

PIN Services Backup Configuration, Use and Administration

This document describes the normal function and use of the PIN Services Backup and Recovery System. It consists of two parts. The first part describes the basic configuration of Acronis True Image Home, the structure of the back up folders on PIN00-oldPC and PIN03-newPC, and the overall back up, recovery, and archival strategy for PIN Services. The second part describes how to alter or configure backups, and how to restore data or images in the event of data loss or system software and/or hardware failure.

Part A - Normal Configuration and Use

1. General Description of Backup/Recovery Strategy



Setting up an easy-to-use-and-maintain, reliable and simple data management and backup plan and an easy-to-use-and-maintain, reliable and simple system recovery plan can be very challenging. However, if this is achieved it means you will no longer have to waste unnecessary time and energy recovering or recreating valuable data or completely reinstalling and reconfiguring Windows and software and hardware from scratch. The worst possible outcome imaginable is that all your systems and data for every PC would need to be restored. With a good managed plan even this level of disaster can be recovered from with minimal effort and cost.



The most likely events to cause data or system loss are hardware failures (usually hard drives or motherboards), accidental hardware damage, theft, or loss, **OR** system corruption due to poorly designed software, viruses or other malware, or intentional or un-intentional user error. All of these events can be recovered from in only minutes to a few hours if the backup and recovery plan is well implemented and maintained, and without additional expense. In addition, over time the accumulation of data and software may cause your system performance to degrade and require a reinstallation of the operating system to improve performance. A well maintained and set up current generation PC (2009) can easily last at least 5 –8 years, with minor hardware upgrades, without needing to be replaced unless you run very resource intensive applications such as Photoshop, Video Editing, large databases, etc. For basic to intermediate use a well set up and maintained system should run with a minimum of expense and frustration.



The best strategy to adapt when using your computer, particularly if it performs some critical functions for you, is simple: If it ain't broke, don't fix it.

Constantly upgrading and experimenting with a mission critical computer is a guarantee that something will go wrong eventually. If what your computer does for you is more important than being able to do everything that is possible to do with it then setting it up from the start with a flexible game plan and then not tinkering when it is working the way you want is always the best strategy in terms of peace of mind!

The PIN Services Backup and Recovery System depends primarily on three aspects:

- The hardware used to back up systems and data
- The folder structure set up for the backups
- The program used to complete the data and system backups

Definition of Key Terms

a) a Backup, Backing Up



A Backup involves the making of copies of data files or entire folders for redundancy on one or more separate physical devices in case of loss, corruption, or system failure. One backs up primarily data, not system configuration. The files copied and their folder structure, or in the case of True Image Home, the Data image files (.tib files) are both considered 'Backups'.

b) Recovery Image, Archive or Backup, System Image, Archive or Backup



Recovery or Fault Tolerance is the ability to restore the operating system and/or software and hardware, and possibly data, in the event of loss, corruption, or system failure. A Recovery, Backup, or System image is a single .tib file containing either data, system configuration or both.

2. Hardware components of PIN Services Backup and Recovery System

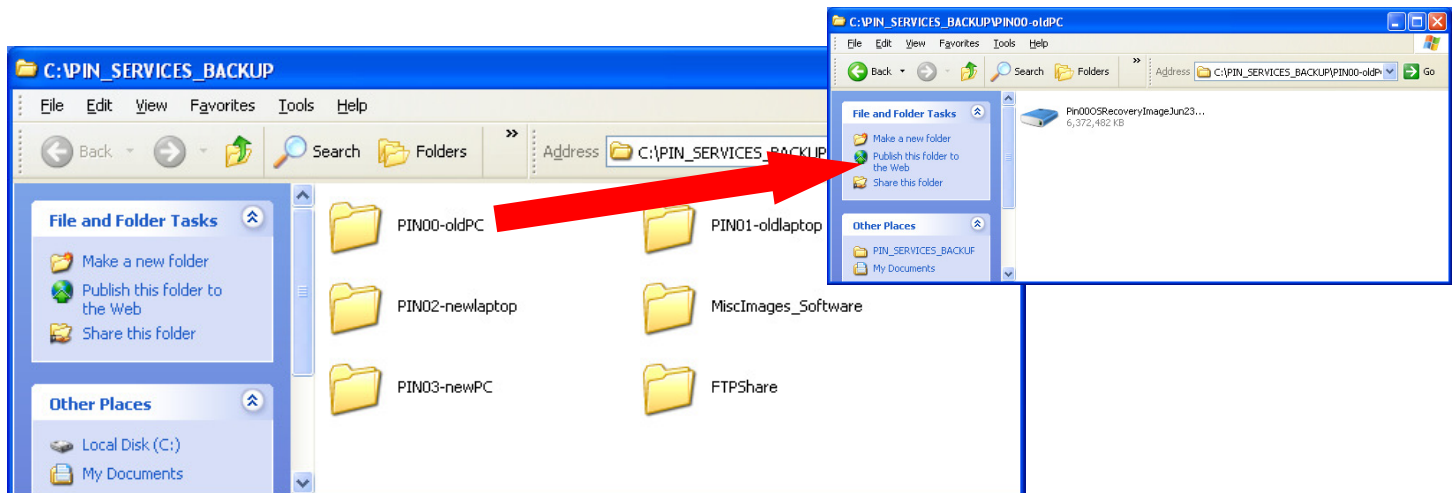
a) **PIN00-oldPC** - PIN00-oldPC functions as a backup/file server for recovery images, miscellaneous manual backups, most scheduled backups, software and drivers, and the network shares **FTPShare** and **Restricted FTP**. It is the main backup server for PIN02-newlaptop, PIN01-oldlaptop, and PIN00-oldPC and is the site for the second level of backup of PIN03-newPC. Files on PIN00-oldPC are either stored on its internal SATA drive (180 GB) or on a 1TB mirrored external drive (2TB total in non-mirrored configuration). Snapshots and general descriptions of the folder structures on each of the drives follow.

i) Internal 180 GB drive (**C:**): The main backup folder on the internal drive (**C:\PIN_SERVICES_BACKUP**) is mapped to PIN03-newPC and PIN02-newlaptop as the **Z** drive.

Each folder stored here and named after a PIN Services computer contains a single file – a redundant copy of a basic recovery image.



These images are only updated if they need to be restored and brought up to date. If a recovery image is used and brought up to date a new one should be created after the software is updated but before the data is restored. Once the new image has been used successfully for a few weeks the old one may be deleted if storage space becomes limited.





The folder **MiscImages_Software** is the default location for storing any and all software downloads, copies of purchased software, drivers for specific hardware and/or computers or peripherals, ISO files (CD images such as the modified XP install for PIN00-oldPC).

FTPShare is the default folder for the **PS_Backup** FTP account. It also contains the folder **For_Download**, which is used for files made available to upload as links in email.



There is another FTP folder in **C:\PIN_SERVICES_BACKUP**. This is the folder **Restricted FTP Folder**. This folder is for files that are accessed through custom FTP accounts. **FTPShare** is a shared folder for the default FTP account. The **Restricted FTP Folder** is separated from the other FTP folders to maximize security for sensitive information.

ii) External USB RAID0 1TB Drive

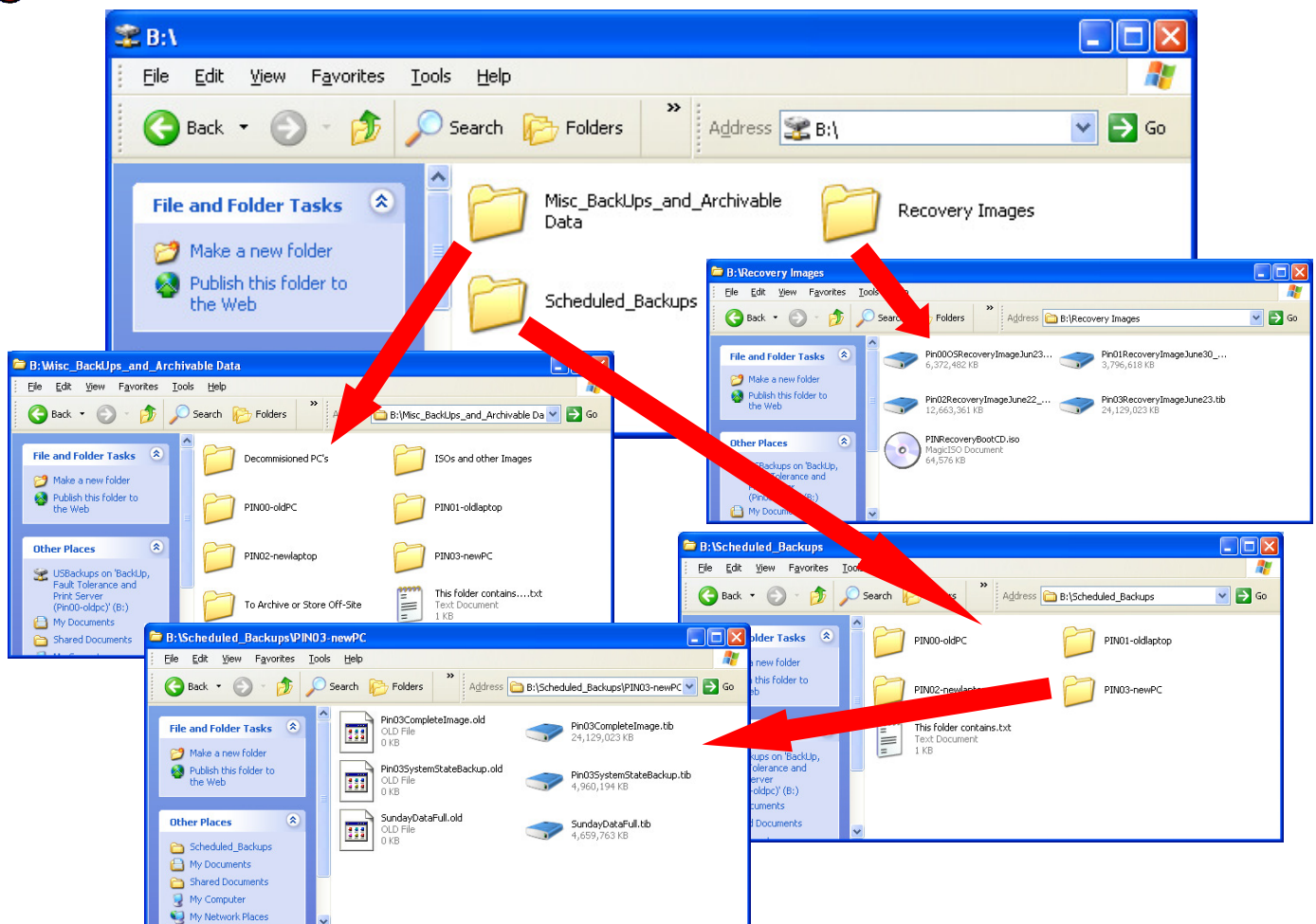
The main backup folder on the external USB drive (**I:\Backups** on PIN00-oldPC) is mapped to PIN03-newPC and PIN02-newlaptop as the **B** drive.



