# Take Control

## *of* Mac OS X Backups

*by* Joe Kissell

### Table of Contents (2.1)

$10

# Read Me First

Welcome to *Take Control of Mac OS X Backups,* version 2.1.

The data on every Mac should be backed up to protect you against theft, hardware failure, user error, and other catastrophes. This book helps you design a sensible backup strategy, make sense of the wide variety of backup hardware and software, and understand how to make your backups as painless as possible. This book was written by Joe Kissell, edited by Jeff Carlson, and published by TidBITS Publishing Inc.

The price of this ebook is $10. If you want to share it with a friend, please do so as you would a physical book. Click here to give your friend a discount coupon. Discounted classroom copies are also available.

You may not have the latest version of this PDF. To find out if there's a new version, click the Check for Updates link on the cover. Once you click the link, you'll be taken to a Web page where you can learn about any available or planned updates, and sign up to be notified about updates to the PDF via email. You may also find minor update information directly on that Web page.

## Path Syntax

This book occasionally uses a *path* to show the location of a file or folder in your file system. Path text is formatted in bold type. For example, Mac OS X stores most utilities, such as Terminal, in the Utilities folder. The path to Terminal is: **/Applications/Utilities/Terminal**.

The slash at the start of the path tells you to start from the root level of the disk. You will also encounter paths that begin with a tilde (**~**), which is a shortcut for the current user's home folder. For example, if a person with the user name **joe** wants to install fonts that only he can access, he would install them in his **~/Library/Fonts** folder, which is another way of writing **/Users/joe/Library/Fonts**.

## What's New in This Version

Version 2.1 of *Take Control of Mac OS X Backups* contains a number of differences from the 2.0 release. The most significant changes are these:

- Toned down recommendations for Retrospect.
- Changes to my recommendations for a backup approach in Decide on a Basic Backup Strategy (p. 9). In this section, I also now cover:
    - ◊ Backup software that can update archives on a byte-by-byte (rather than file-by-file) basis. See The Archive.
    - ◊ Information on peer-to-peer backups in Network backup approaches.
    - ◊ Additional backup software that can back up changed files without waiting for an explicit schedule to run. See the sidebar The End of Scheduling?.
    - ◊ Updated information about Time Machine based on details Apple has made publicly available. See the sidebar Time Machine and Archives (last page in this section).
- Slightly updated instructions pertaining to your Windows files backup strategy to reflect changes in Windows Vista (p. 48).
- In Choose Your Hardware (p. 53), I added:
    - ◊ New information about using Blu-ray Disc drives for backups in Optical Media.
    - ◊ Discussion of NDAS (network direct attached storage) devices in SAN, NAS, and NDAS.
    - ◊ Greatly expanded coverage of Internet Backup Services, resulting in changes in Joe's Hardware Recommendations.
- In Choose Your Software (p. 84), I added a new section, CrashPlan: Breaking the mold, and I discussed new and changed software options, along with a new bottom line, in Joe's Software Recommendations.
- Information on new and changed features in JungleDisk. See Appendix E: Backups with Amazon S3 (p. 167).

# INTRODUCTION

Nearly everyone understands why backups are important: hard drives fail, computers are stolen or damaged, and files are accidentally deleted. Backups are insurance against all these problems and more. If you've ever lost data—and I certainly have, on more than one occasion—then you know what I'm talking about. (And if you haven't lost data, you're computing on borrowed time.)

Apple feels so strongly about the need for good backups that they're building a backup feature called Time Machine into Mac OS X 10.5 Leopard, due to ship in October 2007. I talk more about Time Machine later (see the sidebar Time Machine and Archives), but for now, I want to make two important points. First, there's still plenty of time for disaster to strike *before* you upgrade to Leopard. And second, as wonderful as Time Machine may be when it arrives, it won't address every backup need you may have. Don't wait for Apple to solve your backup problems for you. Take control of your backups right now!

So, you know that backups are important, but when it comes to *how* to back up a computer, the options are so numerous that even the geekiest of us can find it difficult to wade through them and make intelligent choices. Which files should you back up? How often? Onto what media? Do you need to make bootable backups? How many sets of backup media do you need? Which backup software should you use? And what exactly do you do in case of a disaster, when you need to restore files from those backups?

There is no single correct answer to any of these questions. However, you can follow some straightforward steps to come up with your own answers. Regardless of the details of which hardware or software you use, your biggest concern should be *whether your data is safe*.

What some people call a "backup" is simply copying files from your hard disk onto another volume—either manually or using a utility of some kind. I'm a firm believer in the principle "something is better than nothing," so I don't want to make it sound as though this type of backup is useless. However, let me be candid: it's not enough. Too many different kinds of things can still imperil your data under such a scheme. A well-thought-out backup strategy will ensure the safety of your data—and helping you to develop such a strategy is one aim of this book.

Before we get started, however, I need to mention a few important caveats:

- I do not cover in any detail command-line software such as **`cp`** or **`rsync`**, except for one appendix (Appendix D: Unix-Based Backups). Although such tools can certainly be used to perform backups, my goal is to make the process as simple as possible—ideally, without requiring you to open Terminal or know anything about Unix. So this book concerns itself mainly with software that uses a graphical user interface (GUI).
- I've written this book primarily for people who need to back up either a single computer or a small network—not for system administrators who need to back up dozens or hundreds of machines. As a result, I say little about the expensive, high-end equipment typically used for backing up large networks—focusing instead on simpler devices you can purchase at your local computer store and plug directly into a stock Mac.
- Because every backup system is different, I can't give you explicit, foolproof, step-by-step instructions for setting up whichever hardware and software you purchase to perform your backups. But by the time you've finished reading this book, you should have enough background information to determine, with the help of your software's documentation, the preferences and settings you need in order to achieve your desired outcome.

I've been writing about Macs for well over a decade and using them much longer than that. During that time, I've experimented with a variety of backup systems for my own Macs, and as a consultant, I've installed backup systems for individuals and businesses. I've also spent long hours researching backup software and hardware and discussing backup strategies with my colleagues, including several other Take Control authors. These experiences have led me to form some rather strong opinions as to what constitutes a good backup system. I don't pretend that the method I use for my own Macs is the only one that will work, or that it's ideal for everyone. Rather than explore every alternative exhaustively, though, in the pages that follow I'm going to guide you gently but firmly into a fairly narrow set of options that should yield excellent results for the vast majority of Mac users.

While preparing this book, I tested a large number of backup applications under Mac OS X Tiger 10.4, but almost everything you read here should be applicable to older versions of Mac OS X too, from 10.1 onward (versions before 10.1 had serious limitations with respect to restoring backups). Although most of this material applies in a general way to machines running Mac OS 9 and Windows, I do not cover these other operating systems in any detail; but do see Windows Files and Volumes, which discusses backing up Windows when it's running on your Intel-based Mac.

## Quick Start to Mac OS X Backups

You can read this book in any order, but I recommend starting with the section Decide on a Basic Backup Strategy in order to understand the rationale behind the hardware, software, and setup advice I give later. Here are the components of a solid Mac OS X backup plan:

**Decide on a backup strategy:**

- Understand the crucial differences between a *duplicate* (a complete and usually bootable copy of your hard disk) and an *archive* (containing multiple copies of files as they existed at various points in time)—and why a good backup strategy includes both. See The Duplicate and The Archive.
- Learn the value of using a single system to back up all the Macs in your home or office. See Backing Up a Small Network.
- Find out how to deal with backup needs that don't fit neatly into the duplicate or archive categories in Consider Special Backup Needs. As appropriate, read about Digital Photos, Video and Audio, Version Control, Applications, Backing Up While Traveling, and Windows Files and Volumes.

**Choose your hardware:**

- Learn the pros and cons of each media type (from CD-R to camcorders) and how to estimate the amount of storage space you'll need. See Choose Your Hardware.
- Discover what's new (or newly affordable) in the world of Internet Backup Services.

**Choose your software:**

- Find out what to look for when comparing backup applications. See Choose Your Software for a feature overview, then consult Appendix A: Backup Software for details and sources. If you're tempted to eschew commercial backup tools and create your own command-line backup script, read Appendix D: Unix-Based Backups for a reality check.

**Set up your backup system:**

- Make a bootable copy of your hard disk and test it to make sure it works. See Set Up Duplicates and Test Your Duplicate.

- Configure an archive for your most frequently used data files, and verify that you can retrieve stored files. See Set Up Archives and Test Your Archive.
- Put your backups on autopilot so your files are protected even when you aren't paying attention. See Automate Your Backups.
- Learn how and where to store backup media, and discover what to do with the media when it gets full. See Mind Your Media.
- If disaster strikes and you need to recover files, be sure you're familiar with the steps in Restore Data from a Backup.
- Are you using Retrospect as your backup software? If so, be sure to read the detailed instructions for major Retrospect tasks in Appendix B: A Retrospect Primer.
- If you're called upon to set up a (mostly) idiot-proof backup system for a relative or friend, read Appendix C: Set Up Backups on Your Uncle's Mac in Seven Simple Steps.
- If you want to wrangle the Amazon S3 service into a backup solution, read Appendix E: Backups with Amazon S3.

**TIP** I recommend watching a very funny video about the importance of backups, featuring none other than John Cleese (The Minister of Silly Walks, Q, Nearly Headless Nick, etc.). Visit the LiveVault site: http://www.backuptrauma.com/video/default2.aspx

LiveVault, incidentally, sells Internet-based backup systems to businesses—unfortunately, their products don't run on Macs.

## Decide on a Basic Backup Strategy

I know a number of people who have made decisions about backing up their computers based on what hardware or software they already own. Others buy a product that's received good reviews and then figure out how to use it for effective backups. I believe these approaches are backward. If your data and your time are truly important, it makes sense to think about your needs first, then develop a strategy based on those needs, and finally choose hardware and software that fits your strategy.

After the first edition of this book was published, several readers commented that the strategy I suggest here, while perfectly reasonable, may be inappropriate for "low-end" users because it presumes a significant expenditure of money and effort. Less-advanced users, the argument went, just want a backup system that's inexpensive, easy-to-use, and effective. Don't we all! Unfortunately, there is no such thing. You know the old saying: "Cheap; good; fast—pick any two." The same goes for backups. I can tell you how to do them effectively or how to do them quickly and cheaply, but the less time and money you're willing to spend, the less safe your data will be.

With that in mind, I want to begin this strategy section with a quick, high-level overview of several approaches you might choose to take, depending on your tolerance for cost, effort, and risk (see **Table 1**, "Sample Backup Approaches," on the next page). Later on, I describe in detail each of the hardware, software, and strategic components of these options; I cover the "Ease of Use" approach in Appendix C: Set Up Backups on Your Uncle's Mac in Seven Simple Steps.

While the approaches I outline are just a few examples of the many paths one could take to performing backups, I personally feel the importance of protecting your data trumps all other concerns. Therefore, in **Table 1**, I outlined the Data Safety approach in blue, because I believe it is the approach that provides the best combination of safety and speed, though with somewhat high cost and less ease of use than you might prefer. I also outlined a new "Compromise" approach (in orange), which also offers excellent data safety—with a different set of trade-offs: low cost on the one hand, but slow speed and more awkward data restoration on the other.

**Table 1: Sample Backup Approaches**

| Major Objective | Suggested Approach | Risks and Trade-Offs |
|---|---|---|
| Saving Money | • Hardware: Your Mac’s built-in SuperDrive.<br>• Software: Data Backup ($30 with 50% off coupon).<br>• Strategy: Scheduled weekly duplicates and daily archives to DVD-RW or DVD+RW. | • You have no bootable duplicate, making it difficult to recover after a hard drive failure.<br>• You must be present when backups occur to swap media.<br>• Restoring files from an archive will be time-consuming. |
| Data Safety | • Hardware: Three external FireWire drives.<br>• Software: Retrospect Desktop.<br>• Strategy: Scheduled weekly duplicates and daily archives, alternating among drives; one drive always stored off-site.<br>• Optional: Use an Internet backup service for easy extra copies of important files. | • Significant hardware and software costs.<br>• Learning curve to set up and use Retrospect software.<br>• Inconvenience of moving drives around each week. |
| Ease of Use | • Hardware: A single external FireWire drive.<br>• Software: SuperDuper<br>• Strategy: Schedule duplicates to run automatically one or more times each week. | • No archives to protect you against file changes and deletions.<br>• Without redundant, off-site media, you risk data loss due to theft, fire, etc. |
| | **OR** | |
| | • For archives, use CrashPlan. It provides its own software and requires no hardware if you back up to their servers. | • No bootable duplicates.<br>• Can be extremely slow.<br>• Your data is unavailable if you lose Internet connectivity. |
| Compromise | Combine both of the “Ease of Use” strategies:<br>• Use CrashPlan to archive your most important files.<br>• Use SuperDuper to make weekly bootable duplicates to an external hard drive. | • Some backup and restoration operations may be slow, cumbersome, or both. |

**TIP** There's an even more secure level beyond the "Data Safety" option in the table on the previous page, but implementing it takes a bit of doing. Make these modifications to the plan:

- Use hardware-encrypted hard drives (see Choosing a hard drive).
- Using SoftRAID, partition each of the external drives into a volume for archives and a volume for duplicates (see Can a RAID Substitute for Duplicates?).
- Rotate the drives more frequently (say, once every 2 or 3 days) and keep one or more of them off-site at all times.

## Do You Need Duplicates?

Let's begin by assuming you have original (CD-ROM or DVD-ROM) copies of your operating system and all installed software. Now consider this question:

> If your hard drive suffered a complete failure, how much time could you afford to spend restoring it to working order?

If you use your computer to run a business, do your homework, or trade stocks, for example, your answer may be "a few minutes at the most." If no critical projects depend on a functional computer, you may be able to afford several days to restore it after a failure. Most of us are somewhere in between.

In the best case, it will take you several hours—and possibly a day or more—to reinstall a typical set of software onto a new or reformatted disk. However, if you do not have original copies of all your software, if you have a large number of third-party applications, or if you've customized your computer extensively, returning your computer to operation could take much longer.

The more you need to avoid that potential loss of time, the more you need to maintain duplicates (for more info, see The Duplicate, next page).

## Do You Need Archives?

Regardless of your need for duplicates, consider your answer to this much different question:

> If your computer were stolen, how difficult would it be for you to live without the data on it?

Do you have years of bank records, email, poetry, academic papers, photos, movies, and so on stored on your computer? If so, chances are your answer is "extremely difficult." On the other hand, if you use your computer only for casual Web surfing, playing games, and listening to music, living without the data on your computer may be little more than a minor inconvenience.

Although a duplicate includes a copy of your data, an archive includes many different versions of your data, making it much more likely that you'll be able to retrieve the information you need in the event of a problem.

The greater the amount of personal data on your computer—and its importance to you—the greater your need to maintain archives (for more info, see The Archive, ahead).

Though there may be some exceptions, the ideal backup strategy for most people consists of both duplicates and archives. I discuss each of these in the pages that follow.

## The Duplicate

Whether you call it a clone, a bootable backup, a mirror, or a carbon copy, a *duplicate* is a complete, exact copy of your entire hard disk that (if it's stored on, or restored onto, a hard disk) you can use to start up your computer if necessary. Duplicates are wonderful because they enable you to get back up and running extremely quickly—in some cases, with only minutes of down time.

Consider this typical scenario: you've duplicated your Mac's internal hard disk onto a FireWire drive. One day your computer won't start at all; the screen displays a blinking question mark indicating that it can't find a valid system. You suspect a catastrophic hard disk crash. No problem: you quickly hook up your backup drive and boot from that. Your computer will behave exactly as if it were running from the internal disk, with the exception that files added or changed since you performed the backup will be missing or out of date. You can then repair the internal disk—or if it's completely dead, simply replace it.

You might think it would take a while to make a copy of your entire hard disk, and you'd be right. But most software capable of making a bootable duplicate can also duplicate *incrementally*—meaning that after the first time, updating your duplicate to reflect the current state of your hard disk requires only copying files that are new or different. Because duplicates are so powerful and useful, I recommend that you make them part of your backup strategy.

However, due to the proliferation and simplicity of synchronization utilities, many people use duplicates as their *only* backup (see the sidebar Synchronization Utilities). This is a bad idea. Here's why:

- Duplicates provide no insurance against damaged or accidentally deleted files. If your hard disk is missing files, or contains damaged files, when you perform the duplication, those problems will appear in the duplicate as well.
- Duplicates quickly go out of date. Even while your backup is in progress, files may change. So if your only backup is a duplicate, you may increase your risk that backed-up files will not be current.

For these reasons, although I urge you to duplicate your hard disk regularly, you should supplement the duplicates with archives (as I describe in The Archive, just ahead).

**NOTE** An extra hard drive is certainly the *best* way to make a duplicate, but you can also duplicate a volume onto a disk image, which can be stored on removable media such as CD-R or DVD-R—and then restored onto a hard drive when needed. By the way, it is possible, though not easy, to make a bootable Mac OS X CD or DVD. Because this process goes far beyond normal backups, I do not cover it here.

## Sidebar Can a RAID Substitute for Duplicates?

*RAID* stands for Redundant Array of Independent (or Inexpensive) Disks; it's a way of combining multiple physical hard drives into a single logical volume using either software or a special hardware controller. One way to configure a RAID, known as *mirroring,* is to have the same data written simultaneously to two or more drives. If any one drive fails, another can take over instantly and seamlessly with no loss of data and no down time; you can then replace the faulty drive at your leisure.

I have nothing against RAIDs, and if you need to keep a mission-critical computer running without any hiccups at all, a mirrored RAID might be just what you need. However, I strongly believe that a RAID, by itself, is no substitute for multiple duplicates as described in this book. A mirrored RAID's best feature is also its Achilles' heel: because changes are reflected on all drives simultaneously, an accidentally deleted file will be immediately deleted on your "backup" drives too! (Stand-alone duplicates—especially if you maintain two or three of them—reduce this risk greatly.) RAIDs address the problem of spontaneous drive failures, but don't insure against human error, theft, natural disaster, or any of the other catastrophes that make backups so important.

That said, you *can* have your cake and eat it too (for a price). If you use SoftRAID (http://www.softraid.com/, $129), you can set up a RAID in which your internal hard disk is mirrored onto *two or more* external drives at once. You can then periodically rotate one of the drives off-site, where it will function as a stand-alone duplicate of your hard disk at an earlier state. When you plug it back into your computer, it will automatically synchronize itself with the remaining drives in the RAID. The beauty of this approach is that you never have to set up, schedule, or run backup software to make duplicates—it just happens automatically.

This scheme can even be expanded to include archives (see The Archive, just ahead). Using SoftRAID, it is possible (though somewhat awkward) to partition an external drive in such a way that one partition can be used along with your internal drive to form a mirrored RAID while another, non-RAID partition on the external can hold archives. Set up two external drives this way and you're in business—as close to a painless backup system as I can imagine.

**SIDEBAR**

### SYNCHRONIZATION UTILITIES

Lots of utilities—including several that bill themselves as backup tools—perform *synchronization*. As the name implies, synchronization means maintaining identical copies of a file, folder, or even an entire disk in two or more locations. Some synchronization utilities can run on a schedule, automatically "backing up" files from a location you specify to another volume. And some can create a bootable duplicate by synchronizing an entire disk to another disk.

There's nothing wrong with synchronization—in fact, it can be incredibly useful in certain circumstances, such as keeping your laptop's hard disk updated with documents you use frequently on your desktop Mac. As a quick and easy way of making an extra copy of certain files, it can serve as a type of primitive backup.

If you want to use a synchronization utility to make duplicates as part of your backup strategy, that is perfectly valid too. However, please do not mistake synchronization for a true backup—no matter what the utility's advertising says.

What's true of duplicates is equally true of individually synchronized files and folders: you get only the most recently modified version. You lack the ability to recover an older version of the file, which is a crucial part of a solid backup program. Also, if you don't notice that a file is damaged before synchronizing it to another volume, you may end up with two useless copies. If you synchronize deletions, you lose your insurance against accidentally trashing files. And it's all too easy to accidentally copy data in the wrong direction!

All that to say: a single copy of a single version of your data does not a backup make. By all means, synchronize if you wish, but not as a substitute for proper archives and complete, bootable duplicates.

## The Archive

Sometimes referred to simply as a *backup*, an *archive* contains copies of your files as they appeared at multiple points in time. If you want to see the version of a file that existed on your computer 2 weeks ago, an archive can deliver that—along with today's version and the version that existed a month ago.

An archive starts with a complete copy of all the files in one or more folders. The next time the backup runs, your backup software could make another complete copy, but because most of the files probably have not changed in the meantime, that would use up a great deal of space—not to mention taking a long time. So backup programs typically perform an *incremental* archive. This means that on subsequent runs, the software scans the files in the folders you've designated and copies only those files that are new (or newly modified) since the last backup. To be truly useful, archives should also be *additive,* meaning the backup program adds the new or changed data to the archive without overwriting the files already there. That way, you can retrieve many different versions of a given file, and if you delete it on your hard disk, you can still find it in your archive. Thus, what I refer to as an archive is technically an *additive incremental archive*.

Until recently, almost all Macintosh backup software performed incremental archives on a file-by-file basis. In other words, if just 10 bytes of a 10 GB file change, that marks the file as modified, and the whole file must be copied on the next backup run. Some software (such as CrashPlan), however, can perform *byte-level* incremental archives. If only 10 bytes of a file change, only those 10 bytes are added to the archive. The advantage of such an approach is that backups go much faster after the initial run and take up far less storage space; this is particularly important when backing up over the Internet. The disadvantage is that restoring a file requires the backup software to reconstruct it by putting together the pieces from all its incremental backups. If even a single one of those incremental bits were to become damaged or lost, you might be unable to restore the file.

**Note** Some backup programs use the term *archive* to describe files that have been copied to removable media of some kind for long-term storage and then deleted from the source volume.

Archives sometimes make use of a *snapshot*—a list of all the files in the designated folders at the time a backup runs. Even though a certain file may not be copied (because it hasn't changed since the last backup), it will appear in the snapshot list. You can easily see what the entire contents of a folder looked like at various arbitrary points in the past, and restore it to any previous state in a single operation.

After the initial full backup, archives usually take comparatively little time to run, making it easy to back up your data once (or even several times) each day. This ensures that your most recent backup is never more than a day old. Because they also offer tremendous insurance against accidental deletion (or change) and file damage, archives are an essential part of a good backup strategy. But archives alone are not an adequate solution. I say this for two main reasons:

- Because of the way archives are stored, they do not represent a complete, intact version of your entire hard disk. Ordinarily, an archive is not bootable (at least, not until after you've restored it to a fresh disk). If your main hard drive is completely dead, you won't be able to do any work at all until you've replaced it.
- It often makes sense for an archive to include only data files—not your operating system or applications (Archive strategy, ahead, discusses the pros and cons of such an approach). But reinstalling Mac OS X and applications from their original CDs or DVDs is a lengthy and cumbersome process that you could avoid (or speed up dramatically) with a duplicate of your hard disk.

**NOTE** **INCREMENTAL OR DIFFERENTIAL?**

Some backup programs distinguish between *incremental* and *differential* archiving schemes. Although not all software uses the terms in exactly the same way, the difference is typically that in an incremental backup, only the files changed or added *since the last time the backup ran* are added to the archive. With a differential backup, all the files changed or added *since the initial full backup* are added to the archive. Thus, differential backups take longer to run than incremental backups.

This distinction is important when backing up to tapes or other removable media, because it affects the speed with which a backup can be restored. When restoring from an incremental backup, the software must copy the entire initial backup and then step through each of the incremental backups to retrieve all the updated files. This can require a great deal of media swapping. A differential backup, on the other hand, can be restored more quickly because the software must copy only the original backup and the most recent one. When backing up to a hard drive, however, this distinction is less significant, because the random-access nature of a hard drive enables it to restore either sort of backup with roughly equal speed.

Archives protect you against inadvertent changes over time, but only a duplicate can get you up and running again quickly after a major problem. In other words, the best backup strategy includes both duplicates and archives.

That said, you can set up duplicates and archives in many different ways, depending on the hardware and software you have, the types and sizes of files you work with, and other variables. I make some general suggestions ahead under Joe's Recommended Basic Strategy, and provide detailed instructions later in Set Up Your Backup System.

## Scheduling Backups

I can say from personal experience that backups are far more likely to happen regularly if your backup software runs automatically on a schedule. And let me be quite clear: *regular* backups are the only kind that matter. I think it's fair to state this as a corollary to Murphy's Law: "The likelihood of suffering data loss increases in direct proportion to the elapsed time since your last backup." In other words, if you're performing all your backups manually, the one day you forget (or run out of time) will be the day something goes wrong.

One consideration in choosing a backup schedule is media management. For example, if you're backing up to a recordable DVD, you must be prepared to insert a blank disc whenever the schedule runs. Swapping media can be an intrusion into your normal routine (especially if that routine involves the frequent use of other discs in the drive you use for backups). On the other hand, if you schedule backups to run when you're not around, you must always think ahead and make sure the drive has the necessary media ready. If, on the other hand, you're backing up to a hard disk or network device that can stay connected all the time, this problem occurs less frequently, if at all.

Depending on the speed of your computer, which software you use, and how you configure it, you may find that your computer slows down significantly while backups are running. This could be an argument for scheduling backups for when you're not using the machine. However, if you do not leave your computer on all the time, you will need to take special care to ensure that it's on and ready when the backups are scheduled to run (see the sidebar Power Management and Backups, later, for more information).

How often should you back up your computer? And if you're making both duplicates and archives, how often should you update each?

No single answer is right for everyone, but as a starting point, my rule of thumb is that duplicates should be updated *at least* as frequently as major changes to your system (such as installing Mac OS X updates or new versions of applications), and archives should be updated every day you make minor changes (receiving email, modifying text documents, and so on). Thus, if you use your computer heavily every day, and often install new or updated software, you might opt for weekly updates of your duplicates and daily updates of your archives. On the other hand, if you use your computer only occasionally, the schedule could become once a month for duplicates and once or twice a week for archives. Under no circumstances do I suggest backing up less frequently than once a month or more frequently than twice a day—the risk is too high in the former case and the aggravation too great in the latter.

**TIP** Always update your duplicate just *before* installing system software updates. That way, if the new version of the software contains any serious problems, you can easily roll back your system to its previous state.

There may be some cases in which you could not afford to lose even a half day's work in the event of a serious problem, making twice-daily archives seem inadequate. If you're working on an important document, there's nothing wrong with copying it to another volume once per hour or as often as you feel it's necessary—or scheduling your backup software or a synchronization utility to do so for you. But updating an entire archive that frequently is likely to slow your work. (See Version Control for another approach to this problem.)

For more specifics about configuring your backup software to run on a schedule, read Automate Your Backups, later in this book.

## Keeping Multiple Backups

A sound backup strategy always includes backups of your backups! Picture this: you've diligently backed up your computer's internal hard disk to an external drive. Then one day, lightning strikes and *both* drives are damaged—or your home is robbed and all your equipment stolen. So much for your backup. Backup media can fail for all the same reasons your hard drive can fail. So having just one backup, in my opinion, is never enough. You should alternate between two or more sets of backup media for greater safety. If you've set up your backups to run on a schedule, this might mean using set A (a hard drive or a stack of CDs) every day for a week, then switching to set B (a different drive or stack of CDs) for each day of the following week, then switching back—and so on.

So are *two* sets enough? It depends. Most experts recommend using at least three sets, of which one is always stored off-site. (See Mind Your Media, later, for more detailed discussion about media storage.) But this advice was first given in the days when the media commonly used for backups was much less reliable than what's available today. And the cost of three sets of media—especially hard drives—can be hard to swallow for the average home or small-business Mac user.

In my opinion, except for mission-critical business use, two sets each of duplicates and archives should be adequate for most users. If you back up to hard drives, this can mean two drives, each of which is partitioned to store both a duplicate and an archive (see Partition Hard Disks). Of course, if you can afford a third set, your data will be somewhat safer—and your backup routine will be somewhat easier. In any case, you certainly should keep one of those sets in another location all the time (see Off-site storage, later in this book).

## Backing Up a Small Network

To this point, I've assumed that you're backing up a single Mac. But what if you have several in your home or office? How does this affect your backup strategy?

One approach is to back up each machine separately. This may involve keeping separate stacks of recordable CDs or DVDs beside each machine, or hooking up external FireWire drives to each one (though you could, of course, move a single high-capacity drive from one computer to the next). If your backup needs are relatively small, there's nothing wrong with this approach. But if you have more than a couple of machines—especially if their hard disks contain a lot of data that you can't afford to lose—a wiser strategy would be to back them all up at the same time over your network.

**NOTE** You do have a network, right? If you have multiple machines that aren't currently connected (whether by Ethernet cabling or AirPort wireless networking), you should hook them up. Not only does a network enable better backups, it makes transferring files and accessing the Internet much easier.

### Network backup approaches

In a network backup, one computer typically functions as the backup server. This is the machine to which your backup device(s) are physically connected. Files from your other machines are copied over the network onto each backup device. Network backups can proceed by four different methods:

- The server shares its backup volume (using *AFP*, *FTP*, or *SMB*), which the client machines mount as a volume in the Finder. Then each client machine uses its own backup application to back up files to the network volume (rather than a *locally* attached hard drive or optical drive). This is sometimes called a *push* backup, as each client "pushes" its data onto the network volume.

- Each client machine shares its hard disk (again, using AFP, FTP, or SMB). The server mounts each of these volumes in the Finder, and then the single copy of the backup application running on the server copies files from each of the network volumes onto its locally attached backup volume. This is sometimes called a *pull* backup, as the server "pulls" data from each of the clients onto its backup volumes.

- The server runs backup software that supports *client-server* network backups, and the other machines run client software that communicates with the server directly—without any of the machines having to share or mount volumes.

- Each computer on the network runs backup software that can act as both a client (backing up that computer's files to other computers) and a server (hosting the backed-up files from other computers)—again, with no need to share or mount volumes. When two or more computers use software that allows mutual backups of this sort, it's called *peer-to-peer* backup. CrashPlan is an example of a program that supports peer-to-peer backups.

**NOTE** Some SMB servers limit the size of any single file to 2 GB; others limit it to 4 GB; still others have limits as high as 2 TB. Because some backup software transmits *all* your data over the network as a single file, you may run into situations where you cannot back up more than 2 GB (or 4 GB) of data to an SMB server. If you can't persuade your system administrator to update the server software to a version that supports larger file sizes, you may need to use a different server (or different backup software).

Almost all backup applications support push and pull network backups, but I recommend against them. For one thing, network volumes can become disconnected for any number of reasons, and if a volume is unavailable when it's time for a scheduled backup, that backup will fail. A few applications can try to mount missing volumes for you (even remembering user names and passwords, if necessary), but even this is no guarantee of success. Push and pull backups are also inherently less secure than client-server backups, and are sometimes quite slow. Also, in the case of pull backups, file ownership may change in unacceptable ways, making bootable backups impossible. Sometimes push backups can be bootable, but it's a dicey operation.

Client-server and peer-to-peer backups require less effort, are more secure, and generally offer more flexibility. Often, client-server and peer-to-peer backup software also supports multiple platforms. Of the software covered in this book, CrashPlan, Retrospect, RsyncX, and BackupSW offer client-server backups; of these, only CrashPlan also performs peer-to-peer backups. Retrospect and BackupSW both support Mac OS X and Windows; Retrospect also supports Mac OS 9, while BackupSW supports Linux. CrashPlan runs on Mac OS X and Windows, with Linux support planned for the future.

If you need to back up a small Mac or Mac/Windows network, the two best options at the moment are CrashPlan and Retrospect.

CrashPlan comes in regular and Pro editions; definitely go with the Pro version, even though it's more expensive ($60 instead of $20, but see the coupon at the back of this book), because it has a few crucial extra features. You'll need a license for each computer that will be backing up its files, but if a computer will only serve as a repository for other machines' backups—and not be backing up its own files—that computer needs no license.

If you choose to use Retrospect (which comes in numerous editions), I recommend Retrospect Desktop, which includes a license to back up the machine on which it's installed, plus two more client computers (additional client licenses are available at $37 each, with volume discounts if purchased in packs of 5, 10, 50, or 100). You'll get the best results with the Backup Server script (see Set Up a Backup Server Script), using hard disks that are large enough for all the data on all the Macs (see Does size matter?).

### Special considerations

Besides selecting the right software, several other matters require your attention when planning a network backup system:

- **Media:** Although optical media or other removable storage may be acceptable for single-machine backups, for best results, network backups require storage devices that are always available. In other words, hard drives are the best bet for small networks. (See Choose Your Hardware, a few pages ahead.) Also, if you're making duplicates that you may later wish to boot from, be sure to partition the hard disks so that each startup disk on the network gets its own partition for a duplicate (I cover this in Partition Hard Disks).
- **Bandwidth:** You can perform a network backup using an AirPort wireless network, but even with an 802.11n AirPort Extreme network, real-world performance is such that you get less throughput than a wired 100Base-T Ethernet connection will give you—so backups will take longer, especially if you're duplicating an entire hard disk. In any case, you definitely want the highest-bandwidth network connection you can get. If your computer uses multiple network interfaces, open System Preferences, go to the Network pane, and choose Network Port Configurations from the Show pop-up menu. In the list that appears, drag Built-in Ethernet to the top and click Apply Now to ensure that the wired network is used in preference to AirPort when both are available.

**NOTE** Every network is different, but I have seen cases where Retrospect client-server backups are unreliable when client machines' IP addresses are dynamically assigned by an AirPort base station. If this happens to you, consider assigning (private) static IP addresses to each client.

- **Availability:** For a scheduled network backup to occur, both server and client machines must be turned on and awake. If your machines are currently not left on all the time, check the Energy Saver pane in System Preferences on each computer to ensure that it will not be off or asleep when backups occur. (For more info, read the sidebar Power Management and Backups, later.)

**SIDEBAR** **THE END OF SCHEDULING?**

Scheduling network backups for times when all machines are available can be a challenge—particularly if you have laptops that aren't always on the network. But explicit schedules have increasingly become "old school," as more-sophisticated options are appearing.

For example, Retrospect has a feature called Backup Server that constantly polls all the clients on a network. If it sees one that hasn't been backed up in at least 24 hours (or a period you specify), it performs the backup right away. That way, you needn't set up an exact schedule for each machine. Backup Server can be restricted to run only during certain hours on certain days, and it can also use any available, designated hard disk as a destination—so you don't need to figure out in advance when to swap media (to learn more, read Set Up a Backup Server Script.

CrashPlan runs in the background during the hours you specify (or all the time, if you prefer). During its active periods, it can back up files almost as soon as they change; you can set an interval (such as 15 minutes) after which any new or modified files will be backed up immediately. Similarly, Mozy can operate either on a schedule or automatically in the background, and both Versomatic and NTI Shadow can back up designated files each time you save them.

## Joe's Recommended Basic Strategy

What I recommend for most users is a two-pronged approach: periodically scheduled (say, weekly) duplicates of your entire hard disk, and even more-frequent (say, daily) archives of your data files. The duplicates will provide you with a complete, bootable copy of your hard disk, while the archives will pick up all the files that change regularly. Users with extensive photo or video data may need to go a step or two further—separating that data from their main backups and using special strategies to keep it safe without incurring enormous media and equipment expenses (see Consider Special Backup Needs, ahead, next main section).

### Duplication strategy

You should create duplicates (onto hard drives, ideally) of your primary disk and any other startup volume you normally use. If you have a single, unpartitioned hard disk, then you have only a single volume to worry about. If you have multiple partitions (or multiple internal or external hard drives) that contain bootable systems, I recommend making duplicates of *all of them*. If a hard drive fails, after all, it can take with it all the partitions it contains; and a disaster that wipes out a single drive could wipe out all of your drives.

**NOTE** When you create a duplicate, you copy *everything* from the source drive to the target drive—including, of course, all the files that make up Mac OS X. Therefore, there is no need to install Mac OS X on your external drive before creating a duplicate.

Most duplication software enables you to deselect individual folders you wish to exclude from a duplicate; some use selectors, exclusions, or both (see Selectors and exclusions in "Choose Your Software," later). Although you could make an argument that some files are not worth including in a duplicate (such as the cache files located in **`~/Library/Caches`**), the safest and most reliable tactic is simply to include everything. A file or folder that seems irrelevant to you may turn out to be crucial to the functioning of your system.

### Archive strategy

The archives you create should include all your important files (on each volume you use regularly, if you use more than one). The main question, though, is how you determine which files those are.

Some people suggest performing a full archive—that is, archiving every single file on your disk, just as you do when creating a duplicate. (Time Machine will follow this approach.) Others suggest performing a selective archive that includes only user-created data files, especially those that change frequently.

With a full archive, you have yet another copy of all your files besides your duplicates—an extra insurance policy. Restoring a full archive to an empty disk requires fewer steps, and less time, than restoring a selective archive (since in the latter case, you must restore a duplicate first). On the other hand, a full archive requires significantly more storage space, increasing your media cost, and takes longer to run. In addition, some backup software does not enable you to restore an archive as a bootable volume. My own preference is for selective archives, though I would not discourage you from performing a full archive if resources permit.

If you do choose to archive selectively, a good starting place is your home folder. By default, this folder contains most of your preference files, the files shown on your Desktop, and data for many of Apple's applications (Address Book, iCal, iTunes, iPhoto, Mail, Safari, and so on), among others. Although you can organize your hard disk however you want, Apple encourages you to keep all your user-created documents in the `~/Documents` folder or elsewhere in your home folder. So it could be that all your important, user-specific data files exist somewhere inside your home folder—and if not, presumably you are aware of the locations of folders you've created elsewhere.

