.
System Monitor  	System Monitor presents a running graphical representation of system CPU usage
Removable Media Manager  	Left-Click on Removable Media Manager to view and manage attached removeable devices, like USB disks
Network Connections   Active connection(s) Wired connection 1 Wi-Fi network(s) Known connection(s) Wired connection 1	Network Connections allows for easy display and management of running network settings Left-Click on Network Connections to view available and active network adapters. Right-Click on Network Connections to bring up a menu of management options.

 Enable Networking Enable Wi-Fi Enable notifications Connection information Debug information Wifi - request scan Edit connections... About Quit	Connection Information displays active IP address and connection information. Edit Connections allows for manually configuring static IP address settings. If using wireless adapters select Wifi Request Scan to scan for available networks.
World Clock 	Current Time and Time Zone are displayed.

Disk Manager

Disk Manager is located on the Desktop, as well as within the Recovery Tools folder on the Launcher menu. Use Disk Manager to display the list of all attached disk devices in the system, and mount or dismount disk volumes for file access.

When the x360Recover Recovery Toolkit initially boots, only the Linux operating system on the CD itself is mounted.

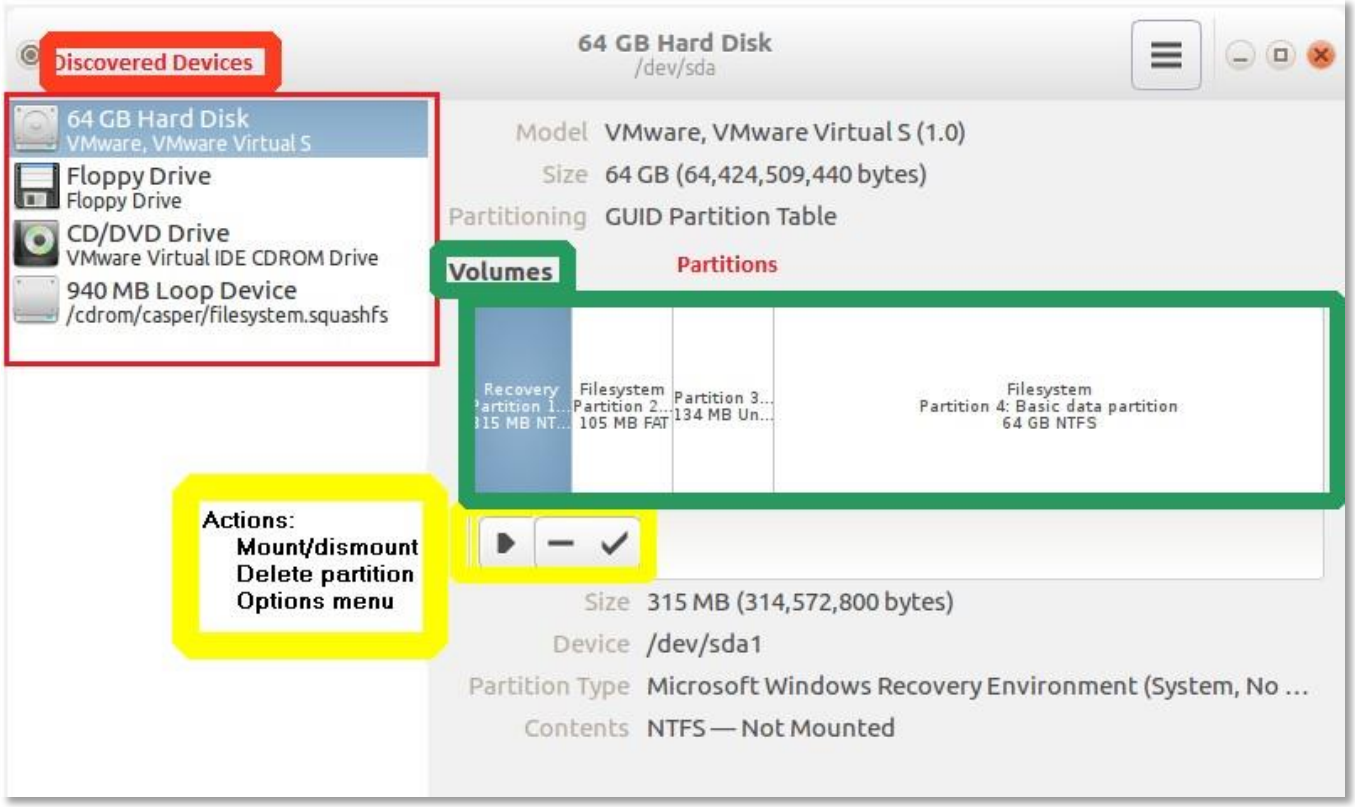
To browse and recover files from disks installed within the physical system, you will first have to open Disk Manager and mount the local disk volumes.

Using Disk Manager to mount locally attached Volumes

Within Disk Manager, there are several different panels:

- The left pane displays Discovered Devices and logical volumes.
- The right pane displays Volumes, showing partitions on the selected device.

- The *Actions pane* offers choices to mount/dismount, delete partition, or perform other options on the selected partition.



64 GB Hard Disk
/dev/sda

64 GB Hard Disk
VMware, VMware Virtual S

Floppy Drive
Floppy Drive

CD/DVD Drive
VMware Virtual IDE CDROM Drive

940 MB Loop Device
/cdrom/casper/filesystem.squashfs

Model VMware, VMware Virtual S (1.0)

Size 64 GB (64,424,509,440 bytes)

Partitioning GUID Partition Table

Size 315 MB (314,572,800 bytes)

Device /dev/sda1

Partition Type Microsoft Windows Recovery Environment (System, No ...

Contents NTFS — Not Mounted

Notes:

- Items you have selected in the Devices and Volumes panes will be highlighted in gray.
- The area *above* the Volumes pane displays detailed information about the selected device.
- The area *below* the Volumes pane shows details about the selected partition or volume.

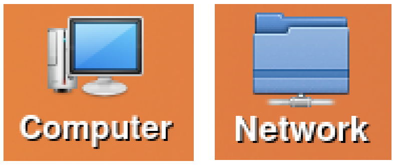
If you receive an error when trying to mount a volume (for example, indicating that an NTFS partition cannot be mounted because it is not in a clean state), repair it as follows:

1. Open QTerminal from the System Tools folder on the Launcher menu.
2. Run *sudo su* to elevate to the *root* user.
3. Identify the device name, like /dev/sda1 (See the bottom pane of DiskManager above)
4. Run *ntfsfix <device>* from the shell window. (i.e. *ntfsfix /dev/sda1*)
5. Once the partition has been repaired, mount it with Disk Manager by selecting the Volume, and then clicking on Mount from the Actions menu pane.

Note for Advanced Users: The Menu icon in the top right of the Disk Manager window offers the option to create or restore a selected disk partition to or from an image file. If you would like to save this image file to a network location, first open the File Manager and browse to the desired network location in order to mount that network share.

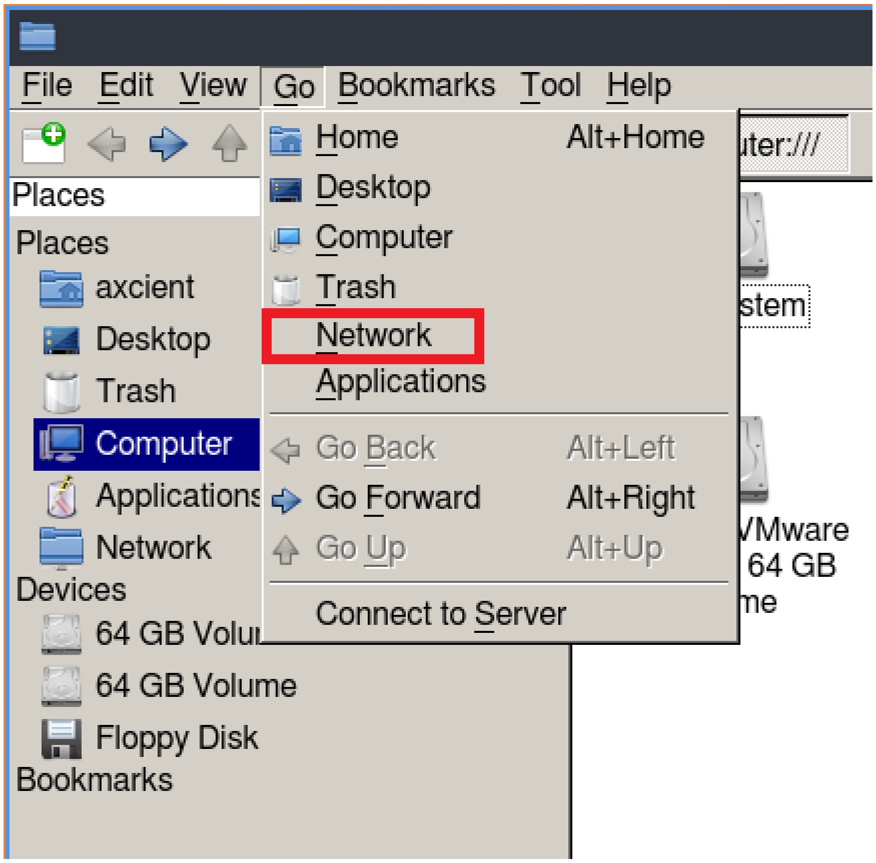
Computer (File Browser)

The File Browser operates similarly to Windows Explorer. The left pane contains devices and familiar places, and the right pane contains the filesystem content. Double-click items to open or right-click for a menu of options.



Access Windows Network Shares

To open a Windows network share, select Go from the top menu and click Network. A list of local Windows hosts will be displayed. Double-click a host to open a connection dialog window. You may also double-click the Network folder on the desktop.



When opening Network locations, a login dialog will be displayed to enter your credentials. Once you open a network share, it will be mounted and appear as a new folder on the desktop. Mounted network locations will also appear for selection in the *File >Open* dialog of any application.

Drives and Paths: How Linux differs from Windows

- IMPORTANT NOTE: Unlike Windows, Linux does not use drive letters

  (such as C:\) to reference physical disks. Instead, everything within Linux is referenced from a hierarchical top-down pathing tree. The top of the tree is referred to as the root and is represented with the forward-slash '/' symbol. All physical devices and mounted disks are represented with a path proceeding from root.

For example, user home folders are generally located in '/home'.
So, the Replibit user's home folders would be in '/home/replibit'.

Note: Linux uses a FORWARD slash '/' within path names, whereas Windows uses a BACKSLASH '\'.

- Physical devices on the system all have special reference files located within the '/dev' folder.

- Hard disk devices are generally referenced using a name containing three-letters, like hda or sdb.

- Names beginning with the letter 'h' are IDE based devices (uncommon on modern systems), while those beginning with the letter 's' are SCSI, SATA, or USB type devices. In this naming scheme, the second letter is always 'd' for 'Disk', and the last letter is an alphabetical progression from a-z designating the order for multiple disks.

For example, the *first* IDE hard drive found on the system would be '/dev/hda', the *third* SATA disk would be '/dev/sdc' and so on.

- Partitions and volumes created on a physical disk are represented by adding a number to the device name.

For example, the *first* partition on the disk '/dev/sda' would be referenced as '/dev/sda1'.

Note: Some RAID controllers (for example in HP servers) have different naming conventions. A complete list of discovered disk devices can be found by running Disk Manager.

- The special device files found within '/dev' are not directly accessible for file access.

For example, you cannot browse to '/dev/sda1/Windows'. You must first mount the desired partition somewhere within the root filesystem, in order to access its contents.

- Using Disk Manager, you would first select the disk from the left pane, then select the partition from the Volumes pane, and then click on the Mount button in the Actions menu.

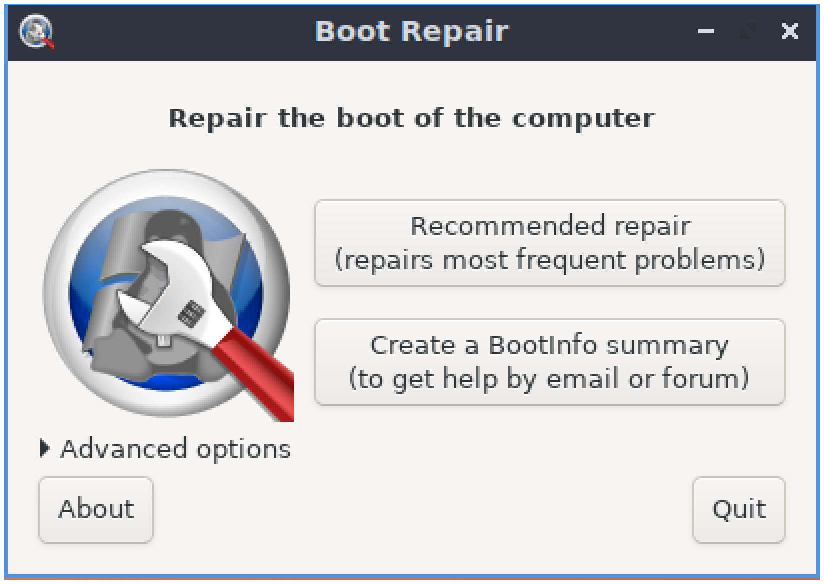
- The partition will be mounted at the path '/media/axcient/<Name>' where <Name> is the label or logical unit ID of the selected partition. The full path, including the <Name> used will be displayed in Disk Manager below the Volume window, as a clickable link.

Mounted volumes will also appear as an icon on the desktop labeled <Name>.

Available Utilities

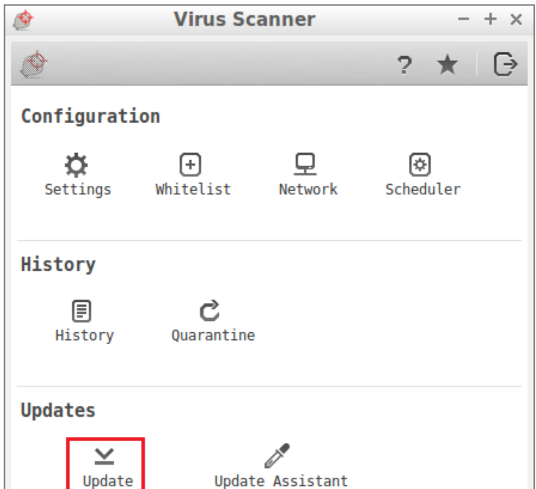
Boot Repair

Boot Repair is an open source software wizard designed to analyze and fix most types of boot related problems on Windows and Linux systems. Click on the desktop icon or select Boot Repair from the Recovery menu to perform an automated or manual repair process.


Boot Repair
Repair the boot of the computer
Recommended repair
(repairs most frequent problems)
Create a BootInfo summary
(to get help by email or forum)
Advanced options
About
Quit

Clamtk

This utility is a graphical front-end for the ClamAV command-line antivirus scanner, used to scan and remove virus and malware on an infected system, from the safety of an offline environment.

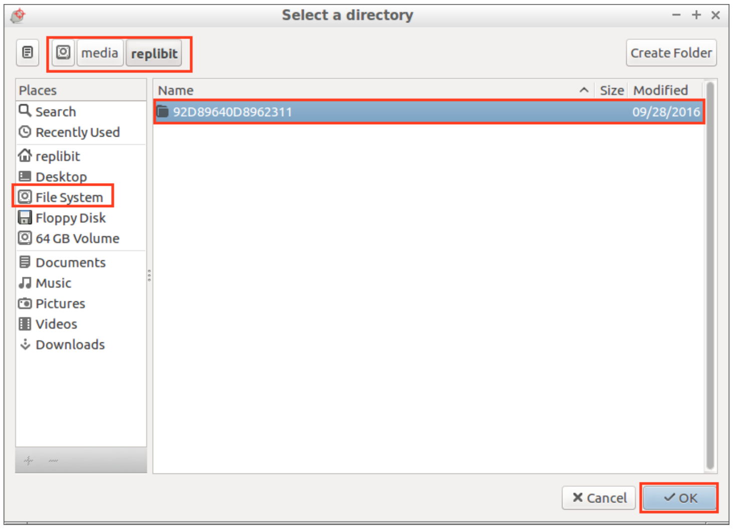


- Before launching Clamtk, use Disk Manager to mount the infected volume(s) of the offline system.
- Since we are running from a Live CD environment, there will always be a more current antivirus definition file available online. Click the Update button within the *Updates* section, and then click OK next to 'Check for Updates'. Once the updates have been downloaded, click Back to return to the main

window.

- To begin a scan, select Scan a Directory from the *Analysis* section.

- To browse to the offline system, select File System from the left pane and navigate to '/media/axcient/'. Click to select the mounted volume you would like to scan. If no volumes have been mounted, use Disk Manager to mount one.

