Midland Computer Club

Midland Michigan

BITS AND BYTES

October 2016

http://mcc.apcug.org/

President Piper's Ponderings....

October's Midland Computer Club meeting will be the most important meeting of this year, or any year in the history of our Club.

First, our topic is very timely to living in the Digital Age. It is titled *Personal Privacy* presented by Joe Lykowski. Joe will be talking about how the digital devices you own or may be considering buying can be used against you. If you want a preview of some of Joe's topics, go to Google and type in "WiFi" in conjunction with words like "pineapple" or "rubber ducky" or "LAN turtle". This is a subject that will help you understand the inherent dangers in using any device connected to the Internet, including such things as your refrigerator and your car.

Secondly, our Board has reached the decision that, due to a number of circumstances, the best course of action is to formally dissolve the Club, but continue to meet in an informal setting.

If this sounds either exciting and/or confusing, then come and hear the details. I have given you some background (and homework) by posting a correspondence I had with John Kennedy, our Regional APCUG representative. You can see this letter on the Club website (under **/Piper** folder), in a link **APCUG Letter** for September.

I hope to see you Wednesday, October 26 at our General Meeting.

(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)

GENERAL CLUB MEETING

Midland Community Center, 2205 S Jefferson Ave, Midland MI
Room K111, Barstow Shipps Wing

Wednesday, October 26, 2016
7:00 P.M.
Topic: Personal Privacy - Joe Lykowski

2016 BOARD MEMBERS

MCC OFFICERS

President	Larry Piper	larryp56@chartermi.net
Treasurer	Jan Ensing	btiger6@yahoo.com
Membership	Gary Ensing	btiger6@gmail.com
Editor & Webmaster	Carol Picard	webbyte@yahoo.com

AT-LARGE BOARD MEMBER

Joe Lykowski joseph@lykowski.com

PROGRAM COORDINATORS

Howard Lewis lewis3ha@chartermi.net
Bill Tower tower.w@gmail.com
Please let Howard or Bill know of topics you would like covered at future meetings.

PUBLICITY

Al Adams aladams12@yahoo.com

Board Meeting

First Thursday of the month
7:00 PM
Chapel Lane Presbyterian Church,
5501 Jefferson Ave., Midland MI

FREE - APCUG 2016 FALL VIRTUAL TECHNOLOGY CONFERENCE (VTC)

Saturday, November 5
1:00 – 4:00 pm ET

Attend the FREE conference from the convenience of your own home! All you need is your computer, tablet, etc. and Internet access. The sessions are 50 minutes in length and offer attendees the opportunity to ask questions via Q&A; the questions are answered by the presenter at the end of the presentation or via e-mail if there isn't enough time after the presentation.

APCUG uses ZOOM for the VTC webinar presentations (www.zoom.us). If you have not participated in a VTC, go to https://zoom.us/download to download the app for the device you will be using to 'attend' the conference.

Videos from earlier conferences can be found on APCUG's YouTube channel www.youtube.com/apcugvideos.

- To register for this VTC, please click on the below link:
  https://apcug-fall-2016- vtc

Educational, Fun, and Interesting Web Sites: (submitted by Howard Lewis)

With the 2016 elections right around the corner, the following websites may help you make your decision for voting. The first group of sites are non-partisan sites to check out the candidates. The second group are websites for specific candidates and the third group are websites for the various political parties on the November ballot. Whatever your decisions are for the various positions, make sure that you vote on **November 8**!

Non-partisan sites:

http://www.vote411.org/ League of Women Voter candidate information on your ballot
https://ballotpedia.org/Main_Page Find candidate information on your ballot
http://www.factcheck.org/ Fact check the candidates statements
http://www.politifact.com/ Fact check the candidates statements
http://www.snopes.com/ Fact check the candidates statements
http://www.politico.com/ Inside information on politics
http://ontheissues.org/default.htm
http://votesmart.org/ Get the facts on a candidate
http://www.opensecrets.org/ Find information on candidate funding

Official candidate websites:

President:
https://www.hillaryclinton.com/ Hillary Clinton/Tim Kaine website (Democratic)
https://www.donaldjtrump.com/ Donald Trump/Mike Pence website (Republican)
https://www.johnsonweld.com/ Gary Johnson/Bill Weld website (Libertarian Party)
http://castle2016.com/home/ Darrell Castle/Scott Bradley website (US Taxpayers)
http://www.jill2016.com/ Jill Stein/Ajamu Baraka website (Green)
http://www.rev16.us/ Mimi Soltysik/Angela Walker website (Natural Law)

U.S. House (Michigan 4th Congressional District)
http://johnmoolenaarforcongress.com/ John Moolenaar website (Republican)
http://www.wirthforcongress.com/ Debra Wirth website (Democratic)
http://www.leonardschwartz.us/ Leonard Schwartz website (Libertarian)
http://jordansalviforcongress.com/ Jordan Salvi

Official national political party websites:

https://www.democrats.org/ Democratic National Committee
https://www.gop.com/ Republican National Committee
http://www.lp.org/ Libertarian Party
http://www.constitutionparty.com/ Constitution Party
http://www.gp.org/ Green Party
http://www.natural-law.org/ Natural Law Party
http://workingclassfight.com/ Working Class Party

Official Michigan websites
http://www.migop.org/ Michigan Republican Party
http://www.michigandems.com/ Michigan Democratic Party
http://michiganlp.org/ Michigan Libertarian Party
http://ustpm.org/ US Taxpayers Party (the Michigan branch of the Constitution Party)
http://www.migreenparty.org/ Michigan Green Party

ARTICLE INDEX

Back to Basics - Changing to another Email Service

By Jim Cerny, Chairman, Forums Committee, Sarasota Technology UG, Florida
June 2016 issue, Sarasota Technology Monitor - www.thestug.org - jimcerny123 (at) gmail.com

Almost all computer users use email – and you are one of them, right? Have you ever had to change your email address or change to another email provider? Recently here in Florida (and I hear in Texas and California as well) our internet provider Verizon has been taken over by Frontier. As a result of this, EVERYONE had to change from Verizon to AOL for their email. Fortunately their Verizon email address will continue to be accepted by AOL (for now). The purpose of this article is to help you understand what steps are needed to change to another email. I do recommend Gmail because it comes with several other tools provided by Google and you most likely will never have to change to another email address.

