



Bits & BYTES

WAYNE PALMER

JPEG format: Killing image files bit by bit

When you press the shutter button on your digital camera, an amazing amount of information is processed in a matter of seconds. Keep in mind; a digital camera is a small hand held computer set up to perform certain tasks. Just like your computer, it understands only bits and bytes — that's 0's and 1's for the layman.

Instead of a piece of film, a digital camera records the light gathered through the lens on to a CCD or CMOS chip. This is the equivalent of light hitting film.

These chips consist of rows and rows of tiny little microscopic sensors. Each one of these sensors records the amount of light that hits it and passes it along to the camera's processor, which then converts it into the bits and bytes that can be read by a computer.

To make this process even more complex, the sensors technically see black and white only, not color. Tiny little red, green and blue filters are placed in patterns over the sensors. The camera does a complex mathematical process, called demosaicing, to determine what the color is. The processor creates three different layers, red, green and blue, tripling the initial capture.

It is through the interrelationship of the three layers that allows for the creation of 65 million colors in 8 bit color mode. For example, if you have a 6 megapixel camera, it will create an 18 megabyte file, with each layer of color being 6 megabytes.

In addition, your camera then further processes the file based upon camera settings, adding color adjustments like white balance and sharpening. Finally, the file is saved to the camera's storage card. Again this all takes place in a matter of seconds.

After all this processing has been done, most cameras have saved the file in a format called JPEG, an acronym for the Joint Photographic Experts Group who developed the file format.

This format reduces the amount of information by abbreviating repetitious data and even eliminating small amounts of data through a process called compression.

If you have ever worked with a ZIP file, it is the same idea, only JPEG is for photographs.

Here's how it works. Your image is made up of rows and rows of little blocks called pixels, an abbreviation for picture elements. The compression process divides the pixels into groups of eight. The group is analyzed and the strongest colors in the group are kept, while any stray colors are deleted and replaced with one of the dominant colors.

An image with lots of blue sky will compress much more

highly than a picture of a field of multicolored wildflowers. The more similarities there are in the image, the greater the compression that can take place. This is why not all the file sizes are the same.

On the surface, JPEG is great since it allows us to make small files from large files. So a 6MB camera instead of being forced to store an 18MB file can compress the file to 3MB or less.

This allows you to record many more images on your camera card, but ultimately your file is paying a price in the amount of details it maintains. Some of the information that originally was in the file is deleted.

The amount of JPEG compression is variable. A high amount of compression creates a very small file and consequently deletes more information. A low amount of compression creates a larger file and ultimately you may see no difference between a file that has been compressed and one that hasn't. Camera manufacturers use a high quality compression scheme in the recording of your images.

With all this being said, the JPEG file format is not an ideal file format for saving images you edit. Opening and closing the file is not editing.

An edit is changing the file in any way, which can include lightening or darkening, cropping, or even rotating the image.

Every time you resave a file in the JPEG format, the image is compressed again. With enough resaving of the file in JPEG, you can eventually degrade the file to the point that it becomes a blocky mess.

If you value the integrity of your files, and want to maintain as much detail as possible, never resave an original file in the JPEG format.

Save the file in a format that does not recompress the image. Most photo-editing programs create their own proprietary format, so instead use the TIFF file format. TIFF is fairly universal and can be read on almost all computer platforms.

Remember that using this format will save the file in its original size, which is three times the camera's mega pixel capture.

Of course, this will require much more storage space on your hard drive.

Keep in mind JPEG is a compromise between image quality and file size. It is a great way to reduce a file's size, but there is a price paid in the amount of details removed from the image.

The first time an image is compressed, the effect may be negligible, but future compressions by resaving the file in the JPEG format may eventually ruin the image.

Experience Works plans classes

Experience Works will hold courses in Personal Computing, Introduction to Microsoft Word, and Introduction to Microsoft Excel beginning Monday and ending May 1 at its offices at 140 W. Fourth St.

Classes will be held Mondays and Wednesdays. The Introduction to Excel course will run 1 p.m. to 3 p.m.; the Personal Computing course will run 3 p.m. to 5 p.m.; and the Introduction to Word course will run 5:30 p.m. to 7:30 p.m.

