Founded 1982
www.rcsi.org

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

MONITOR

Vol. 35, No. 7 July 2017

"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
Mobile Payments
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

Tuesday, July 11
Movie & Video Night
with popcorn

Tuesday, August 8, Annual Picnic, at
Henrietta Town Park, Robinson Cabin

In This Issue

President's Corner

Where to Get Tech Today

By Greg Skalka, President
Under the Computer Hood UG, CA

It seems we have more and more technology available in the products we buy. Almost everything is getting networked these days, and the categories of products where electronics now play a major part continue to increase. This has expanded the number of places to get tech far beyond the traditional sources of a decade ago. A lot of stores that used to be the traditional sources for computers and technology have gone away, while a lot more shopping for the devices we need is done online.

It seems you can't swing an HDMI cable in practically any room in the

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
Saturdays from 1-5 pm, on

May 6, 2017
August 19, 2017
November 4, 2017

---

typical house these days (including the garage and often the back yard) without hitting something containing electronics. Never mind the TVs, computers, game systems, tablets and phones - electronics and connectivity have worked their way into almost every device and appliance you see. Practically every kitchen appliance has the strong possibility of being connected to the Internet, controlled by a timer or digitally enhanced. Refrigerators, microwaves, stoves and dishwashers are now loaded with tech. Even the lowly meat thermometer has gone digital.

Digital thermostats keep the house temperature comfortable while saving energy. Wi-Fi reaches into every corner of the house and even out onto the patio, through repeaters and extenders. Voice-operated assistants like Amazon's Echo and Google's Home Assistant provide information and control anywhere your voice can be heard. Lights, camera, action - home control and alarm systems control lights and appliances, allow remote monitoring and signal when security has been breached. Even the laundry room gets into the act with efficient washers and dryers with sophisticated features. With so much electronics in a modern automobile, you might have as many processors in your garage as in the rest of the house.

With all this technology spread throughout the items in your home, practically every store has had to become a technology store. Home improvement stores like Home Depot and Lowe's are now much more than lumber yards; since they sell so many smart appliances and smart home devices, their employees have to know more than just nails and screws. The trick is getting good tech advice from all those diverse stores that now sell smart stuff. You can expect the Sprint, Verizon and ATT stores to have tech-savvy employees, but what about Walmart, Target, Costco, Ace Hardware and O'Reilly Auto Parts?

Ghosts of Tech Stores Past

A few decades ago, there were specific places to go to get high tech items, places like RadioShack, CompUSA and Fry's Electronics. There used to be lots of small independent computer stores in San Diego, mostly in the Kearny Mesa area. Maybe it was the decline of the computer, the rise of tech in everything or competition from the Internet, but many of those tech stores are long gone, and the ones remaining are struggling.

Many RadioShack stores have closed, and most of the remaining stores are branded as "Sprint" stores. Remember CompUSA, Circuit City and Incredible Universe? All of those chains couldn't make it and closed down. Best Buy and Fry's Electronics have managed to survive, but are having to work hard to compete with online retailers and all the big box stores selling electronics. Apple and Microsoft have established their own stores, but only in very limited markets.

The real battle in tech retailing is probably in online sales versus brick and mortar stores. Amazon not only sells technology, but with their Kindle e-readers and tablets, Echo / Dot / Tap assistants and their warehouse automation to speed up order fulfillment (and maybe even delivery drones), they are also developing technology. The irony is that while brick and mortar stores are working hard to push their own online sales, Amazon is starting to open physical stores.

So, where will your next tech purchase come from? Will it be from Amazon, Fry's, the Apple Store, the Toyota dealer or REI?

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

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

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 June 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.*

Rational Backup Strategy

By Dick Maybach
Brookdale Computer Users' Group, NJ

In developing a plan to defend against the loss of data and software from operator, hardware, and software failures and malicious acts, it's important to take a systematic approach rather than responding to the latest sensational article or alarming ad. Your first step should be to identify the threats. Otherwise, you could end up with a Maginot Line, an expensive defense against an attack that didn't occur and was ineffective against the one that did.

Common threats to PCs and the information they hold include the following:

- Operator errors are common. You mistakenly delete a file, a directory, or an entire partition. If this involves your software, it may disable the PC.
- Software sometimes contains coding errors that create problems, which if serious enough can crash the operating system. Simply repairing the resulting damage doesn't cure the root cause. However, often symptoms appear only under rare conditions, which means you can only repair the damage and hope these don't recur.
- Hardware malfunction often immediately disables the PC, and the solution is to repair the failure and then restore any damaged data. Some problems, such as intermittent RAM failure can be difficult to identify and may require a visit to the shop. Disk failure is common and this requires replacement of the disk and then restoration of the software and data it held.
- Malware is software that is designed to cause damage. Individual programs acquire colorful names, such as virus, ransomware, rootkit, and Trojan horse. Each newly discovered name results in a new commotion, but the remedy is the same for all – remove the malware and then repair the damage. A worry here is that the malware may reside for some time before damage appears, so that you back up the problem as well as your software and when you restore from a backup, you also restore the malware.
- PC loss can occur when traveling with a laptop or when one fails to the extent that repair isn't economically practical. You must replace not only the hardware, but any original equipment manufacturer (OEM) software that is licensed only for the lost machine. You can restore only your data from backup.
- Environmental catastrophe most commonly results from burglary, fire, storm, or flood. Here you lose not only the PC, but perhaps all the material associated with it, including documentation and backup media. At some level, perhaps nuclear holocaust or asteroid strike, you probably decide you don't care as the loss associated with your PC is trivial compared to other damage.

You will surely find that no single approach will protect against all of these, and you may decide to ignore some threats.