Your first task is to go to the website and establish a new email account -- that is get your new email address and password. Please write it down and do not lose it! Once you have your new email ID your major concerns are forwarding your old emails to your new email address, getting your address book (or contact list) to your new email and to notify everyone of your new address. Some emails (such as Gmail) may ask you what your other email address is and automatically bring your contact list and forward any emails from your old address to your new address. They want your email business. But if your address book is not copied over for you then you will have to do it yourself. By all means "ask Google" how to do it. For example, ask Google "How do I get my AOL address book to my Gmail contacts?" What you will most likely have to do is to create a file of your address book by "exporting" it and giving it a file name, then copying that file by "importing" it into your new email. After you do this you need to examine your entire address book, name by name, to see that all the data was copied correctly. You will probably have some editing to do to straighten things out. For example, some phone numbers may not have been copied over or a nickname may have been placed as the last name, etc.

Next it is helpful to have all your old email "forwarded" to your new email address. This way you do not have to hurry to notify everyone on your list that you have a new email. If this is not possible, you may

have to go into your old email and actually forward those important emails to your new email. From now on, only use your new email address.

Finally, send a nice email to everyone telling them your new email address. It also is essential that you read the “help” or “options” for your new email so that you are aware of how to create new email folders, sort your emails, find emails, etc. Although every email can do these basic functions, how it is done may be different on different emails. And if you are converting to Gmail, be sure to check out the many apps that are available to you with your Gmail account ID. Now you are ready to enjoy using your new email.

One word of caution -- what if you have used your email address to establish accounts with various on-line businesses or services? Movie channels, banking, club memberships, etc. may be using your OLD email address as your account ID. Unfortunately, all of these accounts must be changed to your new email ID. This may entail you having to enter all new passwords for all these accounts as well. This can be a real pain if you have many accounts, but there is really no other way around this, sorry. Be sure to write down ALL your IDs and passwords for EVERY service or app which requires an account.

Good luck and please don’t forget to Ask Google anything about your email. You will find very helpful instructions and videos to guide you. Now here’s hoping that you will never have to change your email address again!

Device Transparency (DT)

By Eric Moore, President, Computer Users’ Group of Greeley, CO
May 2016 newsletter, Random Access - www.cugg.org - moore.e.s@att.net

As computer users increasingly have multiple devices—laptops, desktop computers, tablets, smartphones—on which they keep important data, being able to seamlessly access a file from any location or device becomes a challenge. Say if you are on a business trip with your laptop and smartphone, but realize you forgot to copy a report from your desktop computer to one of your mobile devices, you may find it a challenge to get what you need. Remote control software such as LogMeIn can allow you to remotely connect to the computer to download the file you need. Dropbox provides a means of sharing files with yourself and others through a cloud-based storage. VPNs and collaboration services such as Microsoft SharePoint are other possibilities for getting access to a file you need while away from home or the office.

"Device transparency" (DT) is a concept which could provide a seamless means of managing your files from any of your devices. Whether you need to transfer a photo from a smartphone to your laptop, play a music file residing on a Mac PowerBook on your Android device, or access a Word document from home on your tablet computer, device transparency would make this all possible. In a paper published at http://www.brynosaurus.com/pub/net/devtransp.pdf, researchers with MIT and the Max Planck Institute for Software Systems describe how such an ideal service would function. (At the time of the paper’s writing, there was no service they were aware of that provided all of these features they propose.)

To summarize, the service would provide a means by which "metadata"—information about your files—would be shared between your devices. Such information would include the file types, names, and on which devices the files are stored. Without you needing to be consciously aware of where a particular file is located, you would be able to download the file from the device on which it is stored and open it on any other device you are using (provided it has sufficient storage space). The only requirement is that the device that has the file you need is "linked" into the file sharing service, is powered on, and has an active Internet connection.

Adobe DC to some extent has such features, although it is geared toward working with PDF documents. Services such as Dropbox are available for multiple devices and operating systems, so they can to some extent meet such needs, provided you carefully configure the software on each device to share the files you need. One downside to sharing your files through Dropbox is that they must be uploaded to the "cloud"—which is simply a server that the vendor provides for storing your files. This may be a privacy

concern, depending on the contents of the files, and could be costly in terms of the amount of storage space required (especially if you have a large music or photo collection). DT would mitigate this issue, as the files would not be stored in the cloud. It would also alleviate the need of every one of your devices synchronizing copies of all your files. Instead, the sharing of metadata would enable every device to be "aware" of your complete collection of files, so you can download what you need when you need it. Although the metadata may require many megabytes of storage, it would not be nearly so great as the storage space for the files themselves—especially high-fidelity photos, movies, and music files—which could require hundreds or thousands of megabytes of storage.

Device transparency is an interesting concept which could revolutionize how we work with our multiple computing devices. I am interested in seeing if such a service is developed sometime in the future. Depending how well-designed (easy-to-use) it is, and what measures are taken to protect users' privacy, I might consider using such a service for my laptop, desktop PC, and tablet computer.

Google Virtual Tours

Geof Goodrum, Potomac Area Technology and Computer Society
May 2016 Issue, PATACS Posts - www.patacs.org - Director1(at)patacs.org

Explore and plan travel with Google Street View!
https://www.google.com/maps/streetview/

Google Data Center, Lenoir, NC
Google provides a guided video tour and Street View virtual access to its data center in Lenoir, North Carolina.
https://www.google.com/about/datacenters/inside/streetview/

McMurdo Station, Antarctica
Take a walk inside the Crary Science Center.
https://www.google.com/maps/streetview/#antarctica/crary-science-center

Yosemite National Park
Hike the steep and well-named Mist Trail.
https://www.google.com/maps/streetview/#us-national-parks-and-historic-sites/yosemite-national-park-mist-trail

The Bluebird Cafe, Nashville, TN
Famed local venue for Nashville's songwriters and musicians.
https://goo.gl/maps/a7u7yE36RKK2

Ransomware - Protecting your ability to recover from an attack

John Langill, Newsletter Editor, STPCC (Southern Tier Personal Computing Club)
June 2016 issue, Rare Bits - http://www.pageorama.com/?p=stpcc1979jlangil1 (at) stny.rr.com

A recent posting to Yahoo.com reminded me that the key element to recovering from a ransomware attack is to have a reliable system image backup. Most computer users — you among them, I'm sure — are aware of this and have diligently performed regular backups. Some may have chosen to back up their systems to a Cloud-based service for which, if their backup files are sufficiently large, they pay a monthly fee based on the storage capacity required. Others have preferred to keep things "close to the vest" and store their backup files on a local external hard-drive (never, ever store backup files on an internal hard drive) for which one with a three-terabyte capacity, for example, presently costs about $100.