Anyone in the community can enroll, regardless of age. Those interested should call 321-5811 or stop by Experience Works' office at 140 West Third Street in Williamsport.

Each 16-hour course is \$45 and can be completed in four weeks. Experience Works is a nonprofit organization.

Vigilante patching

Third parties fixing Explorer security faster than Microsoft

By ALLISON LINN
AP Business Writer

SEATTLE — When Microsoft Corp. researchers learned recently that a software flaw had been made public and could prompt Internet attacks, the company ordered a team to devote all its time to fixing the flaw and making the repair work with other products.

Microsoft argues that's the approach customers want and expect, but some security experts complained that the software company's traditional method, which could take days or weeks, wouldn't help people fast enough.

So for the second time in three months, outside programmers took matters into their own hands by quickly releasing their own fixes, days ahead of the official Microsoft patch for its market-dominant Internet Explorer browser.

Microsoft doesn't endorse such third-party fixes, warning it can't vouch for whether they will work smoothly with Microsoft products and other applications. But those providing them argue they have a responsibility to protect users from attacks.

"It's kind of like having the cure and not sharing it with anybody," said Marc Maiffret, chief hacking officer with eEye Digital Security Inc. of Aliso Viejo, Calif., which earlier this week released such a fix.

Rather than replacing Microsoft's own patch, Maiffret says he is hoping to provide a bandage for the interim.

The security expert also doesn't fault Microsoft for taking time to finalize an official patch because it can be difficult to make sure that repairing one part of the complex Windows operating system, which includes Internet Explorer, doesn't cause problems elsewhere.

He also realizes that a patch like this can cause any of the thousands of non-Microsoft applications running on Windows machines to stop working, crippling businesses and frustrating home users.

But Maiffret argues that Microsoft should be the one providing the type of temporary treatment his company was able to quickly pull together in response to what the industry refers to as "zero-day" problems — vulnerabilities that attackers can immediately use to try to infiltrate other people's computers.

Johannes Ullrich, chief technology officer with the security research organization SANS Institute, also recognizes that Microsoft needs time to build patches but believes the company can more quickly



ASSOCIATED PRESS

Marc Maiffret, chief hacking officer with eEye Digital Security Inc., says outside programmers have a responsibility to provide security patches for popular Microsoft products when they can.

release a "beta" patch so users would have temporary — if not perfect — protection in the interim.

"The real problem is that Microsoft leaves that opening," Ullrich said.

Such problems are relatively rare. In most cases, Microsoft learns about flaws in its systems confidentially from security experts, who hold off on making their findings public — and alerting potential attackers — until Microsoft can release an official patch.

But occasionally, reports of a vulnerability leak out before Microsoft has time to build a fix, creating a dangerous situation in which attackers can take advantage of the flaw while users have little protection.

When Microsoft faced such a problem a few months ago, SANS recommended that users download the third-party fix because of the unusual severity of the threat. This time, Ullrich said the flaw appears to be less worrisome, so SANS is recommending that people either disable part of Internet Explorer or temporarily use an alternative browser, such as Firefox or Opera.

Microsoft says it is hoping to release a patch for the most recent IE flaw by April 11, its normal time of month for issuing security updates, and sooner if possible.

In the meantime, Stephen Toulouse, a program manager with Microsoft's Security Response Center, said the company is working with other security companies to help guard against attacks, and helping to shut down the Web sites that exploit the flaw.

Toulouse said the company also is trying to find ways to create and test its patches faster — for instance, by conduct-

ing tests in tandem rather than one after another.

But Microsoft, he said, cannot risk releasing a patch that causes problems for even a small number of users because people may decide not to use the fix at all if they hear it's problematic.

"The huge responsibility we have is that we have to answer to our customers, and our customers represent potentially hundreds of millions of different configurations," Toulouse said.

Third-party fixes also create the potential for a malicious person to release a pretend fix that is really an attack, much like the occasional e-mail falsely attributed to Microsoft and others, masking as legitimate communications but really luring users to malicious Web sites.

Even well-meaning programmers have the potential to wreak havoc on businesses if their unofficial fix has even a minor problem, said John Pescatore with research firm Gartner.

