Founded 1982
www.rcsi.org

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

MONITOR

Vol. 35, No. 6 June 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, June 13
The Connected Home
by Arpad Kovacs, RCSI

Tuesday, July 11, Movie & Video Night
with popcorn

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

In This Issue

Drones

by George Harding Treasurer
Tucson Computer Society

I am amazed at the rapid development of the drone industry and the uses to which drones are being put.

Here are a few of the uses so far:

- **Package delivery:** UPS has stated that their plan is substantially complete and will be introduced soon. It has limits for weight, distance and delivery address.

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

- **Weddings and other similar events:** Drones make it easy to record events that are important to family and friends. Viewpoints can include those that an individual cannot do.
- **News gathering:** Many TV channels now use drones to access accident sites and other events of interest to a broadcast.
- **Site inspection:** Viewing construction as it is occurring is valuable to identify problems that may not otherwise be seen. Checking electric and other similar supports can be done with drones without the necessity of having a human climb up a tall tower to inspect.
- **Agriculture:** Drones are used to check field sizes, crop progress and limited spraying, without the dangers associated with crop duster planes.
- **Police and Fire observation of sites:** This saves the need for a human to be in danger.
- **Security:** Drones can inspect premises to identify risks that would be difficult for a human to do quickly and economically.
- **Safety:** Australia has started using drones to survey beach areas for sharks.
- **Photography:** Drones can deliver video and photographs in high resolution of just about anything: nature, colorful situations, traffic, events and more.
- **Search and rescue:** Drones can access locations that are difficult or dangerous during severe storms, earthquakes, and hurricanes to find survivors and help with rescue.

With the FAA promulgation of Rule 107, individuals and business can operate drones with assurance that they will not run afoul of government oversight. Some of the rules are:

- Line of sight. The operator must keep the drone in sight at all times.
- Night operations not allowed.
- Maximum ground speed of 100mph and maximum altitude of 400 feet.
- Drone must be lighter than 55 pounds
- Operations in commercial airspace (airports, etc.) only with ATC permission.
- Preflight inspection of drone required.
- Remote pilot airman certificate required. Pilot aeronautical knowledge required, unless the operator of the drone already has a pilot license.
- Registration of drone required. Over 500,000 drones have been registered already.

Intel has made some interesting innovations in drone technology. They have available, a ready-to-fly drone that incorporates their Real Sense technology. It allows the drone to see conflicts ahead and move to avoid them. So, instead of flying into a tree, its drone can see the tree and maneuver around it to keep on track for the target. See intel.com/aero for more info.

Intel is also working on the ability to control more than one drone at a time. At **Interdrone 2016,** a video was shown of a demonstration of controlling 100 drones at a time over the opera house in Sydney, Australia. It showed the drones circling around in what appeared to be a random pattern and ended with an oval of drones in the sky with “Intel” in blue drones in the center. Most amazing!

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

Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/19
Tony Dellelo 734-6149
tonydel@techie.com, 9/18
Bob Avery 385-4491
webmaster@rcsi.org, 9/17

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 May newsletter was printed at St John's/Chestnut Court by the printing group of Don Nichols, Chuck Wells and Steve Staub 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.*

The drone market is exploding as to usage. There are many uses today for drones, but the future will open up many more, things we have not even thought of today.

From the www.aztcs.org, georgehardingsbd@earthlink.net.

Recover, restore, backup, clone, image?

By Carol Picard, Editor / Webmaster
Midland Computer Club, MI

At our January club meeting we discussed how to recover in case of hard drive failure, virus, or if Windows won't start.

The most important steps for recovery need to be completed before a problem occurs. First step is to create a recovery drive. Depending on the computer, this could require a 16Gb or 32Gb flash drive. My suggestion is to use a 32 Gb flash drive. Everything on the flash drive will be deleted and you cannot use the drive for anything else. Well-known brands, 32 Gb flash drives, were recently on sale for less than $10.00.

To create a recovery drive on a Windows 10 computer, connect the flash drive to the computer, search for recovery, click Create a recovery drive. Follow the prompts to create the drive. Make sure "Back up system files to the recovery drive" is selected. The minimum size of flash drive needed will be indicated.

A flash drive has less usable space than the amount of space indicated on the label, so, if it indicates 16Gb needed, you will actually need a 32Gb flash drive. It could take an hour or more to create the recovery drive. During the process, you will see a prompt to "Delete the recovery partition from your PC".

Do not click that option, so you still have the ability to run recovery from the hard drive. Make sure you get the message that the recovery drive was successfully created. If not, try again. After safely removing the flash drive, label it and store it in a safe place. The flash drive is bootable. When you need to use it, insert it in the computer, turn on the computer, and it should automatically boot from the flash drive. However, depending on the computer, you may have to access startup or bios options to boot from the flash drive.

The recovery drive offers more than one recovery option. Depending on what is wrong with the computer, you may be able to save personal files, or may only be able to reinstall the Windows operating system and any programs that were installed by the manufacturer, which is why it is important to have a good backup.

The next step is to back up personal data, e.g., documents, photos, videos, etc. If you are using an email client installed on your computer, such as Outlook or Thunderbird, find out how to back up contacts and emails. Other software programs may store data in special locations, so you will need to find those as well.

Backing up personal data is not a one-time event. Develop a backup plan and follow it because the time that you miss creating a couple backups is when you are going to need them. One of our members mentioned he uses five flash drives for backing up data, backing up once a week, rotating through the flash drives. Based on your use of the computer, you may decide to back up more or less often. Why have more than one or two backups? If you accidentally delete a file, you may not realize it right away and, if you only have a couple backups, by the time you realize the file is missing, you may have written over the last backup that contained that file. Store backup drives in a safe place, e.g., fireproof safe, or at least in another area in your house, away from the computer. For pictures, videos, really important documents, you might want to copy them to an additional flash drive and store that drive at another location.

Most software programs are downloaded directly to our computers so we don't have CD/DVD drives to reinstall from. Generally, if you need to reinstall the software, you can go to the vendor's website and download it again.

However, there may be restrictions on downloading the software more than once, or there may be a charge to upgrade to a more current version. After downloading new software, copy the installation files to a flash drive or external hard drive. When software comes with activation codes, I print that information to a pdf file and save the pdf file on the same drive as the installation files.

You can manually back up files by copying them from your computer to your flash or external drive. Or you may decide to use a software program to manage the backup process. Both free and paid backup programs are available, although some free ones have limited functionality. When purchasing a new external hard drive, it may include backup software. Backup software lets you specify what to back up and to set a schedule for automatic backups. Some have the option to schedule an initial full backup and subsequent smaller backups, called incremental backups, backing up files that have changed since the last full backup. One caution is that viruses can spread to attached drives. Instead of automatic backup, which requires the backup drive be connected at all times, you can run manual backups, connecting the drive only while running the backup.

Online backup and cloud storage are other options to consider. There is generally a charge for online backup service and may be a charge for cloud storage, depending on how much data you have. An advantage is that you can generally access your data from another device, e.g., computer, tablet, smartphone. Onliine/Cloud storage may not prevent loss of data if your computer is locked by ransomware.

With any backup solution, you should occasionally check to make sure the backups are running successfully and that you can recover files. Consider using a program that allows you to restore select files without using the software that was used to create the backup. You may find you need a file while your computer is out of commission and you want to be able to connect the backup drive to another computer and access files without having to install software on that computer. Also, if you only need one or two files, you don't want to have to restore the entire backup.

Whatever backup strategy you use, make sure it is backing up everything you need. I installed a new hard drive for someone whose hard drive had failed. He was using online backup so was confident he would recover all of his data but, the default settings for the service he was using did not include videos, so they were not being backed up and we were unable to recover the videos from the failed hard drive.

Another backup/recovery option we discussed was creating an image (also called system image) of the hard drive. If necessary to wipe/format a hard drive, an image can restore the entire contents of a hard drive; the operating system, programs, and personal files. Some backup programs also provide the option to create an image.

While the terms image and clone are often used interchangeably, the exact definition of clone is when two hard drives are installed in a computer and data is copied from old to new, which requires that the original hard drive is still working. The last time I purchased a new hard drive, it came with a version of True Image software that provided this capability and I was up and running in a short period of time with all of my user ids, programs, data and settings.

When creating a system image most flash drives will be too small so you will need an external hard drive. Depending on the size of the external hard drive, multiple images can be saved to the same drive. Name the image (or the folder you save it in) so you can identify when it was created and, if you have multiple computers, which computer it was created from. The program used to create the image prompts you to create a bootable flash drive, which only has to be done once. You boot the computer from the flash drive and it contains the software to restore the image from the external drive. If you have multiple computers, you may need to create a bootable flash drive for

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

each computer. In most cases, an image or clone can't be used to restore to a different computer, although some software may support this.

Another term discussed was System Restore. This option usually requires being able to boot into Windows. System Restore can be used if the computer isn't working correctly and you suspect recent changes caused the problem, or as an initial troubleshooting step, before resorting to recovery. Make sure system restore is turned on. After upgrading from Windows 7 to Windows 10, I discovered that system restore had been turned off. Windows automatically creates restore points before performing certain actions. You can manually create a restore point, e.g., before installing new software.

To access system restore, search for system and click create a restore point. It should open System Protection under System Properties. Under Protection Settings, it will list the drives on the computer and whether protection is on or off. Normally, you just want protection on for (C:). If it is not on, click Configure and turn it on. Make sure the percentage of disk space available for system restore is set to something other than 0, 10% should be good in most cases.

To create a restore point, click Create and follow the prompts. To revert to a previous restore point, click System Restore… , click Next. To see more restore points, click to place check mark in box to left of "Show more restore points". Click the restore point you want to use and click Next. If you know when the problem started, chose the restore point just before that date/time. If you don't know which restore point to use, start with the most recent and, if that doesn't fix the problem, run System restore again and choose a different restore point. System restore is not supposed to affect your personal files, but make sure your backup is current, just in case.

In some cases, system restore fails and Windows automatically returns the computer to how it was before system restore ran. There is also an option to undo a system restore. After restoring to a date prior to a Windows update or a software installation, it may be necessary to reinstall the update or software.

If you suspect you have a virus on your computer, and don't know whether any of the images/backups contain the virus, it is probably best to use the Windows recovery drive to reinstall Windows and then manually restore personal files. If you don't have a recovery drive, but have access to another computer, you can create recovery media for Windows 10. (https://www.microsoft.com/en-us/software-download/windows10). Previous versions of Windows required entering a code to activate. However, once Windows 10 has been installed and activated, you don't need to enter a code when reinstalling Windows 10 on that computer. When restoring from a backup that may contain infected files, don't restore executable files (.exe) as they are more likely to contain viruses.

With the recovery drive and good backups, you will be prepared when a problem occurs. From the February 2017 issue, Bits and Bytes, http://mcc.apcug.org, capmidmi@yahoo.com.

Ask Leo !

By Leo Notenboom, https://askleo.com/

Making Technology Work For Everyone

How Does a VPN Protect Me?

A VPN, or Virtual Private Network, is a fully encrypted and private internet connection via a VPN provider. I'll look at what protection it offers.

