

printout

Keystone MacCentral Macintosh Users Group ♦ <http://www.keystonemac.com>

AppleScripts and AppleScripting

by Tim Sullivan

Applescript is an English-like language used to create script files that control the actions of the computer and the applications that run on it. AppleScript scripts can automate much of what we do, make your time spent of the computer more productive, less stressful, and save us time and money.

That's according to Apple. Actually AppleScripting is a great hobby and, for me, the ultimate computer game — a game of strategy and perseverance. And the end result is something useful.

I hope that some members will find it interesting enough to try their hand. We'll talk a bit about how to modify Applescripts. (*Rule of Thumb #3: Don't write your own Applescript. Plagiarize, purloin, and pilfer any and all coding that you can, then twiddle & fiddle it to work for you.*) Along the way, we'll give some insights to programming in general. ☐

Meet us at

Gannett Fleming

Gannett West Building

209 Senate Ave ♦ Camp Hill

Tuesday, November 20, 2007, 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

AppleScripts and AppleScripting by Tim Sullivan	1
President's Corner by Linda J. Cober	3
Keystone MacCentral Minutes by Gary Brandt	4 - 5
Are Your Fonts Ready for Leopard? by Sharon Zardetto	5
Leopard Compatibility List Updated by TidBITS Staff	6 - 7
Spaces: A First (and Very Happy) Look by Matt Neuburg	7 - 9
Spotlight Strikes Back: by Matt Neuburg	9 - 12
Welcome macprovideo.com by Gary Brandt	12
Time Machine by Joe Kissell	13 - 14
Trojan Horse warning: by Rob Griffiths	15 - 16
November Software Review by Tim Sullivan	16 - 18

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral Printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Computer, Inc. Copyright © 2007, Keystone MacCentral, 305 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles from the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple Computer, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors

President

Linda J Cober

Vice President

Tom Owad

Recorder

Gary Brandt

Treasurer

Jim Carey

Program Director

Gary Brandt

Membership Chair

Eric Adams

Correspondence Secretary

Abigail Schearer

Newsletter Editor

Tim Sullivan

Industry Liaison

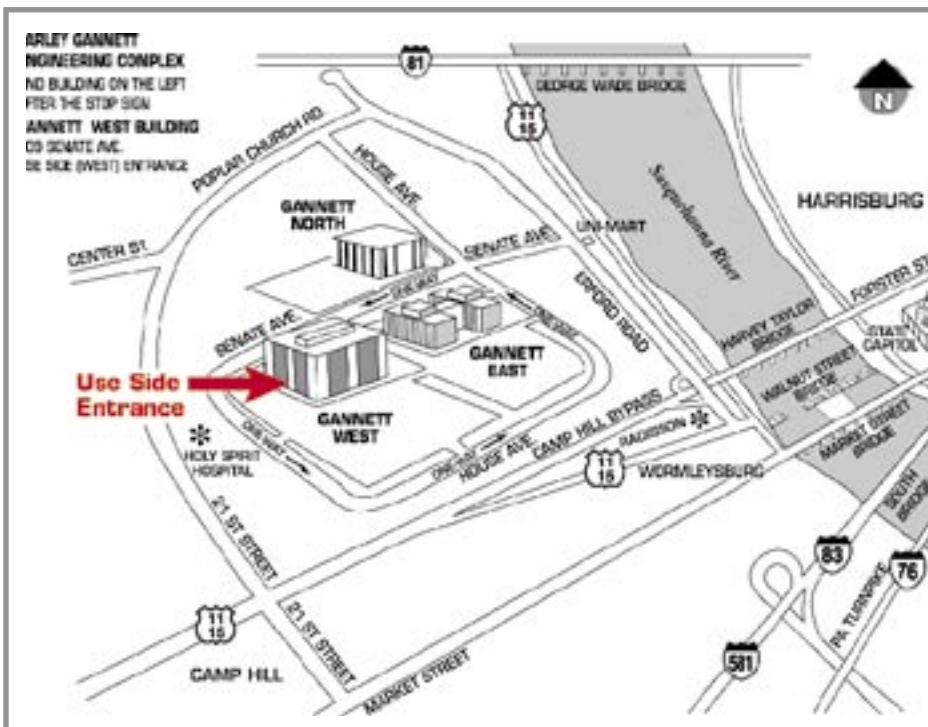
Wendy Adams

Web Master

Linda Smith

Librarian

Tim Sullivan



Keystone MacCentral Essentials

Meeting Place

Gannett West
209 Senate Avenue
Camp Hill

Web Site

<http://www.keystonemac.com>

Mailing Address

305 Somerset Drive
Shiresmanstown, PA 17011

President's Corner

Already it is November, the usual month for our KeyMac auction, but as you have probably noticed, there is no major auction this month. Instead, our auction has been moved to April when it will not occur during a holiday week and when the weather is likely to cooperate. We hope this does not disappoint any of you too much. Since our auction is my favorite meeting, I am sorry to have to wait until April to enjoy it, but I know that I will also enjoy Tim's lesson on AppleScript. In addition to Tim's program, we will have a raffle this month, while our December meeting and holiday party will feature a mini-auction for your enjoyment.

Since Halloween is over and the Christmas goodies are ahead, you may find yourself with leftover Halloween candy. If so, please consider bringing it to our November 20 KeyMac meeting and donating it to the club so we can continue to offer the always popular candy tin to all attendees. I am bringing some to share and hope you will too. Note: the candy does not have to be Hershey's even though that is the label on our tin. We are an equal opportunity candy-loving group!

Leopard is the new cat on the block and from all reports has a lot to offer. We will soon have Leopard on our club laptop and will be showing you some things. We also have Tiger on there and plan to keep both operating systems available since many of you will not be upgrading to Leopard right away. With both systems, we can have the best of worlds, the new world and the old. Note that we will not have system 9 running, as that is now the ancient world! Before you system 9 aficionados get upset, jk, folks, jk, as the kids say. (For those of you who are not up on kidspeak, jk is

the quick, text messaging way to say 'joke.')

See, being a teacher helps one to keep up with the world!

If you have visited the Apple website since Leopard debuted, you may have noticed the words, "All new Macs ship with Leopard." This is true. I, however, in my naiveté, thought that meant Leopard would be installed on the new Macs. Silly me! I learned of my error when the new MacMini that I ordered for Capt'n Don and Janet, my friends living in the Caribbean, arrived quite promptly (ordered on Monday, delivered on Wednesday with free shipping,) but booted up with Tiger. The promised Leopard was there all right but on a disk, not on the machine. Having to install Leopard oneself is not a bad thing since one thus receives two operating systems for the price of one, but I was surprised until I reviewed the words, 'All new Macs ship with Leopard' and realized that the word 'installed' was missing. Once they quit sending an installed Tiger and an accompanying Leopard disk for self-installation, my bet is that 'installed' will be added to the banner.

On another note, if you have not seen the beautiful, new, aluminum iMacs with the gorgeous 20-inch and 24-inch screens, you should! My sister, a Windows person since day 1, saw the new iMacs at Best Buy and astonished me by announcing that she wants one, a 24 inch one to be specific. She was blown away by its crispness and brilliant colors, coupled with the photo applications (iPhoto, iMovie, and PhotoBooth) that show what one can do with pictures and a Mac. She hasn't bought one yet, as rumors of an Apple tablet computer which would utilize the touch screen of the Apple phone and the touch iPod have her waiting until after MacWorld to make her decision, but it looks like by the time of our April auction, she won't be laughed at for being the only 'PC person' in a room of Macaholics!

Come join the rest of your Mac loving friends on November 20 as Tim Sullivan teaches us all how to use AppleScript to make our computing lives easier. Hope to see you there! ☺



Keystone MacCentral Minutes

October 16, 2007

Business Meeting

President Linda Cober reminded everyone at the October meeting of the postponement of our auction to the April 2008 meeting. We will have a meeting in November, with a program on AppleScript planned, presented by Tim Sullivan. We would also be interested in comments on Leopard by any early adopters we have in the group.

Q&A & Comments

The first question was about repairing Epson inkjet printers. The printer was in heavy use so its inkwell ends up getting saturated and then an internal sensor shuts down the printer. Jim Carey mentioned that he had heard of some people reporting success in cleaning Epson printers. He suggested doing a Google search to find what has been written about the procedure. Linda Cober mentioned that some vendors will allow you to return unused ink cartridges.

