NSS Volume Data Recovery

Preliminary Document

September 8, 2010

Version 1.0

The Portlock storage management software described in this document is furnished under a License Agreement and may be used only in accordance with the terms of the agreement.

Version: 1.0

Date of Publication: September, 2010

NO WARRANTY. The technical documentation is being delivered to you AS IS and Portlock makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical errors, typographical errors or other inaccuracies. Portlock reserves the right to make changes without prior notice.

Table of Contents

Chapter 1. Introduction to NetWare Data Recovery

Notice

It is not the intention of our products to circumvent company policy. There are legitimate cases where companies can no longer access data that they own. Portlock does not endorse or support accessing data that you do not have the rights to access.

Overview

NetWare NSS Volumes are an advanced file system similar to NTFS or ReiserFS. The NSS file system consists of metadata and file data. The metadata is normally organized into a B+Tree (Binary Tree) and manages file system structures such as the:

- Free Block Tree
- Name Tree
- Object Tree (Novell calls this the Beast Tree)
- File Salvage Tree
- MFL Tree (Modified File List)
- File Purge Log
- User Tree
- Journal (this is not a B+Tree)

The file data consists of blocks of data representing files. The file data block list is managed by the Object Tree.

The size of a block of data on NSS volumes is 4 KB. This size was primarily chosen to match the virtual memory paging system on Intel processors.

There are two primary methods to recover data from a corrupted NSS volume. The first is to use the Name Tree to locate each file and directory on the volume. The Name Tree provides the Zid of the object for location in the Object Tree. The second is to use the Object Tree directly to recover files with or without the directory structure (e.g. you can recover a file without knowing the directory that the file is part of).

The Name Tree is a B+Tree of object names within the file system. These names primarily represent files and directories but also represent other objects such as Pools, Volumes, etc. The Name Tree is redundant as all information in the Name Tree is also located in the Object Tree. However, the Name Tree provides a very fast sorted lookup of objects based upon its name. An object name has multiple representations based upon the name space of the object name. For example the MAC name space has different naming rules compared to the Windows name space. Therefore an object can have multiple entries in the Name Tree, one for each name space where the object name is different.

FYI: When rebuilding an NSS volume or NSS pool using Novell's volume or pool rebuild command, the Name Tree is discarded and recreated from the Object Tree. This is the reason that pool rebuilds in old

versions of NSS would lose files. The issue was bugs in real-time synchronization of names in the Name Tree and Object Tree. However, these issues no longer exist based upon our experience with NSS.

The Object Tree is a B+Tree of objects within the file system. The order of objects is based upon the object ID (Novell calls this a Zid). The Object Tree is also a linked list of blocks and this feature can assist in recovering files where the B+Tree has been corrupted. However, if a block within this linked list becomes corrupted, then recovery stops at this block as the pointer to the next block is gone. In this case a combination of using the Name Tree and the Object Tree can maximize data recovery.

Two Portlock programs support recovering data from NSS Volumes (corrupted or not). The first is Portlock Storage Manager and the second is Portlock Drive Explorer.

Portlock Storage Manager is a large product supporting a vast number of features for managing NetWare storage and file systems. There are a number of features for recovery and repairing NetWare partitions and file systems.

Portlock Drive Explorer is similar to Windows Explorer but also supports NetWare file systems including NetWare Traditional volumes, NetWare 5.x NSS volumes and NetWare 6.x Pools and Volumes. If the file system structure is not severely corrupted, Portlock Drive Explorer can copy files and directories from a Netware volume to another location such as:

- An external attached device such as a USB disk drive.
- Network share mapped as a drive letter.

Data Recovery Cost

Considerations

There are a number of cost factors to consider when there is data loss:

- What is the cost to recreate the data.
- What is the cost to restore from backup and then recreate the newest data.
- What is the employee cost in lost productivity.
- What is the employee cost in self-recovery using software.
- What is the cost to employ an expert to recover the data.

Software

Software written to access and recover data is the least expensive method. There are several companies that write software to recover data on Novell NetWare servers. Portlock does recommend any company and we have not used any other company's products except for our own. Note: Portlock often refers customers to Ontrack.

- Portlock Storage Manager. Cost $495.00
- Stellar Phoenix Novell Data Recovery. Cost $399.00
- Nucleus Data Recovery. Cost $199.00
- Ontrack Data Recovery for NetWare. Cost $495.00

Consulting

This is moderately expensive but is usually the best solution as data for most companies is more valuable than the cost to recover. Advice: do not shop based upon price as true experts in data recovery are very expensive for companies to employ. Typically an engineer that can analyze the bits and bytes of a file system on disk are the very best software developers in the world. Expect to pay between $250.00 to $1,000.00 per hour for the consultant's time with no guarantees of success except where you pay for the consultant to analyze the data first. Typical data recovery time for NetWare NSS based upon our experience is four hours based upon thousands of data recoveries. However, there are many cases where we worked 24x7 for three weeks.

Hardware Recovery

Data recoveries requiring hardware based recoveries are usually the most expensive. This includes RAID-5 failures to directly accessing a disk drive's media platters. Recovery starts at $10,000 and goes up quickly. The hardware required for this level of data recovery is very expensive and often requires clean room environments.

Data Recovery Success

A common question is "will my data be recovered?" The answer depends on what caused the data loss or file system corruption.

Lost Credentials

In this case there is no data corruption, only the loss of access rights to data. The quickest solution is to use Portlock Drive Explorer to copy the entire volume to another location that you can access.

Note: It is not the intention of our products to circumvent company policy. There are legitimate cases where companies can no longer access data that they own. Portlock does not endorse or support accessing data that you do not have the rights to access.

Corrupted RAID Array

No Portlock products can handle this problem.

This has to be one of the worst cases. When RAID is used to protect data, failure of the array generally means significant data loss or corruption. For example, you have a RAID-5 array using a stripe size of 64 KB, with five drives in the array. The loss of parity across the drives will result in one block out of four being missing. If a file is striped across the faulty stripe, you have data loss within the file. Plan carefully when restriping the array (failed drive recovery) as a failure during the rebuild will render all data corrupted. You are advised to consult an expert on RAID disk array recovery.