I fall into the latter group.

Cost aside, both methods provide protection but also have their own particular drawbacks that are too often overlooked. What will happen, for instance, if some enterprising ransomware purveyor one day successfully manages to hijack (encrypt) all the client files that have been stored with the cloud-based service. Not possible, such services say. Well, that may be but just how sure of that are you really — or are they, for that matter? And, as sure as God made little green apples, you can bet that there is at least one someone somewhere trying to do just that.

The uncertainty of cloud-based services is what led me to rely on a USB-connected external hard-drive for storing my backup files; and I have been doing so for years with a blissful — and perhaps a false — sense of confidence that they would be secure and uncorrupted should they be needed. Ok, so what's the drawback in this method? The fact is that a ransomware attack will — along with all files stored on the internal hard-drives — also hijack the backup files stored on an external hard-drive unless the drive is either powered off or physically disconnected from the computer at the time of the attack. Not a problem, said I — my USB 3.0 external hard-drive is equipped with an On-Off switch and I power it ON only for the time it takes to create a backup.

There's one other precaution I take and that's to set my cable modem to "Stand by" mode to disrupt Internet traffic during the time that a backup is created; thereby assuring that my system and external hard drives will not be vulnerable to attack while a backup is in progress.

Accordingly, I considered the risk of the backup files becoming corrupted was minimal. And all was fine and dandy until I decided to swap a relatively low-capacity external hard-drive over to my laptop PC and to install two larger capacity USB 3.0 hard-drives on the desktop PC. The problem with doing this was that the newer drives did not have On-Off switches; and rummaging around behind my desktop PC (which, despite what it's called, is actually located under a desk) to connect and disconnect the USB cables from either the drives themselves or the PC was a real pain — it's a rats-nest back there, as many will probably know.

My solution: I purchased a powered 4-port USB 3.0 hub (under $20) specifically for use with the two newly installed external hard-drives. Now, all I have to do is connect/disconnect the one cable between the hub and the PC. Fortunately, a USB 3.0 port on the front of my PC that makes this convenient and easy. The only thing I need to be careful of is making sure that the external hard-drives have both completed their respective operations before disconnecting the hub from the PC which, by the way, also removes power to the drives (i.e., acts as a defacto power On-Off switch).

Of course, if you use just one external hard-drive to store your backup files, and it has an accessible On-Off switch, you've no problem. Even if the drive doesn't have an ON-Off switch it's likely that restricting Internet access to it will be simply a matter of disconnecting the USB cable from the back of the device and that should not be much of a problem either.

Why do I have two external hard-drives? One is used to directly store backup files — which by the way, are always full system image backups — as they are created. The other serves to archive copies of previously created backups; that is, to back up my backups.

OK, so I'm paranoid when it comes to protecting my system image backups — it's not the worst of my faults. Admittedly, over the past 25 years or so, I can recall only once having to restore a system from a backup. I consider myself lucky on that score. But, with the chance of suffering a malicious attack rapidly increasing at the rate at which it is in today's world — and the risk will only get worse with time — I'd rather be overly cautious than suffer the consequences that could result from a lack of vigilance.

Virtual Reality & Augmented Reality Explained

By Sandy Berger, Compu-KISS - www.compukiss.com - Sandy (at) compukiss.com

If you want to be up-to-date in the high tech world you need to understand the terms VR and AR. They are both amazing technologies that are quickly moving into our everyday world.

Preface

It has always been a joy to be transported to a different time and place. The Greeks, Romans, and American Indians did this for their listeners by telling wonderful stories. These story tellers transported their listeners to alternative realities. With radio we were immersed in tales like Fibber McGee and Molly where we could listen and vividly imagine being right in the McGee's home. Then came movies, television, and gaming devices. These devices totally immersed us in their stories.

Now we have moved on even farther into other realities and amplified realities with two newer technologies: Virtual Reality (VR) and Augmented Reality (AR).

Virtual Reality Explained

Virtual Reality replicates an environment that lets you see and feel like you are in another world. This is generally done by wearing goggles which put a screen in front of your eyes to show you that new world. Some of these VR devices have built-in audio and vibrations and other haptic feedback that help to make the new world feel quite real.

Many have immersive 360 degree visual capabilities so you are completely surrounded by the new world. Often you can interact with that new world as when you might play a VR game. This new storytelling technique is totally immersive since you are completely pulled into the world inside the headset.

Dedicated VR devices started reaching the market in 2016. Samsung and Oculus have recently released their first everyday consumer product, the Samsung Gear VR headset. At $99 it is well-priced, but must be paired with a newer Samsung Galaxy smartphone to make it work. Other VR devices like the Oculus Rift and the HTC Vive and start at $599 and require a powerful PC to work. Sony will soon release their PlayStation VR at $399.

Augmented Reality

Augmented Reality is another way to look at a different world. Instead of replacing the current reality with an alternate reality as VR does, AR adds to our current reality. So with AR, you can still see the real world around you, but certain things in your world are augmented. With AR, information about the real environment and its objects is overlaid on the real world. For instance, a nurse wearing a pair of AR glasses would be able to see everything in the room exactly as it really is. However, when he or she is ready to insert an IV into your arm, the veins in your arms would be totally visible.

AR technology is sometimes accomplished with goggles, like VR, but there are also AR applications that use lightweight glasses or partial glasses. There are also small handheld AR displays, digital AR projectors, and even contact lenses that project AR information. Several companies, including Google, are working on lasers that send information directly to the eyes.