This drive actually consists of two separate but identical drives on which all the data is automatically duplicated or **mirrored** (RAID0 in the tech-speak, RAID stands for redundant array of identical disks). Mirroring the critical backup drive means that even if one drive fails the data is still protected.



In the event that one of the mirrored drives fails that drive should be replaced as soon as possible, and the data will be automatically re-mirrored.



The series of snapshots shown above unfolds the most essential folders on the external USB Drive and how they are related (**I** on PIN00-oldPC and **B** on PIN03-newPC and PIN02-newlaptop).

The folder **Misc_Backups_and_Archivable_Data** contains all the manual backups for all PIN Services hardware, including some images. Specifically, all data recovered from old or decommissioned PCs is stored here.

The folder **Recovery Images** has all the recovery images for the four in-use PIN Services computers and a copy of the ISO image of the True Image Recovery Boot Disk. This image, when burned to a CD, is used to boot a computer with the external USB drive attached to run True Image Home to recover a system image and/or data in the event the operating system fails or needs to be re-installed. This boot disk is also able to load drivers for SATA and/or SCSI drives (PIN03-newPC and PIN00-oldPC have SATA controllers and hard drives).



A copy of this recovery boot disk has been made and labelled as part of the entire Network Configuration Package. This boot disk image can be burned to a blank CD using the ISO burning feature of **CDBurnerXP** (installed on PIN00-oldPC). The ISO image can also be recreated using True Image Home (installed on all PIN Services PC's). The original True Image Home installation disk is also a recovery boot disk itself.

The folder **Scheduled_Backups** contains all the backups that are created by any pre-configured **Backup Task** using True Image Home. These may be run manually (unscheduled) or automatically (scheduled).



No data should be manually copied to this folder to prevent these critical backups from being accidentally deleted or altered. This folder contains the most critical active second level backups from PIN03-newPC, where most of the sensitive data for PIN Services is stored.

b) Hardware configuration on PIN03-newPC



PIN03-newPC has two identical SATA 300GB hard drives installed. Ideally, one could implement RAID0 (mirroring) on PIN03-newPC and then simply schedule a remote backup of the system and data, weekly or monthly, to the external USB drive. Unfortunately, the PC can only be put into a RAID0 configuration by reinstalling the operating system from scratch. As the current system is operating well this would be over-kill. As a result the second hard drive on PIN03-newPC is being used as the primary target for all scheduled backups of the system and data. Once a month a new complete disk image and system backup image are copied to the USB drive for archival purposes. The weekly Sunday Full Data backup is also copied to the USB drive.

2. Software components of PIN Services Backup and Recovery Plan



The key piece of software used to realize the PIN Service Backup System is **Acronis True Image Home**. This versatile software accomplishes both backups and system recovery. It is an example of disk imaging technology. Disk Imaging is the process of copying all or some of the contents of a hard drive at the level of the actual bits (the 1 and 0's that everything on your computer is encoded as). Disk Imaging was originally used to clone operating systems to specific hardware configurations. The idea is simple. Build one operating system, install all the hardware and software and then duplicate the setup onto as many identical or near-identical computers as required. Early on disk imaging came to be used as a quick and dirty method for backup but these early tools required that the entire image be restored to suitable hardware before

the original data could be recovered. The current version of True Image allows selective parts of the system and data to be backed up and restored as well as allowing the configuration of specific types of backups, such as incremental and differential back ups.

3. Basic Recovery Strategy for PIN Services

Every PIN Services PC has either had its operating system and software rebuilt from scratch or cleaned up and reconfigured. Each PC has then had a complete image taken. These images do not contain data, only the operating system and software. In the event of a system software or hardware failure, or if the performance of the computer has degraded significantly these recovery images can be restored to the appropriate computer, updated (operating system updates, software updates, new software added since original image), and the data restored returning the system to a usable state much more quickly and efficiently than a complete rebuild. The steps to follow to recover a system are found in Part B of this document.

4. Basic Backup Strategy for PIN Services

Every PIN Services PC has True Image Home installed and has 3 or 4 pre-configured **Backup Tasks**. On PIN03-newPC and PIN00-oldPC these Backup Tasks are automated to run without the need for intervention. On the other PC's unscheduled Tasks have been preconfigured that may be run manually if and when a backup is required. A break down of these Tasks for PIN00-oldPC, PIN02-newlaptop, and PIN03-newPC follows.

a) PIN00-oldPC

Currently a Backup Task is scheduled to run the first Sunday of every month at 6:00pm on PIN00-oldPC that takes a complete disk image. A **pre-command batch file** runs before the backup task starts deleting the now 2 month old PIN00completeimage.old and renaming the now 1 month old image PIN00completeimage.tib to PIN00completeimage.old.



The batch file is stored here: **C:\Program Files\Acronis\TrueImageHome\PreCom.bat**
A copy is placed in the **XXXXXXXXXXXXXX** on PIN00-oldPC and on the System DVD.

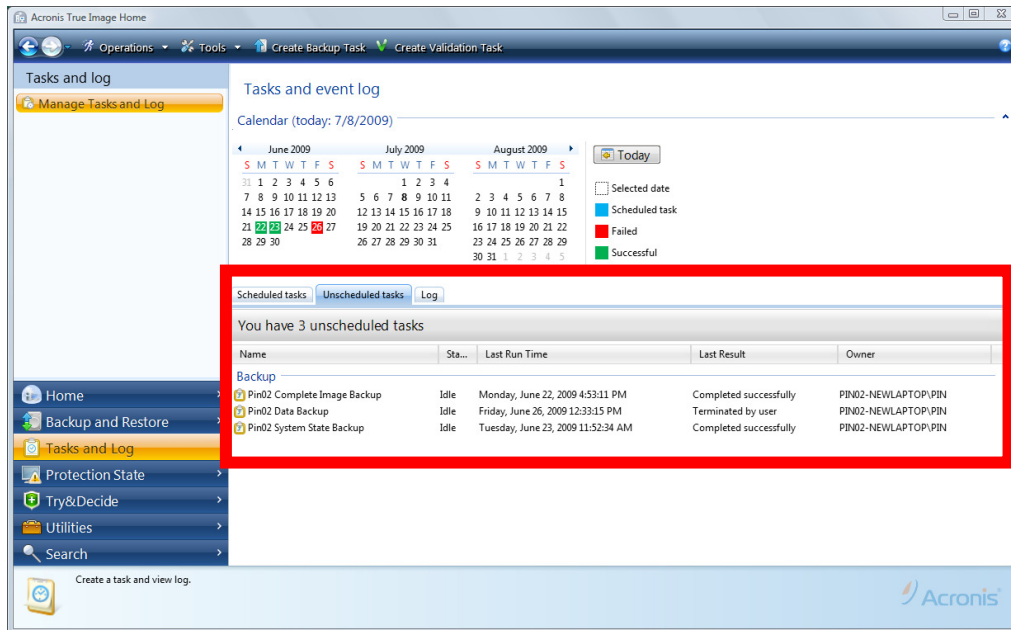
The result of this task is a complete image of the entire computer, OS, software, and data on **C**, going back to the first Sunday of the month and a month before that. These image files are stored on the external USB drive. The purpose of this Task is to keep a more up to date image for recovery purposes and some basic level of data backup. However the **C** drive of PIN00-oldPC is not the best place for sensitive data. **In the current configuration data that is stored only on PIN00-oldPC is more vulnerable than data stored on PIN03-newPC.**



Never configure a Backup Task to backup backup images! This will cause the size of backups to spiral out of control. Only hard drives without images on them should be backed up, or if a data backup is made be sure to not back up any images. The contents of the external USB drive contents are themselves never backed up as image files. The fact that the USB drive is mirrored and the implementation an off-site archival plan will ensure that the backups are themselves as safe as required for peace of mind.

b) PIN02-newlaptop

PIN02-newlaptop has 3 manual (unscheduled) Backup Tasks pre-configured (snapshot shown below)



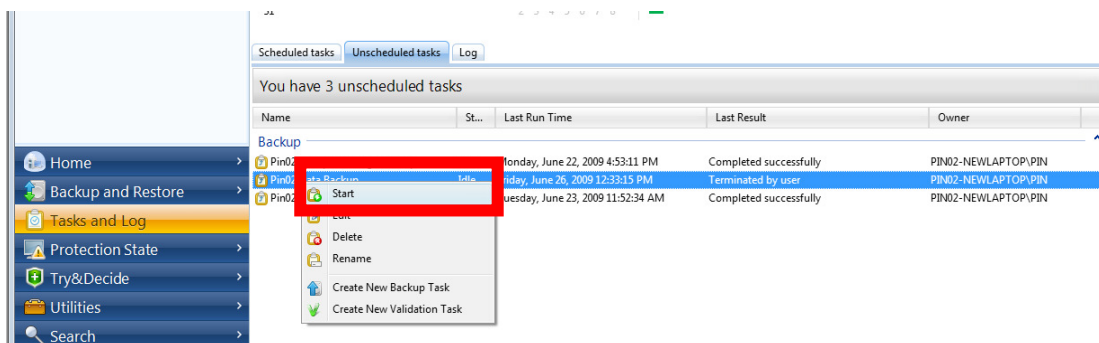
They are ***Pin02Complete Image Backup***, ***Pin02Data Backup***, and ***Pin02System State Backup***.

i) Pin02Complete Image Backup

This backup takes an image of the entire hard drive. It will create a file roughly half the size of the used disk space so only make complete image backups sparingly and only store a couple on the external USB drive to prevent backup image bloat. It will also take as much as an hour or more to complete.



Ideally PIN02-newlaptop must be connected in the office to complete this Task. It is not recommended to attempt a complete image over the VPN as this would likely take a day or more and be very prone to failure. To run any pre-configured unscheduled task simply ***right-click*** on the Backup Task icon and ***select Start*** as shown below. More detailed information on running and configuring backups is included in Part B.



Simply wait until the Task completes successfully and then shut down the program. The Tasks are configured to ignore errors but some errors might require user intervention.



It is always best to run a backup right after booting and before running any applications. If you don't reboot first it is best to shut all files, folders, and applications before running a backup. This decreases the likelihood of files being locked. Locked files may not be successfully backed up in Data backups.

ii) Pin02System State Backup

This backup takes a snapshot of the entire system and application setup without any consideration of the associated data. System State backups allows the system to be restored without requiring a complete image and data recovery and is the first line of defence if a system failure is preventing normal use of the computer. If a system state restore doesn't fix the system a complete image restore and data recovery is probably necessary.