//

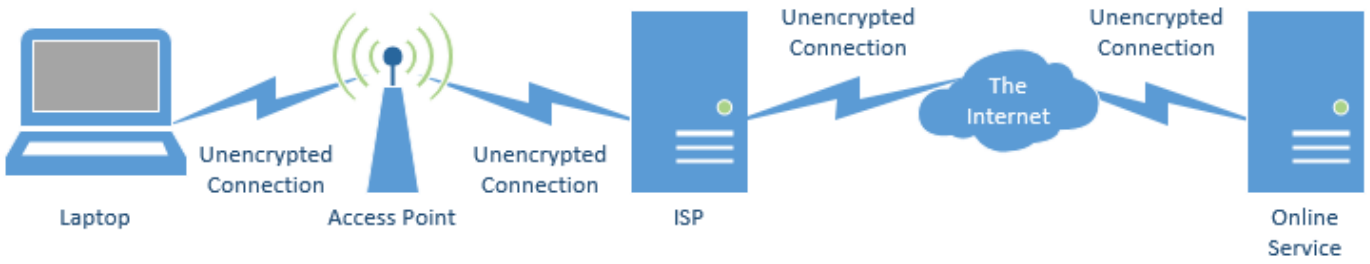
So there's a lot of talk about using a VPN to hide what we do from our ISPs, and you've mentioned using it when using open WiFi. So just how and what are the protections of this versus just connecting through my ISP? What limitations does this have? Can they "see" what I'm doing (like using a BitTorrent), and that is coming from my account?

A VPN, or Virtual Private Network, is one approach to securely connect to a remote resource. Depending on the VPN, that privacy can extend from one end of the connection to the other, or it can protect you only for a certain portion.

I'll describe the different scenarios and how you are, and perhaps are not, protected by a VPN.

No VPN at all

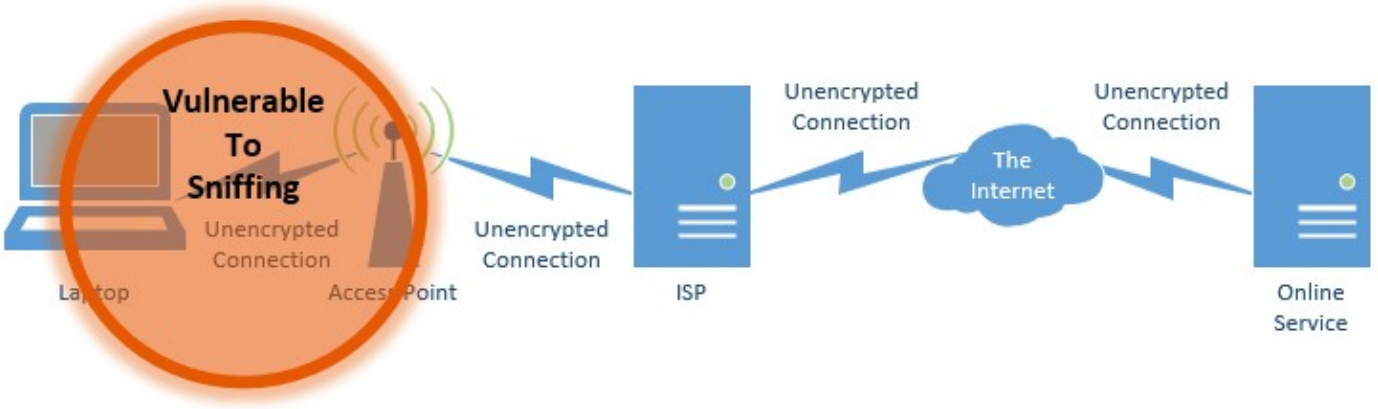
I'll use this scenario as the base: you're in an open WiFi hotspot, connecting to a remote resource like your email, or your bank.



All the connections are unencrypted. That includes:

- The connection from your laptop to the wireless access point (aka hotspot).
- The connection from the wireless access point to the ISP providing the internet connection.
- The connection from that ISP to the rest of the internet.
- The connection to the specific service you're using.

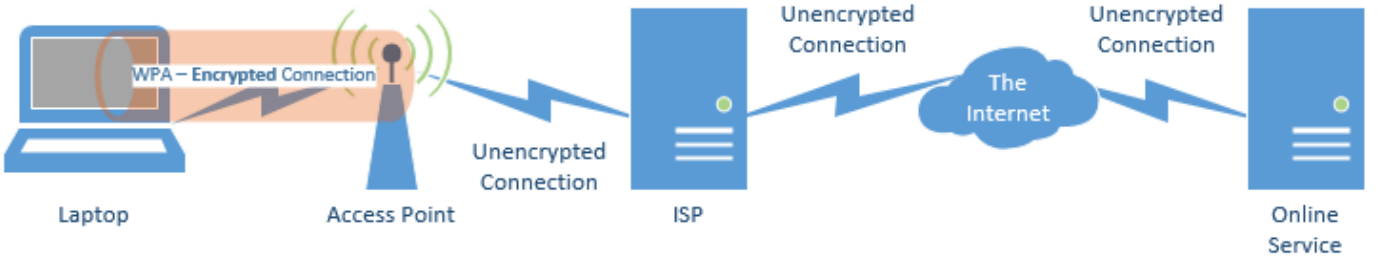
The largest area of concern is the connection from your laptop to the WiFi access point. That open WiFi signal traveling through the air can be "sniffed" (or read) by anyone in range with a laptop and the appropriate software.



Lately, however, there's been concern about the fact that your ISP can monitor what you're doing. Specifically, they can see every remote site or service you connect to, and can examine all data not otherwise encrypted you exchange with those servers.

WPA encryption

The traditional approach to protect yourself from open WiFi sniffing is to use WPA1 encryption built into the WiFi specification.



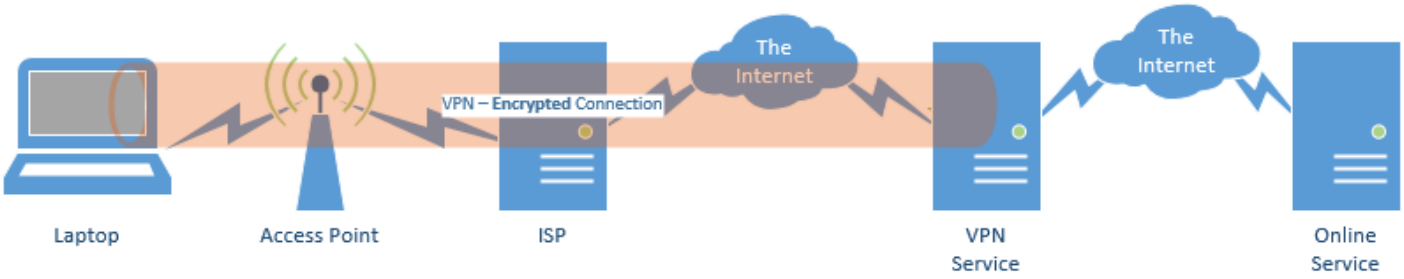
This secures the path between your computer and the WiFi's access point. Hopefully, it's how your home WiFi is configured, so as to prevent nearby homes or others from connecting to your WiFi, and through it, to your network, without the appropriate encryption password.

There are problems with this approach:

- Most open hotspots at coffee shops, airports, and elsewhere don't use encryption; the password requirement would confuse their customers more than it's worth. That's why these hotspots are called "open".
- When WPA is used, it protects only the connection between your computer and the WiFi access point.

Everything past that point in the diagram above remains "in the clear".
That last point becomes important because all the traffic is visible to the hotspot's owner, should he or she care to peek, and to the internet service provider to which that hotspot is connected.

A VPN service
To protect yourself further, a VPN is a common solution.



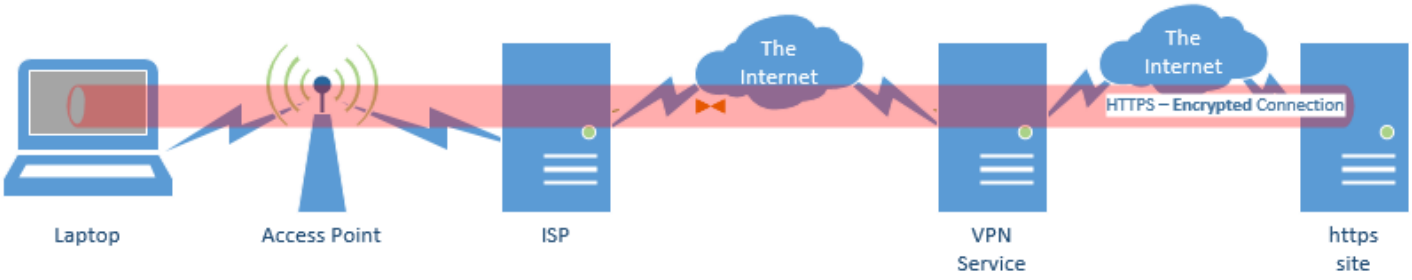
A VPN securely encrypts the entire path from your computer to the VPN provider. No one along that path can see your data: not other WiFi users, not the people managing the hotspot, and not the hotspot's ISP.
For open WiFi, or other situation with questionable security (such as connecting to the internet at your hotel), a VPN can be a great solution.
But it's not perfect.
There are some things to note:

- The connection is only secured up to the VPN's servers; the connection from the VPN provider's servers to the final destination is once again unencrypted. That means the VPN provider, as well as any other networking equipment along the rest of the way, may be able to see your data, and can at least see which servers you're connecting to.
- You're adding steps between your computer and the server you're accessing. The practical effect of this is that your connection becomes slower. How much slower varies based on the VPN service you're using, their capacity, and the server you're attempting to access.
- Not all VPN services support all protocols. For example, your web browsing might work, but your attempts to use BitTorrent might not.
- Not all remote servers allow connections through VPNs. One non-security-related reason to use a VPN is it can make you appear as if you're located in another country. As a result, many services – such as streaming video services – block connections using VPNs.
- Not all governments allow VPN connections out of their countries, so as to effectively censor what their residents can view.

The ISP you're connecting through can't see, for example, that you're using BitTorrent, but the VPN service can.
Your ISP would still see that:

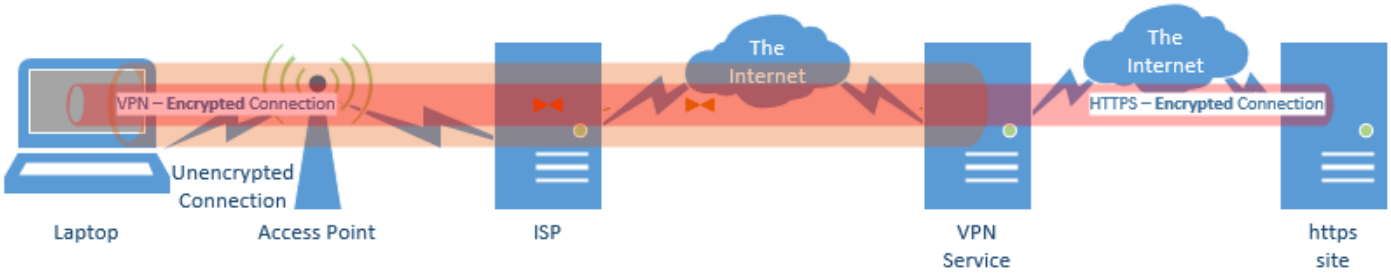
- You're using a VPN (and which VPN service you're using).
- You're sending and receiving an awful lot of data.