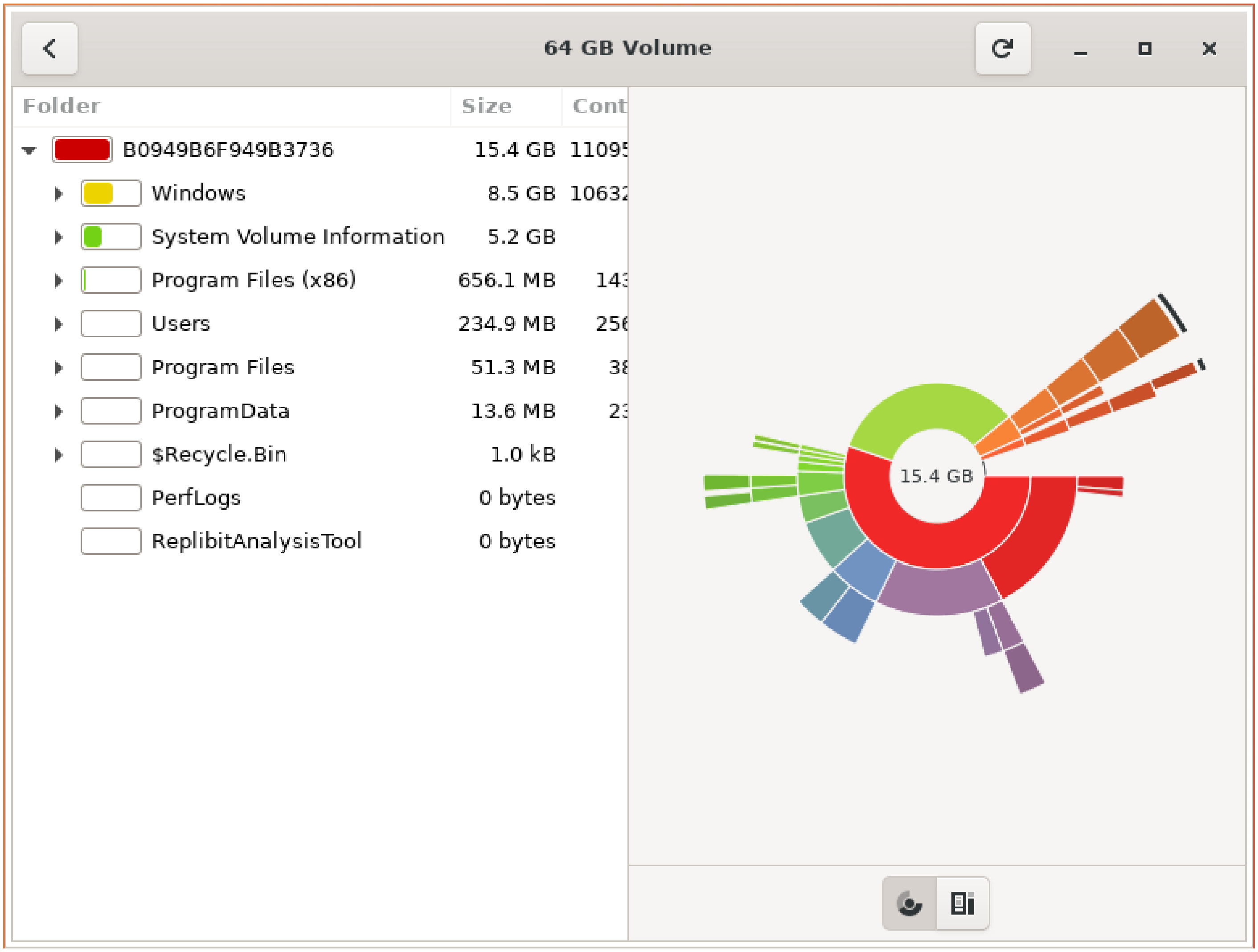


A new window will appear displaying scan progress. (The windows will be blank when the new window first opens; it may take a minute for the scan to begin.) Once the scan is completed, select the discovered items, and choose an action, such as *Clean* or *Delete*.

Note: Since we are running as a Live CD, choosing Quarantine moves the file to a location in RAM which will be lost when the system reboots. This is effectively the same as choosing Delete. If you get a questionable result (such as Windows systems files), select Analysis and the file will be checked against many other antivirus vendor databases for comparison.

Disk Usage Analyzer

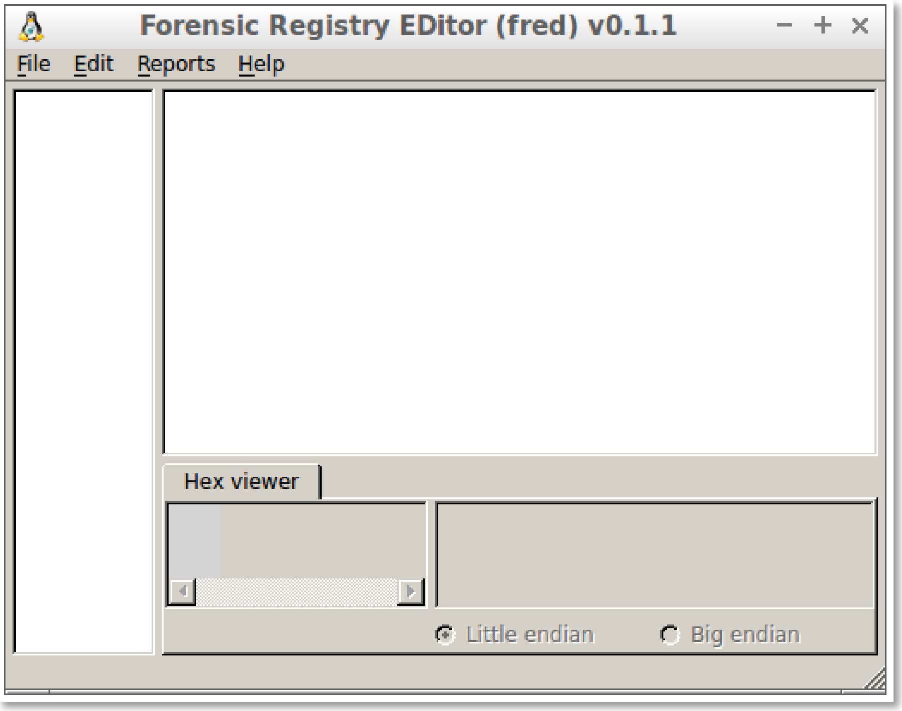
The Gnome Disk Usage Analyzer (Baobab) is a disk usage profiling utility that generates an expandable tree view and graphically displays disk usage statistics for any attached volume. Launch the Disk Usage Analyzer from the Utilities menu and select a drive or folder to profile.



Folder	Size	Cont
🟥 B0949B6F949B3736	15.4 GB	11095
🟨 Windows	8.5 GB	10632
🟩 System Volume Information	5.2 GB	
Program Files (x86)	656.1 MB	143
Users	234.9 MB	256
Program Files	51.3 MB	38
ProgramData	13.6 MB	23
$Recycle.Bin	1.0 kB	
PerfLogs	0 bytes	
ReplibitAnalysisTool	0 bytes	

Fred

The Forensic Registry Editor (Fred) is a utility to browse and edit Windows Registry files from within a Linux environment.



This utility looks and operates similarly to the Windows Regedit application, but one key difference is that Fred does not automatically open the Windows registry on launch.

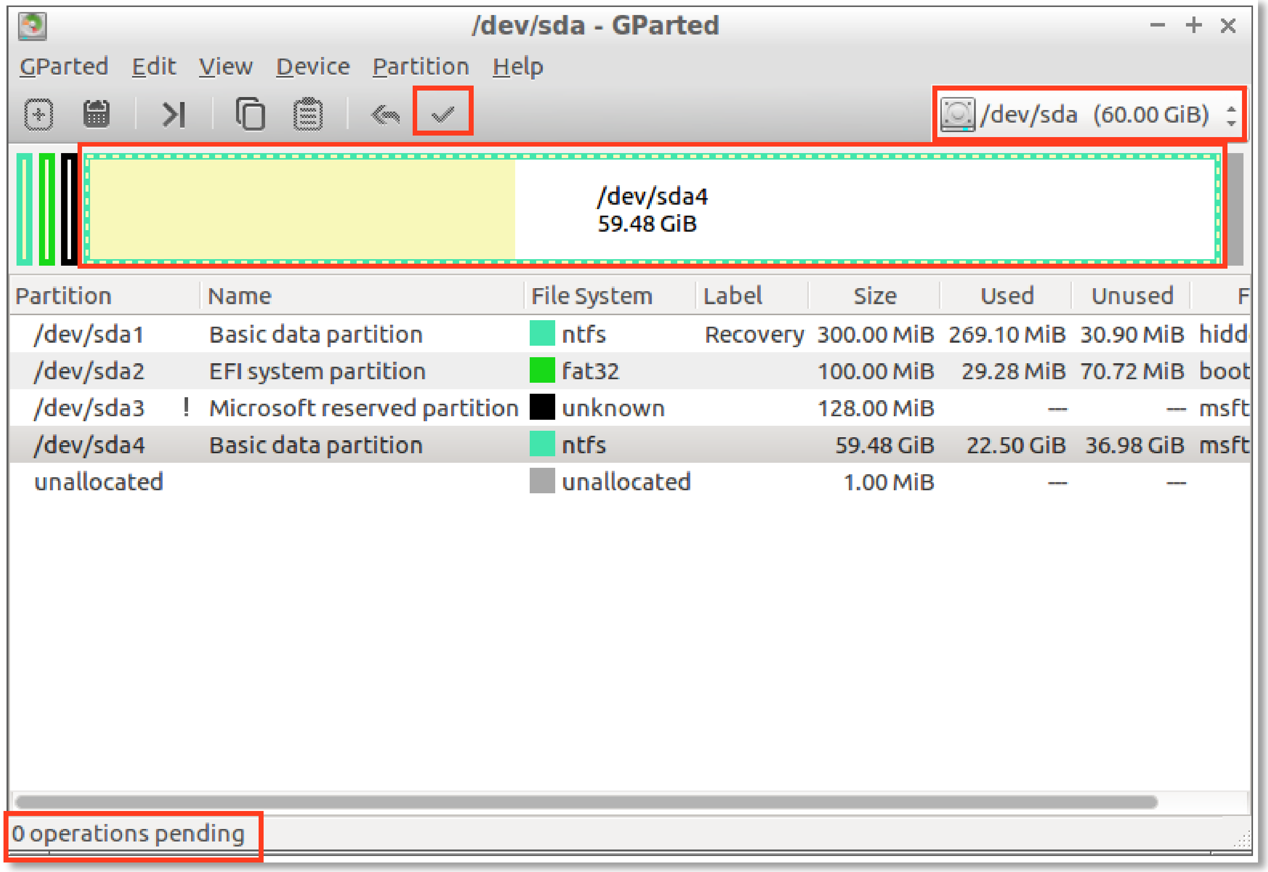
Before launching Fred, make sure that you have first run Disk Manager and mounted the disk volume containing the Windows system folder that you would like to edit.

- Launch Fred and then select File -> Open Hive.
- Browse to '/media/axcient/<Name>/Windows/System32/Config' where <Name> is the volume label of the disk containing your Windows instance.
- Within the Config folder, select the Windows Registry hive file you would like to edit (such as System or Software)
- Unlike Windows Regedit, Fred only allows access to one registry hive at a time. Fred does not display the entire registry tree at once.
- By default, Fred opens the registry hive in read-only mode for forensic analysis.
- If you wish to make changes to the registry, after you have opened a registry hive, click on the Edit menu, and then select Enable Write Support.

GParted

This application is a powerful partition management utility and includes:

- The ability to check, create, delete, resize, move, format, or copy partitions.
- Robust support for multiple operating systems, computing platforms, and filesystems.
- Support for all filesystems commonly available under Windows, Mac, and Linux.



/dev/sda (60.00 GiB)

Partition		Name	File System	Label	Size	Used	Unused	F
/dev/sda1		Basic data partition	🟩 ntfs	Recovery	300.00 MiB	269.10 MiB	30.90 MiB	hidd
/dev/sda2		EFI system partition	🟩 fat32		100.00 MiB	29.28 MiB	70.72 MiB	boot
/dev/sda3	!	Microsoft reserved partition	■ unknown		128.00 MiB	—	—	msft
/dev/sda4		Basic data partition	🟩 ntfs		59.48 GiB	22.50 GiB	36.98 GiB	msft
unallocated			▨ unallocated		1.00 MiB	—	—	

0 operations pending

1. Select the desired physical disk using the drop-down selector at the top right.

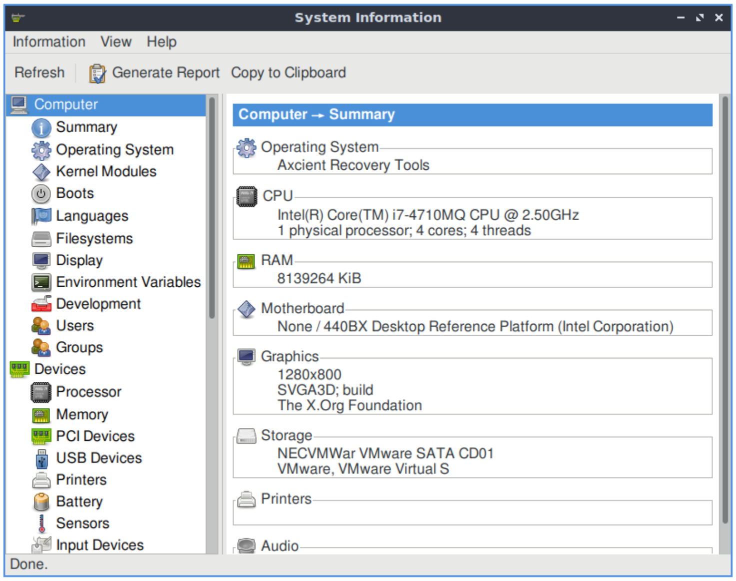
2. Right-click on individual partitions within the main window for a list of operations that may be performed.

3. After selecting a Move or Resize operation, click and drag the body or edges of the partition, or enter exact numbers in the operation dialog window to specify how you want the operation to be performed.

4. GParted does not perform most actions immediately, but rather queues them up into a batch. The list of pending actions is displayed in the lower half of the window. You may right-click pending operations and select *delete* to remove them from the list.

5. Once you have selected all of the operations that you require, click the check-mark button in the top toolbar to perform all pending actions.

Hardware Info



Computer → Summary

Operating System
Axcient Recovery Tools

CPU
Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
1 physical processor; 4 cores; 4 threads

RAM
8139264 KiB

Motherboard
None / 440BX Desktop Reference Platform (Intel Corporation)

Graphics
1280x800
SVGA3D; build
The X.Org Foundation

Storage
NECVMWar VMware SATA CD01
VMware, VMware Virtual S

Printers

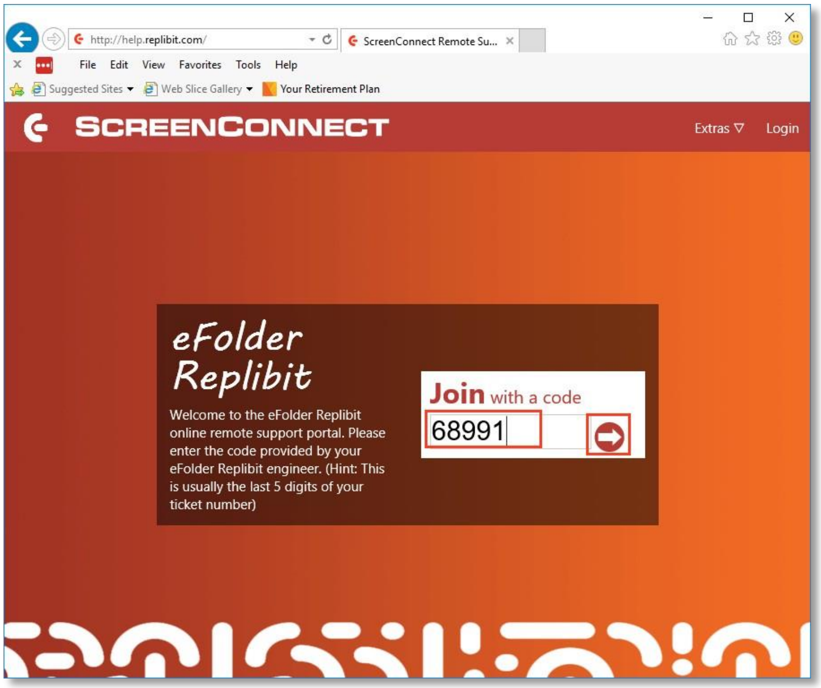
Audio

The Hardware Info utility provides a convenient graphical display of discovered hardware within the system. This is useful for determining which drivers you may need to install when recovering a protected system to a different hardware or virtual device than it was originally running on.

For example, to determine which Hard Drive controller is installed in the system, select PCI Devices from the left pane, and scroll through the main window looking for *IDE*, *SATA*, *SCSI*, or *Serial Attached SCSI* devices. Select the device and the window will populate with detailed identification data.

Remote Support

Clicking the Remote Support icon on the desktop will launch Firefox and take you to the eFolder Replibit remote support site.



Welcome to the eFolder Replibit online remote support portal. Please enter the code provided by your eFolder Replibit engineer. (Hint: This is usually the last 5 digits of your ticket number)

Enter the code provided by your Replibit support engineer and then click on the large arrow button to the right in order to share your screen.

This will provide remote access to the running Recovery Tools environment and enable direct support assistance from the eFolder Replibit engineering team.

TCP Ports 8040-8041 need to be open for outbound connections on your firewall to use our Remote Support.

