Founded 1982
www.rcsi.org

The Rochester Computer Society, Inc.
a computer/tech club open to everyone

MONITOR

Vol. 36, No. 02 February 2018

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415

The RCSI '**Monitor**' newsletter can be found in most public libraries in Monroe County. *Free* copies can also be found in the following computer stores: Microworx, Just Solutions, TSC Electronics, and Pod Computers. Digital copies may be obtained from **www.rcsi.org** or my cloud storage at **http://tinyurl.com/tonydel-rcsi-newsletters/**.

Some Past Presentations:

Open Source and Free Software
Protecting Your Identity
Keeping Mobile Devices Secure
3D Printing, ENABLE project
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Close up Photography

Member of apcug An International Association of Technology & Computer User Groups

Tues, Feb 13,
'Your Smartphone is Like a Swiss Army Knife',
by Bill James,
Computer Club of Oklahoma City

Tues, March 13, 'The Linux Software Store',
by John Kennedy ("Free-John"),
East-Central Ohio Technology Users Club

In This Issue

Can You Beat the Bots?	David Kretchmar
Is Mobile Broadband More Secure than Wi-Fi?	Ask Leo!
Google, the World's Biggest Advertising Company, Will Block Ads Soon. Is That Good?	Justin Pot
Associations – We need them!	Phil Sorrentino
High-Tech Remembering	Greg Skalka
Meet the many members of the Arduino family	Dick Maybach
California company gets FCC approval for at-a-distance device charging	Ethan Baron
Scrap the stethoscope	Syl Kacapyr

Kretchmar's Korner

Can You Beat the Bots?

By David Kretchmar, Computer Hardware Technician,
Sun City Summerlin Computer Club, NV

When tickets for a musical I wanted to see (Book of Mormon) went on sale at the Smith Center's website, I immediately went on line to buy tickets. I was surprised to learn that only a few scattered seats remained, even though tickets had only been on sale for a few hours. Yet ticket scalpers had plenty of seats available - for double or triple their original selling price.

When the play returned to the Smith Center last year I went on online the minute as soon as tickets were available (12:00 A.M.) and I could score

Special Interest Group

Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. www.interlockroc.org

Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). Bring your system in so we can help you get the most out of it. Hope to see you there.

Free, online
Virtual Technology Conferences,
presented by APCUG

Check back, next month
for the 2018
conference dates

---

4 tickets for great seats (about 5th row center orchestra) at a reasonable price, but I noticed many good seats had already been sold. How could this be, I wondered?

The answer is, of course, Bots; they are software robots that enter multiple orders, sometimes many thousands of times instantly, for scarce items. Often popular items such as show, and sporting event tickets, popular electronics, and hot children's toys are the target of Bots.

Since the dawn of the Internet, scalpers have been using shopping Bots to scoop up online ticket sales within seconds of their being offered. They then sell the tickets for huge markups. Often shoppers will place orders and tickets will disappear from their virtual shopping carts before they can check out.

Congress acted to stop ticket scalping by passing the Better Online Ticket Sales Act of 2016 AKA the Bots Act of 2016, but the new regulations apply only to event tickets. The popular East Village and then Broadway play Hamilton is credited with helping to precipitate the legislation. The Broadway show sold out more than a year in advance, and $200 face value tickets were going for $800, shutting out even members of Congress.

This holiday season Shopping Bots will again be used to snatch up hot toys and electronics as soon as they become available online. Then they will only be available on sites such as eBay, or maybe Craig's list where they will be sold at inflated prices. But if your grandchild just must have the latest incarnation of a certain toy (remember "Tickle Me Elmo" a few years ago), the outrageous price will often be paid rather than having to deal with a very disappointed kid.

Many vendors have attempted to limit the power of shopping Bots with software programs, with limited success so far. Vendors identify Bots by their Internet IP address, but Bots have learned to disguise these. Bots can also pay in a variety of ways to obscure the fact they are Bots. In this cat and mouse game of vendors vs. Bots the Bots have usually eventually been successful.

Some vendors are having some success addressing the issue. Adidas, the sports shoe manufacturer, has initiated a new program called Confirmed. This App lets a buyer reserve and pay for shoes online, then pick them up in person at a retailer (you go brick and mortar!). You might have noticed some online sellers require potential buyers to put an item in their virtual shopping cart before the price is revealed. This is partially designed to prevent shopping Bots from zeroing in on a good price and blocking out retail buyers.

You can do some things to prevent Bots from stealing your successful online buying experience. Learn what the suggested retail price of an item is before you shop, and don't pay any more. The biggest way to defeat scalpers is to shop early. And good luck with that toy.

From the November 2017 issue, Gigabyte Gazette, http://www.scscc.club, tomburt89134@cox.net.

RCSI Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com
Treas: Dennis P. McMahon
. 235-1260
denmac733@gmail.com
Secretary: www.rcsi.org
Help's Half Hour . . Jan Rothfuss

Board Members at Large

Bob Avery 385-4491
webmaster@rcsi.org, 9/20
Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/19
Tony Dellelo 734-6149
tonydel@techie.com, 9/18

Standing Committees

Linux SIG: . . . Carl Schmidtmann
unixgeek@faultline.com
Programs: . . . . . Tony Dellelo
Webmaster: . . . . . Bob Avery
Membership: . . . . . Steve Staub
Monitor editor: . . . . . Tony Dellelo

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, at St. John's Meadows, Briarwood building.

Newsletter Printing

The newsletter was printed at St John's/Chestnut Court by the printing group, with the help of Don Wilder (computer and printer operator). *We will try and print on the 1st or 2nd* ***Thursday morning,*** *following the monthly meeting.*

Ask Leo !
By Leo Notenboom, https://askleo.com/
Making Technology Work For Everyone

Is Mobile Broadband More Secure than Wi-Fi?

Mobile broadband is a popular Internet connection alternative. As with any connection, it's important to understand the security ramifications and tradeoffs.

//

I recently upgraded my mobile phone and can now connect it to my laptop to get Internet access almost anywhere. The salesperson said it will be more secure to use, even in places that offer Wi-Fi. Is it more secure?

Yes, but.

By and large, data connectivity through the cellular network is more secure than open Wi-Fi.

That's not a reflection of some inherent security difference in the technology, but more a reflection of just how ubiquitous and *in*secure open Wi-Fi really is.