Microsoft is working on a HoloLens AR headset that will work with Windows 10. Google is still working on their Google Glass project which will now focus on the workplace.

With AR you can interact with it through gaze, voice, and/or hand motions. If you saw the movie Minority Report and remember Tom Cruise moving information around in the air you have seen an accurate depiction of an augmented reality device.

When Minority Report came out in 2002, it was very futuristic. Now that future is already here.

Voice Control: HEY CORTANA, OK GOOGLE, SIRI & ALEXA

Phil Sorrentino, Contributing Writer, The Computer Club, Florida
http://scccomputerclub.org / Philsorr.wordpress.com - philsorr (at) yahoo.com

Remember Dragon Naturally Speaking? It was, and still is, Voice Recognition software mostly used to control the operation of a word processor like Word. Certain words were used for very specific manipulation of the cursor and the text. Naturally Speaking came on the scene and became useful sometime around 1999 to 2003, depending on how much you needed to transcribe documents into the computer. Early versions had to be “trained” by the user to recognize their individual voice, and the speed and accuracy were sometimes acceptable, and sometimes not so much. Things have really improved since then; now the manufacturer, Nuance, claims in its advertising that “Dragon is 3x faster than typing and it’s 99% accurate”. So, Voice Recognition software has really come a long way.

(For those of you, who are not familiar with Naturally Speaking, it has three primary areas of functionality: dictation, text-to-speech, and command input. The user is able to dictate and have their speech transcribed as written text, or they can have a document synthesized as an audio stream, or they can issue commands that are recognized by the program.)

Naturally Speaking is an example of a local computer application or App. All the computing needed for it to operate is on the computer that runs it. Naturally Speaking doesn’t take advantage of Client-Server technology. If you attended one of our classes, you will recall that when an application is implemented with Client-Server technology, the heavy lifting (computer processing) is not done locally, but rather at a Server that is very powerful and very fast, but remote from the Client. The remote Server is connected to the Client by the internet, which allows rapid movement of data between the Client and the Server. So the Client App runs on the local computer and is connected to the Server Software, running in the cloud, via the internet. This combination provides the total Voice Recognition & Control System. The client collects input from the user and sends it to the Server where all the really complex computing is accomplished. The Server analyses the input and develops the responses and sends them to the Client where the results are presented to the user in audio and/or display formats.

Naturally Speaking is certainly a useful product, but the voice recognition and control that has really gotten the attention of the public lately, are the intelligent personal assistants that are provided by some of the leading computer companies, Apple, Microsoft, Google, and Amazon. Apple was first on the scene with “Siri”, followed by Google’s “Ok Google”, then, with Windows 10, came Microsoft’s “Hey Cortana”, and finally Amazon’s “Alexa”.

All of these are Client-Server implementations. The Servers are somewhere in the cloud and the Client resides on your smartphone, in the case of Siri and “OK Google”, or on your laptop (or desktop, or tablet) in the case of “Hey Cortana”, or on a special device that is placed centrally located in your home, in the case of “Alexa”.

All of these assistants use a Natural Language User Interface to answer questions. You’ll need a microphone on your device to take advantage of this capability. The Client app, on the device, uses the microphone to listen for a “Wake Phrase”. After this phrase is recognized, the following intercepted speech is then sent to the Server where it is analyzed via speech recognition software, and converted to commands. The Server then uses these commands to gather answers to the original spoken inquiry. All of these assistants can make recommendations and perform various actions via their Server capabilities. (For example, a verbal request for the “weather” might yield various audible statements about the weather in your location. Or, a request for “traffic” might yield audible indications of the traffic in your location, or possibly maps indicating traffic problems. Or, a request for the best restaurant might yield a list of restaurants near your location. Or, if you have things set up, the statement “Add eggs to my shopping list” will yield an updated shopping list including eggs.)

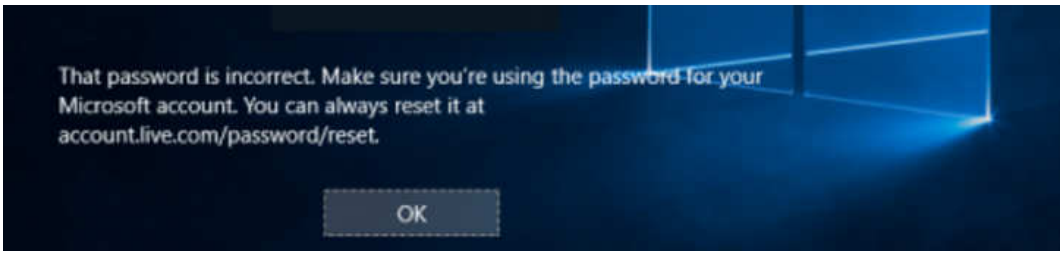
Here are some descriptions (and advertisements) found for each of these Voice Recognition & Control Apps.

- Siri (Speech Interpretation and Recognition Interface) is a computer program that works as an “intelligent personal assistant” and “knowledge navigator”, according to Wikipedia. “The software adapts to the user’s individual language usage and individual searches with continuing use, and returns results that are individualized”, also from Wikipedia. “Hey Siri” is the wake phrase, which can be turned on or off.
- OK Google lets you do things like search, get directions, and create reminders. For example “OK Google do I need an umbrella” to see if there is rain in the weather forecast. To use “OK Google”, make sure you have the latest Google Search App and turn on “OK Google detection” in settings.
- Cortana is an App with which you can use your voice to make a call, send a text message, search the web, or open another App. Cortana can help you: schedule a meeting, set a reminder, get up-to-date weather or traffic.(Note: you need a Microsoft account to use Cortana.)“Hey Cortana” seems to be tied to the “Notebook”, and thus is setup in the Notebook-Settings, which may not be obvious. (You get to the Notebook-Settings by clicking in the search bar on the Taskbar, then selecting Notebook [the square icon under the home icon], and finally Settings.)
- Alexa is the name of Amazon’s assistant that comes with the Amazon Echo. Echo is a wireless speaker and voice command device. The device consists of a 9.25-inch tall cylinder speaker with a seven-piece microphone array. “Alexa”, the “wake word” is always on and can be changed by the user to either “Amazon” or “Echo”. The device is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audio books, and providing weather, traffic and other real time information. It can also control several smart devices. Echo requires a Wi-Fi internet connection in order to work. The Echo must be plugged in to operate since it has no internal battery.