But even if you have assiduously colored within the lines and kept all your personal data in your home folder, should you archive the whole thing? In some cases, the answer is no.

Because Apple designed the home folder as a catchall, it has the tendency to swell to enormous sizes. For example, if you maintain the default settings in iDVD, iMovie HD, iPhoto, and iTunes, all your digital media will be stored in your home folder. If, like me, you've imported your entire collection of CDs into iTunes, you may be looking at a huge Music folder (mine is nearly 50 GB, and that is small compared to some). If you store digital video on your computer, your Movies folder will certainly be even larger.

Although there's nothing *wrong* with adding all those files to your archive, it may not be strictly necessary either—because all those files should already be backed up safely as part of the duplicates you maintain. If, as in the case of imported CD tracks, digital photos, or video downloads, you modify those folders less frequently than you perform duplicates, you might consider saving time and space by excluding them from archives. But if in doubt—especially when it comes to irreplaceable photos and video—err on the side of including them; having an extra backup just may save your bacon one day. Purchases from the iTunes Store also require special handling as I describe next.

### SIDEBAR BACKING UP ITUNES STORE PURCHASES

Audio or video content purchased from the iTunes Store differs from music imported from CDs you own. Besides the fact that with downloaded files you don't have an original copy to serve as an extra backup, iTunes Store files include special copy protection to ensure that they can be played only by the purchaser, and only on one of up to five authorized computers. Because iTunes Store files are especially valuable, you should take extra steps to protect them:

- Always include iTunes Store tracks in your archive backups. If you import tracks from CDs as MP3 files, you can use your backup software's exclusion feature to filter out all MP3 files while keeping the AAC files (with an extension of .m4p) and MPEG-4 video files (with an extension of .m4v).
- Be sure to include the **`/Users/Shared`** folder in your archive backups as well; this folder contains hidden data required to enable authorization.
- If you suffer a severe crash and decide to erase your hard disk (in order to restore all your data from a backup), deauthorize your computer first. (This prevents you from losing one of your five authorizations if your computer turns out to require major repair.) To do this, open iTunes and choose Advanced > Deauthorize Computer. Choose Deauthorize Computer for Apple Account, and click OK. After restoring your backup, re-authorize the computer by opening iTunes and choosing Advanced > Authorize Computer.

Besides digital media, you may wish to manually exclude certain other files from an archive, if needed to save space (see Selectors and exclusions in the "Choose Your Software" section, later). For instance:

- **Downloads:** Applications and other files you've downloaded from the Internet can nearly always be downloaded again. It may not be worth dedicating significant media space to hold such files.
- **Cache files:** Temporary cache files, such as the ones stored in **`~/Library/Caches`**, are not crucial to an archive, as they will be recreated automatically if needed.

Before moving on to make decisions about what hardware you will need (see Choose Your Hardware), take a moment to Consider Special Backup Needs, such as photos, video, and version control.

### Sidebar Time Machine and Archives

Mac OS X 10.5 Leopard's Time Machine feature promises to take archives to an entirely new level. If you decide to use it, you'll start by designating a volume—an external hard drive, a second internal drive, or a network volume—to store your backups. You'll optionally tell Time Machine which files to exclude, and when to run its backups. Then, every day, it'll make a copy of all your files except the ones you excluded, leaving previous versions intact. So far, that sounds very much like ordinary archives.

Time Machine offers a couple of twists, though. First, when you need to restore a file, you won't have to open a separate application or search through confusing lists. You'll click an icon in your Dock or press a few keys, and find yourself looking at a groovy 3-D interface in which you can zoom backwards in time to see how any folder or volume looked on any day in the past. When you find the version of the file you want, you just select it and it's magically restored to its proper home. Second, Time Machine will work not only with whole files in the Finder but with individual entries in programs such as Address Book and iCal, as well as within applications such as iPhoto and iTunes. So you'll get much more granular control over restoring data than is possible today.

If Time Machine works as advertised, I may very well recommend abandoning other archiving programs in its favor. However, until Leopard is released, we won't know about some crucial details:

- Can Time Machine create bootable duplicates?
- Can you adjust the backup schedule to be more (or less) frequent than once a day?
- Can you use removable media (CDs or DVDs) as your destination?
- If you need to back up multiple computers over a network, will Time Machine be as convenient as a client-server program like Retrospect or a peer-to-peer program like CrashPlan?

Until I have answers to these questions and have had a chance to test Time Machine thoroughly, I can't say how enthusiastically I'll recommend it. But after Leopard's release, click the Check for Updates link on the cover; I'll make updated information available as soon as I can.

## Consider Special Backup Needs

Although duplicates and archives cover most situations the typical user will encounter, some people have special backup needs that don't quite fit the mold. I'm thinking, for example, of users with large numbers of digital photos and those who work extensively with the huge files required for digital video or pro audio applications. Other special needs may include using version-control software to save copies of your files more frequently than archives would permit, making backups of certain applications, backing up your data (especially photos) while traveling, and backing up Windows volumes on Intel-based Macs. All these situations may require additional steps beyond setting up conventional duplicates and archives.

### Digital Photos

Many people, when asked what one item they would try to save if their house were burning down, would answer "my photo album"—because furniture can be replaced, but memories cannot. The same thing is true of the memories stored on your hard disk in the form of pictures you've taken with your digital camera.

Most of us have at least a few digital photos on our computers. But some people take pictures constantly, and feel justifiably concerned about entrusting this irreplaceable data to their computers. Also, digital camera resolution is constantly on the rise—meaning the next new camera you buy is going to require more space for the same number of images as your previous one. Your new mobile phone probably has a camera too. As the number and size of your images increases, you may find that duplicates and archives alone don't entirely meet your backup needs.

For one thing, it can be extraordinarily difficult to find just the right photo from among thousands of similarly named files when it comes time to restore your data from a backup. Although Spotlight can use keywords and other metadata to help you find photos when they're on your hard disk, it won't help you when they're on a stack of DVDs. (For solutions to this problem, see Cataloging software, later.)

Photos are also among the files you're most likely to share with other people. If you've ever created an online photo album using iPhoto, iWeb, or .Mac HomePage, you know how easy (and addictive) photo sharing can be. Although the files you've shared on the Web do, in a sense, constitute a backup of the ones on your computer, you probably haven't shared *all* your files online—and you most likely uploaded low-resolution copies of the images anyway. Wouldn't it be great if you could back up all your photos online, and still have the ability to share just the ones you want? (You can! I explain how in Photo-sharing services.)

Finally, let's not forget that photos are especially valuable. Although you wouldn't enjoy spending months rewriting The Great American Novel, it's at least possible. Recreating photos of a new baby or an important life event, on the other hand, simply can't be done.

Luckily, numerous tools, services, and strategies exist for the express purpose of making photo backups as painless and secure as possible.

## Photo backup strategy

If you've determined that your digital photos require special backup attention, consider these options in addition to (or, if you prefer, instead of) duplicates and archives.

### *Cataloging software*

I have nothing at all against iPhoto—in fact, I quite like it. It even has the built-in capability of backing up your photos to optical discs (although it's a manual process). But iPhoto is a consumer-level application that wasn't designed for the needs of professionals—or amateurs who have tons of photos and take their images seriously. When your photo management needs outgrow iPhoto, you can move up to serious image-cataloging software.

For Mac OS X, you have two main choices: Microsoft Expression Media, formerly called iView MediaPro (http://www.microsoft.com/Expression/products/overview.aspx?key=media, $299) and Extensis Portfolio (http://www.extensis.com/, $200). Both have similar feature sets, including flexible searching, contact sheet creation, and much more. Crucially for our purposes, they maintain thumbnail catalogs of all your images even if you move the original files to another volume (and even if that volume happens to be sitting at the bottom of a pile of junk in your closet).

**NOTE** Apple's Aperture application (http://www.apple.com/aperture/, $300) and Adobe's Photoshop Lightroom (http://www.adobe.com/products/photoshoplightroom/, $300) also contain cataloging and archiving tools for digital photos, though those are a small part of the programs' capabilities, and they're overkill if you need just those features.

By using one of these applications to back up your photos (whether or not you delete the originals), you gain the ability to search a visual index for your images. When you find the one you want, the software will tell you which DVD, CD, or hard drive it's stored on.

On the downside, these third-party tools are more expensive than iPhoto, and they are not quite as easy to use; they also lack iPhoto's integration with applications such as Mail and iDVD. But these are minor complaints. For heavy-duty photo backups and cataloging, Expression Media and Extensis Portfolio can't be beat. (And if I had to choose between the two, I'd go with Expression Media: I prefer its interface and feature set, despite the higher price.)

If you choose one of these tools, I suggest excluding photos from your regular archives and using the cataloging software's built-in backup tools for your photos instead. It'll be slightly more effort, but you'll dramatically increase the ease with which you can find and restore your photos. You can also, optionally, delete older photos from your hard disk after you've backed them up—you'll save room on your startup volume while still maintaining a handy catalog of thumbnails.

#### Photo-sharing services

If you're a .Mac member, you probably know that you can create Web pages to share your photos online. Of course, you pay for that privilege, and even with 10 GB of storage space (or as much as 30 GB, which you can get for an additional fee), you may not have room for all your photos on your iDisk. Internet backup services (see Internet Backup Services, later) will gladly sell you more space on a server, but such services won't enable you to share your photos on the Web.

**TIP** I cover sharing your photos on the Web using iWeb, iPhoto, and .Mac HomePage in detail in my ebook *Take Control of .Mac* (http://www.takecontrolbooks.com/dot-Mac.html).

Never fear, though: several companies provide *unlimited* storage for your digital photos, along with complete control over which ones are shared and with whom, for as little as zero dollars! (Yes, there's a catch, but it's surprisingly minor.)

Photo-sharing sites spring up all the time. Here are some of the more popular ones I knew of at the time I wrote this:

- **Flickr:** Basic accounts, which limit monthly uploads to 20 MB of bandwidth usage and store only scaled-down images, are free. Flickr Pro Accounts cost $25 per year and include a generous 2 GB monthly upload limit and unlimited storage of full-resolution images.
  http://www.flickr.com/

- **Fotki:** Free accounts give you 50 MB of space. Premium accounts, which cost $50 per year, provide unlimited storage and a number of advanced features.
  http://www.fotki.com/

- **Kodak EasyShare Gallery:** Membership is free and includes unlimited storage, but with a catch: you must make a purchase of some kind (such as prints from your photos or other merchandise) at least once per year. Purchases need not be large, however, so if you're likely to purchase some prints anyway, it's effectively free.
  http://www.kodakgallery.com/

- **Phanfare:** This service costs $7 per month—or, if you prefer, $55 per year or $300 for a lifetime subscription. It lets you store an unlimited number of photos and videos, though individual photos are limited to 20 MB in size and individual videos are limited to 2 GB (or 10 minutes).
  http://www.phanfare.com/

- **SmugMug:** Membership levels are Standard ($40 per year), Power User ($60 per year), and Pro ($150 per year). All levels include unlimited storage; higher levels provide more customization options and higher monthly traffic quotas.
  http://www.smugmug.com/

- **Snapfish:** Like the Kodak EasyShare Gallery, this service provides free, unlimited storage as long as you make at least one purchase annually.
  http://www.snapfish.com/

Except for Fotki, all these services offer Mac-compatible photo upload software; Fotki Premium members can upload photos via FTP.

Beyond the basics of photo storage and sharing, these sites differ in the range of features they offer. Most offer prints of your digital photos for a fee; some will send you CDs or DVDs with backups of your photos, too. And the range of additional services is varied and extensive; visit the sites and try their free trial memberships to get a feel for what they can do. (My favorite is SmugMug. The service is reasonably priced for unlimited storage, has the features I need, and offers upload software that integrates easily with iPhoto.)

Considering that you can back up *all* your photos for as little as a few dollars per year using one of these services, it's almost a no-brainer. In fact, even if you ignore all the other advice in this book, please take the easy step of backing up your photos with one of these services. Although you may already include your photos in your duplicates and archives, another off-site backup never hurts—and you'll get easy photo sharing as a bonus. The only people who might want to be circumspect about these services are those without broadband Internet connections: uploading photos over a slow connection can take a long, long time.

Finally, remember that you may wish to back up your photos while still on vacation. For my recommendations about how to do that, read Backing Up While Traveling.

**TIP** For more info on backing up your digital photos, see my article "Make your images last" in the August, 2005 issue of Macworld: http://www.macworld.com/2005/07/features/photosmanage/.

## Video and Audio

Video files consume an enormous amount of disk space, and when you're working on editing a large video project or producing DVDs, the file sizes can become truly staggering. Add HD video content to the mix, and the file sizes balloon even further. Because of the sheer quantity of data you may generate, conventional duplicates and archives may not make the most sense. You're also likely to create numerous intermediate files between the raw footage and the final product, and deciding whether or how to back up that data can be challenging.

All this is equally true for those working with audio production, especially when your Mac functions as a multitrack recorder; it also holds for photographers working with gigantic, ultra-high-resolution images and several other categories of user.

So ask yourself this question:

> Do you frequently generate more than a few gigabytes of new or modified files in a single day?

If you're working with large video, audio, or still image files, the answer is likely yes. Read on for my recommendations.

## Video and audio backup strategy

If you regularly edit video on your computer, you may need to adjust your backup strategy to account for the special requirements of these jumbo-sized files. (Although I speak of "video" throughout this section, keep in mind that essentially the same issues and strategies apply to pro audio files and other extra-large documents.)

### *Video data types*

Think about the different forms video data may take:

- The original footage you shot with your camcorder—stored on whatever medium your camera uses: analog or digital tape (usually), or (occasionally) a DVD, built-in hard drive, or flash memory device.
- The raw files you transferred from the camcorder onto your hard disk.
- A project (in, say, Final Cut Pro or iMovie) containing a particular selection of video files plus all the information about how they fit together—not to mention music, narration, titles, special effects, and so on. In the case of Final Cut Pro and Final Cut Express, this also includes video and audio cache files, which could be located on a separate connected hard disk.
- A final, rendered movie, in one or more sizes and formats (DVD-ready, Web-ready, etc.). Needless to say, a given project may be "final" and still undergo changes later!

Which of these items should you include in your backup plan—and how?

- **Original footage:** Let's begin with the tapes from your camcorder. The work you put into editing video clips into a finished product is valuable, but in most cases, the original footage is irreplaceable. However time-consuming or painful it may be, you could recreate a project from scratch, as long as you had a copy of the source material. So, when thinking about video backups, give special weight to that original footage.
- **Raw files on your hard disk:** If you've copied the data from your camcorder to your computer, you now have two copies. But not all your raw footage will end up in a movie; if you're like most people, you probably shoot a lot of extra material you'll never want to look at again. Those raw files—before they become part of an actual movie project—are generally the least important to back up (assuming, naturally, that you still have the originals).
- **Project files:** The project files are perhaps the most challenging component, because you may modify them many different times. If you include these files as part of a standard additive incremental archive, you may find (depending on which video editing and backup software you use, and several other variables) that even a tiny change to a 20 GB video project results in the *entire* 20 GB file being *added* to each day's archive. If you happen to have a few terabyte or larger drives sitting around, that's not much of a problem, but such drives are still on the expensive side for most of us.

  Archives of your project files can be worthwhile, but such archives generally benefit work in progress more than older material. In other words, once you've completed this year's holiday DVD and sent it off to your family, you're unlikely to need all the intermediate versions of the project files again—though you may want the final project files later on.
- **Final, rendered movies:** As for the final product, it goes without saying that it's important, but as long as you still have the project files, you can recreate it if necessary. So it's a bit less crucial to back up than your project files.

### *Recommendations*

Although I can't offer a one-size-fits all approach to video backups, I would like to make some recommendations that you can tailor to your specific situation. All these suggestions presume that you're already making duplicates and archives of your non-video data:

- Exclude video data from your regular archives and duplicates. That'll make those backups more manageable, saving both time and media.
- Assuming your camcorder stores its data on removable media, *always* keep the original media—don't overwrite it for your next project, even though you've copied the data to your computer. Instead, treat that tape, DVD, or cartridge as though it were a film negative and store it in a safe place. You'll use up more media this way, but you'll have an automatic backup of all your footage.
- Consider making a duplicate of each piece of original media (if your video equipment provides a way to do so). Remember, every piece of backup media is subject to deterioration over time, so an extra copy is never a bad idea.
- You probably do *not* need to back up video data that you've copied from your camera to your hard disk but are not actively using. (After all, you already have one or two backups of this data in the form of your original tapes and, perhaps, duplicates of them.)
- As for your active video projects, at minimum, you should use your backup software to copy them onto an external hard drive and update that copy periodically. Better still, set up an archive of your active video data—separate from your regular data—on a hard drive. This will give you at least a few intermediate versions of your work in progress, should you need to go back to an earlier one. (How often you update this archive will depend on your available disk space.)
- When you've finished a project and know you won't be editing it again in the near future, copy all your project files onto optical media—preferably, two or more sets that you'll store in separate places. Then delete the project files from your hard disk and recycle your video archive disk by erasing and starting over again with a full backup of your next project.

- If your finished product is a DVD, be sure to save an extra copy of that DVD as a backup. For movies in other formats, consider copying them manually onto optical discs for long-term storage.

**TIP** Don't be tempted to think that your final DVD project is also a backup. DVD video is compressed with MPEG-2 encoding, which means the DVD you watch on television contains video at a lower quality than what you edited. If you need to go back and re-edit it, the results won't be as good as if you used the original source material from the camcorder or hard disk. Plus, you can't easily pull video from a DVD disc; you need special conversion software.

In other words, treat your video data with the same care you give all your other files, but don't get hung up on long-term storage of every single edit you make of every movie. The most important things to back up are your original footage, archives of work currently in progress, and your final project files.

## Version Control

Although archives are tremendously useful for keeping multiple versions of files, they only store new versions when your backup runs—perhaps once a day. In some cases, that's not enough. Although you may modify and save a document 50 times in the course of a day, an archive may enable you to go back to just one of those versions later on. Suppose you added a chapter to your dissertation yesterday morning and then accidentally deleted it before saving it for the last time at the end of the day. Even a daily archive can't bring back that missing material.

The problem becomes especially acute when you're not the only person working on a document. If you and one or more coworkers are all modifying a document that's kept on a shared volume, for instance, one person could change or delete sections that another person still needs.

### Programmers' tools

Programmers working in groups often use version-control software to eliminate all these problems. Open-source software such as CVS (Concurrent Versioning System) and Subversion, and commercial software such as Perforce, can be configured to retain a copy of each file every time it's saved (or as often as the user manually *commits* the file) and either prevent or coordinate changes to a single file made by more than one person. (For links to further information on these programs, see Version Control Software.) Unfortunately, the Mac programs available for working with these systems have interfaces only a programmer could love. And, for most of us, their advanced features are way too complex for day-to-day use.

### Application-specific version control

Some Mac applications feature a built-in capability to save multiple versions of each document. The best-known example is Microsoft Word. In Word, choose File > Versions and click Save Now to store a record of the current state of any document; check the Automatically Save a Version on Close box to update the internal list of changes whenever the document is closed. To return to an older version of the document, choose File > Versions again, select a version in the list, and click Open.

Although this feature can be helpful, it's limited. First, it works only when you explicitly click that Save Now button; simply saving files in the usual way doesn't add revisions to the list. Second, Word stores all the revisions within the same file, so if that file becomes damaged, you could lose every version you've stored. And finally, it works only within Word; you're on your own for documents in other applications.

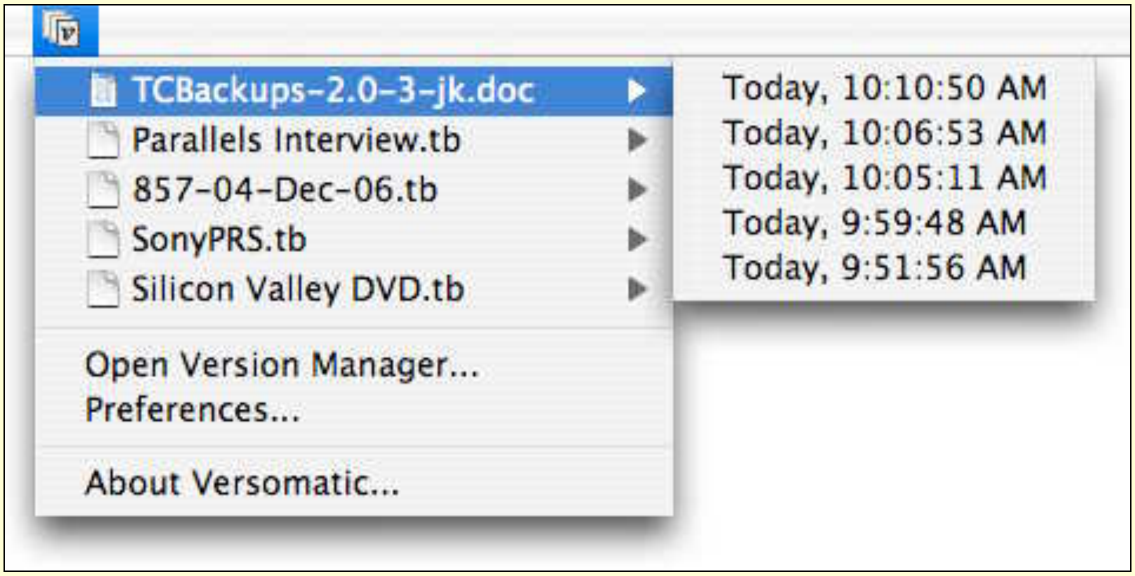
### Versomatic

Versomatic is an unusual type of version-control software that's easy enough for anyone to use, works with any file type, and stores copies of your files every single time you save them. A newcomer to the Mac world, Versomatic has been available as a Windows application for some time. It sells for $50. http://www.acertant.com/web/versomatic/

After installing Versomatic, you tell it which folders and volumes it should watch and which it should ignore; you can also specify particular file types to track or ignore anywhere on your hard disk. Other settings include how many revisions of each file to store, the maximum disk space Versomatic can use to store revisions, and where all those extra copies of your files should be kept.

If you decide you want to retrieve an older version of a file, you can do so in any of several different ways. The simplest is to right-click (or Control-click) the file in the Finder, go to the Versomatic submenu of the contextual menu, and choose the date and time you want. Versomatic immediately opens that version of the file. (This approach vaguely reminds me of what Time Machine will offer, if not quite so snazzy.) You can also click the Versomatic icon in your menu bar to quickly open any saved version of recently modified files, as shown in **Figure 1**.

**FIGURE 1**



The Versomatic menu gives you quick access to revisions of recently modified files.

Because Versomatic backs up only certain files, and only when you save them, it's not an all-purpose backup program. However, over time, as you resave all your important files, Versomatic could conceivably replace regular archives for some people. The benefit is that you never have to wait for your backup software to run; the downside is that you'll use up a *lot* of disk space, because Versomatic stores a *complete*, uncompressed copy of a file every time you save it. For this reason, and to protect your revisions from all the usual problems that could affect your startup disk, I recommend storing your Versomatic data on an external hard disk.

**NOTE** Another backup program, NTI Shadow, also offers the option of archiving files every time they're saved, though it doesn't boast Versomatic's convenient interface for retrieving older copies. See Archiving software.

### Do you need version-control software?

If you work with certain documents over a long period of time and want to be sure you can go back to any previous state, then version-control software can give you greater peace of mind than even the best archives provide. And, as version-control software for Mac OS X goes, Versomatic can't be beat for convenience and ease of use. I use Versomatic to track only specific types of documents, such as books and articles I'm writing, for which I can't afford to lose even an hour of work. But in those cases, I'm extremely glad for the extra security.

## Applications

If you create duplicates of your hard disk, they will naturally include all your installed applications. Ordinarily, I advise excluding applications from archives, however, as they seldom change, take up a lot of media space, and are easily reinstalled from CD, DVD, or a downloadable file.

However, in some situations, you may want to back up certain applications separately from your duplicates and archives. Consider these scenarios:

- You download an update to an application, but after installing it, discover that it has a serious bug or incompatibility. Downgrading to the previous version is sometimes difficult.
- You've lost your original media for an application, and are unable to replace it or download a copy of the software.
- You rely on software that has been discontinued or is no longer supported by its developer, and want to be certain you don't lose it to a disk crash or other problem.
- You decide to delete an application because you seldom use it or are running low on disk space, but want to be sure you can retrieve it if necessary, even if you don't have its original installer.

In cases like these, you may wish to make backup copies of the applications and their supporting files—either manually or with your favorite backup program. Doing so can be tricky, because you may need more than the application file itself; applications frequently store support files in various locations on your hard disk.

### Application backup strategy

If you want to make backups of any of your applications, I suggest starting with a rather unintuitive step: using software designed to *delete* applications completely!

Let me explain, using iDVD as an example. The iLife installer puts iDVD in your **`/Applications`** folder. It also puts a huge folder in **`/Library/Application Support`**, adds preference files in both **`/Library/Preferences`** and **`~/Library/Preferences`**, and puts two or more receipt files in **`/Library/Receipts`**. Other applications similarly store a variety of files in numerous places on your disk. Searching for all those pieces manually is both time-consuming and error-prone, but you'll want to find them all to ensure a successful backup of the application. The easiest way I know of to do this is to use any of several utilities that specialize in locating, and deleting, all the components of an application. The trick is to stop at the step where the utility has identified all the pieces and *not* click that Delete button! Instead, use that list to tell you which files you must back up.

Among the utilities that can perform this function are the following:

- AppCleaner: http://www.freemacsoft.net/AppCleaner/ (free)
- AppDelete: http://reggie.ashworth.googlepages.com/appdelete (free)
- AppZapper: http://www.appzapper.com/ ($13)
- CleanApp: http://synium.de/cleanapp/index.html ($10)
- Uninstaller: http://macmagna.free.fr/Uninstaller/ ($25)
- Yank: http://www.matterform.com/mac_software/uninstaller/ ($20)

If you don't plan to use the backed-up programs regularly, I suggest storing them on CD or DVD, rather than mixing them with backups you store on hard disks—you'll be less likely to delete them inadvertently. But make at least two copies; optical media occasionally develop errors that prevent their data from being read.

## Backing Up While Traveling

It's relatively easy to back up your data when you're at home or at the office: you can set up a system that fetches data from one or more computers and stores it on the media of your choice automatically. But when you're away from your usual equipment, backups become more difficult. Furthermore, you might want to back up some data—specifically, digital photos and videos—even when you're traveling *without* a laptop.

### Traveling with a laptop

If you bring your computer along, you face two main questions. First, do you back up your data to local media (DVDs, say, or an external hard drive), or use the Internet to back up to a remote location? Second, if you do choose to back up remotely, what's the best way to do so safely and efficiently?

**NOTE** I cover a variety of options for backing up your laptop while on the road in an August 2006 Macworld *article,* "Mobile backup tips": http://www.macworld.com/2006/07/secrets/augmobilemac/.

#### *Local or remote?*

Backing up your laptop directly onto a hard drive or to optical discs is invariably quicker than backing up over the Internet. You also avoid any worries about sensitive data being intercepted in transit, and you have a handy copy of your data available for instant restoration if you need it. On the other hand, if your laptop is stolen, left in a car trunk, or otherwise lost, you're likely to lose all your backups at the same time. So a word to the wise: if you choose to keep your backups with you, at least keep them separate from your computer.

Local backups are best for people who generate large volumes of data—videos, for example. If you create several gigabytes of new files every day while away, backing up remotely might simply be too time-consuming. A local backup is also the only good option if you're going somewhere without high-speed Internet access. Backing up files over a dial-up connection is almost invariably more trouble than it's worth.

On the other hand, if you generate only a modest amount of data on the road and fast Internet access is available (especially if it's *free* fast Internet access!), backing up remotely is an excellent option, because all your data is kept safely off-site.

**TIP** Regardless of which method you use, I strongly suggest performing a full backup just before you leave for your trip. That will minimize the amount of data you have to back up during your trip, and give you a safety net in case your laptop is stolen.

### *Local backups*

The CD or DVD burner built into your Mac laptop makes optical media the most convenient option while on the road. You can store a number of blank discs comfortably in the computer's carrying case and can perform backups without needing any external hardware. Keep these tips in mind:

- Even if you normally back up every file on your Mac, save time and media while traveling by backing up only your most important files—specifically, those you've worked on during your trip.
- If you need to back up just a few files each day, you can get away with inserting a blank disc, manually dropping files on the disc's icon, and using the Finder's File > Burn Disc command. Otherwise, you can use backup software just as you would normally. But configure it to back up only those files that have been modified since your trip began.
- Retrospect can keep adding to a CD or DVD until it's full. If you use other backup software, you may use up a lot of discs backing up relatively few files per session.
- If your backup software supports encryption, use it. You wouldn't want someone who stumbles upon your backup discs to get easy access to any personal information stored in your files.
- If you're going to be gone for more than a few days, consider mailing one of your backup discs home once a week or so; that gives you an additional measure of safety.

Another alternative is an external hard drive; for portability, I suggest a bus-powered (no AC adapter required), pocket-sized model. See Choosing a hard drive for more details. In a pinch, you can press your iPod into service as a backup device while traveling, though you'll have to sacrifice space you'd otherwise use for music or videos. You can also use a flash drive (see Flash Drives), but the ratio of cost to capacity is significantly worse than for hard drives—even the more-expensive pocket drives—so they're not my first choice.

### *Remote backups*

You can go about backing up your files remotely in any of several different ways, depending on your needs and circumstances.

For backing up a relatively small quantity of data, consider using an online backup service. For example, CrashPlan can back up your laptop's files to the company's own servers (called CrashPlan Central), to another computer you own back at home or the office, or to a friend's computer anywhere on the Internet.

Alternatively, use your iDisk if you're a .Mac member (see iDisk), but be sure to encrypt your files before uploading them, as Apple does not currently offer secure iDisk connections.

Finally, if you have conventional backup software running on a server back at home or the office (see Backing Up a Small Network), you may be able to connect to that server remotely, but that's not as easy as it may sound. "Push" backups work only if you can mount your backup server's volumes remotely; "pull" backups work only if your server can mount your laptop's volume remotely. Sometimes this is possible, but often not—your firewall at home must enable access to the necessary ports, and the ISP providing your remote access must also permit file-sharing access over their network. You also run a risk that your files may be intercepted in transit by a hacker, unless you take extra steps to encrypt the network link between your laptop and your server.

Client-server backup software, such as Retrospect, normally polls only the local network for available clients. In some cases—for example, with the more-expensive Retrospect Workgroup or Retrospect Server packages—you can manually enter an IP address for a computer outside your local network. However, if you're traveling and don't know what IP address you'll have at any given time, this method is problematic.

A possible solution is to use a dynamic DNS service, such as the one provided by easyDNS, to assign your laptop a domain name whose IP address changes as needed, and then enter that domain name in Retrospect (http://www.easydns.com/dynamicdns.php3). In most cases, CrashPlan can figure out how to contact the other computers you (or a friend) are running it on, even if they don't have routable IP addresses.

You can get around most difficulties in contacting your backup server remotely by using a VPN (virtual private network) connection to your home network, but the details of setting up such a system go beyond what I can cover in this book. To learn how to do this, read *Take Control of Your Wi-Fi Security* by Glenn Fleishman and Adam C. Engst (http://www.takecontrolbooks.com/wifi-security.html).

## Traveling without a laptop

Imagine this: you're on a dream vacation to the middle of nowhere, and you've spent the last two weeks snapping some amazing photos with your digital camera. Then, a day before you fly home, your camera is stolen. Or lost. Or accidentally dropped into that scenic canyon. Your insurance might cover the camera, but you'll never be able to recreate the photos.

Had you been traveling with your laptop, you could have transferred your photos to the computer and then saved them onto an optical disc or uploaded them to a photo-sharing site over the Internet before the camera disappeared. But you left the laptop at home for a reason: you're on vacation! Without it, all you've got is that valuable memory card, and you have no way to back it up—or do you?

As a matter of fact, you do have several backup options. They'll cost a bit of money, but you may find the investment worthwhile. In some cases, you may even be able to use the same techniques to back up video from your digital camcorder. Consider these backup devices:

- **Your iPod.** If you're packing a full-size iPod with color display (including iPod with video), you may be able to plug your digital camera right into it and use it as a backup device. As long as you have a compatible camera all you need is Apple's $29 iPod Camera Connector (http://store.apple.com/1-800-MY-APPLE/WebObjects/AppleStore?spart=M9861G%2FB).
- **A portable video player.** A number of pocket-sized gadgets are designed expressly for backing up and viewing photos and videos. You pop your camera's memory card into a slot on the device (or hook up your camera using a USB cable) and transfer the photos

to an internal hard drive; you can then display the photos on the built-in screen and even create slide shows.

Macworld reviewed three of these devices: the Nikon Coolwalker MSV-01, the Epson P-2000, and the SmartDisk FlashTrax (http://www.macworld.com/2005/03/reviews/photostorage/); other options include the Hyperdrive, which has various models holding up to 160 GB (http://www.hypershop.com/shop/); the Cowon A2 (http://www.cowonamerica.com/products/cowon/a2/); and a wide selection of portable video players made by Archos (http://www.archos.com/products/video/).

- **A borrowed computer.** If you pack an appropriate USB card reader or adapter, you can pop into a local cybercafé, copy your photos onto one of their computers, and then upload them to a photo-sharing site or email them to yourself. Be sure to delete the photos from the borrowed computer and empty the Trash before you leave!

**TIP** Jeff Carlson, who edited this book, gave even more tips for backing up your digital photos while traveling in an article he wrote with Glenn Fleishman for Macworld: "Back up photos on the road" (http://www.macworld.com/2006/10/secrets/novdigitalphoto/).

## Windows Files and Volumes

Owners of Intel-based Macs can now run Windows alongside Mac OS X, using either Apple's Boot Camp software (which puts the entire Windows installation on a separate hard disk partition) or virtualization software such as Parallels Desktop or VMware Fusion (which stores the Windows environment in a special disk image file). Either way, the presence of a second operating system, with its own applications and files, increases the complexity of your backup needs.

**TIP** If you're interested in running Windows on a Mac, check out my book *Take Control of Running Windows on a Mac* for instructions (http://www.takecontrolbooks.com/windows-on-mac.html).

If you use Windows only occasionally and don't store much data on your Windows volume, you might consider forgoing Windows backups altogether. Reinstalling Windows and a few applications (as you might have to do in the case of a disk problem) is annoying but not the end of the world. However, if your use of Windows is more extensive, read on for instructions on keeping your data safe.

## Windows files backup strategy

The way you back up your Windows files depends partly on the way in which you're running Windows and partly on your specific needs. The main consideration is whether you're using Boot Camp or a virtualization environment.

**TIP** As you'll soon see, some of these procedures are more complex than others. If you haven't yet installed Windows and are contemplating doing so, please consider this advice:

- Backing up and restoring files is easier under a virtual machine than under Boot Camp. (Both Parallels and VMware Fusion can read Boot Camp volumes directly, so you can use both if you wish.)
- If you are running Boot Camp, backing up and restoring files is much easier if your Windows volume uses the FAT32 format than if it uses NTFS. However, NTFS is the only format available for Windows Vista installations.

So, if you have a choice, use virtualization software (with or without Boot Camp); if you use Boot Camp alone with Windows XP, choose FAT32.

### *Boot Camp*

The Windows partition Boot Camp creates is, as far as Mac OS X is concerned, just another volume. So most Mac backup software can read its files the same way as your Mac files. However, a few issues quickly appear:

- If you've formatted your Windows volume as NTFS (the only option for Windows Vista), Mac OS X can read from, but not write to, that volume. This means you can back up your files but not restore them from within Mac OS X—a potentially significant problem. (Unfortunately, though you can easily convert a FAT32 volume to NTFS, you can't do the reverse without reformatting your drive or using special commercial software such as Norton PartitionMagic.)

**NOTE** **NTFS OR FAT32?**

When you install Windows XP under Boot Camp, the installer asks you to choose whether to format the Windows volume using the FAT32 system or the NTFS system. Both formats have their pros and cons; FAT32 tends to make life easier for Mac users, while NTFS has advantages in reliability and efficiency for Windows users. If you're unsure which format you used, you must find out before proceeding. To check, from within Windows, choose Start > My Computer. Right-click the icon for your `C:` drive and choose Properties. The window that appears indicates the file system that volume uses.

- Some backup software, including SuperDuper, cannot read from Windows partitions at all, regardless of whether they're formatted as NTFS or FAT32.
- Although you can back up the entire contents of your Windows partition, you have to follow a special procedure when restoring files to make sure your restored Windows volume is bootable.

Therefore, follow the approach here that best meets your needs.

### Create archives from a FAT32 partition

Because Mac OS X can read from and write to FAT32 volumes directly, you can generally use your existing Mac backup software to create and restore archives of your Windows files. Simply add the appropriate folder(s) to your source—for example, **`/Volumes/Windows/Documents and Settings/`*`your-user-name`***.

### Create archives from an NTFS partition

You can follow the procedure just above for backing up files on an NTFS partition, but you'll be unable to restore them from within Mac OS X. If your backup program stores the files in Finder-readable format *and* your backup drive is formatted as FAT32 (which could be problematic if you're using the same drive to back up your Mac files), you can reboot into Windows, mount the backup drive, and manually copy the files back to their proper locations. Alternatively, use a Windows backup program to copy Windows files directly to your backup medium.