Someone reported that photos imported into iMovie from iPhoto sometimes appeared with a red cast. This seems to be an isolated incident as no one else had experienced this problem. Another question dealt with the "suspend mode" in Parallels and whether a user is still susceptible to viruses. It appears so and the Microsoft Internet Explorer might be less secure than other browsers. It might be worth trying the Windows version of Firefox if you need to surf from Windows.

Surfing with a Mac browser under OS X is probably even more secure. If you surf when logged in to a user account without administrative privileges, you can add another level of security.

Program Notes

Our October program was of great benefit to the digital photographers among us. According to a show of hands at the meeting, that includes nearly all of the members in attendance. Another show of hands indicated that most were not yet saving their photos in Raw format. Professional photographer Bryson Leidich came in to explain and demonstrate some of the advantages of Raw as compared to the JPEG format. Bryson runs Digital Camp workshops on photography and we got a free preview of some of the topics he will be discussing at his Raw 4.0 workshop scheduled for November 17. He pointed out some of the links he has posted on his web site. In the Learning Resources section, you can download a PDF on digital imaging basics. Articles are frequently updated.

Bryson opened a sample Raw image shot with its white balance set "as shot" and then used a Raw 4 converter to adjust the white balance. The results showed a dramatic improvement in the image.

Professional photographers normally avoid using automatic color balancing for their shots. Images saved as JPEGs have their file settings locked in so bad information will result in a bad photo. A JPEG image protects highlights so more adjustments might

later need to be made to get a desirable final image. If you will be saving images as JPEGs, Bryson recommended shooting at the highest possible settings that storage space allows. That image information will still be compressed when saved as a JPEG. A camera capable of shooting in Raw format eliminates this compression. It saves 4096 pieces of information for each pixel as compared to the 256 for JPEG files.

Bryson discussed working in different color spaces. The ProPhoto color space is widely used in the photo industry. The Adobe RGB color space is another option along with the sRGB color space.

Working with the Raw converter, Bryson explained that exposure can be adjusted by up to four stops. New controls for Recovery and Fill Light are now available in the Raw 4 converter. If you will be saving to JPEG and adjusting images in Photoshop, Bryson suggested setting contrast and sharpening settings in your camera to their lowest settings. This allows for better adjustments to be made with Photoshop. Once a JPEG has been edited in Photoshop, it should be saved as a TIFF or PSD file so it is not recompressed. A JPEG should be considered as an output file.

The Raw 4 converter can process JPEG and TIFF files. All of the global processing can be done in one interface. Changes made to Raw files are saved as metadata in a .xmp file without changing the original Raw image.

Bryson suggested formatting a new card in the camera twice before using it. He demonstrated changing image dimensions and resolutions. He

explained that a file has pixel dimensions and that resolution is only meaningful to the output device. He suggested sending photos in e-mail as 4 x 6 inches for best results. Bryson demonstrated a nice feature of Adobe Photoshop CS3. He showed how easy it is to make

a panorama out of nine individual images using Photoshop CS3 to align and blend layers.

I am certain that all of us amateurs learned something from Bryson. Those of us with the capability will

probably start shooting in Raw soon, while some others might be wishing for a new camera for the holidays. KeyMac would like to thank him for taking the time to come in and pass along his knowledge so that we might take better photos. 🗑️

by Sharon Zardetto

Are Your Fonts Ready for Leopard?

[With the word on the Web being that Mac OS X 10.5 Leopard doesn't support the Classic environment, we asked Sharon Zardetto, author of three Take Control titles about fonts, including the soon-to-be-released "Take Control of Fonts in Leopard," to give TidBITS readers the low-down on how to make sure old font suitcases from Classic are successfully packed for their trip to the future with Leopard. -Tonya]

If you're planning to upgrade to Leopard but are still hanging on to the Classic environment, it's probably time to let go: reports indicate that Leopard won't let you run it, even on a PowerPC-based Mac (Intel-based Macs can't run Classic even under Tiger). But before you go bravely out into the Leopard world, take stock of your fonts - because if you have old ones hanging around, this could be your last chance to straighten out your font suitcase files for free, using Apple's ancient Font/DA Mover utility, which you can still run under Classic.

Two types of font files that predate Mac OS X are still totally useable, but possibly prone to problems: Mac TrueType suitcases and PostScript Type 1 suitcase files (the "screen font" companion files to the "printer font" files). Both of these suitcase-type files have icons that are stamped FFIL and are identified as "Font Suitcase" as their Kind in the Finder.



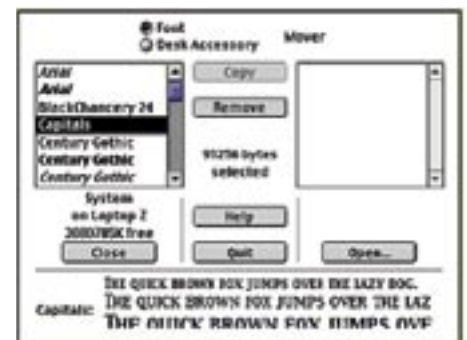
These elderly font files might have inherent internal problems (for the most part, those can be identified, although not fixed, by Font Book's automatic validation process), but the problems I'm referring to here are user-introduced ones.

Pack Your Suitcases for Leopard — To use old fonts in Leopard without trouble, make sure that your suitcase files are:

- Limited to a single type of font. An older suitcase might contain both Mac TrueType and older bitmapped fonts; you should have the TrueType fonts alone in one suitcase, and the bitmapped fonts alone in another if they're serving as the companions for PostScript Type 1 fonts.
- Confined to a single font family, but with all its faces. Wolfson, Wolfson Bold, Wolfson Italic, and Wolfson Bold Italic all go in one suitcase; Wolfson Gothic is a different family and goes in a different suitcase file.
- Named for the font family within. Don't succumb to "MyFavorites" because that's just not helpful, even if your taste won't ever change.

In addition, although pre-Mac OS X systems allowed "loose," non-suitcased font files (a single TrueType face, for instance), Mac OS X can't use that kind of file, and it must be put into a suitcase.

If you remember the ease with which you could manipulate fonts and suitcases under Mac OS 9, you'll be disappointed that you can't do that under Classic - because Classic isn't really an operating system, it just pretends to be under pre-Leopard systems. But what you can do is download Font/DA Mover 4.1, last updated for System 6 (no, that's not a typo!) and run that under Classic to clean up your old suitcase files.



Sometimes you just have to go back before you can go forward.

If You Don't Have Classic Already — If you don't have the option of working under Classic, you needn't scrap your old suitcase files. Two utilities that run under Tiger - Smasher (\$50) and FontDoctor (\$70) - let you manipulate suitcases, and they will, presumably, be updated for Leopard. Both are quite pricey if all you need to do is shuffle suitcase contents. FontDoctor, which is available as a standalone program or with the font manager Suitcase Fusion (\$100), also fixes corrupt font files. 🗑️

Leopard Compatibility List Updated

Rather than write oodles of short articles that mostly note that a new version of some utility adds compatibility with Mac OS X 10.5 Leopard, we're going to take advantage of our new TidBITS Publishing System to create a list of important or interesting software that has been updated. (Our definition of "important or interesting" largely revolves around products that we've covered in the past or plan to cover in the future; there's no way this can or should be a comprehensive list.) It's important to note that this list also doesn't include software that runs fine in Leopard without needing an update - don't infer anything if a program isn't included on the list.

We'll add new items to the top of the list, blog-style, and we'll tweak the modification date each time so those reading via RSS will be alerted when there are changes. We won't be publishing this article in an email edition of TidBITS, since it will continue to grow over time. Eventually, of course, Leopard compatibility will no longer be interesting, and we'll let the article remain static after that point. Until then, though, here's what we know. For releases that are purely for Leopard compatibility, we won't go beyond listing the name, version number, and link; for those releases that are more significant, we'll toss in some notes as appropriate.

02-Nov-07 — Lots more updates today as we work our way back through our press release list.