If these personal digital assistants are successful, many more may show up. I just read that the company that brought us the SoundHound App also has a personal assistant called Hound that they hope to embed in other applications so that those Apps can be voice controlled. Imagine setting up an Uber ride by voice. (If you will recall, SoundHound is like the Shazam App, just hum a tune and it will tell you the tune’s name.) With all these personal assistants around, we certainly will never have to feel lonely.

I Lost (Forgot!) my New Windows 10 Admin user password

Art Gresham, Editor, UCHUG Drive Light - www.uchug.org = 1editor101 (at) uchug.org



So yes, I upgraded a computer to Windows 10. On purpose. That was several weeks ago. But now I have forgotten what the password for that administrator, named “Admin” was set to. And since it is a local account (I have no use for creating a Microsoft Hotmail Account for every one of the computers I manage), I could not use the usual, published, methods for recovery using the Password Reset Tool for Microsoft Live Accounts.

I tried all my usual, possible and variations of passwords. No luck of course. This would call for the brute force method of recovery. Now I do have a log-in on the computer, as a non-administrator user. And there were no files or programs installed as that new administrator that had to be recovered. But I could not install/ uninstall, or do the normal set-up things that I need to do to put it in use again. I had to either get access by password, or create an entirely new administrator, which was a perfectly acceptable option for this situation.

After much searching, trying various easy (“Easy?”) fixes, I gave up. For a several weeks. Then in frustration I made more searches. Lots of fixes to be had, if I wanted to pay $17 or $35 for a 5 minute fix that is 'guaranteed to be easy and fast'. Pass.

More searching and I found a method that recommended making a couple of simple changes to some file names, and editing, done from a command box. Easy. Except it requires access beyond the normal login as a non-administrator. The file changes needed require administrator privilege, or to be accessed outside of a normal Windows boot up.

The method published would have you use the Windows distribution disk to go in a particular way, open the command box, do those commands and be back in business. Only one problem. Obviously I do not have a Windows 10 distribution disk. If I had that I would have been back in it long ago. What I needed was a way to access those files.

Many of us know that one way to have direct access to your hard drive files is to boot with another CD/ DVD or Flash Drive, with another operating system. One which does not adhere to the file locks enforced by a Microsoft boot up. Since I run Linux Mint on all my home computers, and have the install on a thumb drive, and I have done several boots with other computers I knew this might hold the answer.

1. The first step was to get into the menu that selects startup boot process. That will be different for each manufacturer, but usually involves pressing a key during the early startup process, something like F11, or escape, or F8. Check with your manufacturer's model instructions, or just watch the screen as it starts and try to catch that quick message as it passes by. You may need a couple tries to succeed.

Once I was able to boot from my Linux thumb drive I used the instructions given from the original solution, performed the steps needed, rebooted into Windows 10, performed a couple more steps, this time in the Windows command box. I now have a fully normal operating Windows 10 system.

So what is the magic? The original article I based this on is here:
http://www.howtogeek.com/222262/how-to-reset-your-forgotten-password-in-windows-10/

But since I do not have the needed disk as described in the article, I skipped down to the section of that article which begins:

> **Create a New User to Save Account Files**
> If none of this works, there's another measure you can take which will (in a very round-about way), allow you to regain access to your computer.

2. So instead of following the boot up instructions using the Windows disk, I booted with Linux.

The instructions then have you use the Windows command box to do the following two commands:

```
move d:\windows\system32\utilman.exe d:\windows\system32\utilman.exe.bak
copy d:\windows\system32\cmd.exe d:\windows\system32\utilman.exe
```

3. Basically, rename the program file utilman.exe to have the dot bak extension, making room for a new file of the same name. Then replace it with a copy of the cmd.exe file, renamed to utilman.exe.

So in my Linux file manager I simply did the same things. Rename, Copy, Rename.

4. That was done. Next I removed the Linux boot thumb drive and restarted, allowing Windows to start normally. This brought up the normal Windows 10 screen, and ready to log in in as the non-administrator user. No problem.

Here is where it can get a little sticky. You need to run that program (formerly known as utilman) from the login window. It may not appear on your initial login screen so you may have to start a log in as another

user in order to make it present itself at the bottom of the screen. And the popup help message will not say it is utilman, but rather something about setting up windows. Trust me. Just click it.

Click Utility Manager icon

5. Since we replaced the Utility Manager with the cmd.exe, a command prompt window should open now. Don't worry about the error message.

You can now do one of two things. Either create an entirely new Admin account. OR change the password on the existing one. Since there was nothing to be lost by creating a new one I used that method. I have not tried the rename option which I will show at the end as step 7.

6. You can now add a new user with the command below. We also have to add the user to the administrator group so that we regain full control of our Windows installation. Replace <username> with the account name of your choice. Note that the account name must not exist on this Windows installation. (Don't let the Windows 10 screen saver distract you.)

```
net user <username> /add
net localgroup administrators <username> /add
```

Click the screen (get out of the command window) to make the sign-in page appear again. Your new account should show up, and you can sign in without a password.

7. A shorter way to reset the password of a local account is to replace the first command in step 6 with the following command. (In this case, you don't need to create a new user.)

```
net user <username> <password>
```

Now you can do all the normal things you may want to do, like change the password, after you write it on a sticky note!

Finally, remember to go back and delete that fake utilman.exe, and restore the name of the old one, if you ever want to get into those functions again. (using the Linux boot again)

My thanks to **Michael Pietroforte** for his article at (and credit for his images)
https://4sysops.com/archives/reset-a-windows-10-password/

as well as to **Chris Stobing** for his article at How-To Geek (credit for his login screen image)
http://www.howtogeek.com/222262/how-to-reset-your-forgotten-password-in-windows-10/

Please read their articles for more tips and instructions.