### Create and restore duplicates of a FAT32 partition

Because of the way Boot Camp expects your disk to be configured, making bootable duplicates of your Windows partition is a much different proposition from making a bootable duplicate of your Mac partition. On the plus side, you can use almost any software to copy the files—even copying them manually in the Finder works fine—as long as you include every single file on the Windows volume. You can even restore the backed-up files to your existing Windows volume the same way. But there's a catch: your backup drive itself will almost certainly *not* be bootable.

The only reliable way to get your Windows volume back to its previous state is as follows:

1. When running Mac OS X, drag all the files on your Windows volume to the Trash. Four files will be locked and will therefore refuse to go into the Trash: NTDETECT.COM, ntldr, IO.SYS, and MSDOS.SYS. To enable those files to be deleted, select them, choose File > Get Info, and uncheck the Locked checkbox in each of the four windows.
2. Empty the Trash.
3. Copy the entire contents of the Windows backup—again, assuming you included *every single file* on the volume—back to the Windows volume, either manually or using backup software of your choice.

You should now be able to reboot into Windows normally.

**WARNING!** One thing you cannot do is restore your Windows installation to a *different* partition type from the one it started on. The result will not be bootable. Specifically, you cannot restore files from a FAT32 backup onto an NTFS volume or vice-versa, nor can you create a new, empty partition using Disk Utility (even if you choose FAT32 as the format) and restore the files onto that. The *only* way you can currently get your Mac to boot from a Windows partition is if Boot Camp created that partition, and if the Windows files on it come from an installation with the same volume format.

### Create duplicates of an NTFS partition

If you've formatted your Windows volume as NTFS, the easiest way to duplicate (and restore) it without leaving Mac OS X is to use a free utility called Winclone (http://www.twocanoes.com/winclone/). It's a simple, straightforward program: you choose a source (your Boot Camp volume) and then click the Image button to create a disk image with a copy of all your Boot Camp files; you can store that image anywhere you like, including on your internal hard disk. You can also restore a Boot Camp volume without rebooting from another drive.

**NOTE** Several Windows utilities exist for backing up entire volumes to disk images, which can be restored in a bootable state. If you're already familiar with such utilities as DriveImage XML (http://www.runtime.org/dixml.htm, free) or Norton Ghost (http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=br&pvid=ghost10, $70), feel free to use them. However, I prefer the simplicity of using Winclone.

#### *Virtualization software*

If you use virtualization software—such as Parallels Desktop or VMware Fusion—your Windows files live in a special disk image that appears as a regular volume within Windows. Mac backup software can't see inside that image to back up individual files, which means that in order to use your Mac OS X backup software, you must back up the entire disk image.

Unfortunately, simply running Windows modifies the image file—a problem for any backup software that does file-by-file incremental archives, because it will consider the whole file to have changed each time. As with FileVault images (see the sidebar FileVault and Backups, later), adding these disk images to your archives will rapidly chew up your disk space. Therefore, if you include these images in your archives, consider backing them up separately (and less frequently than your other files)—or using backup software (such as CrashPlan) that supports byte-level incremental archives.

However, you do have three other options if you don't need to create complete, bootable backups of your Windows installation. The easiest tactic may be to use a shared Mac OS X folder to save the Windows files you create and modify, and simply be sure your backup software includes that folder in your backups. A second approach is to run Retrospect Desktop in Mac OS X, install the Windows version of Retrospect Client, and treat the Windows virtual machine as a network client. With either of these methods, you still use only one backup application; you can also store both Mac and Windows backups on the same media and manage them in the same way.

Alternatively, run Windows backup software within your virtual machine to back up your Windows files separately. (When it comes to selecting Windows backup software, I'm afraid you're on your own!)

# Choose Your Hardware

I remember vividly the days of backing up my hard disk onto a tall stack of floppies. Back when a 40 MB drive was standard, I would have been thrilled to think I could put 16 or more copies of my disk on a single CD-R. A few years later, conventional wisdom held that DAT (digital audio tape) drives were the way to go for many power users. Now, however, with hard disk sizes routinely reaching 400 GB, we have to reconsider old notions about backup hardware and media. You probably have a lot of data to copy, and the amount will only increase. But you don't want to spend a fortune on your backup system, and you don't want backups to take all day. What to do?

Although floppy disks are effectively dead, optical drives (to burn CDs and DVDs), tape drives, Zip and Jaz drives, and the like are still common, and since you may have these already, you will certainly want to consider the pros and cons of using them for backups. Hard drives are much less expensive than they once were, and for many people make the ideal backup device. There's also the possibility of backing up to a network server of one kind or another—and even your camcorder. In this section, I sort through all the major hardware options and help you to decide which is best for your backups.

## Hard Drives

Let me begin with my favorite option: hard drives. I use and suggest hard drives as a backup medium, and in almost every case I believe they're the best choice for individuals and small networks. If you can possibly manage it, you will achieve Maximum Backup Happiness by using external hard drives.

**Note** I deliberately said *external* hard drives—even though you could save some money on the enclosures and extra electronics by buying drives that can be mounted inside your desktop Mac Pro or Power Mac. I advocate external drives because:

- You can disconnect an external drive and store it off-site—an important safeguard against theft.
- If your computer suffers severe damage due to a power surge, a leaky roof, or being knocked off the desk accidentally, your internal hard drives may fail along with the rest of the machine.

### Hard drive virtues

I suspect that your initial impulse, like mine, is to cringe at the cost of external hard drives—especially since, as I explained earlier in Keeping Multiple Backups, you should have at least two, and perhaps three of them. They may seem extravagant in a way that DVD-Rs, say, do not. So let me sing the praises of hard drives for a moment, while at the same time explaining why they're not only the best solution, they're economical too. Here's what makes hard drives great:

- **Speed:** The first thing hard drives have going for them is speed. You may have tens or hundreds of gigabytes of data on your computer's internal hard disk. But copying such large amounts of data can be extraordinarily time-consuming under the best of circumstances. Even fast optical drives and tape drives generally transfer data at a fraction of the speed of a slow hard drive. If you want to do more with your computer than watch it back up your data, you'll appreciate the time savings a hard drive provides.
- **Capacity:** If you're backing up to a medium with less capacity than your hard disk, sooner or later you'll have to swap media. Even the newest double-layer DVDs can't store the entire contents of a moderately large hard disk on a single disc. Swapping media isn't the worst thing in the world, but the more often you have to do so, the more of an aggravation backing up becomes. If, on the other hand, you use an external hard drive with sufficient capacity, you'll never have to swap media—and you can allow your backups to run unattended at any time of the day or night.

**WARNING!** **BACKING UP TO ANOTHER PARTITION**

If you have a nice, large internal hard disk and far too little data to fill it, you may be tempted to partition it into several volumes and store backups on each one—instead of using separate physical drives. Although this is marginally better than not backing up at all, it's still an incredibly bad idea. Hard drives usually don't die one partition at a time. You could easily encounter a problem that makes it impossible to access any part of the disk, in which case your backups would be of no use. And just like a second internal drive, a second partition is vulnerable to theft and damage that affects your entire computer.

- **Random access:** In addition to raw speed in copying files, hard drives offer the enormous advantage of random access. Besides using space more efficiently, this means that it takes no longer to restore files recorded over a period of weeks than it does to restore files recorded on a single date.

- **Versatility:** When you use a hard drive for backups, you can put both duplicates and archives on the same device. You can (usually) boot from it, and even, in a pinch, use it as supplemental storage for other projects. Perhaps more importantly, using a hard drive keeps your optical drive (or other removable storage devices) free for installing software, burning DVDs, or other day-to-day tasks.

- **Economy:** As I write this, 250 GB FireWire drives can be found at retail for well under $200, and if you look online at discount stores and eBay auctions, you can find them for even less. That's quite a bargain—especially when you factor in the recurring costs of optical media or tapes. Further, how much is your time worth? Can you afford to spend an entire day restoring from a stack of CD-ROMs? If, instead, you could be up and running minutes after a drive failure, what would that be worth to you? Based on my own experience, I can say with conviction that an initial investment of a few hundred dollars pays for itself many times over when you consider the time and aggravation it saves in the long run.

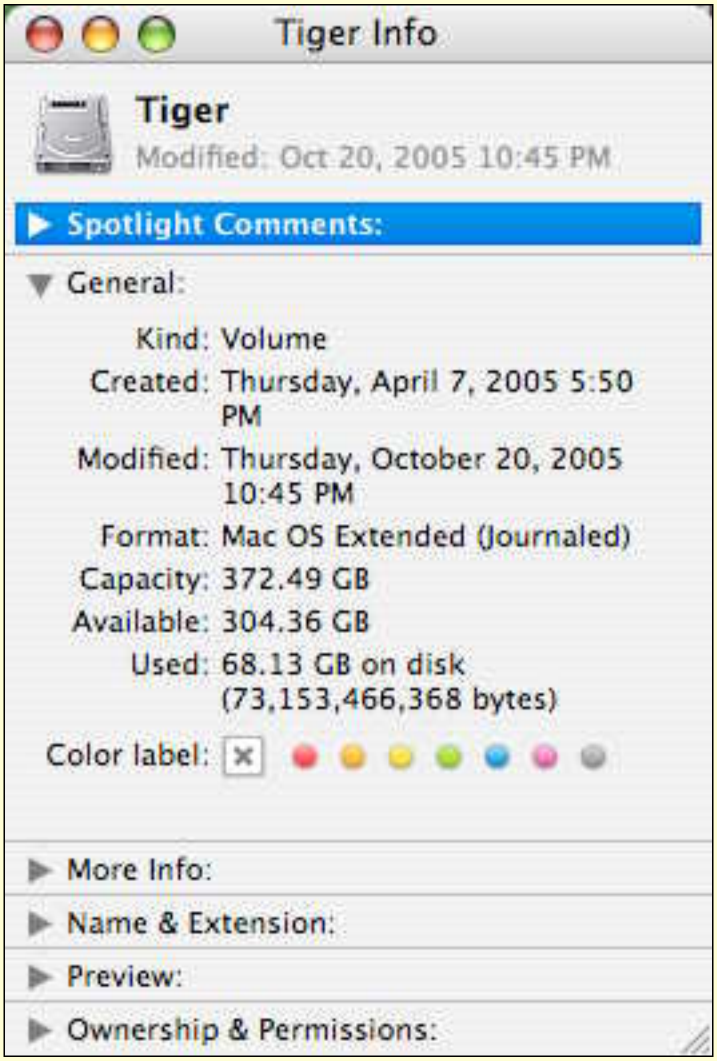
## Does size matter?

If you're using a hard drive for backups, how large does it need to be? This seemingly tricky question has a relatively easy answer: as a rule of thumb, a destination volume should have between 1 and 1.5 times the capacity of the source volume. Sometimes one can comfortably store both a duplicate and several months' worth of an archive on a single disk the same size as the one being backed up—but you can check this with a little bit of math.

I advocate partitioning each backup disk into two volumes—one for a duplicate and one for archives (see Partition Hard Disks, later). It's easy to figure out how much space you need for each, and then *add the two amounts together* to get a total disk size for the backup drive.

For duplicates, you need a volume that will hold all the data on your hard disk—which may be much smaller than its actual capacity—and provide some extra breathing room. To find out how much space your data currently occupies, select your hard drive's icon in the Finder and choose File > Get Info. The figure next to the word "Used" (**Figure 2**) is the amount of space the data currently occupies.

**FIGURE 2**



Tiger Info

Tiger
Modified: Oct 20, 2005 10:45 PM

▶ Spotlight Comments:

▼ General:

Kind: Volume
Created: Thursday, April 7, 2005 5:50 PM
Modified: Thursday, October 20, 2005 10:45 PM
Format: Mac OS Extended (Journaled)
Capacity: 372.49 GB
Available: 304.36 GB
Used: 68.13 GB on disk (73,153,466,368 bytes)
Color label: ☒ ● ● ● ● ● ● ●

▶ More Info:

▶ Name & Extension:

▶ Preview:

▶ Ownership & Permissions:

The Finder's Get Info window for a hard disk. The number next to "Used" indicates the amount of data currently stored on the volume.

Assuming that you regularly add new files to your computer, you will want to leave yourself a significant cushion—make the volume for the duplicate enough larger to hold the files you're likely to add during the next 6 to 12 months. If you do not have a good sense of the rate at which your data will grow, multiply the Used figure by 1.5, and then round up to the nearest gigabyte. (In this example, the volume "Tiger" would require at least 103 GB for a duplicate.) In any case, there's never a need for your duplicate volume to be larger than the total capacity of the disk you're backing up.

**NOTE** **HARD DRIVES AND LONG-TERM STORAGE**

According to conventional wisdom, hard drives are a poor choice for *long-term* data storage. Exactly how long "long" is can be debated. If you believe manufacturers' specifications for mean time between failures (MTBF), the typical drive should run continuously for at least 10 years before failing. However, the magnetic particles coating the platters are likely to randomly lose their charges much sooner than that, and many other causes of drive misbehavior don't technically count as "failure" as far as the manufacturer is concerned.

Data corruption can occur at any time, but my confidence in a hard drive begins to deteriorate after about 3 years, and after 5 years or so, I no longer consider it a safe bet for backup data storage.

You could have a hard drive that behaves perfectly for decades, but the odds are against you. As a practical matter, I suggest factoring in the purchase of new backup drives when you buy a new Mac—or every 2 to 3 years, whichever is more often.

For archives, the situation is slightly different: on the one hand, your backup software may compress your data, decreasing the space used; on the other, you will continually add new and modified files, increasing the space used.

Begin by determining the total space occupied by the data you plan to archive (again, use the Finder's Get Info command), which could be your entire disk if you perform a full archive, or perhaps only your home folder and a few other items if you perform a selective archive. Next, subtract the total size of any subfolders you intend to exclude (for example, **`~/Music/iTunes/iTunes Music`**).

Now multiply this total by 1.5. The resulting figure—let's call it *x*—is the minimum amount of space you should allot for an archive partition if you're using compression. Without compression, multiply *x* by two.

**NOTE** If you're backing up several computers over a network to a single set of media, be sure to perform these calculations for each computer, and then add them together. Although some network backup software (including Retrospect) can save space by maintaining just one copy of a file that's identical across multiple computers, you'll be safer if you ignore that possibility and allow more breathing room.

I hasten to point out that these figures represent recommended *minimums*. They will enable you to back up your data comfortably today, but as your hard disk fills up, you want a backup disk that can keep up with it. So all things considered, you should buy a backup disk no smaller than your source disk.

It could be, for instance, that on a 60 GB hard disk, you currently have 20 GB of data in total, of which your home folder, not counting excluded files, is only 6 GB. If you allow 30 GB (20 GB x 1.5) for a duplicate and 9 GB (6 GB x 1.5) for an archive, that yields 39 GB. Resist the temptation to save money by purchasing a 40 GB disk, because sooner or later, you're likely to fill up that internal disk and wish you had more backup space. You know the saying: you can never have too much money or disk space. Buy a 60 GB disk—or, if you can afford it, an 80 GB disk.

Why not 120 GB? Or 250 GB? Why not buy the biggest disks you can afford? There's nothing wrong with getting a bigger disk, but after about 1.5 times the capacity of your internal disk, you reach a point of diminishing returns—by the time you fill it completely (assuming a compressed archive), the drive will be too old to depend on (see the note on the previous page: Hard Drives and Long-Term Storage).

Likewise, you may be thinking that if you bought a larger disk than necessary, you could use the extra space for other data. But I strongly encourage you to use a backup drive exclusively for backups. Otherwise you may be tempted to keep the backup drives hooked up instead of storing them more safely (see Off-site storage, later).

### Choosing a hard drive

Because so many different external hard drives exist, the choice can be daunting. Here's my quick guide to what you need to know:

- **Interface:** All things being equal, get a drive with the fastest interface your computer supports. (FireWire 800 and USB 2.0 are faster than FireWire 400, which is much faster than USB 1.1; with add-in cards, you can get even faster interfaces than FireWire 800, such as Ultra 320 SCSI, Fibre Channel, SATA (Serial ATA), and SATA II. However, be aware that not all add-in cards enable you to boot from external drives; if in doubt, check with the manufacturer before purchasing the card.) Up to a point, a faster interface typically translates into quicker backups—though in real-world use, FireWire 800 is usually not dramatically faster than FireWire 400. Many modern drives offer combinations of two or more of these interfaces.

### NOTE USB 2.0 DRIVES, INTEL MACS, AND BOOTABILITY

Almost every Mac with a FireWire port can boot from an external FireWire drive (either the 400 or 800 variety). However, only Intel-based Macs can boot into Mac OS X from USB 2.0 hard drives. Therefore, if you're looking for a drive on which to store duplicates, I suggest choosing either FireWire-only or combination FireWire/USB hard drives, which will give you the broadest compatibility.

However, be aware of two important points regarding Intel Macs:

- Despite Apple's claims to the contrary, Intel Macs *can* boot from hard disks formatted using the Apple Partition Map (APM) scheme, which has been the norm on PowerPC-based Macs for years—as long as they're connected via FireWire (you can't boot an Intel Mac from an APM-formatted drive that uses USB).

  The catch is that currently, the Tiger *installer* won't recognize such disks as a valid destination and instead requires you to reformat the drives with Disk Utility to use the new GUID Partition Table (GPT) scheme. Luckily, however, you don't need to worry about any of this when making backups. If you use a utility described in this book to create a duplicate from your Intel Mac onto a FireWire drive, it will be bootable even if the volume uses APM.

- If you have an Intel Mac with any version of Tiger (10.4) on it and make a duplicate of your startup volume, that volume will *not* boot a PowerPC-based Mac; likewise, a duplicate of a PowerPC-based Mac's Tiger startup volume will not boot an Intel Mac. Apple is expected to eliminate this inconvenience with the release of Mac OS X 10.5 Leopard, which should be a universal system that will boot Macs with either type of processor.

- **One-touch backups:** Maxtor sells OneTouch external hard drives with a button that enables you to launch software and execute a backup just by pressing it. Seagate offers something similar, the Pushbutton Back-up Hard Drive. IOGEAR ups the ante on their Tri-Select ION drives, which feature three buttons (each of which can run a different backup script). I'd rather have my backups run on a schedule—one less button to press! However, the Maxtor and IOGEAR drives include a free copy of Retrospect Express, so they're worth a few dollars extra. (The Seagate drives include a copy of CMS BounceBack Express, a limited version of the BounceBack Professional duplication software.)

  You can ignore the button(s)—or, if you prefer, set a button to run your Duplicate or Archive script and press it to make an instant backup after you've made especially important changes.
  http://www.maxtor.com/en/
  http://www.seagate.com/
  http://www.iogear.com/

- **Automatic backups:** CMS Products' ABSplus drives include software that performs a duplicate as soon as you plug in the drive. That's great—but only part of what we want. I'd opt instead for the flexibility of standard backup software. Feel free to get an ABSplus, but plan to supply your own software, at least for archiving.
  http://www.cmsproducts.com/product_absplus_desktop_fw_mac.htm

- **Build-your-own:** Numerous companies sell FireWire- or USB-equipped cases into which you can place your own IDE drive mechanism. If you're comfortable doing some minor tinkering and bargain hunting, you may be able to save a bit of money this way. Be aware, however, that some older cases cannot accommodate disks over 120 GB; check the manufacturer's specifications before making a purchase.

- **Hot-swappable assemblies:** Granite Digital and WiebeTech sell hot-swappable FireWire hard drive assemblies. You get a single case, power supply, and cable, to which you add one or more hard drives, each in its own special carrier tray. You can pop out one hard drive and pop in another quickly, making it quite easy to rotate backup sets—no messing with cables. I've used Granite

drives and they're certainly nice, but you pay quite a premium for what amounts to a small added convenience.
http://www.granitedigital.com/
http://www.wiebetech.com/

- **Multi-drive enclosures:** Another new trend in external hard drives is enclosures containing two or more drive mechanisms (whether individually removable or not) that you can optionally configure, using included software, as a RAID (see the sidebar Can a RAID Substitute for Duplicates?, earlier).

  Examples include FirmTek's SeriTek Series of eSATA (external SATA) drive enclosures, Maxtor's OneTouch III, Turbo Edition (which also, naturally, has the one-touch backup feature mentioned just previously), and LaCie's Two Big device (which uses a SATA II interface). Such drives can provide either redundancy for your backups (if configured as a mirrored RAID) or more speed (if configured as a striped RAID). Although I can think of many excellent uses for these devices, they may be overkill for backups; I think most people would be better served with two physically separate drive units than one enclosure with two mechanisms.
  http://www.firmtek.com/seritek/
  http://www.maxtor.com/en/
  http://www.lacie.com/

- **Pocket-sized hard drives:** If you need to back up large amounts of data while traveling, or if your laptop lacks a CD or DVD burner, consider a pocket-sized hard drive. These drives typically use the same 2.5-inch mechanisms that laptops do, and can be powered through the FireWire or USB cable, eliminating the need to carry a bulky AC adapter with you. Some examples:

  - ◊ **LaCie Mobile Drives:** LaCie makes several different lines of pocket-sized hard drives, with various interface options and capacities up to 320 GB (in some cases using two drives in a single enclosure). Some of their mobile drives offer special features such as shock-resistant enclosures or built-in cables.
    http://www.lacie.com/products/range.htm?id=10036

  - ◊ **Maxtor OneTouch III, Mini Edition:** Maxtor's pocket-sized drives hold up to 100 GB and use USB 2.0 interfaces.
    http://www.maxtorsolutions.com/en/catalog/OTIII_Mini/

  - ◊ **OWC Mercury On-the-Go:** These drives are available with several different combinations of USB 2.0, FireWire 400, FireWire 800, and SATA interfaces, in capacities up to 200 GB. http://eshop.macsales.com/shop/firewire/on-the-go
  - ◊ **Seagate USB 2.0 Portable Hard Drives:** Similar to the other drives listed here, these range in size to 160 GB but, like the Maxtor drives, don't have the option of a FireWire interface. http://www.seagate.com/www/en-us/products/portable/portable_drives/

**NOTE** Seagate purchased Maxtor in mid-2006, but the new combined company is keeping the two brands separate for the time being.

  - ◊ **Seagate Pocket Hard Drives:** These drives use the tiny 1-inch mechanisms found in some iPod models, but are available in capacities only up to 8 GB. http:// www.seagate.com/www/en-us/products/portable/pocket_drives/

- **Encrypted hard drives:** A problem with putting a bootable duplicate on an external drive is that you can't use your backup software's encryption feature; if the files must be decrypted by software before the system can read them, you won't be able to boot from that drive. (And thus, ordinarily, only archives can be encrypted.) This isn't much of a worry unless, as I suggest, you store a backup drive off-site at all times—if someone else gets their hands on it, they have immediate access to all your data.

  The way to get encrypted bootable backups is to use a drive that features *hardware* encryption. Everything written to such a drive is encrypted automatically, and everything read from the drive is decrypted automatically, by circuitry in the drive enclosure; instead of typing a password, you secure the data with a physical electronic key. (Needless to say, you have to keep that key in a safe place, separate from the drive itself!)

  Several manufacturers now make such drives (or enclosures to which you can add your own drive); they come in full-size (3.5") and pocket-sized (2.5") models, with a variety of interfaces. They're more expensive than standard drives, but are an excellent

investment if you wish to store sensitive personal data. Examples include RocStor's Rocbit drives and RadTech's Impact enclosures.
http://www.rocsecure.com/
http://www.radtech.us/Products/Impact.aspx

- **iPods:** You can use an iPod as a backup device—but remember, that will limit the number of songs and other media that you can store. (Only older iPods with FireWire interfaces can be used as startup disks for PowerPC-based Macs.) iPods are also more vulnerable to theft, since you're more likely to carry them around with you—so be sure your backups are encrypted! To use your iPod as an external hard drive, open iTunes, select your iPod in the Devices list on the left, and check the Enable Disk Use checkbox.

- **Brands and warranties:** Although hard drives are in some ways commodity items, you'll still pay more for a brand name than a generic drive. Is the extra money worth it? Often not. The drive mechanisms come from relatively few manufacturers, all of which are reputable—it's the cases, power supplies, and electronics that vary from vendor to vendor. Look for a 1-year or better warranty, and check the manufacturer's Web site for signs of life and Mac support. But don't be afraid of second-tier brands. (For instance, I had a pair of FireWire drives from Buslink—a brand that doesn't even claim Mac compatibility—that served me flawlessly for years, even though I bought them dirt cheap on eBay.)

**TIP** You can often find bargains on hard drives from a wide range of manufacturers and dealers at dealmac, http://www.dealmac.com/. Drive prices are constantly dropping, and special offers and rebates appear frequently. If you're looking for a particular type or capacity of drive, consider signing up for dealmac's watch list—you'll get an email alert when a deal matching your criteria appears.

## Optical Media

The various flavors of recordable CDs and DVDs are collectively known as *optical media,* because they rely on lasers to read and write data to them. Most of the Macs made in the past several years include a *SuperDrive*, which can write to and read from DVD media (up to 8.5 GB) and CD media (up to 800 MB); some have *Combo drives* that can read from DVDs and write to CDs.

Meanwhile, new standards continue to emerge. Several third-party vendors are now selling Mac-compatible Blu-ray Disc optical drives with up to 50 GB capacity. Drives supporting the competing new standard HD DVD (up to 30 GB capacity) have yet to appear for the Mac, but I expect to see them soon.

Historically, Apple has regularly upgraded SuperDrives to support higher-capacity standards. For example, starting in mid-2005, some Macs included SuperDrives that could read and write to double-layer (8.5 GB) DVD+R discs, and by late 2006, all new SuperDrives had this capability. Apple has not yet shipped any SuperDrives with Blu-ray or HD DVD support, but I wouldn't be surprised to see this in the future. See **Table 2**, on the next page, for an overview of current optical media types.

Because built-in optical drives do not require an additional purchase (except the media, which is relatively inexpensive), it's logical to consider using them for backups. In a few cases they may be adequate, but in general I'd like to steer you away from backing up your Mac onto optical media.

The first thing I should point out is that backing up to any optical media is *slow*. If you have only a few gigabytes of data to back up, this may not bother you, but as your storage needs increase, you're more likely to find it problematic. True enough, some optical drives are faster than others; a 52x CD burner will obviously require much less of your time than a 2x burner. Even so, the fastest optical drives transfer data at less than one-tenth the speed of the slowest hard drives. And if you're talking about backing up many gigabytes of data, you're still looking at an extremely lengthy process.

Another disadvantage of using your optical drive for backups is that it requires your attention. If your backups run automatically on a schedule, you must make sure a blank disc is in the recorder at the proper time. If you schedule backups for when you're using the Mac (so that you can easily swap discs), you face the possibility that you'll want to use your optical drive for some other reason—and even if not, your Mac may slow down unacceptably during the backup process.

Financial considerations alone make optical media an attractive option, despite their disadvantages. But before you decide on an optical drive as your backup device, consider the following factors.

### Table 2: Optical Media Types

| Name | Capacity | Rewritable? | Use with Combo Drive | Use with SuperDrive |
|---|---|---|---|---|
| CD-ROM | up to 800 MB | No | Read-only | Read-only |
| CD-R | 650, 700, or 800 MB | No | Yes | Yes |
| CD-RW | 650, 700, or 800 MB | Yes | Yes | Yes |
| DVD-ROM | up to 4.7 GB | No | Read-only | Read-only |
| DVD-R | 4.7 GB | No | Read-only | Yes |
| DVD-RW | 4.7 GB | Yes | Read-only | Yes [1] |
| DVD+R | 4.7 GB | No | No | Yes [2] |
| DVD+RW | 4.7 GB | Yes | No | Yes [2] |
| DVD+R DL (double-layer) | 8.5 GB | No | No | Yes [3] |
| DVD-RAM | up to 9.4 GB | Yes | No | No |
| Blu-ray Disc (BD-R/BD-RE/ BD-ROM) | up to 50 GB | BD-ROM: No<br>BD-R: No<br>BD-RE: Yes | No | No |

[1] Except on very early SuperDrive models. Although the Finder does not support DVD-RW media on older SuperDrives, some third-party software may.

[2] All SuperDrives shipped in 2005 and later included DVD+R and DVD+RW support.

[3] Apple began phasing DVD+R DL support into SuperDrives in 2005, and all new SuperDrive-equipped Macs released since late 2006 have had DL capabilities.

**TIP** Not sure which kinds of media your Mac's optical drive can record onto? Open Terminal (in **`/Applications/Utilities`**) and enter:

```
drutil info
```

A list of supported media types will appear after the label CD-Write (for CD formats) and DVD-Write (for DVD formats). (In this list, "DL" stands for double-layer.)

### Recordable CDs

CDs (including CD-R and CD-RW) make a poor choice for duplicating your entire hard drive. The highest-capacity CDs you can buy—which, by the way, may or may not be compatible with your hardware and software—hold 800 MB. (Standard CDs hold either 650 or 700 MB.) In order to duplicate your entire hard disk—even with the smallest possible installation of Tiger—you would need four to six discs, depending on their capacity. And if you want to duplicate a full 120 GB hard disk, that will require upwards of 170 discs! Even then, you will not be able to boot from your duplicate; you'd need to restore it to a hard disk first. Because of the number of discs required, the amount of user interaction the backup will require, and the inability to boot from the final product, CDs are a bad idea for duplicates.

When it comes to archive backups, CDs show a bit more promise. Yes, it still takes a stack of them, and yes, that means time-consuming sessions of swapping (and labeling!) discs. However, if you're backing up only your data files (not your entire hard disk)—and particularly after your first session, when you're incrementally backing up only changed files—the time and aggravation it requires will be much less. As CDs go, CD-RW media has an edge over CD-R (even though it's almost twice as expensive) in that it can be erased and reused when your stack of discs becomes too large (see Recycling vs. long-term archives, later).

### Recordable DVDs

Recordable DVDs may all look alike, but they vary in format and capacity. (See **Table 2**, on the previous page, for an overview of the different formats.) Early Apple SuperDrives supported only DVD-R media, though with the right software, you could also use erasable DVD-RW media. A pair of competing standards—DVD+R and DVD+RW—is supported by currently shipping SuperDrives and most third-party external DVD recorders. In addition, newer third-party drives—and SuperDrives in most Macs shipped from mid-2005 on—can use double-layer DVD+R media with a capacity of 8.5 GB (a single-layer DVD can hold up to 4.7 GB).

**NOTE** You will sometimes see drives described as supporting “DVD±R” or “DVD±RW.” The ± symbol means both + and - (as in, DVD+R *and* DVD-R). And if a drive supports a rewriteable format, it also supports the corresponding write-only format. So, for example, a DVD±RW drive also supports DVD-R and DVD+R.

Another standard, known as DVD-RAM, is also supported by many third-party drives (as well as some older Macs). Depending on the format, a DVD-RAM disc can hold up to 9.4 GB of data. And third-party drives using the new Blu-ray Disc format can put as much as 50 GB on a disc.

First, the good news: if you want the lowest possible cost per gigabyte of storage over the long run, you can hardly do better than DVD-RW (or DVD+RW) discs—if your optical drive and software supports them. Buy a package of 50 (typically sold without cases on a plastic spindle) for under $50, and you have enough media to back up a medium-sized hard disk for a couple of years. When all the discs are full, erase them and start again. DVD-R discs, although not erasable, are a bit cheaper than rewritable DVD-RW or DVD+RW media, and will work with any SuperDrive. DVD+R DL discs hold more data, but are not erasable, while Blu-ray discs are still quite pricey (a single rewritable 50 GB disc can run upwards of $50).

But there’s a catch—several catches, in fact:

- Even the highest-capacity recordable DVDs may not be able to store the entire contents of your hard disk.
- In cases where you can duplicate your entire hard disk onto a DVD, you will still, in general, be unable to boot from the DVD. As with CDs, you must restore the duplicate onto a hard disk first.
- Erasing rewritable DVDs (DVD-RW, DVD+RW, and Blu-ray) can be rather time-consuming.

### Optical media longevity

With proper care, CDs and DVDs you record should still be readable years or even decades from now. However, I must emphasize the word *should*. Numerous people, including me, have had the unpleasant experience of trying to read an old optical disc and finding that over time, its data had become corrupted. Although any CD or DVD—

including prerecorded commercial discs—can theoretically lose data, the risks are greater with recordable discs, which use different technologies for storing information.

One set of dangers comes from physical damage. If you expose a disc to heat, humidity, or bright sunlight, or if you bend or scratch the disc, it can physically degrade in such a way that some or all of its data can't be read. But another danger comes from the disc itself. Depending on the materials used, the manufacturing process, and numerous other variables over which you have no control, even discs that are treated with the utmost care can sometimes warp, peel apart, or otherwise deteriorate over the course of several years. Either way, even a disc that *looks* perfectly good can suffer from subtle corruption that makes it unusable.

Although there are no ironclad guarantees when it comes to the longevity of physical media, I can recommend several steps that will greatly minimize your risks when using optical discs:

- **Make extra copies.** If the chance of a single disc losing data is small, then the chance of two copies both losing data is much smaller. Time and money permitting, keep duplicates of your backup CDs and DVDs—and store the two sets in different locations.

- **Avoid rewritable discs.** Although you'll use a greater number of recordable discs (CD-R or DVD±R) than rewritable discs (CD-RW or DVD±RW), each time you erase and rewrite a disc you introduce another opportunity for data errors and physical damage to creep in. All other things being equal, recordable discs are somewhat safer.

- **Handle with care.** For best results, store your media in its plastic case, upright, in a cool, dark, dry place. Be careful to avoid scratches or fingerprints. And, although I personally consider this overkill, if you want to avoid any possibility of damaging the disk by writing on it or labeling it, you can label the case instead.

- **Periodically re-record your discs.** If you want to keep your backups on disc indefinitely, then every 2–3 years, take your discs out of storage and make copies of them on fresh media.

- **Buy quality media.** Although the quality of optical media doesn't necessarily correlate with its price, it's true that some generic media is manufactured using inferior materials and techniques. Using name-brand media is a better bet. Based on numerous reports I've read, two brands with particularly good track records are TDK Professional and MAM (formerly Mitsui). The MAM discs have their reflective layer made out of 24-karat gold, rather than the more usual silver, and are reputed to be highly resistant to deterioration.
http://www.tdk.com/professional/
http://www.mam-a-store.com/standard---archive-gold.html

### Final thoughts on optical drives

I believe the best backup strategy is the one that requires the least manual effort. Because optical media tend to require a lot of manual effort—and because they do not provide you with a bootable backup—they're less than ideal. However, if you've just spent your entire savings on a new iMac and you can't possibly spring for even a single external hard drive, backing up onto optical media is vastly better than not backing up at all. Just keep these thoughts in mind:

- For minimum inconvenience, use the highest-capacity discs your drive supports (i.e., DVD rather than CD).

- If saving money is paramount, use rewritable media (DVD-RW or DVD+RW), if your drive and software support it.

- Because incremental duplicates are impossible with optical media, plan on making a duplicate just once a month.

## Magneto-Optical Disks

Several different manufacturers offer magneto-optical (MO) drives and disks, ranging in capacity from 128 MB to 9.1 GB. Some of these are write-once like CD-Rs (the acronym WORM, for Write Once, Read Many, applies to such disks and drives); others are rewritable like CD-RWs and can be erased. The primary advantage of MO technology over CDs and DVDs is longevity: MO media is typically rated for long-term archival storage on the order of 100 years. On the other hand, MO media is extremely expensive, as are the drives themselves. The mechanisms are considerably slower than conventional optical drives. And MO media comes in many different formats and sizes—once you choose a media type, your future options may be limited.

The latest development in MO is called UDO (Ultra-Density Optical), with disks that can hold as much as 30 GB each. If regular MO drives and media are expensive, UDO is out of this world: plan on spending about $4000 for a low-end drive, plus upwards of $60 for a single rewritable cartridge.

Because the backup plan I'm recommending here does not require extremely long-term storage of media, and because I assume you do not wish to spend more on your backup device and media than what you paid for your Mac, I see no reason to consider MO or UDO drives.

## Other Removable Media

Besides optical discs and magneto-optical disks, you can find many other removable storage devices, from a wide range of manufacturers. The most popular ones—and, for our purposes, the only ones potentially worth considering—are made by Iomega.

### Iomega Zip and Jaz

Iomega Zip drives store 100 MB to 750 MB on removable magnetic disk cartridges that are slower than hard drives, but usually faster than optical discs and much faster than tape drives. Although the cost of media per gigabyte is comparatively high, Zip disks can be reused indefinitely. The same is true of the now-discontinued Jaz drives, which support 1 GB and 2 GB Jaz disks. Unfortunately, Zip and Jaz disks have a reputation for being unreliable, so I recommend against using them for backups.

### Iomega REV

Iomega's latest removable-storage device, REV, uses rugged, hard disk-based cartridges that hold either 35 GB or 70 GB each. Designed as a faster and more robust backup platform than tapes or DVDs, REV even includes a free copy of Retrospect Express. Configurations with various interfaces are available, though only the 35 GB model offers a FireWire interface.

Although REV is certainly an improvement over Iomega's earlier Zip and Jaz drives, it has several issues. For one thing, performance is significantly slower than ordinary hard drives. And when you factor in media, REV is considerably more expensive than regular hard drives too. The 35 GB REV drives run about $350, while the 70 GB models cost about $500. To that you'll have to add the price of disks—roughly $50–60 each. In other words, a 70 GB drive with two disks will run you over $600, for which price you could buy half a dozen stand-alone 80 GB FireWire drives, with change left over. Another significant downside is that even 70 GB is not large enough to hold the contents of some users' startup volumes; although you can certainly split a backup onto multiple disks, this would prevent you from making a bootable duplicate.