End-to-end encryption
The only true privacy is achieved with end-to-end encryption. Unfortunately, that isn't possible in many cases, since it must be supported by the service to which you are connecting.
Https is end-to-end encryption



Connections you make via https are completely encrypted along the entire path from your machine to the remote server you're accessing. That's why banks (and other services that allow you to access sensitive data) should use https. Most web-based email providers also provide full https connectivity. In fact, more and more sites — including *Ask Leo!* — are switching to support https.
Similarly, when configuring a POP3, IMAP, or SMTP connection in your email program, if your email provider supports it, choose SSL or TLS. That's the underlying encryption protocol used by secure connections like https. That way, your email uploads and downloads – as well as your log-in information – is completely encrypted along the entire path to your mail server.
Note, however, that even when using https, your ISP can still see which sites you connect to. Only a VPN can hide that information from them.

Https overa VPN?
Just to complete the picture, if you're using a VPN, and you happen to connect to an https web site, your data is doubly encrypted for part of the trip.



- The VPN protects you between your computer and the VPN service.
- Https protects you between your computer and the service to which you're connecting.

There's really no practical harm. One benefit is that the VPN prevents your ISP from seeing which site you're connecting to.

It's Innovation Time

Best of Innovation Honorees for CES 2017

By Lou Torraca, President, MOAA-The TUG, Hawaii

The Consumer Technology Association (CTA) producer of the Consumer Electronics Show (CES), the world's gathering place for all who thrive on the business of consumer technologies, announced the Best of Innovation Honorees for CES 2017. The annual CES Innovation Awards honors outstanding product design and engineering across 28 product categories. The show, in January, annually attracts around 150,000 folks to Las Vegas, who represent consumers, company CEOs, venture capital money folks as well as a huge contingent of media who document it all. With 28 categories, you can imagine how much time it takes to see it all. Since each category picks a winner, I have picked six I think will interest you. Next time, I'll cover another six in different categories. To give you an idea of how these winners are chosen, here are the criteria the judges use:

- Engineering qualities
- Aesthetic and design qualities
- The product's intended use/function and user value. For Tech for a Better World entries, this also includes how it can make a positive impact to the quality of life for its users, or those affected by its use.
- Why the product deserves the Innovation Award, including specifics regarding its unique/novel features and features that consumers would find attractive
- How the design and innovation of this product directly compare to other products in the marketplace

And here are the winners in six of the categories

uBolt, an innovative and unique multi-factor authentication personal identity wearable device combining biometric fingerprint and voice recordings and a secure element to ensure "you are who your say you are" to establish trust and verifiable confidence in a user identity.

COMPUTER PERIPHERALS

Predator Z301CT monitor
The Acer Predator Z301CT is the world's first 21:9 curved monitor with eye-tracking functionality.

HOME APPLIANCES

Sleep Number
Sleep Number's 360 smart bed will forever transform the way people sleep. The new integrated design includes a proprietary algorithm (powered by SleepIQ technology) and machine learning to intuitively sense and automatically adjust all night for an effortless and optimized sleep experience.

Integrated Connectivity Cluster
Bosch

The ICC is the all-in-one information and communication system for motorcycles – and riders. It is the first of its kind integrating head-unit functionality into a cluster. The HMI clearly displays nothing more (and nothing less) than the information essential to riders looking to take their experience to the next level.

TECH FOR A BETTER WORLD

Tobii Dynavox PCEye Mini with IS4 Eye Tracker

The Tobii Dynavox PCEye Mini featuring IS4 eye tracker is the world's smallest and most robust eye tracker. Optimized for individuals that do not have use of their hands due to various disabilities, the device enables users to control a computer, laptop or tablet using only their eyes.

SMART HOME

Smart Remote by Sevenhugs
Smart Remote is the world's first contextual control system for connected homes. It lets you control everything at home with just one touch. When you point Smart Remote at a device, the screen automatically adapts and you just need one touch to control it. A seamless and intuitive control system.

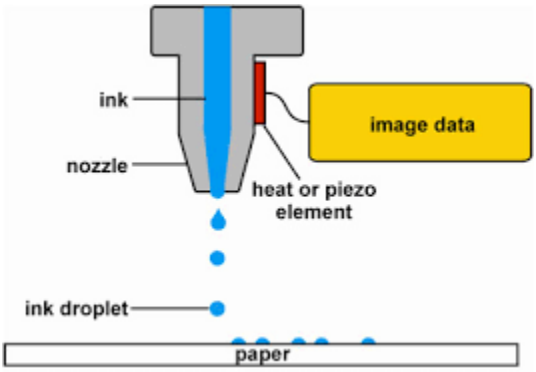
That's it for January, hope your New Year will be a wonderful one for you and yours. Aloha,
Around Hawaii, Oceanic Time Warner Cable, http://www.aroundhawaii.com/lifestyle/innovation-time-vegas/, www.the-tug.org

Inkjet Printers

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

The inkjet is the most common type of printer used at home. These are inexpensive (although the ink is relatively costly), and they print color, including photos, with high enough quality for most users. The other common type for home use is the laser, which is more expensive (although the per-page costs is lower because toner is less expensive than inkjet ink) and require more power. For example, most UPSes won't power them.

Typically, inkjets use four inks, cyan, yellow, magenta, and black, with separate cartridges and print heads for each. The ink is ejected, one drop at a time, by either thermal or piezo-electric means. Thermal heads heat a tiny amount of ink and the resulting steam propels a single drop, while piezo-electric ones change shape slightly to propel an ink drop mechanically. The great majority of consumer printers are thermal, but they require compromises in the ink design, since it must endure high heat. See https://en.wikipedia.org/wiki/Inkjet_printing for a good introduction to the technology.



If you print only on letter paper, use Windows, and connect to a PC's USB port, almost any inkjet will give satisfactory service. Linux and Mac users and those networking their printer or printing on other media have to be more careful.

Printers are remarkably inexpensive, but my experience is that they have fairly short lives, and a printer is the PC component most likely to fail. Expensive models don't appear to last any longer than cheap ones, so unless you have special needs, buy something cheap. My inkjets always wait to fail until I've purchased a large supply of ink cartridges, which are never usable in the replacement, even a similar model from the same manufacturer. The defense strategy is obvious; keep only a small supply of cartridges on hand. Although a set of ink cartridges will often cost more than the printer, you should buy a replacement set soon after you get a new printer, as many printers are shipped with only partially-filled cartridges.

The quality of off-brand cartridges varies, and some I've used tended to clog or fail in other ways. Refill kits seem to be disappearing, probably because printer manufacturers have devised schemes to discourage their use. You can buy refilled cartridges, but here too the quality varies. Considering the low cost of printers and the high cost of name-brand ink, you may wish to explore here. Using other than your printer manufacturer's cartridges usually voids the warranty, so it would be wise to wait until the printer warranty has expired to experiment; after that you have little to lose. I do relatively little printing, and the frustrations of dealing with cheap cartridges are not worth the savings for me.

Be careful when buying other than letter paper, such as business cards or labels, as many are printer specific. Using laser stock in an ink-jet guarantees smearing. Download the manual before you buy a printer and check that it will do what you need, especially if you will be using other than 8 ½ by 11 letter paper. Despite what the manual says, non-standard paper sizes may not feed properly. I recently tried to print name-tags that came in 4 ¼ by 11 inch sheets. Although envelopes of about the same size printed fine, the name tags sheets would not feed. I had to fashion a custom guide, and even then, the feeding was far from reliable. My printer also would not feed card stock when I first got it, but this improved after a few days. Apparently, the feed rollers needed to be roughed up to work properly. Some printers don't like mixed paper in the tray. I've had problems mixing card stock and letter paper, even though both were the same size, but the manual warned against this. Many printers include a duplexer that implements double-sided printing. However, these often work only with standard-weight letter paper.

The most common problems are clogs and paper jams. Clearing an ink clog generally requires no more than running the printer's cleaning routine. (Again, see the manual.) This can sometimes be started by the proper dance on the printer's buttons, but may require a maintenance utility that you can install from the CD supplied with the unit. Unfortunately, these may not be available for OS X and are never available for Linux. Many Mac and Linux users have Windows available on a virtual machine or can dual boot to it. If you don't, do your research before you buy.

If you do experience a paper jam, don't yank, as this will almost certainly break something, and printer repairs are seldom economical. Instead, get on the Internet and find how to clear it. Similarly, do some research if you begin to experience paper misfeeds; often, this can be cured by a proper cleaning of the feed mechanism.

Some years ago, Windows-only printers were common. These had non-standard interfaces and required proprietary drivers, which were available only for Windows. The switch to USB has eliminated most of these, except for Canon. My experience is that no new Canon printer is usable with Linux. After a while, Linux developers may manage to reverse-engineer the interface, so that many older Canons are usable, but each new model requires a repeat of the process. At the other extreme, HP has traditionally been Linux friendly. If your operating system is not Windows, you may not have support software to do such things as checking ink supplies and trouble-shooting. However, printers are now beginning to include status displays and control panels to make them more OS agnostic.

All-in-one models that combine a printer with a scanner and a fax are common. Fax is quickly going the way of the dial telephone, which makes it, at least for me, a useless feature. I also prefer a separate scanner as I use this much less than the printer, and I feel it adds enough mechanical complexity to make an already failure-prone device even more so. Again, scanners are a problem area for Linux, and finding a compatible printer-scanner is more difficult than finding just a printer.

With respect to the interface, USB is almost universal, but many models also include Ethernet and/or wireless ports. The last two allow more than one computer to share a printer; however, the configuration is sometimes not trivial. In particular, encrypted wi-fi can be troublesome (and you are foolish if you use non-encrypted wi-fi). WPS can make this easier, but be sure to disable it after you configure your printer, as it makes your network less secure. These networking ports are cheap to add and are unlikely to present a reliability problem, but unless you have some network configuring experience, you may find them unusable.

Again, read the manual, even if you print only on standard paper. For example, many printers must be shut down with their power switches. Turning off using the outlet strip into which they're plugged may lead to problems, such as ink clogs.

The promise of a paperless world has proven to be false, and few of us would be comfortable without a printer attached to our computers. However, their mechanisms are complex and subject to malfunction and failure, and they require more care than most other computer components. Spending a few minutes with the manual can extend the life of yours and will probably reveal new abilities.

From the December 2016 issue, BUG Bytes, www.bcug.com, n2nd@att.net.