You have two software and data repair approaches: reinstall from the original sources or recover from a snapshot of your disk taken previously. Only the latter is possible with data; the receipts needed to recreate your 2012 tax return are long gone, as are the vacation photos on your camera's SD card. However, with software, you have choices:

1. Use the original distribution media to create a fresh installation, configure it, and apply any updates for the

OS and all the applications. This is tedious, but the result is a clean system, free of whatever problem (assuming it's not with your hardware) that corrupted your system. Most PCs are delivered with the operating system already on the disk and without its installation media; they have instructions on how to create a repair disk, although you may have to dig to find them. Most also have a recovery partition on the disk that you can use to recreate the initial configuration. In my experience, the hard disk is the PC component most likely to fail, which of course makes the recovery partition unavailable. The software supplied with a PC is almost certainly sold as OEM products, which means it is licensed only for that hardware, and it often includes feature to prevent it from being used elsewhere. As a result, you need a separate set of recovery media for each PC, and you need to be able to identify to which hardware each set belongs.

2. Recovering the software from a backup is far simpler, because it restores all the software in one step, which has already been configured and updated. However, if the failure was the result of a developing software problem, you also install its root cause. For this reason, many keep backups made at different times, hoping that if they go back far enough, they'll find a clean one. Of course, when you restore an old backup, you most likely also restore your old data, destroying any acquired since. Your recovery plan must include a remedy for this.

There are several choices of backup media:

1. a backup directory on your system disk,
2. a backup partition on your system disk,
3. a separate internal backup hard disk,
4. an external backup disk, and
5. a cloud service.

Only hard disks and cloud services have the capacity to back up modern disks. Optical media capacities have not kept up with those of hard disks, and far too much of it has poor reliability. Cloud service adds security concerns, both because your data travels over the Internet and because you have entrusted it to an outside entity.

As with the backup medium, you have choices about what to back up. These include:

- a complete disk image,
- all the data files in the home directory, and
- only those data files in the home directory that have changed since the last backup.

Some strategies include backing those OS and application files that have changed, but this can be risky, as these often depend on each other. If you replace a file but not something with which it interacts, the result can be an inoperable system. With software, it's safer to replace everything.

Some backup program developers recommend that your PC have constant access to the backup medium. While this insures that all your data is backed up as soon as its created, it also insures that malware also always has access to the backup. This is a good scheme for protecting against operator error, but less so for protecting against malware and software errors. For the latter, you want your backup medium to be accessible for only very short periods of time. You may decide to use two methods, one that backs up continually to protect against operator error, which are common, and a second that backs up only periodically to protect against such threats as malware.

Backup software is a poor area in which to experiment. Obtain it from well-known vendors with good reputations. Consider only products with favorable reviews from responsible experts. Microsoft includes a suite of recovery

Computer Recycling

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

Deeley IT
—-(Pittsford), 585-381-3100
Tech Source
—-(Rochester), (585) 789-1785
Stereo Shop
----(Webster), 585-787-7467

Certified Document Destruction & Recycling, accepts electronic waste, but charges 40 cents/pound for crt type monitors. Located in Rochester at 1133 Emerson St, 482-9400, www.cdd-r.com

TSC Computer & Electronics Repair, accepts most electronic waste, including printers. Does not accept crt type monitors or tvs. They are located at 765 Elmgrove Road, Gates. 429-6880, www.tscelectronics.com

software with its operating systems, and you should have a good reason for using something different. I discussed their Windows 7 version of this in the February 2012 issue of BCUG Bytes and the Windows 10 version in the May 2016 issued, available at www.bcug.com.

After obtaining your choice, test it as best you are able. For a thorough test, you would have to erase your disk and restore a backup, but don't do this. Instead, make a copy of just one file or directory; then backup, delete, and restore it. Compare the original and restored versions. If the recovery software includes a bootable disk, test it on the PC where you will use it to be sure it does boot. This will probably require that you make some changes in your BIOS. Record these before you change them back, as frequently, the BIOS settings must be different for internal disks and external media. You may also wish to obtain and test a reliable repair utility disk. If you suspect a virus infection, you can boot with it and the virus won't be active. This will allow you to copy your data files to an external drive without its interference. I discussed some of these tools in articles in the April, June, July, and August 2012 issues of Bytes.

My strategy is that every week I have a scheduled backup of all the data files that have changed since the previous backup. This is to an internal hard drive, separate from my system and data drives. As a result, I limit my loss from most causes to the data I generate in one week. Once a month, or when I think of it, I back up to an external hard disk, all the data files that have changed since my last external backup. My operating system is Linux, and I have its installation USB memory stick. Almost all my applications are available from the distribution's repositories. As a result, it's convenient to restore all my software as a fresh install, and I do this every two years, even if I have no problems, just to clean out the accumulated cruft. Reviewing this plan against my list of threats, we see the following:

- An operator error can destroy at most a week's work.
- Similarly, most software errors and hardware failure can delete up to weeks of work. Although if one affects both the service and the on-line backup disk, I could lose up to a month's worth, but this is very rare.
- Malware could cost me up to a month, if it affects all the disks. But malware in Linux is uncommon and, so far, I not had this problem.
- Although I do have a laptop, I transfer any data to my desktop as soon as I get home. As a result, losing it would lose only the data acquired on that trip.
- The weak point in my plan is environmental catastrophe, as all my PC gear resides in one room, and I could lose all of it in one incident. I could improve by adding a backup file server to our home network and locating it in the basement or better by storing a backup drive at a neighbor's or in my bank deposit box or using a cloud storage service.

You should make a similar assessment of your backup plan against your own list of threats to see if it needs adjustment.

Your recovery approach of course depends on what is damaged. Your data resides in what is often called the home directory, and this can be restored only from a data backup. However, Windows may store some of your data (such as Internet favorites and e-mail data) in the system area, and recovering them requires a system restore. The operating system and applications reside in what's known as the system area. They can be recovered by restoring a system backup or by making a fresh install from the original distribution media.

If you use Microsoft's backup software, system backups are in the form of full disk images. If your system won't boot, it may be because the boot loader, or in new PCs the UEFI partition, has been damaged. These can be repaired in Windows system using the Windows recovery disk. See the MS Website for instructions. If the BIOS ROM is corrupted, a competent shop may be able to help, but you may have to return the machine its manufacturer.