File Encryption

Dick Maybach, Member, Brookdale Computer Users' Group, NJ
July 2016 issue, BUG Bytes - www.bcug.com - n2nd (at) att.net

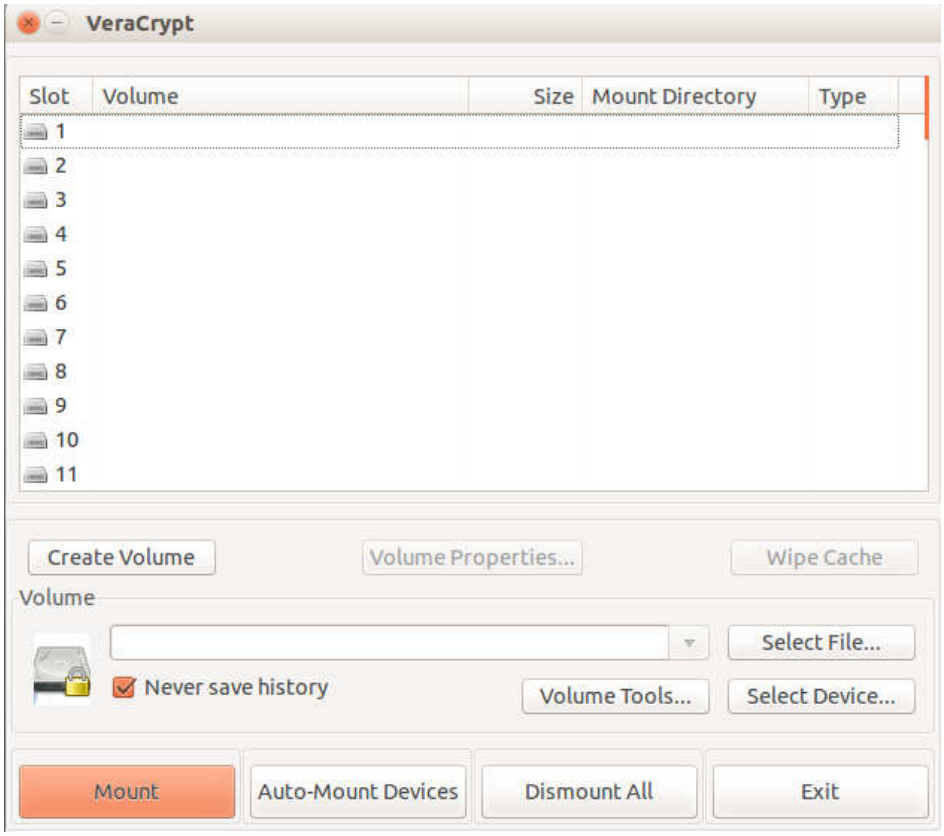
I wrote an article on file encryption that appeared in the August 2014 Bytes, available at http://www.bcug.com. While I was writing, TrueCrypt, a popular tool for this task, was discontinued by its anonymous developers amid speculation that it had been compromised. As a result, I recommended using GnuPG for file encryption. This is still valid advice, but two successors to TrueCrypt have since appeared, CipherShed, http://ciphershed.org/, and VeraCrypt, http://veracrypt.codeplex.com/. Both can read files encrypted with TrueCrypt, but only CipherShed can write in this format. If compatibility with TrueCrypt files is important, you should use CipherShed, otherwise use VeraCrypt, which has somewhat improved security and appears to be the more active project. The remainder of this article will discuss only VeraCrypt, which is available at the CodePlex site given above. You can also get from SourceForge, but this site has been known to include malware with its downloads. SourceForge now has new owners and may again be reliable, but why take a chance?

You may be using GnuPG with its public/private key method to encrypt your e-mail, and as I discussed in my previous article, you can also use it for file encryption. The advantages of doing this are fewer keys to manage and having only one encryption program. However, you may find some features of VeraCrypt useful, and its single-key encryption can be more secure than the GnuPG's public/private type, provided you use a strong password. You should view encryption as a means of reducing, not eliminating risk. If the NSA really wants to decrypt your file, it most likely can.

VeraCrypt creates and maintains on-the-fly-encrypted volumes, and data is automatically encrypted before it is saved. No data stored in an encrypted volume can be read without using the correct password. VeraCrypt stores decrypted data only in RAM; it stores only encrypted data on a disk. Even when the volume is mounted, data on the disk remains encrypted. When you restart or turn off your computer, the volume will be dismounted and files stored in it will be encrypted. To read them, you have to mount the volume with VeraCrypt and provide the correct password.

You can download a 162-page manual from VeraCrypt's Website, but I won't try to cover that here. Instead, I'll walk through establishing and using an encrypted volume to show how easy this is. The screen-shots are from a Linux machine, but the differences for other operating systems are quite minor.

Screen 1 shows VeraCrypt's opening screen. (On Windows the slots column would be labeled “Drive” and the rows would be labeled D:, E:, etc.) Your first step will be to create an encrypted volume, which you do by selecting a slot and clicking the *Create Volume* button.

