May 2012
Vol. XXIII, No 5

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ http://www.keystonemac.com

Using Photoshop Elements: A Continuation

For the May meeting Ernie Levasseur will review some of the material he covered at our January meeting on the basics of Photoshop Elements. He will continue his presentation by demonstrating some of the ways to select objects in Photoshop Elements. Ernie's presentation was well received in January so we hope you can attend the May meeting for another informative evening.

The election of board officers will be held during the May meeting. Current board members have agreed to run for another two year term. Members can nominate other interested members to run for any position.

Meet us at

Giant Food

Corner of Trindle Road & 32nd St (Route 15)
3301 East Trindle Road, Camp Hill, PA 17011

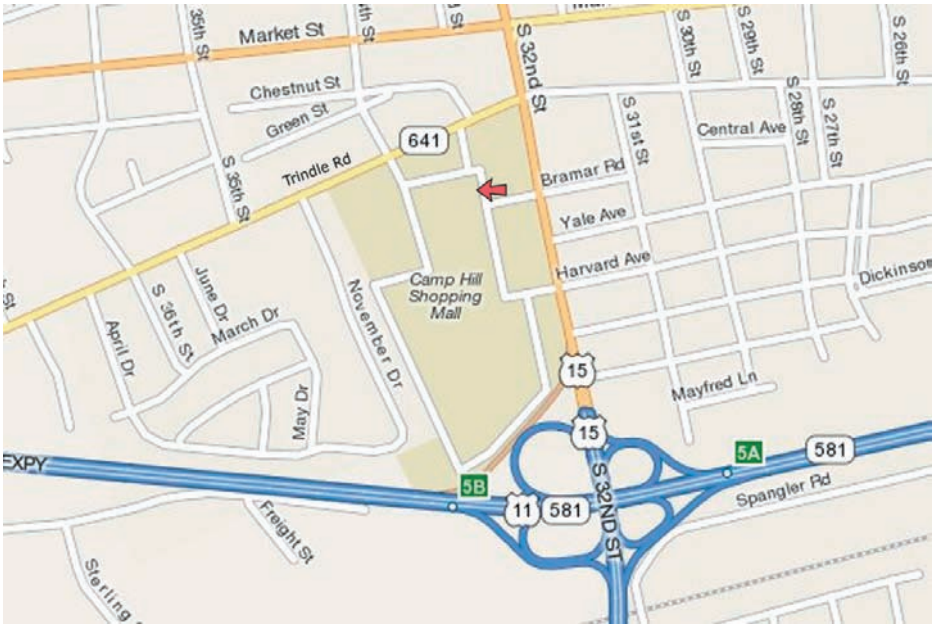
Tuesday, May 15, 2012 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

Using Photoshop Elements: A Continuation 1
President's Corner *by Linda J. Cober* 3
Keystone MacCentral Minutes *by Gary Brandt* 4
How to Tell If Your Cloud Provider Can Read Your Data *by Rich Mogull* . . . . . 4 - 6
Use Dropbox to Troubleshoot Family Macs *by Jeff Carlson* . . . 6 - 7
Rumors and Reality *by Tim Sullivan* 7
May Software Review *by Tim Sullivan* . . . . . 8 - 11
Mac 911 *by Christopher Breen* 11- 12

Board of Directors



Keystone MacCentral Essentials

Meeting Place
Giant Food (upstairs)
Corner of Trindle Road & 32nd St (Route 15)
Camp Hill

Web Site
http://www.keystonemac.com

Mailing Address
310 Somerset Drive
Shiresmanstown, PA 17011

by Linda J. Cober

President's Corner

Wow! Our April meeting/auction was a great one, so I am sorry for anyone who missed it! As I had predicted based on the number of donations from generous vendors, we raised a record amount of money for the club. Please remember to check the vendor list on our website when you are looking to make a purchase since we want to support the vendors who so graciously support us! Also, a big "thank you" to Chuck Joiner who once again served as our guest auctioneer and did a good job of describing each product before bidding began. With Chuck's expertise on all things Mac/Apple, vendors can be assured that their donations were properly displayed and appreciated.

Just as in our private lives, however, when additional money is available, there is always something that requires an upgrade. Thanks to Lion, both our webmaster and our newsletter editor have to upgrade to the newer versions of InDesign and Dreamweaver in order to continue providing us with our website and newsletter. Because of the May 6 deadline to upgrade and save over $200, the officers authorized the expenditure instead of waiting for the club meeting to ask for member approval. We figured that any club members who did not want us to spend the money for the webmaster or newsletter editor would thus be volunteering to take over the jobs themselves. Any opposition? :) By the way, even if you do not oppose our expenditures, you are welcome to run for a seat on the board at our upcoming May 15 meeting since that is our election day. Fortunately, all our current officers are willing to continue in their current roles, but none of us have any objection to allowing someone else to take over the officer duties. Any takers?