The risks of open Wi-Fi

From a security point of view, the difference is simply this: anyone with a Wi-Fi enabled computer has what they need to be a hacker. There's no special equipment needed, and the software required is free, open source, and easily available for download. It's even aboveboard, as there are many legitimate uses for what's called "packet sniffing" software.

The result is that anyone can use almost any laptop within range of an open Wi-Fi hotspot and sniff the traffic.
It's easy. That's why I have a full article on the ways to use an open Wi-Fi hotspot safely. And, indeed, one of the ways to be safe is to not use it at all, and use a mobile broadband connection instead.

The risks of mobile broadband

With mobile systems, such as your phone, the situation isn't nearly as simple. Here, hackers need special equipment to start sniffing, and need to be able to decrypt the data as it is encrypted.

Neither of those are particularly difficult obstacles to overcome. I'm sure the hardware needed is available on the Internet (isn't everything?). As it turns out, the encryption isn't particularly secure either, having been developed many years ago when mobile phones didn't have the computational horsepower necessary for today's more secure alternatives.

In other words, it takes some extra steps and expenses to start hacking the mobile network, but it's possible. However, given the ubiquity of open Wi-Fi, the fact that you don't need special equipment, and the general lack of security employed by most people using the hotspot, the open Wi-Fi scenario is simply a much bigger, easier target to go after.

What if they're after ME?

Now if you, specifically, are being targeted — say as part of some corporate espionage — perhaps it's worth it for the

hacker to invest in that additional technology. In that case, you're better off with a wired connection, avoiding the airwaves completely. (Though, even then, depending on how lucrative a target you are, you could still be at risk.) But if you're an average user, a mobile device coupled with a firewall and generally good internet behavior on your part, gets you all the security you typically need.

Costs

I mentioned costs above, and there are several trade-offs to be aware of.

- You're paying extra for that monthly data plan on your mobile device. You could, instead, pay perhaps even less to a VPN to be secure in those open Wi-Fi hotspots. This would actually be more secure than either Wi-Fi alone or mobile broadband, and you could even use the service over your mobile connection should you feel the need.
- You may pay a price in speed. My experience is that mobile broadband is almost always slower than Wi-Fi. Granted, that depends on your mobile carrier and coverage, compared to how strong an Internet connection the Wi-Fi access point is connected to and how many other people are using it at the same time you do.
- You may pay a price in location. With Wi-Fi, you need to locate a hotspot you're allowed to use. Yep, it seems like they're everywhere, and more seem to be appearing every day. With mobile broadband, however, as long as you're in range of a tower, you have connectivity.

Finally, lest you think that plugging into a wall socket for hardwired ethernet connectivity is the safest of all, let me remind you that Wired connections can be as dangerous as Wi-Fi . Often overlooked, wired connections (particularly in public venues such as hotels) share almost all the risks of open Wi-Fi hotspots.

***** End of article *****

Computer Recycling

Some Residential Drop off Locations: **Call first**, to find out what is accepted, especially for 'tube type' tvs or monitors.

Sunnking (we rule electronics recycling), 585-637-8365, 4 Owens Road, Brockport, **some other drop off locations:**

Mirecycle, 49 Stone Street, Rochester, 585-224-4040
Goodwill Industries of the Fingerlakes;
Rochester – 451 South Clinton Ave
1518 West Ridge Road
376 Jefferson Road
885 Long Pond Road
Webster – 1217 Bay Road
50 Webster Commons Blvd
Fairport – 1200 Fairport Road
7450 Pittsford-Palmyra Road
Victor – 2 Commerce Drive
Honeoye Falls – 201 West Main St
Macedon – 1635 North Wilson Rd
Brockport – 1807 Nathaniel Poole Trail

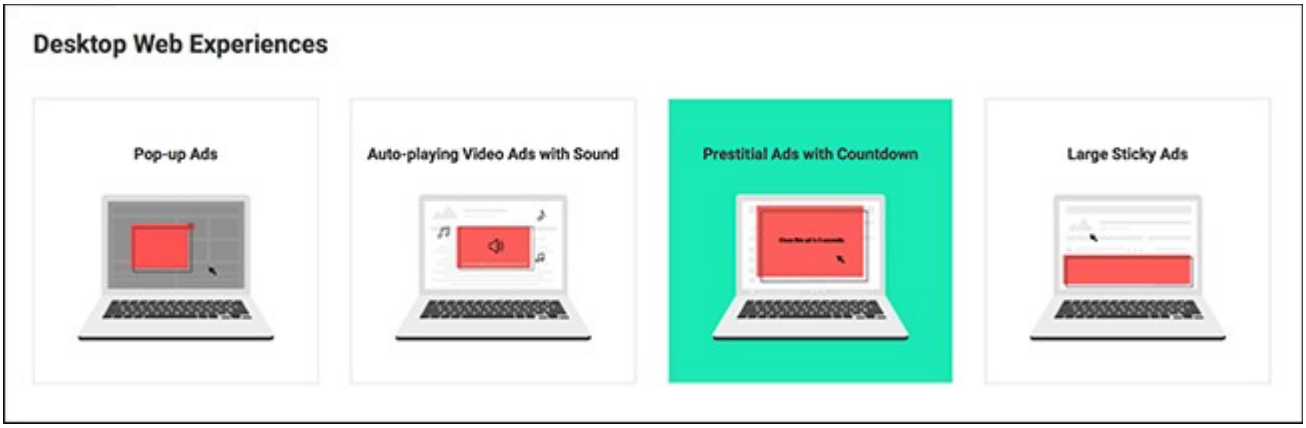
Google, the World's Biggest Advertising Company, Will Block Ads Soon. Is That Good?

by Justin Pot

It's finally happening: on February 15, 2018, Google's Chrome browser will block some ads out-of-the-box, regardless of whether you have a separate ad blocker installed. That means Google, the web's biggest advertising company, will start deciding which ads do and don't get blocked in your browser. Should users be happy about this, or apprehensive about what Google is up to?