How you recover depends of course on how you backed up:

- The fastest is to restore from backup as the result will be software that is updated the last version of your data. If this includes restoring the OS, you must be able to boot from live media, which means you have to properly set up your BIOS. Later PCs use UEFI, which adds complexity.
- If you decide to re-install the OS you can try to restore from the PC vendor's recovery partition, which places your computer to its state when you first purchased it. You will have to reinstall all your applications from their distribution disks and your data from a recent backup.
- If the recovery partition isn't available, you'll have to use the OS distribution disk if you purchased it

separately or its recovery disks if the OS was installed by the PC vendor. (This of course assumes you created these.)

- As a last resort, if the former isn't possible or if you doubt your abilities you can take your PC back to the vendor who sold it to you or to an independent shop to have the OS re-installed. You then must restore any applications and your data yourself. It should be clear that record-keeping is a very important component of your plan. In particular, be sure to label your external backup media and any notes. You don't want to restore from the wrong computer.

Creating and following a good backup discipline require more than trivial knowledge, thought, and time. Many computer owners choose to take a "Do nothing and hope for the best" approach or they follow the advice in the latest article or ad they've read, and neither approach is sound. As a last resort, there are commercial firms that will attempt to recover data from damaged or corrupted storage media, but the results aren't certain and the costs are high (up to multiple thousands of dollars).

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

Online Safety

February Meeting Recap
By John Weigle, Editor
Channel Islands PCUG, CA

Online safety was the primary topic of the February program, with member Michael Shalkey discussing the amount of personal information that's on the internet and many of the dangers that creates. He used chayn.co/safety, which was designed for women but has tips for everyone in its online security guide as a general guide to dangers and solutions, and familytreenow.com, a genealogy site, to demonstrate the amount of information that's easy to find.

The chain.co/safety site offers a starter pack and an advanced guide about possible scams, dangers and solutions. Both are free and part of the website. Its introduction includes this statement: "Modern technology such as the internet/mobile phones etc., has made it increasingly easy for abusive partners to stalk, intimidate and threaten their targets both online and offline. The good news: you can take measures to protect yourself! Assess your risk and take back control with this guide of best practices."

The site emphasizes that everyone posts all kinds of information on social media, opens accounts of many kinds, logs in to sites, and have apps on our computers or smart phones that have information we seldom think about, such as Wi-Fi signals and GPS locations, websites we've visited and pictures we post. It also suggests considering how your children's posts might affect your privacy. Are they posting their addresses, schools, activities, and places they like to visit? General recommendations:

- Use a strong password — at least 15 characters, upper and lower case letters, and numbers and symbols.
- Don't use the same password on many sites.
- Don't let your browser save your passwords.
- Think passphrase instead of password.
- Use a password manager and change your passwords periodically.
- Use two-factor authentication.

Browser recommendations

Use the Electronic Frontier Foundation's Panopticlick at https:// panopticlick.eff.org. (The writer tested the site and it recommended installing Privacy Badger, which it says blocks tracking ads, and invisible trackers, unblocks third parties that promise to honor do not track and determines if the browser protects you from fingerprinting (it lists the information that's shared).

The site has instructions on privacy settings for Chrome, Firefox, Safari, Explorer, and others, and discusses private browsing techniques within browsers and with add-ons. Facebook and Twitter settings are explained as are location apps in smart phones. Message apps WhatsApp and Signal are also discussed. The Advanced Guide

discusses how to identify your security risks and what to do about the ones you find, starting with documenting any abusers who are bothering you. Sections include securing mobile phones, laptops, computers, and apps; browsing the web, social engineering and phishing, IP addresses and Wi-Fi, among others. Other topics include anti-virus and firewall software, encryption and deleting information, remembering that deleting computer files does not remove files. It just changes the file name, which tells the computer other files can write over the "deleted" one.

FamilyTreeNow.com - As noted above, this is a genealogy site, but it could be used by stalkers and others who want to learn more about an individual. "This is a scary, scary thing," Shalkey said. The opening page asks for the first and last name of the person you want information about and a state or all states.

Shalkey used himself and the result was ultimately a long list of associated names, possible relatives, possible associates, current and past addresses and phone numbers. Most of the entries were valid and names that he recognized. (The writer visited the site and the first result was a list of nine people with the name John Weigle. I selected myself and got a much shorter list than the one Shalkey found. My name and my deceased father's name were correct. I did not recognize the sole possible associate. Of the eight current and past addresses, four were correct home or mailing addresses, one was a business site my brother and I co-owned, and three were wrong. Three phone numbers were correct.).

A member of the audience noted that the ease of finding former addresses is a good reason not to use them as part of a password. Clicking on an address brings up a picture of the location. “When you think ‘nobody knows anything about me’ — not necessarily true,” Shalkey said. The site has an opt-out page.

Questions and answers Q: Are maiden names on the site? A: Yes.
Q: Is there a fee? A: I'm sure there is somewhere, but so far what I've shown you is free.
Q: Is the site tracking you? A: I'm not sure. I could have used incognito browsing, which is not tracked.

From the March 2017 issue, The TOE, www.cipcug.org, jweigle@vcnet.com.

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

How Do I Know If My Computer Has Been Compromised?

You can't rely on yourself as a malware detector. Learn how to be a malware avoider.

//

What are the signs that my PC has been compromised, if nothing is visibly noticeable? By that I mean that perhaps someone is quietly reading my e-mail, or even somehow sees my screen or logs my keystrokes?

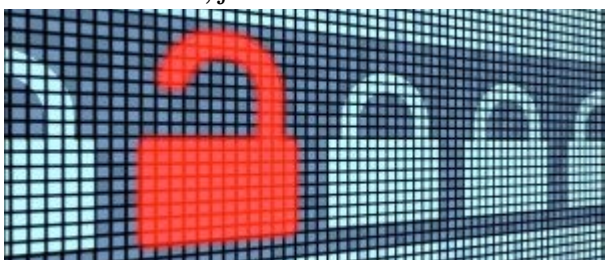
You’re not going to like the answer to this one.
There may be no signs at all. It’s possible for a machine to be compromised even though it seems to be working properly. That’s why we need help.