On the plus side, a stack of REV disks takes up much less space than a stack of hard drives, and uses fewer cables and adapters. If space is a bigger concern than money or performance, REV might be worth a look. http://www.iomega.com/direct/main/target.jsp?family=drives&category=rev

**TIP A REMINDER ABOUT REDUNDANCY**

As I suggested earlier in Keeping Multiple Backups, no matter which type of backup medium you use, you should always keep multiple copies of your backups. That means multiple hard drives or multiple sets of removable media (of whichever sort). There's always the chance that a single backup will suffer the same fate as your hard drive: a random failure of some sort. If you attempt to restore files from a backup and find that it's damaged, you'll be grateful that you had a spare copy.

Better yet, if possible, consider maintaining *three* sets of backups, one of which is kept at a separate location from your computer at all times. I discuss off-site backups in more detail later on under Mind Your Media. Although an off-site backup is possible even if you have only two sets, having three makes it much more convenient.

## Tape Drives

For many years, digital tape drives were considered the only reasonable, cost-effective way to back up large quantities of data. They're still extremely popular in large businesses. Common digital tape formats include VXA and DDS (a data-optimized variant of DAT, digital audio tape). Although at one time tapes were notorious for losing data spontaneously, they have now achieved a comfortably high level of reliability and longevity. And in (extremely large) quantity, they can be quite economical—though most of us will never get to the point where that economy of scale kicks in.

Tape drives have many virtues, but speed is not one of them—at least, not for the lower-end tape drive most of us mere mortals can afford. It takes far longer to back up a given amount of data to a tape than to even a slow optical disk. Restoring files is even more time-consuming, because tapes must be rewound or fast-forwarded to the correct spot before the data can be transferred. And you will never be able to boot your Mac from a tape drive.

When truly phenomenal quantities of data must be backed up, when money is no object, and when time is plentiful, tape drives are perfect. High-capacity tape libraries—automated systems that can robotically swap tapes into and out of a bank of tape drives—are marvelous (and marvelously expensive) toys that form the backbone of many corporate backup systems. But for ordinary people with modest amounts of data, too little time, and even less money, they make little sense. Consider that you may spend about $1600 for a drive that supports 80 GB tapes, which in turn cost about $80 each. For that price, you could buy sixteen 80 GB hard drives or four 500 GB hard drives, which should be enough to provide speedy, redundant backups for all but the most extreme Mac setups.

## Flash Drives

Flash drives, those small, solid-state, keychain-sized gizmos you plug into a USB port and use to shuttle files around, are all the rage these days. Because they're compact, have no moving parts, and can store, in some cases, several gigabytes or more of data, they make a tempting choice for a backup medium.

For quick, one-off backups of files you're actively working on, flash drives are a perfectly reasonable choice. But the biggest issue for serious backups is cost. As I write this, an 8 GB flash drive is considered a good deal if you can find it for under $100; a 16 GB flash drive might cost $200 or more. That's vastly more expensive per gigabyte than even a high-end hard drive.

At some hypothetical future date when you can buy, say, a 64 GB flash drive for little more than a comparably sized hard drive, they may be useful for day-to-day duplicates and archives. For now, they're best for travel and other situations where you only need to back up a few files.

## SAN, NAS, and NDAS

Another trendy buzzword in data storage is *SAN,* or storage area network. A SAN is nothing more than one or more hard drives able to be shared among several computers, generally via high-speed FireWire, Fibre Channel, or SCSI connections (without using a conventional Ethernet-based network).

In contrast, *NAS,* or network attached storage, typically refers to one or more hard drives with their own Ethernet (or wireless) interfaces, sort of minimalist file servers. (Increasingly, they're simply called "network drives" or "Ethernet drives.") In other words, SAN and NAS equipment may be nearly identical, except for their interfaces.

*NDAS,* or network direct attached storage, is a relatively new NAS variant that promises faster speeds and easier configuration.

### SAN

SAN devices are used most commonly in situations where massive quantities of data must be recorded to or read from a shared drive at high speed, video being the canonical example. Such systems are rarely found in home and small-office settings. If you happen to have one, you can certainly use it for backups, but if that's your primary intended use, SAN is extreme overkill. Depending on the type of SAN equipment you have and how it's formatted, you may or may not be able to use it as a bootable duplicate, so you may still require external hard drives for that purpose.

### NAS

NAS devices, on the other hand, are frequently marketed as backup (and all-purpose file storage) solutions for small networks. The idea is that you can set up a centralized file server without needing an additional computer, and every computer on your network can back up files to it. Some NAS equipment can also communicate with your home entertainment system, providing storage for audio and video.

Apple's new 802.11n AirPort Extreme Base Station has a USB port that supports, among other things, external hard drives. With a hard drive attached, the AirPort Extreme becomes a NAS device that can offer storage to any computer on its network, whether connected wirelessly or via an Ethernet cable. I suspect that when Leopard ships, Apple will promote this setup as a way to back up your whole home or office network using Time Machine.

Although NAS marketing paints a rosy picture, I urge circumspection when considering NAS as a backup medium, for several reasons:

- Even though the drive functions as its own file server, a NAS device can't run backup software directly. You must still run a backup program on each of your network's computers individually. Your NAS drive may come with free backup software, however.
- Some NAS devices can only be formatted using FAT32, a Windows file system. (The AirPort Extreme Base Station doesn't have this limitation, of course.) Although Mac OS X can read from and write to FAT32 volumes, some data (such as resource forks) may not be stored properly. Your backup software may be able to overcome this limitation by storing data in a special archive file, but if you use software that backs up files in a Finder-readable format, you risk losing data.
- It may not be possible to boot your machine directly from a duplicate stored on a NAS device (even if you have an AirPort Extreme); in general, you will have to restore (or re-duplicate) a duplicate to another hard drive first. Your NAS drive may have a USB port, but USB ports on NAS devices are usually used only to hook up shared printers or, in some cases, secondary hard drives.

All that said, with the right hardware and software, NAS could make a perfectly good storage medium for archives of several computers' files. If you buy a model that supports a secondary, external drive, I strongly recommend using one (or two) to rotate copies of your backups off-site. Because a NAS drive can serve many other useful purposes in your home or office, I wouldn't discourage you from buying one. But if you need shared storage only for backups, conventional hard drives (attached to a computer that functions as a backup server) are more versatile.

### NDAS

A company called Ximeta has patented a technology they refer to as NDAS, which they claim is better, faster, and easier to use than NAS. Several companies have licensed this technology and sell NDAS products under their own brands; among these are Other World Computing and Macally, names that should be familiar to most Mac users.

Like NAS, NDAS gives you a box with a hard drive inside and an Ethernet port that you can connect to your network. The difference is that instead of appearing as a file server on your network, the device acts as though it were a directly attached hard drive. In order to achieve this effect, NDAS devices require you to install software on each computer that will connect to them. However, other than that, no special configuration is required—no Web-based interfaces, fiddling with the Connect to Server dialog, or anything of that sort. Once connected, the drive "just works," and because it eliminates some of the networking layers that slow down NAS devices, it provides much faster performance, as well as increased security (in some senses) and better expandability.

Or at least that's the theory. I haven't worked with any NDAS devices personally yet, but from what I've read, they suffer from the sorts of problems one might expect from any first-generation technology. For example, although an NDAS volume can be shared across platforms, you can't access the drive from both a Mac and a Windows computer at the same time. If you have both sorts of machines on your network, that could be a deal-breaker.

On the plus side, though, it *should* be possible to create a duplicate to an NDAS drive—assuming you have an Intel-based Mac—and then plug the drive directly into your computer's USB port and boot from it. Again, I want to emphasize that I can't guarantee this will work, but it appears to be technologically possible.

Apart from that one potential advantage, what's true of NAS devices is true of NDAS devices. Because of their inherent limitations and the newness of the technology, I'm reluctant to recommend them yet—except to people who like to experiment and are willing to risk some of their money to do so.

## Local Network Servers

If, in your home or office, a computer is functioning as a file server, it's certainly worth considering whether you could use a network volume (*AFP*, *SMB*, or otherwise) as a backup destination.

In general, if you have control over the server, I recommend adding a separate physical hard drive and installing client-server backup software (see Network backup approaches, earlier). Otherwise, your backups will be commingled with other files, making it difficult to store them off-site and potentially creating a security risk.

If you do not personally have control over the server (i.e., if it's a shared company server), be circumspect about using it for backups. You could easily use up more space than you should, and you risk incurring the wrath of your IT manager. Even if she's willing to give you your own capacious partition on a server hard disk, you'll have much less flexibility and control over your data than if you backed it up to local media.

## iDisk

Subscribers to Apple's .Mac service (at $100 per year) currently get 10 GB of storage space, with the option to increase that figure to 20 GB for $50 per year or 30 GB for $100 per year. This space must be shared among email, .Mac Groups, and iDisk (where your backups, if any, are stored—along with any photos, videos, or Web sites you've posted). Apple's Backup application, and most other backup utilities, can use an iDisk as a backup destination. Unfortunately, even 30 GB is far too little space to meet most users' backup needs; the cost is excessive if backups are your primary consideration; and transfer speeds to the .Mac servers are often quite slow, even for users with broadband connections. In addition, you cannot make a bootable backup onto an iDisk. For these reasons, your iDisk is not an ideal backup destination.

On the other hand, for casual (manual or automatic) backups of just a few files between regularly scheduled archives, an iDisk does make a convenient—and inherently off-site—destination. And if you happen to have any of numerous programs with a built-in .Mac backup or synchronization feature (including Yojimbo, SOHO Organizer, and NetNewsWire, for example), by all means use it!

## Internet Backup Services

The idea behind Internet backup services is simple: using either a conventional backup program or proprietary software, perform backups as usual, but use secure Internet file servers—rather than local or network volumes—as the destination. In other words, an Internet backup service is basically a more-sophisticated version of using Apple Backup with your iDisk.

In earlier versions of this book, I described a few such services and said that although they might be useful in some cases for easy, supplemental off-site backups, the cost was too high, and the speed too slow, to make them interesting as primary backup destinations. Since then, much has changed: many new services have appeared, prices have fallen, and software has become more sophisticated. As a result, online backups may now be worth serious consideration.

A few things haven't changed, though: whatever other virtues these backup services have, they still can't make bootable duplicates; they're constrained by your Internet bandwidth (meaning they're invariably many times slower than a local network backup); and they could leave you stranded if your Internet connection goes down and you need to restore some files. For these reasons, you should consider Internet backup services as a supplement to conventional backup methods, not as a replacement.

To oversimplify matters, I think of Internet backup services as falling into three main categories: traditional, modern, and BYOS (bring-your-own-software). These are my own, rather arbitrary labels, but I think they provide a useful way of slicing up the landscape.

### Traditional Internet backup services

The term "traditional" may seem odd for a concept that stretches back barely a decade, and I don't mean that these services are obsolete. What sets these services apart is their similar pricing structure, which reflects the higher technology costs from a few years ago—but also a greater emphasis on customer service and, perhaps, more cautious business strategies. Services in this category include the following:

- **BackJack**: BackJack charges $12.50 per month for 2 GB of storage space, with more space available at $2.75 per gigabyte (the per-gigabyte cost decreases as you add storage). An alternate plan, which includes extra, redundant backups, costs $17.50 per month for 2 GB and $6.00 per additional gigabyte (again, with cost reductions as you add storage). See the included $25-off coupon. http://www.backjack.com/

- **Clunk Click:** This backup service, located in the UK, starts at £5 (about $10) per month for 550 MB of storage up through £40 per month (about $80) for 20 GB, with several other levels available. http://www.clunkclick.net/mac_pro.html

- **Datatrieve:** Also located in the UK, Datatrieve uses a Java-based client. They charge £5 (about $10) per month for 1 GB of storage, and £64 (about $130) per month for 20 GB. Intermediate levels and higher storage quotas are also available. http://www.datatrieve.co.uk/

- **Depositit:** Yet another UK service, Depositit offers a variety of plans beginning at £60 (about $120) per year for 250 MB of storage or £720 (about $1450) per year for 20 GB of storage, with intermediate and higher levels available. http://www.depositit.com/

- **FilesAnywhere:** Prices for this service range from $9 per month for 5 GB of data to $225 per month for 120 GB of data. The included software, called FASync, is actually a synchronization program; it creates neither archives nor duplicates. http://www.filesanywhere.com/

- **MacBak:** Focusing on graphic designers, MacBak offers backup services starting at $89 per month, which includes a total of 120 GB of storage, with a maximum of 10 GB uploaded each month. One-time setup fees are an extra $89 per computer. http://www.macbak.com/

- **Prolifix:** Prolifix uses cross-platform, Java-based software. The company charges $9.95 per month for 500 MB of storage and $28.95 per month for 8 GB, with intermediate levels available. (Contact Prolifix for quotes on higher storage quotas.) http://www.prolifix.net/

**NOTE** All these services also compress your data, so you may be able to fit much more on their servers than the amounts listed.

### Modern Internet backup services

The services I classify here as "modern" have significantly lower prices than the "traditional" ones I listed previously. In some cases, they've achieved these lower prices partly by taking advantage of newer, less-expensive technology; in some cases, they've outsourced software development to countries where labor costs are lower; and in some cases they've cut certain corners—spending less money on documentation and customer support or relying on word-of-mouth advertising, for instance. On the plus side, the cost savings makes online backups a sensible choice for a great many more people. On the minus side, only time will tell whether this is a sustainable business model—if you entrust all your data to a company that can't afford to stay in business, you could suffer serious consequences.

The Internet backup services in this category that seem to have reasonably good Mac support at the moment include the following:

- **CrashPlan:** Using Code 42 Software's CrashPlan software, you can back up data to their servers (called CrashPlan Central), to other computers you own, or to friends' computers. The software itself comes in two versions: CrashPlan ($20) and CrashPlan Pro ($60); the latter supports automatic, continuous backup and additive incremental archives, and you can save 10 percent with the coupon at the end of this book. The software can be used without cost, however, if a machine is only a backup destination (not a backup source).

  Storage space on CrashPlan Central costs $5 per month for up to 50 GB and $0.10 per month for each additional gigabyte. CrashPlan is currently my top pick from among Internet backup services; I discuss it in more detail in the software section; see CrashPlan: Breaking the mold.

- **Mozy:** In recent months, Berkeley Data Systems' Mozy has been the source of tremendous Internet buzz. It gives you 2 GB of storage for free, or *unlimited* storage for a flat fee of $5 per month (and there's no extra charge for the Mozy software itself). There's just one catch, but it's a significant one: their Mac client, still in beta at press time, is limited and buggy. It doesn't offer nearly the flexibility of CrashPlan, or even of the Windows version of Mozy. However, if you have an enormous amount of data to back up, that low price covers a lot of evils.
  http://www.mozy.com/

- **Steekup:** This service, based in France but also available in an interesting variety of English, includes a cross-platform, Java-based backup client with a respectable array of options and secure online storage. Prices range from $25 per year for 1 GB of storage to $99 per year for 100 GB of storage.
  http://www.steekup.com/en/

**NOTE** Like the traditional Internet backup services, these services compress and encrypt your data for efficient uploads and secure storage.

### BYOS (bring-your-own-software) Internet backups

The last category of Internet backup services isn't explicitly designed for backup at all—it's just storage space that you can use in whatever way you want. In order to use it for backups, you must supply your own backup software, and in some cases, additional software that enables your backup program to mount or otherwise interact with the storage space. Although there are numerous examples of services like this, I've chosen just a few as examples:

- **Amazon S3:** Amazon.com's S3 (Simple Storage Service) offers virtually limitless—yet reasonably inexpensive—online storage, complete with encrypted transfer. Getting at the storage space so that you can use it for backups, though, requires third-party software and some fiddling. Read Appendix E: Backups with Amazon S3 for details. S3 charges you separately for data storage ($0.15 per gigabyte per month), data transfer ($0.10 per gigabyte for uploads, and $0.13–$0.18 per GB, depending on volume, for downloads), and requests, or operations that affect the data in any way ($0.01 per 1,000 or 10,000 requests, depending on the request type; delete requests are free). http://www.amazon.com/s3/

- **BingoDisk:** This online storage provider offers a variety of plans, starting with 10 GB for $19 per year, up through 100 GB for $199 per year. Because it uses the WebDAV protocol for file access, you can mount your BingoDisk space with the Finder's Go > Connect to Server command. Once the network volume mounts, you can copy files to or from it using your choice of software. http://www.bingodisk.com/

- **OmniDrive:** OmniDrive offers four levels of online storage: free (1 GB), Pro1 (10 GB for $40 per year), Pro2 (25 GB for $99 per year), and Pro3 (50 GB for $199 per year). Their free OmniDrive software lets you mount your online storage space as a network volume; then, you can use almost any backup program to copy your files to or from it. http://www.omnidrive.com/

### Internet backup services: pros and cons

On the plus side, Internet backup services keep your files safely off-site with absolutely no effort on your part—and they do so for every backup, not merely on a weekly (or "whenever-I-remember") basis. They also encrypt your files (unlike Apple Backup) and make their own redundant, off-site copies of your data (though BackJack charges extra for redundant backups). If, despite my repeated encouragements (see, for example, Off-site storage), you are unable or unwilling to store a set of backup media outside your home or office, an Internet backup service can make that process painless. Even if you do maintain diligent off-site backups, an Internet backup service can provide extra insurance for particularly important files.

These services are no substitute for duplicates. As for archives, the biggest issue is speed: even with a fast Internet connection, you could easily spend *weeks* doing an initial full upload of a moderately large hard disk. So you may wish to limit the files you back up with such a service. In addition, think about cost: while the "modern" options are temptingly inexpensive, the "traditional" options could overwhelm your budget if you upload everything. Still, all things considered, if I had to choose just one of these services to recommend at the moment, it would be CrashPlan: not only is their Internet backup service versatile and reasonably priced, but their software can be used for backups on your local network or with a friend's computer, making it a great all-around choice.

## Camcorders

Say you can't afford to buy two or three hard drives. On the other hand, you find optical media too limited in capacity. Then you hear about an amazing product called DV Backup (http://coolatoola.com/). This software enables you to use your FireWire-enabled digital camcorder as a backup device. Because MiniDV or Hi8 tapes are relatively inexpensive and easily reusable, media cost is reasonable—but more importantly, you avoid the expense of conventional tape drives by pressing into service a device you already own. Best of all, a single 60-minute tape can store as much as 16.5 GB of data, and larger backups can span multiple tapes. You may think this is the ideal solution—what's not to like?

I have rather mixed feelings about using a camcorder as a backup device. Well, not truly mixed: I wouldn't do it myself. All right, if I were stuck on a desert island with just my PowerBook and a camcorder, then maybe; as I mentioned earlier, I believe that something is better than nothing. But for regular, day-to-day use, I worry that your camcorder may actually be worse than nothing.

With all due respect to author Tim Hewett, who has done what can only be called an extraordinary engineering job, DV Backup is at the mercy of your camcorder and tapes, which were not engineered to provide the bit-perfect quality you need for backups. DV Backup, to its credit, does provide user-adjustable error correction as well as an optional data verification pass after recording your data. However, you trade security for speed and capacity; at the highest level of error correction, which essentially puts two copies of each data block on the tape, backups take twice as long as without (logically enough) and use up twice the tape. Magnetic tape is notoriously error-prone, so I wouldn't recommend using anything less than the best protection. But doing so significantly reduces the advantages of this approach.

Here are some other reasons I urge you to think twice before trusting your backups to your camcorder:

- The speed of backups and restoration is much slower even than that of optical media, and nowhere near the speed of hard drives.
- Restoring arbitrary individual files is possible (though time-consuming) only if you store your data uncompressed.
- Your computer monopolizes your camcorder. If you want to shoot video, you have to go without backups for a while (and vice-versa).
- Because digital camcorders were not designed for data backup, the (often miniature) electronics may wear out prematurely due to the frequent stops and starts imposed by backup software.

If you still think a camcorder backup is right for you, you can minimize your risks by observing the following advice:

- Buy high-quality tapes, and use only brand-new tapes for backups. And always stick with the same brand of tape for best results.
- Use the SP speed rather than the LP speed.
- Always use the highest level of error correction; always select the auto-verify option; never use compression.

- Perform test restorations of your data on a regular basis.
- Consider supplementing your camcorder with a secondary backup method, such as periodic backups to optical media.

## Joe's Hardware Recommendations

I strongly believe that decisions about hardware should not be made on price alone. You may find the cost per gigabyte of storage to be only $0.15 for DVD-R, for example, versus $1.00 for a hard drive—but that's only part of the story. Speed, convenience, flexibility, and the ability to make bootable backups all add tremendous value to hard drives. Even if you can afford only one external drive, making it part of your backup system will pay for itself many times over in saved time and aggravation. If your budget permits, two or even three moderately large external hard drives are a good way to go.

If you're looking purely for the most economical hardware path, use your built-in SuperDrive and record backups onto DVD-RW media. Your hardware cost is zero, and $50 should buy you enough blank media to last years.

The Iomega REV comes much closer to the sweet spot at the intersection of capacity, speed, and affordability than optical, magneto-optical, or digital tape media, not to mention Zip and Jaz drives, though it's still a bit expensive for my taste. Assuming REV turns out to be reasonably reliable, it's not a bad choice, but I recommend it only if you can comfortably fit a complete duplicate of your main startup volume within the 35 or 70 GB limit of a single REV disk.

**Tip** If you have more FireWire devices than your Mac has FireWire ports, consider picking up an inexpensive FireWire hub rather than daisy-chaining drives together. A hub gives you the ability to connect or disconnect any drive without affecting the others.

Finally, don't overlook Internet backups. If the volume of files you need to archive is reasonably small and your Internet connection is fast, Internet backup services could be a good supplement or a substitute for conventional archives. You might, for example, use a single hard drive for local duplicates and archives, and then use an Internet backup service to provide both redundancy and off-site storage for your archives—without requiring you to move any hardware around.

# CHOOSE YOUR SOFTWARE

When is a backup program not a backup program? A lot of software that calls itself "backup software" does not actually perform backups in the sense we're discussing here. That is to say, some backup programs do not create additive incremental archives, some do not create duplicates, and some do neither!

Unfortunately, because software developers use terms such as "incremental," "archive," and "backup" differently, you may think you're getting certain capabilities when you buy a product that later turn out to be missing. Thus it is extremely important that you read the fine print, and understand exactly what it is you're looking for.

## Duplication Features

Many different applications have the ability to create a bootable backup. This entails copying all the files (including hidden files) on your hard disk to another volume while preserving Unix ownership, permissions, and symbolic links. Assuming you use the correct settings, such applications can also update a duplicate incrementally (rather than recopy every single file each time).

However, you should consider a few other things when looking at a duplication program:

- Can it create a restorable duplicate onto optical media or a disk image? Sometimes this feature is useful, other times not.
- Can it automatically update the duplicates on a schedule?
- When updating a duplicate incrementally, can it also delete files that were deleted on the source volume? If not, your duplicate may include extraneous files that you don't want. (Of the software discussed here that offers both duplication and archiving features, all have the capability to synchronize deletions when updating duplicates.)
- Does it have any other features you might use, such as file and folder synchronization?

The duplication programs I've tried are more alike than different, so for basic duplication needs, just about anything should do the trick. Joe's Software Recommendations, ahead, offers further advice.

**NOTE** **RETROSPECT DESKTOP VS. RETROSPECT EXPRESS**

EMC Insignia’s Retrospect software comes in several different editions, including Retrospect Desktop ($129) and Retrospect Express (bundled free with some external hard drives and optical drives; also available in a special software bundle from Allume called the CheckIt System Performance Suite—see Appendix A: Backup Software).

The two programs are quite similar, the main differences being that Retrospect Express does not support tape drives or client-server backups and that its facility for selecting or excluding files is more primitive. You can find a list of differences, as well as the features of Retrospect’s Workgroup and Server editions, at http://www.emcinsignia.com/en/products/mac_compare.dtml. One important issue not on that list: technical support. No matter which one you have, free support is limited to the FAQs, knowledgebase, and community forums on the EMC Insignia Web site. Paid support is available for both products; EMC Insignia charges $40 per incident for Retrospect Express and $70 per incident for Retrospect Desktop.

In this book, when I refer to “Retrospect” (without any other qualifiers), I mean that the features in question apply to all editions of the program. If a feature is applicable only to a particular edition, I specify “Retrospect Desktop” or “Retrospect Express.”

## Archiving Features

Among applications that provide archiving features, there’s a huge range of variation in how they work—and how easy they make it to restore your work later. The fact that an application stores multiple revisions of each backed-up file does not, by itself, make it good for creating archives.

### Archive varieties

First, there’s an important distinction to make: true archives versus *rotating backups*. In a true archive—that is, an additive incremental archive—every version of every file you designate is saved, but identical files are never duplicated. In a rotating backup, the program creates a complete, separate copy of all your files every day—basically a non-incremental archive. Then, after a certain number of days has passed (specified by the user), the backup program erases the oldest backup and adds a new one.

Rotating backups, because they copy every single file each day, take longer to perform and require more storage space. If you've got room and time, there's nothing wrong with that approach, and it removes the need for a snapshot list (see Snapshots and file lists) since all the files are there. However, because you're erasing files older than a certain date, you're restricting your restoration ability. If you keep, say, 5 days worth of rotating backups and find you need a file you deleted a week ago, you're out of luck.

A few applications offer the best of both worlds: *rotating archives*. Like a conventional archive, new files are added to the backup incrementally (without overwriting older versions). However, to conserve space, you can opt to erase the oldest versions of selected files at the same time—for example, all versions older than 30 days, or versions copied more than 30 sessions ago.

**WARNING!** Not every program uses the same criteria to determine when a file should be added to an incremental archive. Some rely exclusively on modification dates, which is an error-prone method. For instance, simply changing the name of a file does not change its modification date. And some applications do not correctly set the modification date each time you save a file.

Most backup software is intelligent enough to figure out when a file has changed, regardless of its modification date—or at least provide an option to check other criteria. But some is not. Worse, unless you carefully crosscheck archived files against the originals, you may not notice such an error until it's too late.

The best way to guard against this problem (apart from buying high-quality backup software) is to spot-check the modification dates of files from applications you use frequently to be sure they were correctly updated the last time you saved them.

### File format, compression, and encryption

To oversimplify somewhat, most software employs one of two basic methods to copy files when performing a backup. One way is to copy each file in a stand-alone Finder-readable format, so that the backed-up files look and act exactly like the originals. Another way is to copy all the files into a single, larger file (sometimes called an archive file or a backup set). Each approach has advantages and disadvantages.

Finder-format copies can be restored without the use of a backup program—just drag and drop. Some people also feel more secure knowing they can get at their files easily even if their backup software goes south. Of course, the backed-up files generally take up exactly as much space as the originals (see just ahead for a discussion of RsyncX, which changes this equation somewhat).

Archive files can be compressed as they're stored, potentially saving a large amount of hard disk space. They can also be encrypted, so that if your backup media were lost or stolen, no one could read your files without knowing your passphrase. And unlike Finder copies, which normally take as their owner the user name of the person currently logged in, archive files can preserve original Unix ownership and permissions. Of course, you will need the backup software to restore files, and you could have a slightly higher risk of data loss due to file corruption (since all the data is stored in a single file)—but most backup software has verification mechanisms to compensate for this.

**NOTE** Not all programs that offer compression or encryption copy data into a single archive file. A few can compress or encrypt individual files, such that they can be moved or copied (but not opened) in the Finder. You must still use the backup software to restore them to their original state. Other backup programs use compressed disk images (discussed just ahead)

RsyncX (based on the open-source command-line program **`rsync`**) deserves special mention here. Its unique copying method produces space-saving incremental archives that nevertheless look and act like complete Finder-readable copies. Here's how it works: When you perform your first archive backup with the Rotating Backup feature, RsyncX makes a complete copy of the selected files—with Unix ownership and permissions intact. When the next incremental backup runs, the program creates a new folder that *appears* to contain another complete copy of all your files. In fact, only modified files are copied; for files that haven't changed, RsyncX uses a Unix trick to create a link to the original copy that appears in the Finder to be an ordinary file. This link functions somewhat like an alias in that it takes up virtually no space and merely points to another file. But when you copy this special link to another volume (when restoring files, say), you automatically copy the entire file. The upshot of this technique is that RsyncX comes quite close to offering the best of both worlds: Finder-readable files that require no more space than an archive file.

However, you should also be aware of another option: disk images. Some backup software, at least when backing up to a hard disk, stores files in a disk image. (Apple Backup 3 uses this technique, although its disk images are hidden inside packages that look like ordinary files.) Like an archive file, a disk image is a single file that contains all your other files—and can optionally be compressed, encrypted, or both. The difference is that you can double-click a disk image, and after supplying the passphrase (if necessary) it will mount on the Desktop as a regular volume—after which you can read and copy files using the Finder. Sounds great, doesn't it? It can be, but keep in mind that in most cases, each incremental archive backup is stored on a *separate* disk image, so without a snapshot or file list provided by the backup software (see "Snapshots and file lists," just ahead), restoration can be quite involved.

When making a duplicate onto another disk, Finder copies are obviously mandatory. For archives, though, I strongly prefer a format that offers compression and encryption—and in this respect, archive files are generally more elegant and convenient than disk images.

**NOTE** Maxtor OneTouch drives include software with a feature called DiskLock, which prevents access to the drive's contents unless you enter a password. DiskLock does not encrypt the drive's contents, though—it merely hides them. Although this feature may protect your data from a casual snoop, it won't stop a determined hacker nearly as effectively as encryption will.

## Snapshots and file lists

When it comes time to restore files from an archive, you must be able to locate the versions you're looking for quickly and easily. Some backup programs facilitate such restorations by offering *snapshots*—lists of all the files on your computer as they existed at the time of each backup, even if they were already present in the archive and therefore not copied during that particular session. Suppose you want to restore all the files on your machine as they existed last Tuesday. Having a list of all the files as they appeared on Tuesday—and an automated way to restore them—can be extremely valuable.

On the other hand, imagine that you want to look back at every version of just one particular file as it existed over the past month. In this case, you don't want to wade through snapshots—you simply want a list (sorted by file name or date—or better yet, searchable) of each version of the file in the archive, from which you can choose just the ones you want. Without either a snapshot or a file list, you'll need to locate each version of the file manually—often in a series of dated folders. This makes for a long and tedious restoration. (For another take on dealing with multiple versions of files, see Version Control.)

## Sources and destinations

The volume *from* which you back up files is known as the *source*; the volume *to* which you back them up is known as the *destination* (or target). Be sure the software you select can accommodate the sources and destinations you wish to use.

All backup programs can copy data from your startup disk. Most can also copy data from other attached hard drives, network volumes (including AppleShare volumes, FTP servers, and iDisks mounted in the Finder). And usually you can select arbitrary folders or files anywhere on those volumes to be backed up. However, there are exceptions. Backup Simplicity, for example, supports only your startup volume.

**NOTE** Even if your backup software supports copying files from a mounted network server, you will generally be unable to make a *bootable* backup of a network volume. As far as I know, only Retrospect offers this capability.

In most cases, your range of destination options also includes any Finder-mountable volume. (So, you could even back up one network volume to a different network volume if you wanted to.) If you wish, you can even back up your files onto a disk image. Most programs require that you manually create the disk image using Disk Utility and mount it in the Finder before you can use it as a backup destination.

A similar issue exists with optical media. A backup program can support recordable CDs and DVDs in either of two senses:

- You pop a blank disc into your drive, give it a name, and allow it to mount in the Finder. The backup software sees the disc as a possible destination like any other volume. After running the backup program, you then return to the Finder to manually burn and eject the disc.
- The backup program itself asks for blank media when needed, writing to it directly without the intervention of the Finder.

The first way of supporting optical media is trivially easy for software developers to implement, so that is how many backup programs work. But this approach does have some problems. First, it requires much more human intervention—performing manual steps despite the fact that the backup itself runs automatically on a schedule. Second, it eliminates the possibility of *multisession* recording (the ability to record additional chunks of information on a partially used disc after the initial write session) since the Finder does not include this feature. This is a problem because without multisession capability, you will use a much larger number of discs—increasing not only media cost, but inconvenience. (Note, however, that some applications, including Retrospect, use a packet-writing technique to add data to partially used optical discs. This is even more efficient than multisession support, but it means that only the application used to record the discs can read them later.) Therefore, if you need to record backups onto optical media, I strongly recommend using an application with multisession (or packet-writing) support.

A related issue is what I'm going to call *media spanning*. Suppose you have more data than will fit on a single CD or DVD—or even that you have a single file that's too large to fit on a single disc. Some backup programs intelligently manage backups that span multiple discs, prompting you for new media when required during a backup (splitting files if necessary), and asking for the proper discs when restoring files (rejoining split files). Although the need for media spanning could affect those backing up onto hard drives as well, it's most crucial for those using optical media. Only a few backup programs offer media spanning, and even fewer include both media spanning and multisession or packet-writing support.

## Selectors and exclusions

Selective archive backups (see Archive strategy) do not include every file on your hard disk. But archiving even your entire home folder may be overkill, since it includes things like cache files, which serve no useful purpose in the context of a backup, and digital media files (such as MP3s ripped from your CD collection), which, because they change infrequently, are adequately backed up by your duplicates. So instead of simply selecting one or more folders to archive, you may wish to explicitly include or exclude certain types of files.

Some backup programs include user-definable criteria specifying which files should be included (selectors) or excluded (exclusions) from a particular folder or volume—and a few programs offer both. Depending on the program, these criteria may include file names, sizes, Finder labels, extensions, modification dates, and other factors.

In general, I find exclusions more useful than selectors, though I would not generally consider either an absolute must in a backup program. Your mileage, of course, may vary.

## Ease of restoration

No matter how easy it is to back up your hard disk, if your software makes it difficult to restore files, you're going to be unhappy with it. After all, a backup that you can't restore is worthless. Backup programs typically offer one of three main approaches to restoration:

- **Finder restoration:** The backup program has no Restore command; to restore files, you drag them manually from the backup volume onto your hard disk. This is fine if you're restoring an entire folder, but if you've done an additive incremental archive, you may have to sort through dozens or hundreds of folders to locate the right versions of each of your files.

- **Reverse backup:** In this scheme, the backup program once again does not offer a Restore command, instead it expects that you'll swap the source and destination locations and perform your backup again—in reverse. While this may reduce manual effort somewhat, it's still going to be a hassle when restoring versioned files from an archive (except, perhaps, in the case of RsyncX, as I discussed previously). And even in the best cases, a reverse backup can be confusing and stressful, because it's easy to get the source and destination mixed up when their contents are so similar.

- **A Restore command:** The backup program (usually) keeps track of all the files you backed up during each session, allowing you to copy them back to their proper locations—or another destination of your choice—with a few clicks. In most cases, before starting the restoration, you can choose a subset of the files, or even pick out one version of a single file if that's all you need. Restore commands and snapshots tend to appear together.

It probably goes without saying that I prefer applications with a Restore command—they make the restoration quicker and easier. Of course, the presence of a Restore feature does not, by itself, mean the process will be easy, but it's a hopeful sign.

### Restoring a full archive as a bootable volume

If you choose to perform a full (rather than selective) archive, bear in mind that not all backup software can restore your archive from an arbitrary point to a blank disk in such a way that the resulting volume will be bootable. In order for a restored full archive to be bootable, several things must be true:

- All files needed for your computer to start up—including many hidden files—must be included in the backup and restored later.
- The backup software must preserve Unix ownership, permissions, and symbolic links during the backup and restoration processes; doing so requires that you enter an administrator's password.
- When restoring the files, the destination disk must not contain any extraneous files that could interfere with booting; normally, this implies erasing the disk before restoring the archive.

Most backup software that provides both duplication and archiving features also enables you to restore a full archive as a bootable volume, assuming that you set it up properly. Some programs, however (notably Synchronize Pro X), can restore a bootable volume only from a duplicate, not from an archive. A few applications permit full archives to be restored as bootable volumes, but lack a snapshot feature—meaning you must manually locate and copy a large number of documents to return your disk to the state you wish to recreate.

## Ease of Use

In addition to ease of restoration, an application's overall ease of use is also important. The interface should be self-explanatory—ideally, clear enough that you can figure out how to perform a basic backup and restoration without ever looking at a manual.

If your backup software is difficult to learn or set up, you're less likely to use it. So you want an application you can configure in an hour or so—not something that takes you an entire day to figure out. You also want your backup software to perform its duties on a schedule with as little interruption to your routine as possible. The best backup software would be completely invisible, working silently behind the scenes until you needed it.

Even so, don't underestimate the importance of good documentation. A well-written manual can be a godsend when trying to comprehend the minutiae of rotating archives or client-server configuration.

## Support and Reputation

Some backup software is published by individuals who like to program in their spare time. At the other end of the spectrum, some backup software is published by large corporations with a small army of programmers and a full-time, paid technical support staff. Ironically, I've often received better and quicker technical support from individual authors—even those who give away their applications for free—than big companies. On the other hand, if you're entrusting all the data on the computers in your home or small office to a backup application, you may feel more comfortable knowing that a professional staff stands behind the product.

**NOTE** **COMMAND-LINE BACKUPS**

As I mentioned in the Introduction, this book is mainly about backup applications with user-friendly graphical interfaces. However, it is also possible to create a backup system using Unix command-line tools. If you're curious to know what's involved in doing this, consult Appendix D: Unix-Based Backups.