If radical changes have been made to the system or software on PIN02-newlaptop it would be useful to take a system state backup. Otherwise this sort of backup is not usually required for PIN02-newlaptop.

iii) Pin02Data Backup

This unscheduled Backup Task is currently configured to back up all the following data:

My Docs, My Pictures, Desktop, Chrome user data (config and bookmarks), Skype user data (config and contacts), emergency backup Outlook PST, and misc other data.



There is still some data in **My Documents** on PIN02-newlaptop. This data was manually backed up to **B:\Backups\Misc_BackUps_and_Archivable DataPIN02-newlaptop** in the process of creating a recovery image. It is unknown if this data is duplicated elsewhere.



Currently there is only a recovery image, and one Pin02Data Backup stored in **B:\Recovery Images** and **B:\Scheduled Backups** respectively.



If the laptop is used primarily to remotely access PIN03-newPC there is no need to run any of these pre-configured backups regularly, only once or twice a year, after major changes, or if an emergency scenario requires use of the laptop as the main PC. If PIN03-newPC is unavailable for any length of time it would be best to reconfigure the unscheduled Tasks as scheduled tasks to ensure PIN02-newlaptop's data and system is secure.

c) PIN03-newPC

PIN03-newPC has four automatic (scheduled) Backup Tasks pre-configured as shown in the snapshot on the following page.

They are **Complete Image Backup**, **Daily Data Backup**, **MonthlySystemStateBackup**, and **Sunday Full Data Backup**.

i) Complete Image Backup – runs on the first Saturday of each month at 3:00 am.

ii) MonthlySystemStateBackup – runs monthly on the first Sunday of the month at 10:00 pm.

Associated with these two backup tasks is the running of a simple batch file using **Windows Task Scheduler** that re-organizes old Complete and System State images on the external USB drive and copies the latest image there for a second level of backup and archival purposes. The configuration of these batch files is covered in Part B of this document.

The batch file is stored here:

C:\Program Files\Acronis\TrueImageHome\MonthlyCopy.bat

A copy is placed in the **XXXXXXXXXXXXXX** on PIN00-oldPC and on the **XXXXXXX**.

iii) Sunday Full Data Backup – runs every Sunday at 4:00 am and backs up all files and folders identified as data. This is currently configured to include:

My Docs, My Pictures, Desktop, Chrome user data (config and bookmarks), Skype user data (config and contacts, current year Outlook PST, and misc other data.

This Backup currently creates a 5-6 GB image file. It is overwritten every Sunday. The primary image file is created on the **D** drive on PIN03-newPC and then copied to the external USB drive on PIN00-oldPC by a batch file scheduled to run in Windows Task Scheduler.

The batch file is stored here:

C:\Program Files\Acronis\TrueImageHome\WeeklyFullDataCopy.bat

A copy is placed in the **XXXXXXXXXXXXXX** on PIN00-oldPC and on the **XXXXXXX**.

iv) Daily Data Backup – an incremental back up that runs every day, except Sunday, at 4:00 am



This data only backup is only saved to the second hard drive on PIN03-newPC. Every week a new Incremental cycle is implemented. The first new incremental backup is essentially a full backup. Depending on when the incremental cycle is started this second full backup could fall on any day but Sunday. This is not critical to the overall backup strategy.



An incremental backup only backs up files that have changed since the last backup in the series, which in this case is the first new incremental backup. This keeps the backup images small and allows them to complete in minutes instead of an hour or more. Running a daily incremental backup in conjunction with the Sunday full backup achieves the following:

- There is up to a week's worth of immediately available version control and file recovery. You may look at any end of day modifications made to any backed up data for up to one week depending on where you are in the cycle. The version of a file to be restored is at worse one week old, at best one day.
- There are always three snapshots of the data available going back in one week increments from Sunday Morning at 4:00 am
- There are three snapshots of the data available going back in one month increments from the First Saturday of the month taken at 3:00 am
- There is access to whatever annually or semi-annually archived data has been backed up off-site. Currently there is no structured or documented archival plan. Best practice would be to store one complete image, one system state, and one Full Data Backup at end of year at some location not in the office, in password protected images.

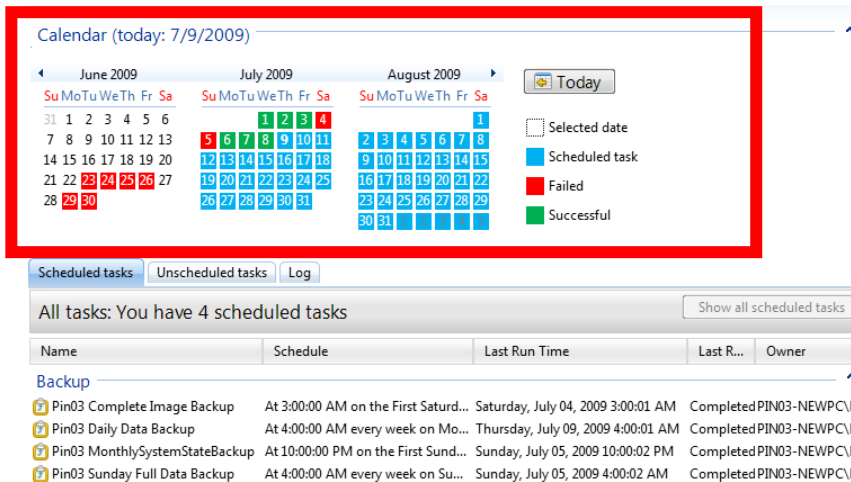
5. A Bird's Eye of the Backup Folders and File Structure, and Maintenance of Backup Plan



If the backup plan is set up and well maintained you may never need to use it and it will simply provide the peace of mind required to get on with life. However, in the event data needs to be recovered it is essential that we have confidence in the system and this means we need to take a peek at it, at least monthly, to ensure that it is working as expected and that data is not accumulating too rapidly. The following snapshots show how we can determine this quickly by looking in True Image and checking the contents of the main backup folder on PIN00-oldPC and PIN03-newPC to make sure that things are running smoothly.



True Image Home is currently configured to send an email to you so that you may confirm that the scheduled backups have completed without serious errors. Within True Image a calendar system with colour-codes also shows at a quick glance how the backups are running.



The red dates indicate failed backups. Most of the failed backups shown above happened in configuring and testing the system. The green dates are successful backups. This is what we want to see. The blue dates show days when Tasks are scheduled.



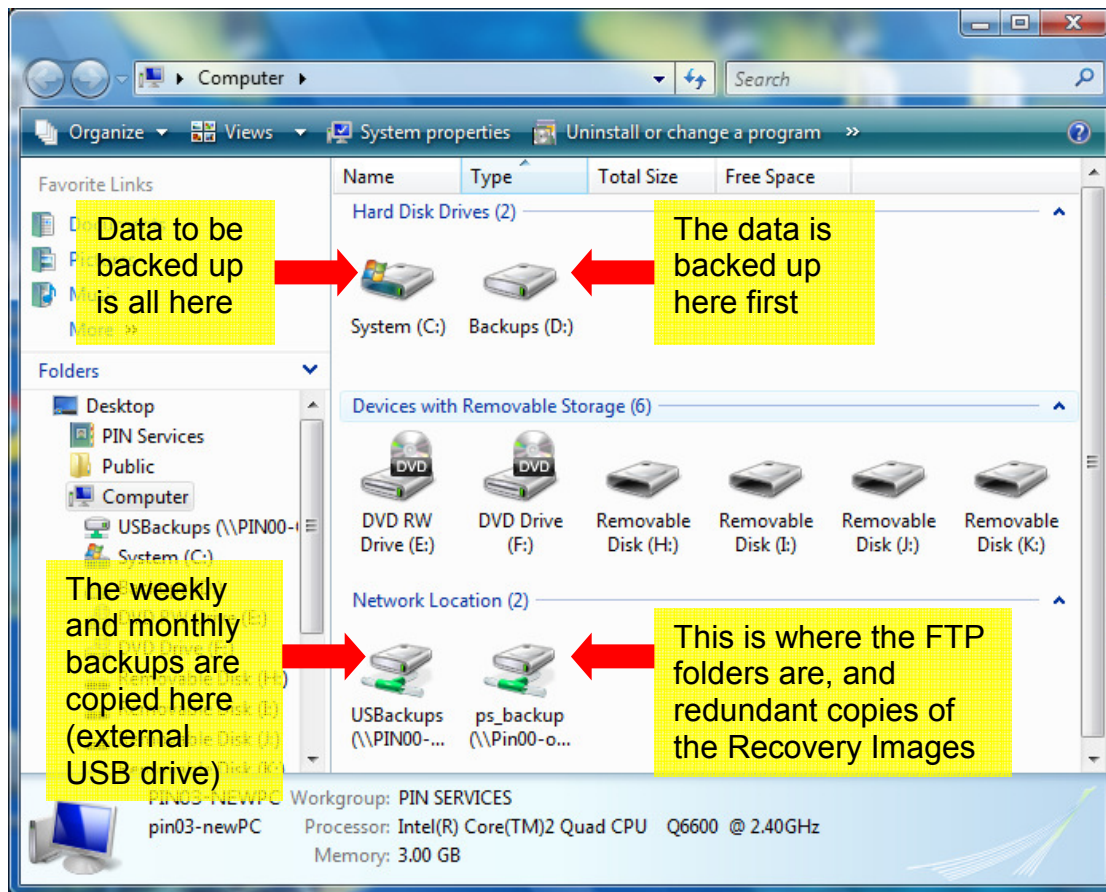
Backups may fail occasionally without that meaning data is not backed up. If a single file can not be backed up the Backup Task may 'fail' that one time without any cause for concern. What we are looking for is a pattern of 2 or more failures of the same kind for the same backup task. This is a cause for concern and needs to be investigated.