- Snapz Pro X 2.1.2 and WireTap Studio 1.0.1 from Ambrosia Software: The Snapz Pro X update includes a variety of other minor fixes and enhancements. The WireTap Studio update adds an export drop zone for the iPhone, provides more granularity for

the VU meters, and includes various other bug fixes and enhancements.

- Parallels Desktop build 5540 from Parallels
- Interarchy 8.5.4 from Nolobe
- OmniWeb 5.6 from The Omni Group: Includes a new WebKit-based browser engine for faster rendering performance, the capability to view PDFs in browser windows, a new automatic software update mechanism, improved plug-in and JavaScript performance, and more localizations.
- PasswordWallet for Macintosh 4.2 from Selznick Scientific Software: Also enables you to export your passwords to your iPhone with the \$10 PasswordWallet for iPhone (and iPod touch) add-on.
- 1Password 2.5 from Agile Web Solutions: A significant update that also adds a refined look-and-feel, a new Wallet feature for credit cards, the capability to export passwords to the iPhone, and more.
- DragThing 5.9.1 from TLA Systems: Also includes optional icon reflections, Leopard-related themes, display of EXIF photo data in previews, and the capability to insert and rearrange items by dragging.
- PopChar X 3.3 from Ergonis
- Phlink 3.6 and GeoPhoto 1.6 from Ovolab
- EyeTV 2.5.1 from Elgato: EyeTV 2.51. goes beyond Leopard compatibility to add specific support for Cover Flow, Quick Look, iChat, and Spaces.
- SOHO Organizer 6.5.2, SOHO Notes 6.5.2, SOHO Business Cards 2.5.1 from Chronos

- Simon 2.3 and Caboodle 1.1.2 from Dejal Systems

- The Missing Sync from Mark/Space: Updates coming soon; the company recommends not using The Missing Sync with Leopard until those updates arrive.

- RapidWeaver 3.6.4 from Realmac Software

- Freeway 4.4 from Softpress: Also adds support for Quick Look.

- iDive 1.8.6 and PulpMotion 1.4.6 from Aquafadas

- Merlin 2.5b2 from ProjectWizards: Also includes supports for Quick Look.

- ConceptDraw Mindmap 5.2 from CS Odessa: Includes support for Quick Look and Cover Flow, and can export to iCal in Leopard only.

- iPresent It 2.0 from ZappTek

- Synk 6.3 from Decimus Software


01-Nov-07 — We're mostly catching up with the entries so far.

- Timbuktu Pro 8.7 from Netopia: A \$4.95 upgrade from previous 8.x releases to obtain Leopard compatibility. You need the serial number and the activation code to purchase the upgrade version.

- TextExpander 2.0.3, BrowseBack 1.4.1, and PhotoPrinto 2.1.1 from SmileOnMyMac

- Macaroni 2.1 from AtomicBird

- CSSEdit 2.6 from MacRabbit: Added Leopard compatibility and the capability to open CSS files whose names don't end in ".css", in addition to bug fixes.

- NoteBook 2.1 v261 from Circus Ponies
- KeyCue 4.0 from Ergonis: Major release that also makes it possible to click the keyboard shortcuts revealed by the utility's cheat sheet.
- Miro Public Preview 3
- Hazel 2.1 from Noodlesoft: Also includes several new actions for creating aliases and revealing files.
- Radioshift 1.0.3 from Rogue Amoeba
- Fission 1.5.2 from Rogue Amoeba
- Audio Hijack Pro 2.8 Preview from Rogue Amoeba : The Instant Hijack component is not yet supported on Leopard.
- Airfoil 2.1 Preview from Rogue Amoeba: The Instant Hijack component is not yet supported on Leopard. 

by Matt Neuburg

Spaces: A First (and Very Happy) Look

When Apple posted its list of 300 features that are new in Leopard, your eyes may have glazed over. Many of these new features won't mean anything to you until you've tried them, and, in Apple's list, you can't readily distinguish something small and cute from something massive and profound. (Let's face it, the "Arabesque Screen Saver," while pleasant, is hardly on a par with being able to "Back Up Everything" with Time Machine.) Furthermore, some new features are just hard to describe in a sentence or two, so a proper sense of their implications doesn't come across to the reader. In my view, Spaces is one of those features: It's massive and profound, but Apple's own explanation fails to do it justice. If someone asks you, "Why upgrade to Leopard?" the three little words, "To get Spaces," could be a sufficient reply. For sheer productivity potential, making your computer easier and slicker to work with, Spaces may be the single most important benefit of upgrading to Leopard. In this article, I'll try to help you see why.

So... what is Spaces?

Well, it's a "virtual desktop" implementation. Now, all you Unix X Window virtual desktop users can stop reading right here, or at least skip the next few paragraphs. Those of you who have tried VirtueDesktops (abandoned early in 2007) or the

commercial CodeTek VirtualDesktop also have a sense of what Spaces is about (though these, to be clear, were effectively hacks; the only clean way to implement a virtual desktop feature is to integrate it at system level into the windowing system, as Apple has now done with Spaces). Right now, I want to talk mostly to the virtual desktop newbies who haven't a clue. You others, stick your fingers in your ears and go "La la la," okay?

Okay, clueless newbies - we're all alone together. Come closer. Closer! Good. Here's the deal.

Spaces is all about straightening out the clutter of windows on your screen. What is the biggest problem with windows? It's that there are always too many of them, and most of them are covered by other windows. Thanks to Mac OS X's great memory management, you can run lots of applications at once, and you can have lots of windows open at once; but, no matter how big your screen is, you usually can't actually see all of more than one or (at most) two windows at the same time. Everything else is just a big overlapping mess. And on Mac OS X, as opposed to earlier Macintosh systems, it's even more of a big overlapping mess because the windows of different applications can end up all intertwined with one another.

The result is that when you're trying to get anything done that involves

working in more than one window at once, things get difficult. There's a window in front, and then there's everything else, little corners and title bars sticking out here and there, like the aftermath of a wild game of Fifty-Two Pickup. Where is the precise other window you need to be able to see at this moment? You have no clue.

Notice, please, that I keep talking about windows - not applications. When you come down to the nitty-gritty, getting complex stuff done on your computer is not really about applications; it's about particular windows. Those windows might come from any applications: they could be different windows of the same application, or windows from various different applications.

That's why the simple tools available to you for switching between applications are never quite enough. For example, you can simplify the display on your screen by choosing Hide Others from the frontmost application's menu. Now only the windows of this application are showing. But perhaps you really want to see just one of this application's many windows, plus one window from some other application. So first you might scurry around minimizing the windows from this application that you don't want to see. Then you have to switch to the other application, making it

Continued on page 8

Continued from page 7

Spaces: A First (and Very Happy) Look

visible, and find its desired window and bring it to the front and position it. Then you have to switch back to the first application. Now you can work in both windows. Great, but what happens when you suddenly need a different window from the first application? You have to hunt for it in the Dock, and when you expand it, there it is, blocking everything and complicating the picture. Or perhaps you need a window from a third application: you bring that application to the front, and presto, all of that application's windows are plastered all over the screen, blocking everything and complicating the picture. Is it any wonder tabs have become so popular?

Spaces is all about this problem. It lets you work with sets of windows. That's all a space is - a particular set of windows. When you are "in" this space, just this set of windows is visible. When you switch so that you are "in" a different space, a different set of windows is visible. In the previous paragraph, I was trying to make two points: (1) it's hard to arrange things to see just the small set of windows you need for Task A, and then, (2) when you want to perform Task B, bringing different windows into play complicates the whole picture. With Spaces, Space A could consist of just the windows you need for Task A, and Space B could consist of just the windows you need for Task B. You can then switch between spaces, meaning visible window sets, and everything stays simple: you are always seeing all and only the windows you want to see.

So the main thing Spaces is about is switching spaces. In fact, you can turn Spaces on and never switch spaces, and then you won't even know or care that Spaces is on! You'll be living in exactly the same world you always lived in. In fact - oh my gosh! We'd better actually turn Spaces on, or all

the rest of this discussion is going to be pointless! So, do this:

Choose Apple Menu > System Preferences. Click Exposé & Spaces. Click Spaces. Check "Enable Spaces." Whew! Now Spaces is on.