Device Failure

No Portlock products can handle this problem.

If a storage device fails and is no longer accessible to the operating system or firmware, then you will need to contact a company that specializes in repairing the drive or recovering data from the media platters. This can be very expensive.

Defective disk sectors

This can either be a very simple problem or a massive problem depending on what part of the file system is stored on the defective sectors and how many sectors are defective. In most cases due to the high percentage of file data compared to meta data, the data loss is localized to individual files.

Logical File System Corruption

When the file system meta data becomes corrupted, the extent of the corruption depends on what is corrupted. For example, the corruption of the Name Tree is not serious as all of the data in the Name Tree is replicated in the Object Tree. However, if the Object Tree is corrupted then data loss can be extensive. Corruption of other meta data objects such as the Journal or the Salvage Tree may prevent the volume from mounting but file recovery will be easy with probably no data loss.

Summary

Without actually having an engineer analyze a particular situation, there is no way to determine success or failure of a data recovery. The answer really depends on the type of data corruption and how much time and resources can be allocated to the data recovery.

The best step to minimize the impact of data loss or corruption is:

- Have a good backup and restore plan in place. Verify that you can restore from your backups.
- Schedule and implement periodic system maintenance. This includes downing servers, checking file systems, purging unneeded data, installing service packs and hot fixes, etc.
- Schedule hardware replacements. A ten year old system is more likely to fail then a one year old system. Most companies recycle systems on a 24, 30 or 36 month cycle.
- Once you notice data corruption, STOP and create a plan to recover or restore the data. Do not try ad-hoc methods of recovering data as this often change a simple problem into a disaster.
- Duplicate the data or storage device to another device and attempt data recovery from the copy. In the event of very large data sets, make several copies and work on different recovery techniques in parallel. For example if a volume is 4 TB in size and software can process 25 MB of data per second one pass will take approximately 44 hours.

Chapter 2. Using Portlock Storage Manager to Recover an NSS Volume

Overview

1. Boot the server with the Portlock Boot CD
2. Map a network share to a drive letter
3. Launch Portlock Storage Manager
4. Select the volume to be recovered
5. Review the recovered data

Step 1: Boot the server with the Portlock Boot CD

Using Portlock License Manager, download the latest version of the Portlock Boot CD. Then "inject" your Portlock Storage Manager license into the ISO image. Burn the ISO image to optical media (CD-R, DVD-R, etc.). Insert the media into your server and reboot. Once the Portlock Boot CD boots a system you will have screen similar to this one:

Step 2: Map a network share to a drive letter

Portlock Storage Manager requires a location to write the recovered files. Ensure that the selected location has enough free space to hold all of the files on the volume (both normal files and files that have been deleted but not yet purged).

Portlock Storage Manager also supports external USB drives, but this method will use a Windows drive letter mapped to a Windows workstation or server.

Note: The location selected should be formatted with NTFS and not FAT32 if you have files larger than 2 GB on the volume being recovered.