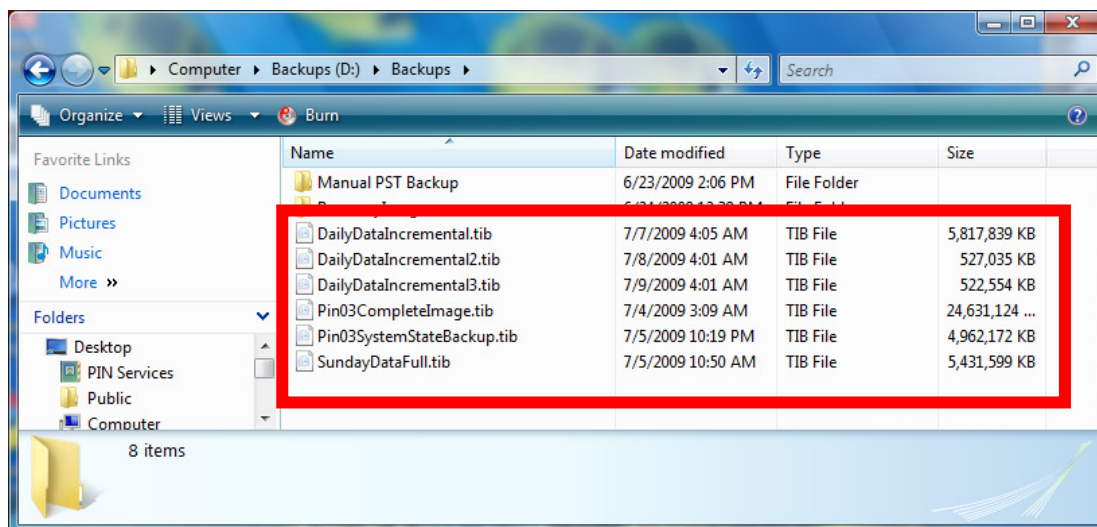
It is always the best practice to shut down all application and close all files at the end of the day to ensure files may be backed up. This is true even if backups aren't being run. Open files are always at greater risk of corruption than closed files. It is also best to shut down Outlook. If the same files and programs are left open every day there is a risk that data will not actually get backed up. There is no way around this limitation. As a bare minimum the computer, all applications, and files should be shut down for the Sunday morning full data backup. This means shutting everything down, and not using any remote services Saturday night before bed.



The following snapshot shows the folder structure on **My Computer** on PIN03-newPC and what the drives are used for in terms of the Back Up and Recovery Plan.



The next snapshot shows what the normal folder structure on **D:\Backups** should look like. The number of incremental images will be between one and six depending on where we are in the weekly cycle. General things to check for are:



- **Pin03CompleteImage.tib** should be roughly half the size of the used space on **C**
- **Pin03SystemStateBackups.tib** will be at least 5 GB
- **SundayDataFull.tib** will be at least 5 GB but never as large as the complete image
- **DailyDataIncremental.tib** should be roughly the same size as SundayDataFull.tib
- Subsequent Incremental image should always be much smaller than the first incremental or SundayDataFull.tib. There should never be more than 6 of them.

- The **Date Modified** values should reflect that last date the task was scheduled to run
- The amount of space used on **D** should always be greater than **C** and neither should increase dramatically from week to week, or even month to month.



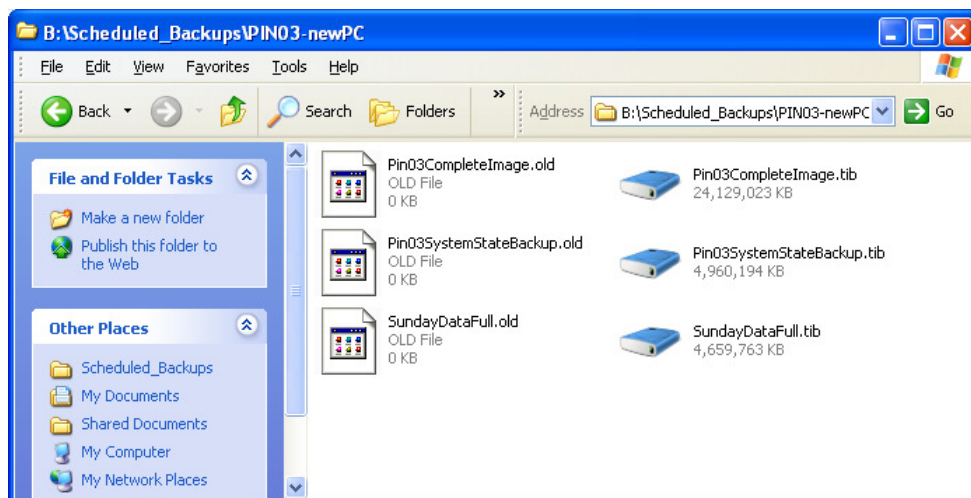
If you discover any pattern that does not match these expectations this is a potential cause for concern and needs to be investigated.

The final snapshot (below) shows how the file structure on the external USB Drive (**B:\Scheduled_Backups\PIN03-newPC**) should look if the weekly and monthly backup images are being properly and regularly copied. General things to check for are:

- there should be no more or less than six files, 3 .old files and 3 .tib
- the .old files will generally be slightly smaller
- the creation dates and sizes of the 3 .tib should be identical to the files stored on the **D** drive of PIN03-newPC



If you discover any pattern that does not match these expectations this is a potential cause for concern and needs to be investigated.



6. Miscellaneous Best Practices



In the ideal a well designed and maintained back up and recovery plan is never needed. In reality the plan, if needed, will only work if it has been tested and is maintained. Here are some additional best practices not covered or implemented that further harden your backup and recovery plan.

- Be critical in determining what data you keep, where you keep it, and what actually needs to be backed up. This prevents data bloat and running out of hard drive space.
- Check the free space on all drives on PIN03-newPC and PIN00-oldPC monthly. Make plans to increase capacity, delete unneeded backups, or archive data to DVD or off-site if there is less than 25% free space on any drive. Computer performance can be greatly degraded if less than 25% of the hard drive is free space
- Be careful not to create backup images that have images in them. This will cause image size to spiral out of control. True Image is configured by default to prevent this.

Part B – Administration and Configuration of Backup and Recovery

This part of the document provides additional configuration information for creating new Backup Tasks or modifying existing ones as well as procedures to follow to restore data or systems. It also includes a brief description of how backup archive maintenance is configured using Windows Scheduler to run simple batch files.

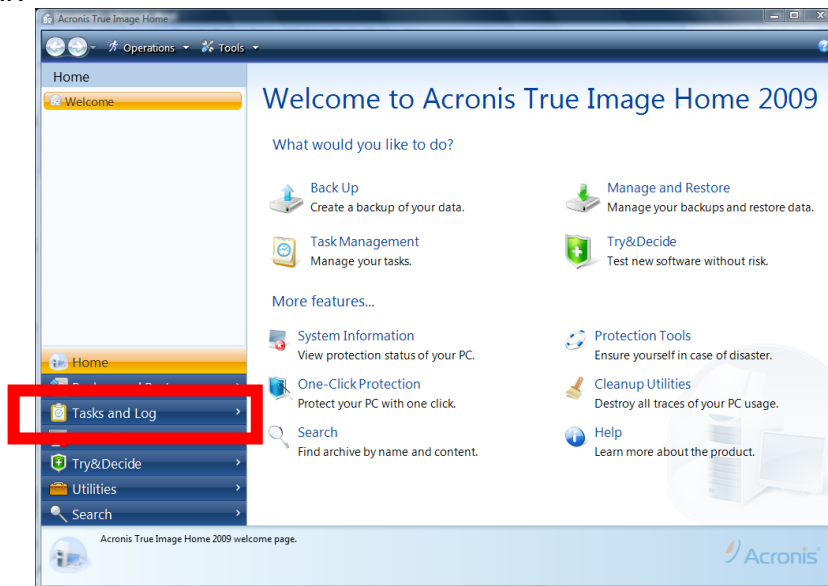
1. Modifying Existing Backup Task



The most likely administrative tasks you will have to perform are trouble-shooting or reconfiguring backups based on changing backup needs; either modifying existing backup tasks or creating new one. This might include, but is not limited too:

- adding or removing files or folders to be backed up
- changing times or days backup tasks are run
- changing scheduled tasks to unscheduled tasks and vice versa
- creating a new backup plan for existing or new hardware

All backup and recovery administration is accomplished in Home True Image by running the program from the Start Menu, Program Group, or Desktop shortcut. The following **Welcome** window will appear:



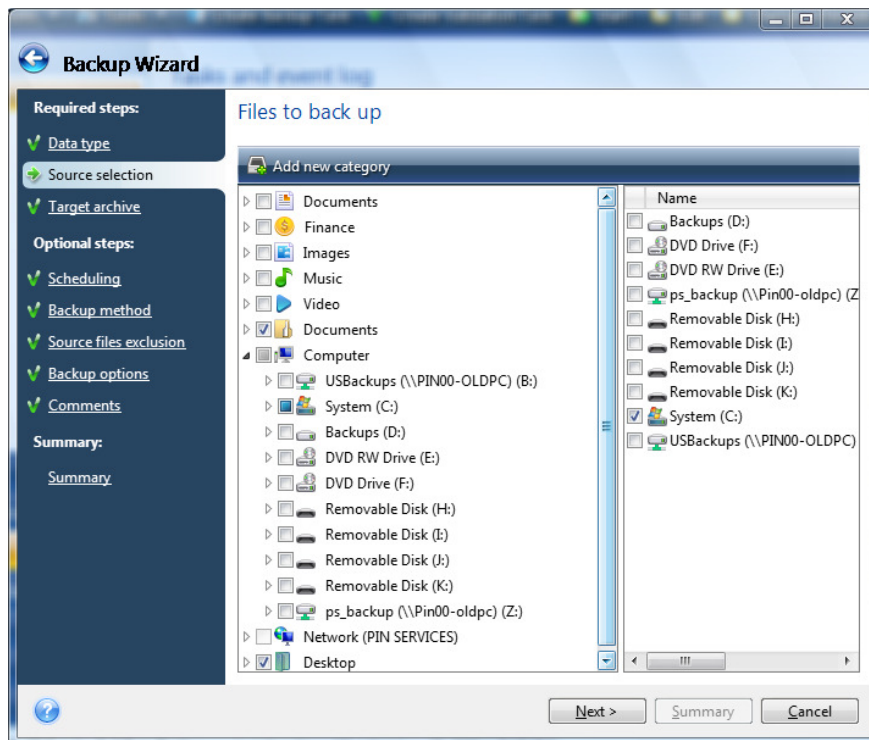
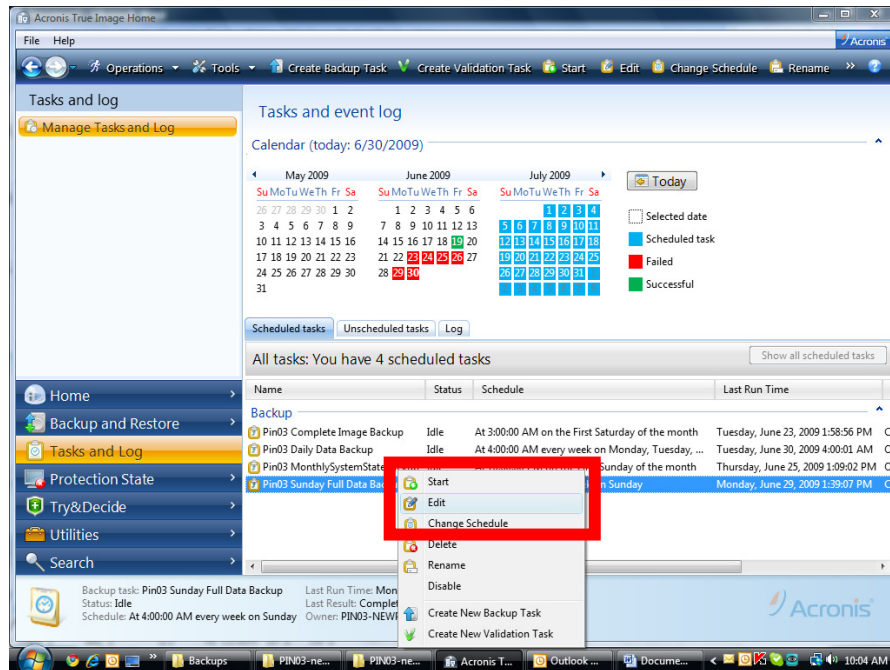
Click **Task and Log** to modify existing Backup Tasks. The window shown on the following page will open. Simply *right-click* on the Task to modify and *select Edit*.