So how do you switch spaces? There are four (count 'em, four) ways:

- All Spaces mode. This is what you get when you press F8, or click the Spaces icon in the Dock. (If you don't see the Spaces icon in the Dock, drag it in from the Applications folder.) It behaves a little like Exposé, in that it provides a reduced, schematic version of the world: all your spaces are shown at once, in a grid, and now you can click one to switch to that space. This is nice because you can sort of see what windows are in each space. Plus, if you want to get really cool, while you're in All Spaces mode you can press F9 to enter Exposé's All Windows mode, and now each individual space shows each of its individual windows (which are getting pretty tiny at this point) and you can click a window to pick a space and a particular window all at once! (Note: I'm saying "F8" and "F9", but those might not be your actual shortcuts for these actions, because they are customizable.)

- Use the Spaces menu. If you don't see the Spaces menu, check "Show Spaces in menu bar" in the Spaces preference pane in System Preferences. It displays nothing but numbers: the numbers of your spaces (1, 2, and so on). Choose one to switch to that space.

- Use a number. By default, the number shortcuts for switching between spaces involve the Control key. So, press Control-1. Now press Control-2. Congratulations, you just switched spaces.

- Use an arrow key. This is trickier, because it relies on a concept I haven't introduced yet. You see, your spaces are imagined as lying in a grid. You can see this imaginary grid in the Spaces preference pane where we just were a little while ago. By default,

there are four spaces, and the grid is a 2-by-2 rectangle. (This grid is customizable - you can change how many spaces you have and how the grid is arranged - but for this example I'm pretending you haven't yet departed from the default.) So if you are in space 1, you can switch to space 2 by pressing Control-Right arrow, because space 2 is imagined as being to the right of space 1; but, again, if you are in space 1, you can switch to space 3 by pressing Control-Down arrow, because space 3 is imagined as being below space 1. Feeling a bit seasick? Maybe it would better not to use this way of switching between spaces until you are a certified expert (or just plain certified).

There is one more elementary concept connected with Spaces that we need to get clear on: How does a window come to be in a particular space to start with? Well, there are two ways:


- You created the window while you were in that space. For example, you are in space 2, and you start up TextEdit. TextEdit wasn't running before, and when it launches it creates a new window. So you are in space 2 and you are creating a new window, and therefore that new window will be in space 2. Of course there are many other ways to create a new window in various applications.

- You moved the window from one space to another. Huh? Since you can only be in one space at a time, how can you possibly do that? Well, if you're in All Spaces mode, you can actually drag a miniaturized window directly from one space to another. Or, while you are in one space, hold the mouse down on a window's title bar and switch directly to another space with a keyboard shortcut; the window will travel with you to the new space. Or, drag the window to the edge of the screen and pause with the mouse still down and at the screen's edge; you'll switch spaces automatically, bringing the window with you. Keen, eh?

That's all there is to know about elementary use of Spaces. I'm not

going to talk about “application bindings” right now; it’s too advanced for this discussion (you can learn more about that by experimentation, or you can check out my new ebook, “Take Control of Customizing Leopard,” for more info). But there is just one point that I want to leave you with as you start experimenting with Spaces, and it’s this: Spaces is complicated but simple. It’s complicated because there are lots of different scenarios, but it’s simple because Spaces always does “the right thing.”

For example, let’s say you’ve opened TextEdit in space 2, and that’s the only place where any TextEdit windows are. And let’s say you’re now in space 1. And let’s say you use the Dock, or Command-Tab, to switch to TextEdit. What will happen??? Well, what’s the right thing? TextEdit’s windows are all in space 2, so the only sensible thing is that you should automatically be switched into space 2 so you can see them. And sure enough, that’s exactly what does happen. I could go on and on positing various scenarios of greater and greater complexity, but that’s pointless; all you need to know is that Spaces will behave sensibly and simply, and that you’ll catch on to its logic almost immediately with a little experimentation.

So, congratulations: You are no longer a clueless newbie. You’re a clued-in newbie! With a little practice, you will soon find ways to use Spaces that will make your computer life simpler and easier. I can’t tell you what they are because I don’t know what kind of thing you do. Perhaps you’ll usually have a space for all your Internet apps and another space for all your writing apps. Perhaps you’ll have spaces for certain particular tasks that you typically perform. It’s all up to you. I do have one piece of advice, though: Try it, you’ll like it! Whether you’ve got a big multi-monitor setup or a tiny portable screen, Spaces has the potential to make your life a lot easier. You simply have to remember to use it. With a little practice, you will. 

by Matt Neuburg

Spotlight Strikes Back: In Leopard, It Works Great

In earlier articles, we’ve talked about some of the great new features of Leopard that might make an upgrade worthwhile. I wrote an article about Spaces, Glenn Fleishman explained how File Sharing is light years better than it used to be, and Joe Kissell gave us the low-down on Time Machine. (The best way to reference that coverage is from our “Leopard Arrives” series.) In this article, I want to tell you about what I think is the last big piece of the Leopard improvement puzzle - the all-new, all-singing, all-dancing Spotlight.

In order to explain why Spotlight in Leopard is so good, I have to talk briefly about why Spotlight in Tiger was so bad. If you already know that, or if your teeth can’t handle any gnashing, you might want to skip this next section, where I recount a bit of regrettable history.

Tiger Spotlight: The Good, the Bad, and the Ugly – When Spotlight was introduced in Mac OS X 10.4 Tiger, it was touted as a major improvement for users; and it’s not hard to see why. Finding things on your hard disk(s) has always been hard - my mother can’t find a newly created Word document five seconds after she’s saved it - and now that your hard disk is really big and you’ve got lots of files, it’s getting harder. The old-style Finder Find involves searching through the hard disk, file by file and folder by folder, so it’s slow; and besides, it requires that you know, with a fair degree of correctness, the name of the item you’re looking for, which is often exactly what you do not know.

Back in the old System 7 days, on the other hand, a lot of us were crazy

about a wonderful utility called ON Location, from ON Technology. It generated an index of the names of your files, so searching for a file by its name was very fast. What’s more, it used third-party translators to look inside your files, regardless of their format, read their content, and index that as well, so you could do a fast search for a file based on some words used inside the file. Well, Spotlight promised to bring that kind of technology to Mac OS X, only even better. ON Location had to build its index, and to keep the index up to date, it had to rebuild it periodically. Spotlight, on the other hand, once its initial index was built, would always be up to date, because every time you made any change to the hard disk, Spotlight would be notified right then and would modify the index accordingly. Small wonder that Glenn’s article introducing Spotlight to our readers was so hopeful (“Spotlight on Spotlight”, 2005-05-02).

Right from the beginning, however, there was trouble. Some features didn’t work; for example, there was an option to search for invisible files, but no invisible files were ever found. Some areas of the hard drive were excluded from the index, so files in those places couldn’t be found, even by name; this exclusion was hard-coded into Spotlight (it wasn’t a preference the user could access), so there was no way even of learning what the problematic places were. Files of certain types were not found properly; I experienced this particularly with some font files, and Apple confirmed that this was a bug (perhaps caused by the distinction between a file’s visible name and its “display name,”

Continued on page 10

Spotlight Strikes Back: In Leopard, It Works Great

which was sometimes a weird string to which the user had no access). The indexing would mysteriously stop working, and would have to be restarted using the Terminal command line.

Worst of all, however, was the interface through which you actually performed a search and viewed your found results. There were three such interfaces: the Spotlight menu, the Spotlight window, and the Finder search window.

- The Spotlight menu didn't act like a real menu, it often froze up as you were typing your search, and it displayed only a limited number of results. To see all the results, you had to open the Spotlight window.
- The Spotlight window was annoying in every conceivable way. It belonged to no application; it just hung there mysteriously on your computer, refusing to come to the front when you cycled through your windows or your applications. Its interface was unlike any other window; if anything, it seemed like something out of a Web browser, or a Windows machine. Results were clumped by default into annoying categories; getting information about found results (such as, "Where is this file?") required a great deal of clicking; results could not be easily manipulated; and the search could not easily be refined (beyond the simple default refinements listed down the right side of the window).
- The Finder search window had one big advantage: a search could be refined through a Location Bar and multiple Criteria Bars that could be summoned to describe in detail what you wanted to look for. However, you were inconveniently forced to do this even for something as simple

and common as searching for a file by name; you could use the Finder search window only to look for files (not, for example, iCal events); and things were still clumped into groups (mysteriously, not the same groups as in the Spotlight window), though you could ask for a flat list. When you did ask for a flat list, the Finder search window became almost downright good: it started acting quite like a normal Finder window, a familiar and effective interface for working with your results.