The goal of most malware is to hide

Hiding is the holy grail of malware: to be able to do something malicious without being caught.
“Malicious” can literally mean anything. Malware that sends spam, steals your information, or monitors your activity would like very much to never, ever be caught. To that end, such malware uses techniques that minimize any signs of its presence. It hides, and tries to hide for as long as it possibly can. If written properly, malware might not do anything noticeable during normal computer use. There would be no signs at all.

The goal of some malware is to cause trouble

Other malware is more obvious — but often not until it's too late. For example, malware that encrypts your files and extorts a payment for recovery — ransomware — clearly wants to be discovered, just not before it has done its damage. While it encrypts your files, it might do so in a way that is virtually undetectable to you or me. Some ransomware minimizes its impact by performing the encryption slowly, taking days or weeks to complete the task, at which point it presents its demands. Other malware doesn't really *want* to be discovered, but discovery is an inevitable side-effect of its more explicit goal. As soon as your files are missing, your network connection overrun, or other malicious impacts, it becomes clear you have a problem.



Some malware is just poorly written

Fortunately, a lot of malware is easy to spot, regardless of its goals. Staying stealthy is hard, and not all malware authors are up to the task. As malware has transitioned from an annoyance to a business, it has certainly become more sophisticated. Still, the vast majority of malware is relatively easy to spot with the right tools. But just because "most" might be easy to spot doesn't mean all are.

Your own observations are the worst

You cannot and should not rely on what you see happening on your computer as a way to detect malware. Chances are you'd be very, very wrong. As I've said, malware tries to hide, and if well constructed, can do a pretty good job of it. What I see more often is the reverse: people who are concerned — even convinced — that they have malware, or are being spied on, when they are not. The clues they see are frequently explained by significantly more mundane and less nefarious causes.

Using the right tools

Since you can't rely on yourself as a "malware detector", you need to rely instead on three things:

- **Rely on yourself as a "malware avoider".** Understand what it means to be safe on the internet. Don't put yourself into positions where you are likely to allow your machine to be compromised in the first place. You are the first line of defense when it comes to staying safe.
- **Rely on your anti-malware tools for detection.** Make sure you're running anti-malware tools, and that they are up-to-date. That also means keeping all your software up to date, including the operating system and the applications you run.
- **Rely on your backups for recovery.** *When*, not if, "stuff" happens, you'll be able to undo the damage done to your files and other important data by recovering from your backups.
-

There are no guarantees

There is simply no way to guarantee 100% safety. There just isn't.

Technology is a lot like life that way. Getting out of bed in the morning involves risk; using your computer involves risk. There's no guarantee you'll notice malware. All you can do is reduce the risk and stack the deck in your favor with good behavior and good tools. And backups. Always backups.

Good Computer House Cleaning, CCleaner

By Len Nasman, Editor / Webmaster
Bristol Village Computer Club, OH

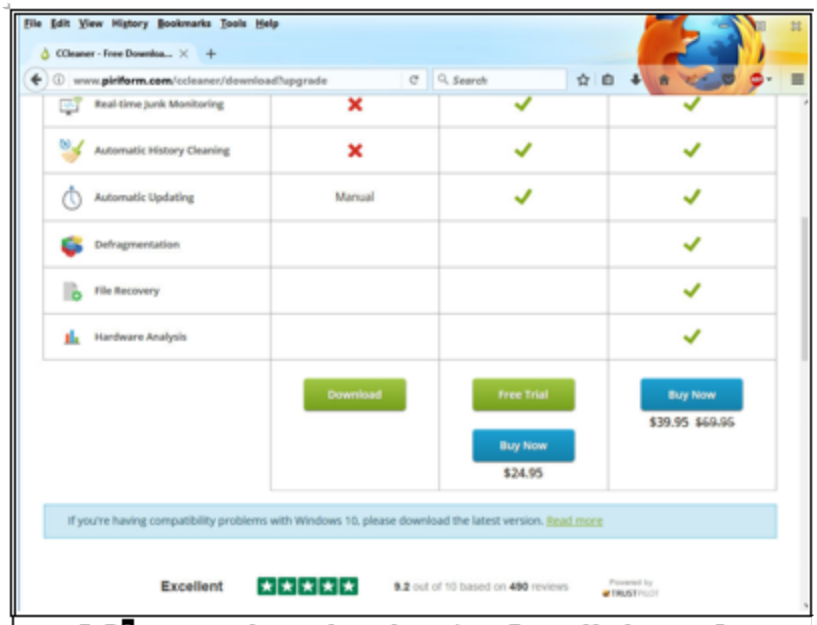
As you use your computer, some things get a little messy. For example, each time you uninstall or update an application an area of memory called the registry is changed. When you install some programs, they might add a feature that keeps part of them running in the background. An example might be when you install software for a printer, a background program might be installed that keeps checking printer use and pops up a reminder to order supplies. If you get too many unnecessary things like this running in the background, it will slow down your computer.

Also, whenever you visit websites, they make copies of things and store them in so-called temporary files. The files are called temporary, but they remain there until you remove them.
For example; Internet Explorer saves things in a number of categories. BTW, if you have more than one user that can login to your computer, these files are saved separately for each different user. Each web browser program (Internet Explorer, Chrome, Firefox) maintains a similar list of files.

In any case, it is a good idea from time to time to clean up the registry, stop unnecessary background programs, and remove temporary files. A useful free program to keep your computer tidy is CCleaner. This program has options for taking care of the issues mentioned earlier. If you have already installed CCleaner, jump to the update section.

Installing CCleaner

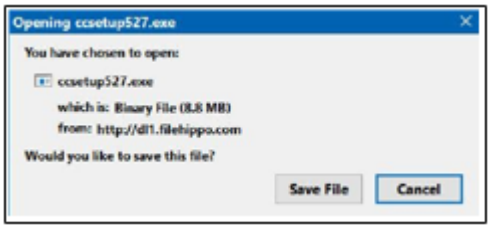
When you go to the CCleaner download web page you will see three different versions offered.