Of special note in this regard is EMC, developers of Retrospect. They charge $70 to speak to a technical support representative on the phone—a seemingly outrageous fee. However, I've used technical support from Dantz (which was purchased by EMC) more than once, and I believe you get what you pay for. The technicians answer promptly, are highly trained, and continue working with you—even over multiple phone calls—until the problem is solved (without charging you for each call). When I'm terrified that I might have just lost all my data and my software doesn't seem to be functioning correctly, I'm only too happy to pay $70 for the reassuring voice and advice of an expert who can help me get things working again.

## Price

The backup software included in Appendix A: Backup Software ranges in price from free to $129 (before discounts). The price does not necessarily correlate to capabilities, but I urge you not to skimp when it comes to backup software just to save a few dollars. After all, time is money. If you lose a day of income because your backup program makes you jump through too many hoops when restoring files, that's likely to be a bigger financial hit than the cost of better software.

## Joe's Software Recommendations

Having reviewed the most important criteria for selecting backup software, I'd like to give you some specific recommendations. (Appendix A: Backup Software provides Web addresses and pricing information for each program.)

In the past, I recommended using a single program for both duplicates and archives on the grounds that it should save you both money and effort, ensure that you will not experience conflicts in schedules or requests for blank media, and generally make for a less complicated backup system. Given recent developments in backup software, that's somewhat less true than it once was. There's still an admirable simplicity to using just one program for all your backups, but you may achieve better results all around, and perhaps even save money, by using one application for archives and another for duplicates.

## Combination (duplication+archiving) software

The following applications offer both duplication and archiving features as I described them here, as well as scheduled backups:

- Backup Simplicity
- Data Backup
- Déjà Vu
- Retrospect Desktop
- Retrospect Express
- RsyncX
- Synchronize Pro X
- Synk Pro
- Tri-Backup

In a pinch, any one of these could potentially do the trick. That's not to say they're equivalent, though—or even adequate for most user's requirements. You can examine each program's features and price in Appendix A: Backup Software to see which one best meets your needs. But allow me to offer some advice:

- If you back up to CDs or DVDs, you want software that can automatically split large files to span media and does multisession or packet recording—making Retrospect the only good option.
- If you back up to a hard disk, I recommend both compression and encryption; and you shouldn't have to create and manage your own disk images to get them. This consideration leaves Data Backup, Retrospect, Synk Pro, and Tri-Backup as candidates.
- If ease of restoration is a significant concern to you—and it should be—choose an application that offers snapshots, enabling you to restore all the files from a given point in time in one fell swoop. Your choices once again include Data Backup, Retrospect, and Tri-Backup. RsyncX also qualifies here; even though it doesn't offer snapshots as I define them, it doesn't truly need them, because each incremental archive effectively functions as its own snapshot. RsyncX's method for storing archives makes restoration from an arbitrary point in time fairly easy.

- And finally, if you need to back up multiple computers to a single server, you'll be best served by an application that offers true client-server operation—meaning Retrospect Desktop or RsyncX.

### *Retrospect: The (g)old standard?*

Astute readers may have noticed that Retrospect popped up in each of those lists. Retrospect Desktop is the most expensive of the programs I discuss here, at $129 (though you can frequently find it at a significant discount), but it's far and away the most full-featured Mac backup application.

On the other hand, Retrospect has some disadvantages. It has a steep learning curve, making it intimidating for less technically inclined users. (I offer advice later, in Appendix B: A Retrospect Primer, to ease your initial configuration.) I've also encountered bugs from time to time—and technical support, should you need it, is pricey. And, EMC is sometimes slow to add support for newer storage devices; if you buy the latest and greatest optical drive, you may have to wait several months before an update includes the necessary driver. (FireWire hard drives are always supported automatically.)

Causing more concern, since Retrospect was acquired by EMC, it's had few updates and has given the appearance of significantly slowed development. Even as of mid-2007, there is no Universal Binary version of Retrospect, meaning that it runs more slowly than it should on Intel-based Macs. Although EMC has stated that it will update Retrospect for Leopard compatibility, a number of signs suggest that the Mac version of Retrospect could be on its last legs.

For these reasons, although I've long recommended Retrospect as my top choice in Mac backup software—and although it still has features unmatched by any other product—I'm finding my enthusiasm waning. If you already own a copy and it's working well for you, by all means continue using it. If you have a PowerPC-based Mac and need some of Retrospect's unique features, I still think it's a fine choice. (And if you happen to purchase a drive that includes a free copy of Retrospect Express, that's an equally good option unless you need to perform client-server network backups.) But I have a hard time recommending Retrospect as a new purchase for people with Intel-based Macs, especially with the recent improvements in Prosoft's Data Backup 3 and the prospect of Time Machine on the horizon. (This book includes a coupon for 50% off Data Backup.)

The bottom line: If you're choosing an application from this group, think about Data Backup, Tri-Backup, and Retrospect—in that order. But also consider using one program for duplicates (SuperDuper or Carbon Copy Cloner) and another for archives (such as CrashPlan).

### Duplication software

The following applications (including some that bill themselves as "backup" or "synchronization" software) can create bootable backups but *not* additive incremental archives:

- BounceBack Professional
- Carbon Copy Cloner
- Clone'X
- CopyCatX
- FoldersSynchronizer
- MimMac
- Personal Backup X4
- SilverKeeper
- QuickBack (part of SpeedTools Utilities)
- SuperDuper
- Xupport

Although each of these applications has a different interface and a variety of additional features, as far as I'm concerned they're all more or less equally capable in terms of making a bootable backup of an entire hard disk for the average home or small-office user. Most of these applications offer limited-time demos or trial versions, so if you're considering such an application, you can download a copy and make sure it meets your needs before making a purchase.

I do, however, want to mention one unusual capability. Version 3.0 of Carbon Copy Cloner can create a bootable duplicate *onto a network volume*. That doesn't mean you can boot over the network, but it does mean that you can restore a duplicate over the network and then boot from it, or directly connect the target drive to your Mac via FireWire (or USB, for Intel-based Macs) to boot from it. The only other Mac backup program I'm aware of that can pull off this trick is Retrospect.

If you want to create a bootable duplicate onto a disk (or a partition of a disk) connected to a network volume—without spending $129 on Retrospect—Carbon Copy Cloner is what you need.

Apart from that specific situation, if I had to recommend just one program from this list, I'd give the nod to SuperDuper—in addition to a thorough feature set, it excels at giving plain-English explanations of what it's about to do, making a potentially troubling task much less nerve-wracking. It also preserves some metadata that some other utilities don't, making for the most exact copies you can get. Although the full version costs $28, you can use the free demo version to create one-off duplicates; buying a license unlocks features such as scheduling and incremental updates.

But if you happen to have another of these utilities (or prefer a different interface for some reason), any of them should do the job.

**NOTE** **DISK UTILITY AND DUPLICATION**

Although Apple's Disk Utility, included with Mac OS X, can make bootable duplicates, I omitted it from the list here because this feature is obscure (it's a side-effect of a Restore feature) and limited (you have almost zero control over what happens during duplication—and no scheduling capability).

If you *must* use Disk Utility to make a duplicate, follow these steps:

1. In Disk Utility, select any volume in the list on the left and click the Restore tab.
2. Drag the volume you want to duplicate from the list on the left into the Source field.
3. Drag the destination volume from the list on the left into the Destination field. (This works even though the field looks disabled.)
4. Select the Erase Destination checkbox.
5. Click Restore.

### Archiving software

The following applications offer additive incremental archives, but lack the capability to create bootable backups:

- Apple Backup 3 (but not earlier versions)
- Archive Assistant (part of StuffIt Deluxe 10.0 and later)
- BackupSW
- BRU LE
- ChronoSync
- CrashPlan Pro
- Dobry Backuper
- Mozy
- NTI Shadow
- Steekup
- SmartBackup (formerly known as SyncupX)

Unlike the programs that offer only duplication features, these applications vary significantly in their capabilities (see **Table 4** in "Appendix A: Backup Software").

As with the combination applications, desirable features for optical media backups include media spanning (offered by Apple Backup, Archive Assistant, BRU LE, and Dobry Backuper) and multisession recording (absent in all of these). Several of these applications, including Apple Backup and Dobry Backuper, require considerable scratch space (up to the size of one disc—CD or DVD), which reduces their usefulness for backing up almost-full volumes.

Compression is found in Apple Backup, Archive Assistant, BRU LE, BackupSW, CrashPlan Pro, Datum, Dobry Backuper, Mozy, and Steekup. Only Archive Assistant, CrashPlan Pro, Mozy, and Steekup offer encryption. BackupSW provides client-server operation (of a sort), while CrashPlan Pro can perform either client-server or peer-to-peer backups, as well as Internet backups. Apple Backup, CrashPlan Pro, and Mozy provide snapshots; the others make restoring of an arbitrary day's worth of files unnecessarily complex.

Given those features and the impressions I've formed from a great deal of testing, I can't get terrifically excited about the current versions of Archive Assistant, BackupSW, ChronoSync, or SmartBackup as archiving programs. I'll say a few words about each of the others, though:

- **Apple Backup 3:** Unlike earlier versions, Apple Backup 3 offers very respectable capabilities and a reasonable interface. *If* you're a .Mac member, and *if* you're backing up to hard drives, and *if* you're the only user on your machine, Backup 3 makes a fine choice, and you can get it without any additional expense. (See the sidebar on the next page, "Backup 3: A Big Step Forward," for more details.) However, if you don't meet those criteria, you can get a better solution for less money.

- **BRU LE:** BRU LE is a fairly robust application, but it's designed primarily for use with tape libraries. Performing backups to a hard disk or optical media with BRU LE is less than ideal, and despite some recent improvements, I find the user interface to be overly complicated—setting up even a simple archive requires several confusing steps. But if you're willing to master its interface (admittedly, a less daunting task than with Retrospect), you may find that it can be persuaded to carry out all sorts of complex backup tricks.

- **CrashPlan Pro:** If you have more than one computer (or if you're willing to use a server or a friend's computer as your backup destination), CrashPlan Pro is my top pick from this list. It won't help you if you need to back up to optical media or (at least in the current version) a locally attached hard drive, but otherwise its features, ease of use, and price are compelling. I say more about CrashPlan ahead in CrashPlan: Breaking the mold.

- **NTI Shadow:** Somewhat like Versomatic (see Versomatic), NTI Shadow offers the option to archive a copy of selected files every time you save them. In this way, it functions as a cross between a backup utility and a version-control application. However, in other respects, it's a bit thin on features I consider important in archiving software.

## SIDEBAR Backup 3: A Big Step Forward

In earlier versions of this book, I made no secret of my dislike for Apple's Backup application. Backup versions 1 and 2 did not even qualify as backup software in my estimation, since they offered neither archiving nor duplicating capabilities. But in late 2005, Apple released an entirely new, rewritten-from-scratch Backup version 3. I'm delighted to be able to say it's no longer terrible! In fact, it has some downright useful features and a comprehensible user interface. Most importantly, it now creates additive incremental archives, thus qualifying it as a "real" backup application.

However (and you knew there would be a "however"), despite these significant improvements, I have a few reservations about Backup 3.

First, it still can't create duplicates. This is not a deal-breaker—you can use any of dozens of other applications to do that, and some of them are even free—but you'll then have to set up and maintain two different backup applications.

Second, it only backs up files belonging to the currently logged-in user. If you're the only person using a machine, that's no big deal. But if two or more users share a Mac, each one must log in and run Backup separately to back up that user's files. Virtually all other backup programs can handle data for multiple users at once, correctly maintaining ownership and permissions for each user.

Finally, although Backup 3 can handle optical media just fine (and ably spans your data across multiple discs when necessary), it cannot write to a given disc in more than one session. So if, during a certain backup run, Backup needed a new DVD for just the last megabyte of data, all the rest of the empty space on that DVD would go to waste. You could not write anything more to it during your next backup run; you'd have to provide a new, blank disc. This limitation can greatly increase your media costs.

I'm happy to recommend Backup as an archiving tool for .Mac members who have just one user account, and who are backing up to hard disks (avoiding the optical media problem just mentioned). For everyone else, though, stick with one of the more mature third-party products such as Retrospect, Data Backup, or Tri-Backup.

### *CrashPlan: Breaking the mold*

One particular archiving program requires a bit of elaboration, because it's unlike all the rest in several respects. CrashPlan doesn't fit into my previously neat divisions between hardware and software, local storage and Internet services, or push/pull and client-server network backups. It's a refreshingly different way to think about backups. (See the back of this book for a CrashPlan coupon.)

The key component of CrashPlan is its eponymous software, which is capable of creating archives (but not bootable duplicates) using any of several destinations:

- **CrashPlan Central:** Send your data over the Internet and store it on Code 42's servers for as little as $5 per month (for up to 50 GB).
- **Another computer on your local network:** You can use CrashPlan to set up client-server or peer-to-peer backups on your local network. So if you have three computers, for example, one could serve as the sole destination for all the backups—or they could all back up each other's files.
- **A friend's computer anywhere on the Internet:** Any computer in the world with high-speed Internet access (Mac, Windows, or—soon—Linux) can serve as a host for your files. You can even back up your data to several friends' computers, and optionally back up their data on your disk as well.

(Curiously absent from this list is an external hard drive; at the moment, you can't designate a volume mounted on your computer as a backup destination for your own files, but Code 42 says this feature is on its way.)

CrashPlan is different in other ways, too. For one thing, it has the unusual capability of incrementally updating *portions* of files—if you change just a few bytes of a huge file, CrashPlan copies only the changed part on its next run, not the whole thing, saving time and storage space. (The basic edition of CrashPlan stores just the most recent version of each file, while CrashPlan Pro creates true additive incremental archives, with as many old versions as you want.) And, rather than running backups on a fixed schedule, such as once a day, CrashPlan Pro can dynamically watch your computer as you work, backing up any new or changed files right away (or after a user-defined delay). This means that backups, after the first one, appear to take no time at all; they simply happen automatically in the background as needed.

In almost every case, CrashPlan simply does the right thing without presenting lots of confusing options. Backups are always compressed and always encrypted, so you need not worry about your friend being able to read the data you've backed up to his computer. Files you've modified more recently are backed up first, so that even if you're waiting days for an initial full backup over the Internet to finish, the files likely to be most important to you are protected; it even backs up multiple versions of files you modify while that backup is in progress. You can specify files, folders, or extensions to exclude, set times when CrashPlan won't run at all, and throttle its bandwidth use if need be.

CrashPlan still has some rough edges, though. RAM usage is extremely high, for example, even during times when CrashPlan is set not to run. Documentation is virtually nonexistent. Some of the default settings are weird and problematic—most troubling, unless you intervene, CrashPlan stores all your backed-up files *inside the CrashPlan application itself*, which can make that single file balloon to many gigabytes in size.

However, despite CrashPlan's current deficiencies, it does enough things right that it's well worth considering as a tool to create your archives—either instead of, or in addition to, conventional backup software. If you choose to use CrashPlan, keep in mind the following:

- Mutual peer-to-peer backups on your local network (I back up to you, you back up to me) can reduce your need to buy separate hard drives, assuming each computer's internal drive has enough free space.

- If you *don't* have enough free space on your drives for peer-to-peer backups, you can use any one of your Macs as the destination for all the others, choosing an external drive on that Mac as the location for backup data.

- Although an online backup (to CrashPlan Central or another remote computer) gives you an offsite copy of your data, both backing up and restoring files over the Internet can be very slow. You may wish to have other offsite backups as well.

# Set Up Your Backup System

You've laid out a backup strategy, procured the necessary hardware and software, and now have a stack of boxes and discs on your desk. Now it's time to set everything up, run your first backups, and verify that they work correctly. Because I don't know which hardware and software you've selected, I can't give you detailed setup instructions. However, I want to outline the procedures you should always follow.

## Test Hardware First

If you've purchased hard drives or other external devices, connect them and make sure your computer can write to and read from them before installing your backup software. Although I've seen a few cases in which a backup application can communicate with a device that does not otherwise appear visible to the computer, this rarely happens with hard drives and optical drives. If you connect a device after installing your backup software and it does not work, it will be harder to determine whether the device or the software is at fault.

## Partition Hard Disks

If you're using hard drives for backups, you may wish to partition the disks. (To determine how large each partition should be, review Does size matter? earlier in this book.) To partition a hard disk:

1. After connecting the drive, launch Disk Utility.
2. From the list on the left, select the hard disk you want to partition, and click the Partition tab on the right.
3. Under Volume Scheme, choose the number of partitions you want. For each partition, give it a name, and choose a format. Mac OS Extended (Journaled) is the default and recommended choice.

**Warning!** If you want to be able to boot into Mac OS 9 from this volume (and if your machine supports that option), be sure the Install Mac OS 9 Disk Drivers checkbox is selected. (This setting applies to the whole disk, not to a particular volume.) You can't change this later without erasing the disk again, so if in doubt, leave the box checked.

4. Resize the partitions manually by dragging the dividers, or enter a size for each partition.

5. When you're happy with your settings, click Partition. You can then quit Disk Utility.

Your hard disk is now partitioned into multiple volumes, each of which will show up in the Finder as an independent disk.

**SIDEBAR**

### PARTITIONING WITHOUT REFORMATTING?

Four utilities offer the capability of partitioning your hard disk *without* having to reformat it first, preserving all your data. I've generally found such utilities to be frustratingly slow; I've also read numerous reports of data loss when using these tools. Therefore, I strongly recommend that you not attempt to repartition a drive without backing it up first—and if you're going to do that anyway, these tools lose much of their appeal. Since you can buy a moderately sized external hard drive for the cost of one of these applications, using Disk Utility to partition your drive still seems like the best deal.

- **Drive Genius:** This $99 application from Prosoft Engineering offers disk testing, repair, and optimization. You can also use it to add, delete, or resize partitions without reformatting a drive—though it can't merge two partitions, keeping the data from both intact (http://www.prosofteng.com/products/drive_genius.php).

- **VolumeWorks:** The $60 VolumeWorks from SubRosaSoft is basically the partitioning portion of Drive Genius packaged as a stand-alone product (http://www.SubRosaSoft.com/Mac_Software/OS_X/Drive_Repartition/VolumeWorks).

- **DiskStudio:** Micromat's $50 DiskStudio provides only partitioning tools, not testing or repair. Like Drive Genius, it can add or delete partitions without erasing your entire disk. But it offers no way to *resize* partitions (http://www.micromat.com/?option=com_content&task=view&id=33).

- **iPartition:** From Coriolis Systems, the $45 iPartition, like DiskStudio, is strictly a partitioning tool. Unlike DiskStudio, it can resize partitions without erasing your data. It does not include its own bootable CD—to use it on your startup disk, you must boot from another volume or create your own bootable CD that includes a copy of iPartition (http://www.coriolis-systems.com/).

## Install and Test Software

Installing backup software may be a simple matter of dragging a downloaded file to your Applications folder, or you may need to run a more complex installer. In any case, follow the developer's directions to install your backup software now.

**TIP** If you have more than one startup volume (not counting duplicates), consider installing your backup software onto each of them. This will make things easier if your main disk is unavailable and you need to restore files.

Read, or at least thoroughly skim, the documentation that came with your backup software. Acquaint yourself with the terminology the program uses and how its features are organized. Backup programs are notorious for being unintuitive, so spending some time with the manual before you do any heavy-duty configuration will save you grief later.

Next, just to get your feet wet, try backing up one arbitrary file (or small folder) from one volume to another—and then restoring it. This seemingly small step can go a long way toward helping you to understand how the software works.

## Label Media and Files

Most backup programs ask you to give descriptive names to each recurring backup procedure—"Daily Archive," "Weekly Duplicate," "Backup Set A," or whatnot. Some applications use these names to label archives, bookmarks, catalogs, or other files stored as part of the backup, while others simply use them as an internal reference. In any case, applications usually make a distinction between the name of a given backup and the name of the media on which it is stored. You may duplicate a volume named "Greg" onto a volume named "Marcia," and you may store your daily archive, which you've named "Backup Set Delta," onto a volume named "Cindy." If you aren't careful with these names, confusion can easily result.

I strongly recommend consistency and clarity in names. Here are some specific guidelines:

- If you are using hard disks, give each volume (disk or partition) a different name in the Finder. Although you can use sequential letters or numbers to label the volumes, longer and more meaningful names may be less confusing. For example, if you use two rotating disks, each partitioned into two volumes, the first drive might have a piece of tape on it with the name "Bart." Bart could be partitioned into a volume named "Bart Duplicate Disk" and another named "Bart Archive Disk"; another drive, labeled "Lisa," would have "Lisa Duplicate Disk" and "Lisa Archive Disk." Notice that I used the word "Disk" to differentiate the name of the volume from the name of the backup procedure.

- Resist the temptation to name the backup disks the same as the source disks! After all, you'll still be able to boot from "Greg" if duplicated onto "Homer Duplicate Disk."

- If your software asks you to label backup procedures, *scripts*, files, or backup sets, follow a similar pattern, but add the frequency. For example: "Bart Weekly Duplicate" or "Lisa Daily Archive." And be sure to store a given backup on media with the corresponding label! That way you can easily keep track of which backup is stored on which media, without getting the labels of the procedures confused with the labels of the volumes.

- Put *physical* labels on all media (which could be writing on a CD with a marker or sticking a piece of masking tape on a hard drive). The label should indicate the names of the volume(s) on the media.

- For multi-CD or -DVD sets, be sure to label each disc separately, following the name and sequence number the software gives it.

## Set Up Duplicates

With your hardware and software installed, it's time to configure your first serious backup: a duplicate of your startup volume. The exact procedure varies from one application to the next, but I walk you through the basics.

**TIP** For detailed instructions on setting up duplicates in Retrospect, see Set Up a Duplicate Script.

In your backup application, select the function for making a bootable backup. Some applications distinguish between commands that are performed immediately and commands that can be performed on a schedule. Given the choice, select the option that can be scheduled.

Some applications require that you select a checkbox or otherwise indicate whether Unix ownership and permissions should be preserved; for duplicates, they should. If the application includes an option to follow aliases and symbolic links, be sure to *deselect* it.

If requested, give your duplication procedure a descriptive name, and select a source and destination volume. Keep in mind that the destination volume, if a hard disk or partition, must be at least as large as the amount of data on the source volume. Also, check to see that the destination volume does not ignore ownership; if it does, your duplicate will not be bootable. To check this, select the destination volume's icon in the Finder and choose File > Get Info. In the Ownership & Permissions portion of the window, make sure the checkbox labeled Ignore Ownership On This Volume is *deselected*.

You may have an option to turn incremental duplication on or off. If so, be sure to turn it on! Otherwise, every time you perform the duplication, the application will copy every single file on your hard disk, even though most of them have not changed.

If your application offers compression and encryption, be sure to turn them off. On the other hand, if it offers *verification* (checking that files were written properly), turn it on. Without verification, errors in writing files may go unnoticed, and even a tiny error in a single file could prevent your duplicate from working properly.

Finally, start the backup. Often this is just a matter of clicking a "Backup" button. (I look at adding a schedule for this script later in Automate Your Backups.)

Now wait. Even if you have a fast computer, a fast hard drive, and a fast interface, duplicates can take some time. In some cases, you'll be able to continue using your computer while the files are being copied, but remember that if you modify files during this process, the duplicate will no longer be an accurate copy of your entire hard disk as it existed at a single point in time. It may be worth noting how much, if at all, the operation of your computer slows down while a backup is in progress, because this could affect when you schedule backups to run (see Automate Your Backups, ahead).

After testing your duplicate (see below), you can repeat this procedure to set up duplicates on additional hard disks or other media. If you are creating duplicates of more than one volume, set up those additional volumes at the same time.

## Test Your Duplicate

Even if your backup application reported no errors, you should test the duplicate to make sure it truly is bootable. If your duplicate was stored directly on another hard disk, testing it is easy. (If it was stored on optical media, see Restore a CD/DVD duplicate onto a hard disk. Follow these steps:

1. Open System Preferences and click the Startup Disk icon.

2. Select the volume where your duplicate is stored. (You *did* give it a unique name, right?)

**NOTE** If you duplicated your hard disk to an external drive connected to a server, you must physically connect that drive directly to the Mac you want to start up. If it's on another machine, it will not appear in the Startup Disk preference pane. The only way to boot a Mac over a network is to use NetBoot to load a special disk image stored on a central machine running Mac OS X Server; an ordinary hard drive won't work, even if it contains a bootable copy of Mac OS X.

3. Click Restart.

4. After your computer restarts, verify that it used your duplicate as the startup volume. If your Finder preferences are set to display mounted hard disks on the Desktop, the one shown at the top is your startup volume. (To set this preference, choose Finder > Preferences, click the General icon, and make sure the Hard Disks checkbox is selected.)

If your computer did not start from the correct volume, restart it again, holding down the Option key until the screen displays icons for each of the valid startup volumes. Click the volume you wish to use and then click the right arrow button to complete the startup.

**TIP** If your computer refuses to boot from a FireWire drive even after holding down the Option key at restart, one possible cause is a conflict with other FireWire devices (such as an iSight camera). Disconnect all other FireWire devices from your system and try again with only your external hard drive attached.

5. Do a few spot checks to confirm that important files are where they should be, that you have network access (try viewing a Web page), and that a few applications launch. I recommend *not* checking your email, though, as doing so may download messages and delete the originals from the server—you'll miss them when you return to your usual startup disk.

6. Return to System Preferences, click the Startup Disk icon, choose your usual startup disk, and click Restart.

You've just confirmed that your duplicate works correctly. If your computer does not restart from your duplicate volume, however, your backup software may have malfunctioned. Try performing the duplication again, consult your software's documentation, or contact the developer's technical support department for assistance.

**NOTE** **USING AN EXTERNAL DRIVE AS A STARTUP VOLUME**

All modern Macs (those manufactured since approximately 2000) can boot from an external FireWire hard drive, assuming the drive was manufactured to the proper specifications; Intel-based Macs can also boot from USB 2.0 drives. See the sidebar USB 2.0 Drives, Intel Macs, and Bootability, earlier, for more information.

If you have trouble booting from an external drive, check Apple's Web site to confirm that your machine supports booting from the interface you're using. Also check the drive manufacturer's site to see whether any firmware updates are available for your drive.

## Set Up Archives

Next, configure your archive backups. As with duplicates, the exact procedure varies from one application to the next, but again, I give you a basic overview.

**TIP** If you're using Retrospect, you can find detailed instructions for creating archives in Set Up a Backup Server Script.

In your backup program, select the function for making an archive. (Appendix A: Backup Software has notes on how some applications name this feature.) Note again that some programs distinguish between commands that happen immediately and commands occur on a schedule (or automatically when needed). Given the choice, select an option that can run without manual intervention. If requested, give your archive procedure a descriptive name.

Select your source(s). This may be a simple matter of navigating to your home folder, or it may involve adding many different folders from all over your hard disk. See Archive strategy, earlier, for details on choosing which files to include in an archive. If you wish (and if supported by your software), choose selectors or exclusions. Once again, refer to Archive strategy for more information on why this may be a good idea—and which files you may want to exclude.

Select your destination. If you are archiving files to a hard disk, choose that disk. You may wish to create a new folder on that disk to contain your backups, especially if the disk also holds other files.

If you're storing your archive on optical media or a disk image, your backup software may require that you first mount the volume in the Finder. To do this:

- For blank optical media, simply insert the disc into your drive; when prompted, give the disc a name and choose the (admittedly confusing) action Open Finder. (This is not required in Retrospect, which can write directly to optical media. When creating your backup set, choose "CD/DVD" as the backup set type.)
- For a disk image, launch Disk Utility (located in **`/Applications/Utilities`**) and choose Images > New > Blank Image. Specify a name and location for the image. Select Sparse Disk Image as the format, meaning that the image will automatically grow as necessary

to accommodate more files, with its *initial* size being whatever you select from the Size pop-up menu. Optionally (but recommended) choose AES-128 from the Encryption pop-up menu. Click Create, and if you previously chose to encrypt the image, specify a passphrase when prompted. Disk Utility automatically mounts the new image in the Finder, ready to be used by your backup software.

**NOTE** **FILEVAULT AND BACKUPS**

Mac OS X's FileVault feature optionally encrypts the entire contents of your home folder, so that your files are protected from prying eyes and thieves. It accomplishes this behind the scenes by storing your home folder in an encrypted disk image. Using FileVault may complicate backups.

If you ask your backup software to archive the entire disk image, it will be unable to perform incremental archives of your home folder, instead making a complete copy of the image each time it runs. This is because, from the point of view of the backup software, your entire home folder is a single file—so any change to the data in your home folder, no matter how small, must result in that entire FileVault disk image being copied again.

You can work around this problem by instructing your software to ignore the FileVault disk image and instead look only at the files stored within it; you must then make sure your FileVault-protected home folder is unlocked and mounted when your backup software runs. However, if you have backups running when you are not at your machine, an unlocked FileVault disk image can jeopardize the security of your files. For this reason, if you must use FileVault, you should schedule backups to begin when you are physically present.

But my recommendation, instead, is to avoid using FileVault in the first place. Backup concerns aside, the way FileVault stores your data in day-to-day use makes it extremely vulnerable to corruption; theoretically, even a tiny amount of damage could render your entire home folder unusable.

Some software requires you to specify whether your backups should be *incremental* or *additive* (though the terminology differs with each application; once again, see Appendix A: Backup Software for notes on how some applications name these features). If so, be sure to select those features now.

If your software offers compression and encryption and you haven't already turned them on, consider doing so now. Compression will slow your backup but enable it to occupy much less space—normally a good thing. If you select encryption, choose a secure passphrase—and don't forget it! Also, if the software offers *verification* (checking to see that files were written properly), turn it on. Verification alerts you to errors in writing files that may otherwise go unnoticed and cause problems when you try to restore the files.

Finally, start the backup. Often this is just a matter of clicking a Backup button. (I describe adding a schedule for this script later in Automate Your Backups.) After testing your archive, you can repeat this procedure to set up archives to additional drives or other media.

### Sidebar The "Other" Archives

I mentioned earlier that some backup programs use the term *archive* to describe files that have been copied to removable media of some kind for long-term storage and then deleted from the source volume. Although the rising capacities and falling costs of hard drives make this sort of archive less and less necessary (except, perhaps, for video and other large files; see Video and Audio), the need may occasionally arise. For example, you may want to keep your email from the 1990s, all the shareware installers you downloaded this year, or all your Classic applications for future reference, but because you're unlikely to need the files any time soon, you could save space on your hard drive by offloading them to other media.

If you're considering making this sort of archive, consider the following suggestions:

- **Make sure it's worth your while.** Make a quick tally of the file and folder sizes of the items you want to offload. If you stand to free up only a few gigabytes on your hard disk, creating and maintaining this kind of archive may not be worth the effort.
- **Get all the pieces.** If you're backing up applications, read Applications to make sure you're getting all the components scattered around your hard disk.
- **Choose your media wisely.** Since you'll be deleting the original files after backing them up, use high-quality media. If you're using CDs or DVDs, consider buying one of the brands mentioned in Optical media longevity. Also, don't forget to make multiple copies—and to re-record them at least every few years.

## Test Your Archive

When the backup is complete, test it by choosing a few random files or folders from the archive to restore. If your backup software has a Restore feature, use it; if not, select your former destination volume as the source. To test your archive, follow these steps:

1. **Restore to a different location:** You can usually restore files either to their original locations or to another location of your choice. For this test, restore your selected files to a *different* location—say, your Desktop folder or another spot where you can find them easily.

2. **Check the restored files:** Compare the restored files to the originals using the Finder's File > Get Info command. Each pair of files should match exactly: same name, size, icon, creation date, and modification date. If the files were not copied to your selected destination or they are not identical, then either your backup software or its user made an error! Check your software's documentation, and if necessary contact the developer's technical support department for assistance.

3. **Try an in-place restoration:** Temporarily move one of the original files you backed up to a different location (again, the Desktop folder works well for this), then use your application's Restore feature to restore the file to its original location.

4. **Check the restored files:** Again, check each file carefully to make sure it is correct.

If the files are correct regardless of the location to which you restored them, your archive is working properly.

**TIP** Although your initial test of a backup may succeed, it's important to test backups regularly to confirm that the archives are still intact, and that all the required files are being updated as they should be. If you're unaware of an error that has been preventing your backups from running properly for the past few months, the consequences could be severe. Get in the habit of doing a test restoration every time you change your car's oil or test the batteries in your smoke detector. By the way, if you haven't changed your oil or tested the batteries in your smoke detector recently… now might be a good time.

## Automate Your Backups

Now that you have successfully performed and tested both a duplicate and an archive, it's time for the last important step: scheduling these backups to occur automatically.

As I mentioned earlier (see the sidebar The End of Scheduling?), some backup software runs all the time in the background, in some cases automatically adding newly created or modified files to your backup as they're saved or shortly thereafter. If you're using such software, you don't have to worry about scheduling as such—your backups are already automated.

If not, take a few extra moments to tell your backup program when you want it to run. Backup software usually makes it easy to put a given backup procedure on a simple, recurring schedule—e.g., Daily Archive every night at 11:00 PM, Weekly Duplicate every Sunday morning at 6:00 AM. But if you have multiple sets of media, creating an alternating backup schedule can be more complex. In this case, you might want Bart Daily Archive to be stored on Bart Archive Disk every night this week, while Lisa Daily Archive is stored on Lisa Archive Disk every night next week, and so on. Instructions for setting up such schedules in Retrospect are in Appendix B: A Retrospect Primer.

When choosing times and days for your backups to run, keep in mind these considerations:

- Will the destination media be ready? If not, will you be available to insert or enable it?
- Do you need to supply a password—for the backup software itself, or to mount a network volume? If you cannot store such passwords in your Keychain, or do not wish to do so, be sure the backups run when you're present to enter the passwords.
- Will the backup slow down your computer? If so, think about scheduling it for a time when you're not busy.

Regardless of your software, begin by scheduling your archives, which will probably run every day. Then schedule duplicates, choosing a time of day well before (or after) your scheduled archive run to avoid conflicts between the two schedules. Repeat as necessary for each media set you will be using.

Be sure to make a note of your duplication schedule in your favorite calendar application or on a paper calendar so that you will know when to swap media for off-site storage (see Off-site storage, a few pages ahead). For example, if you do a weekly duplicate on Sunday, you might create a recurring reminder to swap media every Monday morning before work.

After setting your backups on a schedule, check them periodically to make sure they are running as you expect. Some backup software provides logs for this purpose—or you can look at the files on the backup media and confirm that they are as recent as they should be.

## SIDEBAR POWER MANAGEMENT AND BACKUPS

Although this may seem self-evident, a scheduled backup won't run unless your computer is turned on and awake at the scheduled time. (A noteworthy exception: Prosoft's Data Backup 3 can wake up, or turn on, your computer when it's time for a scheduled backup.) Some people leave their computers running all the time, perhaps setting the display to dim or the hard drive to spin down after a certain amount of idle time to save energy. However, if you normally turn off your computer or put it to sleep when you're done using it—or if you have it set to go to sleep automatically—you may run into problems with scheduled backups. In most cases, these problems are easily solved with a bit of foresight.

Power management on a Mac is controlled using the Energy Saver pane of System Preferences. If you click the Schedule tab, you'll see a checkbox labeled "Start Up the Computer." What it does not tell you is that this setting will also *wake up* a computer at the scheduled time if it's on but asleep. If you select that checkbox and enter the days and times corresponding to your backup schedule (say, Every Day at 2:00 AM), the machine will turn itself on (or wake itself up) at the appropriate times.

A few words of caution, however:

- Be sure to select times at least 5 minutes before your backups are scheduled, to allow the computer time to start up completely.
- If you configured your computer to request your password when you turn it on or wake it up, the computer may get stuck at the Log In screen when you're not there. To turn off the password prompts, first go to the Security pane of System Preferences and deselect the checkboxes labeled "Require password to wake this computer from sleep or screen saver" and "Disable automatic login." Then go to the Accounts pane and click the Login Options icon near the bottom on the left. Select "Automatically Log In As," choose your user name from the pop-up menu, and enter your password when prompted.
- You can also use the Schedule pane of Energy Saver Preferences to turn off your computer (or put it to sleep) after completing a backup. If you do this, be sure to allow plenty of time; full backups sometimes take hours.

## Mind Your Media

So you've got your carefully labeled hard drives, DVDs, or other media with freshly recorded data. Now what?

Taking care of your media is just as important as making proper backups in the first place. If the media is lost or damaged, it does you no good. So I want to say a few words about handling, storing, and caring for backup media.

Whether you use hard drives, optical discs, or another type of media, the same general rules apply: store them in a cool, dry place away from significant sources of light, static electricity, vibration, and other hazards (such as inquisitive pets or children). All this may seem obvious, but it pays to remember that you're doing backups in the first place because your data is valuable—perhaps even irreplaceable. So treat your media with care.

**NOTE** For extra safety, store your media in a container that's rated fireproof for media.

### Recycling vs. long-term archives

If you use hard drives for backups, sooner or later they will fill up. (Whether this takes a few months or a few years depends on the rate at which you accumulate new data and the size of your backup disks.) And if you use lower-capacity removable media, sooner or later you will have a stack so large it threatens to collapse under its own weight. When this happens, you have two options: buy completely new media and start over, or recycle. By "recycle" I don't mean throw your backups in a blue bin—I mean erase the media and reuse it for a new set of backups.