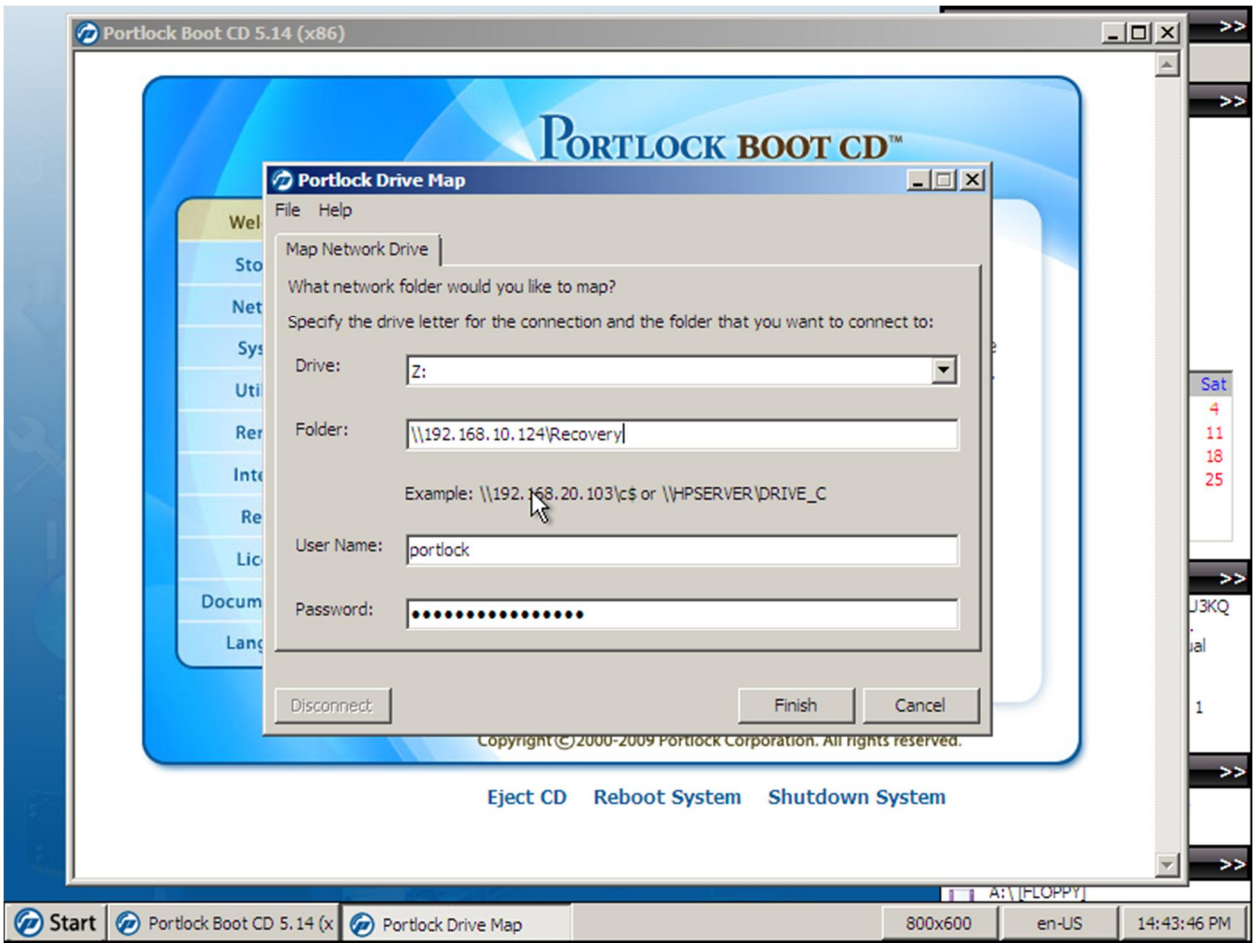
From a Windows desktop or server

1. Select a drive that has enough free space for the recovery.
2. Create a directory on a Windows system (example “Recovery”).
3. Using Windows Explorer right-click on the directory selecting “Sharing and Security” (XP), “Share” (Vista) or “Share with” (Windows 7). This step is different on different versions of Windows.
4. Configure the share so that a client has write permission to the folder. This Windows share will be mapped as drive letter on the Portlock Boot CD. You will need your username and password for the Portlock Boot CD.

From the Portlock Boot CD

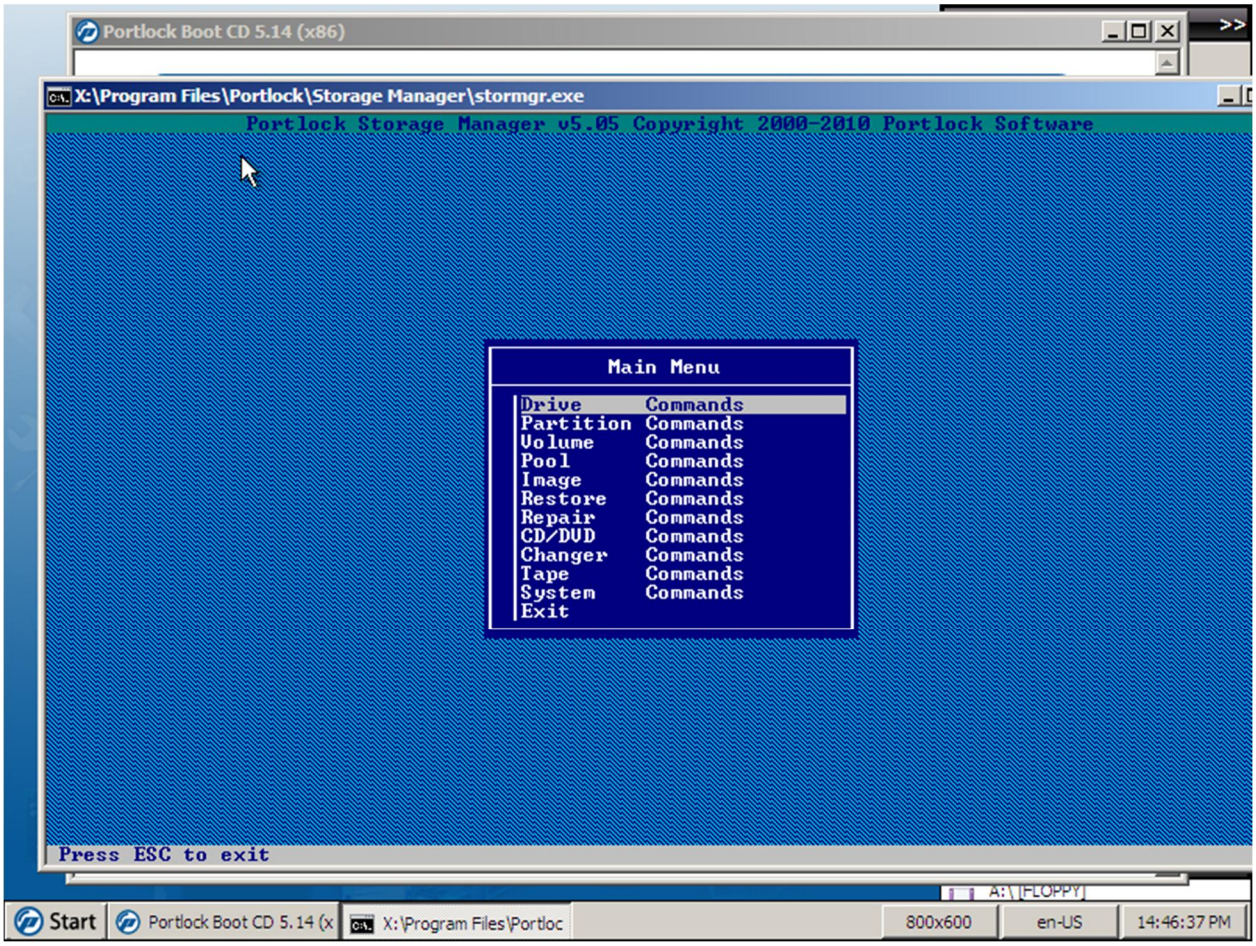
Referencing the Portlock Boot CD screenshot above find the icon for “Drive Map”. Click on “Drive Map” to launch the program. Portlock Drive Map is a program that maps Windows shares to local drive letters. In this example the folder that we shared from the system “192.168.10.124” is “Recovery”. Click Finish to complete the drive mapping. Then click Cancel to close the program.

Once you have started Portlock Drive Map you will have a screen similar to the following.



