Midland Computer Club

Midland Michigan

BITS AND BYTES

JULY 2019

https://mcc.apcug.org/

ARTICLE INDEX

Articles in this Newsletter have been obtained from APCUG with the authors' permission for publication by APCUG member groups. The Midland Computer Club has not verified the information contained in the articles nor tested procedures or hardware/software. Articles do not necessarily reflect the views of the Midland Computer Club.

GENERAL CLUB MEETING
Midland Public Schools Administration Building
600 E Carpenter Street - Room D

Wednesday, (July 24, 2019)
6:00 P.M.

BACK TO BASICS - **Traveling With Your Devices (Computers)**

By Jim Cerny, Forum Leader, Sarasota Technology Users Group, FL
March 2019 issue, The STUG Monitor -- www.thestug.org -- jimcerny123 (at) gmail.com

You are probably used to using your computer devices at home, but what about traveling? Taking your devices with you can make your trip much better with directions, shopping, gas, emergency needs, entertainment, and much more. Whether you are traveling with your smart phone, tablet, or laptop here are some important tips to remember.

1. Backup your device and/or data before you leave. If you are using the "cloud" as your backup, that's fine. But it is wise to check to make sure that you are putting all your important things on the cloud or whatever backup system you use.

2. Bring charging cables and power backups with you, along with ear buds for private listening. You should have a cable in your car as well to keep your devices charged.

3. Check that your destinations have free Wi-Fi. Even if they do, be prepared for much slower response than what you get at home.

4. Take your needed account IDs and passwords with you! If you use another computer or need to access your email in a different way, you will need your IDs and passwords. At home you may have your device remember your ID or password, but when you travel it may not work that way, especially if something goes wrong.

5. Keep your travel information handy – in your smart phone for example. Have an "emergency" note in memory with your medications, doctor information, emergency contacts, etc. You should also have a list of your destination phone numbers, travel club memberships and phone numbers for general travel needs such as hotel chains, airlines, car rental companies, etc.

6. Do a test before you leave on your trip. Go to your local library or coffee shop and test how to get your email or important things on the internet. It is nice to see how things work differently when you are not in a hurry and when you are NOT using your home Wi-Fi network.

7. If there is no Wi-Fi network, you may be able to use your iPhone/smart phone as a "hotspot," so your laptop can connect to the internet using your phone as a Wi-Fi. Note that you will be using the cellular network and such use may use your data and/or add to your monthly phone bill (depending upon your phone contract). You can ask Google how this is done on your particular smart phone and/or contact your cellular provider for help and possible use charges that may be billed to you. Again, do a test of this before you leave.

8. Be aware that using a "public" Wi-Fi network is, well, not private. In other words, others using the same network may be able to see what you are doing. Try to avoid entering passwords, account numbers, and credit card numbers on public networks.

9. Test how you will use Google maps (or other travel apps) before you leave on your trip. Try them around town in your local area when you are not in a hurry to see how they would work, especially if you will be using them in your car. Can you drive using the audio voice directions? Do you need to touch the screen on your device while driving? Do you understand how your travel app displays bad traffic, accidents, gas stations, hotels, etc.? It is ALWAYS better to have a passenger help you navigate with your device while driving. Any distraction taking your eyes off the road is dangerous. If you are driving by yourself pull off the road and stop to use or adjust your device.

10. If you are traveling out of the USA, you will have to get adaptors and arrange for special usage for your devices in other countries. Ask Google or your provider for help and costs.

In summary, it all comes down to being prepared and to “know before you go.” Besides, it can be fun to discover some of those wonderful things those apps can do before you are in a bind with problems on the road. Happy safe travels.

The following .jpg image is optional, but I think it’s fun:

Consider the Risks of Helping Friends with PC Problems

By Dick Maybach, Brookdale Computer Users Group, NJ
www.bcug.com -- n2nd (at) att.net

If you are known as a computer enthusiast, your less-experienced friends probably come to you for help when they run into problems. However, you should consider the risks before you agree. While you have a lot of computer experience, most of it is probably limited to your own system, which you are careful to maintain and back up regularly. You also are aware of the risks and avoid suspicious Internet sites, are alert to e-mail scams, and have installed protection against malware. This may not be true of the owner of a PC you are asked to repair.