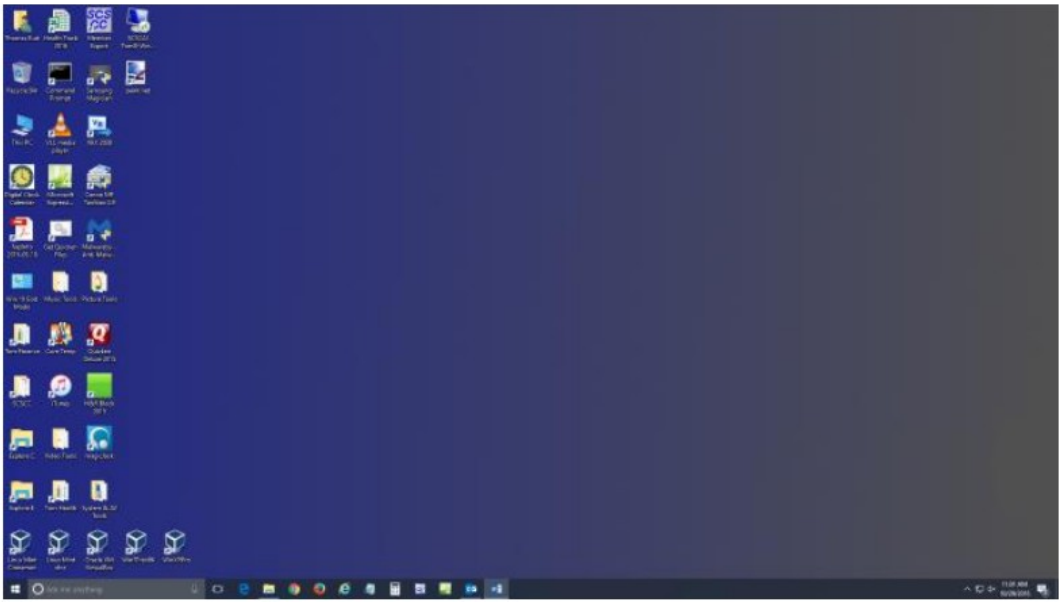
* * * * * * SOFTWARE and HARDWARE * * * * * *

Tom's Tech-Notes

Windows 10 – Tuning Up Your Start Menu

Tom Burt, Vice President
Sun City Summerlin Computer Club, Nevada

Windows 10, originally released in July, 2015, recently saw its second major update (V1607-Anniversary) in July, 2016. By now, most Windows 10 users have received that update. Originally, I had mixed feelings about the new hybrid "list and tiles" Start menu. However, I've gradually come to like it as a way to declutter my desktop and actually make it easier to find things. Here's a screen of my desktop today:



The exact details don't matter. As you can see, I still have a lot of icons on the desktop that I use to launch applications. Over a year of using Windows 10, I've steadily reduced the original number of icons by half to what you see in the screen shot. However, even now, when I'm working intensely and need to start an application while I have others running, it gets irritating. I have to minimize those other apps to uncover the desktop icons so I can double-click the one I need to launch the new app. Also, to launch from a desktop icon, I need to double-click it – something my stiff fingers no longer do well.

The Windows 10 V1607 Start Menu is the best incarnation yet and helps me with some of the above issues. You can open the start menu by clicking the flag icon at the bottom left of the screen or by pressing the Windows key. Following is a screen shot of my current Start menu:

I have stretched the Start menu out to allow four 3-column groups and have almost all my tiles sized to the medium, square size. In this layout, I don't need to scroll to find a particular tile. The tiles are grouped and labeled along functional lines, such as "Tom's Key Apps", Image Tools, "Movie and Video Tools", "Web Browsers and Tools" and others. The app tiles I use most are at the top left.

To launch an app, I just press the Windows key to pop open the Start menu and then click the tile of the app. The app starts up and the Start menu closes back up. I no longer need to uncover desktop icons and double click. Tiles are especially nice on hand-held touch screen devices.

Down the left side of the Start menu is the standard complete list of all installed programs. You can right-click on any program in the list and choose "Pin to Start" to add a tile for that program to the array of tiles. You can then drag the tile to wherever you want it in either an existing group or a new group.

You can right click the tile to adjust its size to small, medium, wide or large. The wide and large sizes are useful for "modern" apps that animate their tiles with "live" content. News and Weather apps are examples. The medium tiles display the app's name and an icon.

You can adjust the width of the Start menu by opening it, positioning the mouse cursor over the right edge until the cursor turns to a double arrow, and then dragging to the right (to widen) or to the left (to narrow). Tile groups will automatically move to fit the new shape of the Start menu window. You can adjust the height of the Start menu by opening it, positioning the mouse cursor over the top edge until the cursor turns to a double arrow, and then dragging up or down.

You can rename tile groups by clicking the space just above the group and then typing a name. You can move entire groups around by clicking and dragging the group's title space.

To remove a tile from the Start menu, right click it and select "Unpin from Start". That program will still be listed in the Start menu's left-side list of all installed programs. I got rid of quite a few of the default tiles for apps I never use.

To add a tile/icon to the Windows Taskbar, right click either the tile or the program name in the program list. In the pop-up menu, hover the mouse over the "More" option to get a second pop-up and choose "Pin to Taskbar". After the icon appears on the Taskbar, you can drag it left or right to where you want it to be permanently.

So, that's a quick summary of things you can do to make the Windows 10 Start menu work better for you!

For additional info, http://www.scs-cc.com, tomburt89134@cox.net.

All that Glitters is not Chrome

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

I love my Chromebook. It's a very handy thing to have when you want some information off the Internet quickly. I don't have a smart phone, so the Chromebook is what I go to when I want to know the locations, hours or phone number of a business, what traffic or weather conditions are like or the answer to any other search question. I keep my Acer Chromebook 11 on our kitchen table so it is available for instant use. It is small and light, yet has an 11.6" screen and a full keyboard, so I find it much more useful (and usable) than a tablet.

When I bought my Chromebook over a year ago, I thought I understood the limitations it had in needing to be connected to the Internet for most uses, and its limited storage and processing power. It has exceeded my initial expectations and I find I often use it nearly as much as my Windows 7 laptop. I love that it boots in about ten seconds, has a very long battery life and is very portable, so I find I'm taking it more and more in situations where I'd otherwise take my 14" laptop. In spite of its advantages, I do still continue to find new annoying shortcomings in the Chrome OS, and difficulties figuring out how to perform a particular task or change a setting. Though I've come up with work-arounds for some of its limitations, my Chromebook still has enough tarnish spots in its capabilities that I doubt it will ever be a complete substitute for my laptop.

I own a lot of computing devices. I probably have more than most people, though I'm sure there are some out there that have more. I admit I am hanging on to some devices that have not been used in many years (that is another story), but there are in my household almost a dozen that I myself have used at least once in the last year. Most run Windows (two laptops, three desktops and a PDA). I don't feel I'm closed-minded, though, as I do have an Android tablet, an iPad mini (iOS) and two Chrome OS devices (Chromebook and Chromebit). I've nothing against Linux, but you don't normally find it in stores on new devices, and I've not yet found a compelling reason to install it on one of my existing devices.

From this, you would probably assume (correctly) that I use Windows most of the time. You could say I was "raised" on Windows, so I tend to judge, for good or bad, all other computing user interfaces with Windows as a reference. As an electrical engineer, I spend most of my work days working on documents, spreadsheets and designs, using software running on Windows PCs, with the traditional keyboard and mouse user interface. I've grown accustomed to the features, capabilities and limitations of Windows on reasonably-powerful Intel-based computers, typically with lots of memory and storage. In spite of the (often unfortunate) changes to the Windows user interface over many years and versions, I usually find it easier to adapt to the next thing Microsoft throws at me than something coming from a seemingly completely different mindset, like iOS or Android.

I was able to figure out how to get around on the web pretty easily on the Chromebook. The OS is based heavily on the Chrome browser, which I use most of the time at work. Though I could get a Bluetooth mouse to use with my Chromebook, the touchpad has unique features that allow me to do almost everything easily. I don't notice any real difference in the Chromebook's ability to serve web pages as compared to my i5-processor-equipped Win7 laptop with IE; processing power is not a big factor in traversing the web.

A main point of contention for me in all non-Windows devices I've used is the file manager. I'm so used to the Windows File Manager that everything else seems alien. The Files app in Chrome is fairly similar, but I only recently found the way to see how much space is available on a drive (it is under "Settings" when looking at that drive). I still don't know if iOS even has a file manager; I have photos on my iPad that I have yet to figure out how to copy off.

My Chromebook uses at least half of its 16G of SSD memory for the OS and apps, and it says even the remaining memory is subject to use by the system. I bought a 128GB USB3 Flash drive to use with the Chromebook, which seems to work great. It would have been more useful if the Chromebook's SD memory slot were the type that keeps the memory card totally inside the body of the Chromebook; unfortunately, the SD card sticks out and is at risk for damage or breaking off.

In addition to saving and editing files in Google Docs on the Chromebook, Microsoft Office files can often be edited in "Office Compatibility Mode". This works even when working offline (no Internet connection), and allows me to take my Chromebook to meetings to take notes, or write newsletter articles on it while riding in the car. It appears to be compatible only with the most recent Microsoft Office file formats. I've had good luck with Word documents, and can edit PowerPoint slides, but I had issues the one time I tried editing an Excel spreadsheet. If I plan on taking notes or editing files offline somewhere, I always test opening the file I'm planning to edit before I leave home.

One unnerving feature of the office compatibility mode is its lack of a "save" feature in the menu. The first time I opened a Word file to edit, I made a few test changes and then closed the document. Fortunately, the changes were present when I opened it again, but I still didn't fully trust it. I finally noticed that it saves each keystroke of change back to the file as it goes; as I would press a key to add a letter, the access light on the external USB Flash drive would flash. While this saving method ensures you don't lose changes, it does wear out the Flash drive's solid-state memory faster in writing to the drive so many times.

Chrome OS is compatible with an extensive list of file types, including most office, media and image files. It can open .pdf files as well as handle compressed files like .zip and .rar. I did recently find out that Windows Media Video (.wmv) files cannot be opened by a Chrome OS device. I had created a photo slide show for my dad's 80th birthday, with the result being a .wmv video. While I did find one app that vaguely mentioned allowing .wmv files to be viewed, most of the search results for this problem suggested converting the video to a supported file type. In the end, I used my Win7 laptop to play the file.

Even files that are supported by Chrome can have problems if a lot of hardware horsepower is needed. I have an auto dashcam that records video in HD as .mp4 files. I can connect the dashcam through USB to my Win7 laptop, which can easily play the video files stored on its memory card. There might be a few slight glitches, but playback appears pretty smooth. If I connect the dashcam to my Chromebook, it can play the video files, but it takes a long time to process before they initially start playing, and the playback is very jerky.

The Chrome OS has its own web store, but since it does not have a large following, there are not that many offerings as compared to the Android app store. There are a couple of VPN apps, but the VPN service I subscribe to, Private Internet Access, does not appear to support the Chrome OS at this time. I was surprised to see that TeamViewer was available as a Chrome app. I've looked through the apps offered a number of times, but have yet to find one I wanted to install at the time.

Chrome OS is also not supported that well by third-party hardware vendors. The Patriot Aero external Wi-Fi hard drive I tried to demonstrate earlier this year has apps to support its use with Android and iOS devices, but they don't have one for the Chrome OS. I have some Western Digital My Passport USB3 external hard drives, which can be set up to use password protection and data encryption. My Chromebook can see and use the drives that are not protected, but cannot use a drive that has protection / encryption enabled, as the program on the drive that is used to enable and disable protection is not compatible with Chrome. The universal in Universal Serial Bus only applies if there is no additional software required.