Step 3: Launch Portlock Storage Manager

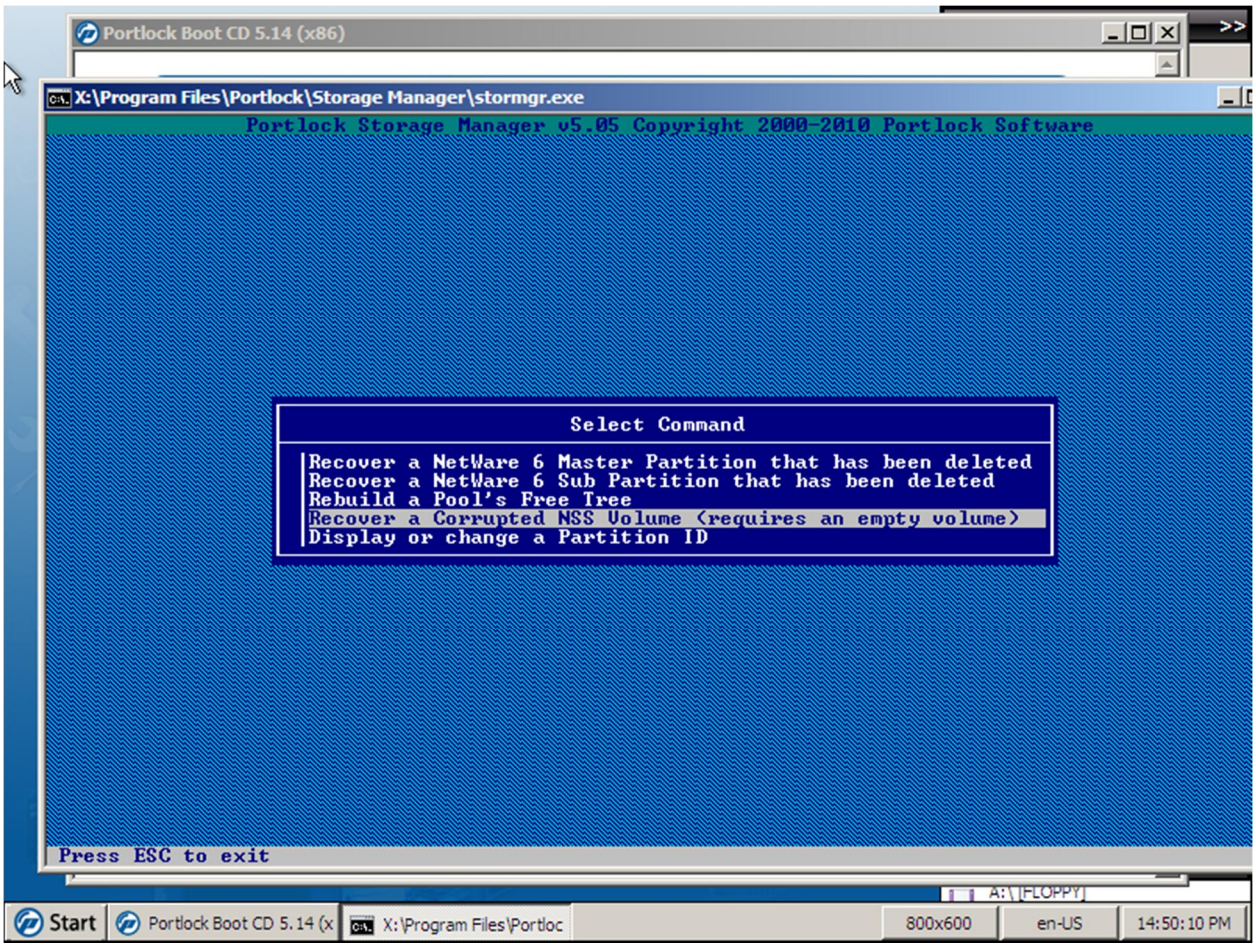
In the Portlock Boot CD screenshot above, click on “Storage Manager” to start Portlock Storage Manager. Accept each of the introductory screens until you reach the “Main Menu”.



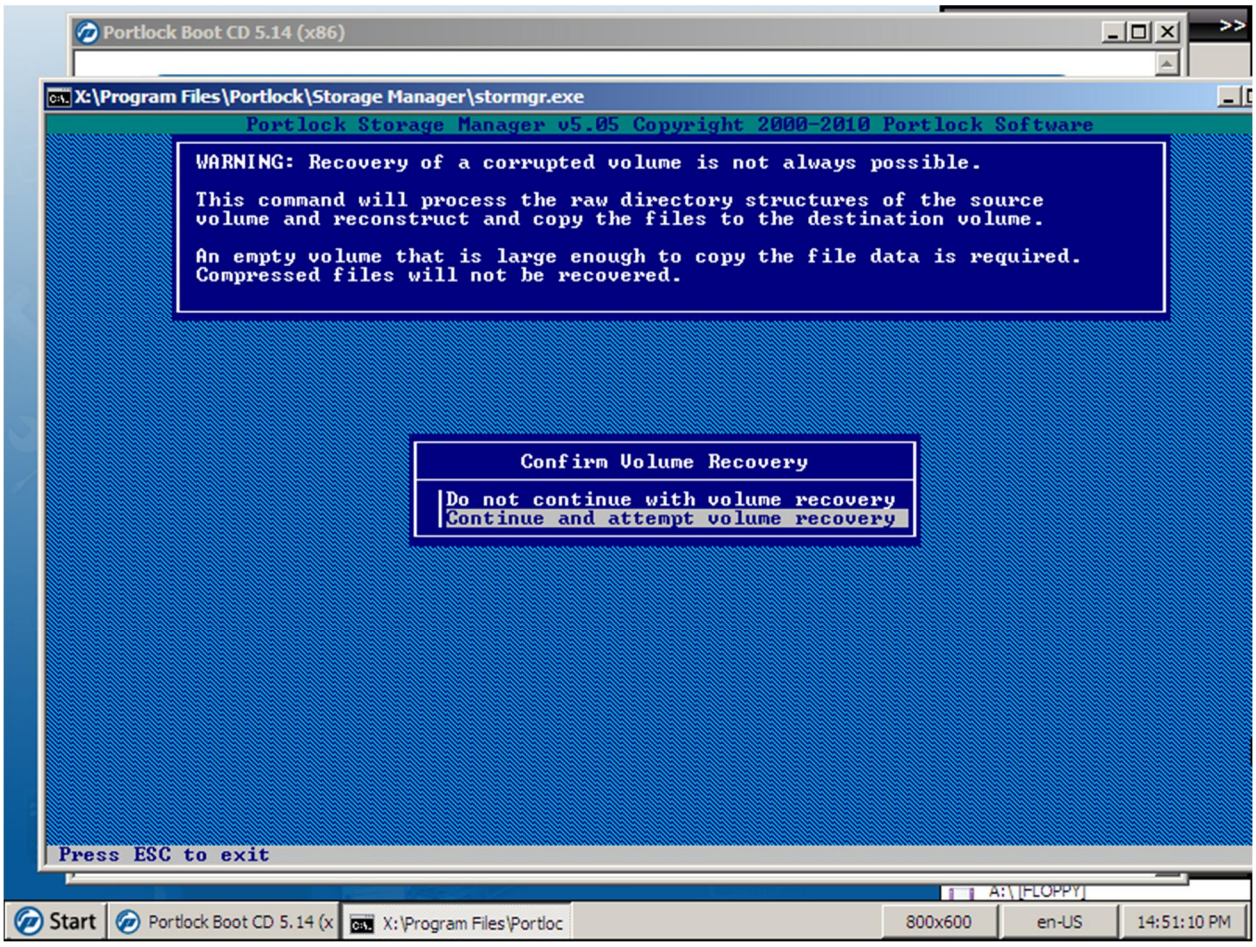
Step 4: Select the volume to be recovered