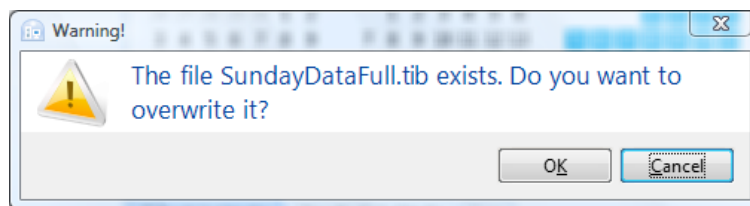
Backup Tasks can also be manually started this way as well a creating new Tasks and other basic administration.

In the following you will be shown how to add new files and folders to the **Backup Source** for **PIN03 Sunday Full Data Backup**.

After *clicking Edit* the second following window will open.



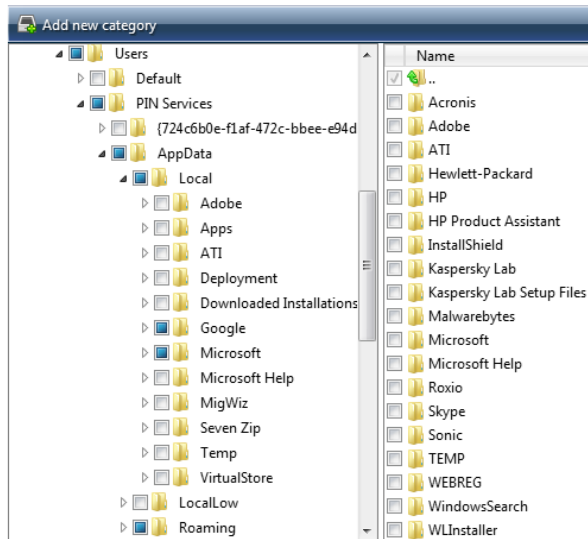
If the following dialogue box opens simply *click OK*.



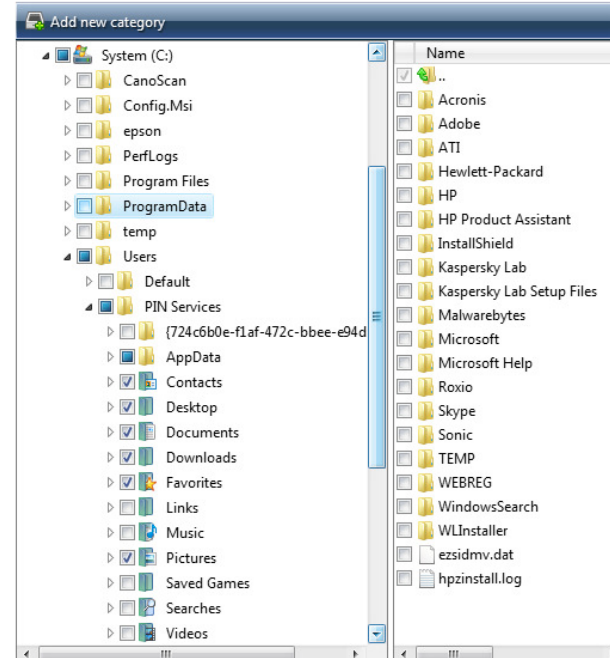
At the **Source Selection** browse window simply *check* or *un-check* the appropriate **checkbox** to add or remove files or folders from the Backup Source. The following snapshots show the folders

that are *checked* that contain most of the data that needs to be backed up, including application specific data such as the main Outlook PST, Chrome bookmarks, and Skype contacts:

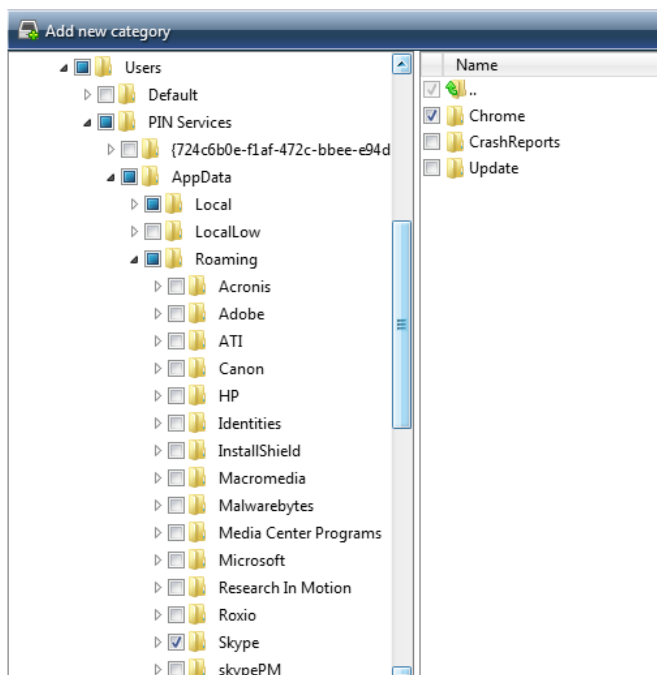
Files to back up



Files to back up



Files to back up



Simply *click* the **Summary** button after making changes and shut down the application when you are finished. Changes will be implemented the next time the Task is executed automatically (scheduled) or manually (unscheduled).



You are encouraged to explore the other Backup Task options – **Target Archive, Scheduling, Backup Method, Source File Exclusions, Backup Options, and Comments**. Here you will find where other aspects of the Tasks are configured such as receiving email notification, password protecting images, running pre or post commands, setting compression levels, etc. Normally these settings will not need to be adjusted unless there is a recurring pattern of backup failure.

2. Recovering Data, System States, or Complete Images (including Recovery Images)

This section describes in detail specific to the PIN Services Backup and Recovery Plan how to recover from data loss or system failure using the backup images or .tib files (archives) and True Image Home.

a) Recovering Data



When recovering data the first step is to determine which backup archive or image is most likely to contain the data to be recovered. In any event it is always best to restore backups to a temporary location rather than the original location.



If a large image has to be restored to look for a single file you may inadvertently overwrite newer versions of current files. True Image Home restores the folder structure along with the folder contents making it easy to search for and find lost or corrupted data and then copy it back to its original location.



The most likely scenario requiring you to restore all the files and folders of a complete data backup directly to their original location would be after a complete image or recovery image is restored. This is usually only necessitated by a system failure or intentional rebuild.

In any event True Image Home provides many options for how data is restored. Choose the method that you best understand, and restore only the files and folders you need, from any data or complete image (system state images contain no user data).



If a file has been corrupted and successfully recovered from a backup it is best to cut and paste the contents of the file, if possible, into a new version of that file type. Whatever caused the file corruption may be still be inherent in the restored file and may lead it to become re-corrupted. Cutting and pasting into a new file will usually permanently repair corruption problems like this.



The general strategies to follow depend on whether you are restoring a file or folder, a few files or folders, or restoring more, or all, of your data due to a system failure.

i) General Strategy for Restoring Data without any related systems failure.



When setting out to restore data due to causes other than system failure such as file corruption, or if files have been intentionally or unintentionally deleted, the first thing to do is to think about when the version of the file you wish to recover was last saved. The following describes which backups you can access from most recent to oldest:

- You have up to a week's worth of incremental restore images to choose from starting from the last successful Daily Data Backup (normally yesterday)
- You have a full data backup from the previous Sunday stored on **D** (on PIN03-newPC), and the two previous Sunday's full data backups stored on the USB drive (**B**).
- If you can not find the missing data in these the data images you would then have to selectively restore data from the last complete image taken at the start of the current month on **D**, or from one of the two previous complete images on the USB drive (**B**).
- If the file is not in any of these images only images older than three months that have been archived may be searched, or data from manual copied backups on PIN00-oldPC (Z drive)



The current configuration allows you to restore files that were in place up to 3 months ago, 2 months ago, 1 month ago, 3 weeks ago, 2 weeks ago, 1 week ago, and up to and including as many as 7 days in the last week.



If you are uncertain when or where the file went missing it is best restore images in the reverse order from the last date you are reasonably certain they were on your system. This is absolutely necessary when dealing with the incremental images, which only back-up files changed since the last successful incremental backup (the first of which is a full backup).



If you have to restore complete images one after the other to search for one file this will be quite time consuming. Normally, if you have some idea of where the file was stored originally you can search for it in the image and restore only the file(s) or folder(s) you need. A complete restore of even an incremental backup can take an hour or more.

ii) General Strategy for Restoring Data or Systems after a system failure

When you are restoring data because of a system failure the steps to follow are more intuitive:

- Restore either the last complete image (includes most of the data) or the recovery image (includes no data)



If you restore a complete image the data is still likely to be out of date so restoring a complete image will be nearly identical to restoring a recovery image. The advantage of restoring the last complete image over the recovery image is that the software is more up-to-date. The recovery image restore requires more system updating but is cleaner. If you are restoring an image simply to improve performance it is best to restore the recovery image.



If you restore a recovery image and update all the software it is a good idea to make a new updated recovery image before restoring the data. If you need or wish to restore the complete system again in the future it will take less time to update the software.

- After restoring the last complete image or the recovery image restore the last Sunday Full Data Backup (only do this for a complete image restore if the Sunday Full Data Backup is newer than the complete image used to restore the system)
- Then restore the first incremental image and all the subsequent incremental images in the order they were created (assuming they were taken after the last Sunday Full Data Backup). This should restore all the data as it was over the last week of use right up to the last day the system was functional and backed up.