One argument for starting fresh is that new media is virtually always more reliable than old media. Another is that you can save your old media as a long-term archive, in case you need to see what was on your Mac a few years ago. On the other hand, recycling media saves money, not to mention physical storage space. And most people have little need for backups stretching back more than a couple of years.

**TIP** For archive backups, you may wish to recycle your media on a regular basis, *before* it fills up. By performing periodic full backups—instead of relying indefinitely on incremental additions since a single full backup long ago—you reduce the risk of data loss due to file corruption or misbehaving backup software. How often you recycle your media is up to you, but in general I'd suggest recycling no less often than every 6 months.

Do, however, be aware that when you recycle media, you lose all the archived files stored since you started that particular cycle. If this makes you nervous, you might consider copying the archive to a set of DVDs before erasing it. In addition, if you recycle more than one set of media (for example, two or three hard drives), stagger them—do one, wait a week or two, then do the next one, and so on. That way, if you suddenly discover that you've erased the archive containing an old file you need, you'll still have a chance to recover it easily from another set of backup media.

The cost of buying a new stack of DVD-R discs is, of course, much lower than the cost of buying new hard drives. In addition, as I mentioned earlier, hard drives make a poor choice for long-term storage (though an older hard drive that you wouldn't trust for backups may be fine for casual, non-critical uses). So, if you use hard disks to store your backups, you should recycle instead of replace. However, remember that hard drives don't last forever—even if they're just sitting on a shelf, your data will deteriorate over time. A reasonable compromise may be to recycle your hard drives once a year or so for 3 or 4 years, and then replace it. If, when it comes time to erase your drives, you still wish to maintain a copy of the old data, use your backup software to duplicate your archives onto a stack of DVDs first.

**TIP** If you're erasing a hard disk anyway, this is a good time to reassess partition sizes (see Does size matter?). If your hard disk or home folder is significantly larger than before, consider changing the partition sizes to better accommodate your current needs.

Be careful when erasing a hard disk that contains months or years of backups—especially if you chose not to copy its data onto optical media. For safety, erase just one disk at a time, then perform (and test) regular backups for 1 or 2 weeks before erasing the next disk. If you erase all your backups at once, you're inviting trouble.

### Off-site storage

Raise your right hand, place your left hand on the nearest sacred text (such as *Real World Mac Maintenance and Backups*), and repeat after me:

> I hereby solemnly swear that henceforth, I will at all times maintain a recent, complete set of backup media off-site.

Good. Now I'm going to tell you why you just made such a promise and how to keep it.

No matter how diligently you back up, if something happens to your backup media, you're in trouble. Now, it is safer to keep your backups on an external volume than on, say, another partition of your internal hard disk. But as long as the media on which your backup is stored is physically located near your computer, your data is unsafe. Consider for a moment the range of events that could wipe out both your internal hard drive and any backups in the same area at the same time: fire, flood, earthquake, hurricane, tornado, burglary, destruction by rambunctious children or pets, wayward meteorites. These things all seem so unlikely until they happen to you. Insurance may enable you to replace your hardware and software, but not your data. So please take seriously my advice to keep at least one set of backups *off-site*, by which I mean *in a different building*.

The best approach is to rotate multiple sets of backup media, so that you always have one near your computer and another stored safely somewhere else. Periodically (say, once a week), bring the off-site media back, adding it to your normal backup routine so that it can be updated—and take your most recent local backup off-site.

**NOTE** At least one scientist has proposed the ultimate off-site storage location: the Moon! To read about this novel idea, go to http://www.newscientist.com/blog/shortsharpscience/2006/09/not-so-local-lunar-library.html.

**TIP** When it's time to replace a hard drive completely, you may consider giving away or selling your old drive. Before doing so, be sure to *securely* erase it so that its new owner cannot use a file recovery program to retrieve all your data! Merely dragging files to the Trash will not erase the data in such a way that it cannot be recovered. Even the default Erase feature in Disk Utility won't do the trick.

Instead, use a tool that can overwrite the entire disk (including free space, not just particular files) multiple times with random ones and zeroes. Clicking the Options button in Disk Utility's Erase pane provides two ways to zero the data. Other examples of products that include this capability are:

- Shredder: http://www.dekorte.com/Software/OSX/Shredder/ ($5)
- Trash X: http://www.northernsoftworks.com/trashx.html ($9)
- ShredIt X: http://www.mireth.com/pub/sxme.html ($20)
- SafeShred Pro: http://www.codetek.com/safeshred/ ($25)
- SPX: http://rixstep.com/4/0/spx/ ($39)
- TechTool Pro: http://www.micromat.com/index.php?option=com_content&task=view&id=31&Itemid=48 ($100)

Although you can use this process with just two sets of media, having three makes it more convenient. At any given time, you'll have one set (A) in use, your next-most-recent set (B) on site, and your oldest set (C) off-site. When you rotate the media, you bring your oldest set (C) back on site and make it active, taking what has now become the oldest set (B) off-site—and so on. For maximum safety, if you use only two sets, don't bring your off-site backup media back to your home or office until *after* you've taken another set away; those few hours when all your media is in one place could be the time when disaster strikes.

You may be wondering where exactly "off-site" could be in your case. Here are some suggestions:

- Your place of work
- A neighbor's or relative's home
- A storage unit
- A remote file server, if you use an Internet backup service

Don’t keep an off-site backup in your car, which is if anything more susceptible to damage or theft than your home. Heat and cold extremes in your car can also hasten data corruption. If you want as much security as possible with a trade-off of less convenience, keep it in a safe deposit box at your local bank.

**WARNING!** Because hard disk-based duplicates are, by definition, unencrypted, storing them off-site presents a significant security risk: anyone who obtains the drive also has complete access to your data. Here are some ways of reducing that risk:

- Store the drive in a safe deposit box.
- Keep all your important data on the drive encrypted within a disk image—perhaps using a utility such as PGPDisk.
- Instead of storing the duplicate directly onto a hard disk, put it on an encrypted disk image that’s stored on the hard disk. This will require extra steps when it comes time for restoring, but it’s much more secure.
- Keep (encrypted) archives and (unencrypted) duplicates on separate media, and store only the archives off-site.

## Restore Data from a Backup

If you’ve followed the directions so far, you’ve already tested the basic process of booting from a duplicate and restoring individual files from an archive. But in the event your data suffers serious damage, you will want to restore your duplicate, archive, or both onto your main hard disk. Read on for tips to help you through this process.

### Repair or erase your disk

If your startup disk (or another volume you’ve backed up) becomes unusable, you should not copy other files onto it while it’s still in an unstable state. In case of serious trouble, the first thing you should do is start up your computer from another volume (a duplicate, a Mac OS X installation CD, or a bootable disk-utility CD such as Alsoft’s DiskWarrior). Run Disk Utility or another disk-repair tool to fix any errors on your hard disk. If you are unable to fix the problems, or if they recur even after the utilities have done their best, use Disk Utility to erase the disk before attempting to restore your old files. (And by the way, if you're planning to restore *all* your files, it makes sense to erase the disk first, whether it appears to have any errors or not.)

### Restore a duplicate

If you've booted from your duplicate disk and erased your primary disk, restoring the duplicate onto the primary disk is a piece of cake. (If your duplicate is stored on optical media, skip ahead to Restore a CD/DVD duplicate onto a hard disk, below.) Follow the same steps you normally would to create a duplicate, but choose your external disk as the source and your internal disk as the destination. When the duplicate is complete, use the Startup Disk pane of System Preferences to set your internal disk as the startup volume, and restart the computer. If all goes well, your Mac will boot properly from the freshly restored duplicate on your primary disk. Just be careful you don't confuse the backup with the original, especially if they have the same name.

After restoring your duplicate—assuming your last archive update was more recent than your last duplicate update—you'll need to restore your latest set of archived files as well, which I describe in Restore archived files, ahead.

### Restore a CD/DVD duplicate onto a hard disk

Let's say you have a duplicate of your hard disk, stored on a stack of CDs or DVDs. Now it's time to restore them onto your hard disk so you can boot from your duplicate, but your internal hard drive is the only one you have. So there's a problem: If you boot from the internal hard drive (assuming it even has a functioning system), you won't be able to restore the duplicate because that would overwrite files that are actively in use. On the other hand, if you have only one optical drive, you can't boot from that either, because you would then be unable to remove the boot CD/DVD to feed in the backup discs. What to do? The process is tedious, but it can be done. Follow these steps:

1. Start up your computer from your Mac OS X installation CD or DVD—the one that came with your computer or one you purchased separately.
2. When the first installer screen appears, choose Installer > Open Disk Utility.

3. When Disk Utility opens, select your hard disk, click the Partition tab, and set up at least two partitions on the disk. (If your disk is already partitioned, you can skip this step.) Your goal is to have one partition that's large enough to hold the restored system and another that's large enough to hold a basic installation of Mac OS X. For the latter, a 5 GB partition should be adequate. (Caution: Partitioning your hard disk erases all the data on it.)

4. Quit Disk Utility, return to the installer, and install Mac OS X onto the newly created (small) partition. When asked to choose an installation type (the default is Easy Install), click Customize. Deselect everything except BSD Subsystem. Now proceed with the installation.

5. When the installation is complete, restart your computer from the copy of Mac OS X you've just installed on your small partition.

6. Reinstall your backup software onto the small partition that is currently functioning as your startup volume.

7. Use your software's duplication or restore feature to copy your duplicate from your CDs or DVDs onto the larger partition of your hard disk.

8. Use the Startup Disk pane of System Preferences to select your freshly restored volume as the startup disk, and restart your computer.

You've now restored your duplicate from optical discs onto your hard disk.

### Restore archived files

If you restored files from a duplicate (rather than from a full archive), once your primary hard disk is fully functional, your last step is to update it with the latest versions of files stored in your archive.

If your backup software has a snapshot feature, you should be able to select your most recent update and restore all the files from that date to their original locations. If your software uses *differential* additive archives, you must first restore the original, full archive backup and then restore the files from the most recent update.

If your backup software creates additive incremental archives—but without a snapshot feature—you must again start by restoring the original, full archive backup. Then, step through each day's update, copying its files into their original locations (overwriting the older versions). Depending on how many files have changed and how long it's been since your last backup, this could be a lengthy process.

**NOTE** If you've chosen to maintain a full archive and your archive backup was updated more recently than your duplicate was, you may opt to restore your archive directly. To restore a full archive:

1. Start up from your duplicate disk.
2. Using Disk Utility, erase your internal disk.
3. Select the icon for the internal disk in the Finder and choose File > Get Info. In the Ownership & Permissions section of the window, make sure Ignore Ownership on This Volume is *deselected*.
4. Open your backup software, and use its Restore feature to copy the archived files (as of their most recent backup) to the internal disk.
5. Use the Startup Disk pane of System Preferences to set your internal disk as the startup volume, and restart the computer.

Your Mac should boot properly from the freshly restored archive. (If it does not, follow the procedure outlined previously to restore your duplicate, and then restore your newer archived files.

# APPENDIX A: BACKUP SOFTWARE

This appendix has more information on the backup software mentioned in this book. These lists are not exhaustive, and backup software is updated frequently. So, before making a purchase, check the developer's Web site for current features and prices.

## Duplication+Archiving Software

The following applications offer both duplication and archiving features. **Table 3**, "Duplication+Archiving Software Feature Comparison" (next page), provides further detail about each one.

Backup Simplicity 3.0:
http://www.qdea.com/pages/pages-bs/bs1.html ($50)

Data Backup 3.0: http://www.prosofteng.com/products/data_backup_info.php ($59; see coupon for 50% discount)

Déjà Vu 3.3: http://propagandaprod.com/ ($25)

Retrospect Desktop 6.1:
http://emcinsignia.com/products/smb/retroformac/
(downloadable, $119; boxed, $129; upgrade from Express, $55)

Retrospect Express:
http://www.emcinsignia.com/en/products/express.dtml
(free with selected third-party hard drives; also in Allume's $99 CheckIt bundle, http://www.allume.com/mac/checkit/)

RsyncX 2.1:
http://archive.macosxlabs.org/rsyncx/rsyncx.html (free)

Synchronize Pro X 5.0:
http://www.qdea.com/pages/pages-sprox/sprox1.html ($100)

Synk Pro 6, Synk Standard, Synk Backup:
http://www.decimus.net/ ($45, $35, and $25 respectively)

Tri-Backup 4.0:
http://www.tri-edre.com/english/tribackup.html ($49)

## Table 3: Duplication+Archiving Software Feature Comparison

| | | Backup Simplicity | Data Backup | Déjà Vu | Retrospect Desktop | Retrospect Express | RsyncX | Synchronize Pro X | Synk Pro | Tri-Backup |
|---|---|---|---|---|---|---|---|---|---|---|
| **Targets** | **Hard Disk** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | **Disk Image** | [1] | [1] | [1] | [1] | [1] | [1] | [1] | [1] | [1] |
| | **CD/DVD** | [2] | Yes | [2] | Yes | Yes | [2] | [2] | [2] | [2] |
| | **• Multisession** | No | No | No | [10] | [10] | No | No | No | No |
| | **• Media Spanning** | No | Yes | [8] | Yes | Yes | No | No | No | [16] |
| | **Network Servers** | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Archives** | **Additive Incremental** | [3] | [6] | Yes | Yes | Yes | [13] | Yes | Yes | [17] |
| | **Rotating Archives** | No | Yes | Yes | No | No | No | Yes | Yes | Yes |
| | **Rotating Backups** | No | No | No | No | No | Yes | No | No | Yes |
| | **Snapshots** | No | Yes | No | Yes | Yes | [14] | No | No | Yes |
| | **File List** | No | No | Yes | [11] | [11] | No | No | No | No |
| | **Selectors** | No | Yes | No | Yes | Yes | No | No | Yes | Yes |
| | **Exclusions** | [4] | Yes | [9] | Yes | [4] | No | Yes | Yes | Yes |
| **Other** | **Compression** | No | Yes | No | Yes | Yes | Yes | [15] | Yes | Yes |
| | **Encryption** | No | Yes | No | Yes | Yes | [15] | [15] | Yes | Yes |
| | **Restore Feature** | Yes | Yes | No | Yes | Yes | No | No | No | Yes |
| | **Client-Server** | No | No | No | Yes | No | Yes | No | No | No |
| **Notes** | | [5] | [7] | | [12] | [12] | | | | |

[1] Only if created by user.

[2] Only if mounted in the Finder.

[3] **/Users** folder only.

[4] Limited.

[5] Can only back up startup volume.

[6] Yes; "Versioned Backup."

[7] Can wake up/turn on your computer to run a backup.

[8] Toast includes a version of Déjà Vu that supports media spanning.

[9] Preliminary support.

[10] Packet-writing support for adding data to partly-used optical discs.

[11] Searchable.

[12] Backup Server function.

[13] RsyncX calls them "Rotating Backups."

[14] RsyncX's incremental archives function as their own snapshots.

[15] Only for disk images.

[16] Manual only.

[17] Yes; "Evolutive Mirror Backup."

### Duplication Software

Applications in this group offer duplication (and, in some cases, synchronization) capabilities but not archiving. With the exception of Clone'X and MimMac, they all offer scheduled duplication.

BounceBack Professional 7.1: http://www.cmsproducts.com/product_bounceback_professional.htm (download only, $39; CD, $49)

Carbon Copy Cloner 3.0: http://www.bombich.com/software/ccc.html (donation suggested)

Clone'X 3.0: http://www.tri-edre.com/english/cloner.html ($49)

CopyCatX 4.0: http://www.subrosasoft.com/OSXSoftware/index.php?products_id=7 (download only, $50; CD, $60)

FoldersSynchronizer X 3.6: http://www.softobe.com/products/flsy/pp.html ($40)

MimMac 1.8: http://www.ascendantsoft.com/ ($10)

Personal Backup X4*:http://www.intego.com/personalbackup/ ($70)

SilverKeeper 1.1*:http://www.lacie.com/silverkeeper/ (free)

QuickBack 2.3 (part of SpeedTools Utilities): http://www.speedtools.com/STUS.shtml ($90)

SuperDuper 2.1:http://www.shirt-pocket.com/SuperDuper/ ($28; free "clone-only" version available)

Xupport 3.0: http://www.computer-support.ch/xupport/ ($20)

* Both Personal Backup X4 and SilverKeeper offer rotating backups, which could substitute for archives in a pinch—but not additive incremental archives.

## Archiving Software

These programs, including software for some Internet backup services, offer archiving and scheduled backups, but can't make bootable duplicates. **Table 4,** "Archiving Software Feature Comparison," next page, provides more detail about each program.

Apple Backup 3.1: http://www.mac.com/ (free with $100 .Mac subscription)

Archive Assistant (part of StuffIt Deluxe 10.0 and higher): http://www.stuffit.com/mac/deluxe/ ($80)

BackupSW 3.4: http://visualversion.com/backupsw/index.html (free)

BRU LE 1.3: http://www.bru.com/products/macosx/le/ ($129)

ChronoSync[*] 3.3: http://www.econtechnologies.com/site/Pages/ChronoSync/chrono_overview.html ($30)

CrashPlan Pro: http://www.crashplan.com/ ($60, coupon)

Dobry Backuper 1.5: http://dobrysoft.com/products/backuper/ ($30)

Mozy: http://www.mozy.com/ (free; requires $5/month Mozy subscription)

NTI Shadow 3: http://www.ntius.com/shadow.asp ($30)

Steekup: http://www.steekup.com/en/ (free; requires Steekup subscription)

SmartBackup 2.1.2: http://www.freeridecoding.com/smartbackup/ (€15—about $20)

[*] Can be coaxed into making duplicates, but the publisher discourages this usage.

## Table 4: Archiving Software Feature Comparison

| | | Apple Backup 3 | Archive Assistant | BackupSW | BRU LE | CrashPlan Pro | ChronoSync | Dobry Backuper | Mozy | NTI Shadow | Steekup | SmartBackup |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Targets** | **Hard Disk** | Yes | Yes | Yes | Yes | No | Yes | Yes | No | Yes | No | Yes |
| | **Disk Image** | [1] | [3] | [3] | [3] | No | [3] | [3] | No | [3] | No | [3] |
| | **CD/DVD** | Yes | Yes | [4] | [4] | No | [4] | Yes | No | [4] | No | [4] |
| | **• Multisession** | No | No | No | No | — | No | No | — | No | — | No |
| | **• Media Spanning** | Yes | Yes | No | Yes | — | No | Yes | — | No | — | No |
| | **Network Servers** | Yes | Yes | Yes | Yes | [6] | Yes | Yes | [9] | Yes | [9] | Yes |
| **Archives** | **Additive Incremental** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | **Rotating Archives** | No | No | No | No | Yes | Yes | No | No | Yes | Yes | No |
| | **Rotating Backups** | No | No | No | No | No | No | Yes | No | No | No | No |
| | **Snapshots** | Yes | No | No | No | Yes | No | [7] | Yes | No | [7] | No |
| | **File List** | No | No | Yes | Yes | Yes | [7] | Yes | No | No | Yes | No |
| | **Selectors** | Yes | Yes | Yes | Yes | No | Yes | No | Yes | Yes | Yes | Yes |
| | **Exclusions** | [2] | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| **Other** | **Compression** | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | No | Yes | No |
| | **Encryption** | No | Yes | No | No | Yes | No | No | Yes | No | Yes | No |
| | **Restore Feature** | Yes | Yes | Yes | Yes | Yes | [7] | Yes | Yes | No | Yes | Yes |
| | **Client-Server** | No | No | Yes | No | Yes | No | No | [9] | No | [9] | No |
| | **Peer-to-Peer** | No | No | No | No | Yes | No | No | No | No | No | No |
| | **No Schedule Needed** | No | No | No | No | Yes | No | No | Yes | Yes | No | No |
| **Notes** | | | | | | [5] | | | | [8] | | [10] |

[1] Backup's archives are based on disk images, but you can store them on other disk images only if they're mounted in the Finder.

[2] Manual only.

[3] Only if created by user.

[4] Only if mounted in the Finder.

[5] Awkward, un-Mac-like interface.

[6] Other computers running CrashPlan, or CrashPlan Central.

[7] Limited.

[8] Uses the term "versioned" to refer to rotating backups.

[9] Backs up to this provider's Internet servers only.

[10] Uses iCal for scheduling.

## Synchronization Software

These utilities provide either one-way or two-way syncing of files and folders. Because they offer neither duplicates nor archives in the sense discussed in this book, I don't categorize them as backup software.

AASync 1.2:
http://www.aasync.com/ (two versions; one free, one $19)

iBackup 5.1: http://www.grapefruit.ch/iBackup/ (free)

iMsafe 2.0: http://homepage.mac.com/sweetcocoa/imsafe/ ($19)

iShelter 1.0: http://www.brattoo.com/propaganda/index.php?s=1102016489&action=software ($10)

Synchronize! X Plus 3.0:
http://www.qdea.com/pages/pages-syncx/syncx1.html ($30)

zsCompare 3.0:
http://www.zizasoft.com/products/zsCompare/ ($35)

## Photo-Cataloging Software

Expression Media: http://www.microsoft.com/expression/products/overview.aspx?key=media ($299)

Extensis Portfolio: http://www.extensis.com/ ($200)

## Photo-Sharing Services

Flickr: http://www.flickr.com/ (free–$25/year)

Fotki: http://www.fotki.com/ (free–$50/year)

Kodak EasyShare Gallery: http://www.kodakgallery.com/ (free with annual purchase)

SmugMug: http://www.smugmug.com/ ($30–100/year)

Snapfish: http://www.snapfish.com/ (free with annual purchase)

## Internet Backup Services

These services include proprietary software. After subscribing and installing the software, you would be able to perform (limited) backups to a secure server over the Internet.

BackJack: http://www.backjack.com/

Clunk Click: http://www.clunkclick.net/

CrashPlan: http://www.crashplan.com/

Datatrieve: http://www.datatrieve.co.uk/

Depositit: http://www.depositit.com/

FilesAnywhere: http://www.filesanywhere.com/

MacBak: http://www.macbak.com/

Mozy: http://www.mozy.com/

Prolifix: http://www.prolifix.net/index.php?option=com_content&task=view&id=25&Itemid=65

Steekup: http://www.steekup.com/en/

## Version Control Software

The tools listed here let you to store unlimited versions of documents from almost any program—in some cases, every time you save a file. Except for Versomatic, they all use a client-server model (though the server can run on the same computer as the client). Before attempting to use CVS (Concurrent Versions System) software, read "Version Control with CVS on Mac OS X," an introductory article on CVS at http://developer.apple.com/internet/opensource/cvsoverview.html.

MacCvs: http://cvsgui.sourceforge.net/ (free)

MacCVSClient: http://www.heilancoo.net/MacCVSClient/ (free; contributions accepted)

MacCVS Pro: http://www.maccvs.org/ (free)

Perforce:
http://www.perforce.com/ (pricing starts at $800 per user)

SmartSVN:
http://www.syntevo.com/smartsvn/ ($69 per user; price decreases with volume)

Subcommander: http://subcommander.tigris.org/ (free)

Subversion: http://subversion.tigris.org/ (free)

svnX: http://www.lachoseinteractive.net/en/community/subversion/svnx/ (free)

Versomatic: http://www.acertant.com/web/versomatic/ ($40)

VOODOO Server: http://www.unisoftwareplus.com/products/voodooserver/ (server license, $79; remote client license, $129)

Darcs: http://darcs.net/ (free)

ZigVersion (a Subversion client): http://zigversion.com/ (free for noncommercial use; $139 otherwise)

## Other Software

DV Backup 1.4: http://coolatoola.com/ ($50; Lite version, $20)

# Appendix B: A Retrospect Primer

Throughout this book, I've discussed Retrospect, the well-known backup software from EMC (formerly from Dantz). Although, as I mentioned earlier, I'm finding Retrospect less appealing as time goes on, I still think it's a generally solid and useful tool—and depending on your backup needs, it may be the ideal program for you. But its biggest problem is the user interface. It's weird. It's confusing. It's 10 years overdue for an extreme makeover. And the difficulty that ordinary users have in getting past the interface to the useful stuff beneath is one reason so many people are looking for alternatives to Retrospect.

When I started using Retrospect way back when, I found it confusing, too. Its 250+ page manual contains plenty of helpful information, but it's a lot to get one's brain around. With some effort, though, I managed to figure out enough of Retrospect to get my own backups working, and eventually I became so accustomed to the interface that I barely notice how weird it is anymore.

In the next few pages, I provide a brief overview of Retrospect's terminology, logic, and interface—with special attention to things you're likely to find confusing. I won't cover everything, of course, but I hope I can give enough information that you can feel comfortable using it for basic duplicates and archives—for a single computer or for a small network. Unless otherwise noted, everything in this appendix applies to both Retrospect Desktop and Retrospect Express.

## Retrospect Terminology

Before I get into specific Retrospect windows or activities, I want to explain some important terms as Retrospect uses them. Understanding these words will make everything else much easier.

- **Backup:** An operation in which Retrospect copies files into a special file called a backup set (see "Backup Set," ahead in this list). Every backup to a given backup set after the first one is, by definition, an additive incremental archive. (Retrospect doesn't perform differential backups.) So, for the remainder of this appendix, I use the term "Backup" to refer to what I would normally call an "archive."

- **Duplicate:** An operation in which the entire contents of a volume are copied *exactly* to another volume. Subsequent duplicates are incremental, and may delete files absent on the source (using the “Replace Entire Disk” option) or leave such files on the destination (using the “Replace Corresponding Files” option). Duplicates of startup volumes to external FireWire drives, secondary internal drives, or partitions on such drives, should be bootable—as long as you chose the “Replace Entire Disk” option. Duplicates do not use backup sets.

- **Archive:** A backup operation in which Retrospect deletes the original files after copying them into a backup set.

- **Restore:** An operation in which files are copied from a backup set to another location—which may or may not be their original location.

- **Script:** A saved set of options for a backup, duplicate, archive, or restore operation, which you can run at any time (manually or on a schedule). Scripts include what data you’re backing up, to what destination, with which selectors and other options, and schedule information. The term “Script” is a bit of a misnomer—unlike with AppleScript scripts, shell scripts, and so on, you don’t actually see a *script* (a sequence of coded instructions); you see only settings in dialogs and windows.

- **Backup Server:** A script type for backups (not found in Retrospect Express) that provides for a flexible schedule and multiple backup sets. Using this script type, Retrospect can back up clients whenever they happen to be available on the network, and store the backups on whatever media happens to be present. This makes backing up laptops and rotating backup media much easier.

- **EasyScript:** A series of dialogs that walk you through the creation of a basic backup script (including a Backup Set, if necessary) by asking you simple questions. I’ve found that EasyScript selections always require significant modification after the fact, so I prefer to skip EasyScript and define my own scripts manually.

- **Backup Set:** A special file that stores all the files and folders you’re backing up; what I refer to elsewhere in this book as an *archive*. A backup set can contain many versions of any given file, and may optionally be compressed, encrypted, or both. Backup sets are readable only by Retrospect; you can't access their contents directly from the Finder.

- **Catalog:** An index of a backup set's contents. For backup sets stored on a hard disk or network server, you can opt to store the catalog in the same file as the backup set or as a separate file (even on a different volume from the backup set), so you can view and search the contents of your backups even if the backup set itself is unavailable. (Backups sets stored on removable media always keep their catalog files on your hard disk.) If a catalog is missing or damaged, Retrospect can reconstruct it from the backup set itself.

- **Source:** Whatever you're backing up—volume(s) or subvolume(s) on one or more physical drives.

- **Destination:** The location where backed-up files will be stored. For backup, backup server, and archive operations, the destination must be a backup set (or more than one backup set); for duplicate operations, the destination must be a volume.

- **Subvolume:** A folder you've designated as a backup source or destination. You cannot create a bootable volume by duplicating a startup volume to a subvolume, because as far as Mac OS X is concerned, a subvolume is just a folder.

- **Client:** A computer on your network that's running Retrospect Client, and which you can back up to a server running Retrospect Desktop.

- **Device:** A physical device that can store data—such as an optical drive or a tape drive. (Hard drives and network servers don't count as "devices" in Retrospect's usage.) Some devices require special setup before they can be used, but in most cases, optical drives are recognized automatically.

- **Normal:** The default backup behavior, which is to copy all the selected files on the first run, and then copy only new or changed files (an additive incremental archive) on subsequent runs.

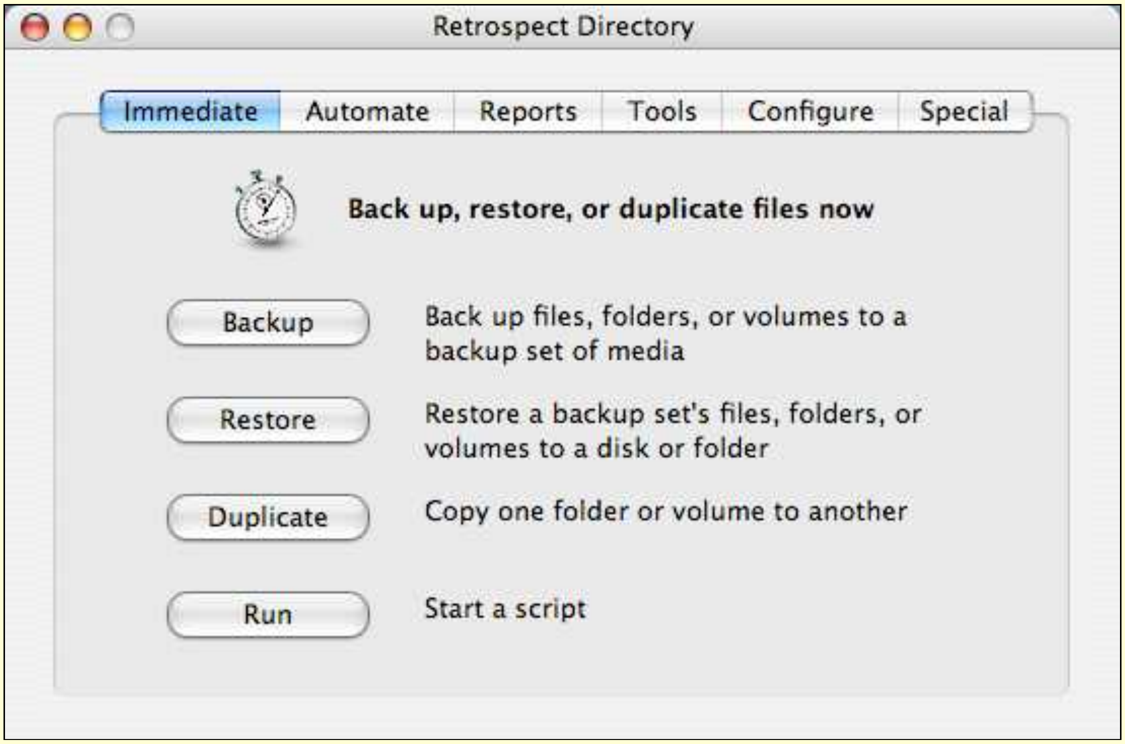
- **Recycle:** This setting instructs Retrospect to erase a backup set and then perform a normal backup.

- **New Media:** This setting instructs Retrospect to create a fresh backup set (with all the attributes of an existing set) on a new set of media, without erasing the existing media.

## The Directory

When you open Retrospect, its main window, called the Directory, appears (see **Figure 3**). You can click any of the tab-like buttons at the top of the window to display a pane containing a few buttons; clicking these buttons opens the windows where you actually perform useful tasks. The number and names of these tabs (and the controls on them) differ between Retrospect Desktop and Retrospect Express.

**FIGURE 3**



Back up, restore, or duplicate files now

Back up files, folders, or volumes to a backup set of media

Restore a backup set's files, folders, or volumes to a disk or folder

Copy one folder or volume to another

Start a script

Retrospect's main Directory window. This figure shows Retrospect Desktop; Retrospect Express has fewer panes and a somewhat different arrangement of buttons.

When you click a button to open a window, the Directory usually remains visible in the background; you can return to it at any time by choosing Retrospect Directory (or Retrospect Express Directory) from the Window menu. Be aware that almost every action you perform in Retrospect opens at least one new window; you could easily end up with half a dozen or more windows open at once.

Because Retrospect helpfully includes explanations of each button right in the Directory window, I'm not going to reiterate all the button names and functions here. I do, however, want to point out where you can find some commonly used features:

- **To set Retrospect's preferences:** In Retrospect Desktop, click Preferences on the Special pane. In Retrospect Express, click Preferences on the Configure pane.

**NOTE** For most users, Retrospect's default preferences are ideal.

- **To set up a recurring Duplicate or Backup:** Click Scripts on the Automate pane. See Set Up a Duplicate Script (this page) and Set Up a Backup Script, ahead.

**NOTE** Backup Server is compatible with your existing, fixed-schedule scripts, including Duplicate scripts. If another script is scheduled to run while Backup Server is actively backing up, the script runs as soon as Backup Server finishes. If Backup Server happens to be idle when another script is scheduled to run, the scheduled script takes over and then returns control to Backup Server when it's done.

- **To restore backed-up files:** Click Restore on the Immediate pane. See Restore a Backup.
- **To duplicate a volume as a one-time activity:** Click Duplicate on the Immediate pane.
- **To prepare client machines on your network for backup:** Click Clients on the Configure pane (Retrospect Desktop only). See Back Up Network Clients.
- **To run a script immediately:** Choose the script name from the Run menu.

## Set Up a Duplicate Script

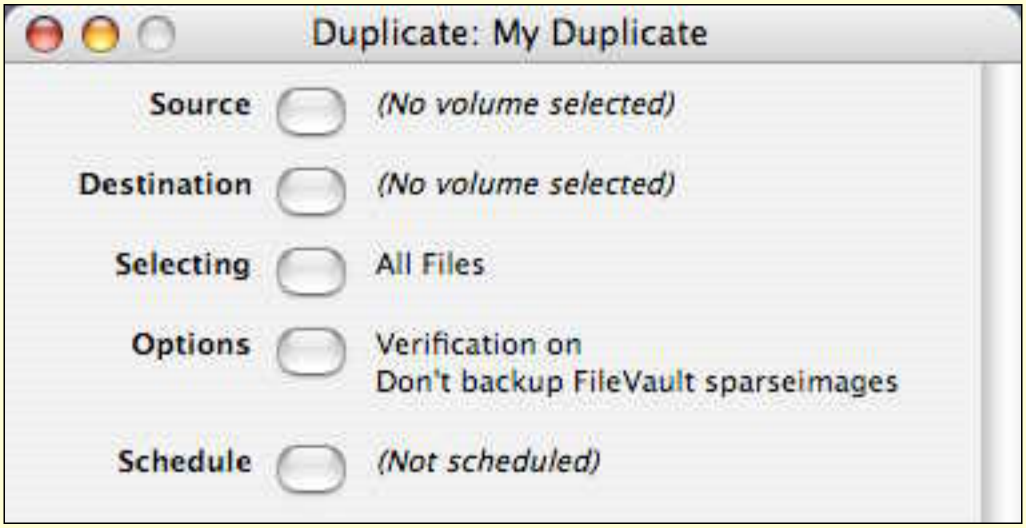
In Retrospect, if you want to make a bootable copy of your hard disk, you use the Duplicate feature. You can create a one-off duplicate by clicking Duplicate on the Immediate tab, but here, we're concerned with setting up duplicates as a regularly scheduled activity. To do so, follow these steps:

1. Click the Automate tab, and then click the Scripts button. The Scripts window appears.

2. Click New to create a new script, and select Duplicate in the dialog that appears. Click OK.

3. Enter a name for your script (see Label Media and Files for suggestions) and click OK. The Duplicate window (**Figure 4**) appears.

**FIGURE 4**



Duplicate: My Duplicate

Source (No volume selected)

Destination (No volume selected)

Selecting All Files

Options Verification on
Don't backup FileVault sparseimages

Schedule (Not scheduled)

The Duplicate window, like other script summary windows, provides an overview of the options selected for this script.

4. Click the Source button. Select the volume you want to duplicate and click OK.

5. Click the Destination button. Select the volume where your duplicate will be stored. Choose Replace Entire Disk (or Replace Entire Contents) from the pop-up menu at the top of the window—*not* Replace Corresponding Files!—and click OK. Keep in mind that the destination volume, if a hard disk or partition, must be at least as large as the amount of data on the source volume.

**NOTE** You must choose a volume icon—not a subvolume or folder icon—as the destination if you wish your duplicate to be bootable.

**Warning!** Check to see that the destination volume does not ignore ownership; if it does, your duplicate will not be bootable. To check this, select the destination volume's icon in the Finder and choose File > Get Info. In the Ownership & Permissions portion of the window, make sure the checkbox labeled Ignore Ownership On This Volume is deselected.

6. Optionally, click the Selecting button and make a selection from the pop-up menu to restrict which files are copied. You might, for example, choose All Files Except Cache Files or All Except Cache & Spotlight; these two choices will speed up the duplication while omitting non-critical files. If you're using Retrospect Desktop, you can click More Choices to access more-sophisticated selectors. When you're finished, click OK.
7. Click the Options button. Make sure the Verification checkbox is selected, and click OK.
8. Click the Schedule button and add in your desired schedule. (I talk more about setting up schedules in Schedule a duplicate, below on this page.) When you finish, click OK.
9. Close the Duplicate window, and click Save when prompted.

Your Duplicate script is now ready to go, and will run on the schedule you set—even if you quit Retrospect. If you want to run it immediately, choose the script's name from the Run menu.

After testing your duplicate (read Test Your duplicate), you can repeat this procedure to set up Duplicate scripts for additional hard disks or other media.