CCleaner download note: Scroll down for downloading the free version

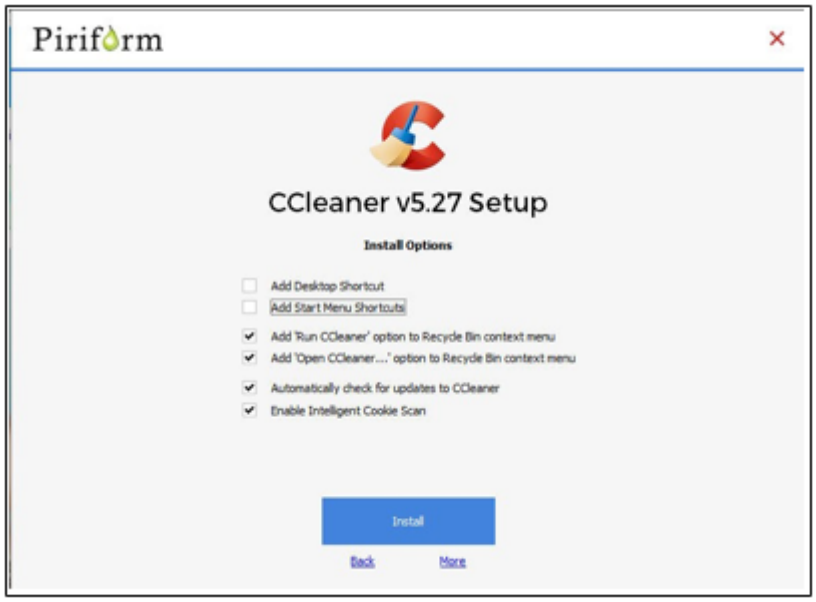
https://www.piriform.com/CCleaner/download

After you select the Download option, a dialog box will pop up that lets you save the install file.



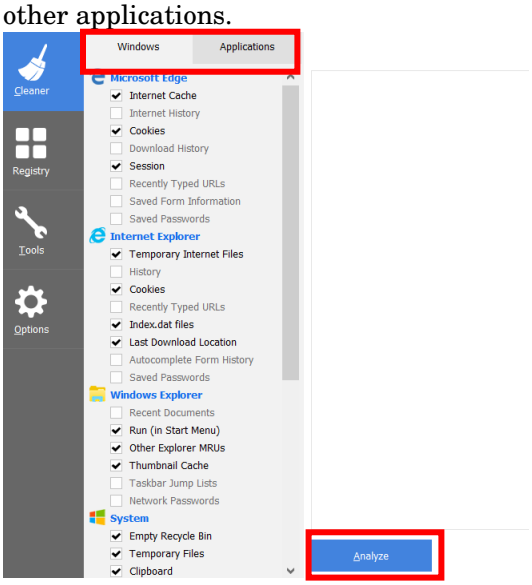
The install program will open an install window that might have a check box that, if not unchecked, will install

other software. Watch out for this. Select the Custom install option and select how you would like CCleaner to be installed.



Using CCleaner

There is a vertical list of options on the left side of the CCleaner window. The Cleaner option allows you to toggle different things to be removed. For example, if you do not want to remove Cookies, or browsing History, select the check marks to toggle the options off. Near the top of the window is a button that has a similar list of options for other applications.

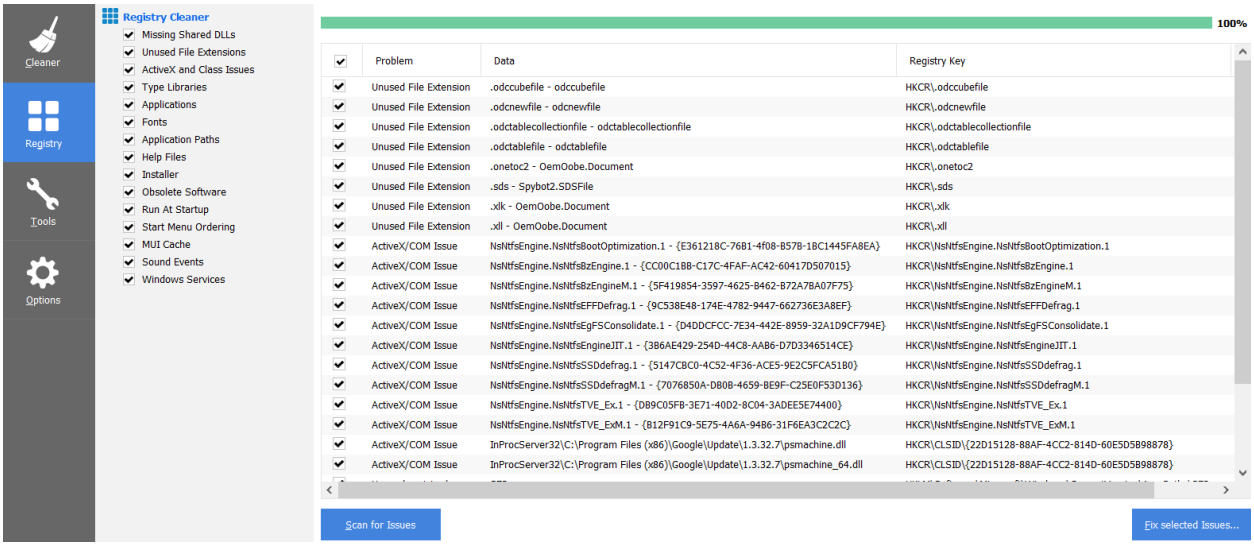


If you select the Analyze button near the bottom of the CCleaner window, the program will go through the motions without deleting any files. It will, however, give you a report of what will be removed if you select the Run Cleaner button.