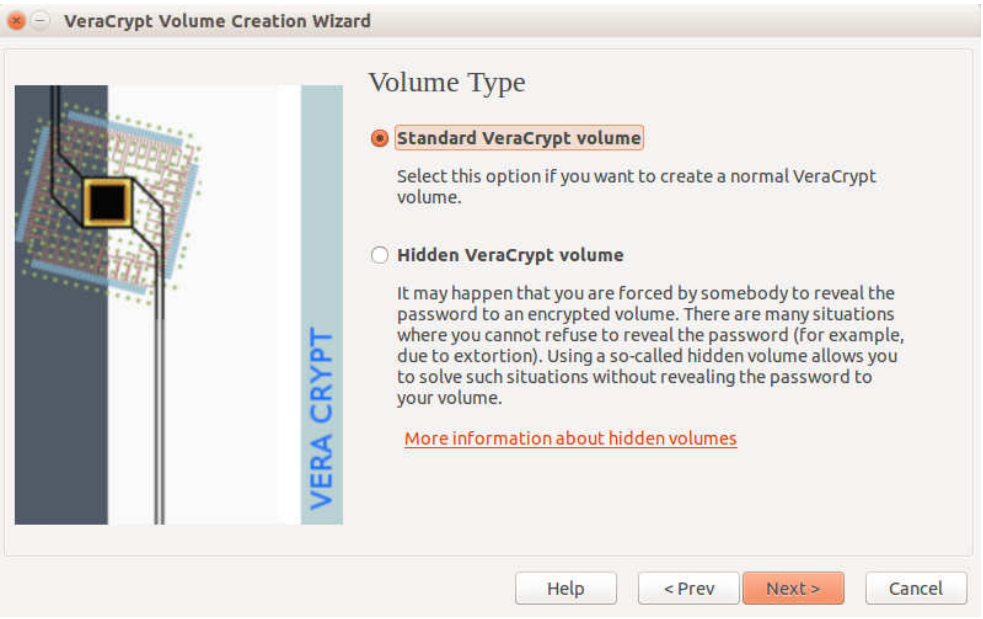


Screen 1. VeraCrypt Main Window

You will then see Screen 2. Select the upper option to create an encrypted volume as a file and the lower to encrypt an entire external device, such as a memory stick. Then click *Next* to continue.

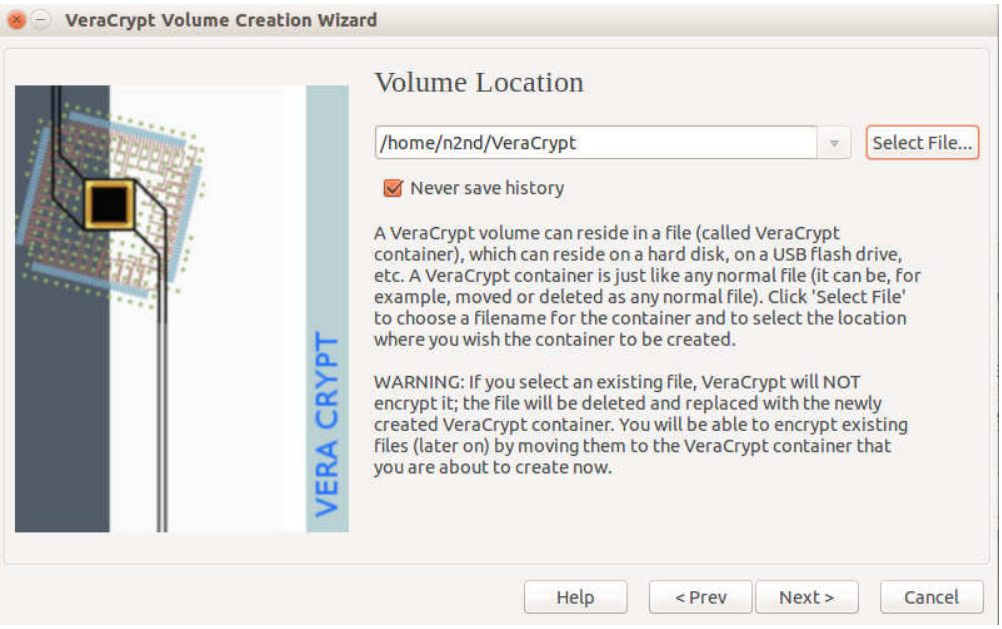
Screen 2. Volume Creation

On Screen, 3 you choose whether the encrypted volume will be visible or hidden. The first choice is by far more common.



Screen 3. Volume Type

You next specify where to store the volume, Screen 4. Initially the location window will be empty. Just click on *Select File...*, choose its directory, and enter a filename. Important – be sure to choose a filename different from that of an existing file in the chosen directory, or the existing file will be deleted!

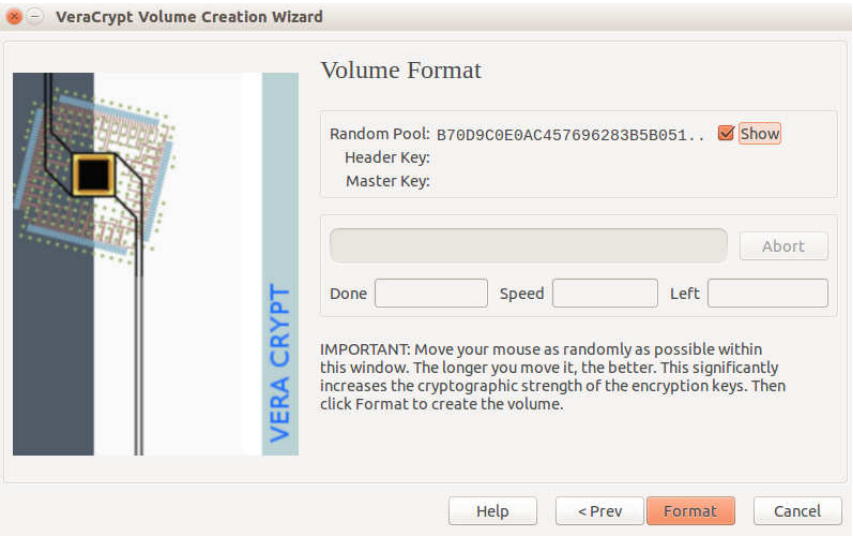


Screen 4. Volume Location

You will then go through screens where you select an encryption method (the default, AES, is fine), a volume size, and a password. Give some thought to the size. If you choose 100 Mbytes, the volume will occupy that much room on your disk, even though it contains only a 1-kbyte file. But if you choose 1 Mbyte and have 10 Mbytes of data, you will have to create another volume with enough capacity for your data. Password choice is also important. For example, if the volume will be stored in the cloud and contains sensitive data, such as passwords to your on-line banking account, you should use a long and