"The analogy I use is, if the FDA was testing an anticancer drug, and your neighbor said, 'I have an anticancer drug,' would you use it?" Pescatore said, referring to the Food and Drug Administration.

Meanwhile, Microsoft will likely have to keep grappling with this problem, despite all the security improvements the company has made in the past few years. It takes only a few programming mistakes to expose Windows users to attacks.

"Even if they're doing everything right," Maiffret said, "there's going to be four to five mistakes a year, and those four to five mistakes are going to lead to the same things you're seeing now."

Internet Archive's value, legality debated in copyright suit

By JOE MANDAK
Associated Press Writer

PHILADELPHIA — An ongoing lawsuit between a company and a popular archive of Web pages raises questions about whether the archive unavoidably violates copyright laws while providing a valuable service, according to attorneys and an independent law expert.

The nonprofit Internet Archive was created in 1996 to preserve Web pages that will eventually be deleted or changed. More than 55 billion pages are stored there.

A health care company claims the archive didn't do enough to protect copyrighted information that helped a competing firm win a trademark suit.

The archive "is just like a big vacuum cleaner, sucking up information and making it available" to anyone with a Web browser, said Scott S. Christie, an attorney representing Healthcare Advocates Inc.

"That has some social value, but in doing so they are grabbing information that they're not entitled to," he said. "More importantly, they are telling people that they will take it off the shelf if you do a certain thing a certain way — but that didn't happen in this case."

Carnegie Mellon University computer science professor Michael Shamos, an expert in Internet law, said archiving like that done by the Internet Archive is "the biggest copyright infringement in the world," but said it is done in a way "that almost nobody cares about."

Shamos said Web site pub-

lishers typically don't mind that their sites wind up on the Internet Archive, because the whole point of posting Web sites is to get as many people as possible to see them. The rub is that a Webmaster loses control over the site, because the Internet Archive keeps that information on the Web even after the page is dismantled, Shamos said.

Copyrights are only effective if the holder is vigilant about maintaining control of the material, Shamos said.

"That's the thing about rights, you have to exercise them. If Pamela Anderson wants to trespass on my front lawn, it's OK with me," Shamos said.

The plaintiff in the lawsuit, filed in U.S. District Court in Philadelphia last year, wasn't OK with how a competitor's attorneys used their archived Web site.

In 2003, Healthcare Advocates Inc. filed a lawsuit claiming a similarly named firm stole its trade secrets from copyrighted brochures.

The defendant's law firm used the Internet Archive to access old versions of the Healthcare Advocates Web site. The law firm won the suit after it showed some of the contested information wasn't secret at all because it had been spelled out on Healthcare Advocates' Web site.

Healthcare Advocates then sued the Internet Archive. It alleged the San Francisco-based archive failed to protect that information after Healthcare Advocates asked the archive how it could restrict access to certain files.

Stefani Shanberg, an attorney for the Internet Archive, said Web page owners can ask

that information be removed from the archive and can keep the archives from grabbing it in the first place.

"We voluntarily inform Web site owners that they can voluntarily restrict access to their material," Shanberg said. "The archive shouldn't have been dragged into this (lawsuit) in the first place."

Federal copyright laws have exceptions designed to protect search engines and online archives from such lawsuits. And Shamos said that copyrights aren't violated when

attorneys are digging for the information in defense of a lawsuit

"The needs of discovery in litigation trump the copyright. You're making one copy for use in court," Shamos said.

But Christie said the archive didn't do enough to protect Healthcare Advocates' Web pages from prying eyes.

"I think Internet Archive does a fine job. I think they're a valuable public resource," Christie said. "I just take issue with the way they perform their public service."

INTERNET
NEW HIGH SPEED
DSL
FREE Static IP Address - Business or Residential
EVENLINK 570-601-0770

Discover the DIRECTV Difference.
Better entertainment more value.™

Guild's TV Sales and Service
1350 W. 4th St., Williamsport • 322-3385
An Authorized DIRECTV Dealer

Hardware and programming sold separately. DIRECTV, the Curves Design Logo and DIRECTV THE ENTERTAINMENT DIFFERENCE are trademarks of DIRECTV, Inc. and are used with permission.