Something Like This Was Necessary

Google isn't blocking *all* ads: just the ones on sites that "misbehave." In the blog post announcing the change, Google stated they will block all ads on sites with a certain amount of ads that violate standards from the Coalition for Better Ads. The Coalition includes tech companies like Google, Microsoft, and Facebook, alongside media organizations including The Washington Post and Reuters. Together, they've built a list of ad types they consider unacceptable. Anyone who uses the web regularly should recognize the culprits: popups, auto-playing video ads with sound, and others will be blocked:



All of these ads are terrible, and the mobile incarnations are arguably even worse: These kinds of ads make browsing the web miserable, and we'd all be better off if they went away. But it's unlikely that publishers would make this decision unilaterally: such ads pay well, and that extra money is hard to resist for media organizations already struggling to get by.

So Google has decided to force the issue.

As of February 15, Chrome's desktop and mobile versions will block *all* ads on any site that uses these sorts of advertisements. It's hard to overstate how devastating this will be for sites that are blocked: Chrome is used by over 60 percent of desktop and mobile users. Publishers have had almost a year to make sure their site fits the standard, and this is some serious motivation for them to do so.

It's easy to see the upside of this development. You, as a user, will be able to browse the web without seeing these horrible ads—either sites will get rid of them, or they'll be blocked. Without some kind of intervention, these sorts of ads would only become even more common, making the Internet worse for everyone. But there's also a potential downside. Google, the world's biggest advertising company, will block ads to control behavior on sites they don't own. Whatever you think about Google, that's a lot of power.

This Isn't Entirely Unprecedented

This isn't the first time something like this has happened. Major tech companies have always changed browsers in order to shape the web in their image, and the results have often been positive. Apple, for example, famously didn't support Flash on the iPhone, a decision that arguably gave us the HTML5 powered Internet we all enjoy today. Early pop up blockers, bundled in Mozilla Firefox and Internet Explorer, undoubtedly hurt revenue for media organizations in the early 2000s, but they also made the web a lot less stressful to use (popups are a lot less common now than they were back then). More recently, High Sierra's tracking prevention deletes cookies regularly to reduce online tracking.

Google has also acted in similar ways in the past. Chrome already blocks automatic audio ads, for example, and has disabled Flash by default for a while now. It's easy to see Chrome's upcoming ad blocker as similar to all of these changes: a simple tweak they can make in order to improve the web for users. But that's not the only reason Google is doing it.

The Market Force Awakens

Google gives a lot of things away. Chrome and Android, for example, are freely available for anyone who wants them. But Google isn't a charity. Whatever blog posts and press releases say, everything Google does is motivated by the bottom line, a trait they share with every other for-profit company. Google's software is insanely popular, but they don't make money. Google has basically one revenue stream: their near total dominance of online advertising.

Ad blocking software like Adblock Plus and uBlock Origin has threatened that revenue. Every user who installs an ad blocker is a user that's not making money for Google, and ad blocking has become much more common in no small part because the ads on websites have become so annoying. By punishing sites that use these terrible ads, Google likely hopes to stem the tide of users installing ad blockers. And Chrome's dominance gives Google this power.

Should Google Be Trusted With This Power?

Google is setting a precedent with this change. Now, Google will decide which sites do and do not get revenue from Chrome users. Instead of blocking only these specific ads, Chrome will block *all* ads on any offending site. The specific reason for this may be beneficial for consumers in the short term, but what's to stop Google from abusing this power later?

The recent Amazon/Google feud over streaming set-top boxes shows Google is willing to leverage dominant platforms in order to settle scores with other technology companies—even if consumers are hurt in the process. The upcoming ad blocker in Chrome gives Google the ability to cripple the revenue of any online rival, instantly. Is it far fetched to believe they might use that power in some future feud?

It may sound alarmist, but it's worth thinking about. Something like this was necessary. These ads needed to be stopped. But whatever you think about Google, this means Google has even more power to shape the web in their image. How you feel about that depends on how much you trust Google's old motto: "don't be evil".

Article was taken from the www.howtogeek.com website.

* * * * * SOFTWARE and HARDWARE * * * * *

Associations – We need them!

By Phil Sorrentino, Contributing Writer
The Computer Club, Florida

Although "guilt by association" may lead you to an incorrect logical conclusion (refer to Association Fallacy in Wikipedia), your computer, without associations, would not be able to make any sense out of any of the files that you use. "What?" you say, why my computer always makes perfectly good sense out of all of my files. I can read all of my documents, even the most complicated spreadsheets, all of my pictures are just picture perfect, my music always sounds beautiful, and my videos are entertaining and enjoyable to watch. Well, that is because you probably have your Associations set properly.

The Association we are talking about here is the Association between a Software Application (App), and a file type on your specific computer. (Remember the file type is shown by the characters after the "." in the file name. For example, the file type of the file name "aletter.doc" is "doc".) Yes, Associations are specific to a computer and are probably different on other computers, though many of the basic Associations that we typically have set up are probably the same on most other computers. For instance, most of us probably have Word associated with .doc and .docx files, and Excel associated with .xls and .xlsx files. (In Windows 10, if you are not seeing the file type as part of the file name, start File Explorer and in the View tab, check the "File name extensions" box.)

The file type is really a description of how to interpret all of the data that is held within the file. (It defines in great detail just what every bit and byte in the file means.) And this is where Files and Applications come together, or where they become "associated". File Association links a file type with an Application. An Application knows how to handle a particular file type because of the file type definition. Fortunately, we, the users, don't have to know anything about the details of the file type, only that a particular file type can be used with a particular Application. So, if a correct association is made, the Application will handle the file in the expected fashion. If an incorrect association is made, the results will be undetermined and possibly problematic.

So, where do we find these Associations? I thought you'd never ask. To see them, just go to the Control Panel (Right-click the Start button, and select Control Panel, or type "Control Panel" on the taskbar.) Make sure "View by" is set to small or large Icons, rather than "Category". Next select Default Programs, and then select "Associate a file type or protocol with a program". (Yes, here they refer to an Application as a Program. Application, App, and Program are synonymous.) This selection will cause the Control Panel App to search the computer and create an alphanumeric list of all of the file types that it finds on your computer. (Have patience, it may take a few minutes if

you have an older computer or if you have an extremely large number of file types.) Once it is finished you will see the list of file types in three columns; Name, Description, and Current Default. Keep in mind that a specific program may handle more than one file type, as indicated by the multiple instances of a program name in the "Current Default" column. (Note that this screen uses the term "Extensions" for what we are calling the "file type". This is just another name for the part of the file name after the ".")