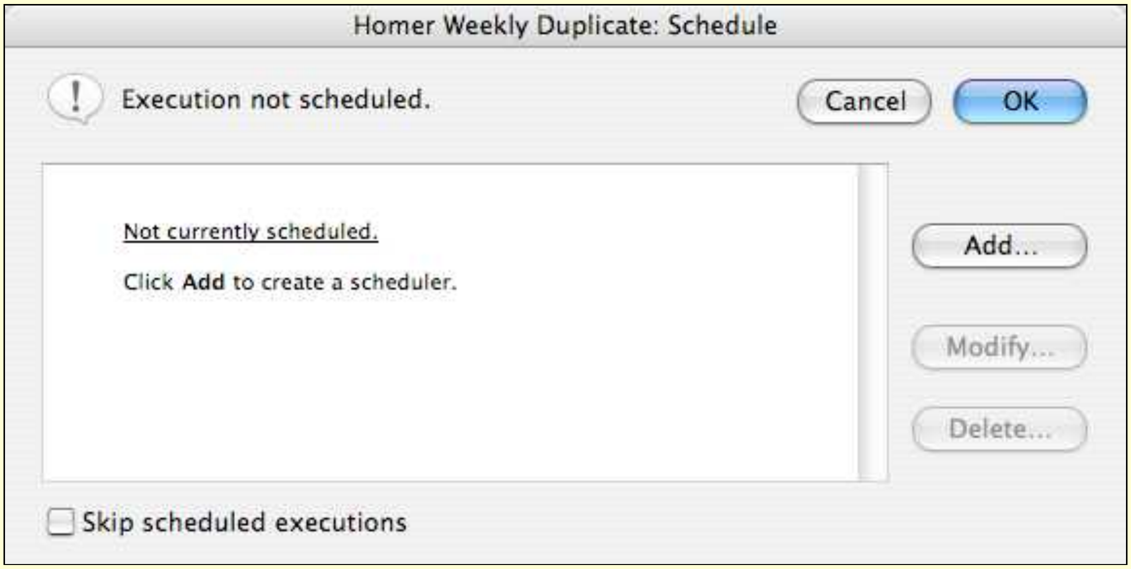
### Schedule a duplicate

You can schedule duplicates to occur as frequently or as seldom as you wish, but I suggest running them at least once a week. Better yet, use two or more hard drives and alternate your duplicates between them—drive #1 one week, then drive #2, and so on. This scheme will enable you to keep one of the drives off-site at all times. In this example, I show how to schedule duplicates to run once a week, alternating between two drives. Feel free to alter these instructions to meet your needs if you're using a different number of drives or want to run duplicates at a different frequency.

To schedule an alternating weekly duplicate in Retrospect, follow these steps:

1. Select the Automate tab and click the Scripts button.
2. Select the Duplicate script that you created for your first drive; then click Edit.
3. Click the Schedule button, and then the Add button (**Figure 5**).

**FIGURE 5**



Homer Weekly Duplicate: Schedule

Execution not scheduled.

Not currently scheduled.

Click **Add** to create a scheduler.

☐ Skip scheduled executions

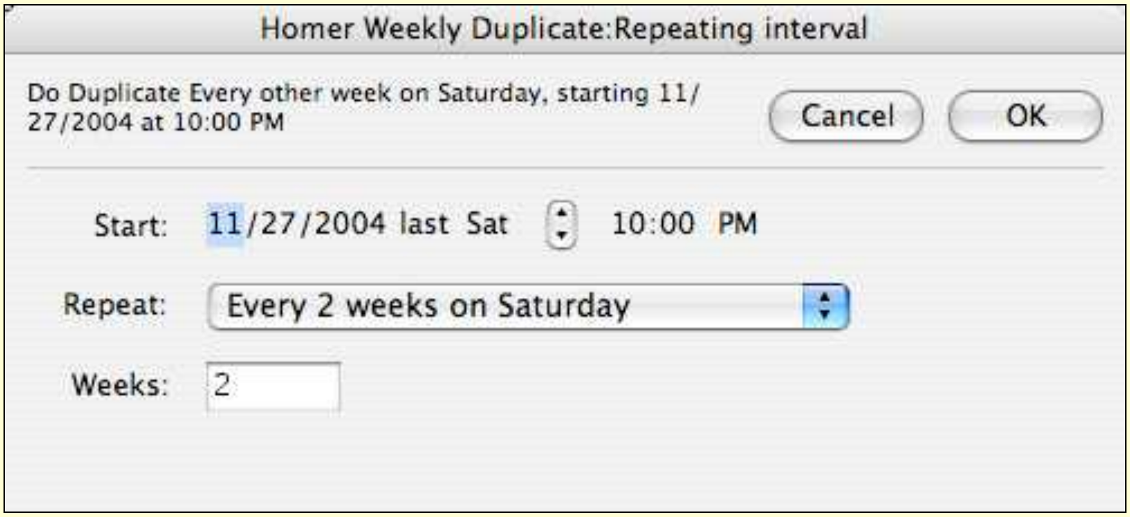
Retrospect's Schedule list (still empty in this example) appears when you click the Schedule button for a script. Add a new schedule by clicking the Add button in this dialog.

4. For the kind of schedule to add, choose Repeating Interval.
5. Enter today's date as the start date.
6. Choose the day of the week on which you want the backup to occur, and select a time.
7. From the Repeat pop-up menu, choose Every <x> Weeks on <day of week>.
8. In the field labeled Weeks, enter **2** if you have two sets of media or **3** if you have three sets of media. **Figure 6,** next page, shows an example of what the finished schedule may look like.
9. Confirm that the text at the top of the dialog matches your expectations, as in "Do Duplicate Every other week on Wednesday, starting 12/01/2005 at 2:00 AM." Then click OK.

10. Select your next Duplicate script and repeat Steps 3–8, but in Step 4, choose a start date 1 week later.

Your selected scripts will now alternate on a weekly basis.

**FIGURE 6**



Homer Weekly Duplicate:Repeating interval

Do Duplicate Every other week on Saturday, starting 11/27/2004 at 10:00 PM

Start: 11/27/2004 last Sat 10:00 PM

Repeat: Every 2 weeks on Saturday

Weeks: 2

This repeating interval schedule in Retrospect runs every 2 weeks on Saturday. To change it to every 3 weeks, enter **3** in the Weeks field; to change the interval from weeks to days or months, use the Repeat pop-up menu.

**NOTE** After you set up a schedule, you can quit Retrospect. Retrospect installs a small background application in your **`/Library/StartupItems`** folder called RetroRun, which monitors your scheduled backups and launches Retrospect, when necessary, to run them at the proper times.

## Set Up a Backup Server Script

Backup Server is a wonderful feature—actually a script type, which can make rotating archives incredibly easy. (Unfortunately, it cannot be used for duplicates.) Backup Server has two main attributes:

- It constantly polls all designated sources (which could be a folder on a local volume or another computer on your network) to see if they've been backed up within the past 24 hours—or whatever interval you choose—and if not, it performs a backup immediately. (You can also restrict the Backup Server to run only during certain times of certain days.) This way, even if your laptop is not available for daily backups on a fixed schedule, you can be sure backups will occur when it is present.

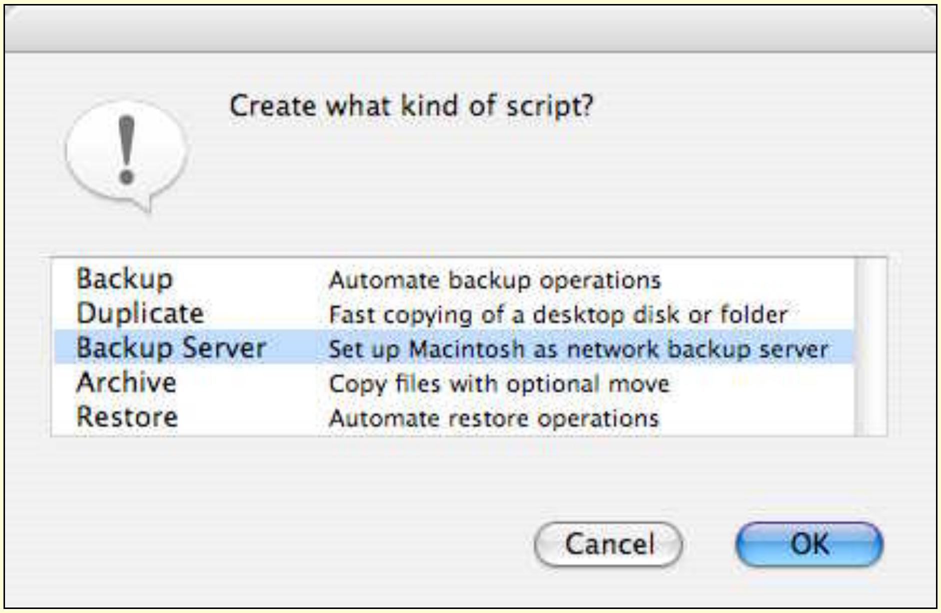
- It uses any designated media that happens to be available at the moment. So you could set up three different hard drives as backup destinations, attach or detach them whenever you like, and Retrospect automatically updates the oldest archive available the next time it runs. This eliminates the need to maintain a strict schedule for swapping media to take it off-site.

If you're using Retrospect Desktop, Backup Server is generally a much better choice for automated archives than a fixed schedule. (This feature is absent in Retrospect Express, so if you're using Express, or wish to follow a fixed schedule, see Set Up a Backup Script, ahead.)

To use Retrospect's Backup Server feature, follow these steps:

1. Click the Automate tab, and then click the Scripts button.
2. In the Scripts window that appears, click New to create a new script, and choose Backup Server in the dialog that appears (**Figure 7**).

**FIGURE 7**



Create what kind of script?

| | |
|---|---|
| Backup | Automate backup operations |
| Duplicate | Fast copying of a desktop disk or folder |
| Backup Server | Set up Macintosh as network backup server |
| Archive | Copy files with optional move |
| Restore | Automate restore operations |

To use Retrospect's Backup Server feature, select it as the script type in this dialog.

3. Enter a name for your script (see Label Media and Files for naming ideas) and click OK. The Backup Server window appears.

4. Click the Source button to display the Volume Selection window. To back up an entire volume, select it in here. To back up just *part* of a volume, select the volume and click Subvolume. Navigate to a folder you'd like to back up (such as your home folder) and click Define. You can repeat this as many times as necessary. Each subvolume you define then appears as a folder in the Volume Selection window. (To select multiple volumes or subvolumes in this window, hold down Command while clicking.) When you're finished selecting sources, click OK.

5. Click the Destination button. *Two* dialogs open: the Destinations dialog and, in front of that, the Backup Set Selection dialog. You should add backup sets for each of the drives you're using to store your archives. If you've already defined the backup set(s) you want to use, select them here (Command-click to select more than one backup set). If not, follow these steps:

   a. Click New to create a new backup set.

   b. Choose File (*not* Removable Disk!) from the Backup Set Type pop-up menu.

   c. If you want to encrypt the backup set, click the Secure button, select an encryption type, and enter a passphrase.

**NOTE** You must decide whether to use encryption when you initially create a backup set. You can't change the encryption settings for a backup set after the fact.

   d. Give your backup set a descriptive name and click New.

   e. Select the volume (normally an external hard disk) where you want to store the backup set and click Save.

   f. Repeat Steps a–e, if necessary, for additional backup sets; then, select the set(s) you want to use and click OK.

   When you've finished adding backup sets to the script, click OK to dismiss the Destinations dialog.

6. Optionally, click the Selecting button and make a choice from the pop-up menu to restrict which files are copied. You might, for example, choose All Files Except Cache Files or All Except

Cache & Spotlight; these two choices will speed up the backup while omitting non-critical files. If you're using Retrospect Desktop, you can click More Choices to access more-sophisticated selectors. When you're finished, click OK.

7. Click the Options button. Enter the maximum frequency for your backups—such as "every 1 day" or "every 4 hours." If you want to turn on compression (a good idea), click More Choices, then select Backup in the list on the left and select the Backup Compression (In Software) checkbox. Click OK.
8. To restrict Backup Server to certain days or times, click the Schedule button. Select the Custom Schedule radio button, and then click Custom. Select the times and days you want the Backup Server to run, then click OK. Finally, click OK again to dismiss the Schedule window, and close the Backup Server window.

Backup Server is now configured to archive your files onto the selected backup media whenever they are available. To activate the Backup Server script immediately, choose Run > Start Backup Server. When Backup Server is running, the main Retrospect Directory disappears and the Backup Server window appears instead. To return to the Directory (to make other changes in Retrospect), you must close the Backup Server window and confirm that you really do want to stop the execution of the Backup Server.

**NOTE** Backup Server is compatible with your existing, fixed-schedule scripts, including Duplicate scripts. If another script is scheduled to run while Backup Server is actively backing up, the script runs as soon as Backup Server finishes. If Backup Server happens to be idle when another script is scheduled to run, the scheduled script takes over and then returns control to Backup Server when it's done.

## Set Up a Backup Script

If you own Retrospect Express and therefore can't use the Backup Server script type—or if you simply prefer to have your backups run on a regular schedule—you should set up a Backup script to perform additive incremental archives. The instructions are similar to those for the Backup Server script, just previously, except that you must specify an explicit schedule.

To set up a Backup script, follow these steps:

1. Click the Automate tab, and then click the Scripts button. The Scripts window appears.
2. Click New to create a new script, and choose Backup in the dialog that appears.
3. Enter a name for your script (see Label Media and Files for suggestions) and click OK. The Backup window appears.
4. Click the Source button to display the Volume Selection window. To back up an entire volume, select it in this window. To back up just *part* of a volume, select the volume and click Subvolume. Navigate to a folder you'd like to back up (such as your home folder) and click Define. You can repeat this as many times as necessary. Each subvolume you define then appears as a folder in the Volume Selection window. (To select multiple volumes or subvolumes in this window, hold down Command while clicking.) When you finish selecting sources, click OK.
5. Click the Destination button. *Two* dialogs open: the Destinations dialog and, in front of that, the Backup Set Selection dialog. Ordinarily, you'll select just one backup set here (and then create an entirely new backup script for each additional destination drive). If you've already defined the backup set you want to use, select it here. If not, follow these steps:

   a. Click New to create a new backup set.

   b. Choose File (*not* Removable Disk!) from the Backup Set Type pop-up menu.

   c. If you want to encrypt the backup set, click the Secure button, select an encryption type, and enter a passphrase.

**NOTE** You must decide whether to use encryption when you initially create a backup set. You can't change the encryption settings for a backup set after the fact.

   d. Give your backup set a descriptive name and click New.

   e. Select the volume (normally an external hard disk) where you want to store the backup set and click Save.

f. Select the set you want to use and click OK.

When you've added your backup set to the script, click OK to dismiss the Destinations dialog.

6. Optionally, click the Selecting button and make a selection from the pop-up menu to restrict which files are copied. You might, for example, choose All Files Except Cache Files or All Except Cache & Spotlight; these two choices will speed up the backup while omitting non-critical files. If you're using Retrospect Desktop, you can click More Choices to access more-sophisticated selectors. When you finish, click OK.
7. Click the Options button. Make sure the Verification checkbox is selected, and if you want to turn on compression (a good idea), select the Backup Compression (In Software) checkbox. Click OK.
8. Click the Schedule button and set your schedule. (For more details about setting up schedules, see Schedule backups, next page.) When you finish, click OK.
9. Close the Backup window, and click Save when prompted to do so.

Your Backup script is now ready to go, and will run on the schedule you set—even if you quit Retrospect. If you want to run it immediately, choose the script's name from the Run menu.

After testing your archive (see Test Your Archive), you can repeat this procedure to set up Backup scripts for additional hard disks or media.

**NOTE** **EXECUTION ERRORS**

After Retrospect completes a backup, it may display a window saying there were execution errors. Don't worry about this. No, really: *don't worry about it*. Execution errors are common and don't necessarily indicate a problem. Most frequently, an "error" means that something didn't match between Retrospect's pre-backup scan and its post-backup verification, which will be the case if files (such as temporary system files) change while the backup is in progress—which they often do.

## Schedule backups

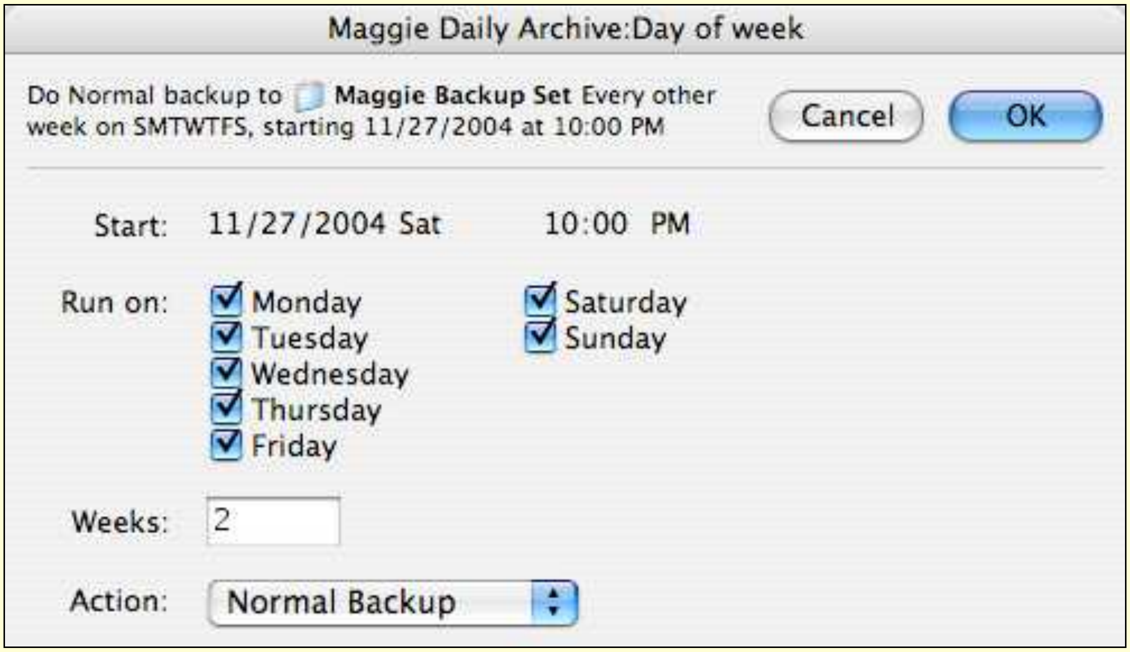
You can schedule backups to occur as frequently or as seldom as you wish, but I suggest running them at least once a day. Better yet, use two or more hard drives and alternate your backups between them on a weekly basis—drive #1 every day one week, then drive #2 every day the following week, and so on. This sort of scheme enables you to keep one of the drives off-site at all times. In this example, I show how to schedule backups to run daily, alternating between two drives on a weekly basis. Feel free to alter these instructions to meet your needs if you're using a different number of drives or want to run duplicates at a different frequency.

To schedule your backups scripts, follow these steps:

1. Select the Automate tab and click Scripts.
2. Select your first Backup script, and then click Edit.
3. Click the Schedule button, then the Add button.
4. For the kind of schedule to add, choose Day of Week.
5. Enter today's date as the start date.
6. Select the days of the week on which you want the backup to occur, (usually all of them) and select a time.
7. In the field labeled Weeks, enter **2** if you have two sets of media or **3** if you have three sets of media (**Figure 8**, next page).
8. Choose Normal Backup from the Action pop-up menu.
9. Confirm that the text at the top of the dialog matches your expectations, as in "Do Normal backup to Maggie Backup Set Every other week on SMTWTFS, starting 12/27/2006 at 10:00 PM." Then click OK.
10. Select your next Backup script and repeat Steps 3–8, but in Step 4, choose a start date 1 week later.

Your selected scripts will now run daily, but alternate on a weekly basis.

**FIGURE 8**



Maggie Daily Archive:Day of week

Do Normal backup to Maggie Backup Set Every other week on SMTWTFS, starting 11/27/2004 at 10:00 PM

Start: 11/27/2004 Sat 10:00 PM

Run on: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Weeks: 2

Action: Normal Backup

This Day of Week schedule in Retrospect runs every day for a week, in alternating weeks. To change it to alternate every 3 weeks (if you use three sets of backup media), enter **3** in the Weeks field.

**TIP** If you have an old Mac (or, say, a Mac mini) that you'd like to turn into a backup server, read my article "Turn your old Mac into a backup server" in the September 2005 issue of Macworld: http://www.macworld.com/2005/08/features/oldmacnewtricks1/.

## Back Up Network Clients

Retrospect Desktop has the capability of backing up the machine it's running on, plus up to three other client machines. (You can buy more client licenses—or, for larger groups, upgrade to Retrospect Workgroup or Retrospect Server.) This means you can use just one set of backup media and one schedule for several computers, instead of setting up a backup system on each one individually. All you have to do is install Retrospect Client on each client machine, add the clients to Retrospect's list, and select the volumes or subvolumes you want to back up on each one.

The first part of the process is to set up the clients. Follow these steps:

1. On a client machine, install Retrospect Client (the installer is included with Retrospect Desktop).

2. At the end of the installation process, the installer asks you for a password. Choose something different from your standard Mac OS X password—it need not be particularly secure—and confirm it when prompted.
3. The installer then asks if you want to enable a firewall exception for Retrospect. If you have Mac OS X's firewall turned on, be sure to answer Yes.
4. Click the installer's Restart button to restart your computer.
5. Open the Retrospect Client application and make sure the On radio button is selected.

Repeat these steps for each client machine. That's it—your clients are now ready to go. The rest of the process happens on the server machine. To configure the server, follow these steps:

1. Open Retrospect Desktop, go to the Configure pane, and click Clients.
2. Click the Network button to display a window listing all the clients Retrospect can find on your local network (these are machines with Retrospect Client installed and turned on which are within the same subnet—and not blocked by a firewall). You should have TCP/IP selected as the Network Protocol, and Mac OS X selected as the Type.

**TIP** If the machine you're using as a server has a firewall turned on, you must also add an exception for Retrospect on the server. Go to the Firewall tab of the Sharing pane of System Preferences, click New, and choose Retrospect from the Port Name pop-up menu. If it does not appear in the list, choose Other and enter `497` in the TCP Port Number(s) field.

3. If the client you want to add appears in the list, select its name. If the client does not appear in the list, click Add by Address and enter the IP address of the client computer; then, select the client's name in the list. Click Log In, and type in the password you specified when you set up that client. Also confirm (or modify) the name for the client as it will appear in the server's lists. Repeat this step as necessary for additional clients.

4. After adding a client, the Client Configuration dialog should appear. (If it does not, double-click the client name in the Backup Client Database window.) On the General pane of this dialog, select Link Encryption if the client is connecting over a wireless network, or you want to add extra security to the data as it travels between the client and the server. From the Backup pop-up menu, choose Selected Volumes.

5. On the Volumes pane, select all the volumes from the client machine that contain files or folders you want to back up. Click OK. Repeat as necessary for additional clients, and close the Backup Client Database window.

Now your clients are ready to be added to your backup scripts. Follow the instructions in Set Up a Duplicate Script, Set Up a Backup Server Script, or Set Up a Backup Script to add clients to your scripts; the volume(s) you selected in Step 5 will appear in the Sources lists, and you can define subvolumes and selectors just as you did for items on the server itself.

**TIP** If you're making *duplicates* of clients over the network, remember to choose a volume—not a subvolume!—as the destination. You'll probably want to store each duplicate on a separate FireWire hard drive, or at least a separate *partition* of a FireWire hard drive, so that you can later attach that drive to the client machine if you need to boot from the duplicate.

## Recycle a Backup Set

If you're storing your archives on hard disks, they will eventually fill up. How long that takes depends on the size of the disks, whether or not you use compression, and how frequently your files change. If the disk holding a backup set becomes completely full, Retrospect will continue attempting to run your backup scripts, but each one will fail due to a lack of disk space. Therefore, you should check on your free space periodically and, when it begins to get low, recycle your media—in other words, erase the backup set and start over with a full backup.

The procedure to do so is easy, but it isn't obvious. To recycle a backup set, follow these steps:

1. On the Configure pane, click the Backup Sets button. The Backup Sets window appears.
2. Select the backup set you want to recycle—the one that's stored on whichever volume is closest to being full. Click Configure. A new dialog opens.
3. Click the Options tab. At the bottom of the Options pane is a Media section with a single button: Action. Click the Action button. The Media Control Manual Override dialog appears.
4. Select the Recycle radio button and click OK. This tells Retrospect that for the *next* run of this script only, it should use the Recycle action—erase the backup set and then perform a full backup.
5. Close all the other windows, saving your changes if prompted.

The next time your backup script runs, it will recycle that backup set.

Needless to say, when you recycle a backup set, you lose all the old incremental archives from that set. Therefore, you should not recycle if you've had any computer problems recently that make you suspect you'll need to access older versions of your files! The best practice, assuming you have more than one backup set for your archives, is to stagger their recycling dates—by a month or more, if possible. That way, you'll always have at least several older copies of your files.

## Restore a Backup

Retrospect's Restore feature can sometimes be confusing. But don't panic. When you need to recover backed-up files, follow the instructions here that most closely match your situation.

Whichever method you choose, remember that Retrospect treats Restore operations in a method very similar to Backup or Duplicate operations—you choose the Source (the volume or backup set containing the files you want to restore), the Destination (where to put the restored files), and various Options. You also, in some cases, choose particular files within the Source that you want to recover. Then you perform the actual restoration.

### Restore a duplicate

Before restoring a duplicate, consider whether that's really what you want to do. Remember that you can boot your computer from a duplicate (as long as it's stored on its own volume on a FireWire hard drive or, if you're using an Intel Mac, a USB drive). If your internal disk has problems, you may find that you can boot from the duplicate and then run a utility to repair your internal disk. That can save you some time and effort over restoring the duplicate.

**NOTE** If you want to boot from a duplicate you created over a network, you must either physically connect the hard drive it's on (internally or via FireWire) to the client machine or restore the duplicate onto the client's hard drive over the network. You can't boot from a duplicate over a network.

However, if disk repair doesn't work (or if, for any other reason, you want to restore a duplicate, in its entirety, to the original volume), do *not* use Retrospect's Restore command! The Restore feature is only for files stored in backup sets (that is, archives). Instead, click the Duplicate button on the Immediate pane. Follow the same procedure you used for creating your duplicate, only swap the Source and Destination drives. Retrospect will then copy your duplicate back onto its original volume.

### Restore the entire contents of a backup

If you've been archiving files to a backup set using a backup script and you want to replace the *entire* set of files on your original volume with the backed-up copies (whether the most recent snapshot or not), follow these steps:

1. On the Immediate pane, click the Restore button. A dialog appears.

2. Select the Restore an Entire Disk radio button (yes, even if you didn't back up your entire disk) and click OK. The Restore from Backup: Source dialog appears.

3. Select the backup set containing the files you want to restore. If you've backed up to multiple backup sets on different drives, you'll generally want to select the backup set with the most recent date.

4. When you select a backup set, the bottom portion of the window displays the most recent snapshot for each of the volumes (or subvolumes) in that set. If you want to restore files from the most recent snapshot, simply select the volume you want to restore in this list. However, if you want to restore the files as they appeared at an earlier time, click Add Snapshot. The Snapshot Retrieval window appears, listing snapshots for every backup session stored in this backup set. Select the one you want and click Retrieve. Then, select that snapshot in the Restore from Backup: Source dialog and click OK.

5. In the Destination Selection dialog that appears, select the original volume or subvolume corresponding to the snapshot you selected in Step 4. Make sure the pop-up menu at the top of the window says Replace Entire Disk (the default setting), and click OK. When the confirmation alert appears, click Replace.

**WARNING!** Although it should be obvious by now, you are about to overwrite the files on your hard disk with the ones from your backup. If you are not completely certain this is what you want to do, select a *different* destination in Step 5 and then manually move the files to their original locations.

6. After a few minutes of file scanning, Retrospect displays the Restore from Backup summary window. This is your last chance to make changes to your source, destination, or options before restoring your files. When you're ready to go for it, click Restore.

Retrospect restores all the files from your selected snapshot to their original locations.

### Restore individual files or folders from a backup

Most of the time when I dip into an archive, it's to find an older version of a particular file or folder I inadvertently modified or deleted. These situations fall into two categories. In the first case, I know (at least roughly) when the version of the file I'm looking for would have been backed up—and thus, I know which backup set likely contains it. In the second case, the file could be in any of several backup sets, and I'm not certain when a good copy was last backed up. Each situation requires a slightly different procedure.

### If you know which backup set contains the files you want and when they were backed up:

To restore your files, follow these steps:

1. On the Immediate pane, click the Restore button. A dialog appears.
2. Select the Restore Files from a Backup button and click OK. The Restore from Backup: Source dialog appears.
3. Select the backup set containing the files you want to restore. If you've backed up to multiple backup sets on different drives, you'll generally want to select the backup set with the most recent date.
4. When you select a backup set, the bottom portion of the window displays the most recent snapshot for each of the volumes (or subvolumes) in that set:

    - If you want to restore files from the most recent snapshot, simply select the volume you want to restore in this list.
    - If you want to restore the files as they appeared at an earlier time, click Add Snapshot.

      The Snapshot Retrieval window appears, listing snapshots for every backup session stored in this backup set. Select the one you want and click Retrieve. Then, select that snapshot in the Restore from Backup: Source dialog and click OK.

**NOTE** Right now, you're only selecting the *snapshot* containing the files or folders you want to restore. Later, in Step 7, you'll narrow that down to particular files or folders.

5. In the Destination Selection dialog that appears, select the volume or subvolume where you want to put the restored files. Although you can choose the original location, a safer option is to leave the existing copies of the files and folders (if any) alone and restore the backups to another location. Make sure the pop-up menu at the top of the window says Retrieve Files & Folders (the default setting), and click OK.
6. After a few minutes of file scanning, Retrospect displays the Restore from Backup summary window. To select the files and

folders you want to restore, click the Files Chosen button. A window appears listing all the files in the snapshot you selected.

7. In the snapshot list, navigate to the file(s) or folder(s) you want to restore. Double-click an item (or select it and click the Mark button at the top of the window) to indicate that you want to restore it. (A checkmark appears next to each file selected for restoration.) Repeat for as many items as you wish. When you finish selecting files, close the window.
8. Back in the Restore from Backup summary window, click Restore.

Retrospect copies the items you marked to the specified destination. It maintains the original folder structure, so what you'll see if you look in the destination location is a folder with the same name as your backup set. Inside that folder will normally be another series of folders mirroring the original folder hierarchy, and if you navigate down through these folders, you'll find the files you just restored.

### If you're unsure where the files you want are located or when they were backed up:

To restore your files, follow these steps:

1. On the Immediate pane, click the Restore button. A dialog appears.
2. Select the Search for Files and Folders button and click OK. The Restore from Backup: Source dialog appears.
3. Select one or more backup sets—if you have no idea where your files may be, select all the backup sets. Then click OK.
4. In the Destination Selection dialog that appears, select the volume or subvolume where you want to put the restored files. Although you can choose the original location, a safer option is to leave the existing copies of the files and folders (if any) alone and restore the backups to another location. Make sure the pop-up menu at the top of the window says Retrieve Files & Folders (the default setting), and click OK.
5. Retrospect displays the Searching & Retrieval dialog. Use the pop-up menus to specify search criteria (just as you would in a Finder search) and click OK. Retrospect searches through the selected backup set(s) and selects all matching files.

6. The Searching & Retrieval summary window appears. In the Files Chosen section, the window lists the total number of matching files it found.

7. If you want to narrow that list down further to just particular files, click the Files Chosen button. In the list that appears, double-click an item (or select it and click the Unmark button at the top of the window) to indicate that you want to exclude it from the restoration. (A checkmark appears next to each file selected for restoration.) Repeat for as many items as you wish. When you finish selecting or deselecting files, close the window.

8. In the Searching & Retrieval summary window, click Retrieve.

Retrospect copies the items you marked to the specified destination. It maintains the original folder structure, so what you'll see if you look in the destination location is a folder with the same name as your backup set. Inside that folder will normally be another series of folders that mirror the original folder hierarchy, and if you navigate down through these folders, you'll find the files you just restored.

**WARNING!** **THE .SPARSEIMAGE BUG**

Retrospect Desktop (though not Retrospect Express) has an option—enabled by default—to skip backing up disk images used by FileVault, whether or not you've explicitly used a selector to exclude them. (To access this option, click the Options button in a script summary window, select FileVault in the list on the left, and make sure Don't Back Up FileVault Sparseimages is checked.) Unfortunately, this currently prevents Retrospect from backing up *any* disk image that uses the ".sparseimage" format, including ones you've created manually. So if you have .sparseimage files that you want Retrospect to back up, be sure to uncheck that box.

Note that this bug applies only to Backup (and Backup Server) script types; .sparseimage files are backed up during Duplicate scripts regardless of this setting.

# Appendix C: Set Up Backups on Your Uncle's Mac in Seven Simple Steps

Most of us have friends or relatives who badly need a solid backup system, but who lack the time, inclination, or technical savvy to read through an entire book like this one and make their own decisions about what to back up, when, and how. Naturally, they'll turn to you, the friendly neighborhood Mac expert, for advice.

Speaking from personal experience, I prefer to provide such people solutions that will require as little of my time in the future as possible. In other words, I want to be able to say, "Look, Uncle John, as long as you keep this box plugged in and turned on, your Mac will be backed up. And if your Mac ever has problems, all you have to do to solve your problems is *XYZ*—you don't even have to call me!"

When Mac OS X 10.5 Leopard ships, I'll be looking very carefully at Time Machine. If it lives up to the hype, perhaps my revised solution for no-fuss backups will be to recommend that your uncle plug in an external hard drive and turn on Time Machine. In the meantime, I suggest the following:

1. Buy your uncle an external FireWire hard drive and plug it into his computer. It can be left on all the time, will never ask for a disc to be inserted, and can be used to boot either an Intel or PowerPC-based Mac. As for capacity, I suggest getting a drive the same size as the one in your uncle's computer.

2. Also buy your uncle a copy of SuperDuper. Unlike Retrospect, it requires precious little configuration and won't be intimidating for someone unaccustomed to backup software.

3. Open SuperDuper and register it. Then choose your uncle's startup volume as the source and the backup drive as the destination. From the Using pop-up menu, choose Backup—All Files.

4. Click Options. Choose the Smart Update option from the During Copy pop-up menu. Choose Quit SuperDuper from the On Successful Completion pop-up menu. Click OK.

5. Click Schedule. Check the Automatically Copy checkbox and enter the times the backup should run. Although this is up to you (and your uncle), the biggest key is that you should choose times when

your uncle is pretty sure his computer will be on (and awake). It’s OK if your uncle is using the computer at the time. My suggestion is to run this backup twice a week—say, every Tuesday and Friday. If you were also performing archives, I’d suggest once a week, but without them, a slightly greater frequency will give your uncle a bit more protection. Click OK, and then close the Scheduled Copies window.

6. Click the lock icon and ask your uncle to enter his password.
7. Click Copy Now to run the first backup immediately; SuperDuper will quit when it’s finished.

Now, on the schedule you set, SuperDuper will create a bootable duplicate of your uncle’s computer without requiring any interaction from him. Explain to him that he can just ignore that application when it launches and go about his business.

If your uncle accidentally deletes or changes a file, explain to him that as long as that happened after his most recent backup, he can retrieve an older copy of the file from his backup drive, in the same relative location as the original.

And if your uncle’s main startup drive fails, tell him to restart, holding down the Option key, and then choose the backup drive as his startup volume. (After that, repairing his internal drive or restoring files might require a phone call to his favorite niece or nephew—sorry about that!)

# APPENDIX D: UNIX-BASED BACKUPS

Why should you bother with expensive backup applications when you can create your own custom backup program from scratch, for free, using Unix command-line tools that are built into Mac OS X? Simply put, you'll spend a lot of time and effort to produce something that, in most cases, will be less capable than a commercial backup tool. If at all possible, I'd like to discourage you from trying to cobble together a command-line backup solution. I think such approaches introduce unnecessary risk and have the potential to chew up a great deal of your valuable time. In this appendix, I want to explain exactly why the problem is so complex. But some people will surely want to experiment anyway, and for such adventurous souls, I provide a few pointers to get you started.

Before reading any further, though, keep in mind that this appendix assumes you are already comfortable using Terminal and have at least a modest knowledge of Unix. If that doesn't describe you, move along—there's nothing to see here!

## Understand Copying Issues

Backups are essentially a matter of copying files. Unix provides numerous ways to do this, and Mac OS X offers more options than most kinds of Unix. But there's copying, and then there's copying. Your first step in creating a Unix backup system is to figure out which "copy" command you want to use.

Consider, for example, the **`cp`** command, perhaps the most common way of copying files in Unix. Under Mac OS X 10.4 and later, the version of **`cp`** included with the operating system correctly copies resource forks, extended attributes, and most other kinds of metadata associated with any given file. But **`cp`** doesn't copy creation dates—copied files show as their creation dates the date they were copied—and that missing information is crucial to many people. In addition, **`cp`** has relatively few features, meaning that if you want incremental backups or any other fancy behavior, you'll have to program all that logic yourself, either in a shell script or in the programming language of your choice. Ditto for the **`ditto`** command, which fails to copy not only the creation date but a file's locked status, HFS+ extended attributes, access control list (ACL), and other metadata.