On another note, I have a book review for a book that you may soon want to buy. As Apple keeps reminding us every time we access MobileMe, time is running out on that service and "it is time to move to iCloud." Like the rest of you, I have known this for some months now, but with the deadline of June 30 starting to loom on the horizon, the need to upgrade to Lion and make the move to iCloud is becoming more urgent. Thus, I figure that learning more about iCloud would be wise. PeachPit Press (which offers user group members a discount on purchases) publishes a Visual QuickStart Guide to iCloud by Tom Negrino. The book cover says, "Learn the quick and easy way!" and I found this to be true. Chapter 1 gets you started, explaining just what iCloud is, the hardware and software requirements (OS 10.7.2 for your Mac; iOS5 on your mobile device), Apple ID considerations, configuring iCloud on your Mac, and migrating to iCloud from MobileMe. Chapter 2 teaches you how to set up iCloud mail accounts on your Mac and mobile device, work with mail on the iCloud website, and send iMessages, which allow you to text for free anyone who is also using a device with iOS5. Carriers such as Verizon and AT&T typically charge about $20 per month for unlimited text messages or pay as you go at 20 cents per text message. If you want to send MMS which include pictures or video, the cost goes up to 25 or 30 cents per message. Hmmm. Pay $240 or more per year or send iMessages for free? See the benefits of iMessage? My sister and I do not pay for text messaging on our iPhones, but iMessages allow us to send texts to each other. Chapter 3 teaches us to work with contacts, including contact groups. Chapter 4 covers working with calendars and reminders. Chapter 5 goes into using iPhoto with iCloud, including setting up and working with Photo Stream in iPhoto and deleting photos. Photo Stream allows you to share your photos with all your devices, so you can display photos from your Mac on your iPad or iPhone anytime you are connected to Wi-Fi. Chapter 6 explains how to use iTunes with iCloud. Now, any music you have in iTunes can be on any of your devices. Backing up is always important, and Chapter 7 covers backing up to iCloud. Here, you will learn how to configure iCloud Backup, restore an iOS device from Backup, and manage iCloud storage. Chapter 8 discusses synchronizing browser bookmarks with iCloud while Chapter 9 shows readers how to configure and work with iWork documents on the iCloud website. The last chapter of this 173-page book discusses how to use iCloud to find people and devices. Find My Mac, Find My Friends, and Back to My Mac are explained in detail.

If you are planning to upgrade to iCloud and need some guidance, this Visual Quickstart Guide to iCloud by Tom Negrino is a good way to go. Like other Quickstart Guides, the book is clearly written and the instructions are easy to follow. Remember your PeachPit Press user group discount too!

See you at our May 15 meeting as Ernie Levasseur continues his excellent presentation of the features in PhotoShop Elements! Bring your questions and a friend or two!



by Gary Brandt, Recorder

Keystone MacCentral Minutes

April 17, 2012

Auction Action

Our annual auction was held on April 17 at Giant, with sodas and snacks provided for all those in attendance. President Linda Cober went over the auction rules and also reminded us that elections of board members would be held at the May 2012 meeting.

Eric Adams succeeded once again in getting many great donations from vendors. Eric was the contact for anyone who needed to register some of the software downloads we sold. Contact Eric if you did not do so at the auction so he can pass your contact information along to the vendors of the products you bought. Chuck Joiner served as auctioneer, with Tucker Hill serving as runner and taking over as auctioneer whenever Chuck was involved in the bidding.

The rest of the KeyMac board did their regular auction duties. Linda Cober brought in the collected items and took payments at the end of the auction. Tim Sullivan had prepared tags for many of the items prior to the auction, so board members could attach the tags to the items before bidding began. Chuck Joiner and Tom Owad gave quick reviews of the items they were familiar with. Tom Bank II navigated to the vendor web sites to display additional product information on the items being auctioned. Eric staged the items for Chuck and passed the auction slips to Gary Brandt who tracked the winning bids. The slips were given to Tim Sullivan who was running the database to tally all of the sales. KeyMac Vice President Tom Owad donated a number of items from his company, Schnitz Technology, including an hour of in-lab computer repair.

Both hardware and software titles elicited lively bidding. The bidding for the G-Drive 2TB drive from G-Technology was particularly spirited. Other hardware that brought in high bids included the Bamboo Connect Tablet, the Matias OneKeyboard, and the items donated from Elgato. Bidding for some of the software was also strong. The auction closed with bidding on an HP Officejet Pro 8600e printer.

For the full list of items that were donated, please visit the Vendors page of our web site. We hope you will support these vendors whenever possible. Thanks go to everyone who contributed to such a great evening. It looked like no one walked away empty-handed.

by Rich Mogull

How to Tell If Your Cloud Provider Can Read Your Data

With the tremendous popularity of services like Dropbox and iCloud there is, rightfully, an incredible amount of interest in cloud data security. Once we start hosting our most sensitive data with cloud services (or any third-party provider) it's only natural to wonder how secure our data is when it's in the hands of others. But sometimes it's hard to figure out exactly who can look at our information, especially since buzzwords like "secure" and "encrypted" don't necessarily mean you are the only one who can see your data.

How Cloud Providers Protect Your Data — In part because there are numerous ways cloud providers could protect your data, the actual implementation varies from service to service. All consumer cloud services are what we in the cloud world call public and are built for multi-tenancy.