You can select a file type with a left click and all three columns will be highlighted for that file type. Try it for one in the list that has a program you recognize in the Current Default column, like "Movies & TV", or "Groove Music". Notice that once you have selected a file type, the "Change program…" button on the right side above the outline box of the file types can be used. This button will allow you to change the program that is associated with the file type that you selected. If you click the "Change program…" button you will see a screen that will show you the currently associated program (under "keep using this App", and a list of other possible programs (under "Other Apps") that can be associated with this file type. This is a list of other programs that are known, to the Operating System, to be able to handle the file type in question. (Other Apps could be selected by selecting "More Apps", at the bottom of the list, and then choosing one in the extended list, but these programs are less likely to be able to handle the selected file type in an expected fashion. Selecting any of these programs could produce undesirable results, so be careful if you make any of these associations.)

To change the association, just select one of the programs in the smaller "Other Options" list and select "Ok". After a few seconds, the newly selected program will be shown in the "Current Default" column for the selected file type, and the name of the newly associated program along with its icon will be shown above the outline box of the file types, on the left side. Now the newly associated program will be used to handle the file type that was selected. That's all there is to changing the association. Keep in mind there may be many programs that can handle a given file type, but be aware that although the new program may work, it may not work the way you would expect. In this situation, it is true that "the devil is in the details". Programs may work in general the same, but may be very different in some specific details, and may not produce a desirable outcome. Don't be afraid to try any of the programs in the shorter "Other Options" list because you will always be able to easily change back to the original program if need be. Now that you are armed with this knowledge you can inspect the associations of the file types of interest, possibly change them, and also see if any new program has hijacked the file types you regularly use. Knowledge is Power.

From The Journal of The Computer Club, Inc., http://scccomputerclub.org / Philsorr.wordpress.com, philsorr@yahoo.com.

President's Corner

High-Tech Remembering

By Greg Skalka, President
Under the Computer Hood User Group, CA

As we get older, our human memory seems to fail us. For some of us, this seems to start at a relatively early age, while others have good recall into our twilight years. Sometimes we have a greater problem retaining short-term memories, like what we had for dinner the night before or where we left our car keys, but can recall in detail events of many decades ago. Most of us just slowly start forgetting things. Of course, a blow to the head or a stroke can degrade even the best of memories.

Our technology today is filled with memories of various kinds - volatile and non-volatile, fast and slow, large and small capacity. The SDRAM (synchronous dynamic random access memory) used for the main storage in most computers and smartphones is the ultimate in short-term memory. If power is removed, all the information stored in it quickly fades away. Flash memory (for small capacity applications) and magnetic media like hard drives (for large capacity) are non-volatile, and can retain their stored data for long periods of time without power. All of these memory types can suffer losses of data due to electrical, magnetic and cosmic ray abuse, and do also degrade over time just from normal use.

In these respects, the memories in our tech devices suffer from the same issues as our human, brain-based memories. Just as with our brains, semiconductor and magnetic memories lose their ability to reliably store information over time. Abuse to these memory devices, through actions like static discharge, extremes in temperature or mechanical shock (to a hard drive) can cause permanent damage, as a concussion or stroke does to a brain.

One means of information loss in our tech memories that does not really have an equivalent in the brain is in deletion. Information in semiconductor memories or hard drives can be deleted or overwritten. We humans don't really have a way to intentionally delete or forget information (this might be convenient for lost loves or humiliating experiences), though trauma may cause memories to be repressed or unconsciously blocked. In theory, therapy may be able to recover repressed memories in humans. In theory, there are also techniques that may be effective in recovering deleted files in semiconductor and magnetic memories.

Deleting a file from your computer (stored on a hard drive, or in semiconductor memory device like a flash drive or memory card) does not initially eliminate the data file, but instead removes the file's location from the computer's file system. In Windows, the deleted file goes into the recycle bin, from which it can be easily recovered. Even if the recycle bin is emptied, the file's data remains in the storage media until it is overwritten. Special software tools (data recovery software) can often recover these deleted files from hard drives, USB flash drives and memory cards. I recently had need of such software, as I accidentally deleted photos and videos from the memory card in my smartphone.

When my wife and I went on vacation to Nebraska to view the total solar eclipse on 8/21/17, I left my Windows laptop at home and instead traveled with my smaller and lighter Chromebook. For its main job, it was well suited - accessing the internet and viewing web pages while on travel. It was less capable at its secondary task, copying photo and video files from the many cameras we took with us to a mass storage.

With four still and four video digital cameras being packed for this trip, I did not want to bring the multiple memory cards for each camera that would be necessary to hold all the files we would generate over the week we would be traveling. On past trips, I'd simply copied the contents of the memory cards from the cameras to the hard drive in my laptop, and then erased the cards for reuse. Since the Chromebook has no large internal storage, I planned to use it to copy my photos and videos to an external USB hard drive I brought.

I practiced copying these files before we left, and this all worked well for the files on my digital still cameras and digital video cameras. For some cameras, I removed the SD memory card and used the Chromebook's SD card reader. For others, I accessed the camera memory through a cable between the camera and the Chromebook's USB port. I also copied the photos and videos from the memory card in my smartphone, also through a USB cable. Since I had switched the micro SD card in my phone to be a 128 GB card the day before we left, I was in no risk of filling it up and really did not need to copy from it, but I did it anyway to be consistent. This later proved to be a big mistake on my part.

I am very familiar with the Windows file manager, but not so much with the file manager in the Chrome OS. While copying the folders of photos and videos from my Samsung Galaxy J3 Prime, an Android-based smartphone, to the external USB hard drive late one night in our hotel room, I got an error message that some files did not copy. I should have stopped right there and then, but haste and late nights make waste. I decided to delete those incompletely copied folders from the hard drive and try again, but due to my lack of familiarity with the Chrome OS file manager, I accidentally deleted the photo folders on my smartphone instead.

In the panic of the realization of what I had just done, I doubled down on my error and immediately copied those folders back from my external drive to the smartphone memory card. After reviewing the photos now on the smartphone, I found many photos and videos, including all I had taken in the last few days on the trip, were missing.