Cleaning the Registry

When you select the Registry button in CCleaner, you will see two buttons near the bottom of the Window; Scan for Issues and Fix selected issues. After you have scanned for issues, you will see a list of things the system detected. If you then select the Fix selected issues button, you will have the option to backup registry changes. Select yes, and then select Fix All Selected Issues option. It is a good idea to repeat the Scan for Issues option until

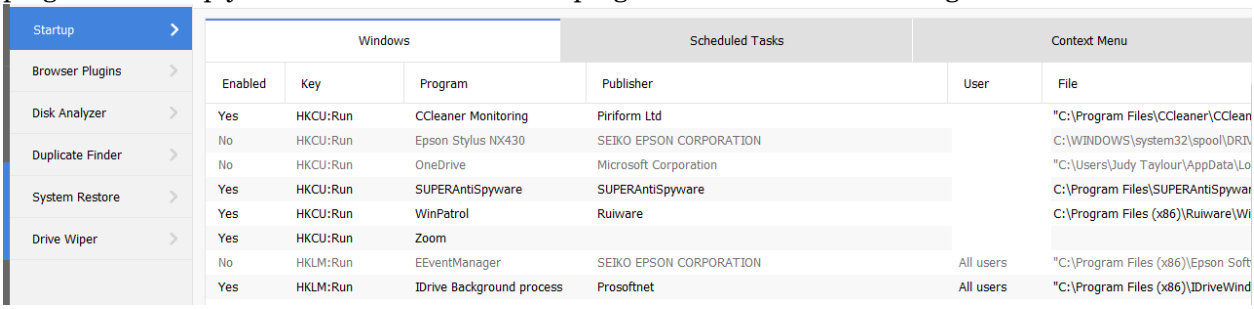
no issues are found.



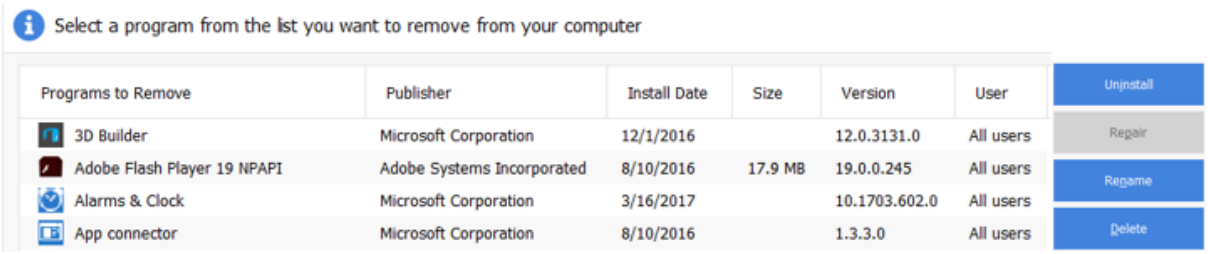
Checking the Startup Programs

CCleaner provides an option to check what programs start running when Windows is first started. In most cases, there are programs that you do not want to always be running in the background.

Select the Tools button in CCleaner, then select the Startup option. Locate a program that you do not want running in the background and right click on Yes, then select Disable. Note that the Disable option does not uninstall the program. It simply removes it from the list of programs that run in the background.



Observe that there is a Tools, Uninstall option that can be used to uninstall programs. It can also sometimes be used to repair programs that have developed problems.



Updating CCleaner

From time to time CCleaner will tell you that an update is available. When you go to the update web page be careful. It will offer an upgrade option. Note that the upgrade option costs money, while there is a free version for updating. Scroll down the page to find the free update. See the download note in an earlier illustration.

From the March 2017 issue, BVCC newsletter, www.bvres.org, bvclub@bvres.org.

Rooting and Custom ROM Installation of Kindle Fire HD 2nd Edition

By Bob Woods, Webmaster
Under the Computer Hood UG, CA

We like to have a radio tuned to a talk radio station or music station during the day. Our location is in a town in a valley surrounded by mountains so our radio reception is poor. As a solution, we have been using a couple of older Kindle Fire HD 2nd generation tablets streaming our favorite stations via iHeart radio. Recently, one of the Kindles started having connectivity issues and was replaced with one of the newer $50 Kindle Fire HD tablets. Since the problematic unit was not being used for anything I decided I would try replacing the Amazon tweaked version of Android with a standard version. I wasn't worried about ending up with a brick as the unit is four years old so not in warranty and was no longer in use anyway.

The files listed and the following steps are intended for the Kindle Fire HD 2nd edition. They will not work on other manufacturers devices or even different models from the same manufacturer. The steps will be pretty much the same, but you will have to conduct an Internet search with your models OS version to get the correct files and any step differences for your device. There are no guarantees that you will not experience any issues. That being said, lets jump into the thick of it.

First, I set the Kindle back to factory defaults. Since I will be replacing the Amazon OS with a standard version of Android I not register the unit. I also logged onto my Amazon account and de-registered the device. Next, onto the internet with multiple Google sessions looking up what was needed.

The first thing I found was the unit needed to be Rooted. This is to allow root access rights to the operating system. On units with proprietary operating systems, like the Kindle or phones tied to a particular service provider, root access is blocked by their version of the operating system. Rooting the unit is done via a root kit, which is an app that has been created specifically to give root access to a specific version of the installed operating system. This required using the Kindles settings setup to obtain its version of the operating system. Then do a Google search to look for the root kit. In my case the search term was "Root Kindle Fire HD OS 7.5.1". What I found was a YouTube video from Tekify with step by step instructions and links to the required software. It also had a link to written instructions.

There are two methods for installation. One with a PC to download, save and run files to do the actual root to the Kindle via USB. And one without a PC where you use the Kindle's browser to download, save and run the files directly. Since I was having Wi-Fi connectivity issues with the Kindle I opted for the method with the PC.