Secure Erase (Scrub)

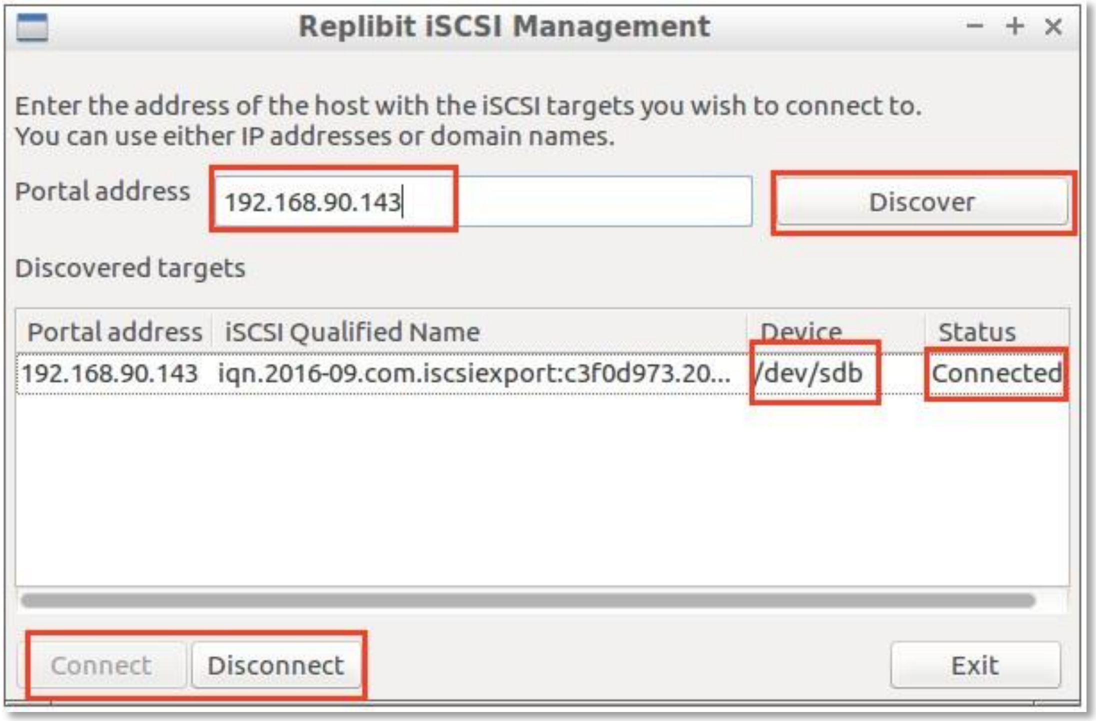
Perform a secure disk wipe and thoroughly erase all data from a disk device, using the scrub utility.
Important! This will overwrite the entire drive with random data!

- From the *System Tools* folder on the Launcher Menu or desktop shortcut, select QTerminal to open a shell window.
- At the command line type sudo su and press enter to elevate your status to the *root* user.
- To wipe a disk, type scrub <Device Path> where <Device Path> is the disk to erase. For example: *scrub /dev/sda*
- This operation may take a long time to complete if the disk is very large.

All data on the disk will become unrecoverable!

iSCSI Manager

A simple utility for managing connections to remote iSCSI disk volumes, iSCSI Manager operates similarly to Microsoft's iSCSI Initiator tool on Windows and may be used to connect to disk volumes that have been exported from a *SAN* or *NAS* device, or from a Replibit Appliance or Vault via the Start iSCSI action from the *Protected System Details* page.


Replibit iSCSI Management

Enter the address of the host with the iSCSI targets you wish to connect to.
You can use either IP addresses or domain names.

Portal address: 192.168.90.143

Discovered targets

Portal address	iSCSI Qualified Name	Device	Status
192.168.90.143	iqn.2016-09.com.iscsiexport:c3f0d973.20...	/dev/sdb	Connected

- After you have exported the iSCSI volumes, run iSCSI Manager from the *Recovery Tools* folder of the Launcher Menu.

- Enter the *IP address* of the SAN, NAS, Appliance or Vault in the Portal Address field and click on Discover. The Discovered Targets will populate with available Disk Volumes.

- To identify which Windows volume is associated with each discovered target, consult the iSCSI tab on the Web GUI of the Replibit Appliance and compare the *IQN* names. (To determine the IQN names exported by a SAN or NAS device, consult the documentation for that unit.)

- Click to select a Target Volume, and then click on Connect to mount the device as a new disk. Once mounted, the Device Name will be displayed in the *Device* column. (i.e. /dev/sdb)

- To disconnect a device, select the target and click on Disconnect. Connected devices are persistent until the system is rebooted, or the target is disconnected using iSCSI Manager.

QTerminal (Linux Command Shell)

Advanced users may find the Linux Shell console to be useful, as there are a plethora of Linux command-line utilities included on the Recovery Tools disk. To open a Linux Shell, select *QTerminal* from the *System Tools* folder on the *Launcher* menu or double click the desktop shortcut.

From the shell, a wide range of command-line utilities are available to assist with troubleshooting, repairing, searching, and so on. Some useful command-line utilities include: clonezilla, ethtool, fdisk, foremost, fsck, iotop, locate, nvme-cli, photorec, tmux and many other commands.

- To attain *root* user access, run the command *sudo su*.

Note: Documentation of Linux command-line features is beyond the scope of this manual

TestDisk

This advanced partition recovery utility can identify and recover deleted or corrupt partitions and data. TestDisk is a Shell console application, recommended to be used only by expert and experienced users who are thoroughly familiar with data recovery and Linux.

WARNING: Improper use of TestDisk can destroy your data.

Documentation of TestDisk is beyond the scope of this document.

USE AT YOUR OWN RISK!!

Overview of bare metal recovery

Bare Metal Recovery (BMR) is the process of restoring a protected system directly back onto a newly repaired or replaced hardware system.

Note: You can also perform a bare metal recovery onto virtual systems. In most cases, this virtual approach is the fastest method of recovering a protected system completely from backup.

With bare metal recovery, (as the name implies), there is no need to first load an operating system before beginning the recovery. Using the Recovery Wizard, you can simply write the protected system image directly back to the recovered system.

Prepare for a bare metal restore

We highly recommend that you practice performing a bare metal restore of your customer systems (a) to become familiar with both the recovery process and limitations and (b) to ensure you are prepared in the event of a real disaster.

The following instructions may be used to recover your protected system back onto either a bare metal system or virtual machine using the Axcient x360Recover *Recovery Toolkit*. (This is a quick overview of the Bare Metal Restore process. For complete documentation of all features of the Recovery Toolkit, refer to the Axcient Recovery Toolkit Guide.)

a. Minimum system requirements

- 2GB RAM
- 1Ghz CPU
- Bootable DVD or USB Support

b. BMR limitations and unsupported configurations

The x360Recover Recovery Toolkit operates from a Linux environment and there are several **unsupported** recovery scenarios:

- BMR recovery cannot be performed onto any hardware platform that requires Windows-only drivers. Examples of this would be any system using an unsupported motherboard RAID adapter. (Dell PERC S3xx series, Intel Cxxx controllers, and HP SmartArray B120/B320, as well as most white-box motherboard RAID controllers are examples of unsupported adapters.)
- The Recovery Wizard cannot recover systems with multiple Windows volumes on a single physical disk. (e.g. C: and E: on Disk 0). If it is necessary to perform a recovery of multiple volumes onto a single disk, refer to the Manual Partition Recovery section of the x360Recover Recovery Toolkit Guide.
- The new Destination disk *MUST* be at least as large or larger than the original disk.
- The size of any partition or volume cannot be changed before or during the recovery process.

Perform Bare Metal Recovery in x360Recover

STEP 1. Boot the x360Recover Recovery Toolkit

1. Download the Replibit Recovery Toolkit from the Axcient downloads page.
2. Burn the ISO to a DVD or create a bootable USB image. (Rufus works well for this.)
3. Boot your destination physical or virtual system from the Recovery ISO/USB.
4. Click the **Start** menu and select **Recovery Wizard** from the *Recovery Tools* menu

STEP 2. Choose the recovery mode

Choose the desired **Recovery Mode.**

You may select from three options: (a) recovery from a local appliance or vault, (b) recovery from an exported virtual disk, or (c) recovery using a disk-to-disk Copy Wizard.

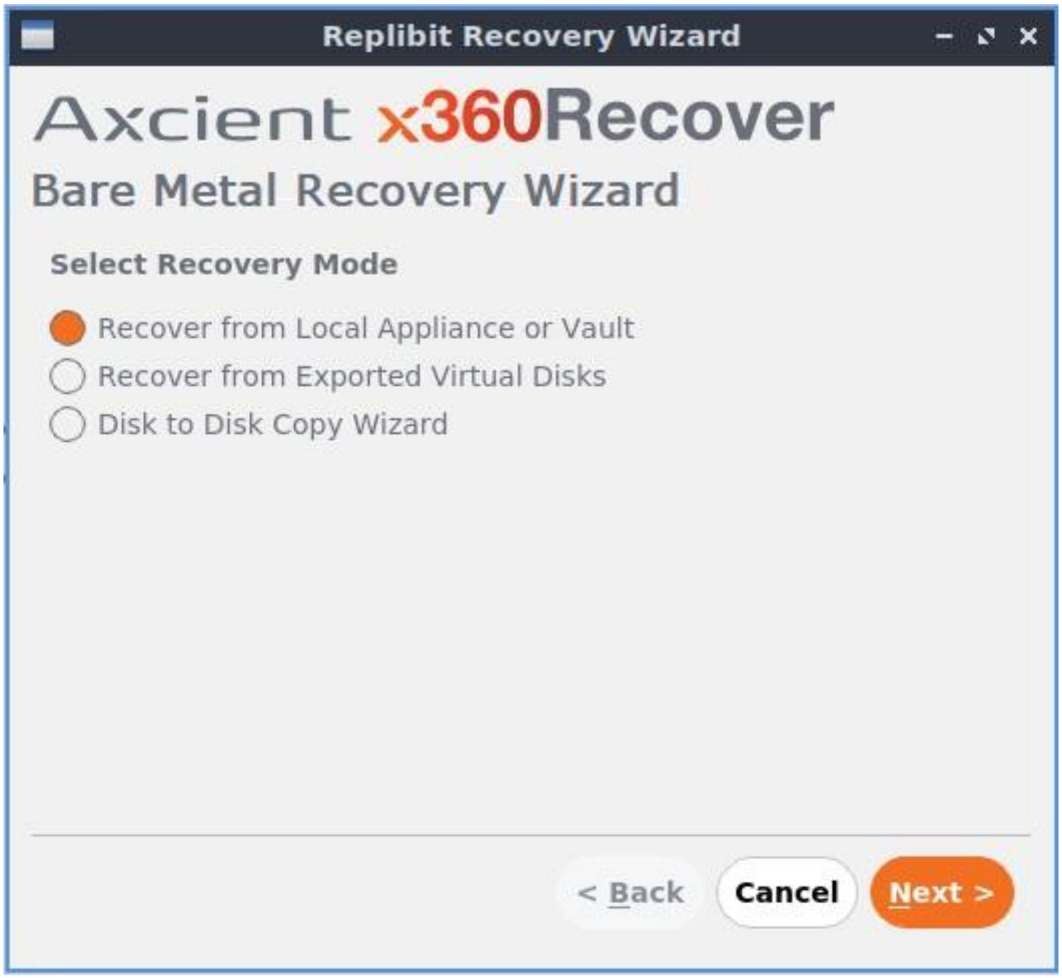
The following instructions explain the process required for each type of recovery:

Option (a) - Recover from a local appliance or a local vault

Use this method to recover from a locally-available BDR device

1. To perform a recovery directly from a locally-accessible appliance or vault BDR device onto your recovery system, select **Recover from Local Appliance or Vault** from the Bare Metal Recovery Wizard.

Note: You can't use the Bare Metal Recovery Wizard to connect to a remote vault over the internet. The connection for a remote vault must be done on the local LAN.

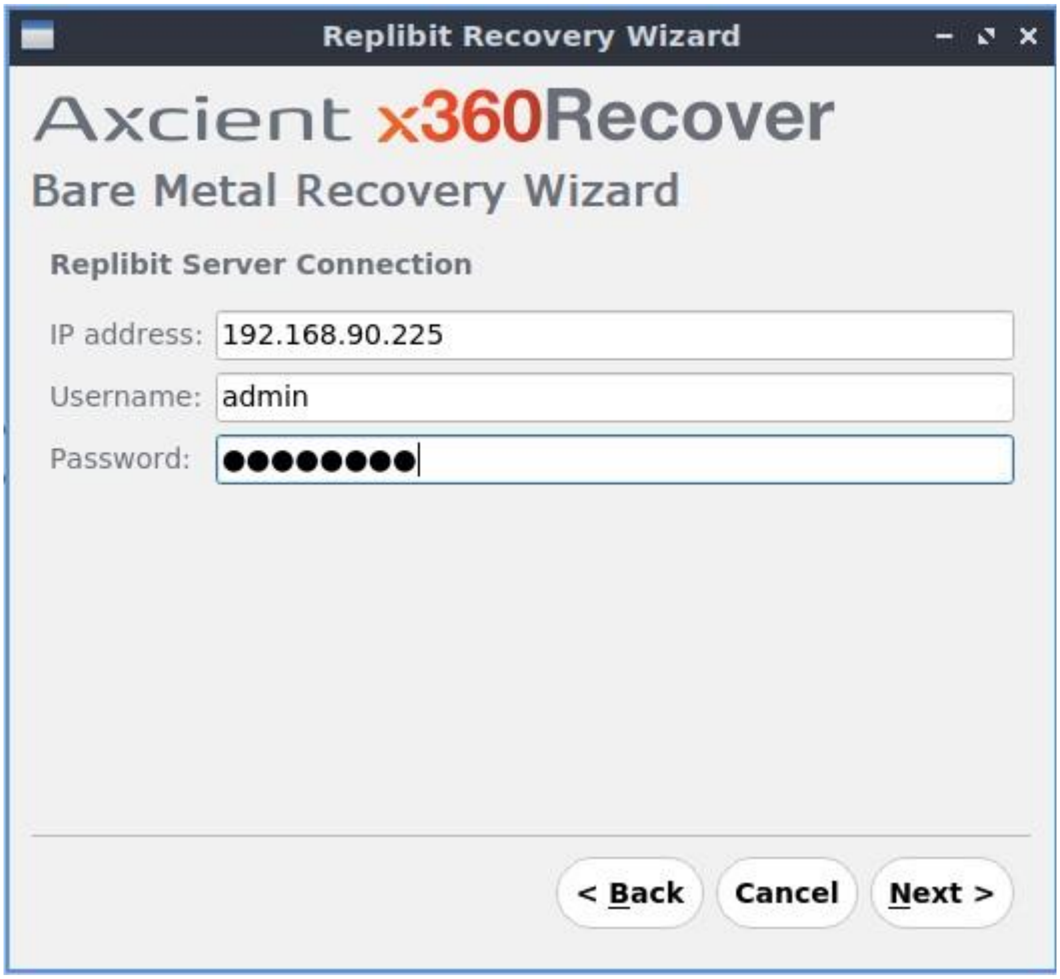


Select Recovery Mode

● Recover from Local Appliance or Vault
○ Recover from Exported Virtual Disks
○ Disk to Disk Copy Wizard

Click the **Next** button to continue.

2. In the *Replibit Server Connection* screen, enter the IP address, username and password of the appliance or vault you are connecting to.



Replibit Server Connection

IP address: 192.168.90.225

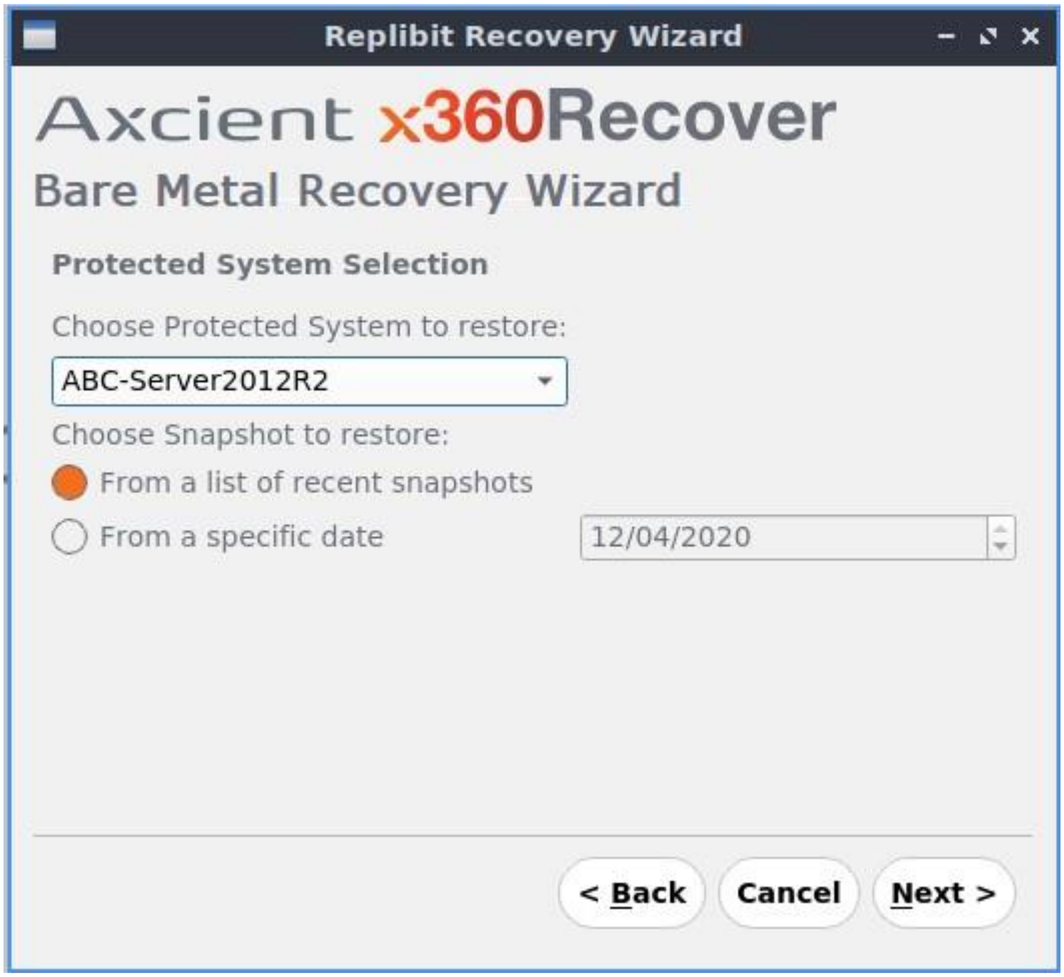
Username: admin

Password: ●●●●●●●●●

Click the **Next** button to continue.