A public cloud service is one that anyone on the Internet can access and use. To support this the cloud providers need to segregate and isolate customers from each other. Segregation means your data is stored in your own little virtual area of the service, and isolation means that the services use security techniques to keep people from seeing each other's stuff.

Practically speaking, multi-tenancy means your data is co-mingled with everyone else's on the back end. For example, with a calendar service your events exist in the same database as all the other users' events, and the calendar's code makes sure your appointment never pops up on someone else's screen. File storage services do the same thing: intermingling everyone's files and then keeping track of who owns what in the service's database. Some, like Dropbox, will even store only a single version of a given file and merely point at it from different owners. Thus multiple users who happen to have the same file are technically sharing that single instance; this approach also helps reduce the storage needed for multiple versions of a file for a single user.

Although multi-tenancy means co-mingling data, the cloud provider uses segregation techniques so you see only your own data when you use the service, and isolation to make sure you can't maliciously go after someone else's data when you're using the system.

The cloud provider's databases and application code are key to keeping all these bits separate from each other. It isn't like having a single hard drive, or even a single database, dedicated to your information. That simply isn't

efficient or cost-effective enough for these services to keep running. So multi-tenancy is used for files, e-mail, calendar entries, photos, and every other kind of data you store with a cloud service.

Not all services work this way, but the vast majority do.

Encryption to the Rescue? — A multi-tenancy architecture has two obvious problems. The first is that if there's a mistake in the application or database the service runs on, someone else might see your data. We've seen this happen accidentally; for example, last year Dropbox accidentally allowed any user access to any other user's account. There is a long history of Internet sites (cloud and otherwise) inadvertently allowing someone to manipulate a Web page or URL to access unauthorized data, and the bad guys are always on the lookout for such vulnerabilities.

The second problem, which has been in the press a lot lately, is that the cloud provider's employees can also see your data. Yes, the better services usually put a lot of policy and security controls in place to prevent this, but it's always technically possible.

One way to mitigate some of these concerns is with encryption, which uses a mathematical process coupled with a digital key (a long string of text) to turn your data into what looks like random gibberish. That key is necessary to decrypt and read the data.

Most cloud providers use encryption to protect your Internet connection to them (via SSL/TLS – look for https URLs) so no one can sniff it on the network. (Unfortunately, some large e-mail providers still don't always encrypt your connection.) Most of the time when you see "encryption" in a list of security features, this is what they mean. But encrypting data in transit is only half the battle – what about your data in the provider's data center? Encryption of storage is also necessary for any hope of keeping your data secret from the cloud provider's employees.

Some providers do encrypt your data in their data center. There are three ways to do this:

1. Encrypt all the data for all users using a single key (or set of keys) that the cloud provider knows and manages.

2. Encrypt each individual user's data with a per-user key that the cloud provider manages.

3. Encrypt each individual user's data with a per-user key that the user manages.

By far, most cloud services (if they encrypt at all) use Option #1 – keys that they manage and that are shared among users – because it's the easiest to set up and manage. The bad news is that it doesn't provide much security. The cloud provider can still read all your data, and if an attacker compromises the service's Web application, he can usually also read the data (since it's decrypted before it hits the Web server).

Why do this level of encryption at all? It's mostly to protect data if a hard drive is lost or stolen. This isn't the biggest concern in the world, since cloud providers have vast numbers of drives, and it would be nearly impossible to target a particular user's data, if the data could be read at all without special software. It also means that providers get to say they "encrypt your data" in their marketing. This is how Dropbox encrypts your data.

Option #2 is a bit more secure. Encrypting every user's data with an individual key reduces, in some cases, the chance that one user (or an attacker) can get to another's data. It all depends on where the attacker breaks into the system, and still relies on good programming to make sure the application doesn't connect the wrong keys to the wrong user. It's hard to know how many services use this approach, but when done properly it can be quite effective. The major weakness is that the cloud provider's employees can still read your data, since they have access to the keys.

Option #3 provides the best security. You, the user, are the only one with the keys to your data. Your cloud provider can never peek into your information. The problem? This breaks... nearly everything. First of all it means you are responsible for managing the keys, and if you lose them you lose access to your data. Forever. Also, it is extremely difficult – if not impossible – to allow you to see or work with your data in a Web page since the Web server can't read your data either. Thus it works for some kinds of services (mostly file storage/sharing) and not others, and only for sophisticated users who are able to manage their own keys.

As is so often the case, these options reveal the tradeoff between security and convenience.

How to Tell if Your Cloud Provider Can Read Your Data — In two of the three options I listed above, the provider can read your data, but how can you tell for yourself if this is the case?

There are three different (but similar) indications that your cloud data is accessible to your provider:

- If you can see your data in a Web browser after entering only your account password, the odds are extremely high that your provider can read it as well. The only way you could see your data in a Web browser and still have it be hidden from your provider is if the service relied on complex JavaScript code or a Flash/Java/ActiveX control to decrypt and display the data locally.