Fortunately, I finally stopped and calmly took stock of my situation. I had deleted all the photos from my smartphone, but fortunately I had backups of all but for the last few prior days of my trip. The photos taken with my smartphone were mainly just supplementals; most of my photography was done with my digital cameras. There were only a few cases where I had lost unique photos not duplicated by my cameras, amounting to perhaps several dozen files. If those missing smartphone photos were lost forever, it would not be the end of the world for me, but I would still like to get them back. If I stopped further photography with my smartphone, I could try to recover the missing files when I returned home. Unfortunately, I had already copied back to the memory card the files I did have on the external drive, and so may have already overwritten some files, and thus lost them forever.

When I returned home, I started looking for a solution to my deleted file problem. A web search turned up many software options for file recovery from memory cards. There were a few programs that were free, but many were not. I then recalled a program I had seen demonstrated at one of the Southwest User Group Conferences. I believe it was Terry Currier of the WINNERS group (WINdows usERS) that gave the presentation, and one program he recommended and demonstrated was Recuva. I decided to make this attempt with something I had seen, rather than an unknown.

Recuva is produced by Piriform (www.piriform.com), the same company that makes Ccleaner. Recuva comes in a

free version, as well as a Pro version for $19.99 (both as downloads). My recollection was that Terry used the free version, so I downloaded it and installed it on my Windows 7 laptop. To make things as simple as possible for Recuva, I removed the micro SD card from my phone and put it in an SD adapter I could plug into my laptop's memory card reader, rather than connect through a USB cable on the phone.

When Recuva starts, it uses a wizard to simplify the process, though you can easily skip it. Being relatively unfamiliar with the program, I used the wizard, which asks just a few simple questions of the user. The first wizard screen asks you to select the type of files you are trying to recover. Since it would not allow the selection of multiple types (pictures and video), I selected "all files". In the next screen, I specified the location of the SD memory card (drive letter). The final screen had a start button, which initiates the search for deleted files. It also has a check box for "deep scan", which I skipped initially.

The first pass took only a few minutes and found 32 files. I selected them all to be copied to a folder on an external hard drive. I examined the folder and found the files recovered were all JPEG photos, almost all from before my trip, and none of the ones I really wanted.

I ran through the wizard a second time, this time with the deep scan selected. It took about two hours, but this time Recuva found 351 files. I had it save them all to a second hard drive folder. There were a lot of files that I already had from back-ups, but there were also the JPEG and MP4 files that I was looking for. It appears that Recuva was able to recover all of the missing files that I could remember.

It will take me a while to sort through them and remove the duplicates, but between the back-ups and what Recuva recovered, I believe I did not lose a single file in my accident. Now I can view those photos and videos and relive those moments. I'll be more careful in deleting files with my Chromebook in the future, and I'm sure glad Recuva works so well and is there when I'm not so careful. I sure wish there was a Recuva program for the human memory.

From the October 2017 issue, Drive Light, www.uchug.org, president@uchug.org.

Meet the many members of the Arduino family

By Dick Maybach, Member
Brookdale Computer Users' Group, NJ

The Arduino is a controller rather than a complete computer like the Raspberry Pi (which I'll discuss next month); it's much simpler and getting started with it is far easier. It has no operating system and runs only one program at a time, which starts when the unit is powered and runs until power is removed.

To start you need only to connect it to a PC's USB port, which provides power, control, and information exchange. As a controller, its strength lies in its ability to control and to collect data from external devices. Thus, using an Arduino invariably involves external circuits and devices. These can be as simple as switches and LEDs or as complex as robots and drones.

There are several Arduino models. You should probably begin with the Uno, the most used and most robust in the family. The Mega and Zero have higher performance and more input/output termArduino-1inals for more complex projects. The Gemma and the Lily pads are smaller and designed to be incorporated into garments. The MKR1000 includes WIFI and is designed to Internet of Things (IoT) projects. There are also dozens of expansion boards, called shields, to add functions to all the models.

The Arduino provides a very easy way to get started with computer hardware technology and software. You work in your native computer environment – Windows, macOS, or Linux.

The Arduino comes complete; you have only to connect it to your PC with a USB cable, which provides both communication and power. The supporting software, the Arduino Integrated Development Environment (IDE), is free; just download and run it.

The first experiment (a "Hello World" program) requires nothing except the Arduino board, a USB cable, and the IDE. You can have it running in just a few minutes.

To go further, you will need some basic electronic parts (switches, LEDs, and sensors), a prototyping board, and some jumpers. Many vendors sell inexpensive kits with these parts and instructions for experiments using them.

The components plug directly into the prototyping board, where the jumpers connect them to each other and to the Arduino ports. No soldering is needed.

At some point, you may wish to add expansion boards (called shields in the Arduino community), and some of

these do require soldering. This is not difficult, as learning kits with the tools, practice material, and instruction are available, and it's a skill you will find useful if you progress beyond a few basic experiments.

Figure 1 shows a naked Arduino (that is one without an attached shield) connected to a PC and running the program of Figure 2.