3. In the *Protected System Selection* screen, select the protected system that should be recovered:

- From the *Chose Protected System to restore* drop-down box, select the protected system you would like to recover.
- In the *Choose Snapshot to Restore* section, select from the following options:
  - From a list of recent snapshots
  - From a specific date



Protected System Selection

Choose Protected System to restore: ABC-Server2012R2

Choose Snapshot to restore:

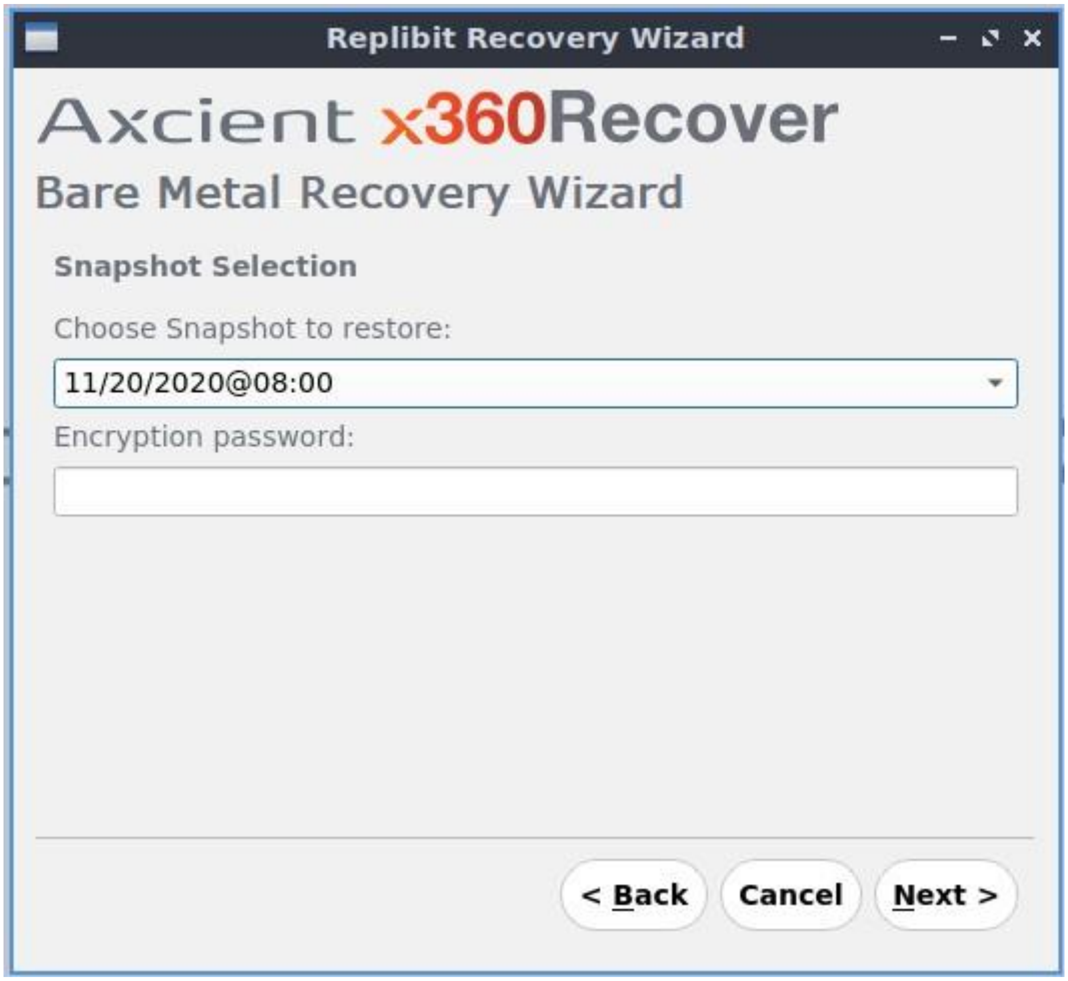
● From a list of recent snapshots

○ From a specific date 12/04/2020

Click **Next** to continue.

4. In the *Snapshot Selection* screen, select the snapshot that should be used as the recovery point:

- Select the recovery point date and time that you would like to use for recovery of the protected system.
- If an encryption passphrase was configured when the agent was installed on this protected system, enter the **Encryption password**.



Snapshot Selection

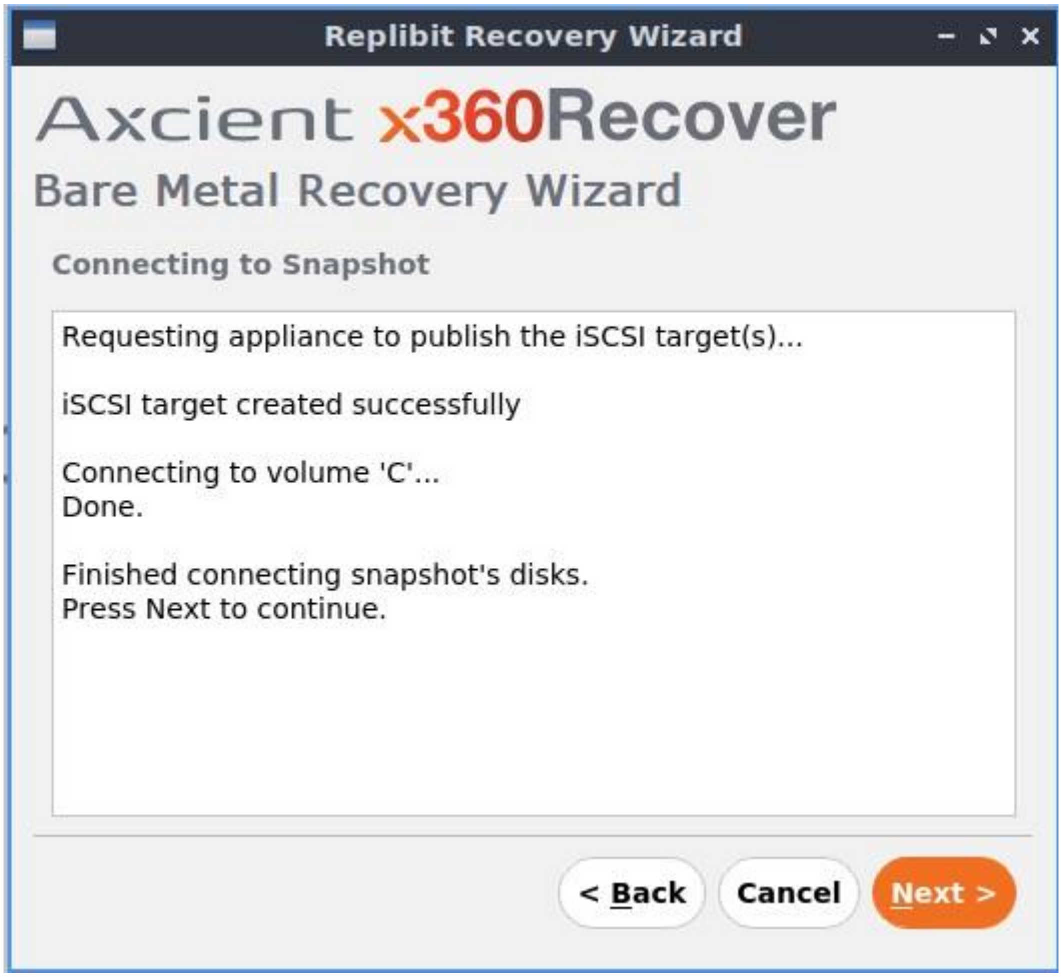
Choose Snapshot to restore: 11/20/2020@08:00

Encryption password:

Click the **Next** button to continue.

5. The Recovery Wizard will now initialize iSCSI services, export the selected recovery point on the appliance or vault, and attach the disk volumes.

Verify that the iSCSI operations completed successfully, and that no errors are reported.



Requesting appliance to publish the iSCSI target(s)...

iSCSI target created successfully

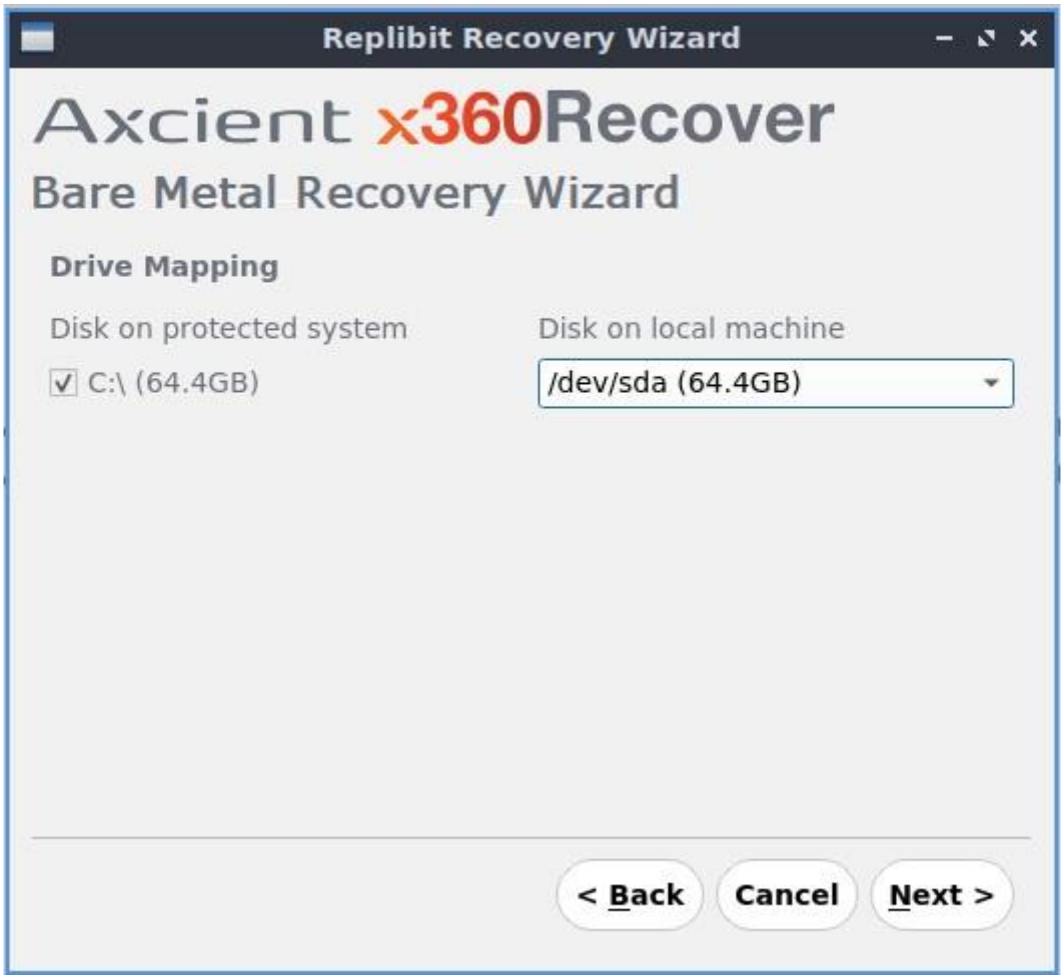
Connecting to volume 'C'...
Done.

Finished connecting snapshot's disks.
Press Next to continue.

Click the **Next** button to continue.

6. In the *Drive Mapping* screen, select the drive volume(s) you wish to recover:

- Check the checkboxes next to the appropriate drive volumes.
- For each volume being recovered, choose a disk to restore it to by selecting from the dropdown list.



Drive Mapping

Disk on protected system: ☑ C:\ (64.4GB)

Disk on local machine: /dev/sda (64.4GB)

Click **Next** to continue.

Regardless of the recovery method you have selected, the data recovery process will now begin.

You will now monitor the overall job progress from the Recovery Wizard status window.

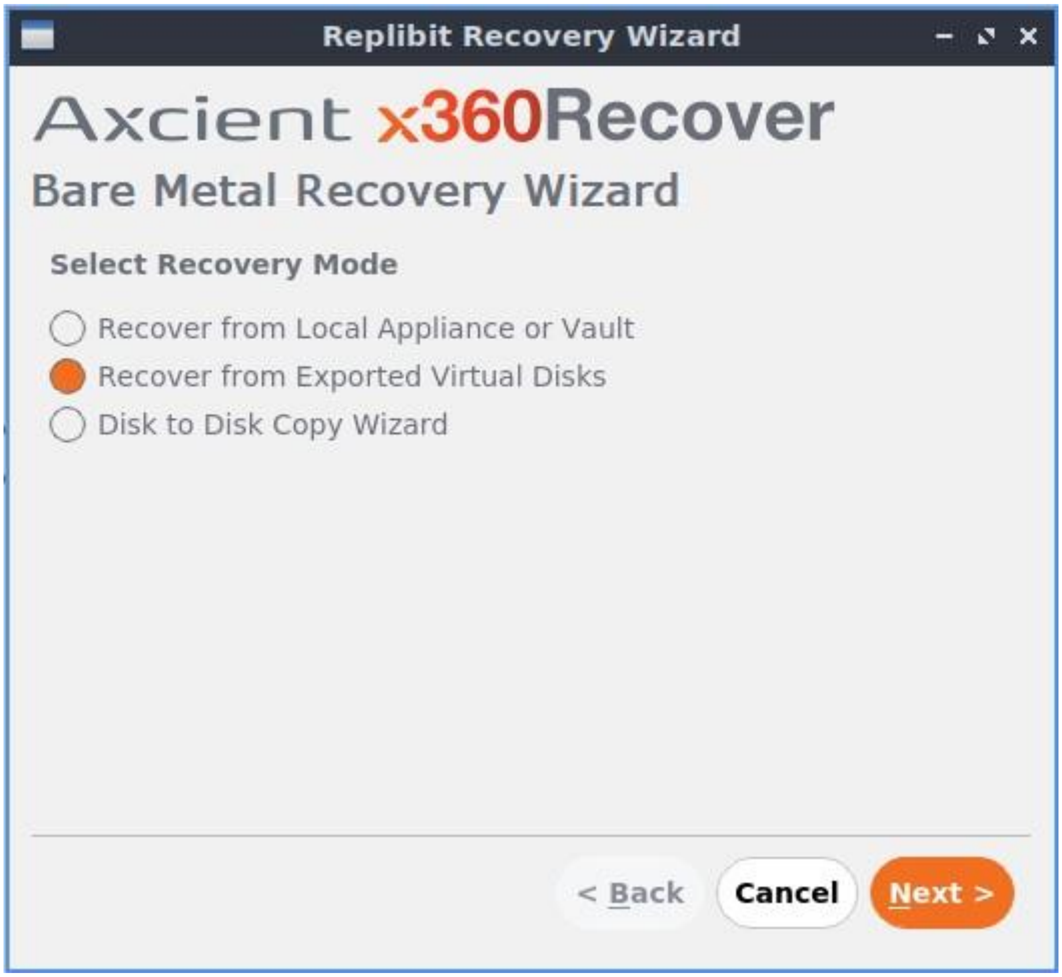
Continue to **STEP 3. Disk Recovery Operation** in the instructions below for more information on how to proceed.

Option (b) - Recover from an exported virtual disk

Use this method to recover from an exported disk image available on USB or NAS storage.

You can use this method to recover a protected system from any VHD, VHDX, or VMDK image file. Create an exported virtual disk image by using **Export** on any snapshot from the protected systems details page.

1. To perform a recovery from an exported virtual disk image, select **Recover from Exported Virtual Disk** from the Bare Metal Recover Wizard.



Replibit Recovery Wizard

Axcient x360Recover

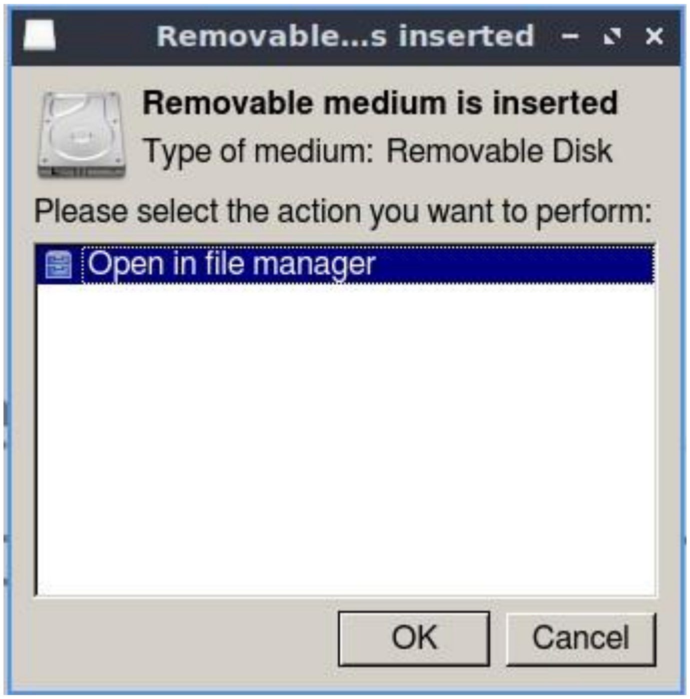
Bare Metal Recovery Wizard

Select Recovery Mode

○ Recover from Local Appliance or Vault
● Recover from Exported Virtual Disks
○ Disk to Disk Copy Wizard

Click **Next** to continue.

2. Attach a USB disk containing the exported virtual disk image you wish to restore to the recovery system. A popup should appear showing that the device has been mounted.