I once agreed to help a friend who was complaining about his laptop being slow. My first clue that I was in over my head was when I saw the missing keys on the keyboard, but by then I was already committed. I did what I could to clean things up, but the slow processor, full disk, and inadequate RAM remained, and my several hours of work produced little improvement. Another experience was more successful. A PC was thoroughly infected with malware when a teen-age son downloaded pirate music. I cloned the disk, mounted it on another PC, and deleted the problem files. The owner used the restoration partition to put the disk back to its condition when the PC was purchased, after which I loaded their files from the sanitized clone disk. This too took several hours.

Your friends may have unrealistic expectations. If the problem appears to be a full disk or inadequate RAM, the money spent on the parts may not result in a dramatic performance improvement. If you suspect malware and recommend they purchase anti-virus software, it may not fix the problem, and may even slow their PC. You’ve cost them money without fixing the computer to the degree they expected. And once you’ve mucked about with their PC, they may suspect that any subsequent troubles are your fault.

Finally, because you are working in an unfamiliar environment, you will probably be spending many hours, even if you aren’t successful. Repairing someone else’s PC is usually a lose-lose situation. If you fail, you lose a friend, and if you succeed you’ll most likely be asked to do it again. The bad habits and poor maintenance that led the initial problem are still present.

If you decide to help, what are some reasonable actions? Your first concern, of course, is to safeguard the owner’s information, which means cloning the entire disk (or disks) to an external drive, which can take several hours. Note that this means you copy every byte, not just the complete files. By doing so you may be able to recover deleted and damaged files, directories, and partitions, should that be necessary. If the

problem PC is dead, you will of course have to remove its hard disk and install it in a good computer to clone it.

Before you try to diagnose the problem, recognize that you may not be able to trust either the hardware or software in the problem PC. My preference is to use a USB memory stick with a bootable diagnostic operating system, such as PartedMagic, which has tools to check hardware, recover files, and test for malware. (See my articles in June, July, and August, 2012 on file recovery, in April 2012 and February 2017 on PartedMagic, in May 2015 on the Trinity Rescue Kit, and in June 2015 on the SystemRescueCD, all available at www.bcug.com.) Whichever diagnostic tool you use, become familiar with it on your own PC before trying it on one with which you aren't familiar.

If you save the user's files you should check them for malware before reinstalling them on a repaired or new PC. Take the clone disk home and run a thorough malware check. (Parted Magic, in particular, has the relatively weak ClamAV, which checks only and doesn't repair. If you use Windows, you most likely have far better software on your machine.) Once you have cloned a disk, you can use PartedMagic's tools, or those of a similar system, to recover damaged files. If, as is likely, the problem PC runs Windows, some user data (for example, Internet favorites and e-mail) may be stored in the system area. The locations vary with the version and restoring them in a new system may be difficult. Before spending a lot of time, ask the owner if they really need to recover these.

Although it can be very time-consuming, you can attempt to clean up the file system. This means removing malware, pop-ups, spurious menu bars, and the like. It may also require disabling programs that launch at boot time, and perhaps editing the registry. This is likely to be frustrating as the owner still has the bad habits that caused these problems, meaning the will most likely recur.

Before you agree to anything, try to find out how the problem began. Did they install hardware or software? Did they see a pop-up or get a phone call or message advising them of a problem? Did they visit a new website? Did they delete files or directories by mistake? Did the symptoms appear suddenly of build over time? You are trying to discover whether the problem resulted from hardware failure, software failure, malware, or operator error.

If you have decided to help, this is what I recommend. (Most likely you'll modify these steps to fit your own experience and tools.) Before you begin, be sure the user understands that you are an amateur, and that you can't guarantee success.