To get to the NSS volume recover command step thru the following menu commands using the up and down arrow keys and then ENTER.

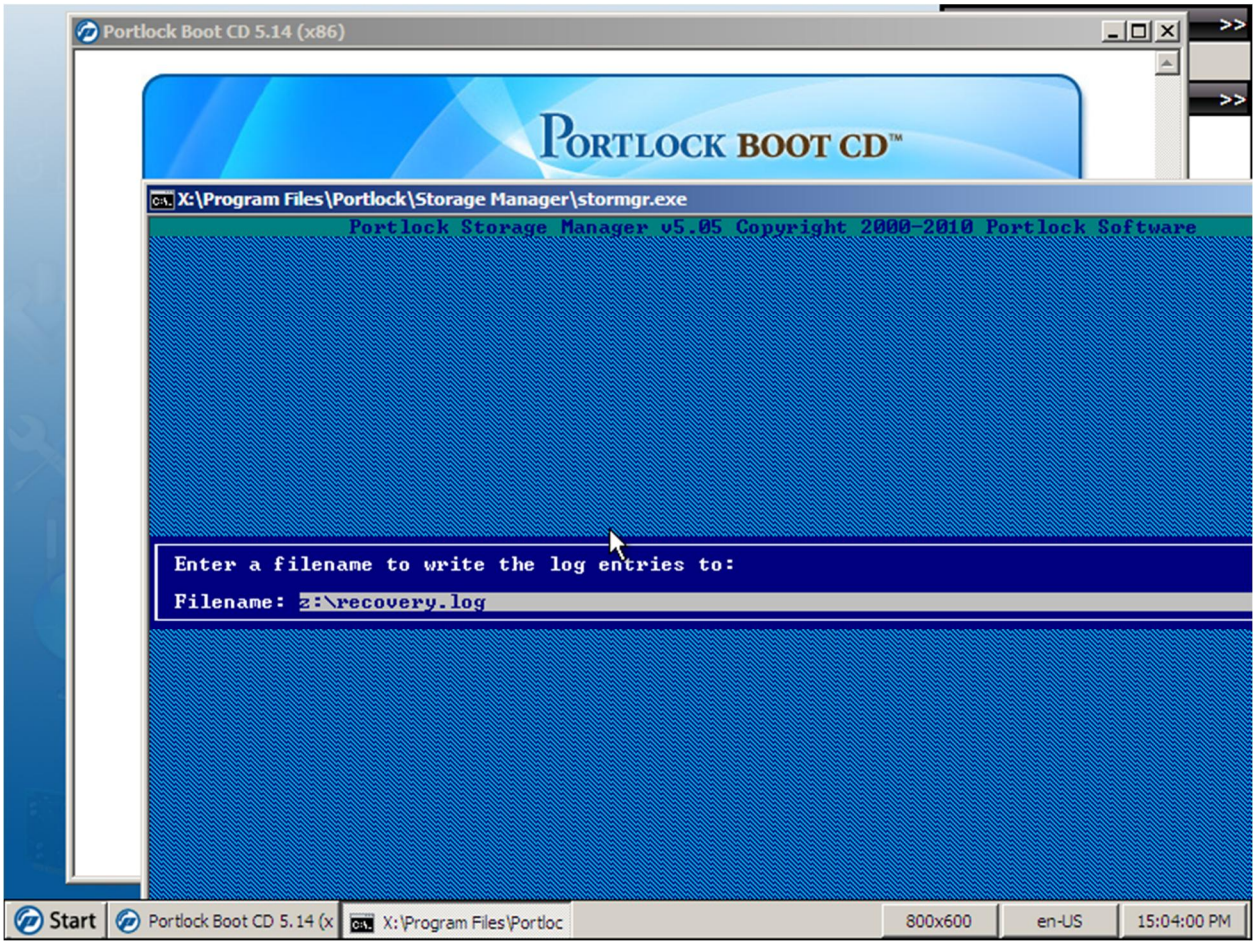
Select “Repair Commands” -> “Netware NSS partition and volume recovery commands” -> “Recover a Corrupted NSS Volume (requires an empty volume)”.