Removable...s inserted

Removable medium is inserted

Type of medium: Removable Disk

Please select the action you want to perform:

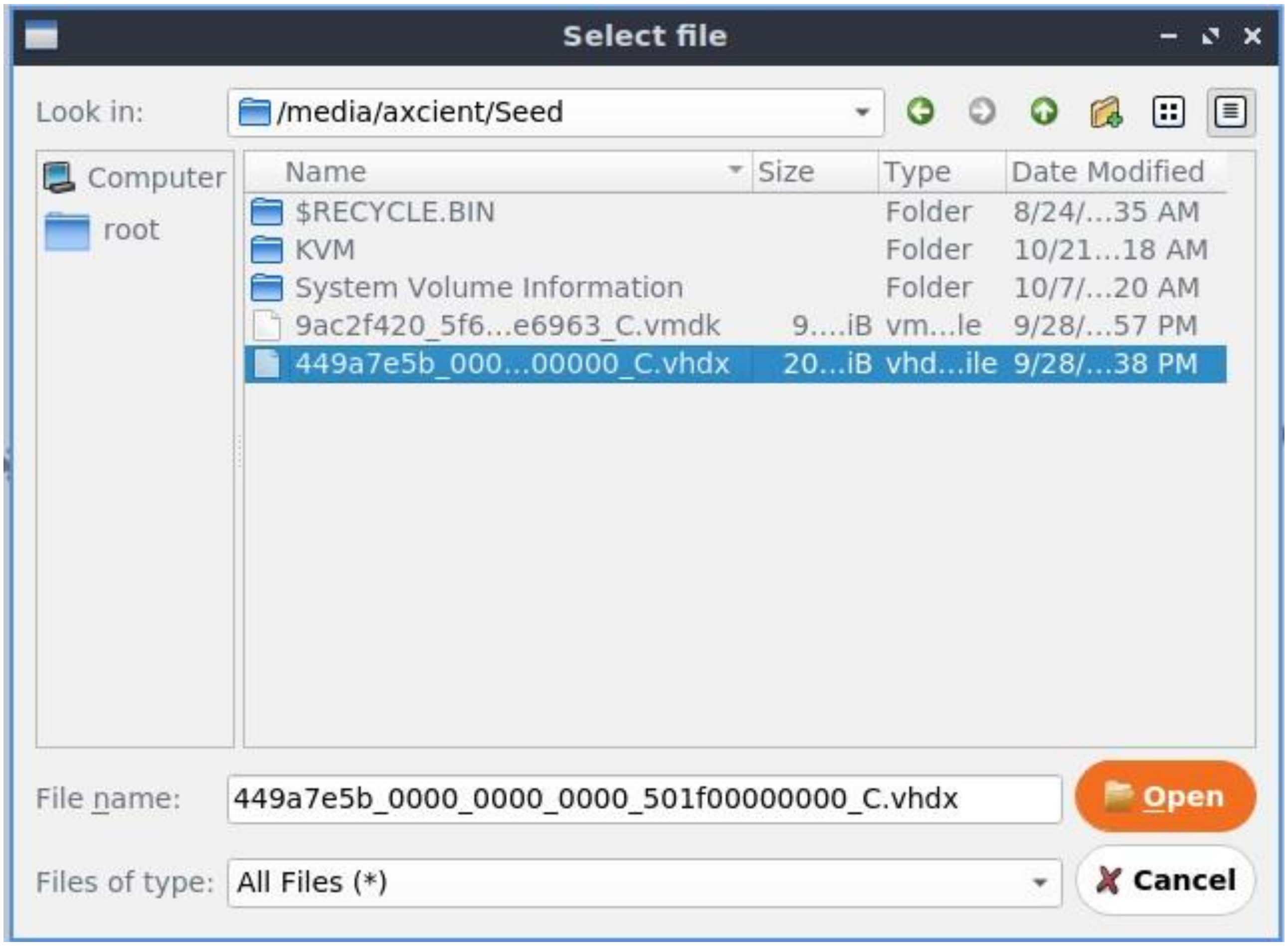
3. Cancel or close the popup and return to the Bare Metal Recovery Wizard.

4. On the *Drive Mapping* page, click the **Browse** button and select the *Source Virtual Disk*.

Locate the mounted USB drives at /media/axcient/<label> (where <label> is the volume label name of the mounted drive).

Browse to and select the VHD, VHDX or VMDK file you wish to recover from.

Click **Open** to continue.



Look in: /media/axcient/Seed

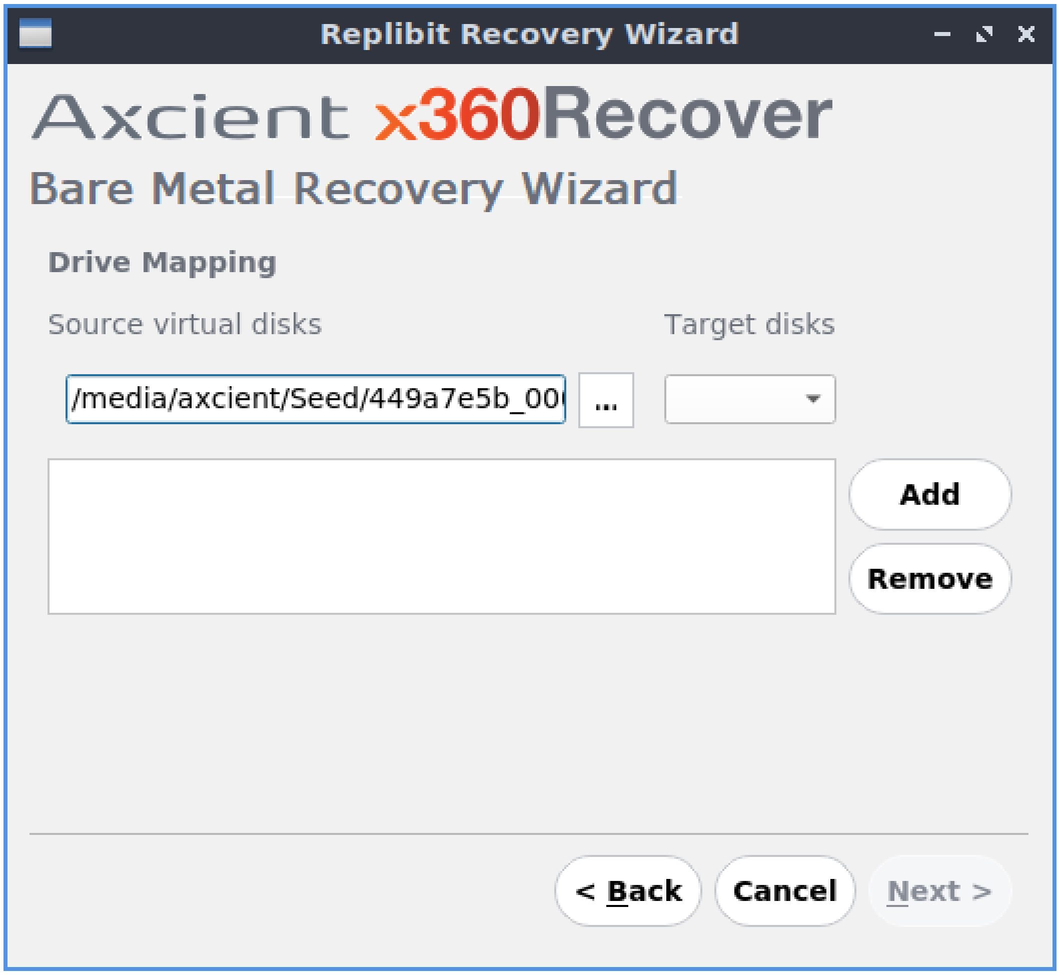
Name	Size	Type	Date Modified
$RECYCLE.BIN		Folder	8/24/...35 AM
KVM		Folder	10/21...18 AM
System Volume Information		Folder	10/7/...20 AM
9ac2f420_5f6...e6963_C.vmdk	9....iB	vm...le	9/28/...57 PM
449a7e5b_000...00000_C.vhdx	20...iB	vhd...ile	9/28/...38 PM

File name: 449a7e5b_0000_0000_0000_501f00000000_C.vhdx

Files of type: All Files (*)

5. Once you have selected a disk, map it to the appropriate *Target Disk*.

Click **Add** to save it to the list.



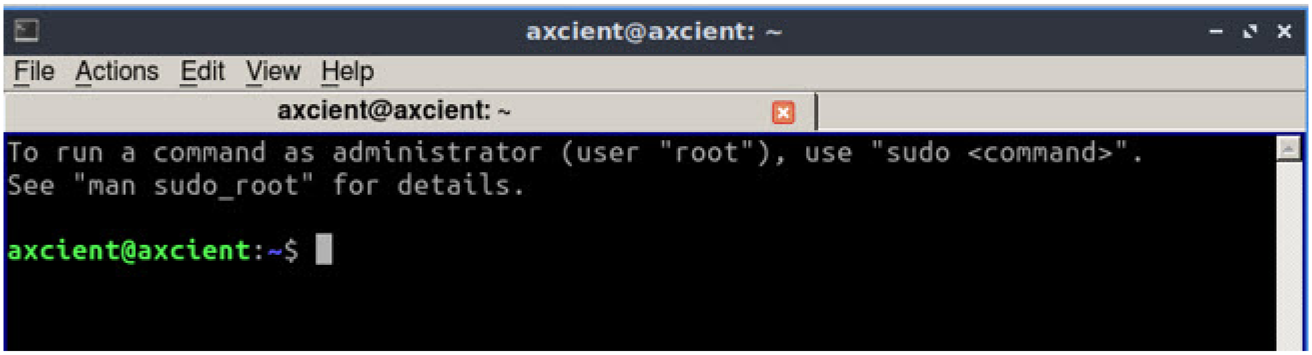
Repeat the above steps to map additional virtual disks to local physical disks for recovery, if necessary.

Click **Next** to continue.

Map a network share

6. If your virtual disk image is located on a network share, you will have to manually mount that share onto the running live CD environment.

Click the **Start** menu and select **QTerminal** from the *System Tools Menu*.



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

axcient@axcient:~$
```

Elevate the command prompt to the root user by executing:

sudo su

Mount the Windows share using the following command syntax:

mount -t cifs -o username="<user name>",domain="<domain name>" //<Windows Server Name>/<Share Name>   /<Mount location>

For example:

Server name is **Server2012**

Share name is **Files**

To login as the user Administrator for domain MyDomain and mount it at */mnt* use:

Mount -t cifs -o username="Administrator",domain="MyDomain" //Server2012/Files   /mnt

Note: If you have issues connecting by server name, you may use the IP address instead.

If you need to mount multiple shares, create folders for each mount point using mkdir

mkdir   /mnt/Share1

Regardless of the recovery method you have selected, the data recovery process will now begin.

You will now monitor the overall job progress from the Recovery Wizard status window.

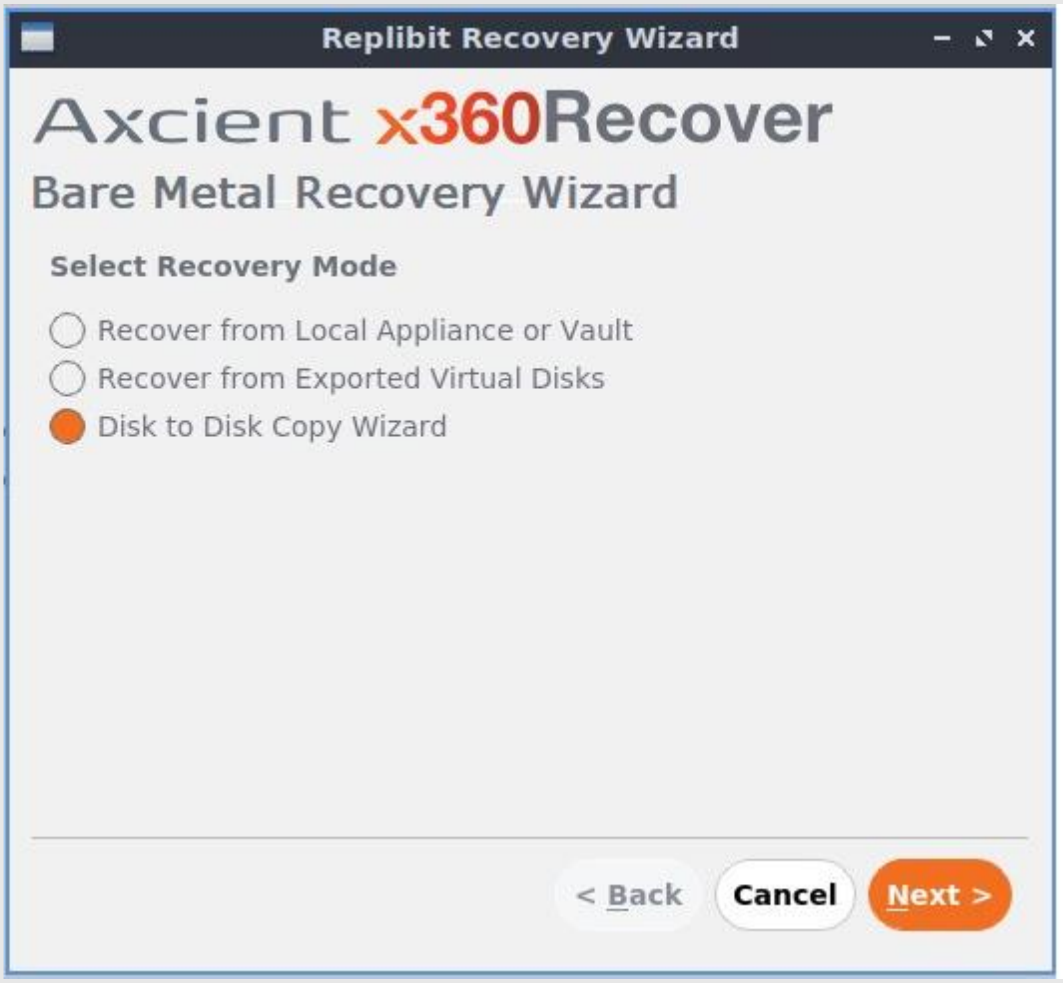
Continue to **STEP 3. Disk Recovery Operation** in the instructions below for more information on how to proceed.

Option (c) - Recover using the disk-to-disk Copy Wizard

Use this method to perform a direct copy of one or more drives to another

Recover using a disk-to-disk Copy Wizard

1. To perform a simple disk-to-disk copy operation for system recovery, troubleshooting or diagnostics, select **Disk to Disk Copy Wizard** from the *Bare Metal Recovery Wizard*.



Replibit Recovery Wizard

Axcient x360Recover

Bare Metal Recovery Wizard

Select Recovery Mode

○ Recover from Local Appliance or Vault

○ Recover from Exported Virtual Disks

● Disk to Disk Copy Wizard

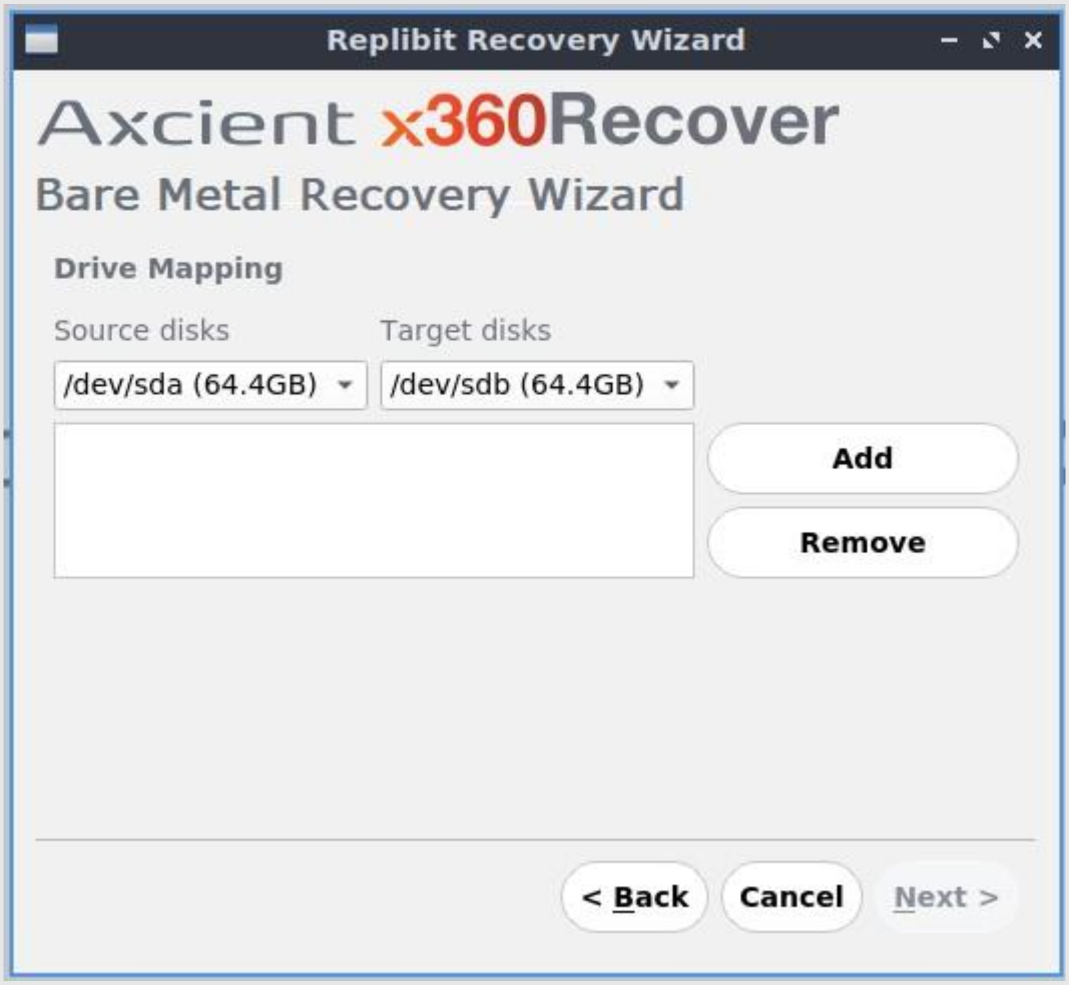
Click **Next** to continue.

2. Select a source disk.

3. Select a target disk.

4. Click **Add** to add them to the list.

Repeat if necessary, to add additional disks to be copied.



Click **Next** to continue.

Regardless of the recovery method you have selected, the data recovery process will now begin.

You will now monitor the overall job progress from the Recovery Wizard status window.

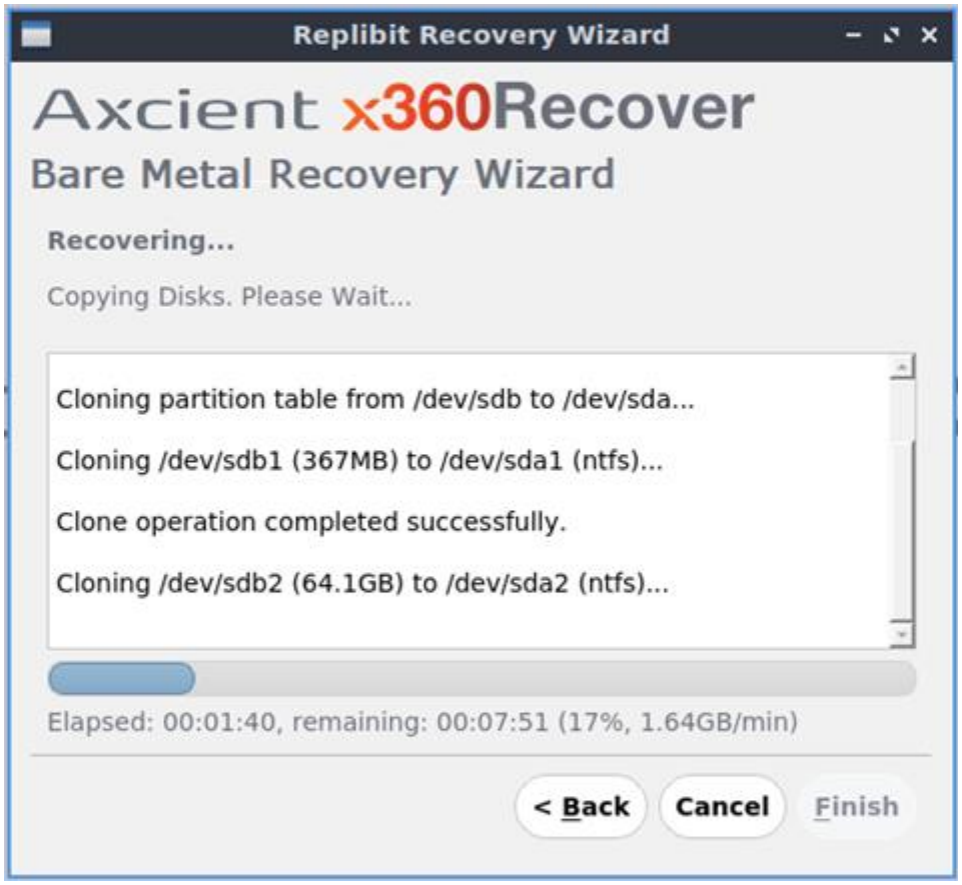
Continue to **STEP 3. Disk Recovery Operation** in the instructions below for more information on how to proceed.

STEP 3. Disk recovery operation (Common to all three modes)

Regardless of which recovery method you selected above, the data recovery process will now begin.

Monitor the overall job progress from the Recovery Wizard status window.

- Detailed job information is presented in the main window.
- Job status and estimated time remaining for the current copy phase are shown at the bottom.