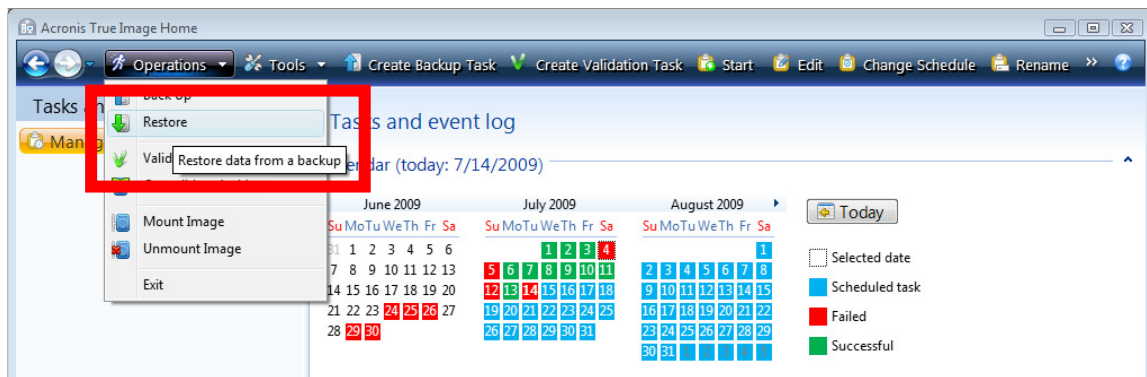
b) Typical Data Restoration



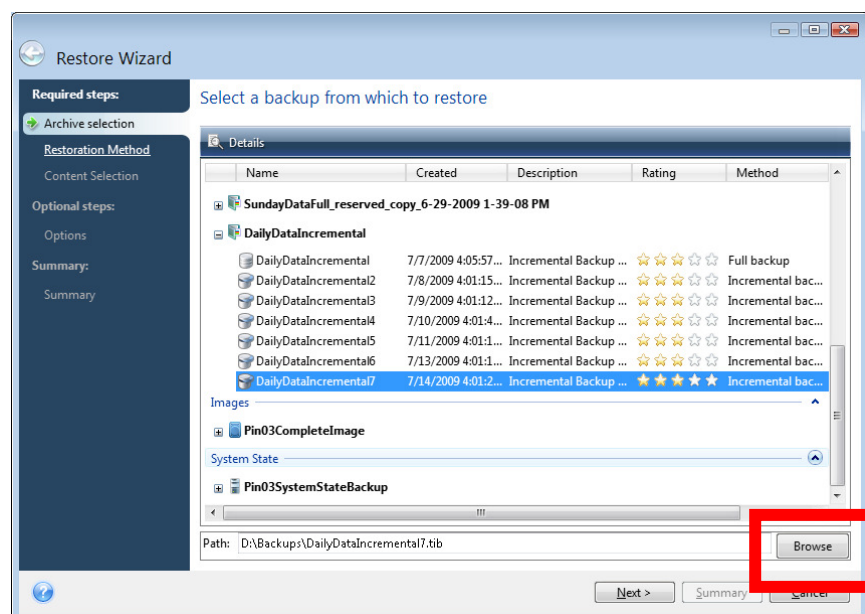
For the following example we are assuming the system is operating normally so that backup archives (images, .tib files) are readily available either locally on PIN03-newPC (**D:\Backups**) or on the network (**B:\Backups**). If there is any associated system problem related to the data loss and data must be recovered directly from the USB drive see the next section for instructions on connecting the USB drive to a computer either directly through **plug and play** or by using the **Recovery Boot Disk**.

To begin a data restore *start* True Image Home. When the main page opens *click* **Operations | Restore** on the toolbar as shown below. You may also start a restore by first *clicking* the **Backup**

and **Restore** button (middle left) and then **Manage and Restore** or by *clicking* the **Manage and Restore** button on the main of Home page of True Image.



The following window will open:



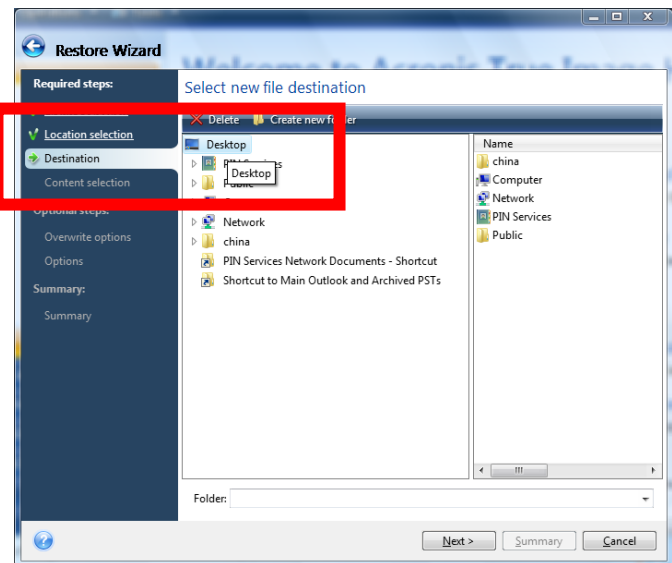
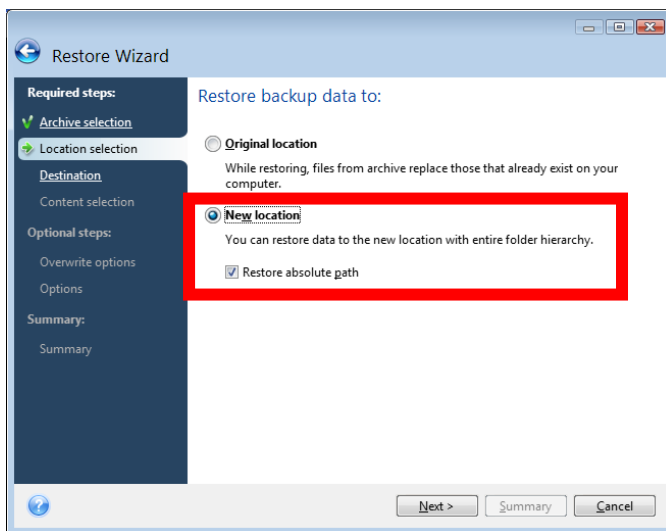
This page shows a database of all the backups run on the computer. They are separated into Data, Images, and System State backups. It is here where the best archive to be recovered is determined. In this example we are going to restore from the last incremental archive as shown above. *Click* on the archive you wish to restore from and *click* **Next**. The following window will open.



If you are running True Image from a boot disk there will be no database available. In this case you will *browse* for the archive to restore by name. Notice the **Browse** button at the lower-right (shown above). The archives will either be on the **D** drive of PIN03-newPC, the **B** drive of the network (the external USB drive on PIN03-oldPC) or on whatever drive letter the USB drive received if you have connected it directly to the PC on which data is being restored.

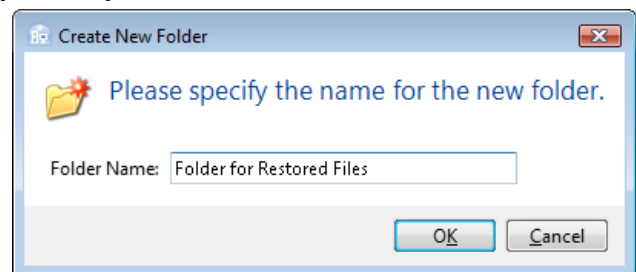
At the **Location Selection** window (shown below to the left) you may choose to restore data to its original location or to a different location. Unless you are restoring all the data to a recovery image rebuild it is probably easier and safer to restore the archive or the selected files and folders to be restored to a different location to prevent overwriting newer files and to avoid confusion between the original data on the PC and the restored data. The best place to do this is the **Desktop**. Make

sure the **Restore absolute path** check box is *checked*. This will recreate the folder structure and help you find the files that need to be recovered more easily. *Click Next* to continue.



When the window shown above to the right opens you may *browse* for the restore **Destination**. We will restore to the Desktop as shown above.

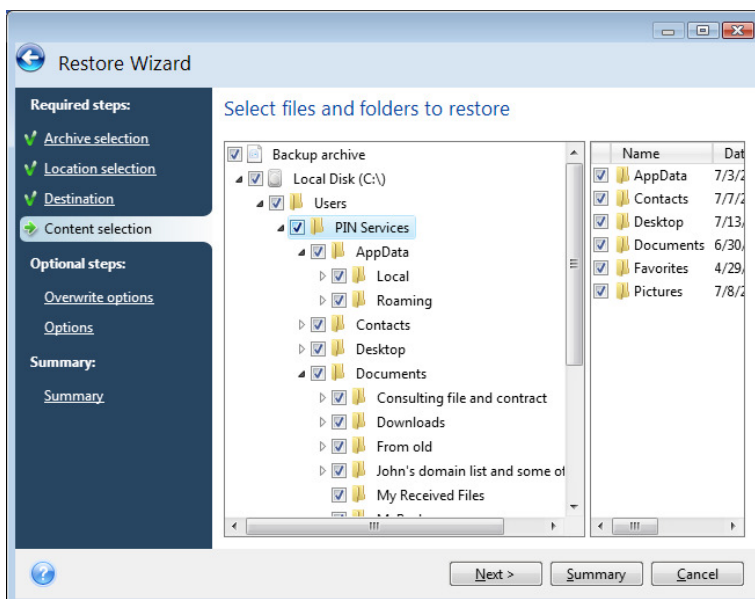
You will be prompted to *name* the folder (see right). *Enter* a name for the folder and *click OK*.



The **Content Selection** windows will open. This is where you can select which files or folders will be restored. By default the entire archive is selected.

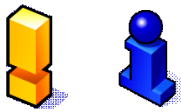


Only restore an entire archive if you absolutely have to. It may take an hour or more to restore. You may continue working on your PC during a data restore, but not a system or complete image restore. Some restores may require that the computer is rebooted.

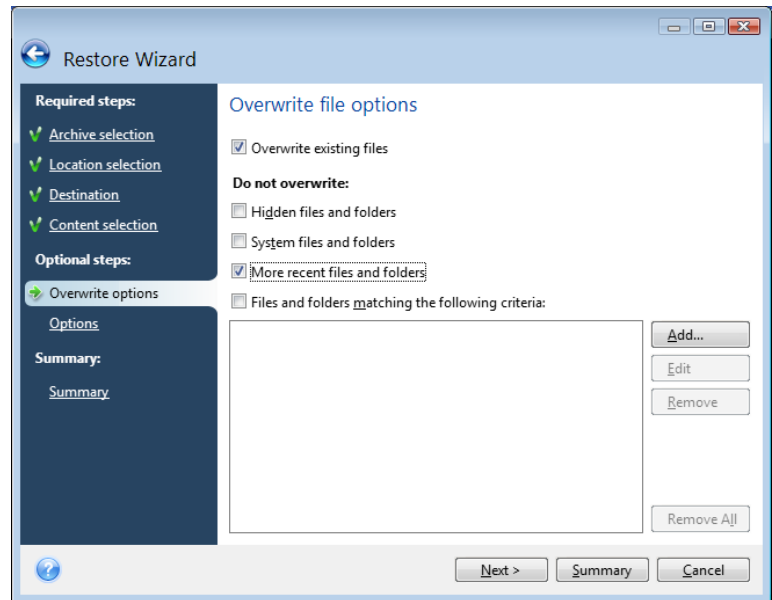


In much the same way that you *select* files to be backed up you *select* the files to be restored. Once you have *selected* all the files and folders to be restored *click Next*.