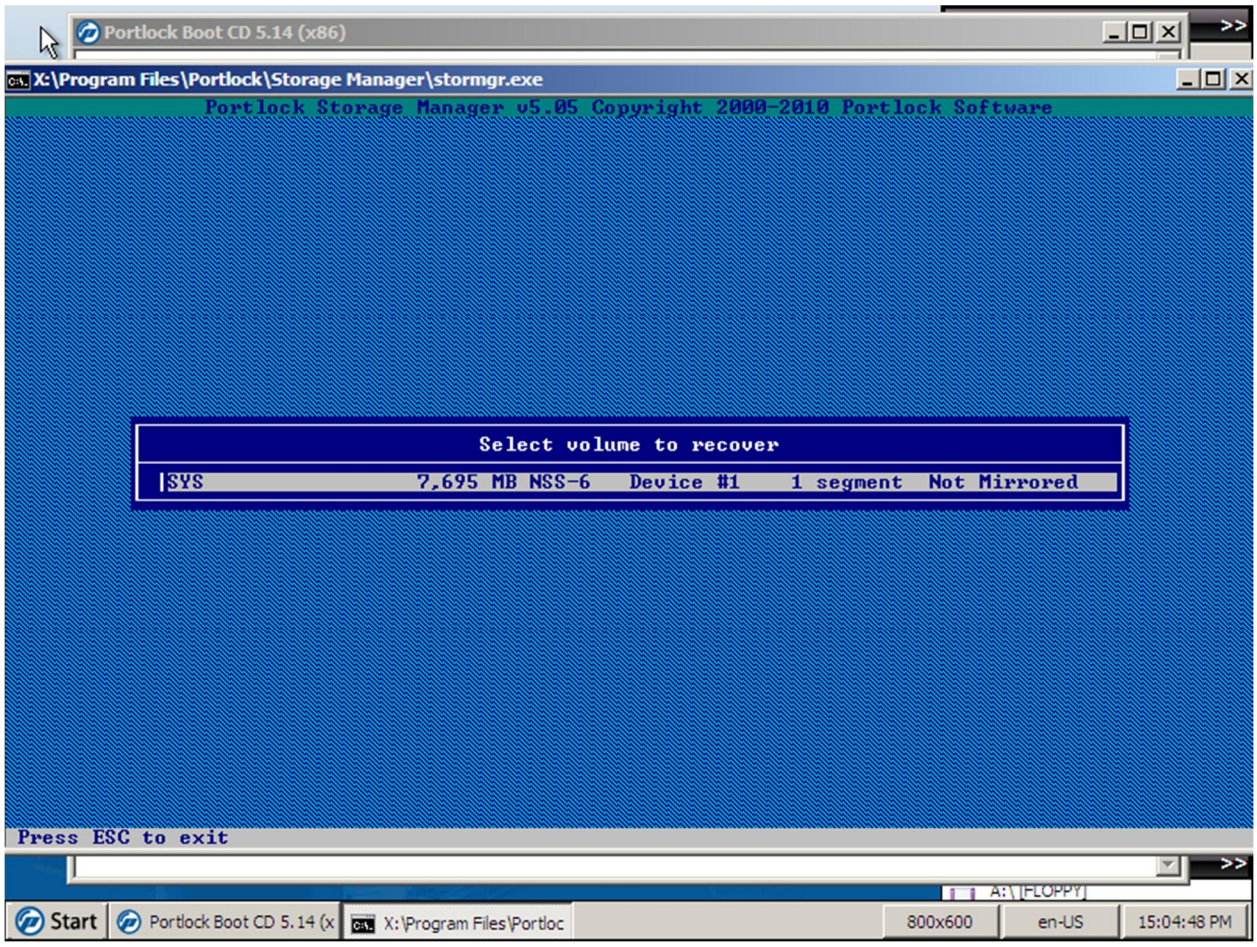
The following screenshots will step you thru recovering an NSS volume.



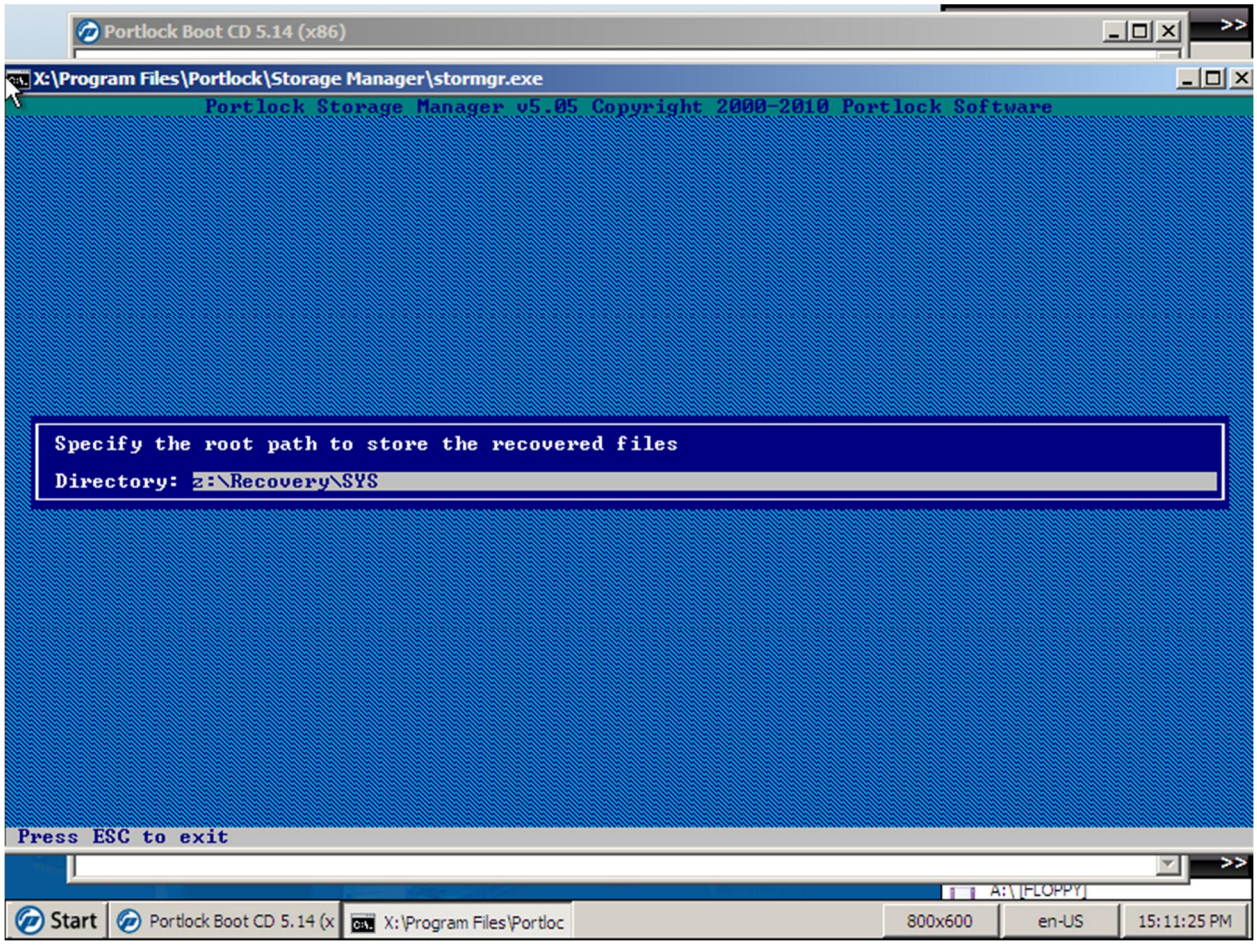
Enter a filename for storing the log the results of the volume recovery. In this example, we mapped the Windows share to “Z:”, so we will specify the logfile as “Z:\recovery.log”.