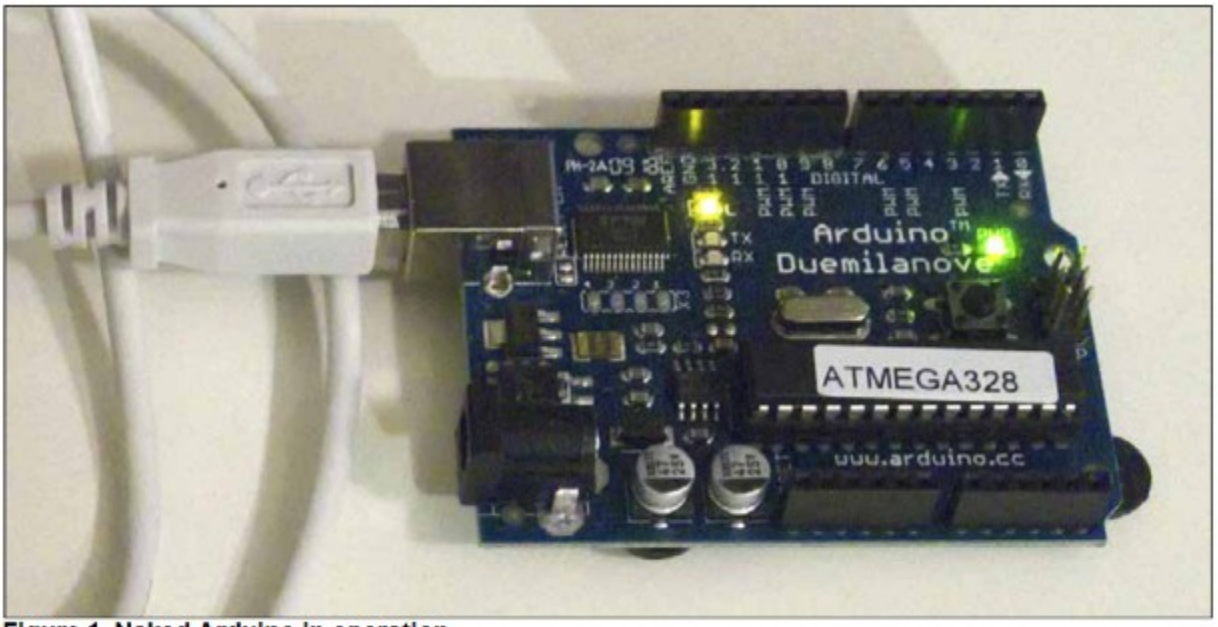


Figure 1. Naked Arduino in operation.

The green LED is a power indicator and the yellowish LED is the one controlled by the program. You can also see the black terminal strips that contain the analog and digital input and output pins to which the shields connect. Once you've loaded the program, you can disconnect the board from your PC.

The program will then start as soon as you power the board, either through the USB port as shown or the black power connector at the bottom-left.

Figure 2 shows the Arduino IDE window on a PC; it's available for Windows, macOS, and Linux. It also shows the Arduino version of "Hello World," the first program you write when learning a new language. Arduino's native language is a simplified form of C++, and

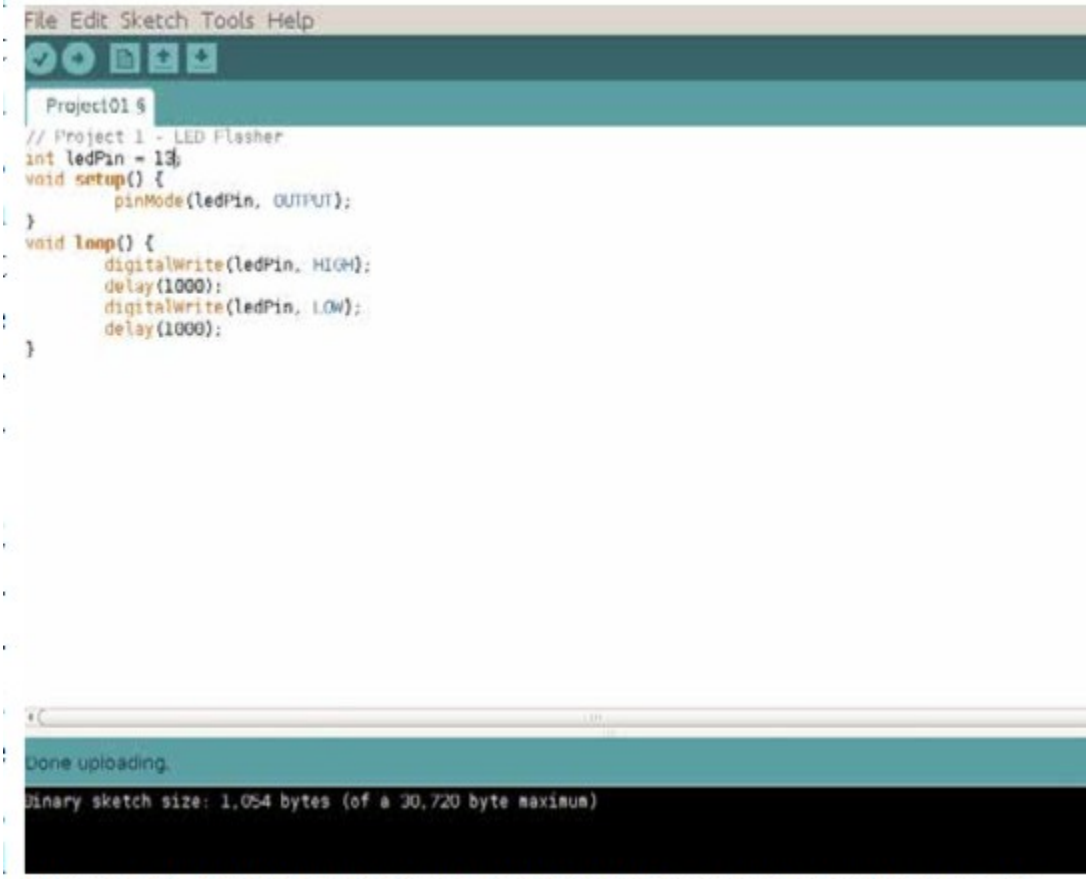


Figure 2. Arduino Integrated Development Environment.

in this program, it just turns on an LED for one second, off for one second, and repeats forever. The first line is a comment, and the next three set up the hardware so that pin 13, which is connected to the LED, will be controlled as a digital output.

The section beginning with "void loop ()" is the program. It moves the pin-13 Voltage high, waits 1000 milliseconds, moves it low, waits 1000 milliseconds, and repeats. Although it looks quite simple, this exercise is far from trivial, as it shows that your naked Arduino is working properly, that its IDE is installed and configured correctly, and that you can program it. If your next project misbehaves, you have only to check its code to find the error.