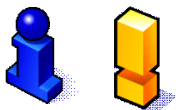
The **Overwrite options** window will open. (shown below)



If necessary you may configure how files are overwritten. You only need worry about these settings if you are restoring data to its original location when other data is already in place. Restoring to a different location removes any worries of unintentionally overwriting newer or identically named files. The settings you choose on this page depend on the specific nature of the restore. If you are uncertain how to proceed ask for some assistance.



Clicking **Next** will bring up the **Options** window. Generally the default settings will be fine. Click **Next** or **Summary** to review the restore configuration. If everything is ok click **Proceed** to start the restore.



Once the process completes you may browse the folder where the files were restored. Copy the restored data back to its original location and then delete any unwanted restored data to prevent it becoming backed up as part of the current backup system



Deleting redundant or unneeded data prevents bloat and keeps your system and backups running smoothly and safely for a long time.

c) Connecting the USB drive to a computer through Plug and Play or using the Recovery Boot Disk

The next two types of restores may require that the external USB drive be connected directly to the computer. This would be the case if the operating systems does not boot normally, or boots but is not running smoothly, or has had a new hard drive installed without an operating system. In all these case we are dealing with some sort of system failure requiring the restoration of either:

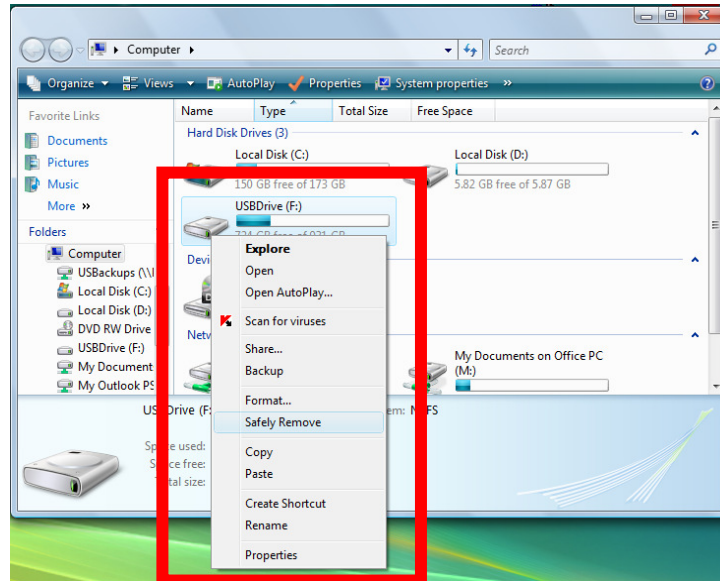
- a System State image to resolve a system problem without using a complete image or recovery image and full data restore.
- a Complete or Recovery image restore that may then require a secondary data restore.



The USB drive can be connected to any current PC by simply plugging it into a free USB port. It will pick up the next available drive letter and will always appear as **USBDrive**.

To safely remove the USB drive it is better to **eject** it first. **Open My Computer** find the USB Drive icon, **right-click** on it and **select Eject** as shown following:

The USB Drive also has a power switch. Once the drive is **ejected** from Windows simply power the drive off. Reconnect the drive to the computer requiring the restore, plug it in and power the drive on.



If you are connecting the USB drive to a computer through Windows simply boot the PC either before or after you connect the external drive.



If the computer won't boot properly with the drive connected, disconnect it, boot to Windows and then connect the drive.

If you are restoring to a computer without an operating system or if the operating system is not working normally first insert the PIN Recovery Boot CD (or the original True Image Installation CD) into the CD or DVD drive.



You may need to first power on the computer to open the CD or DVD drive and then manually restart the computer to get it to boot from the CD.



All the PIN Services computers have been configured to boot from a bootable CD if one is in the CD drive. If a computer ever doesn't boot normally to Windows it is possible a bootable CD was left in the drive. If this happens remove the bootable CD or DVD and manually restart the computer to boot to windows.



As soon as any working image is in place it is easier to restore data by running True Image on the computer rather than the using the Boot Disk.

Once the computer boots to the Recovery CD a **True Image Welcome** window will open. There will be two icon showing; one to start True Image and one which allows you to boot to Windows normally. *Select* the True Image icon to start the program.



The version of True Image on the recovery CD is nearly identical to the one which runs in Windows. The following snapshots are taken from the Windows version so there are some subtle differences in the way the program looks. For example, the archive database on the computer will not be available and you will always have to browse for archives. Once True Image opens you can restore data, systems states, or complete or recovery images from either local drives (such as **D** on PIN03-newPC) or from the USB Drive.

d) Restoring the System State



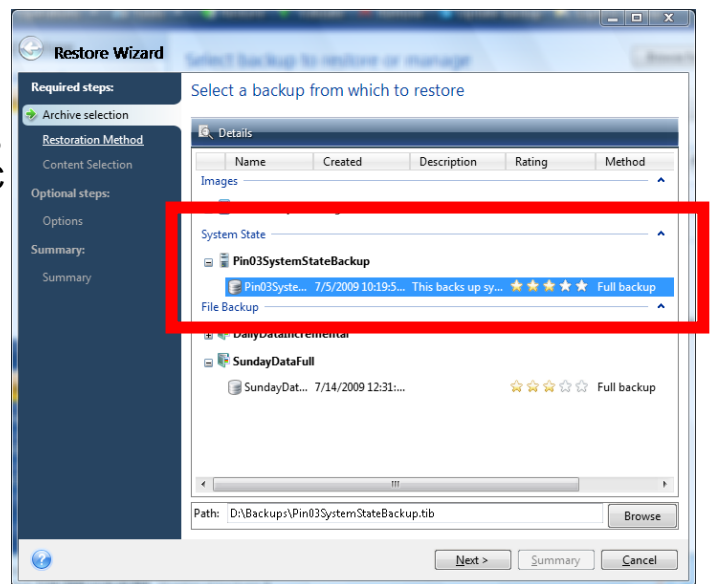
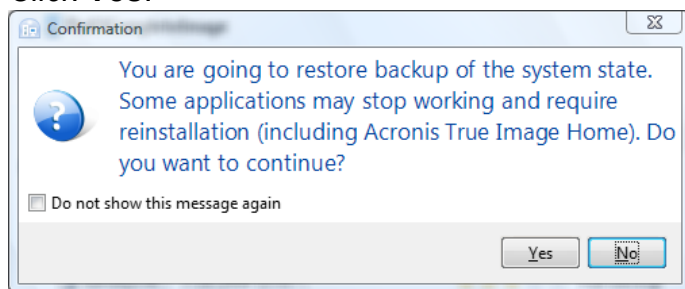
If there is a system problem other than a failed or failing hard drive the first thing to attempt is a system restore. The advantage is that no data will need to be restored. However, it is likely that some software will no longer work and may need to be reinstalled. If a system state restore does not resolve the system failure a complete or recovery image restore will need to be done.



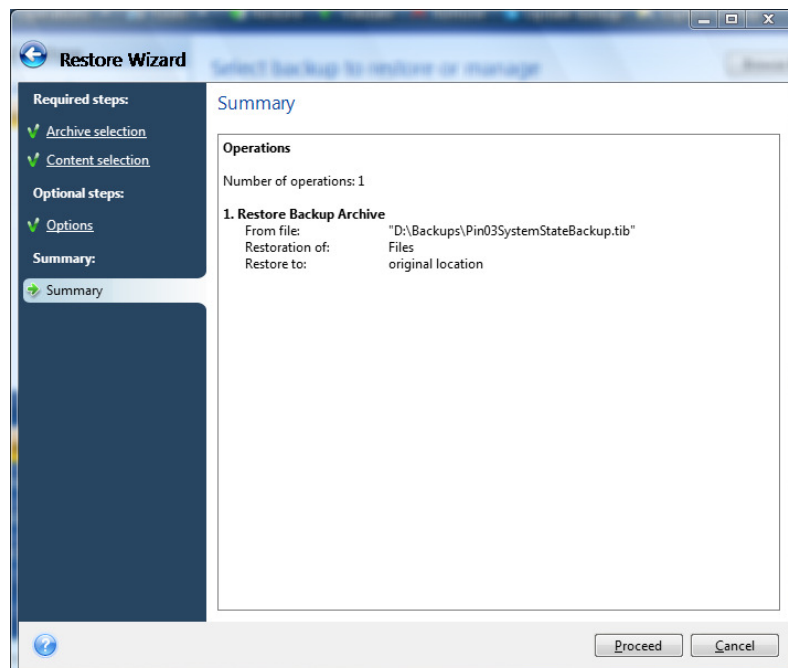
In the event that a complete image or recovery image is to be restored and assuming space is available, and that the computer hard drive is still functional, it is a good idea to take a manual (unscheduled) complete image backup to ensure all existing data is safe. This process may also be used to facilitate recovery of data from a failing hard drive.

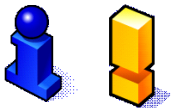
At the **Archive selection** window *browse* for the last appropriate System State archive on the USB drive or if you are restoring data on PIN03-newPC the **D** drive (see right).

Click Next. The following prompt will appear.
Click Yes.



You may now simply proceed to the **Summary** window, review the configuration, and **click Proceed.**





Once the System State restore finishes you will have to determine whether or not this has resolved the system failure and if any of the software needs to be reinstalled. Proceed with the next logical task on the basis of these determinations.

e) Restoring a Complete System and Data

In the event that a System State backup does not recover the system or in the event that you wish to start with a fresh installation of the operating system you will need to first back up the data on the system, and then restore a complete image and additional data, or restore a recovery image and then restore all the data (ideally from the last run Full Data Backup and any incremental backups).

Proceed, essentially, as if you are doing a System State restore.