Printing is another problem issue for Chromebooks, as printers would need drivers. I've not seen any printers that advertise supporting Chrome OS devices. Google claims printing can be done using Google Cloud Print. I've read some about it, but have not yet been able to figure it out. It is made more confusing by Google having a Chrome browser and a Chrome OS. So far, I've settled for taking my files to a Windows PC to print.

Chromebooks offer a lot of promise for speedy and simple computing, but they don't always fully deliver on everything a user might want to do. I love my Chromebook and will continue to use it, but it appears it can't do everything I need. I guess I won't be giving up my Windows computers anytime soon and will continue to use it, but it appears it can't do everything I need. I guess I won't be giving up my Windows computers anytime soon.

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

Back to Basics

Using Windows Explorer Is a Must

By Jim Cerny, Chairman, Forums Committee
Sarasota Technology UG, Florida

This is a start of a series of articles on the basic use of Windows Explorer (known as File Explorer in Windows 10). It is very important for ALL VERSIONS of Windows users. This program (or app) allows you to do everything you can think of with FILES and FOLDERS. The icons for this app (see illustration) have not changed very much over the years, it is basically a yellow folder.

What's the big deal? I have taught classes many times on using "Files and Folders" or "Computer Organization" and in every class many students were amazed to discover answers to most of their computer frustrations just by learning how to use this one app or program. Even if you have used this app before, I believe reading these articles will help you discover more or easier ways to help you with your Windows computer.

Windows Explorer (or File Explorer in Windows 10, why they changed the name I'll never know) can easily perform the following functions. Have you ever wanted to do any of these things?

- Organize all your files and folders on your computer and other memory devices
- Move, copy, delete, and rename files and folders
- Create new folders
- Copy files and folders TO and FROM other devices such as other drives, phones, cameras, disks, etc.
- Create quick and easy backups of your stuff

Windows 7

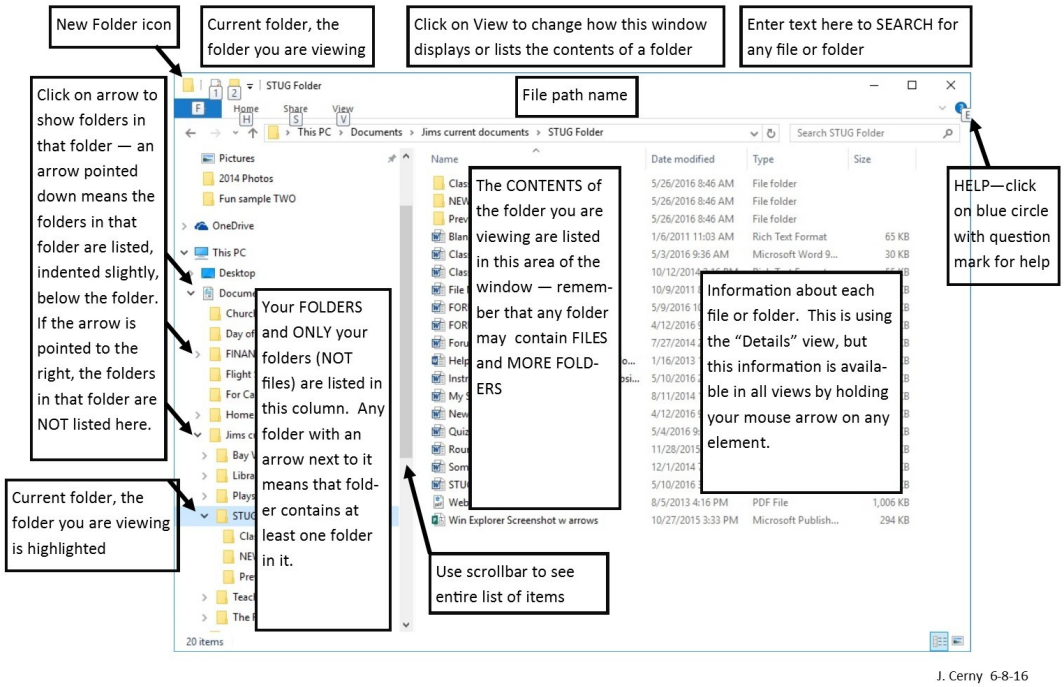
Windows Explorer

Windows 10

File Explorer

Please take a look at the large illustration of a sample of the File Explorer window – I will be referring to it in the next couple of articles. Please remember that this app or program is in ALL versions of Windows and the functions are basically the same. So let's get started simply by understanding what this app shows you in its window without really doing or changing anything. It may help you to think of a steel filing cabinet in an office. You don't want to just throw things into the drawer, you would never be able to find an item without searching through everything. So you use a FOLDER and write a NAME on the folder and put things INTO that folder so you can find them. Everyone has done that, right? Remember that you can put a folder INTO a folder too – so you could have one big folder that you have named "Home Expenses" and have folders IN that folder such as "Electric bills", "Phone bills", "Water bills", etc. So, to get to a specific electric bill you would have to first look IN the "Home Expenses" folder and then open the "Electric bills" folder in it. It's not too hard, right?

BASIC WINDOWS 10 FILE EXPLORER ELEMENTS



Basically, the File Explorer app is a way to find and organize anything in memory on your computer's C drive and any memory device connected to your computer. This is one app that I think Windows has done pretty well to help us all use our computer. The app window has two basic areas (called window "panes", get it?) a left pane and a right. The LEFT pane contains the list of FOLDERS and only folders. You will never see a "file" in this list! The RIGHT pane displays the contents of any folder you have selected in the left pane. When you click on a folder name in the left column, the contents of that folder appears in the right area of the window. EVERYTHING on your computer is organized in FOLDERS. You could think of your entire "C" drive as one big folder. If you connect another drive, that whole drive is a folder as well. Your C drive contains hundreds or thousands of folders, way too many to see them all at one time in the list on the left, so only the highest level of folders are shown in the list. If a folder in this list contains at least one folder then there will be an arrowhead ">" next to the folder name pointing to the right. If you click on this arrowhead (which is pointing to the right) it will change to an arrow pointing DOWN ("v") and will display below, indented, the names of all the FOLDERS in that folder. Thus you can view the contents of any folder on any memory device connected to your computer. If you connect another drive, for example, to your computer, that drive or disc will be given a letter (such as "E" or "F") which is a folder. You will see it appear in the

folder list on the left probably at the bottom of the list. You can explore all you want to look to see what is in any folder on your computer. But remember that YOUR stuff, YOUR files, are in folders put there for YOUR use – such as "Documents" (or "My documents"), "Pictures", "Music", etc. Windows has and needs hundreds of other folders to store their stuff too, so do not go changing any files or folders in their folders, stay in your folders. Although any folder may contain ANY kind of a file, the folders provide for you with Windows means you should put all photo files into "Pictures" all documents into "Documents", etc.

So you can see that folders, which can contain files and more folders, are organized like an "outline" that you did in grade school. You have Roman numerals I, II, III, IV, etc. and under each of these you have the capital letters A, B, C, etc. and under each of them could be numbers 1, 2, 3, etc. Each level is indented slightly to show you visually that a list is contained within the element above, etc. Folders are LOCATIONS in your computer memory into which you put your FILES (or more folders).

Now it's your turn. Open your Windows Explorer or File Explorer app and open some folders to see what is inside them. Use the scrollbars (if they appear) to scroll up and down the lists. When you have clicked on a folder, the contents of that folder will appear in the right pane. Click on some arrows to see how you can list the folders in a folder. Try to stay within your "Documents" or "Pictures" folders. Doing this will only display what you have and will NOT CHANGE anything, so don't' worry about messing anything up. We will get to moving things around later.

Next time we will look at the different ways to VIEW or display the contents of a folder, and this also will not change anything either, so it is safe to play with different display options. If you want to learn more right away, use Google and view some videos. Learning the basics of Windows File Explorer puts you in the driver's seat of your computer.

From the July 2016 issue, Sarasota Technology Monitor, www.thestug.org, jimcerny123@gmail.com.

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

What's New

Energi Charger Station

by George Harding Treasurer
Tucson Computer Society

Here's a handy charger for you. It can charge five devices at once! It senses your device capability for charging and adapts to it. It works with small and large devices. It has a removable external charger.

Tylt offers this product to their long line of innovative tools. I have an external charger for my iPhone that is both a case and a charger. The case provides the usual protective features. The charger fits around the case and connects by the built-in lightning connector. Pretty slick!

Energi is another example of innovative engineering for consumer devices. The main unit connects to a standard wall outlet and provides five USB slots for charging your devices. Each is capable of charging either a smartphone or similar device or a tablet.

Each slot has what the Company calls SmartDetect technology to provide maximum rapid charging. That means both fast charging and no over-charging. The latter benefit is important in today's environment of concern for fires caused by over-charging. The four standard USB slots provide 2.4 amps of power while the fifth slot can provide 3.5 amps for even faster charging.

A unique feature of this charging station is the removable battery pack (the fifth slot). It can be easily removed and carried in a pocket or purse for on-the-spot use. No need to find a wall socket when you run out of charge.

The fins on the top of the unit can be used to organize your cables whether because there are too many or they are too long.

The unit comes with a start-up guide which is very short, with diagrams as well as text in several languages. The unit comes with a one year warranty after you register your unit. Energi Charging Station by TYLT, Price $80, www.tylt.com/charging-station

Review provided by www.aztcs.org, georgehardingsbd@earthlink.net.

Crypto Simulation

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

Most children are fascinated by encryption; certainly, I was. I still remember having to ask my dad for help in learning to use my Captain Midnight Code-O-Graph, which encoded messages by replacing letters with numbers. Given the popularity of documentaries and movies about the British efforts to decode German Enigma messages during World War II, many adults, including me, retain this interest. Understanding modern encryption requires a sophisticated math background, and slogging through a description can be truly tedious. The simple mechanical devices used during World War II are more approachable and have much historical interest. A fascinating way to learn about them is to run simulations on your PC. You can follow the same procedures and tap the same keys that WWII German and American soldiers did, and by doing so obtain a much better understanding of the processes than by watching a movie or reading a book.