```
Cloning partition table from /dev/sdb to /dev/sda...
Cloning /dev/sdb1 (367MB) to /dev/sda1 (ntfs)...
Clone operation completed successfully.
Cloning /dev/sdb2 (64.1GB) to /dev/sda2 (ntfs)...
```

Elapsed: 00:01:40, remaining: 00:07:51 (17%, 1.64GB/min)

Once the recovery process is completed, click the **Finish** button.

You may *Reboot* the system immediately; or if you are restoring to a system with dissimilar hardware, please proceed to **Dissimilar Hardware Driver Injection** instructions below.

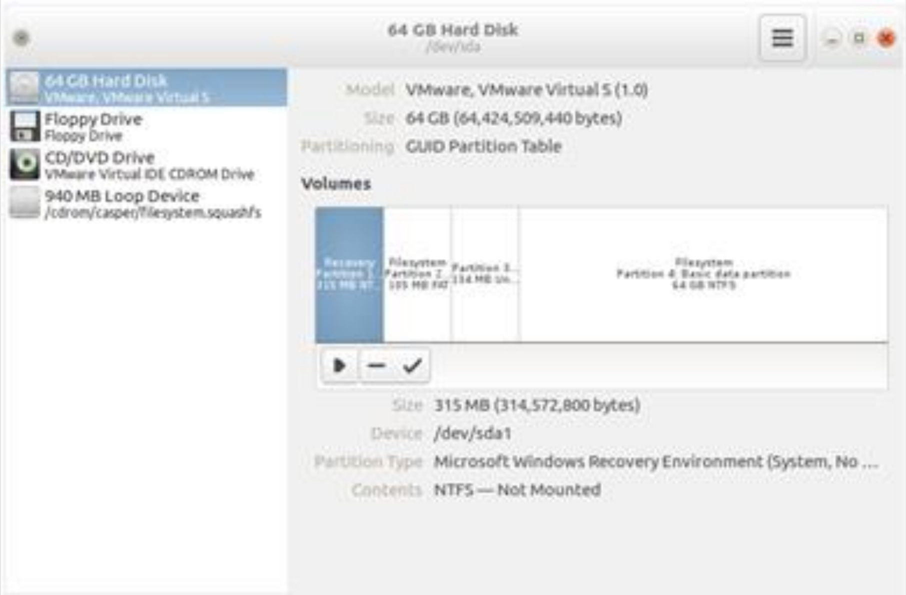
STEP 4. Dissimilar hardware driver injection

If you are recovering to a bare metal system, it is likely that the new hardware is substantially different from the original machine.

This means the recovered system will need to have drivers installed for the new devices.

Perform the following steps to inject drivers into the offline system ***AFTER*** performing the recovery, but ***PRIOR*** to booting it for the first time from the recovered image:

1. Mount the volume containing the *C:* drive of the protected system using *Disk Manager*.



64 GB Hard Disk
/dev/sda

64 GB Hard Disk
VMware, VMware Virtual S

Floppy Drive
Floppy Drive

CD/DVD Drive
VMware Virtual IDE CDROM Drive

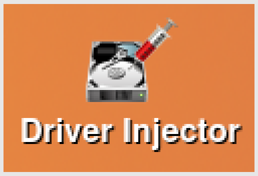
940 MB Loop Device
/cdrom/casper/filesystem.squashfs

Model VMware, VMware Virtual S (1.0)
Size 64 GB (64,424,509,440 bytes)
Partitioning GUID Partition Table

Volumes

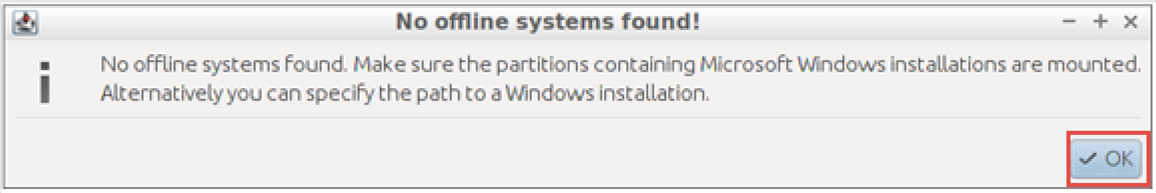
Size 315 MB (314,572,800 bytes)
Device /dev/sda1
Partition Type Microsoft Windows Recovery Environment (System, No ...
Contents NTFS — Not Mounted

2. From the *Recovery Tools* menu or desktop shortcut, click to launch the **Driver Injector**.



3. The *Replibit BMR Driver Injector* screen displays.

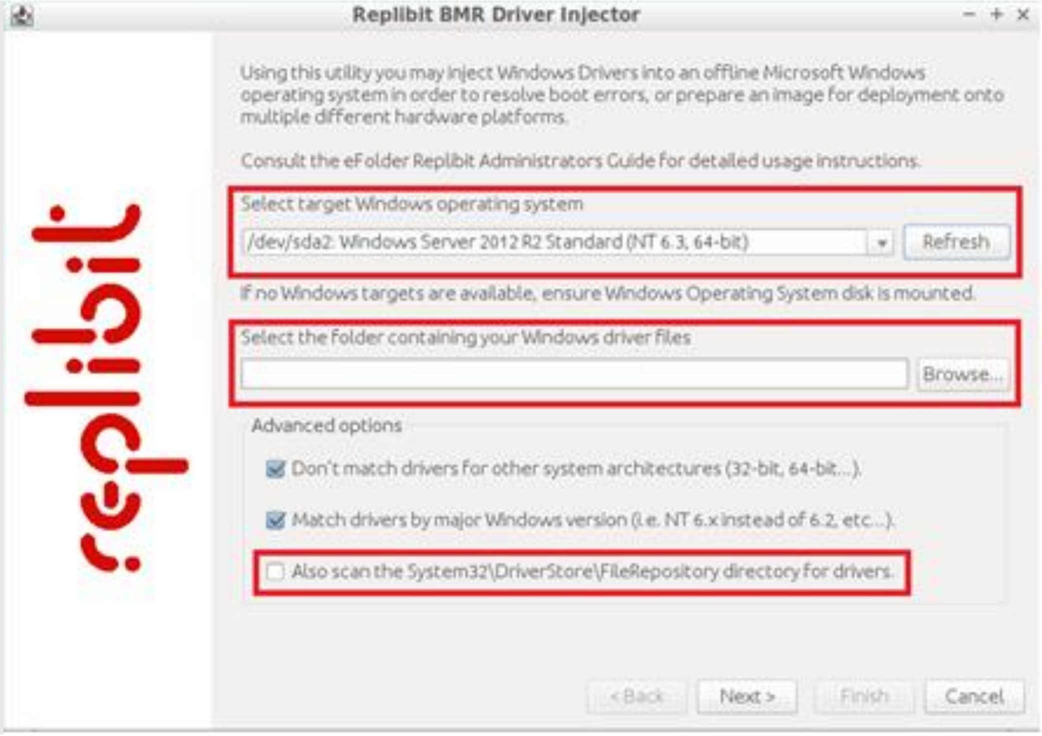
Note: If you have not mounted a disk volume that contains a valid Windows installation folder, you will receive a warning that the Driver Injector could not locate the offline Windows installation.



No offline systems found!

No offline systems found. Make sure the partitions containing Microsoft Windows installations are mounted.
Alternatively you can specify the path to a Windows installation.

Configure the target settings:



Using this utility you may inject Windows Drivers into an offline Microsoft Windows operating system in order to resolve boot errors, or prepare an image for deployment onto multiple different hardware platforms.

Consult the eFolder Replibit Administrators Guide for detailed usage instructions.

Select target Windows operating system

/dev/sda2: Windows Server 2012 R2 Standard (NT 6.3, 64-bit)

If no Windows targets are available, ensure Windows Operating System disk is mounted.

Select the Folder containing your Windows driver files

Advanced options

☑ Don't match drivers for other system architectures (32-bit, 64-bit...).

☑ Match drivers by major Windows version (i.e. NT 6.x instead of 6.2, etc...).

□ Also scan the System32\DriverStore\FileRepository directory for drivers.

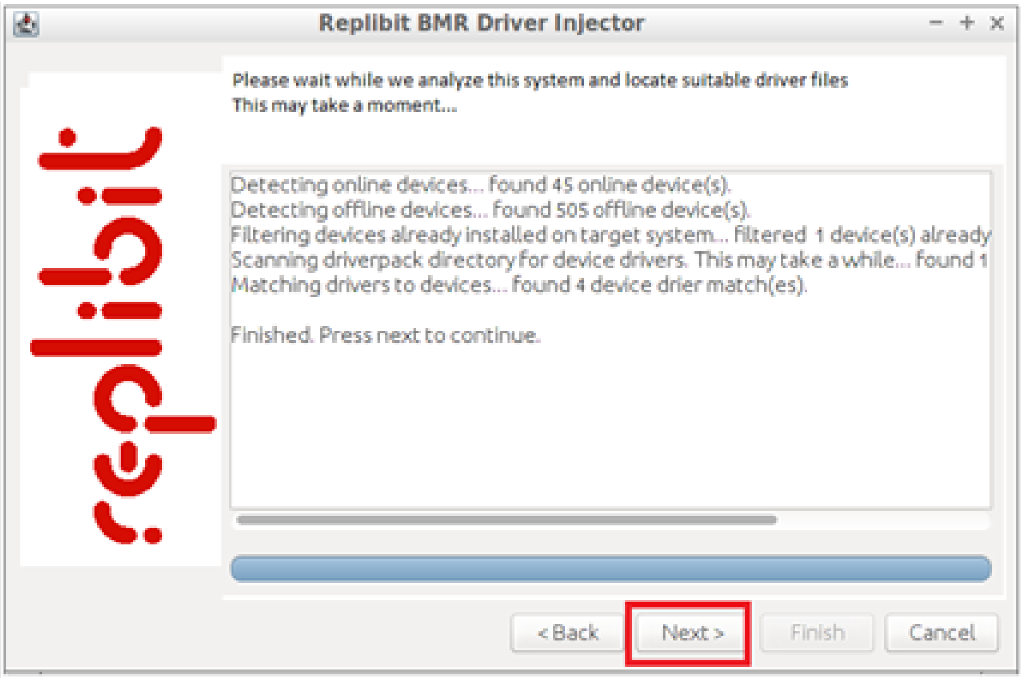
- The *Dropdown* selector **Offline Windows Operating System** should automatically discover the mounted system. If not, make sure the volume containing the C: drive is mounted and click **Refresh**.
- Click **Browse** and select the location containing the Windows drivers you would like to install. To use the basic set of Windows drivers that has been included on the Recovery ISO, select the **/root/Windows-Drivers.**
- If you would also like to scan the native Windows driver library on the recovered system, click to select **Also Scan the System32\DriverStore\FileRepository Directory for Drivers.**

You can leave all other settings at their default values.

Click **Next** to continue.

4. In the *Please wait while we analyze this system...* screen wait for the Driver Injector to read through the provided driver files. It will make matches against the hardware installed within the running system.

When the *Finished* message appears, click the **Next** button to continue.

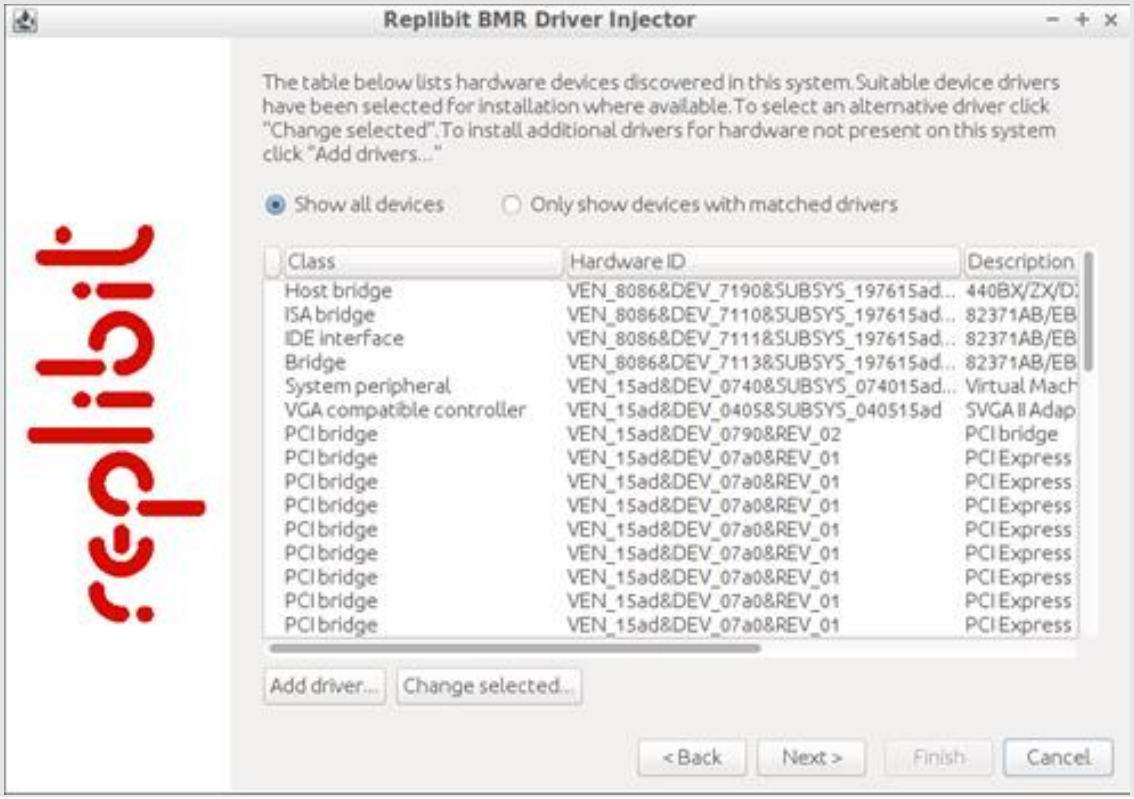


Please wait while we analyze this system and locate suitable driver files
This may take a moment...

```
Detecting online devices... found 45 online device(s).
Detecting offline devices... found 505 offline device(s).
Filtering devices already installed on target system... filtered 1 device(s) already
Scanning driverpack directory for device drivers. This may take a while... found 1
Matching drivers to devices... found 4 device drier match(es).