- If the service offers both Web access and a desktop application, and you can access your data in both with the same account password, odds are high that your provider can read your data. This is because your account password is also probably being used to protect your data (usually your password is used to unlock your encryption key). While your provider could technically architect things so the same password is used in different ways to both encrypt data and allow Web access, that really isn't done.

• If you can access the cloud service via a new device or application using your account user name and password, your provider can probably read your data. This is just another variation of the item above.

This is how I knew Dropbox could read my files long before that story hit the press. Once I saw I could log in and see my files, or view them on my iPad without using a password other than my account password, I knew that my data is encrypted with a key that Dropbox manages. The same goes for the enterprise-focused file sharing service Box (even though it's hard to tell when reading their site). Of course, since Dropbox stores just files, you can apply your own encryption before Dropbox ever sees your data, as I explained last year at Securosis.

And iCloud? With iCloud I have a single user name and password. It offers a rich and well-designed Web interface where I can manage individual e-mail messages, calendar entries, and more. I can register new devices and computers with the same user name and password I use on the Web site. Thus, from the beginning, it was clear Apple had the capability to read my content, just as Ars Technica reported recently.

That doesn't mean Dropbox, iCloud, and similar services are insecure. They generally have extensive controls – both technical and policy restrictions – to keep employees from snooping. But it does mean that such services aren't suitable for all users in all cases, especially businesses or governmental organizations that are contractually or legally obligated to keep certain data private.

Doing It Right — The backup service CrashPlan is an example of a service that offers flexible encryption to fit different user needs, with three separate options. (For more on choosing the appropriate encryption method for CrashPlan, see Joe Kissell's "Take Control of CrashPlan Backups.")

First, by default, your data is encrypted using a key protected by your account password. This still isolates and protects it from other users, while enabling you to view file information through the CrashPlan Web site and the CrashPlan Mobile app. But CrashPlan's employees could still access your data.

Second, if you want more security, you can add a separate backup password that only you know. This approach still allows access through the CrashPlan Web site and the CrashPlan Mobile app, but CrashPlan employees can't see your data except (maybe) during a Web session after you enter your separate password. Attackers can't access your data either, though your password may be susceptible to brute force cracking or social engineering.

Third and finally, you can generate your own per-device encryption keys, which CrashPlan never sees or knows about, rendering your backups readable only by you (or anyone who can beat the key out of you – never underestimate the power of a wrench – props to xkcd!). You could technically use a different encryption key on each device (or share, your choice) so that even if one system were to be compromised, it wouldn't allow access to backups from your other devices. Clearly, this is much more difficult to manage and well beyond the needs or capabilities of the average user (heck, even I don't use it).

So if you want to be certain that your data is safe from both attackers and the cloud provider's employees snooping, look for services that offer additional options for encrypting data, either with a password or an encryption key known only to you. If such an option isn't available at the next cloud service you check out, you'll know that the provider's employees could technically read your data. And when the next big story of a cloud provider reading data hits the headlines, you can smugly inform your friends that you knew it all along.

by Jeff Carlson

Use Dropbox to Troubleshoot Family Macs

The Flashback malware that infected more than half a million Macs creates the kind of situation that's ripe for confusion by friends and family members who aren't technologically savvy. (See "How to Detect and Protect Against Updated Flashback Malware," 5 April 2012.) When news bubbles up to the mainstream media, those of us who help manage these remote Macs often get calls or e-mail messages asking for help.

Apple last week released an update to Java that removes the malware, so anyone who runs Software Update can protect themselves against the threat (see "Apple Releases Flashback Malware Remover," 12 April 2012). But before that update was released, I wanted to check my family members' Macs for infection, something made much easier thanks to Dropbox. Whether you want to share family photos or troubleshooting utilities, the process I describe here makes it easy to distribute files among many Macs, even if they're not all yours.

I wanted to send Marc Zeedar's Test4Flashback application, which could tell immediately whether Flashback has infected a system, to the iMacs owned by my mother and mother-in-law. I'd previously set up Dropbox on both of their systems, and created a "Jeff" folder on each shared with my Dropbox account. Getting the app to their machines was a simple matter of copying it to each shared "Jeff" folder on my Mac. Dropbox then synchronized the file to the "Jeff" folders on their computers (and since I did

this in the middle of the night, I wasn't disrupting either of them – and the program is tiny).

The next day, I called my mother and asked her to run the app; her iMac was not infected. For my mother-in-law's iMac, I connected remotely using a LogMeIn account I'd previously set up and ran the app myself; her iMac was also Flashback free.

Dropbox is ideal for transferring files like this to family members, and better than sending e-mail attachments – which could get caught in e-mail filters – or attempting file transfers via iChat. Here's another example: Instead of directing my mom to Apple's support page to download AirPort Utility 5.6 (the version prior to the current AirPort Utility 6.0, which wasn't recognizing her AirPort Extreme), I downloaded the installer myself and copied it to our shared Dropbox folder.

And since Dropbox offers 2 GB of free storage space, it doesn't cost a thing. In fact, with last week's news that Dropbox was increasing the amount of storage it gives for referrals, you and your friend can both benefit (see "Dropbox Referral Bonuses Doubled to 500 MB, Retroactively," 4 April 2012).