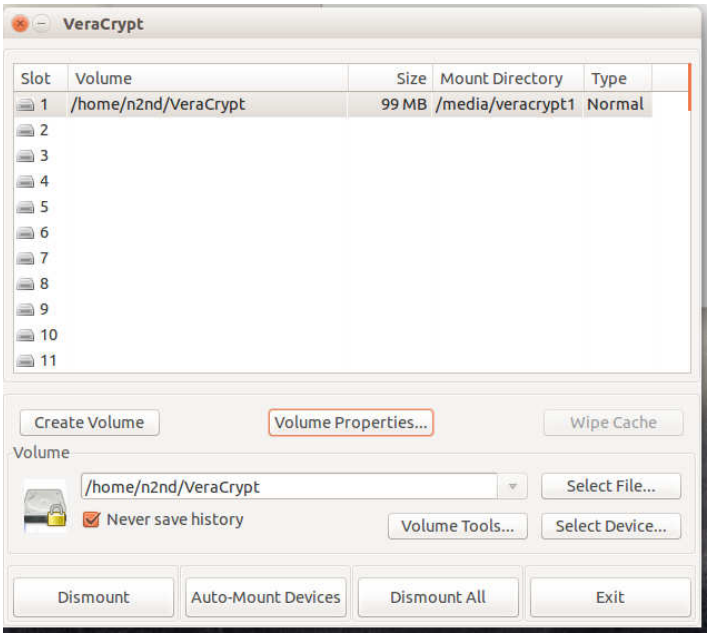
obscure password, which you safeguard, perhaps in a password manager such as KeePassX. The password screen also offers additional safeguards, such as key files; see the VeraCrypt manual for more information. You then select a file-system, probably FAT or NTFS for Windows users.

Finally, you'll see Screen 5. Before you click the *Format* button, move the cursor randomly around the screen, which will increase the strength of the encryption. When you click *Format* VeraCrypt will create an empty volume with the name and location you specified previously.



Screen 5. Format Volume

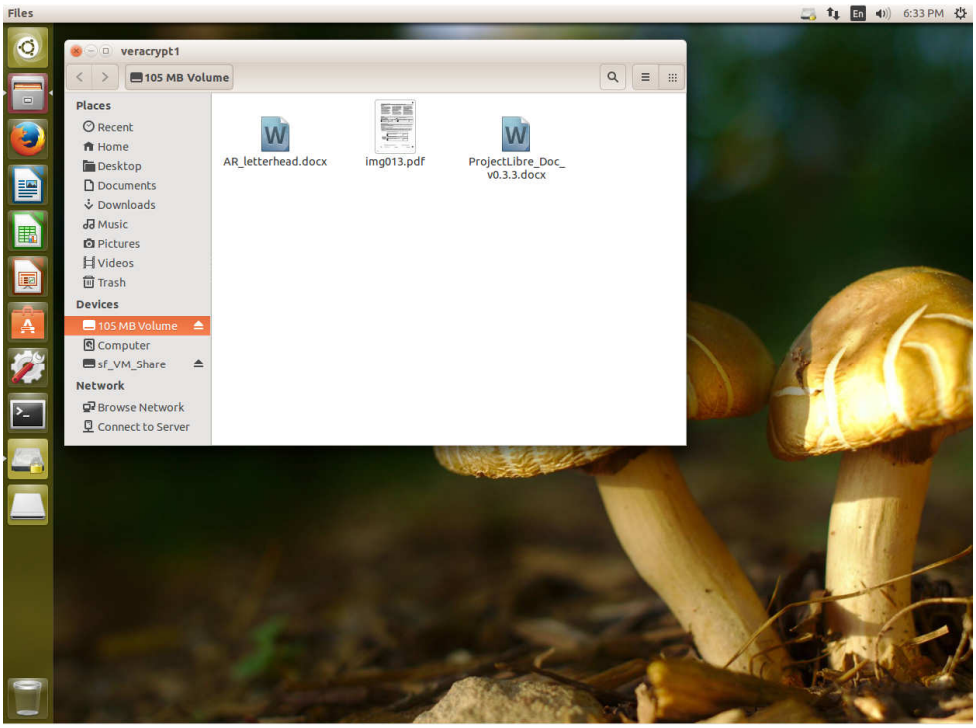
Before you can use the volume, you must mount it. In the VeraCrypt opening screen (Screen 1) click *Select File*, choose the volume you created, click the *Mount* button, and enter its password. (Depending on your operating system and permissions, you may also be asked for the administrator password.) Screen 6 shows the result, in this case, the volume is located at home/n2nd/VeraCrypt and is assigned to Slot 1. (On a Windows PC, the column would be labeled “Drive” and you would see the usual drive letters.) I find it convenient to minimize the VeraCrypt window rather than exit the program, so I can recall it quickly to dismount the volume. This isn't really necessary, as it would be dismounted when you log off or power down.



Screen 6. Volume Mounted.

This discussion has been on using a file as a secure volume, but the procedure for using an entire device, such as a USB memory stick or hard drive is the same.

Screen 7 shows the Linux desktop with the file manager open. The encrypted volume is accessed the same as a normal directory. You can copy and paste files to and from it as usual. Linux users should note the mount directory in Screen 6, which shows where to access files from the command line.



Screen 7. Linux File Manager Accessing a VeraCrypt Volume.

You might be wondering what could possible require a 162-page manual. Although its basic use is quite straight-forward, VeraCrypt has many features, which can make it more convenient and more secure. If your information is sensitive and if the encrypted volume could be accessed by others, for example if it will be stored in the cloud, on a publicly-accessible PC, or a laptop with which you travel, you will want to at least scan the entire manual.

Although both VeraCrypt and GnuPG protect your data using encryption, they do it in quite different ways, GnuPG by encrypting single files and VeraCrypt by creating encrypted volumes. If you want to e-mail a friend some private information, GnuPG will be simpler. and it avoids the issue of securely sending a password. If you have several files containing sensitive data that will stay on your computer or on a memory stick, then creating a secure container with VeraCrypt is preferred. If you will keep the secure container in the cloud or sync it among several computers, its size is important. This is because file sharing is usually done with entire files. If you change one small file in a large encrypted volume, the entire volume must be exchanged, and this probably won't happen until you dismount it. Thus, you must take care to dismount the volume, but stay logged on until the syncing is complete. This isn't an issue with memory sticks, since these are updated incrementally as you change the volume's contents.

Finally, VeraCrypt stresses using hidden encrypted volumes to establish “plausible deniability,” which lets you deny that your computer contains any encrypted data. You shouldn't try to use this casually, for example to bring pirate music or movies into the country, as it could place you in serious conflict with our or another country's authorities.