Following the video instructions:

- On your device go into settings (Swipe down from the top and press more) then scroll to “Security”. Set enable ADB to on and press ‘Ok’ on the warning. Go home on your device, make sure your kindle is NOT connected to the computer yet.
- Download the Tekify – Root Kindle Fire HD .zip file on to your computer and extract it.
- In the extracted folder, you will find another folder and a file named “KindleDrivers”, double click this file and press install, when another window pops up press next and wait for the install to complete, once it is done you can click finish and close out the remaining window. Your computer is now ready to use ADB and Fastboot.
- Once again in the extracted folder open the folder named “Root_with_Restore_by_Bin4ry_v33”. inside is a number of items. Double click “RunMe” (not the .sh file) and a command prompt will open.Plug your Kindle into the computer with a USB cable and press 3 on your keyboard followed by enter.
- After a bit of script has run a message asking you to restore your data will appear on your Kindle, click “Restore my data”, don’t worry this will do nothing.
- 10 Seconds later your device will reboot. Once it has booted up the lockscreen will be black and your device will be slow, this is normal.
- Once your computer recognizes the device again some more script will run and the window will close. Your device will also reboot one last time.
- When your device is booted up you will have Root as well as an app called SuperUser installed.

At this point the Kindle is Rooted. However, the Amazon OS is still on the Kindle. To replace it would require two things:

- A backup and recovery application that sets outside of the OS and can be called up at bootup. Think of this as the equivalent of using the function key to get to a Boot Menu on a PC to boot from a USB or DVD drive. This is the only way to be able to replace the OS as Android devices always boot directly to the OS.
- A custom ROM to replace the Amazon Kindle OS. In the Android world a ROM is not a physical device, Read Only Memory. It is a software package of a version of Android custom configured to be compatible with your hardware. It will be close to stock Android, but usually has some additional features. I found there are different custom ROM builds, each with slightly different extra features over plain vanilla Android. The choice is up to you.

For the backup/recovery program I installed an open source program called TWRP (Team Win Recovery Program). For the ROM I settled on Omni 5.1 which is Android Lollipop 5.1.1. I could have gone with Android Marshmallow 6.1 from Cyanogen, but the Kindle ROM version was an unofficial beta version (CyanogenMod 13).

The instructions for installation of TWRP are at Tekify at http://www.tekify.co.uk/kindle-fire-hd/recovery/. Not wanting to use the Kindle WiFi I again downloaded the three files listed below from the URL links in the instructions and transferred them to the Kindle download folder via USB. These would then be run directly on the kindle. The below instructions are shown in the YouTube video, but since it is easy to brick the Kindle during this process, I wanted to follow the written instructions (also listed) after watching the video.

- On the Kindle, enable Installation of Applications from Unknown Sources. (Settings > Device > Allow Installation of Applications).
- Download the three files onto your device: FireFlash.apk, KFHD7 Freedom Boot.img and either KFHD7 TWRP 2.7.0.0.img or KFHD7 TWRP 2.8.3.0.img (It doesn't matter which one however 2.8.3.0 is obviously the latest version). As before, I downloaded the three files onto my PC and transferred them to the Kindle via USB.
- The rest of the steps for TWRP are then done on the Kindle.
- Install FireFlash.apk and open it up.
  - Grant the app Root Access if necessary.
  - Under the 'Bootloader' heading tick the 'Flash kfhd7-u-boot-prod-7.2.3.bin'. *This is required or your device will be bricked.*
  - Under 'Boot Partition' click 'Not Flashed' and find where you downloaded the files.
  - Select 'kfhd7-freedom-boot-7.4.6.img' (This is the correct one even though we are on a later version).
  - Still under the 'Boot Partition' heading tick 'Apply Stack Override'.
  - Under the heading 'Recovery Partition' once again click 'Not Flashed'.
  - This time select the other file ('kfhd7-twrp-2.7.0.0-recovery.img' the number will be different depending which version of TWRP you downloaded).
  - Make sure to tick 'Disable Recovery Auto Update' .
  - Now at the bottom under the heading 'Execute' press 'Flash, Install Script'
  - Once this has finished (DO NOT CANCEL IT) tap 'Reboot Into Recovery' and wait for your device to boot into TWRP.

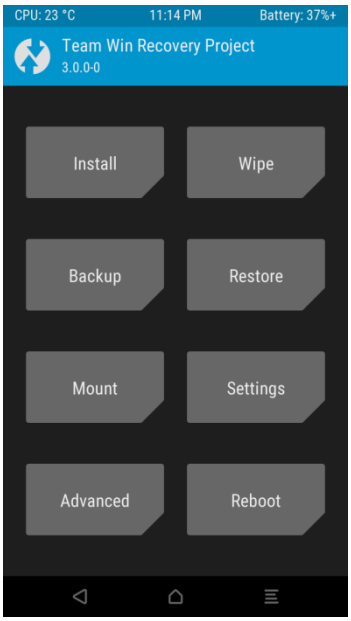
- I would strongly recommend making a backup once in TWRP.
- Finally, you can boot into TWRP any time from a powered off state by pressing the 'Power Button' as normal and then holding just the volume up button until you enter recovery.

Now for the ROM.

Omni 5.1 is a ROM is based on CM12 (Cyanogen Mod 12) however is modified to suit the Kindle Fire HD. Make sure you have at least 70% battery. As a quick warning do not try to overclock the CPU on this ROM as it will cause your device to totally freeze up after a couple of minutes of use. Once again, the instructions are on Tekify at https://www.youtube.com/watch?v=_c5hHSCO_o8 .

- Download the Omni 5.1 ROM, Gapps for 5.0 and Update SuperSU onto your device. once again, I downloaded to my PC and transferred to the Kindle via USB.
- The rest of the instructions are done on the Kindle.
- Reboot into the TWRP Backup/Recovery app.
  - This is done by first, completely shutting down the Kindle (push and hold the power until you get the shutdown button and touch it).

- Then push the power button to boot up. When the Kindle Fire logo shows, push and hold the left volume button (volume up) until the word Fire turns blue and let go of the volume up button after a second or two.
- The Kindle will open in the TWRP application. The TRWP home screen looks like the following image. The video shows the other screens in TWRP you will be dealing with.