Sometimes, especially when you are troubleshooting, it's easiest to have the tools you need appear magically on the other person's computer so you can get right to solving the problem instead of getting hung up on the particulars of downloading files or utilities. Dropbox excels at this magic, and frequently makes my life easier.

by Tim Sullivan

Rumors and Reality

IPv4 is the system used by the Internet for many years. It is the method by which user connect with other computers via addresses. While we humans use URLs such as http://google.com, the URLs get magically converted to numbers such 195.188.2.1. These numbers can be converted to a 32 bit value.

While not exactly in the same category as THE SKY IS FALLING, the world is running out of Internet addresses.

A new method, IPv6, provides for 128 bit values. This will increase the number of available address. Comcast is already offering IPv6 services to home users in two cities and an official roll out later this month.

All of which brings me to Apple. Apple began offering optional IPv6 service with their Airport Utility.

However, in January of this year, Apple released AirPort Utility 6.0, an updated version of the configuration tool for setting up home networks and AirPort products. With a redesigned interface much like the iOS Airport Utility app, many did not notice support for IPv6 was completely removed.

Apple's AirPort products still support IPv6, but users must download the previous AirPort Utility 5.6 tool to access the settings

Acronym of the day: UDID. It is short for Unique Device Identifier. Every iOS device has one. It's the hardware equivalent to a Social Security Number. You know, that thing you give to all kinds of companies, but don't want anybody else to know. We don't expect the companies to share our personal information.

UDIDs are good things most of the time. They allow for features, conveniences (such as push notifications), or tracking bugs

Because of some lurid publicity that wasn't due to misuse of UDIDs, Apple has changed their policy about third-party apps use of them. Path, a social networking app for the iPhone, was uploading a user's iPhone address book and storing it on its private servers without permission. The key word here is"permission".

Apple told developers to start moving their apps to support the "Core Foundation Universally Unique Identifier" (CFUUID) as a more secure replacement for the UDID. Unfortunately, CFUUIDs are not all that unique. Backup your iPhone and two devices will have the same CFUUIDs.

The search by third-parties for a viable replacement is on. Stay tuned.

This could be important to you: Some time back international hackers ran an online advertising scam to take infect and take control of computers around the world. They set up two servers that made thousands of computers reliant on the rogue servers for their Internet browsing.

The FBI after arresting the hackers replaced the servers with clean ones. But the FBI is not in business to run Internet servers, and these are costing over $1,000 a month to maintain. So on July 9, they are going to pull the plug. For infected home computers the Internet will disappear.

The FBI is encouraging users to visit a website run by its security partner. The site will inform them whether they're infected and explain how to fix the problem. After July 9, infected users won't be able to connect to the Internet.

by Tim Sullivan

May Software Review

by Jeff Carlson

PhotoSync Bridges the Mac/iOS Divide for Images

Now that all of Apple's current iOS devices contain decent cameras, people are shooting and storing hundreds or even thousands of photos on their devices. Getting the images off an iPad, iPhone, or iPod touch, though, can be tricky.

Should you import everything into iPhoto or another photo management application? That works when your device is connected via a sync cable, but with Wi-Fi syncing enabled it may be rare to plug directly into the computer. And regardless, it's fussy to have to plug in every time you want to transfer a photo.

Maybe the key is to use iCloud's Photo Stream feature to push images to your various devices and computers automatically? Photo Stream is a great feature, but it gives you little control over which images are shared.

There's also the question of moving images in the other direction: What if you want to copy photos to an iPad, but the computer to which the iPad normally syncs isn't available?

What's needed is a utility that transfers images back and forth between a Mac and an iOS device, with little hassle. For the last several months, as I've worked on several projects that have required a lot of iPad imagery, I've saved a huge amount of time by using PhotoSync, a $1.99 iOS app that works hand-in-hand with a free Mac client.

The Screenshots that Litter the Stream — I may be unusual in this respect, but my iOS devices are jammed full of screenshots. Granted, I write about technology for a living; I recently finished one iPad book ("The iPad for Photographers"); and I'm wrapping up another ("The iPad Pocket Guide, Third Edition"). So, I'm capturing a lot of screens. But I also need to get those images from my iPhone and iPad to my Mac, with as little friction as possible. I'm sure that there are plenty of people in similar situations with other types of images.

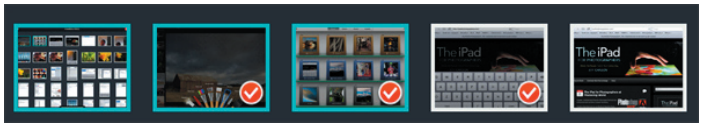
I thought iCloud's Photo Stream would be the answer, and it almost is. Any image saved to the Camera Roll – which is where screenshots end up – is automatically added to the Photo Stream. Within a few seconds or minutes, that image appears on other devices where Photo Stream is enabled. The copying happens automatically in the background.