The upshot was that none of Apple's Spotlight search interfaces was very pleasant, and none of them gave you access to anything like the full power of Spotlight as implemented through the "mdfind" command-line syntax. For example, mdfind lets you specify wild cards, case sensitivity, and sophisticated boolean criteria combinations. That's why a host of third-party alternative Spotlight interfaces sprang up, including my own NotLight. But even these were restricted in what they could do by the underlying Spotlight indexing technology (for example, NotLight couldn't find invisible files, because neither could Spotlight); and many users preferred to revive the pre-Tiger search behavior with a free utility such as EasyFind.

A New Deal — In Leopard, Spotlight is faster, less biased, and far more compliant. Under the hood, the index is both constructed and consulted more quickly, so you spend less time listening to your hard disk thrash and more time looking at search results. Everything within the scope of your permissions is indexed and searchable (or if something isn't, I've yet to hear about it). Searches that are supposed to work (like searching for invisible files, or searching for a file by the name the user believes it has) do work. And the search interface is so good that it might just put third-party interfaces out of business.

The Spotlight window is completely gone. If you want to move quickly and see the top results, you use the

Spotlight menu; if you want to see all results, or get some interface assistance in constructing elaborate search criteria, you use the Finder window. Those are your only options. The Finder window is now really close to being a normal Finder window: it comes in all the normal Finder views except Column view (though, unfortunately, in List view you can't ask for extra columns of information), and you can do in it nearly anything you can do elsewhere in the Finder, so you'll hardly know you're in a special Spotlight-oriented world. And yet, you are in a special Spotlight-oriented world, as is proven by the fact that you can search in the Finder search window for things that aren't files or folders, such as iCal events and Safari history items. (The main difference I've noticed so far between what you can search for in the Spotlight menu versus the Finder search window is that only the former lets you look up a word in the built-in Dictionary.) Plus, the Finder search window's criteria-construction interface lets you say nearly anything you'd be able to say using mdfind in the command line.

So, for the rest of this article I'm going to explain how to construct a search. There are actually two different "languages" for doing this: there's the textual language of what you type in the search field, which works either in the Spotlight menu or in the search field of a Finder window, and there's the more gestural, interface-based language of manipulating the Finder search window's various options.

The Search Term — When you type "tonya" into the Spotlight menu's search field, that's a search term. Spotlight interprets this as a request to seek matches in a fairly broad way. Capitalization is ignored, so a document containing "Tonya" will match. Diacritical markings are ignored too, sort of; a document containing "Tónya" will match, but if your search term had been "Tönya" then the document containing "Tónya" will match but documents containing

“Tonya” will not, as if your use of a diacritical in the search term had indicated a kind of diacritical wild card. You’re doing a word-based search, but what you’re searching for is the start of a word; so, you’ll also match a document containing “tonyastatic”, though not a document containing “retonyafication”. (To specify that you want to match entire words, put “tonya” in quotes; now you won’t match “tonyastatic”. Quotes can also be used to search for exact multi-word phrases.) But the notion of a word includes camel-cased word components, so you’ll also match a document called “HelloTonya”. Oh, and the search is performed over every kind of metadata, so you’ll match documents with “tonya” in their names, in their contents, in their Spotlight comments, and so on.

Two kinds of modification permit to you restrict the search term’s application. First, you can specify the kind of metadata you’re interested in searching. This is done using a colon-based syntax. For example, to find files that have “tonya” in their Spotlight comments in the Finder, but not files with “tonya” in other types of metadata, you’d put “comment:tonya”. The Help documentation gives several other examples of this syntax, some of which are surprisingly powerful. For example, you can ask for files modified on or before a certain date by saying “modified:<=8/10/2007”, or files created in a certain range of dates with “created:8/10/2007-8/12/2007”. The trouble, though, is that as usual Apple spurns the notion of stooping to provide you with any real documentation: there is no complete conspectus or systematic explanation of the syntax, or even a list of the metadata terms you can specify in this way. (The way I found out about “comment:” in the first example was by trial and error.)

Second, you can combine terms using the boolean operators AND and OR (in capitals), and modify a term with NOT; a minus sign before a term, with no space, means “and not”. The

default operator, supplied if you use multiple words without quotation marks or an intervening boolean operator, is AND. Thus, on my machine, searching on “tonya tidbits” finds 103 items, those that contain both terms; “tonya OR tidbits” finds 530 items; “tonya -tidbits” finds just 15 items, because it’s so rare on my computer for Tonya to be mentioned without also mentioning TidBITS.

The Finder Search Window – To summon the Finder search window, click Show All in the Spotlight menu after a search, or press Command-Option-Space, or (in the Finder) choose File > Find (Command-F), or just start typing in a Finder window’s search field. You can use the search term syntax I described in the previous section, but you can also use the Location Bar and the Criteria Bars to restrict and specify your search in a more graphical fashion.

The first question to ask yourself is whether you want to restrict the search location to one particular folder. If you do, then you must start by being in that folder in the Finder before starting the search by pressing Command-F or typing in the search field. When the window changes to a Finder search window, the Location Bar will display the name of the folder you started in; click that name to restrict the search to that folder.

Another nice feature of the Location Bar is that it offers an option to restrict the search to the “File Name”, as opposed to the “Contents” - the latter being a misleading term which actually means the default of searching all the metadata at once. These two choices, search by name or search by all metadata, are the two most common forms of search, so it’s very sensible of Apple to provide some simple, up-front interface for choosing between them.

To tweak your search further, click the + button at the right end of the Location Bar. This reveals a Criteria Bar. Here you can choose a metadata

type in the leftmost pop-up menu. By default, there are just six sorts of metadata listed here: Kind, Last Opened Date, Last Modified Date, Created Date, Name, and Contents. (Here, “contents” really does mean contents.) When you choose one, other operators, fields, and pop-up menus appropriate to your choice appear. So, with “Contents” the only operator is “contains” and you get a text field for typing some text. With “Name” you get a pop-up menu of five operators: “matches”, “contains”, “begins with”, “ends with”, and “is”. (The difference between “matches” and “is” is that “matches” is word-based; thus, “tonya” matches a file named “Adam and Tonya” using “matches” but not using “is”.) With “Kind” you get a pop-up of subtypes, and some of those subtypes have subtypes of their own; thus, the “Kind” called “Music” can be “All”, “MP3”, “AAC”, or “Purchased”.

There is also a seventh item in the leftmost pop-up menu of a Criteria Bar: Other. This is where things really start to get good. When you choose Other, you get a dialog listing all the kinds of metadata the Spotlight index knows about. You can just pick one to use it; you can also mark a checkbox to specify that that option should appear in the menu from now on, so you don’t have to pass through the Other dialog to access it. I recommend that you immediately check two items that I think you’ll be using quite a lot:

- System files. When set to Include, files are sought even in special locations such as /Library/Caches and ~/Library/Preferences. For example, if you search on “com.apple” you won’t find much, but if you include system files, you’ll find hundreds of preference files.
- Spotlight items. When set to Include, expands the search beyond files and folders to include other sorts of entity, such as iCal events, Safari history items, and preference panes.

Continued on page 12

Spotlight Strikes Back: In Leopard, It Works Great

- (Huge Power User Tip: When you summon the Finder search window with Command-Option-Space, or from the Spotlight menu, Spotlight items is set to Include. When you summon the Finder search window with Command-F or by typing in a Finder window's search field, Spotlight items is not set to Include. This is actually quite brilliant. Spotlight is making a very reasonable distinction and assumption here: if you started in the Finder, you probably just want to look for files and folders, but if you summoned the search window in a more global way, you probably want to look at all kinds of entity. Of course you can always summon a Criteria Bar and change the setting if the initial default isn't what you intended.)