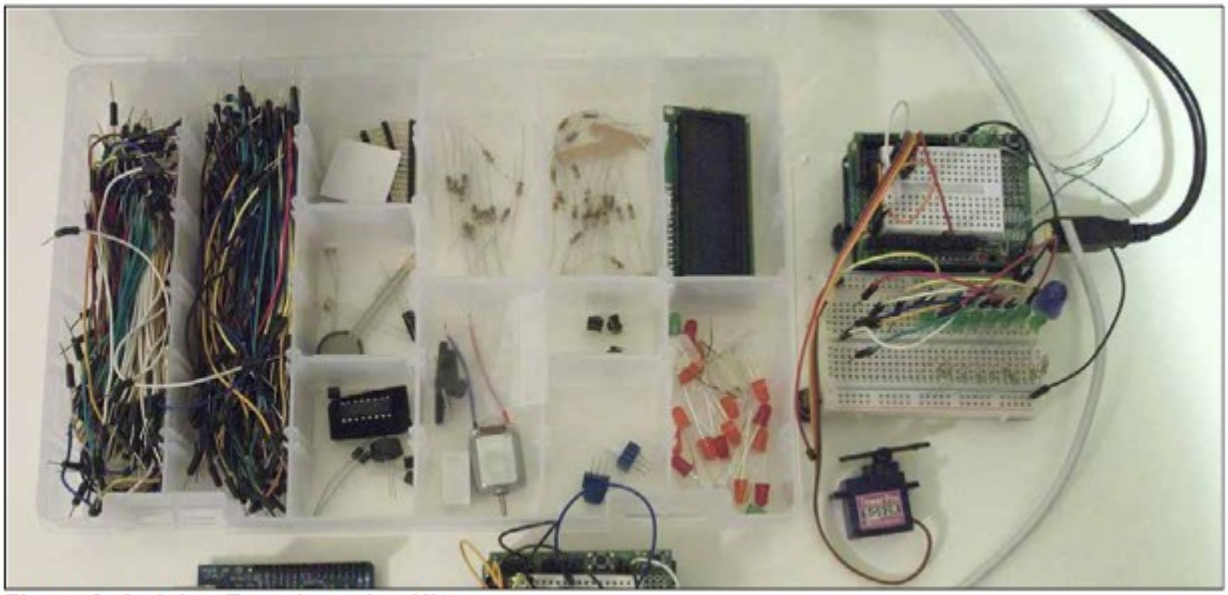


Figure 3. Arduino Experimenting Kit.

Figure 3 shows the Arduino kit I've assembled over several years. At bottom-left is a naked Arduino; this is a complete controller with its one LED and one push-button, with which you can run very simple experiments. At bottom-center is an Arduino with a small prototype board (called a "shield" in Arduino-speak). You plug components and wires into the white board to create simple circuits and connect them to the controller. The compartmented case holds my collection of wires and components (LEDs, switches, sensors, a motor, a servo, and a LCD display. Finally, on the right is another Arduino with a prototype shield and a larger prototype board for more complex circuits.

Arduino and a white prototype board make it easy to get started in electronics. The components don't require soldering, but just plug into the board. Everything is controlled by the processor, which you can monitor using the IDE. The input devices (e.g., switches and light and temperature sensors) and output devices (e.g., LEDs and motors) are visually observable without instruments. (Although you may wish to purchase a cheap multi-meter to check voltages and resistor values, as modern resistors are tiny and their values indicated by even tinier color bands.)

Arduino's strength lies in its relative simplicity. You work entirely from your own PC, which means you are in a familiar environment and can concentrate on the programming and the hardware. Most people will start with Arduino, a prototype shield, and a parts kit, available from several suppliers. Typically, the circuits in published projects are shown pictorially, as in Figure 4, rather than as schematics. As a result, you can assemble them without knowing how to read schematic diagrams.

Most project descriptions will have a paint-by-the-numbers nature. You connect components and jumpers according to the pictorial, paste the code into the IDE, and see what it does. If you do nothing else, you will have learned little. You can learn much more by experimenting with the code and the circuit after you have it working. For example, if the project is a blinking LED, change the code to make it blink faster or slower or with different on and off times.

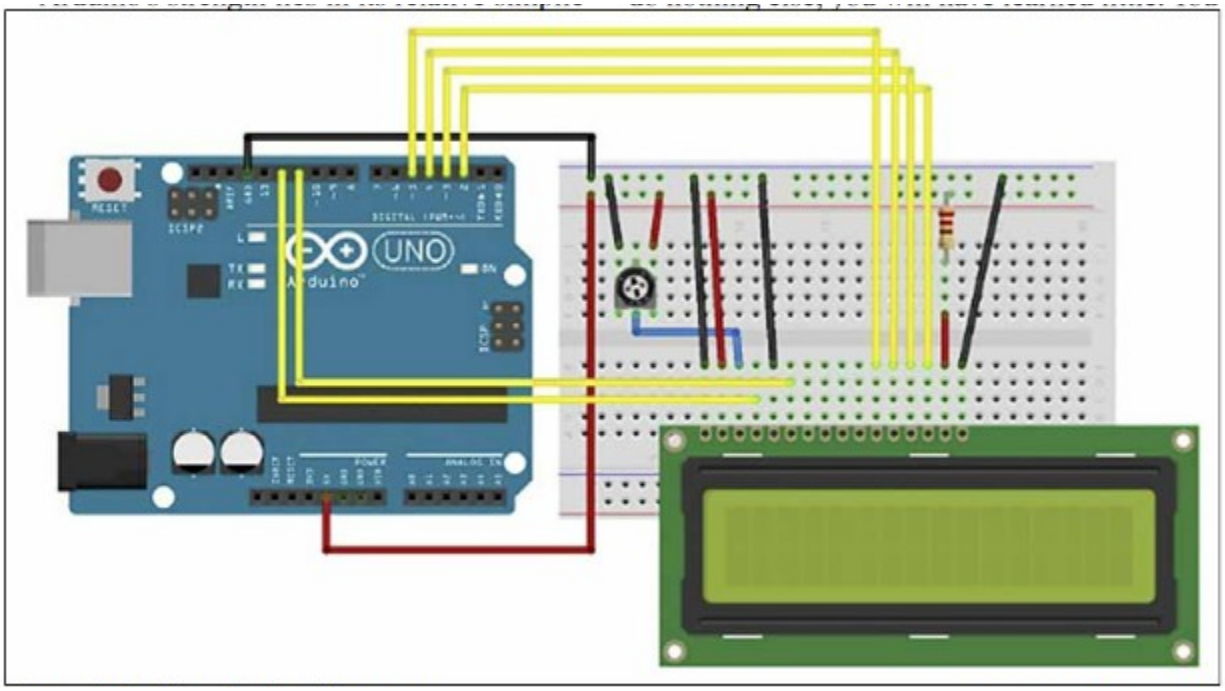


Figure 4. Arduino Project Diagram

Because most Arduino projects include circuitry, you will be learning about electronics as you progress. The prototype boards mean you can assemble the circuits without soldering and can make changes rapidly. Since most of the complexity is handled by software, the circuits are usually quite simple, and this is typical of modern electronics. Open the case of a modern device and compare it to one made years ago, and you will be struck by how much simpler the modern one is, despite its far more complex functions. This means that young people working with Arduinos are preparing themselves for successful careers in electronics.