But once the file is magically transported to my Mac, like Mike Teavee zooming along the ceiling as millions of colorful atoms, it's still trapped within iPhoto or Aperture. (Fortunately, unlike the TV-obsessed tyke from "Charlie and the Chocolate Factory," the image doesn't arrive downsized.) I still need to export it out of the application, which is a non-starter for an efficient workflow.

In the past, I would connect the iPad to my Mac using the sync cable, and then fire up the Image Capture application included with OS X. With that approach, I could copy selected files to a folder in the Finder, bypassing iPhoto entirely. This still works, but isn't as convenient as PhotoSync.

Instead, here's what I do with PhotoSync. After taking some screenshots (by pressing the Home button and the Sleep button at the same time), I launch the PhotoSync app, which displays the contents of the Camera Roll. (You also can navigate to any album on the device.) Images that have not been synced appear outlined in light blue.

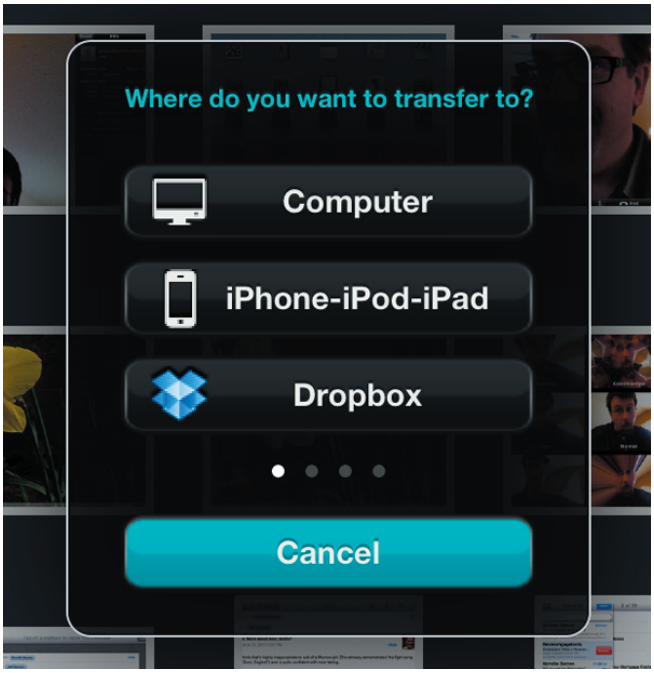
I select the photos I want to sync by tapping them, which adds a red checkmark icon. Sometimes it can be difficult to tell from thumbnails alone which images I want to sync, so PhotoSync also offers a Quicklook mode (tap the eyeball button) to view each photo full screen. In that case, the checkmark button appears in the lower-right corner for me to tap to select the image.



(Here's a tip: Double-tap a thumbnail to enter PhotoSync's range selection mode, and then tap another thumbnail: all images between those two are selected. You can do the same by double-tapping a selected image to deselect a range.)

When I'm ready to transfer the files, I tap the red Sync button in the top-right corner of the screen. This brings up the Select Action popover, providing the option to Sync New, Sync Selected, or Sync All images. I can also mark everything as synced, or switch to the Receive Photos/Videos mode (which I'll explain shortly).

Next, the app asks where the files should go. In my case, I want the files sent directly to my Mac, so I tap Computer. (To make this work, I had previously installed the free PhotoSync Companion utility on my Mac. A Windows version is also available.) After I tap the name of my Mac, the files transfer via Wi-Fi and appear in the Finder. The PhotoSync Companion preferences let you specify where the files end up, either a Finder folder or imported directly into iPhoto or Aperture.



PhotoSync automatically creates its own folder hierarchy, which includes the name of the device and the album from which the images come. It would be nice if PhotoSync would dump anything I transfer into a single folder, but since I often need to massage image files anyway (cropping or converting to a different format for print, for example), having the images appear in a Finder window is good enough.

I also discovered a shortcut that streamlines that process even more, and that quickly became my favorite feature. In PhotoSync's settings, I set a Quick Transfer destination (the same folder on my Mac, in this case) so all I have to do is touch and hold the red Sync button to transfer any new images – no other taps or dialogs required.

That's my setup in my little office ecosystem. But what if my Mac isn't nearby?

PhotoSync can also tie into a Dropbox account, so any photo you transfer appears on all machines on which you've set up Dropbox. You also end up with a backup on the Dropbox servers. If you're traveling and have good Internet access, syncing photos to Dropbox is a great way to make backups of your photos in case your device is lost or broken.

I've also found myself occasionally using PhotoSync's Wi-Fi-based iPhone-iPod-iPad option to transfer photos I capture with my iPhone 4S directly to my iPad, where I prefer to review and edit them. (This is similar to the Beam feature in Apple's new iPhoto app.)

A swipe of the Select Action popover reveals a host of other photo-sharing options: Flickr, FTP/SFTP, Google+/Picasa, FaceBook, SmugMug, iDisk, WebDAV, Zenfolio, and Box.

Mac to iPad — So far I've described my particular setup, which is great if you're a technology writer who generates a lot of screenshots. But another great feature in PhotoSync pushes pixels in the other direction, sending images from the Mac to the iPad.