You specify additional criteria by showing and configuring additional Criteria Bars; to do so, just click the + button in any existing Criteria Bar. But here's the real trick: if you click the + button while holding the Option key, you get a special Boolean Operator Criteria Bar. The pop-up menu here says Any, All, or None (the equivalents of the boolean OR, AND, and NOT operators), and it applies to the Criteria Bars that are grouped just after the Operator Bar and indented to the right. Such groups can themselves include a Boolean Operator Criteria Bar, and so you can form boolean expressions of any depth and complexity (the equivalent of using parentheses in a logical expression). The default operation, used if you simply set multiple criteria without grouping them, is AND (that is, all the criteria must be true at once to get a match).

Conclusions — Spotlight in Leopard is what Spotlight in Tiger should have been but wasn't. (Don't get me started

on a rant about why Apple has so much trouble getting these things right the first time out.) How good is it? Maybe not quite good enough to put NotLight completely out of business. NotLight will need modification in order to take advantage of some of the new features of Spotlight's underlying technology, but it has three features that the built-in Spotlight interfaces do not:

1. With NotLight, the search is not live, so things don't keep flashing and bogging down while you're typing a search term; you type until you're ready, then do the search.
2. The Finder Path Bar is great for determining where a found item is by selecting it, but with NotLight you know where every found item is, without having to select it.
3. NotLight lets you choose between case-sensitive and case-insensitive

term matching; sometimes that's actually useful.

Nevertheless, the improvement in Leopard's Spotlight is very, very dramatic - so dramatic that, whereas, in Tiger, once I'd written NotLight, I never used any of the built-in Spotlight interfaces, but used NotLight exclusively for all searching, in Leopard it is quite probable that I will very rarely turn to NotLight. Coming from me, that's big praise. The fact is that the difference from Tiger to Leopard is like night and day: from being a pain and a trial to use, Spotlight is now a joy; from a wretched, ill-advised interface, we now have a model of how interface ought to be, a gorgeous, easy-to-use graphical expression of a powerful and complex underlying syntax. In short, Spotlight could be another major reason for upgrading to Leopard. ☺

by Gary Brandt

Welcome macprovideo.com

I would like to thank a new supporter of Keystone MacCentral. I have been corresponding with macprovideo.com which has offered us access to some of their training videos. I downloaded two for KeyMac and have begun to preview them. The first one on iMovie taught me a few new things that I had not picked up from other sources.

The video covering Aperture looks to be just as well done. I have not gone through all of it yet but I can say that I could learn more from the video than from reading a manual or help files. And there is a lot to learn about that program.

You can navigate to the macprovideo.com site to see for yourself. Linda Smith has posted a link to their site on our Links page in The Training/

Tutorials section. They offer for free preview several sections of most videos. They have videos covering OS X basics and iLife and iWork applications as well as video training on some more advanced video and audio programs. They sell the videos by download only to be earth-friendly. You need to be using OS X 10.4 or later to view downloaded videos and you should ideally have broadband internet access. The videos I downloaded each pretty much filled up a CD. We will be watching these videos at upcoming meetings.

Here's even better news. They have given us several gift certificates for free downloads which KeyMac will offer as raffle prizes at our meetings. So thanks again to macprovideo.com for your support of user groups like ours. ☺

Time Machine: The Good, the Bad, and the Missing Features

In “Take Control of Upgrading to Leopard,” I spent a few pages talking about how to turn on and configure Time Machine, but I didn’t go into much detail because I already have another book, “Take Control of Mac OS X Backups,” which is all about backups and is therefore the proper place to put a full explanation of if, when, why, and how to use Leopard’s new built-in backup feature. I am at this very moment working hard on a new version of that book that will tell you everything you want to know about Time Machine, and though I can’t project an exact release date yet, we will certainly make it available as soon as we possibly can.

However, my work on the new book has been slowed down considerably by having to take time out, on at least a dozen occasions in the last few days, to answer email messages about what I think of Time Machine, how well or poorly it accomplishes some task, whether it’s appropriate for enterprise backups or a suitable replacement for Retrospect, and so on. (The messages usually start, “I know you’re probably going to cover this in an update to your backups book, but...”) I am, of course, always happy to answer messages from readers, but I never dreamed Time Machine would turn into such a drain on my productivity! So, in the interest of heading off more inquiries for a few more days so that I can actually get the book finished, I’d like to take a moment here to offer my initial impressions of, and suggestions

regarding, Time Machine. For more information... wait for the book!

Out of Time — First, some bad news. At the Worldwide Developers Conference in June 2007 - just four months ago - Steve Jobs announced that Time Machine would work with an AirPort Disk (a USB hard drive attached to an AirPort Extreme N base station). As recently as two weeks ago, the same claim appeared on the Time Machine page on Apple’s Web site. But then it mysteriously disappeared, and sure enough, the shipping version of Leopard offers no support for AirPort Disks. For whatever reason, presumably technical difficulties of some sort, Apple dropped that feature at the last minute. So, while it’s still possible to back up multiple Macs in your home or office over a network, even wirelessly, doing so requires a host Mac (running Leopard or Leopard Server) - a step backward in convenience. The same limitation applies to NAS (network-attached storage) devices from other vendors. Although it may be possible to work around this problem, I wouldn’t trust my backups to an unsupported hack, and I strongly discourage you from doing so as well.

That’s not the only missing feature. Apple had previously claimed that Time Machine would support encryption, but it doesn’t. It does keep FileVault archives encrypted, but the cost of doing so is not being able to back them up until you’re logged out of your account - a significant inconvenience. Yet another missing feature is the capability to specify a time

limit beyond which older files will be deleted from your backup disk; now Time Machine simply keeps going until it nearly fills up your disk, and then starts purging older files - with an optional warning, but without an option to offload those older files to other media for long-term storage.

Apart from things many of us expected because Apple had told us about them, Time Machine lacks numerous important features common in other backup programs. A biggie: it can’t make bootable duplicates; if your hard drive dies, you’ll spend long hours restoring your Time Machine backup to a new drive before you can get back to work. It doesn’t let you schedule times when it won’t run, though you can manually turn it on and off whenever you want. You can’t specify more than one destination disk and switch between them automatically (as you might want to do, for example, to keep an extra backup offsite - something I recommend). (It is possible to work around this in various ways, but I have to do more experimentation before I can provide reliable advice.) You can’t back up to an iDisk or to optical media. You can’t compress your backups - you’re going to need, at a bare minimum, free disk space 1.2 times the size of the data you want to back up. And although you can manually specify files, folders, or volumes to be excluded from your backups, Time Machine offers no intelligent filtering (for example, excluding all disk images or all downloaded videos).

Continued on page 14

Time Machine: The Good, the Bad, and the Missing Features

Go Forward to Go Back — I started with the bad news not to diss Time Machine or persuade you that you shouldn't use it, but to put it in perspective. It's the very first version of a brand-new technology. It has limits and bugs (such as a problem with Aperture - see "Leopard Early Fixes and Warnings"), and seemingly lost some features just before its initial release. So despite the one-click setup (very nice) and the groovy 3-D interface for restoring files (extra super nice), it is not the Ultimate Mac Backup Program. At least, not yet.

On the other hand, I can think of at least one excellent reason you might want to start using Time Machine right now: it's guaranteed to be compatible with Leopard! Some of your existing backup software may not be. For example, the developers of SuperDuper are working hard on a Leopard update, but it's not quite there yet. EMC has announced that a Leopard compatibility update for Retrospect will be available within 30 days, and Prosoft says that they're preparing an update to Data Backup 3. Among the backup software already working under Leopard is CrashPlan, thanks to an update on 27-Oct-07. A new version of Carbon Copy Cloner released last week appears to work with Leopard, but may have a few glitches left. And Apple's own Backup just had a minor update for Leopard compatibility (among other things). If you're using any of the dozens of other backup utilities out there, check with the developer for information on its support for Leopard.

Time Machine Impressions — I've been using the final version of Leopard on my main Mac for the past few days, and based on what I've seen so

far, Time Machine appears to work approximately as advertised. It does back up and restore files correctly when I ask it to. However, a few things are not quite as I expected:


- Hourly backups, even to a fast external hard drive with a FireWire 800 interface, often take as long as a half hour! So basically, Time Machine is actively copying files at least half the time. Why does it take so long? It appears that several factors are involved. First, I have .Mac Sync turned on, which results in quite a few files being modified (and therefore, marked as needing backup) every time it runs, whether manually or on a schedule. Ditto for iDisk Sync - since I have a local copy of my iDisk, every time I modify a file there, Time Machine wants to back up that (very large) disk image again. Also, I have Mail checking six IMAP accounts, and every time I get new mail, not only the messages themselves but also Mail's envelope index file and junk mail filter statistics are updated. A number of other background processes on my machine also change files fairly frequently. The net result: on my Mac, Time Machine backs up tens of thousands of files, totaling hundreds of megabytes, every single hour.