Finished. Press next to continue.
```

5. When the table of discovered devices appears, verify that the driver matches have been located for all critical hardware, such as storage controllers.

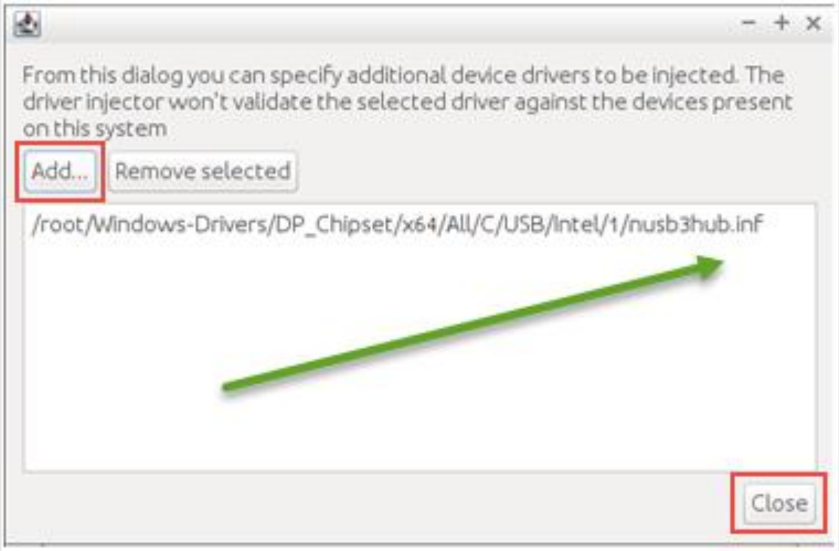


The table below lists hardware devices discovered in this system. Suitable device drivers have been selected for installation where available. To select an alternative driver click "Change selected". To install additional drivers for hardware not present on this system click "Add drivers..."

● Show all devices ○ Only show devices with matched drivers

Class	Hardware ID	Description
Host bridge	VEN_8086&DEV_7190&SUBSYS_197615ad...	440BX/ZX/D
ISA bridge	VEN_8086&DEV_7110&SUBSYS_197615ad...	82371AB/EB
IDE interface	VEN_8086&DEV_7111&SUBSYS_197615ad...	82371AB/EB
Bridge	VEN_8086&DEV_7113&SUBSYS_197615ad...	82371AB/EB
System peripheral	VEN_15ad&DEV_0740&SUBSYS_074015ad...	Virtual Mach
VGA compatible controller	VEN_15ad&DEV_0405&SUBSYS_040515ad	SVGA II Adap
PCI bridge	VEN_15ad&DEV_0790&REV_02	PCI bridge
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express
PCI bridge	VEN_15ad&DEV_07a0&REV_01	PCI Express

- To manually add specific drivers into the offline Windows installation, regardless of whether the hardware is physically present on the running system, click **Add Drivers**.
- From the *Add Drivers* dialog box, click **Add** and browse to the **.***inf* driver file you would like to add. Repeat as necessary to add additional drivers.



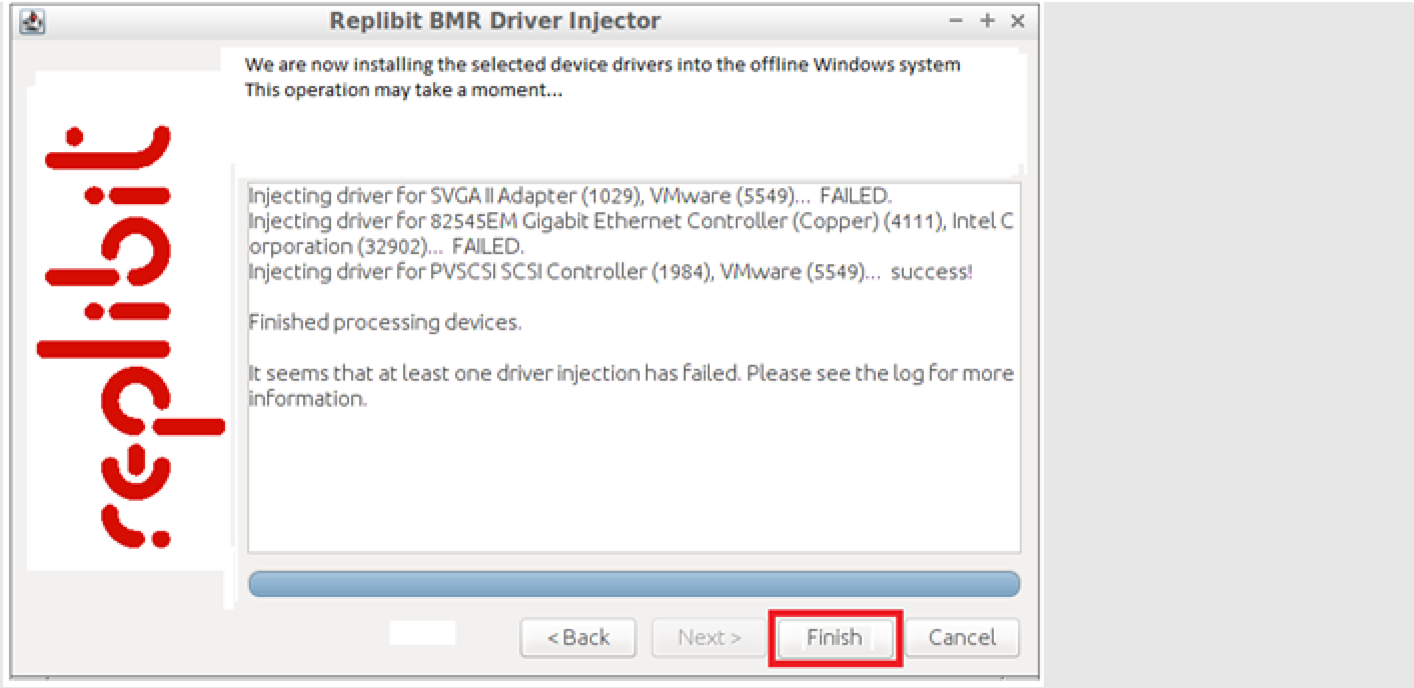
From this dialog you can specify additional device drivers to be injected. The driver injector won't validate the selected driver against the devices present on this system

/root/Windows-Drivers/DP_Chipset/x64/All/C/USB/Intel/1/nusb3hub.inf

Note: No validation is performed on the drivers being selected. Please ensure that you are selecting a *valid* Windows driver file for the correct operating system and architecture.

- When you are finished adding drivers, click the **Close** button.
- Click the **Next** button to continue.

6. The previously discovered and manually selected drivers will now be installed. Click **Finish** when the installation process has completed.



We are now installing the selected device drivers into the offline Windows system
This operation may take a moment...

```
Injecting driver for SVGA II Adapter (1029), VMware (5549)...  FAILED.
Injecting driver for 82545EM Gigabit Ethernet Controller (Copper) (4111), Intel C
orporation (32902)...  FAILED.
Injecting driver for PVSCSI SCSI Controller (1984), VMware (5549)...  success!

Finished processing devices.

It seems that at least one driver injection has failed. Please see the log for more
information.
```

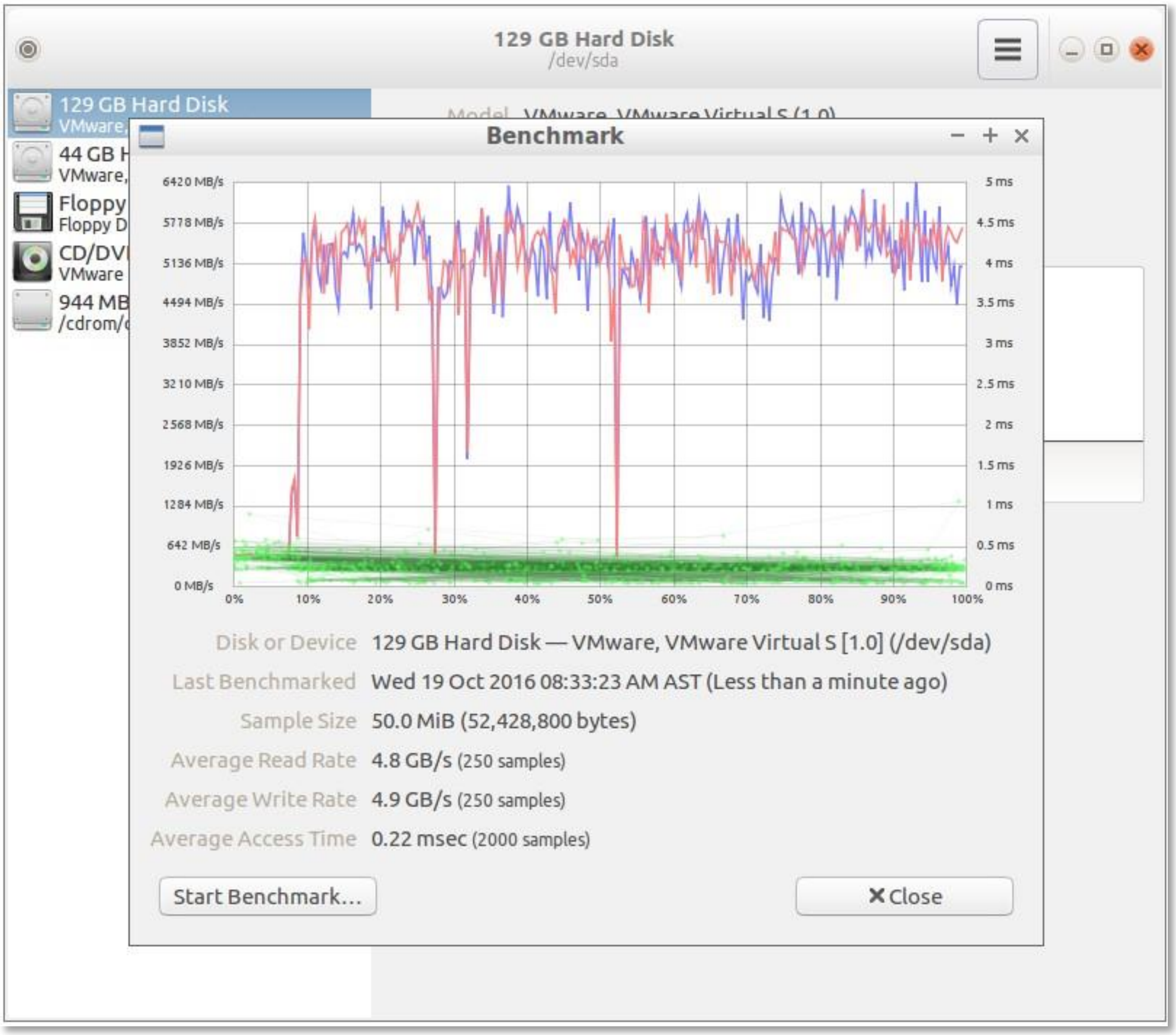
IMPORTANT NOTE:

After performing a full system recovery or virtualizing a system in Live Mode, x360Recover (Replibit) will automatically perform a new full backup at the next scheduled time, in order to synchronize the recovered system with the backup image. This full backup will only write changed data, but it is essential to ensure that the backup image remains in sync with the protected system.

Benchmark tests

Disk Performance

Basic disk benchmarking may be performed using Disk Manager.



129 GB Hard Disk
/dev/sda

Model VMware, VMware Virtual S (1.0)

Benchmark

Disk or Device 129 GB Hard Disk — VMware, VMware Virtual S [1.0] (/dev/sda)
Last Benchmarked Wed 19 Oct 2016 08:33:23 AM AST (Less than a minute ago)
Sample Size 50.0 MiB (52,428,800 bytes)
Average Read Rate 4.8 GB/s (250 samples)
Average Write Rate 4.9 GB/s (250 samples)
Average Access Time 0.22 msec (2000 samples)

1. Launch Disk Manager from the desktop or from the *Recovery Tools* folder on the Launcher menu. Select the drive you wish to test from the Devices panel.

2. Click the Menu button in the top right corner and select Benchmark Disk.

3. Select the Start Benchmark button at the bottom of the window.

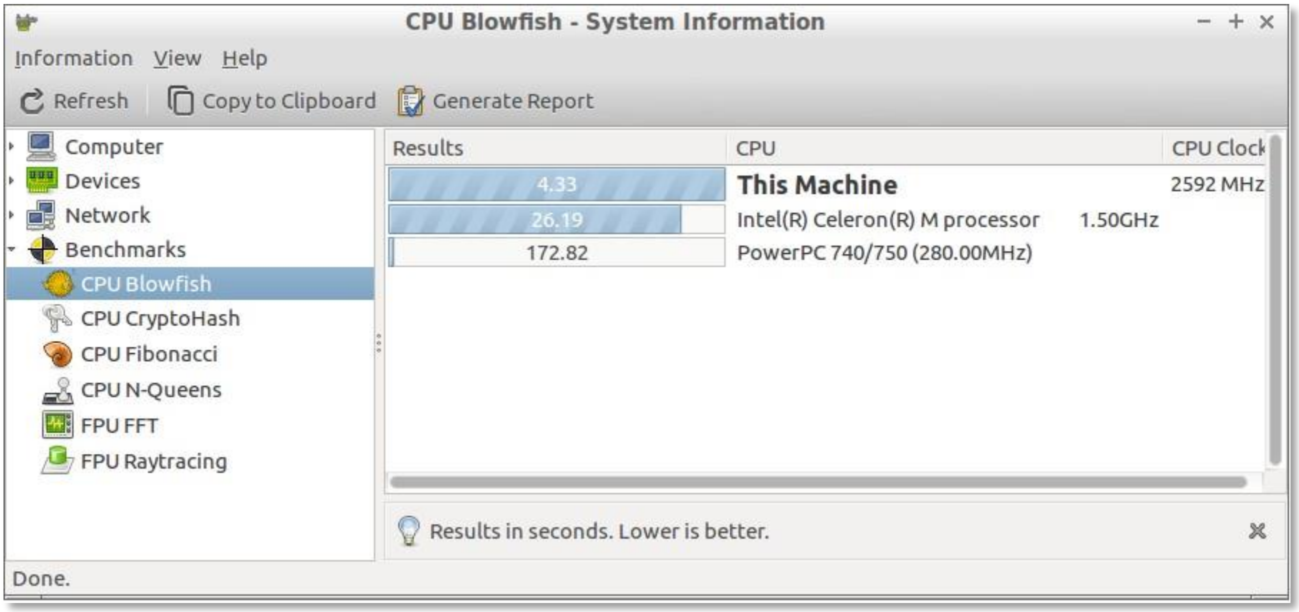
4. Enter your desired values for number of samples, and sample size, or take the defaults.

5. Click on Start Benchmarking to begin the testing process. Read and write performance are graphed in blue and red respectively. Access (seek) time is graphed in green.

CPU Performance

Several different types of CPU benchmark tests are available within the Hardware Info utility.

- Launch Hardware Info from the *Utilities* folder of the Launcher menu.
- In the left pane, collapse the Computer, Devices, and Network sections.
- Within the Benchmarks section, click on a performance test to run that test immediately. The results panel displays a graph comparing this computer to a set of known benchmarks.



Results	CPU	CPU Clock
4.33	**This Machine**	2592 MHz
26.19	Intel(R) Celeron(R) M processor 1.50GHz	
172.82	PowerPC 740/750 (280.00MHz)	

Results in seconds. Lower is better.

Done.

Burn-in Testing

The process of performing a burn-in test involves applying stress for a period of time on a new computer system, in order to try to ensure that there are no faulty components within the system. Forcing the computer to operate under high CPU, memory, and disk IO load operations for an extended period of time can act as a quality control test of the system before delivering it to the customer. Typically, a burn-in test will be run over a period of 6-12 hours.

To perform burn-in testing:

- Run QTerminal from the *System Tools* folder on the Launcher menu.
- From the shell, run *sudo stress-ng* and specify how many threads of each type of load you wish to run.

For example: sudo stress --cpu 4 --io 2 --vm 2--hdd 4 --timeout 6h

Note: *stress* performs hard drive IO testing by writing to the current directory. Ensure the current directory is writable and located on the physical disk you wish to test.

To test a specific hard drive volume, first mount it with Disk Manager, and then change directory to /media/axcient/<Name>, where <Name> is the volume label or ID, before running *stress*.

Advanced Recovery Options

Manually Recreate the UEFI Boot Partition

UEFI systems that were backed up prior to UEFI supported agents, or systems with corrupted UEFI partitions will not be able to boot after using the Recovery Wizard.

The following manual procedure may be used to repair the UEFI boot partitions of these systems:

1. Boot from a Windows Operating System disk or ISO.
   Be sure the system is configured to boot using UEFI mode, not Legacy BIOS mode
2. Click OK or Next on the language selection page, and then select the Repair option on the next screen.
3. Select Troubleshoot and choose Command Prompt to open a recovery shell.
4. Prepare the Destination disk for UEFI
   a. From a CMD prompt run *DISKPART*
   b. Enter *Select Disk x* (where x is the drive number of the target recovery C: disk)
      Note: Use *List Disk* to display a list of attached disk drives
   c. *Select Partition x* (where x is the system partition)
      Use *list partition* to see the list of partitions and identify system

   d. *Delete Partition*
   e. *Create Partition efi*
   f. *Select Partition x* (where x is the System partition)
   g. *Format Quick FS=fat32*
   h. *Assign*
   i. *List volume* (Note the drive letter assignments)
   j. Exit
5. Copy the Windows EFI boot files
   a. Locate the drive letter containing the Windows folder by changing drives and Dir (i.e. enter D:<enter> to change to the D: drive and then *Dir* to list disk contents) Note: You may need to inject a storage controller driver if it is not native on the Windows Operating System disk. See Manual Driver Injection in the next section.
   b. *Mkdir <drv:>\EFI* (where <Drv:> is the drive letter assigned to the System partition)
   c. *Xcopy <winDrv:>\Windows\Boot\EFI <sysDrv:>\EFI* (Where winDrv is the drive containing the Windows folder, and sysDrv is the drive assigned to the System partition)
6. Recreate the Windows BCD boot records and EFI System files
   a. From the CMD prompt and run the following commands
   b. *Bootrec /FixBoot*
   c. *Bootrec /RebuildBCD* (Enter 'Y' when prompted)
   d. *Bcdboot x*:*windows* (Replace 'x' with the Destination drive letter containing the

Windows folder)

7. Remove the Windows Operating System disk and reboot the system in UEFI mode

Manual Driver Injection for Windows Server 2008 R2 or newer

When restoring your system to different hardware, it is likely that the original operating system may not have all the drivers necessary to boot normally after performing the recovery. The following procedure will walk you through manually installing critical device drivers to enable the system to boot on the new hardware.

Note: Use this procedure only if the Replibit Driver Injector utility fails to install your drivers.

1. Start by locating the necessary critical drivers for the new hardware (such as storage and network controllers).

2. Copy the installation files to a USB stick.

3. Make a folder named Drivers and copy each set of driver files into its own folder inside the Drivers folder. Note: Copy only the files for the correct architecture for your operating system. (Copy x86 or x64 files, not both.)

4. Boot the system from a Windows operating system installation disk.

5. Click OK or Next on the language selection page, and then select the Repair option on the next screen.

6. Select Troubleshoot and choose Command Prompt to open a recovery shell.

7. Connect your USB disk to the system.

8. Using DOS commands, switch drives and perform a DIR command, starting from C: and moving upwards until you have identified which drive letter contains your USB stick Drivers folder, and which drive contains the Windows folder. (For example, type C: and press enter, then type DIR and hit enter to list the drive contents.) DOS will inform you if the given drive letter does not exist.

9. If you cannot find the Windows folder on any drive, it means that the Windows Installer media does not have a driver for your storage controller. Switch drives for the USB stick and change directory into the folder containing the storage controller drivers. Run DIR to list the files and identify the *driver*.inf file name. To load the driver into the running system, type *drvload.exe <driver.inf>* where driver.inf is the file you just identified. Repeat the drive switching process above and locate the drive letter that contains the Windows folder.

10. To install the drivers into your recovered system, run the following command:
    DISM /Image:<ImagePath> /Add-Driver /Driver:<DriverPath> /Recurse
    a. Replace <ImagePath> with the drive leter containing the Windows folder
    b. Replace <DriverPath> with the path to the Drivers folder

    Example: DISM /Image:E:\ /Add-Driver /Driver:C:\Drivers /Recurse

11. If successful, DISM will display a message advising that the drivers have been installed. Remove the Windows operating system disc and power cycle the system. Verify that the system boots normally.

Manual Partition Recovery

In some cases, it may be necessary to perform a manual, partition-by-partition recovery operation to restore a system to working order. For example, if the original source disk contains multiple Windows volumes, and you must restore the original topology when recovering the system, you can use a manual copy process to recover the data, one partition at a time. (The x360Recover Recovery Wizard recovers each protected Windows volume to its own dedicated disk.)

The following is an example of how to use Manual Partition Recovery to restore a system where the original Disk 0 drive contains multiple Windows volumes:

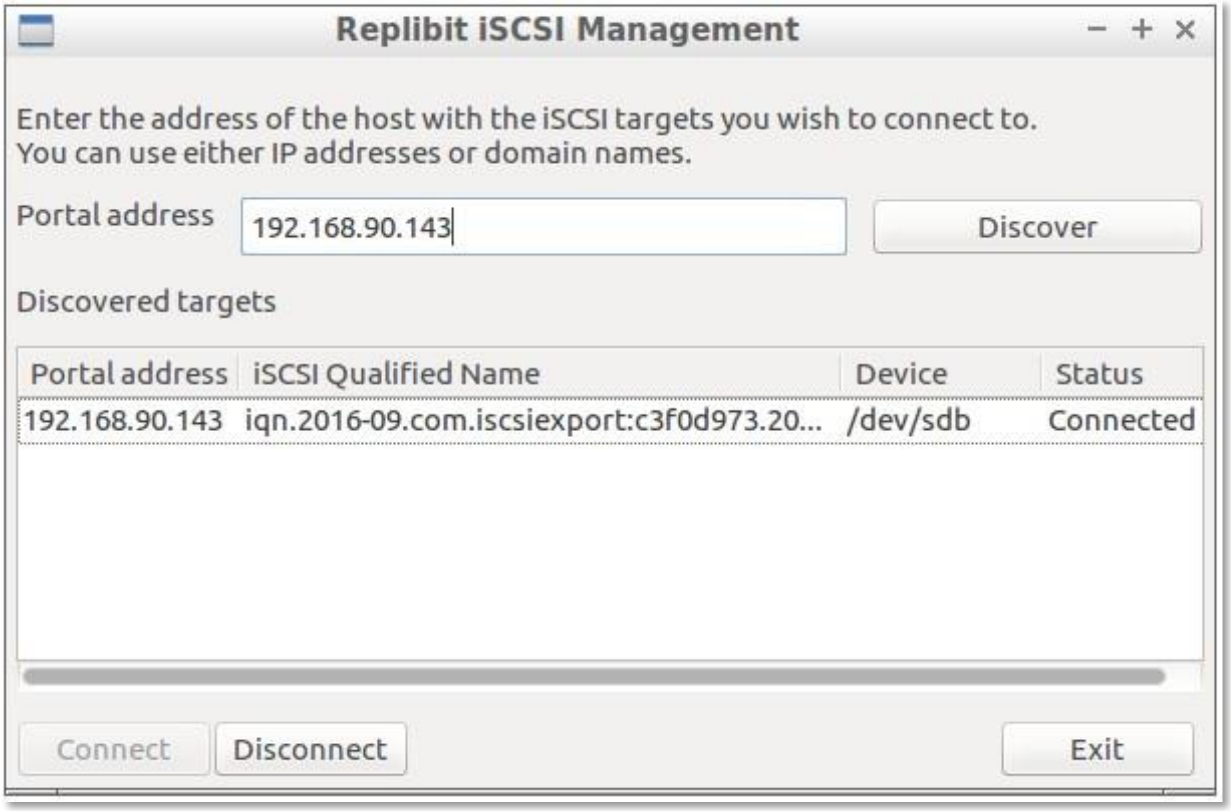
1. Start by exporting the protected system via iSCSI Start. From the Replibit Web GUI, select the protected system details page. Locate the desired snapshot and select iSCSI Start. If you are recovering a system that has been running in Live Mode as a virtual machine on the Appliance, then select Live Mode when starting iSCSI. Otherwise, choose Test Mode.

2. Boot your new system from the x360Recover Recovery Toolkit.

3. When the desktop loads, launch iSCSI Manager from the *Recovery Tools* folder of the Launcher menu.

4. Enter the IP address of your Appliance and click Discover.

5. Select the disk target(s) containing the Windows volume(s) you wish to recover and click on Connect to attach them to the recovery tools environment.



Replibit iSCSI Management

Enter the address of the host with the iSCSI targets you wish to connect to.
You can use either IP addresses or domain names.

Portal address: 192.168.90.143

Discovered targets

Portal address	iSCSI Qualified Name	Device	Status
192.168.90.143	iqn.2016-09.com.iscsiexport:c3f0d973.20...	/dev/sdb	Connected

6. Launch Disk Manager and examine your attached disk devices. Identify the device path for the local disk you intend to restore the C: volume onto, as well as the device path of the original C: volume you mounted via iSCSI Manager.

7. a.) Launch QTerminal from the *System Tools* folder of the Launcher menu.

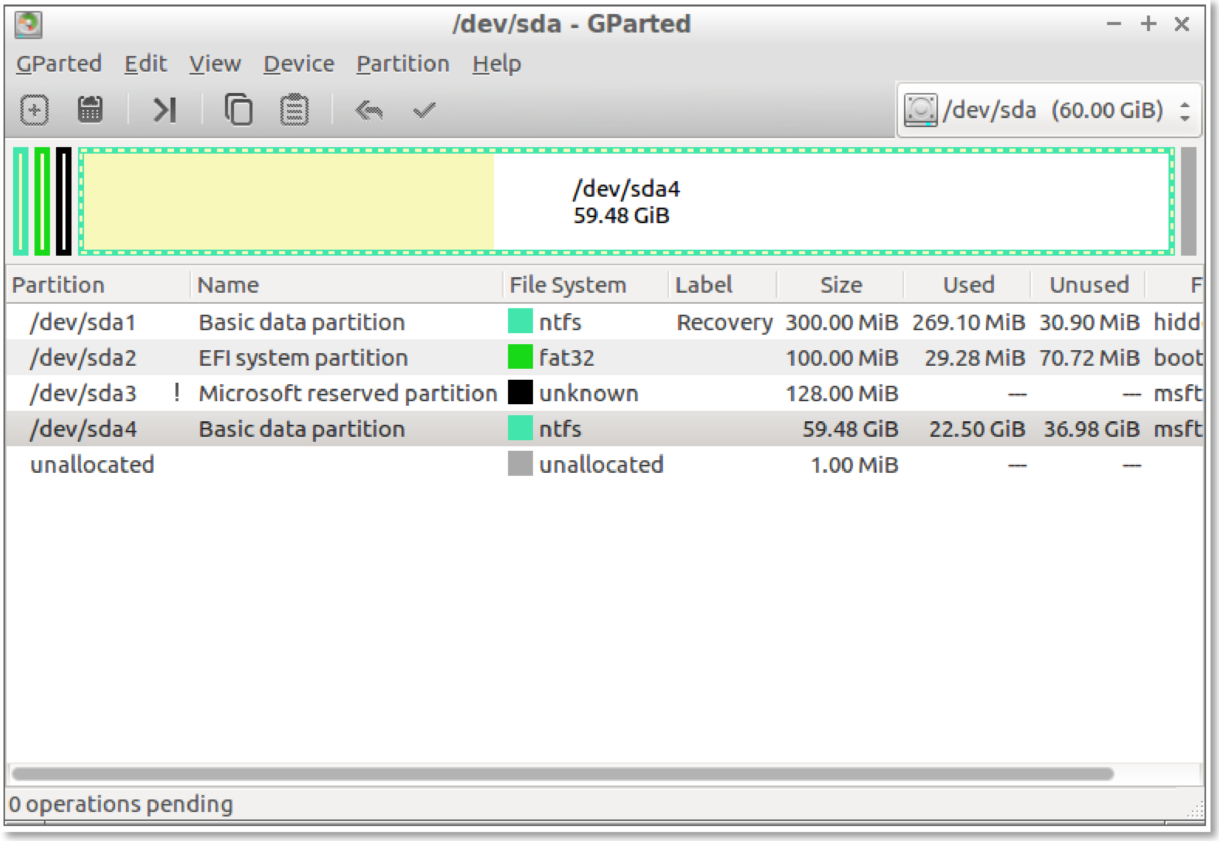
b.) Within the shell terminal, elevate to the root user by running *sudo su.*

c.) Clone the partition table and disk identity onto the new system by running the following command:

```
dd if=<source disk device> of=<destination disk device> bs=1024 count=1024.
```

For example, if your original protected system is /dev/sdb and your new local disk is /dev/sda then you would run dd if=/dev/sdb /of=/dev/sda bs=1024 count=1024

11. Launch GParted from the shortcut on the desktop.



Partition		Name	File System	Label	Size	Used	Unused	F
/dev/sda1		Basic data partition	🟩 ntfs	Recovery	300.00 MiB	269.10 MiB	30.90 MiB	hidd
/dev/sda2		EFI system partition	🟩 fat32		100.00 MiB	29.28 MiB	70.72 MiB	boot
/dev/sda3	!	Microsoft reserved partition	■ unknown		128.00 MiB	—	—	msft
/dev/sda4		Basic data partition	🟩 ntfs		59.48 GiB	22.50 GiB	36.98 GiB	msft
unallocated			▨ unallocated		1.00 MiB	—	—	

0 operations pending

Note:

If a message appears during launch stating that not all available space is in use, click Fix.
For each partition from the original C: drive:

- Select the source disk device from the drop-down choices in the top right corner
- Right-click on the partition and select copy
- Select the destination disk from the drop-down selector

- Right-click the appropriate partition
- Click Paste
- Click OK when the warning on overwriting an existing partition appears.

For additional volumes, repeat the steps above to copy each partition onto the destination disk. Select unallocated space on the destination disk and a new partition will be created. Once all partitions have been selected, click the Check button from the top tool bar to perform the selected actions.

12. When all operations have completed, reboot to verify that the system will boot normally.

Repair a Damaged Boot Record (Server 2008 R2 or Newer)

If your recovered system does not boot (or a Blue-Screen error message appears on startup), it may be necessary to recreate the Windows boot records on the hard drive.

- Boot the system from a Windows operating system disc.

- Click Next on the language selection page, and then choose the Repair option.

- Select Troubleshooting and then select Command Prompt.

- From the command shell, switch disks and locate the recovery partition (if it exists.) This will likely be on C:. The recovery partition will most likely appear to be empty, but verify that you can change directory into the hidden folder named BOOT. Within BOOT, rename the existing BCD file.

  For example: *move BCD BCD.old*

- Run the following commands to replace the boot records
  - bootrec /fixmbr (Only for systems using legacy MBR BIOS, not UEFI systems)
  - bootrec /fixboot
  - bootrec /RebuildBcd

- Select Yes when prompted for Windows instances to install

- Reboot and verify that the system boots normally

Troubleshooting

Below are some possible issues you might encounter while using the Recovery Toolkit, and our recommend work-arounds or fixes.

- For support from our excellent team of engineers, visit http://www.efolder.net/support.
- Click on Start Support Session to create a new ticket. This is the fastest way to receive a call back from the eFolder Replibit engineering team.
- You may also browse our Knowledgebase for answers to commonly encountered issues.

NTFS Disk Will Not Mount with Disk Manager

You may receive an error within Disk Manager stating that an NTFS volume cannot be mounted because it was not shut down in a clean state. To resolve this issue, a disk check must be performed on the volume.

- Open QTerminal from the System Tools folder on the Launcher menu.
- Run *sudo su* to elevate to the *root* user.
- Identify the device name, like /dev/sda1 (See the bottom pane of DiskManager above)
- Run *ntfsfix <device>* from the shell window. (i.e. *ntfsfix /dev/sda1*)
- Once the partition has been repaired, mount it with Disk Manager by selecting the Volume, and then clicking on Mount from the Actions menu pane.

Once the repair has completed, close QTerminal and try mounting the volume with Disk Manager again.

If this fails, launch QTerminal and elevate to root by running *sudo su.* Run ntfsfix <device> to repair the filesystem. (i.e., ntfsfix /dev/sda1)

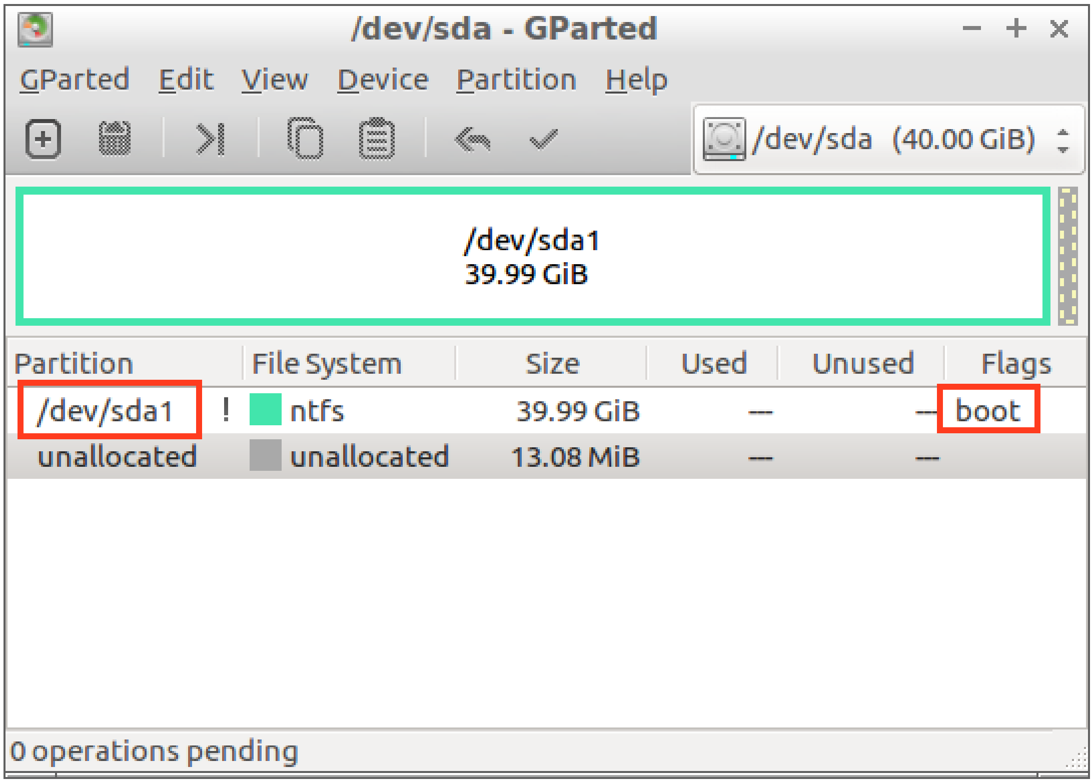
Windows Server 2003 does not boot after recovery

You may receive an error message such as Error Loading Operating System, after recovering a system running Windows Server 2003.

To resolve this issue, boot the system from the Recovery Toolkit again and perform the following steps to repair the NTFS filesystem:

- Open GParted and identify which disk partition has the Boot flag set.

(This is likely to be /dev/sda1, for example.)



Partition		File System	Size	Used	Unused	Flags
/dev/sda1	!	🟩 ntfs	39.99 GiB	—	—	boot
unallocated		▨ unallocated	13.08 MiB	—	—	

0 operations pending

- Open QTerminal from the *System Tools* folder on the Launcher menu.
- Run *sudo su* to elevate your permissions to root.
- Run *ntfsfix <device path>* to perform a file system check and fix any errors discovered. (For example, *ntfsfix /dev/sda1*)