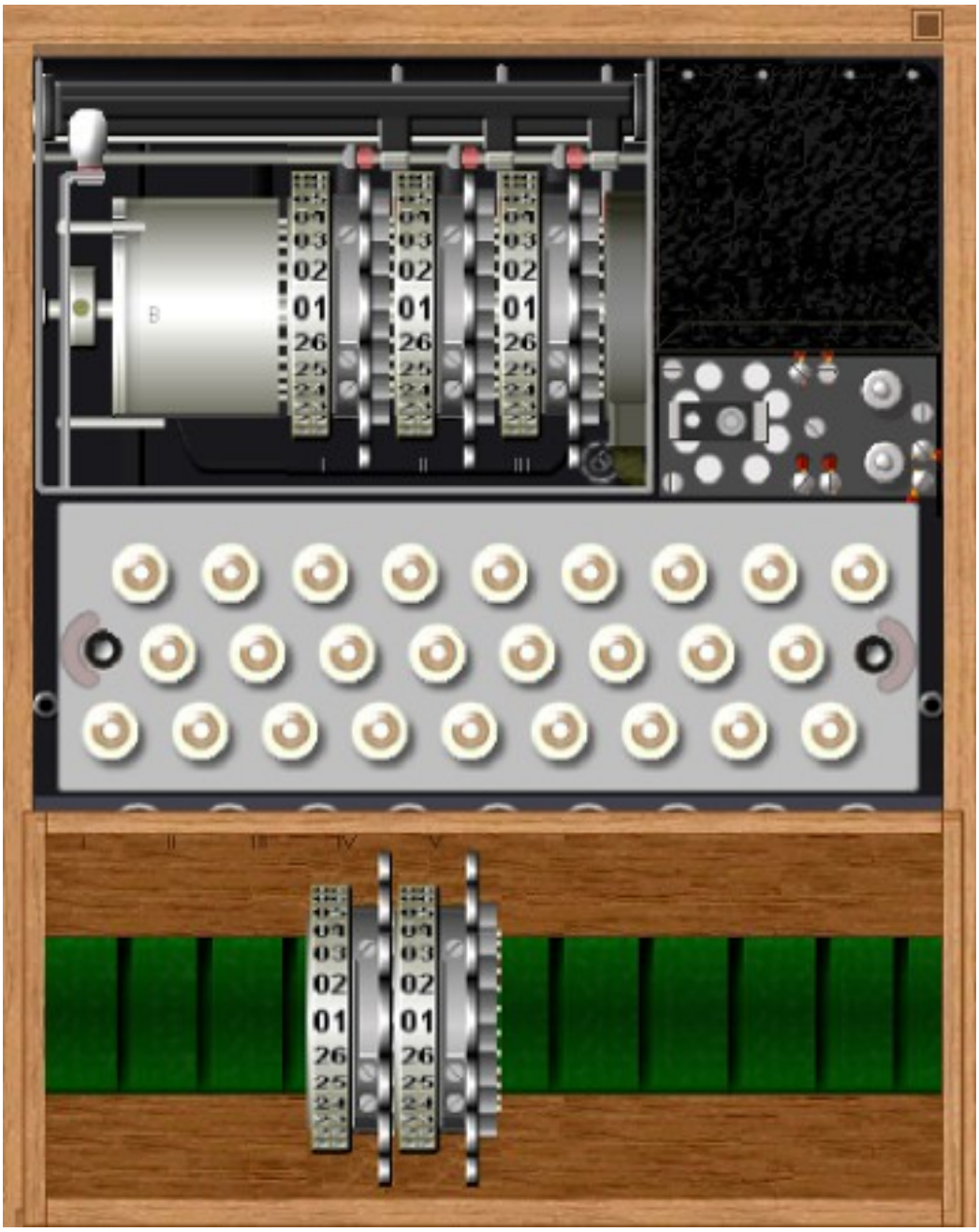
The Enigma is probably the most famous cryptographic device ever. Not only was it effective at the time, but it also significantly influenced World War II. Thousands died as a result of the successes and failures of attempts to decrypt messages encoded by it. The best way to learn about Enigma is to use one. While actual units are available, they are expensive. Instead, you can download an excellent free simulator from http://users.telenet.be/d.rijmenants/index.htm, a site in Belgium maintained by Dirk Rijmenants. Here you can find simulators for several historic crypto machines, instructions for using them, and their histories. These are Windows programs, but OS X users can run them using Crossover and Linux users with Wine. Like all similar devices of that era, the Enigma is a mechanical device, which used a set of disks to scramble the connections between the 26 letter keys of a keyboard and 26 lamps. At least one disk moved at each key press, so that pressing the same key twice produced two different output letters. A battery was needed only to illuminate the lamps. Mechanical connections between the keys and the rotors moved the latter.

Screen 1. Enigma Panel.

Screen 1 shows the keyboard, the (unlit) output indicator lamps, the edges of the three rotors, the power switch, and the terminals for external power. There are some complications, but basically the operator selected three (of the five available) rotors and inserted them in the correct order. Then he rotated them to a given starting position and began typing. The indicator lamps remained lit only while the key was pressed, and a second operator was needed to record the output.

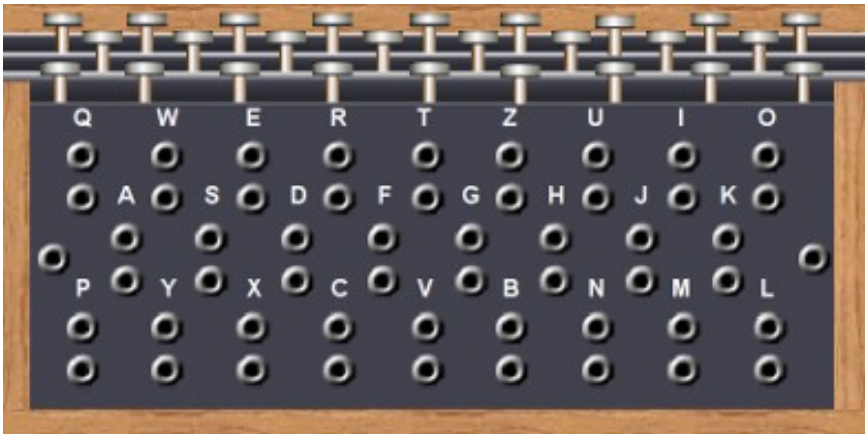
Screen 2 shows the same machine with its cover lifted. The three installed rotors are at the top and the two unused ones in a rack at the bottom. The unused rotors were stored in a separate box, which the simulator shows sitting on top of the keyboard mechanism. The empty space to

the right of the rotors is for the battery.



Screen 2. Enigma Interior.

A further complication was provided by a plugboard, Screen 3, that scrambled the connections between the keyboard and rotors. The simulator also includes this feature to allow setting the Enigma up exactly as it was used.



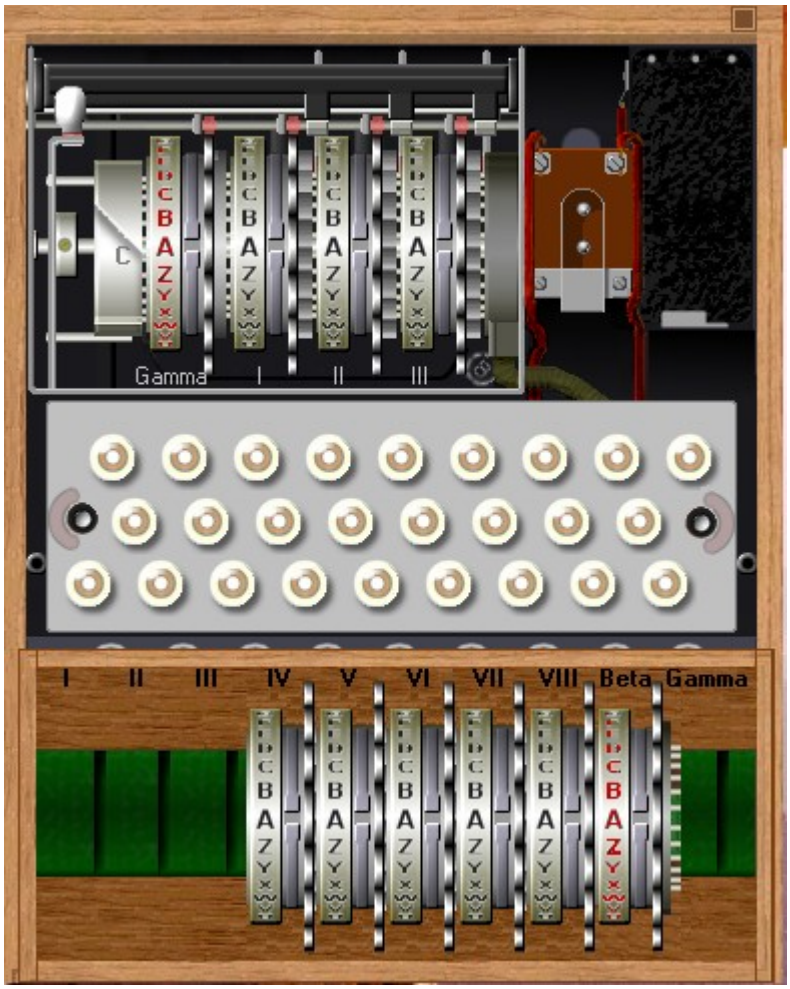
Screen 3. Enigma Plugboard.

Enigma was really a family of devices. Screen 4 shows a model used by the German navy. It had no internal battery, and used a plug instead of screw terminals for power.

Screen 4. Enigma Model Used by the German Navy.

This used four rotors instead of three, and as a result was more secure.

Screen 5. Interior of the Navy Enigma.



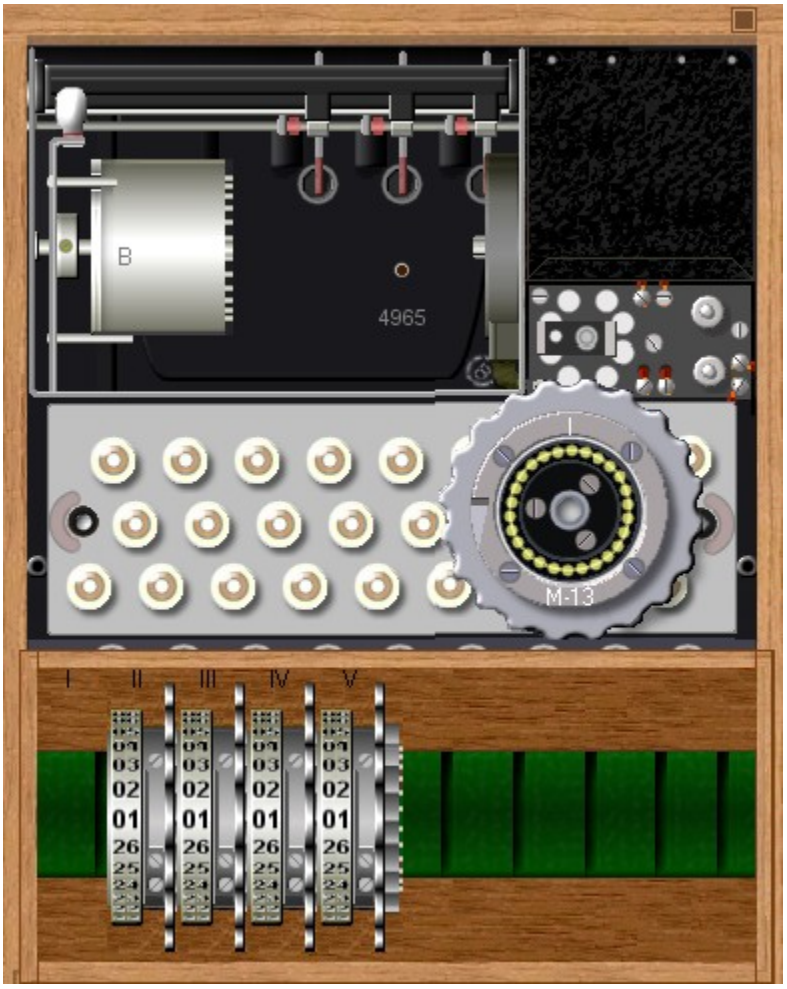
As shown in Screen 5, navy operators had more rotors to choose from, although only the Beta and Gamma units (those with red letters) could be used in the fourth slot.