- Disk images are a bit of a problem. If you use Parallels Desktop or VMware Fusion, you probably have a very large disk image to hold your Windows installation. Every time you change even a tiny file in Windows, Time Machine is obliged to back up that entire huge file again. The same goes for PGPdisk or even an encrypted disk image you create with Disk Utility to hold confidential files: any small change marks the entire large file as needing to be backed up again. This results in a tremendous waste of space on your backup disk, not to mention a longer time spent performing each backup. Several newer backup programs, including CrashPlan and QRecall, can back up just

the changed portion of a large file, but Time Machine's approach makes doing so fundamentally impossible.

- If I activate Time Machine while in Mail, I immediately see dozens of spam messages in my Inbox that were never there before! Mail's junk mail filter intercepted them as soon as they arrived and routed them to my Junk mailbox, but apparently Time Machine doesn't care; Junk is, in fact, the only mailbox that's dimmed when in Time Machine's restore mode, so I can't look at how just that one folder was in the past. I think Apple is trying to be helpful here by highlighting the fact that a "missing" email message may not be missing at all but merely mistakenly filed in your Junk mailbox. But I don't want Time Machine to second-guess me like that.

- Third-party support for Time Machine is still lacking. It's great that I can restore individual items from Mail, Address Book, iPhoto, and so on. But I'd like to restore individual keychain items from 1Password, individual snippets from DEVONthink Pro Office or Yojimbo, and individual records from FileMaker Pro databases. So far, very few non-Apple applications support Time Machine at the record level. If and when they do, Time Machine will become vastly more useful.

Ultimately, I expect I'll continue using Time Machine, but only as one part of a broader backup strategy. Time Machine is pretty good at what it does, and may get even better over time. Even in the best case, though, I'll need some other software to make bootable duplicates, an additional strategy to deal with offsite backups, and probably some fiddling to deal with problem areas like disk images and never-ending hourly backups. And now, if you don't mind, I must get back to my testing, so that I can explain exactly how to do all these things in that book I'm writing! 

Trojan Horse warning: What you need to know

How to detect — and remove — the OSX.RSPlug.A Trojan Horse

As you may have read, a new piece of OS X malware has been discovered. Intego has named this malware the OSX.RSPlug.A Trojan Horse. Note that this malware is not a virus—it can't self-propagate from one machine to another. It is, however, definitely malicious, and it's packaged in a well-designed trojan horse wrapper.

Your machine could be infected if you've recently gone looking for some, um, less-than-flattering pictures of Britney Spears. Thinking you've found what you're looking for, you click a video to watch it, only to see a message stating that your machine lacks the necessary codec. A disk image will then start downloading, and (depending on the settings on your machine) may then mount and launch an installer which asks for your admin password.

Rule #1: Do not install software from untrusted sources, especially if that software comes as an installer package and requests your administrator's password! However, if you do proceed to run the installer, here's what will happen:

- Sorry, but you won't be able to watch those videos, as no codec was installed.
- Your DNS will be changed to point to malicious DNS machines. What this means is that even if you type `www.apple.com` in your browser's URL area, you may be taken there, to a phishing "clone" of that site, or to another site completely—such as a porn site. Where you wind up depends solely on how the malicious

DNS machines are configured. If you consider `ebay.com` or `paypal.com`, for instance, the consequences may be dire.

- A cron job (scheduled task) will run every minute to restore the malicious DNS info, in case you change it.

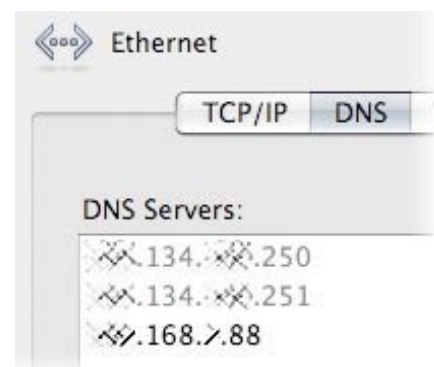
This is really bad. Really. And even though it's targeted at porn surfers today, the malware could easily be associated with anything else, like a new viral video site, or a site that purports to show commercials from the upcoming Super Bowl. Because this thing may spread to other such sites, we spent some time investigating the trojan—no, not its source sites!—to determine the best way to tell if you've been infected, as well as how to remove the software if you do find it on your machine.

How to detect the trojan horse

What makes this trojan sneaky (for OS X 10.4 users, at least) is that there's no visible way to see that the DNS information has been changed. So how can you tell if you've been infected? If you're a VirusBarrier user and you have your definitions updated as of today, VirusBarrier will both find and remove the trojan horse.

If you're running OS X 10.5, open your Network System Preferences pane and select your active interface (AirPort, Ethernet), then click Advanced. On the Advanced screen, click on the DNS tab. The leftmost box contains your DNS servers, and all the entries should be in black. If the trojan has been installed on your machine, you'll see the phantom DNS

in gray, listed above your normal DNS information, as seen in the image below — the first two entries are the evil DNS, the last is the normal DNS.



Note: There are other situations where the DNS info may be gray—it appears that if your DNS is provided by another machine, for instance, then your legitimate DNS information will be in gray, not black. So while this may be an indicator, keep reading for the best way to be certain if your machine is infected.

The easiest way to tell if you've been infected is to go to the top-level / Library -> Internet Plug-Ins folder, and look for a file named `plugins.settings`. If you find one there, chances are, you're infected. However, since the names used by the malware authors may change, it's best to check a couple of other spots as well.

The other thing to check is for the presence of the root cron job. To do this, open Terminal (in / Applications -> Utilities) and type this command:

```
sudo crontab -l
```

Continued on page 16

Trojan Horse warning: What you need to know

Enter your admin password when asked, and Terminal will then display any cron tasks for root. Typically this will be blank. If you see this output, though, it means you've got the malware:

```
***** "/Library/Internet Plug-Ins/  
plugins.settings">/dev/null 2>&1
```

If you really want to be sure, you can run `scutil` in Terminal (it's an interface to `configd`, an OS X system utility). Type `scutil` and press Return, then type this command at the prompt, followed by another Return: `show State:/Network/Global/DNS`. The output will look something like this:

```
<dictionary> {  
  ServerAddresses : <array> {  
    0 : 123.12.34.56  
    1 : 234.65.43.21  
  }  
}
```

Those are all the DNS servers your machine knows about. (You can type `exit` to get out of `scutil` and back

to Terminal.) Look at that list and compare it to what you see in the Network preferences panel—make sure you click into the two-line DNS Servers box there and use your down arrow key, just in case there are more servers listed than you can see. The two lists should be the same. If you see servers in the output from `scutil` that you don't see in the GUI, then the trojan has probably been installed.

How to remove the trojan horse

If you're infected, what's the easiest way to get rid of the trojan horse? As noted above, `VirusBarrier` will do the job, using today's virus definitions. However, you can do it yourself, if you wish, though it will require a tiny bit of Terminal work. Here's what you need to do—and yes, I infected my own machine and tested this (on OS X 10.5, but OS X 10.4 should be identical) to make sure it works.


- In the Finder, navigate to `/Library -> Internet Plug-Ins`, and delete the file named `plugins.settings`. Empty the trash. This deletes the tool that sets the rogue DNS Server information.
- In Terminal, type `sudo crontab -r` and provide your admin password when asked. This deletes the root cron job that checks the DNS Server settings. You can prove it worked by typing `sudo crontab -l`; you should

see the message "crontab: no crontab for root."

- Open your Network System Preferences panel, go to the DNS Server box, and copy the entries you can see to a Stickies note, TextEdit document, or memorize them. Now retype those same values in the box, then click Apply.
- Reboot your Mac.