You might turn instead to **rsync**, which is popular for backups in the Unix world. Not only does **rsync** have numerous intelligent copying features—including incremental and versioned backups—it's designed to work just as easily over a network (including the Internet) as when backing up to a local volume. That looks like a good choice, until you discover that the version of **rsync** that Apple includes with Tiger is buggy. The open-source **rsync** program can't handle resource forks and extended attributes, so Apple created a modified version that does. Unfortunately, Apple's **rsync** is several years out of date, fails to copy several important pieces of metadata, and is reputed to be crash-prone. The developer of RsyncX created his own version of **rsync**, which gets rid of some problems of Apple's version but adds a few more. And there are at least one or two other versions of **rsync** that similarly offer different trade-offs of capabilities and problems.

**NOTE** Mac OS X 10.4 includes an Apple-modified version of **rsync** 2.6.3. Other versions I'm aware of for Mac OS X are:

- **rsync_hfs:** RsyncX is based on this version of **rsync**. It was previously available (as source code only) at the OpenDarwin.org Web site. You may still be able to find the code with some Web searching, but it's no longer being actively developed.
- **rsync+hfsmode:** This is a third-party attempt to patch **rsync** to support Mac OS X resource forks, extended attributes, and metadata that works not only on Mac OS X but on other versions of Unix when backing up Mac OS X clients. http://www.quesera.com/reynhout/misc/rsync+hfsmode/
- **LART rsync**: Another third-party patch, this version of **rsync** is available only as a diff file; you must build the binary yourself. http://www.lartmaker.nl/rsync/
- **AFP548 rsync:** An article by Michael Solberg on the AFP548.com Web site describes a way of building **rsync** that incorporates the **rsync+hfsmode** patch plus other fixes as well. Links to compiled binaries are included. However, the article was written before the release of Tiger, so it's unclear whether this approach has any advantage over the other versions of **rsync**. http://www.afp548.com/article.php?story=20050219192044818

Maurits of plasticsfuture posted a detailed analysis of which command-line tools in Mac OS X have which capabilities (and deficiencies) at http://blog.plasticsfuture.org/2006/03/05/the-state-of-backup-and-cloning-tools-under-mac-os-x/. His conclusion, essentially, is that **cp** is the best option (despite its limitations); **ditto** is marginally acceptable in some situations. All the other available command-line tools have too many issues for his comfort. (Apple Software Restore, or ASR, is great for copying entire volumes but has problems in file-by-file mode; SuperDuper gets very high ratings but lacks a command-line interface.)

Sooner or later, Apple is bound to fix the bugs and deficiencies in **cp**, **ditto**, ASR, and **rsync**. Until then, if you want to use one of those tools for backups, you have to decide which limitations you're willing to accept. If you go with **cp** or **ditto**, you'll have to add a considerable amount of extra code to do anything more than a basic backup. If you choose **rsync**, you must be willing to live without the metadata it can't handle (which may, in fact, be perfectly acceptable for some people) and brace yourself for the possibility of bugs and crashes.

I should point out, though, that there are other ways of copying files beyond those that Apple provides. For example, there's the free tool **psync** (http://www.dan.co.jp/cases/macosx/psync.html), which offers most of the same advantages and disadvantages as **ditto**, but can automatically synchronize source and destination, deleting files from the destination that are no longer on the source, and copying only new or modified files after its first run.

Another option is the open-source backup program **rdiff-backup** (http://www.nongnu.org/rdiff-backup/). Although it uses a library designed for **rsync** for some features, it has its own copying method. **Rdiff-backup** can store many versions of each file it backs up. However, unlike every other backup program mentioned in this book, when incrementally updating your backups, it doesn't copy entire files, but *only the portions of files that have changed*, making it fast and highly efficient in its use of disk space. (You must use **rdiff-backup** to restore files that have been backed up in this manner if the version you need is older than the most recent one.) It even supports most Mac OS X metadata if you have the necessary **xattr** library installed (see http://pythonmac.org/packages/); unfortunately, a universal binary of this library for Intel-based Macintoshes has yet to appear. You can obtain **rdiff-backup** itself using Fink (http://fink.sourceforge.net/), but if you want the latest and greatest version, you may need to build it yourself from the source code.

## Create (or Borrow) a Script

Once you've decided which sort of copy command you want to use, the next step is to wrap the command up in a text file, most likely with some other code to give it some basic intelligence, so that you can execute it simply by running the script. A very basic backup script could be something as simple as this:

```
#!/bin/bash
cp -r /Users/joe /Volumes/Backup
```

This script begins with a line that specifies which shell to use (bash, in this case). It then uses the **cp** command to copy files; the **-r** flag (for "recursive") tells it to copy entire folders. The first argument (**/Users/joe**) is the source; the second argument (**/Volumes/Backup**) is the destination. If you named this script **backup** and stored it in the Applications folder, you could run it time by typing:

```
/Applications/backup
```

Of course, that script isn't very smart; it won't create archives or bootable duplicates, for example. For more substantial backups, you'll have to add more commands to your script.

### Scripts for bootable duplicates

Even if your chosen copy command copies all the files on your source volume and correctly maintains all the necessary metadata, you still need a few ingredients to make the backup bootable. For example, you must run the command with root privileges. Normally this is done by typing **sudo** before the script name and entering a password. Without root privileges, some files won't be copied, and some will be copied but with incorrect ownership and permissions. You may also need to use the **bless** command at the end to make sure your backup is bootable. Mike Bombich (creator of Carbon Copy Cloner) provides all the details of successful cloning at http://www.bombich.com/mactips/image.html.

### Scripts for archives

When creating scripts that will incrementally back up only new or changed files, leaving older copies intact, your approach will depend largely on the capabilities of the copying program you're using. For example, if you're using **cp** or **ditto**, you'll need to come up with a method to figure out which files have changed and what to do with older versions before the copying takes place.

On the other hand, **rsync** offers two interesting options you might consider. If you use the **-b** (backup) and **--backup-dir** flags, **rsync** creates a backup directory, and puts in that directory the old copies of any files that are being updated in your destination. Alternatively, you can use the **--link-dest** flag. When you do this, **rsync** creates an extra copy of your entire backup in the link directory you specify, using hard links to point to the files in the main destination directory for files that are unchanged since the last time the backup ran. This means that both the destination and the link destination directories *appear* to have complete backups and can be used as such, but you don't waste extra disk space on duplicated files. (To learn more about **rsync**'s options, type **man rsync** in Terminal.)

Because the variables are so numerous, I recommend looking for inspiration in backup scripts that other people have written. For example, the article at AFP548.com by Michael Solberg cited earlier, http://www.afp548.com/article.php?story=20050219192044818, includes an **rsync**-based script. Similarly, if you create scheduled backups using RsyncX, you can examine the scripts it creates and use those as the basis of your own scripts. I've found RsyncX's Rotating Backup Assistant, which relies on the **--link-dest** flag, to be a useful starting point. Other useful scripts can be found at MacOSXHints.com:

- Run automated backups to a Unix server: http://www.macosxhints.com/article.php?story=20060113043215181
- Use a shell script for incremental backups: http://www.macosxhints.com/article.php?story=20051005204725280
- Use rsync to perform automatic backups: http://www.macosxhints.com/article.php?story=20050505072407618

**TIP** The open-source program **rsnapshot** , written in **perl**, uses rsync as its copying engine, but offers many prebuilt features, all configurable from the command line (http://www.rsnapshot.org/). Another free tool that uses **perl** and **rsync** is **rsyncbackup** (http://code.google.com/p/). I haven't tested either one, so I can't say how well they perform under Mac OS X.

## Schedule a Command-Line Backup

The final component of any good backup program is automation. Mac OS X provides several command-line scheduling tools, including the venerable **`cron`** and **`launchd`**, a new utility introduced in Mac OS X 10.4. If you've gotten this far, I'm going to assume you either know or can figure out how to use the scheduling tool of your choice.

However, I should point out that you can download easy-to-use graphical interfaces to both **`cron`** and **`launchd`**, which will make the job easier if you're not accustomed to command-line scheduling. Cronnix (http://www.abstracture.de/projects-en/cronnix) is a free, open-source **`cron`** interface; Lingon (http://lingon.sourceforge.net/) serves the same purpose for **`launchd`**. And if you choose **`launchd`**, I recommend reading the article I wrote for Macworld, "Launch Your Mac," which explains its use; http://www.macworld.com/2006/01/secrets/februarygeekfactor/index.php.

## Final Thoughts

Once you've got a backup script running on its own, you're still not quite out of the woods. You have to figure out how to monitor if the script is working and how to restore files if the need arises; I'll leave those as exercises for you to work out on your own. As with any backup, I strongly urge you to check periodically (by doing test restores) to see that your backups are working as expected—especially after applying any updates to Mac OS X itself or to any of the Unix software you use in your scripts.

If you've made it through this whole section without feeling any pangs of anxiety, you're just the kind of person who might enjoy the challenge of creating and debugging a command-line backup system. On the other hand, if all the caveats and gotchas I mention here make you nervous, I urge you to consider buying a commercial backup tool instead of rolling your own. You'll be making a sound financial decision; you'll also have the benefit of being able to ask someone else for technical support rather than solving all your own problems!

# Appendix E: Backups with Amazon S3

Amazon.com's S3 (Simple Storage Service) is little more than extremely inexpensive private file storage on Amazon.com's servers, with transfers to and from the service encrypted for your protection. For details and pricing information, see BYOS (bring-your-own-software) Internet backups. S3 includes no software of its own, but depends on third parties to integrate support for the system into their own products. Furthermore, although S3 uses HTTP to transfer files, it requires explicit support from client applications; most Internet software can't (yet) communicate with S3 directly. S3 is primarily geared toward developers of Web applications and other software that can benefit from massive yet inexpensive online storage.

Just about any backup program should be able to add direct support for S3, so that you could simply choose S3 (rather than a hard disk or DVD) as the destination for your backups, enter your account information, and let the backup software take care of all the other details for you. I fully expect to see such support in future versions of popular backup programs. For now, however, if you want to use S3 for backups in any automated fashion, you must go to extra effort.

**Warning!** Although the total amount of storage you can get with S3 is virtually unlimited, the service currently places a 5 GB limit on the size of any single file. This is significant for backups, because archive files frequently grow larger than that, and because you may have individual files on your computer that are larger than 5 GB.

In addition, as I write this, because of a significant bug in the S3 infrastructure (which Amazon.com says they're working to fix), files between 2 GB and 4 GB in size cannot be uploaded. So, taking both issues into consideration, a 1 GB file or a 5 GB file is fine but not, at the moment, a 3 GB file or a 6 GB file!

Presumably, any backup software that adds direct support for S3 will also know how to intelligently split files and archives so that they don't run afoul of S3's size limits. In the meantime, working around this problem may require some additional manual steps.

## Get Started with S3

To sign up for Amazon S3, simply fill out a form (including credit card information) at http://www.amazon.com/s3/. After your account is activated, Amazon.com provides you with two long strings of characters—an Access Key ID and a Secret Access Key—both of which you'll need to reach your space on their servers.

Next, you need software that can connect to your account and enable you to upload and download files. If you wish to only transfer files manually, you might begin with the free S3 Browser (http://people.no-distance.net/ol/software/s3/), which lists all your S3 files in a window and allows you to upload or download using drag-and-drop.

For more advanced interaction with S3, you can use any of several other applications, including JungleDisk and Interarchy, both discussed ahead.

## Use S3 with JungleDisk

At the moment, the most convenient way to get at your S3 files is to use a tool called JungleDisk (http://www.jungledisk.com/), which performs some magic to mount your S3 storage space as a network volume and, as a bonus, even includes some basic backup capabilities. (JungleDisk is free during beta testing; upon its official release it will cost $1 per month or $20 for a lifetime license.) A program called JungleDiskMonitor handles the back-end communication with S3 and runs a WebDAV server in the background on your local machine; when you run JungleDiskMonitor, it automatically connects to that WebDAV server (or you can do manually by choosing Go > Connect to Server in the Finder, entering `http://localhost:2667/`, and clicking Connect), and your S3 storage space appears as a mounted network volume.

Once that volume is mounted, you can manually copy files to or from it, just as you would with any other network volume. You can also use JungleDisk's built-in backup feature (Backup > Configure Automatic Backup) to copy the files and folders of your choice to S3 on a fixed schedule. (The backups are incremental, on a file-by-file basis, but not additive; only the most recent copy of each file is preserved, though files deleted on your local disk aren't automatically deleted on your S3 volume.)

If you aren't satisfied with JungleDisk's backup features, you can use almost any other backup software, which will recognize your S3 volume as a valid destination for your backups.

### JungleDisk limitations

JungleDisk may sound like a simple solution to a complex problem, but there are a number of hidden pitfalls:

- You can only access your S3 volume when JungleDiskMonitor is running; if it quits or crashes, your connection disappears. You can, however, add the application to your Login Items list in the Accounts pane of System Preferences to make sure it launches every time you log in.
- If you copy Mac files directly to S3, some metadata (including ownership and permissions) may not be stored correctly. The best way to make sure your files retain all their important information is to let a backup program store them in an archive of some sort (such as a disk image file or a proprietary file like Retrospect uses for its backup sets).
- Even assuming you overcome the other problems, you'll still face S3's 5 GB (or 2 GB, as the case may be) file size limit. The only Mac backup software I know of that currently lets you specify an arbitrary limit on the size of archives it stores is Tri-Backup, but it does this only in its Mirror Backup, Incremental Backup, and Archiving modes—not in its Evolutive Mirror Backup mode, which makes what I refer to as an additive incremental archive. In other words, if you're using software that keeps adding to an archive until the media gets full, it will simply fail once that file passes S3's size limit.

### JungleDisk recommendations

Depending on the software and techniques you use, JungleDisk can bring you tantalizingly close to the ideal of automated backups to S3, but every technique involves some tradeoffs. Here are my recommendations:

- **Keep JungleDiskMonitor running.** As I mentioned earlier, since your S3 volume can't be mounted unless JungleDiskMonitor is running in the background, it's a good idea to add it to your Login Items list.

- **For automatic file size management, use Tri-Backup.** If your biggest concern is ensuring that your archives can continue to grow without running into S3's size limits, Tri-Backup is your best bet. You will, of course, have to make sure that JungleDisk-Monitor is running (so that your S3 volume is mounted) before Tri-Backup runs. To set up Tri-Backup to limit archive sizes:

  1. In the Programmed Actions view, click the + button to create a new action.

  2. Give your action a name, and choose Mirror Backup, Incremental Backup, or Archiving from the Mode pop-up menu. (Of the three, Incremental comes closest to the sort of archiving I recommend. What Tri-Backup calls Archiving deletes files from the source after backing them up.)

  3. Click Options. Check the box labeled Partition the Backup in Folders with a Maximum Size Of and enter a number—I suggest 4900 MB to keep your segments well under the 5 GB limit.

  4. Fill in the necessary information on the Items, Trigger, Filters, and Links tabs. Click Save.

- **Keep an eye out for new versions.** I sincerely hope that in the near future, CrashPlan, Data Backup, and my other favorite backup programs will add direct support for S3, eliminating the need to overcome JungleDisk's limitations.

## Use S3 with Interarchy

Interarchy (http://interarchy.com/, $39) is a popular and capable FTP client, with lots of bells and whistles. One of its latest features is S3 support, so you can use it to transfer files to and from S3 just as you would an FTP server. Although Interarchy is not a backup program, you could use it in conjunction with a backup program—in lieu of JungleDisk—to store your backups on S3. Try one or more of these suggestions:

- Before you do anything else, set up a bookmark for your S3 volume. To do this, choose Bookmarks > New Bookmark. Select Amazon S3 in the Protocol list and List in the Action list. Enter your Access Key ID and Access Key; check Add To Keychain if you wish. (You can leave Path empty.) Then click the Bookmark button.

- You may be able to back up your files to a folder or disk image on your hard disk, and then use the Scheduled Bookmarks feature to upload those files to S3 daily (or on some other schedule). This works best when the name and location of the backup files remains the same on successive runs. But note that if you use this feature to copy large archives, Interarchy will re-upload the entire file each time; it can't simply add to an existing file on S3.

- You can use Interarchy's Net Disk feature to mount your S3 volume on your Desktop. However, unlike JungleDisk, an Interarchy Net Disk does not function like a standard network volume; most backup software won't be able to see it. Also be aware that your S3 Net Disk displays a folder (or "bucket" in S3 parlance) at its top level whose name is a long string of random-looking characters.

- Interarchy is highly scriptable. You may be able to use AppleScript or Automator to construct an automated system that uploads certain backup files using Interarchy. (Sorry, but the details are beyond the scope of this book!)

# Glossary

Look here for definitions of a number of terms relating to backing up, which also appear in the text in blue italics. If you are reading this book on a computer, you can click a blue term to move to the glossary page that defines it and then return to where you were using a menu command or keyboard shortcut, as noted in **Table 5**.

**Table 5: Navigating to the Glossary and Back**

| Viewing Software | Menu Command | Keyboard Shortcut |
|---|---|---|
| Adobe Acrobat 6–8 | View > Go To > Previous View | Command-Left arrow |
| Adobe Acrobat 5 | Document > Go To > Previous View | Command-Left arrow |
| Preview | Go > Back | Command-[ |

**additive:** When a backup copies files that are new, renamed, or modified since the last session without deleting or overwriting older versions, that backup (normally an archive) is additive.

**additive incremental archive:** A type of backup in which files that are new or modified since the last run are added to an archive, without replacing or deleting earlier versions of those files.

**AFP:** Apple Filing Protocol, the network file-sharing protocol used by Mac OS X's Personal File Sharing.

**archive:** An archive is a copy of files as they appeared at multiple points in time, sometimes stored as a single, larger file. Some backup programs use the term *archive* for a backup in which the original files are deleted from the source after being copied to the backup .

**client:** A program that works with a *server* program is a client. For instance, Retrospect Client is a small program you can install on each of your computers. Retrospect Client communicates with the full version of Retrospect on the server, which does the bulk of the work. The computer running client software is often called a client as well.

**client-server:** A type of network backup system in which client computers use a small background program to send files over a network without mounting a volume in the Finder. Backups are initiated by the server and stored on media connected to the server.

**Combo drive:** A Combo drive is an optical drive, standard on some Macintosh computers, that can read from DVD media and write to CD-Rs and CD-RW media.

**data fork:** Although this is less common in Mac OS X than in previous versions of the Mac OS, Mac files can be composed of two portions, a data fork and a *resource fork*. In general, the data fork holds data for the file—text, graphics, video, and so on—that could be relevant to any platform, whereas the resource fork stores data that's relevant only when the file is used on a Mac. (Often this data is ancillary, but other times it is quite important. For example, Classic versions of Nisus Writer store formatting in the resource fork.)

**destination:** The volume (hard disk, partition, optical disc, etc.) to which files are copied during a backup. Also called *target*. Compare with *source*.

**differential:** A type of backup in which each run copies all files which are new or modified since the initial full backup. Compare with *incremental*.

**duplicate:** A duplicate is a complete, exact copy of an entire hard disk that (if it's stored on, or restored onto, a hard disk) you can use to start your Mac if necessary. Sometimes called a clone or a mirror.

**FTP:** File Transfer Protocol, a common method of transferring files over the Internet.

**incremental:** A type of backup in which only files that have been added or changed since the last run are copied. Compare with *differential*.

**local:** Think of local as meaning "part of your computer." If you save a file to your Mac's hard disk, you are saving it locally. In contrast, you can save it *remotely* on a file server, which could be down the hall or on the other side of the globe.

**media spanning:** The capability of a backup program to split data (possibly even a single, large file) across multiple optical discs or other media—and rejoin them when restoring the files.

**multisession:** The ability to record additional chunks of information on a partially used optical disc as separate volumes after the initial write session. Some applications, including Retrospect, can add data to partially-used optical discs using a packet-writing technique;

this does not create additional volumes, and it means that only the program used to record the discs can read them later.

**NAS:** See *network attached storage*.

**NDAS:** See *network direct attached storage*.

**network attached storage:** Typically refers to one or more hard drives with their own Ethernet (or wireless) interfaces. Compare with *storage area network*.

**network direct attached storage:** A type of network attached storage that uses proprietary technology from Ximeta, which allows a drive attached via Ethernet to behave for the most part as if it were directly attached via FireWire or USB.

**off-site:** When backup media is kept off-site, it is moved to a separate building from the one where the original data is stored.

**optical media:** CDs (including CD-ROM, CD-R, and CD-RW) and DVDs (DVD-ROM, DVD-R, DVD+R, DVD-RW, and DVD+RW). So named because they rely on lasers to read and write data. (See Optical Media.)

**peer-to-peer:** A type of network backup in which two or more computers back up to each other, without requiring one to function explicitly as a backup server.

**pull:** A backup initiated by a server, in which data is copied from a mounted network volume (a client computer) onto media connected locally to the server. Compare with *push*.

**push:** A backup initiated by a client, in which data is copied from a local disk to a mounted network volume. Compare with *pull*.

**resource fork:** Although this is less common in Mac OS X than in previous versions of the Mac OS, Macintosh files can be composed of two portions, a *data fork* and a resource fork. In general, the data fork holds data for the file—text, graphics, video, and so on—that could be relevant to any platform, whereas the resource fork stores information that's relevant only when the file is used on a Mac. (Often this information is ancillary, but other times it is quite important. For example, Classic versions of Nisus Writer store formatting in the resource fork.)

**rotating archive:** A backup scheme in which new or modified files are added to an archive incrementally (without overwriting recent versions), but files older than a certain date (or backed up more than a certain number of days ago) are removed to save space.

**rotating backup:** A backup scheme in which a complete copy of all selected files is made during each run, the newest set of files replacing the oldest of two or more previously copied sets.

**SAN:** See *storage area network*.

**script:** A set of instructions for a backup program to follow. Scripts may include *source*, *destination*, schedule, and other options.

**server:** A server is a program that sends information to *client* programs. Backup servers, for instance, work with backup clients to copy files from networked computers onto centrally located media. A computer running server software is also typically referred to as a server.

**SMB:** Server Message Block, the network file-sharing protocol used by Windows and Mac OS X's Windows Sharing. Sometimes referred to (slightly inaccurately) as *Samba*.

**snapshot:** A list of all files in designated folders when a backup runs. Backup software that uses snapshots generally enables you to restore data to its state at the time of any backup with a single operation.

**source:** A source is a folder or volume from which data is copied during a backup; the data's original or primary location. Compare with *destination*.

**storage area network:** A device comprising one or more hard drives able to be shared among several computers, generally via high-speed FireWire, Fibre Channel, or SCSI connections (without using a conventional Ethernet-based network). Compare with *network attached storage*.

**SuperDrive:** An optical drive, standard on many Mac models, that can write to and read from DVD-R media and CD-R or CD-RW media.

**synchronization:** The process of maintaining identical copies of a file, folder, or volume in two or more locations.

**verification:** The process by which a backup program confirms that each copied file is identical to the original.

# About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your feedback; click Feedback on the cover. Keep reading in this section to learn more about the author, the Take Control series, and the publisher.

## About the Author

Joe Kissell is Senior Editor of *TidBITS,* a Web site and email newsletter about the Mac, and the author of many print and electronic books about Mac software, including *Real World Mac Maintenance and Backups* (Peachpit, 2007), *Take Control of Running Windows on a Mac,* and *Take Control of .Mac*. He's also a frequent contributor to Macworld. Joe has worked in the Mac software industry for over 10 years, including positions managing software development for Nisus Software and Kensington Technology Group. He also helps run an Internet publishing business called alt concepts. (http://alt.cc/).

In his increasingly imaginary spare time, Joe likes to travel, cook, and practice t'ai chi. He lives in Paris with his wife, Morgen Jahnke, and their cat, Zora. You can contact Joe at jwk@mac.com; put **`Take Control of Mac OS X Backups`** in the subject line.

## Author's Acknowledgements

Thanks to Adam Engst for providing both the inspiration and the opportunity to write this book, and to Tonya Engst and editor Jeff Carlson for applying gentle pressure to finish it. I also appreciate the helpful feedback from other Take Control authors and members of the TidBITS Irregulars list.

## Shameless Plug

Although I write about computers as my day job, I have a great many other interests, which I write about on several Web sites.

**Interesting Thing of the Day** is my virtual museum. Topics include unusual or intriguing discoveries in food, travel, technology, language, philosophy, science, history, and more. Please click on over to http://itotd.com/ and visit.

**SenseList** is a compendium of lists. Ranging from whimsical to practical, these lists create order out of the chaos of everyday life. You can find SenseList at http://senselist.com/.

In **The Geeky Gourmet**, you can read about culinary science, cooking gadgets, and other topics relating to food and technology. You'll even find the occasional recipe! The site is located at http://geekygourmet.com/.

**Truffles for Breakfast** is the ongoing story of how my wife and I are living our version of the dream in Paris. Visit us at http://trufflesforbreakfast.com/.

Last but not least is my personal blog, **I Am Joe's Blog**. Learn what it's like to be me at http://IAmJoesBlog.com/.

## About the Publisher

Publishers Adam and Tonya Engst have been publishing Mac-related content since they first created their online newsletter, *TidBITS,* about Macintosh-related topics in 1990. At the *TidBITS* Web site you can read about the latest news in the Macintosh world, plus read reviews, opinions, and much more (http://www.tidbits.com/).

Adam and Tonya are known in the Mac world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.

## Production Credits

Link-making AppleScript: Matt Neuburg

List macros: Sharon Zardetto-Aker

Take Control logo: Jeff Tolbert

Cover: Sharon Zardetto Aker, Tonya Engst, and Adam Engst

Editor: Jeff Carlson

Editor in Chief: Tonya Engst

Publisher: Adam Engst

*Take Control of Mac OS X Backups*
ISBN: 0-9759503-0-4
September 2007, Version 2.1

TidBITS Publishing Inc.
50 Hickory Road, Ithaca, NY 14850 USA
http://www.takecontrolbooks.com/

TAKE CONTROL books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control books also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

The electronic version of this book does not use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same info in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Although the author and TidBITS Publishing Inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

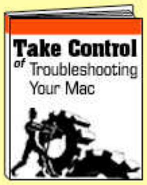
This title is an independent publication, and it has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are trademarks or registered trademarks of Apple Inc.; to view a complete list of the trademarks and of the registered trademarks of Apple Inc., visit http://www.apple.com/legal/trademark/appletmlist.html.

# FEATURED TITLES

Now that you've seen this book, you know that Take Control books have a great layout and real-world info that puts you in control. Click any book image below or visit our Web catalog to add to your book collection!

## Take Control of Troubleshooting Your Mac

by Joe Kissell



Zap Mac problems with Joe's expert advice. Solve 9 common problems and get steps for diagnosing novel ones.

$10

## Take Control of Passwords in Mac OX X

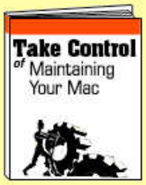
by Joe Kissell

Create and manage strong passwords that keep your data save without taxing your memory!

$10

## Take Control of Maintaining Your Mac

by Joe Kissell

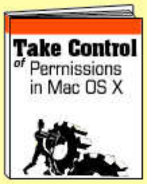


Keep your Mac running smoothly and avoid pesky problems by following an easy maintenance program!

$10

## Take Control of Permissions in Mac OS X

by Brian Tanaka



Solve quirky problems, increase privacy, and share files better by managing Mac OS X permissions.

$10

## Take Control of Your 802.11n AirPort Extreme Network

by Glenn Fleishman

Discover and use the new features in the 802.11n AirPort Extreme Base Station. Solve problems, set up complex networks.

$10

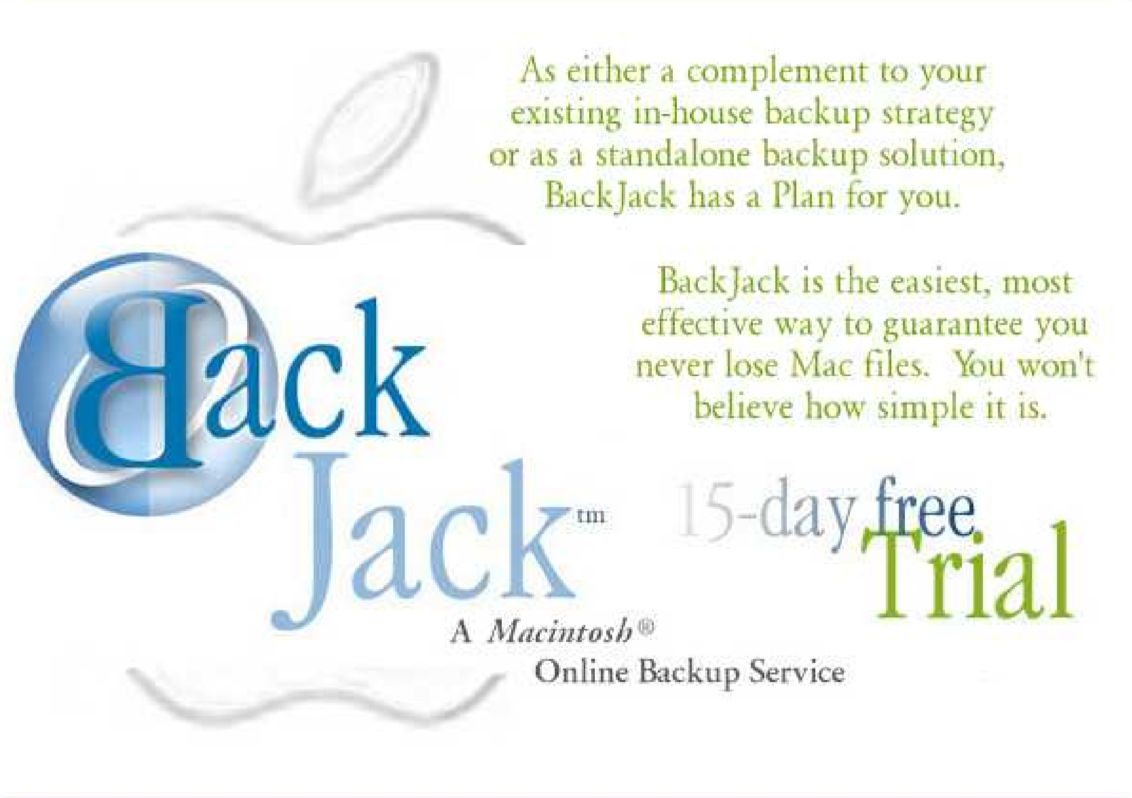
## More Titles!

Delve into even more topics, including:

- Running your Mac—upgrading the OS, fonts accounts, permissions, and sharing files.
- Buying gear—Macs, cameras, and digital TVs.
- More topics—.Mac, AirPort and Wi-Fi security, email, spam, iWeb, iPhone, podcasting, GarageBand, and Microsoft Office.

## Subscribe to BackJack and we'll waive the Billing Activation Fee!
**(a $25 US value)**

$25 $25



As either a complement to your existing in-house backup strategy or as a standalone backup solution, BackJack has a Plan for you.

BackJack is the easiest, most effective way to guarantee you never lose Mac files. You won't believe how simple it is.

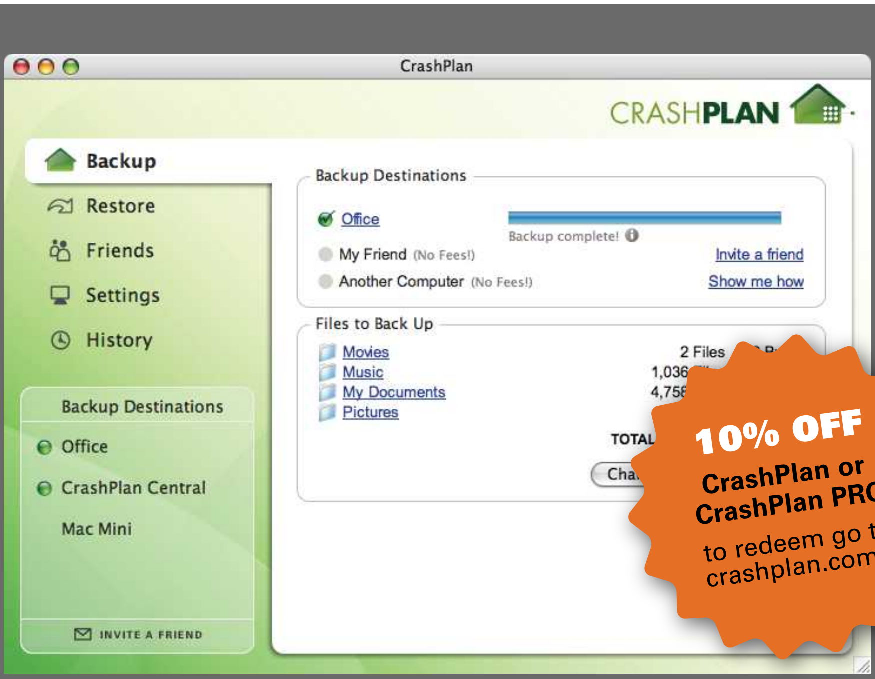
Take advantage of this exclusive offer by visiting
http://www.backjack.com/trial.htm

Enter **TCBU2** in the Promotion Code field.

Once you subscribe to BackJack, we'll confirm the special offer with you directly. We look forward to assisting you with your Macintosh® offsite backup needs!

# Automatic off-site backup for your photos, music, finances and other important files

CRASHPLAN
Automatic Offsite Backup



**10% OFF**
**CrashPlan or CrashPlan PRO**
to redeem go to:
crashplan.com/tc

### Key Features

- ✓ Compatible with non-techies
- ✓ Real-time all the time protection
- ✓ Backup to multiple destinations
- ✓ File encryption & compression
- ✓ Bandwidth throttling
- ✓ Guaranteed restore
- ✓ Supports Mac, PC, & Linux

## Easy to use

No complicated backup schedules, sets or settings. Just press "start backup" and CrashPlan protects your files while you work, without slowing you down.

## Secure

CrashPlan protects your privacy by encrypting files before they are sent.

## Internet Savvy

Problem with your backup? We'll send you an e-mail. Away on vacation? Control your backup from afar.

## Restore in confidence

CrashPlan automatically verifies your backup each night and alerts you if there is a problem. You can't do that with CDs, tapes, or traditional backup software!

## Price

No annoying monthly fees or penalties for how much you backup.

## Better than online backup

It can take weeks to get your data back from an online provider. The more you have, the longer it takes! Also, your data is mixed in with everyone else's making it a juicy target for hackers.

Download free trial at **www.crashplan.com**
CrashPlan for Business: crashplan.com/business

Win Mac Linux

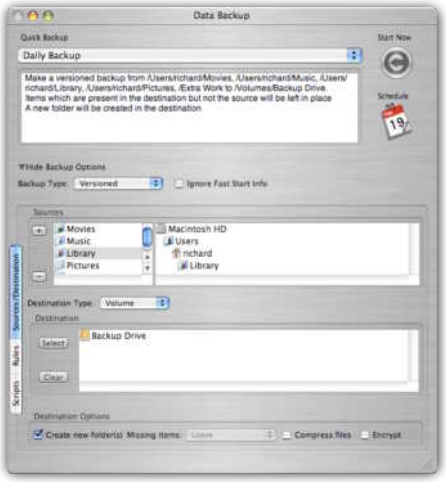
# Data Backup 3

## Easy, Powerful, and Flexible Backups

Data Backup 3 is a powerful utility that allows you to backup, restore, and synchronize your valuable data with minimal effort.  Whether you are a new computer user, or a seasoned professional, Data Backup 3 offers you just the right amount of power, flexibility, and ease-of-use to help you protect your files fast.

Mac Universal

**Data Backup 3**
Mac OS X 10.2.8 or later



Quick Backup: Daily Backup

Make a versioned backup from /Users/richard/Movies, /Users/richard/Music, /Users/richard/Library, /Users/richard/Pictures, /Extra Work to /Volumes/Backup Drive.
Items which are present in the destination but not the source will be left in place
A new folder will be created in the destination

Hide Backup Options

Backup Type: Versioned □ Ignore Fast Start Info

Sources

- Movies
- Music
- Library
- Pictures

Macintosh HD
Users
richard
Library

Destination Type: Volume

Destination: Backup Drive

Destination Options

☑ Create new folder(s) Missing Items: Leave □ Compress files □ Encrypt

## Easy

- No complicated setup – built-in backup sets to quickly backup your iTunes or iPhoto files, other important data or your entire system.
- Easy to define your own backup sets.  Just drag and drop.
- “Fast Start” feature preselects the files to be backed up, saving you time (requires OS X 10.4+)

## Powerful

- Go “back in time” and see your files and directories, as they were when your backups happened.
- Schedule your backups to automatically run at a specific time, on a recurring basis or when a device is connected.
- Have your machine automatically wake from sleep to execute scheduled backups.
- Backups run whether you’re logged in or not.
- Create a bootable clone of your hard drive.
- Choose to compress and/or password protect your backups.

## Flexible

- Backup to any mounted drive including ATA, FireWire, USB, or networked drives
- Backup to CD/DVD disks to automatically span on multiple disks
- Create an exact copy of a folder or a drive, including bootable OS X backups
- Synchronize folders - perfect if you use more than one computer
- Use rules to include or exclude files (such as system files or applications) from backups
- Run scripts before and after your backup executes

SPECIAL OFFER FROM PROSOFT ENGINEERING

Purchase Data Backup 3 for ***50% off***

www.prosoftengineering.com/takecontrol

303 RAY STREET
PLEASANTON, CA 94566
WWW.PROSOFTENGINEERING.COM

PROSOFT
engineering, inc.

Mac mini
iMac