- Make a backup using the default settings just in case something goes wrong and you need to restore to a previous state.
- After the backup, click 'Wipe' and swipe to factory reset. *This MUST be done or you will have problems later*. This does not wipe your Internal Storage don't worry.
- Then press 'Install' and navigate to the folder where you downloaded the Omni 5.1 ROM and tap it.
- Swipe to confirm flash, this will take a while DO NOT cancel.
- After it is done DON'T press reboot system or you will have no Google Apps and you will experience errors.
- Click 'Home' and then once again 'Install'
- Select the 'gapps 5.0' file and once again wait. Once again go 'Home' otherwise you will not have root access.
- Click 'Home' and then 'Install' for the final time.
- Select Update SuperSU.zip and press reboot system once it is done flashing.
- First boot up may take a while. However, if it takes more than 10 minutes hold the power button till your device goes off and try turning it on again. From the video we learned that after a ROM replacement you can get into a boot loop, but it should resolve after one or two reboots.
- If it still won't boot go back to TWRP recovery and restore your backup. This will restore your Kindle OS which was saved during the backup. Then check Tekify for hints on how to proceed.

I did not have any issues with any of the steps and all worked after the process was finished. So, what were the results? So far, the Wi-Fi connectivity issue I was having has not surfaced again, being solid. Could have been caused by a system glitch in the Kindle OS or botched update from Amazon. I can now install applications that previously required the device to be rooted. My efforts will not be over written by any updates Amazon is pushing out as the Kindle is no longer a registered device. If I wish I can try other ROM updates by just loading them through TWRP.

Rooting a device and installing a custom ROM is not for everyone. If something goes wrong during the Root or ROM process you stand the chance of turning your device into a brick, though there are recovery step instructions out on the Internet. Rooting will void your manufacturer's warranty. Installing a custom ROM is not so much a necessity these days as Launchers are available to replace the stock home page launcher that came with your device, often with advantages over the built-inlauncher. However, a launcher is just an app that runs on the stock OS that came with your device with all of the lock down the manufacturer put into the OS. if you are looking for an updated Android version or to completely unlock your device look into Rooting and installing a custom ROM. From the February 2017 issue, Drive Light, **www.uchug.org**, **webmaster@uchug.org**.

Tuesday, August 8, **Annual Picnic**, at
Henrietta Town Park, Robinson Cabin

The club will purchase the plates, plastiware, sodas, meats (hotdogs, hamburgers, sausage), etc, for the picnic. Each attendee is ask for a $5 donation, to help offset this cost. Please **bring a dish to pass** (munchies, main course or desert). Your choice of meat should be given to Steve Staub, so that he may order it, 429-9877 or srstaub1@rochester.rr.com.

Wayne's Computer Class Tips

By Wayne Johnson, Instructor
Golden Gate Computer Society, CA

Wayne's computer class is held the second Monday of every month at 7 p.m. Three standout topics at a recent class included:

Test your internet speed

DSL is slower than cable but not as slow as satellite, but do you know if you are getting the speeds your internet service provider promised? Simply do an internet ("Google") search for "internet speed test." Immediately a handful of sources become available for the test. Try two or three. Each will upload and download to and from your computer. For example, my Comcast cable came in with a 69.4Mbps download and 7.04 upload.

If your speeds don't meet your promised speeds, now you have numbers to give them to effect a repair.

Can you answer this question?

"What is your OS (operating system)?" You don't have to be a mechanic to drive a car, but you need to know the year, make, and model—right? So, in just a few clicks, you will know the "year, make, and model" of your computer.

This info is important for any troubleshooting, but it is also a key for purchasing programs or apps and peripherals such as external drives.

For a Windows 7 PC, right-click on Computer under File Explorer and choose Properties. If you're running Windows 8.1, type "PC Settings" on your Start Screen or into your search box. Click the results.

For Windows 10, type "About Your PC" into your Start menu and click the result. You'll be looking the edition (e.g. Windows 10 Pro), version (e.g. 1511), OS Build (e.g. 10586.63), Product ID, Processor (e.g. Intel i5 CPU @ 1.70GHz), Installed RAM (e.g. 4.00GB), System type (e.g. 64-bit).

Why metadata matters

What the heck is metadata? Remember the old library card system? The card told a lot about a book: title, year, author, subject, where to find it.

Similarly, every file you have can tell more than you think because of metadata.
To find out, go to File Explorer, right-click a document, and select Properties. You can see the size of the file, what program was used to create it, when it was created, when it was last modified, and when it was last accessed.

But wait—there's more! Details can provide how many times it's been revised, when it was printed, how much time has been spent editing it, and even more.

Now imagine you were an editor who billed by the hour, maybe you wouldn't want your client to know how many hours you spent (or didn't). With so much metadata attached to each file, individuals and companies need to be careful when sharing images and documents.

From the February 2017 issue, GGCS Newsletter, www.ggcs.org, editor@ggcs.org.

* * * * * * * REVIEWS * * * * * * *

Whoosh! …

By George Harding, Treasurer
Tucson Computer Society

One of the very useful products I came across at CES was Whoosh!

It is a screen-cleaning product that not only clears out all the grime and fingerprints from your phone's screen, but also protects it from further contamination. It works on other screens, as well. I use it on my tablet and my laptop, too. I could use it on my flat screen TV also, but haven't yet.

The product is a spray bottle of liquid, which is non-toxic. and a polishing cloth. You spray a bit of liquid on the cloth, wipe the surface of your screen, then use a dry part of the cloth to polish the screen to a pristine finish. The cloth has been treated with an antimicrobial product to protect the cloth from contamination.

There are several packages in the product, including packets of screen wipes, as well at the customary spray bottle and cloth packages. The latter come in three sizes. The product is available in most office supply and computer stores.

This is a great product to have at home or office. It gives you clean screens in a flash.

Whoosh!
www.whooshscreenshine.com
Price varies from $10 to $20
From the www.aztcs.org, georgehardingsbd@earthlink.net.

Help's Half Hour

June 13, 2017

Q: Using Microsoft Spreadsheet and wants to move a column rather than copy/paste.
A: It was suggested that he highlight the column, and use the header to drag it over to the new location.

Q: A member is getting a boat-load of email messages from someone that he does not want and they include a huge list of "to:".
A: Send him a message to use blind copy rather than fill up the To: use BBC.