After you reboot, you can confirm you're free of the trojan horse (in OS X 10.5) by opening the Advanced pane of the Network System Preferences panel and looking at the DNS tab—you shouldn't see any gray entries. In Tiger, to really prove that you're free of the infestation, use the `scutil` command detailed above, as that's the only way to see all the DNS Servers your machine knows about.

As always, the best way to avoid these things is to not install software from untrusted sources—especially if it comes as an installer package and requests your administrator's password! But if you do get infected, at least you'll know how to confirm you have an issue, and remove the troublesome software.

[EDITOR'S NOTE: This article has been updated to reflect other causes of gray DNS entries, as well as a better method of detecting the presence of the malware.] 

by Tim Sullivan

November Software Review

Saving stuff on a hard drive is a good thing — until the drive begins to fill up. When that begins to happen, consider archiving rarely used files and folders.

There are many programs that can be called into play. Some are available on your Mac assuming that you are running OS X. You can go to Finder's

File > Create Archive. That will create a .zip file. Or you can use, from the terminal, the Unix tar command to create a .tgz file.

Stuffit, a rather expensive commercial program, is one of several available solutions to archiving.

The whole point of archiving is that there is usually a significant savings

in disk space used when the files are compressed. The downside is that the individual files are no longer readily apparent without uncompressing the whole thing. (We are assuming that the original files were trashed after creating the archive.)

Springy is an inexpensive solution to archiving.



Springy 1.3.3 <http://www.springyarchiver.com/>

Requirements: OS X 10.3 or later for Macintosh computers with PowerPC processor, OS X 10.4.4 or later for Macintosh computers with Intel processor. Universal binary. \$18

Springy is a program for creating, examining, and extracting files from archives.

Springy features at a glance:

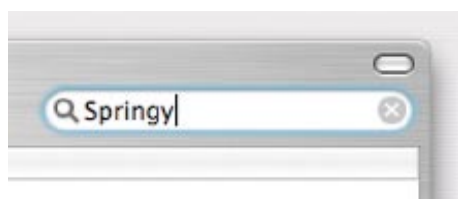
- Archiving and extracting tasks may be accomplished quickly and efficiently using Finder contextual menu and full Drag & Drop support for archiving and extracting from and into Finder.
- Preview any file in an archive or disk image by double click.
- Open and browse the contents of an archive or disk image without extracting any file from it.
- Quickly extract all files or only files of choice from an archive or disk image.
- Modify the contents of an existing archive or disk image: add, overwrite, delete and rename files.

Standard Archive Types

Supports common and most often archive types, compression methods and disk images: ZIP, TAR, DMG, ISO, GZIP, BZIP2, Unix Compress, RAR, SIT, Java archives JAR, WAR, EAR... Support for more types still to come...

Search For Files In Archive

It's no use of being able to extract single file from an archive if you cannot locate that file easily. Search for files with particular names or part of their names. All without extracting.



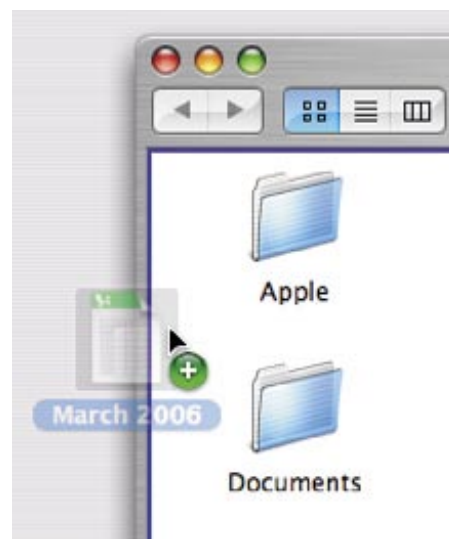
Choose Your View

View and browse files in archive the way you browse files on your disk. Icons, list, or columns, you choose.



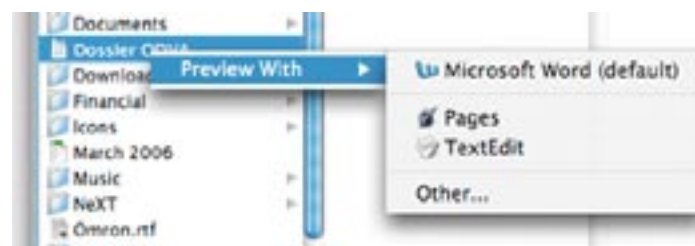
Drag & Drop

Archive and extract files by dragging & dropping them wherever you want. Simple and easy, as it was always supposed to be.



Preview

Preview files inside archives in default application with just double-click. Or if you don't want default application, you are free to choose whichever you want.



Protect Yourself

Keep sneaking eyes away from your important files. Use built in encryption and password protection for all archive types that support it.



Rich Finder Contextual Menu

Do all of your archiving and compressing tasks quickly and easily from Finder contextual menu, which is just one right click away anytime.

Apple Updates

Login & Keychain Update 1.0

10/30/2007

System Requirements

- OS X 10.5

This update is recommended for all users running Mac OS X Leopard.

Aperture 1.5.6 Update

10/26/2007

System Requirements

- OS X 10.4.8 or later
- OS X 10.5
- Aperture 1.5 to 1.5.4

Aperture 1.5.6 addresses issues related to performance, improves overall stability, and supports compatibility with Mac OS X v10.5. This update is recommended for all Aperture users.

Backup 3.1.2

10/26/2007

System Requirements

- OS X 10.3.9
- OS X 10.4.2 or later
- OS X 10.5

Backup 3.1.2 is highly recommended for all users of Backup 3. This update includes reliability improvements and improves compatibility with Leopard and iWork '08.

Continued on page 18

November Software Review

iLife Support 8.1.1 10/25/2007

System Requirements
– OS X 10.4.9 or later

This update supports system software components shared by all iLife '08 applications, improves overall stability, addresses a number of other minor issues, and support

iDVD 6.0.4 10/25/2007

System Requirements
– OS X 10.3.9 or later

This update improves overall stability and supports compatibility with Mac OS X 10.5.

GarageBand 3.0.5 10/25/2007

System Requirements
– Mac OS X 10.5
– iLife '06

This update supports compatibility with Mac OS X 10.5.

iMac MXM Update 1.0 10/25/2007

System Requirements
– OS X 10.4.10
– iMac (Late 2006 24-inch)

The iMac MXM Update improves video compatibility with Boot Camp on certain 24" iMac models.

This installer places the iMac MXM Update firmware updater in the / Applications/Utilities folder on your computer. Run the updater in the Utilities folder to install the update. Updating takes only a few seconds.

ATI Radeon X1900 XT Firmware Update 10/16/2007

System Requirements
– OS X 10.4.10
– Mac Pro

The ATI Radeon X1900 XT Firmware Update will update the firmware on all of the ATI Radeon X1900 XT graphics cards in the Mac Pro. The updater application will be installed in the / Applications/Utilities folder.

[To determine which graphics card is installed on your computer, select "About This Mac" in the Apple menu; then select

"More Info..."; and finally "Graphics/Displays" in "Hardware."]

GarageBand Jam Pack Voices 1.0.1 10/10/2007


System Requirements
– OS X 10.3.9 or later
– GarageBand Jam Pack Voices 1.0

An expansion pack including over 1500 royalty-free vocal loops and vocal instruments performed by professional singers and rappers.

Battery Update 1.3 10/03/2007

System Requirements
– OS X 10.4.10
– MacBook Pro (15-inch)

Battery Update 1.3 updates battery firmware and addresses battery performance issues with the 15-inch MacBook Pro. Your computer's power cord must be connected and plugged into a working power source while running this update.

After the Battery Update has been installed, any additional batteries you put in your 15-inch MacBook Pro are automatically updated. 

Share Keystone MacCentral with other MACaholics

Name _____

Address _____

City _____ State ____ Zip _____

Home Phone _____ Day Phone _____

E-mail Address _____

Date _____

Is this Renewal or New?

How did you hear about us? _____

Dues for one person are \$20/yr.

Family or Corporate dues are \$30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

**Keystone MacCentral
Membership Chair
305 Somerset Drive
Shiresmanstown, PA 17011**

Keystone MacCentral meetings are held at 6:30 p.m. on the 3rd Tuesday of the month at Gannett Fleming, 209 Senate Avenue, Camp Hill.