The Arduino home Website, http://www.arduino.cc/, is where you go to download the IDE, learn about the different versions of the processor, obtain tutorials, and purchase devices and kits.

You will see two product lines, Arduino and Genuino. The development team split and formed two different companies. They have recently resolved their disagreement, and the two product lines will most likely merge. (There are also several clones, but I prefer to purchase Arduino products to support its continued development.)

Many electronics vendors supply Arduino products, accessories, kits, and tutorial material. Three prominent ones are Ad fruit, http://www.adafruit.com/, Spark Fun, http://www.sparkfun.com/, and Element 14, http://www.element14.com/community/groups/arduino. A search for "Arduino" will show you many more. If you prefer to see before you buy, check your local RadioShack, although not all stores will have a good inventory. When you tire of watching blinking LEDs, check the Instructables Website, http://www.instructables.com/id/Arduino-Projects/, for more complex projects. Arduino is popular enough that your local Barnes & Noble probably has several books on it, making getting started easy.

From the August 2017 issue, BUG Bytes, www.bcug.com, n2nd@att.net.

Tidbits of probably useless information

There are 18 different animal shapes in the Animal Crackers cookie zoo.

Should there be a crash, Prince Charles and Prince William never travel on the same airplane as a precaution.

In Tokyo, a bicycle is faster than a car for most trips of less than 50 minutes.

The Mona Lisa has no eyebrows. It was the fashion in Renaissance Florence to shave them off.

There is one slot machine in Las Vegas for every eight inhabitants.

California company gets FCC approval for at-a-distance device charging

December 29, 2017 by Ethan Baron
The Mercury News

Energous, a San Jose, Calif., company, is the first firm to receive federal approval for a wireless charging system purported to power devices from up to 15 feet away, the company said.

The Federal Communications Commission certified the company's "WattUp Mid Field transmitter," which uses radio frequency energy to deliver power from the transmitter to a multitude of device types, Energous said. "The certification marks a significant milestone for the consumer electronics industry and paves the way for future wireless charging ubiquity for nearly any small electronic device, including smartphones, tablets, fitness trackers, smart watches, earbuds, wireless keyboards and mice, smart speakers and more," Energous said.

Energous' system is different from the "resonant induction" technology behind the Pi wireless-charging system, and provides a longer range than chargers from Belkin and Mophie that require contact with a device, Engadget reported, adding that devices to be charged must be equipped with a receiver.

WattUp isn't ready for retail yet, but Energous will demonstrate the system at the Consumer Electronics Show in Las Vegas in January, Engadget reported.

This article was reported in phys.org (Dec 29, 2017). For more information on this charging system: energous.com/technology/transmitters/.

Scrap the stethoscope: engineers create new way to measure vital signs with radio waves

Materials provided by **Cornell University**. Original written by Syl Kacapyr

Date: December 14, 2017 Source: Cornell University

Summary:

Engineers have demonstrated a method for gathering blood pressure, heart rate and breath rate using a cheap and covert system of radio-frequency signals and microchip 'tags,' similar to the anti-theft tags department stores place on clothing and electronics.

A radio frequency identification tag.
Credit: Cornell University

No visit to the doctor's office is complete without a blood-pressure cuff squeezing your arm and a cold stethoscope placed on your chest. But what if your vital signs could be gathered, without contact, as you sit in the waiting room or the comfort of your own home?

Cornell University engineers have demonstrated a method for gathering blood pressure, heart rate and breath rate using a cheap and covert system of radio-frequency signals and microchip "tags," similar to the anti-theft tags department stores place on clothing and electronics.

The cracker-sized tags measure mechanical motion by emitting radio waves that bounce off the body and internal organs, and are then detected by an electronic reader that gathers the data from a location elsewhere in the room.

The system works like radar, according to Edwin Kan, professor of electrical and computer engineering. But unlike most radar systems that rely solely on radio waves to measure movement, Kan's system integrates "near-field coherent sensing," which is better at directing electromagnetic signals into body tissue, allowing the tags to measure internal body movement such as a heart as it beats or blood as it pulses under the skin.

The tags are powered by electromagnetic energy supplied by a central reader, and because each tag has a unique identification code it transmits with its signal, Kan said up to 200 people can be monitored simultaneously using just one central reader.

"If this is an emergency room, everybody that comes in can wear these tags or can simply put tags in their front pockets, and everybody's vital signs can be monitored at the same time. I'll know exactly which person each of the vital signs belongs to," said Kan.

The idea originated after Kan and his graduate student, Xiaonan Hui, visited the Center for Sleep Medicine at Weill Cornell Medicine and NewYork-Presbyterian, where measuring vital signs can interrupt sleep patterns. "We were thinking about the kind of technology we were already using in our lab and thought we could probably get a signal from those vital signs," said Hui. "But after we figured out the theory and did the experiments, the signal quality was better than our prediction."

The signal is as accurate as an electrocardiogram or a blood-pressure cuff, according to Kan, who said he believes the technology could also be used to measure bowel movement, eye movement and many other internal mechanical motions produced by the body.

Kan and Hui plan to do more extensive testing with Dr. Ana Krieger, medical director of the Center for Sleep Medicine and associate professor of clinical medicine, of medicine in clinical neurology and of clinical genetic medicine at Weill Cornell Medicine. They're also working with professor Jintu Fan and associate professor Huiju Park from Cornell's Department of Fiber Science and Apparel Design, who have demonstrated a way to embroider the tags directly onto clothing using fibers coated with nanoparticles.

Hui envisions a future in which clothing can monitor health in real time, with little or no effort required by the user. "For every garment in our daily use, there could be a tag on them, and your cellphone will read your vital signs and will tell you some kind of information about your condition that day," said Hui.

The system is detailed in the paper "Monitoring Vital Signs Over Multiplexed Radio by Near-Field Coherent Sensing," which was published in the journal *Nature Electronics*.

Editor's note: article was taken from the www.sciencedaily.com website.