Although I used this feature a few times to move a few demo photos from my Mac to my iPad, consider this situation, which a friend recently asked about on Twitter: His visiting mother wanted photos of the grandkids on her iPad so she could view them and take them home. The problem was that her iPad syncs to her computer, which was in another city.

The way iOS syncing works, a device can be paired with just one computer. So, my friend couldn't simply plug her iPad into his Mac and specify that some of his images be added to her photo library; iTunes would want to replace her data with his.

PhotoSync bypasses all that. Instead, PhotoSync can act as a small Web server that accepts files and adds them to the iPad's Camera Roll. Here's how it works:

1. With PhotoSync open on the iPad, tap the red Sync button on the iPad and choose Receive Photos/Videos.

2. On the Mac, open a Web browser and point it at the address specified at the bottom of the iPad's screen (such as http://10.0.1.11:8080). You're given a Web-based view of the iPad's entire photo library. (Steps 3—7 all take place on the Mac.)

3. Click the Upload button.

4. Choose one of the iPad's albums (or create a new one), or use the default Camera Roll.

5. Select an album as the destination, and then click the Select button.

6. Click the Choose File button to locate the image you want to send. Or, in Safari, you can also drag a file onto the album name pop-up menu.

7. Click the Submit button to transfer the file.

8. On the iPad, tap the Done button when you're finished.

Of course, this approach isn't the only one my friend could have taken. He could have sent the photos to his mother via e-mail, but photos are large and could run into message size limits. And even then, extracting numerous photos from e-mail messages is awkward. Or, he could have stored the photos in a Dropbox folder and shared that folder with his mother, who could then have viewed the photos in the Dropbox app on the iPad and saved them individually to the Camera Roll. However, with PhotoSync he can install the app on his mother's iPad and transfer the files directly. When she returns home, she can easily import the photos into iPhoto, because the pictures of the grandkids are in the iPad's Camera Roll.

I'm always in favor of tools that save time and avoid drudgery, but I was surprised at just how helpful PhotoSync has been with my projects. If you need to transfer images in any capacity between a computer and an iPad, iPhone, or iPod touch (or all of the above), PhotoSync is far more valuable than the $1.99 it costs.

Apple Updates

HP Printer Drivers v.2.9 OS X
April 26, 2012 - 524.8 MB

System Requirements
— OS X 10.6 or later
— OS X Lion

This download includes the latest HP printing and scanning software for OS X Lion and OS X v10.6 Snow Leopard.

Samsung Printer Drivers v2.4 for OS X
April 26, 2012 - 28.9 MB

System Requirements
— OS X 10.6 or later
— OS X Lion

This download includes the latest Samsung printing and scanning software for OS X Lion and OS X 10.6 Snow Leopard.

Flashback malware removal tool
April 13, 2012 - 557 KB

System Requirements
— OS X Lion without Java installed

This update removes the most common variants of the Flashback malware. This update contains the same malware removal tool as Java for OS X 2012-003.

If the Flashback malware is found, a dialog will be presented notifying the user that malware was removed.

In some cases, the Flashback malware removal tool may need to restart your computer in order to completely remove the Flashback malware.

This update is recommended for all OS X Lion users without Java installed.

Java for OS X Lion 2012-003
April 12, 2012 - 67.3 MB

System Requirements
— OS X 10.7

This Java security update removes the most common variants of the Flashback malware.

This update also configures the Java web plug-in to disable the automatic execution of Java applets. Users may re-enable automatic execution of Java applets using the Java Preferences application. If the Java web plug-in detects that no applets have been run for an extended period of time it will again disable Java applets.

Java for OS X Lion 2012-003 delivers Java SE 6 version 1.6.0_31 and supersedes all previous versions of Java for OS X Lion.

This update is recommended for all Mac users with Java installed.

Java for OS X 10.6 Update 8
April 12, 2012 - 79.9 MB

System Requirements
— Mac OS X 10.6.8

This Java security update removes the most common variants of the Flashback malware.

If you do not use Java applets, it is recommended that you disable the Java web plug-in in your web browser. For more information about how to disable Java in Safari, please see this website: http://support.apple.com/kb/HT5241.

Java for OS X 10.6 Update 8 delivers Java SE 6 version 1.6.0_31 and supersedes all previous versions of Java for OS X 10.6.

This update is recommended for all OS X 10.6 users.

Digital Camera RAW Compatibility Update 3.12
April 05, 2012 - 8 MB

System Requirements
— OS X 10.6.8
— OS X Lion 10.7 or later

This update adds RAW image compatibility for the following camera to Aperture 3 and iPhoto '11

• Canon EOS 5D Mark III

by Christopher Breen

Mac 911

Skirting auto-login in Lion

Reader Ross Anderson wishes to occasionally sidestep a startup preference setting. He writes:

I've configured my Mac running OS X Lion to automatically login to a particular user account. But there are times when I want to instead login to a different account. Is there some way to do that?

To give our readers some context, you can configure your Mac so that it automatically logs into a particular account. To do that, launch System Preferences, select the Security & Privacy preference, click the Lock icon and enter your administrator's name and password to unlock the preference, and in the General tab make sure the Disable Automatic Login option is unchecked.