To see how the Enigma was used, let's work through an example. The first step is to consult a codebook, Screen 6, for the machine settings of the day. There was a separate page for each month, with a line for each day (Tag in German). Using the sample, we see that for the 30th of this month we are to use rotors I, V, and VI, with offsets of 13, 23, and 02, respectively. The offset is how much the rotor should be rotated with respect to its outer numbered shell. (If you download the Enigma simulator, be sure also to get the Enigma Code Book Tool, which generated this example.)

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
30	I V IV	13 23 02	AZ BS CJ DU EV GO HR IQ KT LN	AHA LUO XXF AMU
29	I V IV	14 18 01	AO BC DH IJ KZ MR PV QU SX WY	JHB FVC PBT XPW
28	I IV V	08 01 24	BR DM EZ FW GI HY JO KT LU NQ	YHS JIQ FKY AVU
27	III II V	13 24 04	AV BQ CO FX HK IP LY NW SZ TU	KKM DXA JHF CII

Screen 6. Enigma Codebook Sample.

Screen 7 shows a rotor I removed from the case (by right-clicking on it) and offset by 13 (with repeated clicks on the upper part of the rotor). We'll put it back in the case by right-clicking on the empty position and then set rotors V and IV similarly.

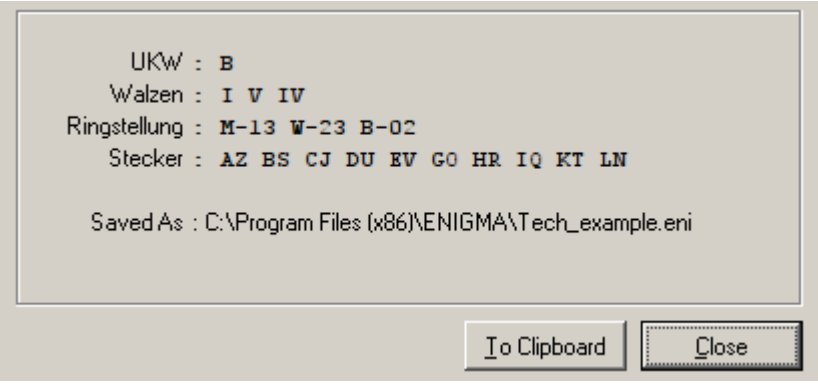


Screen 7. Enigma Being Configured.

The Steckerverbindungen column shows the plugboard connections. It tells us to swap A with Z, B with S, and so on. On the simulator, click on the lower edge of the keyboard to show the panel, Screen 8. (Note that the jacks are arranged like a QWERTY keyboard.) On the actual machine, A and Z would be swapped by connecting the A and the Z jacks with a cord; on the simulator, just click first on A then on Z. The screen-shot shows the panel set-up complete. Note that the A-jack pair is covered with a black shape labeled Z and that the Z pair has a shape labeled A. This is true for all 10 swaps called for in the codebook.

Screen 8. Configured Plugboard.

The simulator provides a check of the setup -- shown in Screen 9. It shows we've used a B reflector (the cylinder to the left of the rotors and the only one available for this model), the arrangement of the rotors, their offsets, and the plug settings. It also allows us to save the settings for later use.



Screen 9. Enigma Simulator Check Screen.

While the settings from the codebook were typically used for one day, each message has its own key. To send a message, the sender first chose two three-letter keys, for example XPH and FWT and used the first to encode the second. In effect, XPH is the key for a three-letter message. For Enigma, a key is the initial setting of the three rotors. Although the keys are specified as letters, the rotors are labeled by numbers, so there was a table attached to Enigma relating the two. The simulator can display this, as shown in Screen 10. The window at the bottom shows the input and output, where we see that FWT has been encoded as WRC. The sender then composes a message header, such as the one shown below.

F7Z DE WN 1340 = 38 = XPH WRC =

Screen 10. Enigma Simulator in Use.

The sending station is WN; the receiver is F7Z, the time is 1340, and there are 38 characters in the message. Only if the receiving Enigma is set up exactly the same as the transmitting one, will it produce the correct message key, and because only three characters are coded, breaking it is nearly impossible. (Although some lazy operators reused keys, and the British made use of this.) The transmitter now resets the rotors to FWT and encodes the message, in this case, "Preserve wildlife. Pickle a squirrel." Note that there are no number, punctuation, or space keys. Words will be run together, and we'll use X to end sentences, as did the Germans. If there were digits, we would have to spell them. A complete encrypted message appears below. As is customary the letters shown as five-letter code groups, and they were sent this way via Morse code.

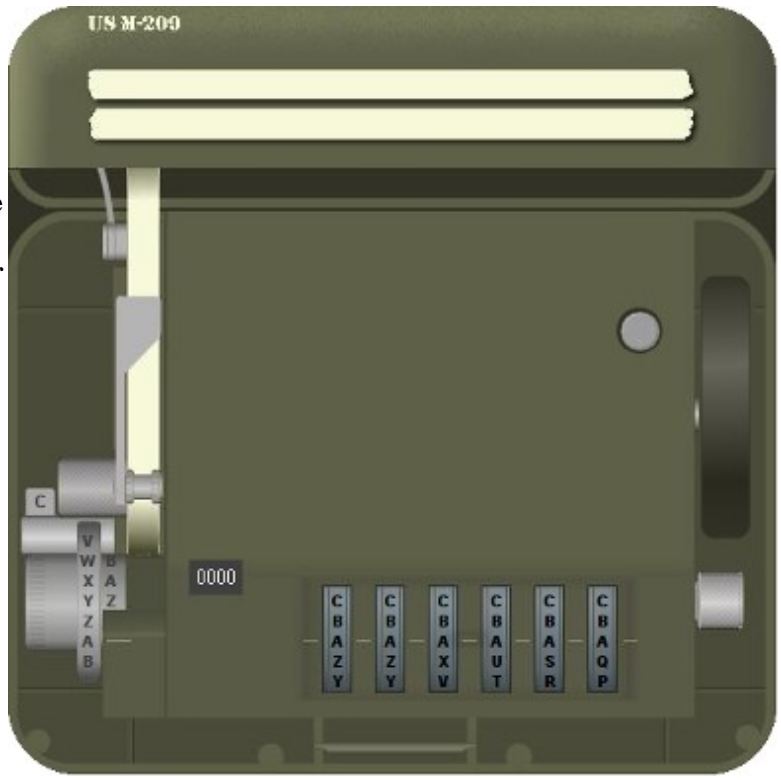
F7Z DE WN 1340 = 49 = XPH WRC =
RTXXF GXBZV GNOVX VFMKK GIXMT SEFLM IVUFW IMG.

The first code group shows which codebook setting was used. (Note the column "Kenngruppen" in Screen 6.) The operator chooses one of the entries for that day and prepends two random letters to make a five-letter code group. Although this group is included in the word count, the receiver doesn't enter it. It sets the rotors to FWT and enters the coded message to produce the result, "PRESERVEWILDLIFEXPICKLEASQUIRRELX". Some punctuation could be represented as letter groups, but we'll skip over that in this quick introduction.

Hopefully, this brief discussion has given you some idea of what the Enigma really did. A few experiments with the simulator will make things much clearer, as will a few minutes spent exploring the Website.

Fortunately for the Allies, the Germans greatly overestimated the strength of their machines. Their primary error was in thinking that its construction was secret, when in fact the allies obtained working Enigma replicas from the Poles in 1939 and captured several during the war. In addition, some operators, especially in the Luftwaffe, were careless or poorly trained, and this allowed the British in particular to deduce codebook settings and changes in the equipment. Finally, many services used the same codebooks, and some, such as trawlers who were providing weather information in the North Atlantic, were vulnerable to capture.

The U.S. rough equivalent of the Enigma was the m-209, although it was known to be much weaker, as the Germans could decode its messages in about four hours. It was thus used only for tactical communications; strategic information was encrypted using other means. The m-209 was smaller (about 3 x 5 x 7 inches) than the Enigma, did not need a battery, and printed its output on paper tape, making it usable by only one operator. Besides being cryptographically weak, it was tedious to configure and slow to use. Despite these drawbacks, it was used through the Korean War and well into the 50s. *Like the Enigma, you can buy models of the m-209, but a better approach is to experiment with a simulator from the same Website that has the Enigma simulator*. Screen 11 shows the simulator view that an operator would see while using it.



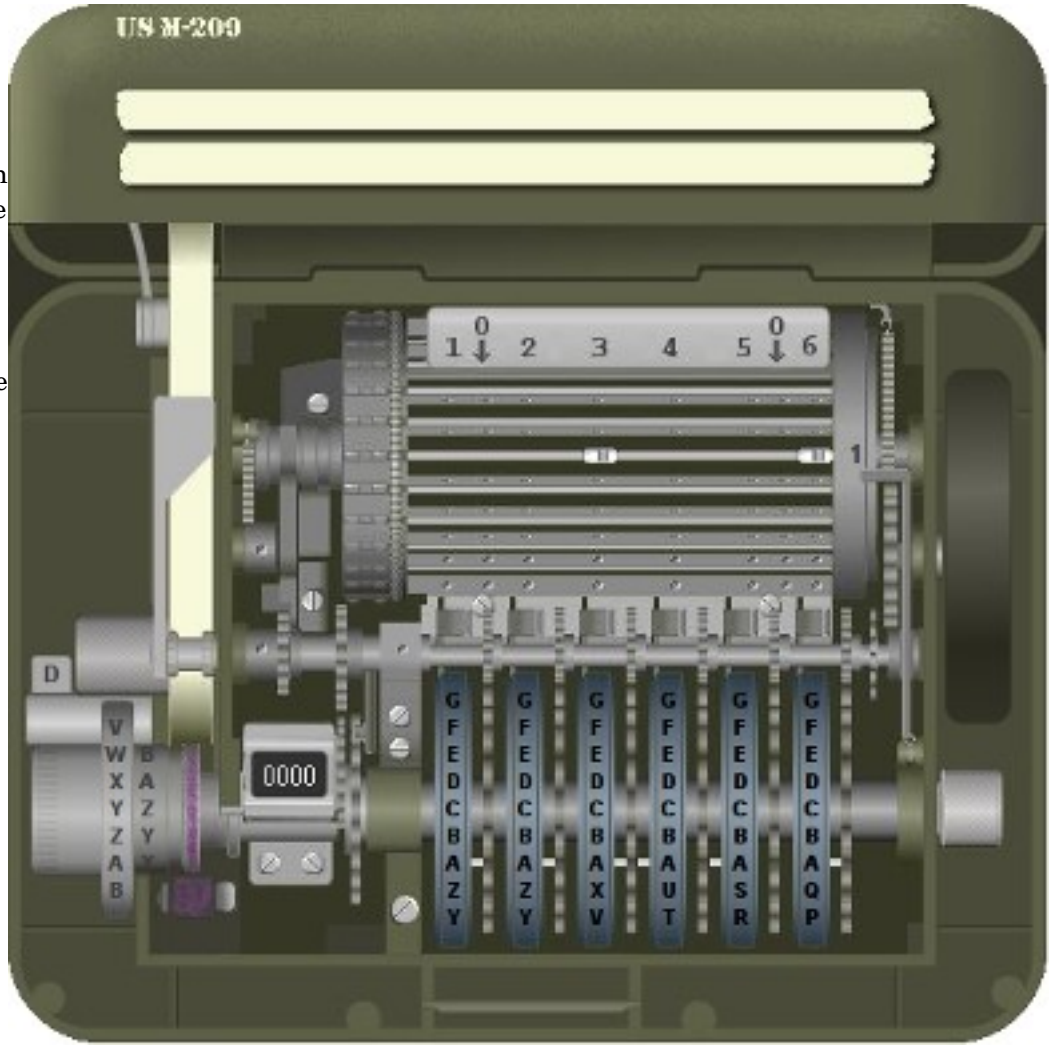
Screen 11. m-209 Crypto Machine.