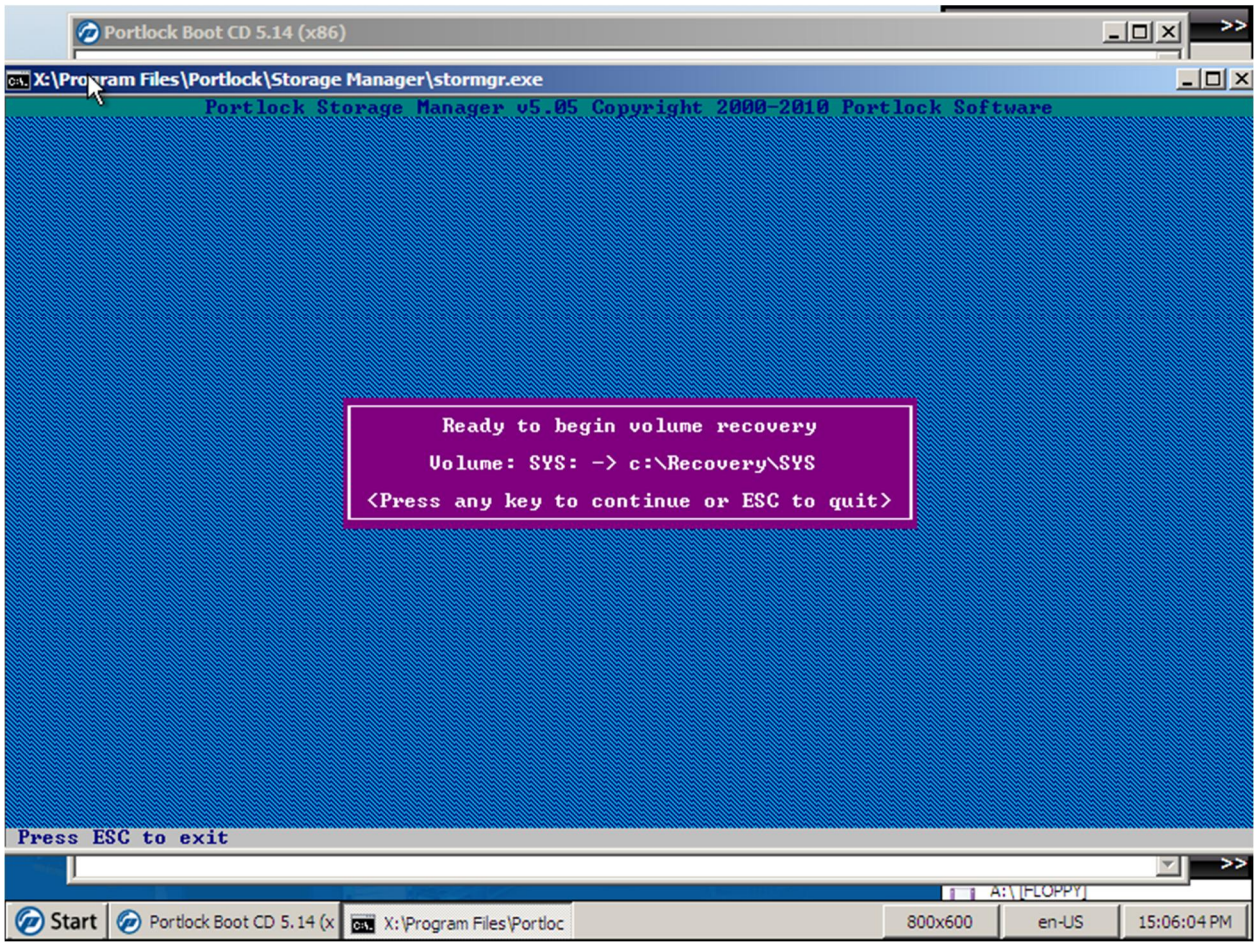
Select the volume to recover



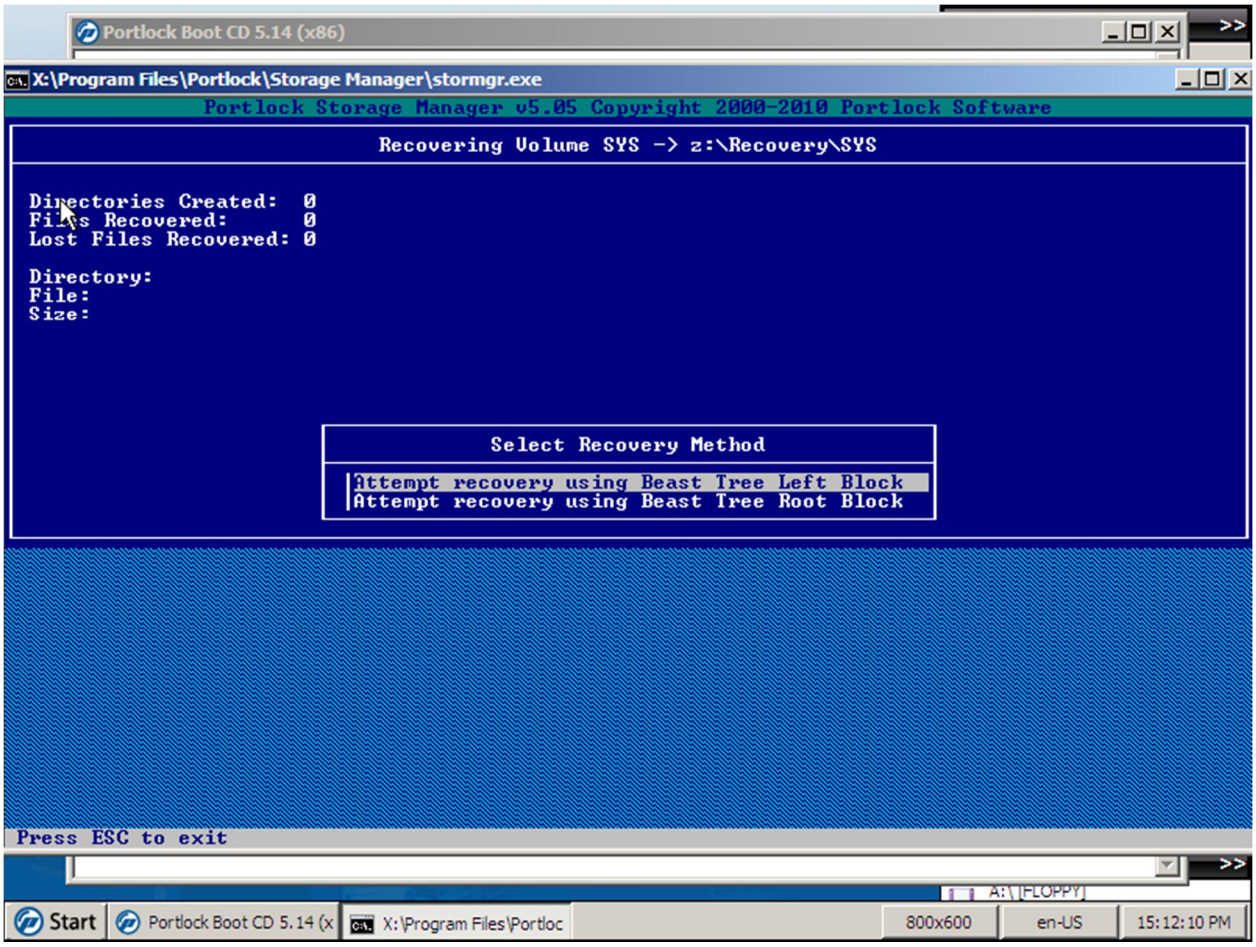
Enter the location to store the recovery files. In this example, the path is automatically completed based upon the volume name. You can change this.



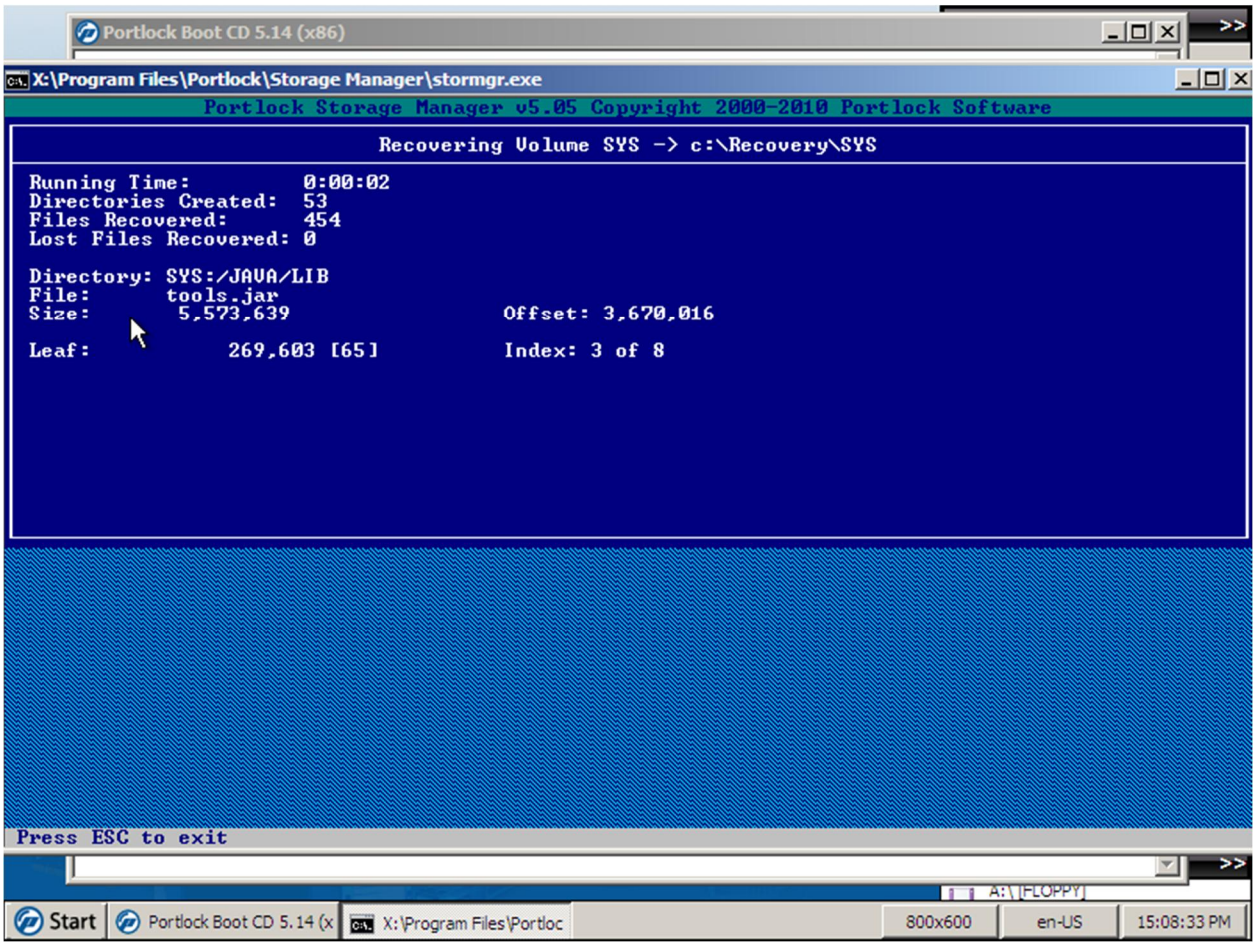
The next screen requests confirmation.



This command supports two methods of recovering data. You may have to try both methods depending on the type of volume corruption. In this example we will select the “Attempt recovery using the Beast Tree Left Block” method.



This is an example screenshot show progress of the data recovery.



[End of Document]