If you're currently logged into an account, the easiest way to get to the login screen is to choose Log Out accountname from the Apple menu (where accountname is the name of the account you're currently logged into). Confirm that you want to do this by clicking on the Log Out button that appears in the resulting window. You'll be logged out of that account and taken to the login screen where you can choose to log in to a different account.

If you simply want to work in another account without logging out of another, it's easy. Go to the Users & Groups system preference, unlock that preference in the same way as you did with Security & Privacy, click Login Options at the bottom of the list of users, and in the area to the right be sure that Show Fast User Switching Menu As is enabled. Now when you want to switch accounts, just choose an account name from the menu bar and you'll be prompted for that account's password. Enter it and you'll switch to that account.

Getting to the login screen when starting your Mac is a tougher proposition. If you press and hold the Shift key at startup before you hear the startup chime you'll eventually be presented with the login screen, but you'll do so via Safe Boot mode. Not only does it take a couple of extra minutes to start up your Mac (because, as part of the Safe Boot process, the Mac attempts to repair any problems it can find), but after you finally log into the account you want, you'll find that your login items have been disabled (hence the "Safe" part of "Safe Boot").

In the old days you could hold Shift after the Apple logo appeared to skirt auto login. I've tried that on my MacBook Pro running the latest version of Lion and it doesn't work.

Because this is a less than ideal way to go about the problem, I'd suggest planning ahead when you can. If you know that you'll want to boot into a different account after your next shutdown, return to the Security & Privacy system preference and enable that Disable Automatic Login option. When you next boot or restart your Mac, you'll be taken to the login screen.

Understanding Apple TV, mirroring, and aspect ratio

Reader Tim Rosenthal is confounded by the relationship between his new iPad and equally new Apple TV. He writes:

I have a new iPad and the just-released Apple TV. Seems like with the resolution the iPad is putting out, I should be able to get 16:9 1080p mirroring from the Apple TV to my television, yet that isn't happening.

Although the new iPad has a load more pixels that the previous model, the display's native 4:3 aspect ratio hasn't changed. So when you pull up the multi-tasking bar, swipe to the right until you see the iPad's play controls, tap on the AirPlay icon, and choose your Apple TV as the destination, it projects to your Apple TV that aspect ratio. This is no different with the second-generation Apple TV.

"Bummer!" you say? You must not be an iPad developer. Imagine having to rework the interface of every app to accommodate 16:9.

That takes care of the interface and the vast majority of your iPad's apps. However, there are exceptions. If you have 16:9 movies or TV shows on your iPad–and that can be either 1080p or 720p video–it will appear on the TV in all its widescreen glory, showing black bars at the top and bottom of the TV. Supported streaming video will also appear in 16:9. Some apps also support 16:9 projection – Firemint's Real Racing 2 HD, for example.

More questions about questionable Apple TV behavior? See my Troubleshooting Your Apple TV article.

Tweaking Lion's firewall

Back in the days of Tiger and Leopard, you had more fine-tuned control of your firewall. With Lion, you can add applications to the "allowed" list and have their network connections pass through the firewall. However, what if I want to manually add a TCP or UDP port?

As you've noticed, OS X's firewall, while potentially powerful, doesn't provide you with a lot of configuration options. This was done so that typical users wouldn't do The Bad Thing and make their Macs nearly unusable because of an ill-tweaked firewall.

But as I say, it's potentially powerful. The trick is getting to the settings you need. Terminal is certainly one avenue but why bother when there's Hanynet's donate-what-you-can-afford-please IceFloor? Like its revered siblings, WaterRoof and NoobProof (which you'd use for earlier versions of the Mac OS), it provides a graphic user interface to OS X's firewall.

In its primary window you find simple on/off options for select services including screen sharing, VPN, iTunes sharing, and ftp file transfer. But if you click on the Advanced Options button you'll reveal an Advanced Options window where you can add custom TCP and UDP ports. You can additionally create a whitelist and blacklist of IP addresses to always allow or always block traffic from particular addresses. If you want to dig even deeper click the Advanced Filtering button in this window and let your geek flag fly.

[Macworld Senior Editor Christopher Breen is the author of "Secrets of the iPod and iTunes (6th edition)," and "The iPod and iTunes Pocket Guide (4th edition)" both from Peachpit Press

and

"OS X 10.5 Leopard Essential Training (video)" from lynda.com Find Chris' books at www.amazon.com and www.peachpit.com. Get special user group pricing on Macworld Magazine! Subscribe today at http:// www.macworld.com/useroffer

Computer Repair

Caller : Hi, our printer is not working.

Customer Service: What is wrong with it?

Caller : The mouse is jammed.

Customer Service: Mouse? ... Printers don't have a mouse!!!

Caller : Mmmmm? Oh really? I will send a picture.

No animals were harmed. The mouse was safely removed and released.

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
310 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral meetings are **usually** held at 6:30 p.m. on the 3rd Tuesday of the month at Giant Foods, Trindle & 32nd, Camp Hill