Characters are entered by twisting the knob at lower left until the desired letter is opposite the index (A in this case). Then the black lever on the right is pressed. This advances the six rotors (visible at the bottom) and prints the output letter on paper tape (to the right of the input wheel). The simulator displays two tapes at the top; the upper one is a record of the input characters, and the lower one the output. The current output character is also visible just to the right of the input wheel (Z in this case). There is also a character counter (here showing 0000), and a round button to reset the machine. Finally, just above the input wheel is a tab marked C, showing the machine is in encrypt mode. This must be flipped to D for decoding.

You can get a hint of how tedious it is to set up the m-209 from its internal view, Screen 12.

Screen 12. m-209 Crypto Machine Interior.

If you look carefully at the rotors, you can see small pins in the A row. Think of a pin to the right as a one and a pin to the left as a zero. The A row thus is set to 111001. However, setting the rotor pins is only part of the configuration. There are also 27 bars, each with two sliders that must be set. Here Bar #1 has been set to 36. Screen 13 shows a complete setup, typically used for one day.



```
------------------------------      --------------------
NR LUGS  1  2  3  4  5  6           BAR 1  2  3  4  5  6
------------------------------      --------------------
01 3-6   A  A  A  -  -  A           01  -  -  X  -  -  X
02 0-6   B  -  B  -  B  B           02  -  -  -  -  -  X
03 1-6   -  -  -  C  -  -           03  X  -  -  -  -  X
04 1-5   D  D  -  -  D  D           04  X  -  -  -  X  -
05 4-5   -  E  -  E  E  -           05  -  -  -  X  X  -
06 0-4   -  -  -  F  F  -           06  -  -  -  X  -  -
07 0-4   -  G  G  -  -  -           07  -  -  -  X  -  -
08 0-4   H  -  H  H  H  H           08  -  -  -  X  -  -
09 0-4   I  -  -  I  I  -           09  -  -  -  X  -  -
10 2-0   -  J  J  -  -  -           10  -  X  -  -  -  -
11 2-0   K  K  -  -  -  K           11  -  X  -  -  -  -
12 2-0   -  L  L  -  -  -           12  -  X  -  -  -  -
13 2-0   M  -  M  M  M  -           13  -  X  -  -  -  -
14 2-0   N  -  N  N  N  N           14  -  X  -  -  -  -
15 2-0   -  O  -  -  -  O           15  -  X  -  -  -  -
16 2-0   -  -  -  P  P  -           16  -  X  -  -  -  -
17 2-0   -  -  -  -  -  Q           17  -  X  -  -  -  -
18 2-0   -  R  R  -  -              18  -  X  -  -  -  -
19 2-0   S  S  S  S  S              19  -  X  -  -  -  -
20 2-5   T  -  T  T                 20  -  X  -  -  X  -
21 2-5   -  U  U  U                 21  -  X  -  -  X  -
22 0-5   V  -  -                    22  -  -  -  -  X  -
23 0-5   W  X  X                    23  -  -  -  -  X  -
24 0-5   -  -                       24  -  -  -  -  X  -
25 0-5   -  -                       25  -  -  -  -  X  -
26 0-5   -                          26  -  -  -  -  X  -
27 0-5                              27  -  -  -  -  X  -
------------------------------      --------------------
TNJUW AUQTK CZKNU TOTBC WARMI O
------------------------------
KEY LIST INDICATOR: XA
------------------------------
```

Screen 13. m-209 Configuration Table.

If a letter appears, the pin in that row should be to the right (or set to 1); a dash indicates that the pin should be to the left (or set to 0). Note that rotor 1 has 26 letters, rotor 2 has 25, rotor 3 has 23, rotor 4 has 21, rotor 5 has 19, and rotor 6 has 17. The LUGS column shows the slider positions on each bar, and the table on the right also shows this, but in a different form. It's a real credit to our soldiers that they were able to perform this intricate configuration under combat conditions. I need several tries to do it at home, in an easy chair, with soft music and a cup of coffee.

When complete, the operator would set the rotors to AAAAAA and encode 26 As. If correctly set up, the result should be the 26-letter sequence below the tables. Every configuration was assigned an indicator (XA for this one) that was attached to the encrypted messages, and the receivers used this to be sure that had their equipment properly configured.

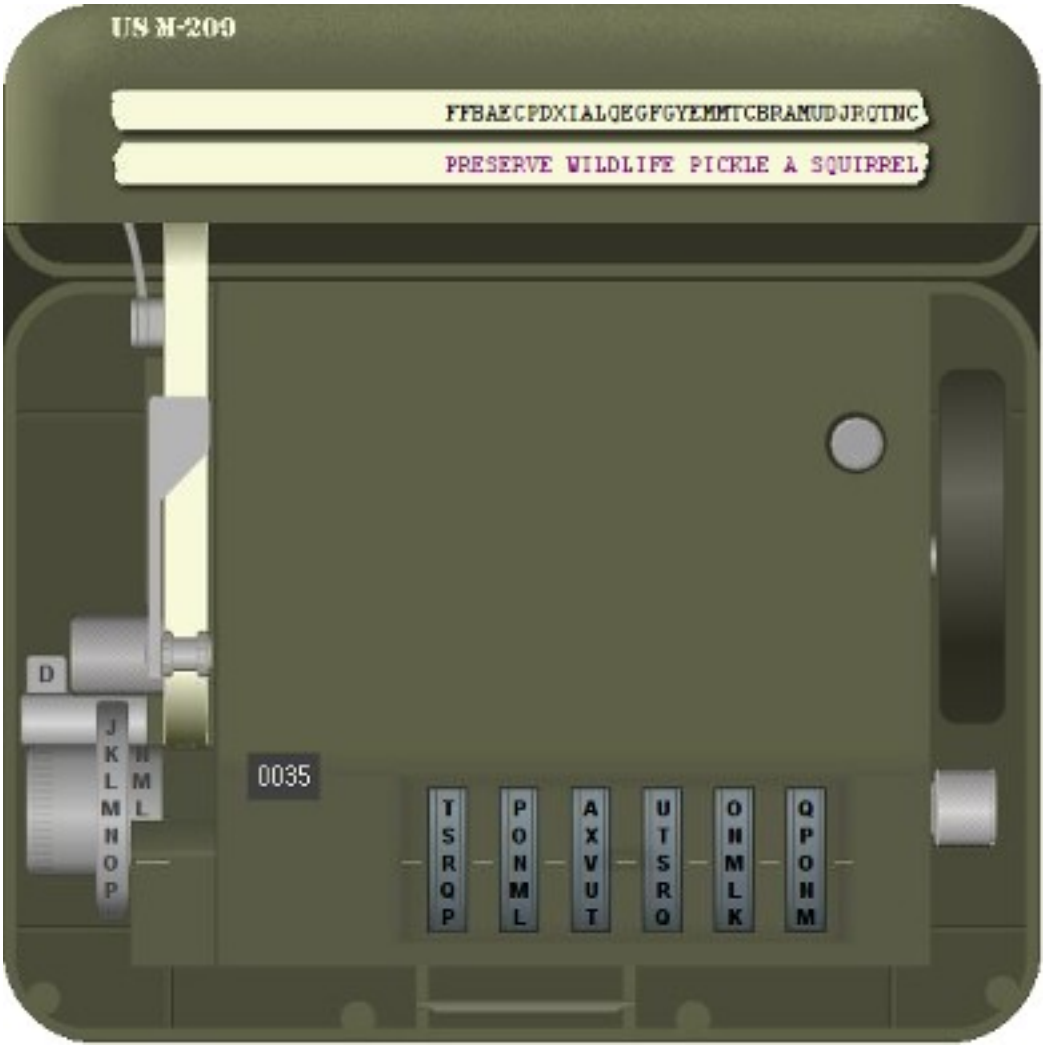
Because it's so tedious and repetitive, I won't go through a configuration. Download and run the simulator if you want to experience this. I do think it will be helpful to run through encoding and decoding a message. For this, assume the machine is configured as described above. Like his German counterpart, the American soldier had to generate message key, and he used a similar procedure, encrypt the message and include an encrypted version of it with the message. Only if the receiver has an m-209 with the identical configuration can he recover the key to decrypt the message.

Again, we'll send the message, “Preserve wildlife. Pickle a squirrel.” We choose CVQIMK, set the rotors to it and encode SSSSSSSSSSSS to produce IDJWE PNWFW XU, which will be our key. Our message will include both CVQIMK and SS, so the receiver can generate the same message key. Why 12 characters when we need only six? Recall that most of the rotors have fewer than 26 characters. In this case, when we go to set the machine, we'll find there is no W on rotor 4, so we'll just skip that letter. As a result, the actual key will be IDJEPN. The Americans replaced every space with a Z, but had no standard for punctuation. (If every sentence ended with “PERIOD,” it would aid those trying to break into the messages.) We'll just eliminate the periods in this simple example. Our input becomes PRESERVEZWILDLIFEZPICKLEZAZSQUIRREL, and produces FFBAE CPDXI ALQEG FGYEM

MTCBR AMUDJ RQTNC. However, we have to add SS CVQIMK XA, where SS shows the letter we used to produce the key, CVQIMK is the setting to produce the key, and XA is the setup. We'll regroup these 10 letters to SSCVQ IMKXA, because encrypted messages always appear as five-letter code groups. We'll also repeat this important information at the end of the message. Thus, the complete message becomes the following.

SSCVQ IMKXA FFBAE CPDXI ALQEG FGYEM MTCBR AMUDJ RQTNC SSCVQ IMKXA

The receiver uses an identical procedure to develop the message key. That is, he sets his rotors to CVQIMK and encodes SSSSSSSSSSSS to produce the message key. He too has to discard a W. He then flips the code/decode tab to D and enters the encrypted message. Screen 14 shows the result.



Screen 14. m-209 Simulator in Use.

Note that the m-209 has replaced Zs with spaces. They would also be replaced in such words as “zero,” but this would be evident from the content.

A little experimenting with these simulators will reward you with a better understanding of the difficulties of communicating securely before the computer age.

From the September 2016 issue, BUG Bytes, www.bcug.com, n2nd@att.net.