Once True Image is running from the boot CD you may, if necessary, take a complete image or data backup before restoring the complete or recovery image. Once this is complete configure the image restore as follows:

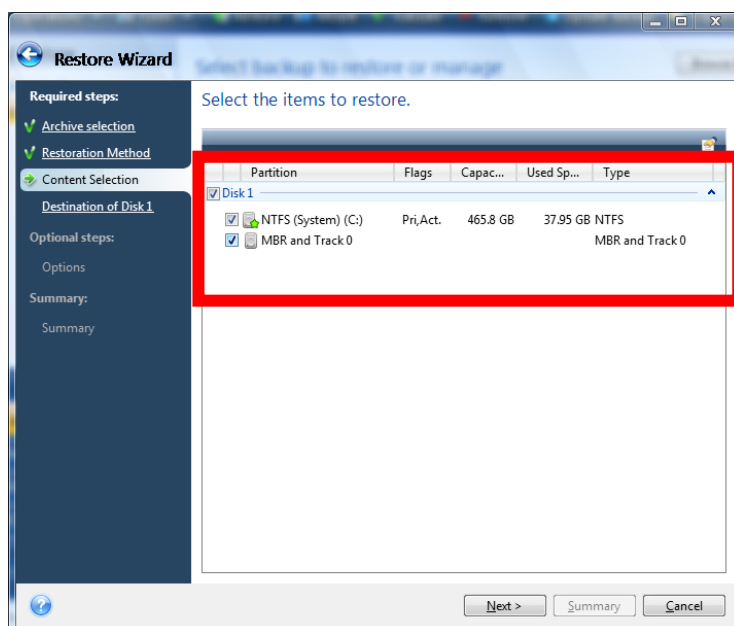
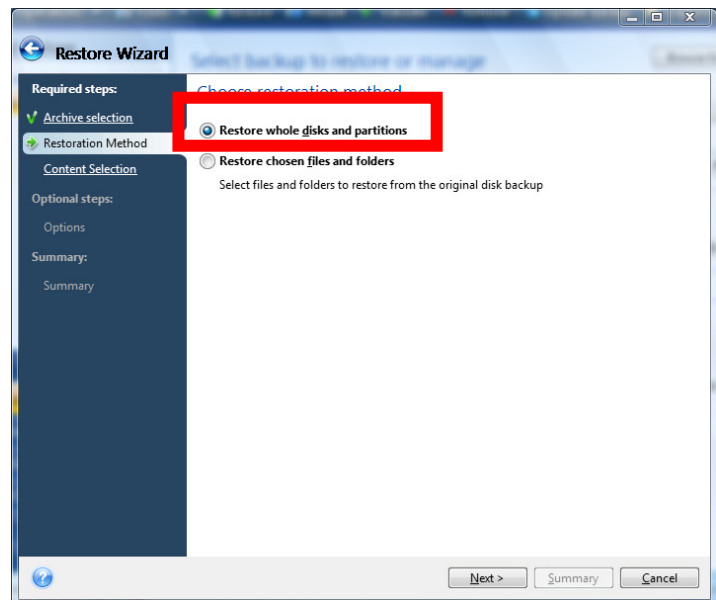
Browse for the complete image or recovery image you wish to restore and proceed to the **Restoration Method** windows by *clicking Next*.

At the **Restoration Method** window *select Restore whole disks and partitions*



If you only wanted to select specific files and folders from a complete image you can configure that here.

Click Next.

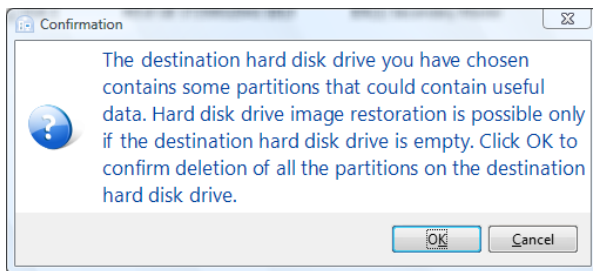


At the **Content Selection** window *check the Disk 1* checkbox.

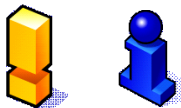
Click Next.

At the **Destination of Disk 1** window *click* the appropriate target drive, usually **Disk 1**. The partitions in the archive should be the same as those on the computer being restored as this is where the image came from in the first place.

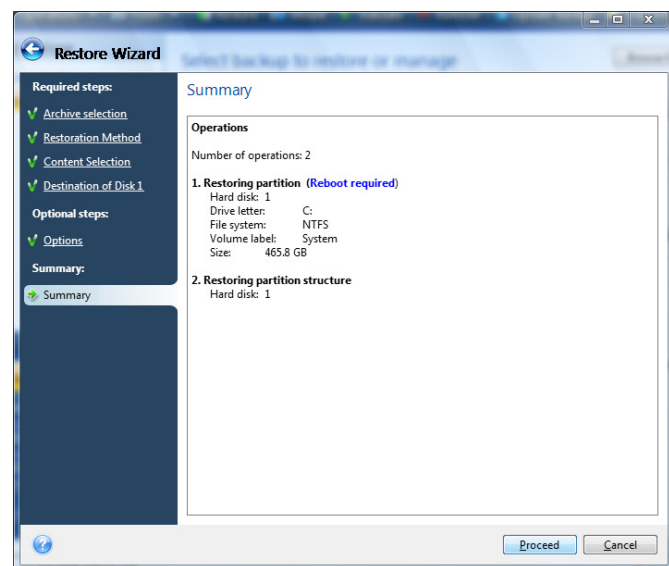
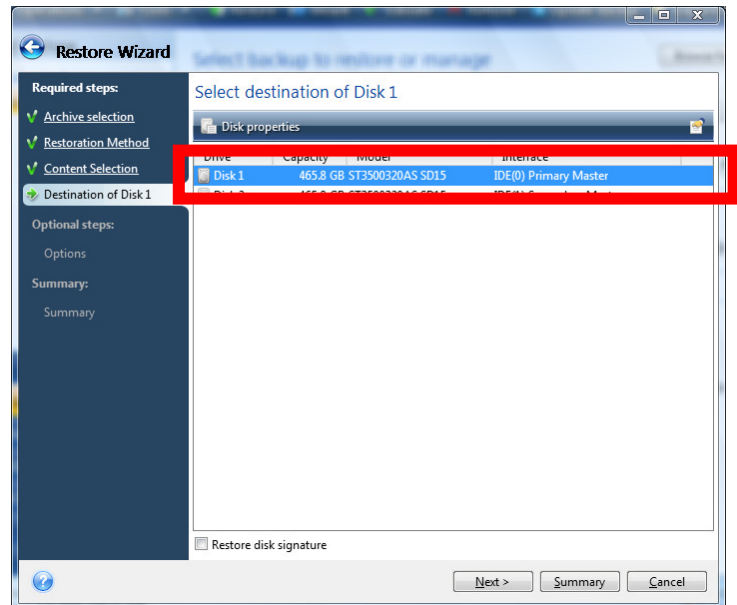
*Click **Summary*** and the following prompt may open. *Click **Yes***.



Review the restore configuration and *click **Proceed***.



After the image restore completes take the next logical steps as required to restore the data as described earlier in this document.



f) How Windows Task Scheduler is configured to automatically manage backup archives

To manage backups and create a second level of backup storage for PIN03-newPC that is not on the **D** drive the monthly Complete Image, System State, and Sunday Full Data backups are regularly copied to the USB drive by simple batch files that are configured to run automatically using **Windows Task Scheduler**.

Windows Task Scheduler may be found in a **Program Group** in the **Start Menu** as shown below.

A snapshot of each Scheduled Backup Task is included as well as the contents of the batch files for trouble-shooting purposes.

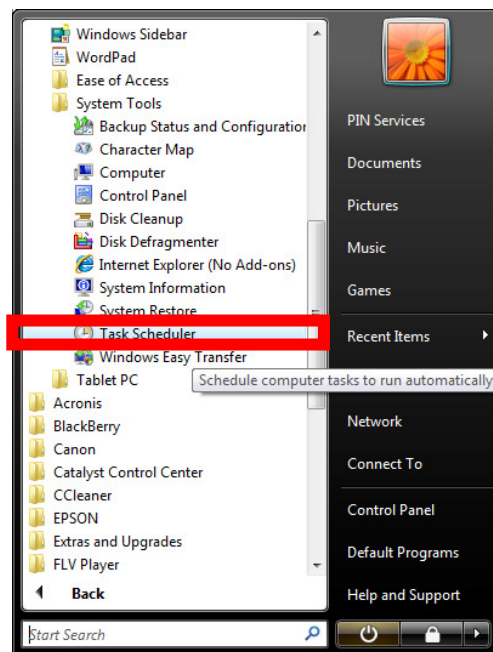
The batch files are configured to accomplish the following:

i) On the last day of the month at 2:00 am a copy of PIN03completeimage.tib and PIN03systemstatebackup are copied to the USB drive from the **D** drive on PIN03-newPC. The now 3 month old complete image is deleted and the 2 month old image is renamed PIN03completeimage.old. The now 3 month old system state image is deleted and the 2 month old image is renamed PIN03systemstatebackup.old.

ii) Every Sunday at 6:00 am (after the Full Data Backup runs) SundayDataFull.tib is copied to the USB drive from the **D** drive on PIN03-newPC. The now 3 week old Full Data backup is deleted and the 2 week old backup is renamed SundayDataFull.old



The most likely issue to create problems with backups and archive management is that as the size of backups grows so much that there is not enough time for one these dependent processes to complete before another is initiated. If overlap between backups and image copying results this might cause one or both of the processes to fail and jeopardize the backup system. Monthly checks of the system are essential to spot and resolve these issues before they arise.

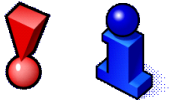


MonthlyCopy.bat

```
@ECHO OFF
CLS
cd /D B:\Scheduled_Backups\PIN03-newPC\
del Pin03SystemStateBackup.old
rename Pin03SystemStateBackup.tib Pin03SystemStateBackup.old
robocopy D:\Backups\ B:\Scheduled_Backups\PIN03-newPC\ Pin03SystemStateBackup.tib Pin03SystemStateBackup.tib
cd /D B:\Scheduled_Backups\PIN03-newPC\
del Pin03CompleteImage.old
rename Pin03CompleteImage.tib Pin03CompleteImage.old
robocopy D:\Backups\ B:\Scheduled_Backups\PIN03-newPC\ Pin03CompleteImage.tib Pin03CompleteImage.tib
```

WeeklyFullDataCopy.bat

```
@ECHO OFF
CLS
cd /D B:\Scheduled_Backups\PIN03-newPC\
del SundayDataFull.old
rename SundayDataFull.tib SundayDataFull.old
robocopy D:\Backups\ B:\Scheduled_Backups\PIN03-newPC\ SundayDataFull.tib SundayDataFull.tib
```



If you need to restore from an image that has been renamed as a .old file you will first need to rename the file with a temporary name and the proper .tib file extension so that True Image will recognize the file.