- For a casual friend, find out what you can over the phone and recommend a shop.
- If you decide to get more involved, go to the house with a diagnostic USB memory stick and check the hardware and file system. Write down what you find and recommend a shop.
- If this is a very good friend or a close relative, tell them not to use the PC until you can image their PC's disk. (If you don't have a spare USB hard disk they will have to purchase one for the purpose.) Then use your diagnostic memory stick to create an image of the system disk on the external one.
- If the hardware is good, use the restoration partition to return the PC file system to its state at purchase time. (In the unlikely case that the owner has a valid Windows installation disk, you don't need a restoration partition.)
- If the hardware has failed, the owner can decide whether to have the PC repaired or replace it. After this, do what you can to restore the data you have saved, but make it clear that some may be lost.
- Be sure the owner understands that a new PC or a clean install of the operating system means any applications installed after purchase will be lost unless he or she has their original installation disks.
- The last option is to attempt a repair. However, before you jump into this tar pit, be sure the owner understands and accepts the risks. He or she should purchase the parts, with your advice of course. Be sure to make clear that you are amateur in unfamiliar territory and that success is not assured. For example, if the disk has failed because of a faulty power supply, its replacement may be damaged immediately. Who pays?

This is not to say you shouldn't try to help, but it would be prudent to think about your possible approaches as well as the risks before you get the phone call. You don't want to disappoint a friend or cause them to lose money.

Cord Cutting or How I Love to Pay Less to Get More of What I Think I Need

By Jan Lann, Editor, Computer Club of Hot Spring Villages, Arkansas
February 2019 newsletter -- www.cchsv.org -- editor (at) cchsv.org

https://www.fastcompany.com/90304498/20-great-free-streaming-services-for-cord-cutters

I may have just stumbled on, for me, the Holey (sic) Grail of news: For years, I have been attempting to get entire news shows from the internet, but only gleaned news clips, necessitating watching a few minute snippets and then having to click on another snippet and another…., which is extremely annoying (at least to my laziness, I mean, my invaluable time).

I am almost certain or 92.5% certain that there are big cities that might provide me with an entire news show, either in real time or archived (i.e., not in real time).

Just today, I found the Answer:

STIRR
https://stirr.com/

Where, after a little experimentation, I was actually and remarkably able to watch a Channel 7 newscast from Little Rock in its entirety (and after it had been broadcast). I hope this encourages others who may not have satellite or cable tv or, like myself, would like to emancipate myself from the costly slavery to these services.

If you have a hunger for less low brow entertainment (no value judgement there, of course), here is an offering:

PBS
https://www.pbs.org/

PBS and PBS KIDS have streaming archived (not live yet, the web sites state) and there is a wonderful service I subscribe to for $5/month where I can access hundreds of previous PBS shows:
https://www.aetnfoundation.org/

For you weather watchers out there, the Weather Channel just threw a wet blanket on me, unceremoniously announcing to me (just me?) that I could not watch them without signing in from a tv provider.

Fortunately, though, Weather Nation, http://www.weathernationtv.com/ came to my rescue, although it was not as simplistically easy for me to navigate as I would have desired, but, for free, I am not complaining (too loudly).

Another service, XUMO https://www.xumo.tv/ offers live tv news, etc.

As I suspected, the article (as above) from Fast Company confirmed my intuition that MSNBC, FOX NEWS and CNN cannot be watched live without another provider, satellite tv, cable, etc. But there are a few free workarounds:

- CBS News for live, anchored news coverage.
- NewsOn for local news from select stations around the country.
- Plex or Haystack TV for a personalized newscast that pulls in clips from various sources (including local stations).

Live news can also be found in Pluto TV, Xumo, Stirr, and The Roku Channel,.

All in all, there is a wealth of avenues to slink off the pay-for-tv reservation. I have listed in this story only a few. Perusing the entire article from Fast Company will yield far too many probably but you can choose your favorites, OR NOT.

Dan's Desk - **Encrypting a Drive**

By Dan Douglas, President Space Coast PCUG, FL
March 2019 issue, The Space Coast PC Journal -- www.scpcug.com -- datadan (at) msn.com

Last month I described a BIOS password problem that I had to solve. This month, we'll look at other password locks such as those used for protecting hard drive data.

One of the added features of Windows 10 Pro over the Home edition capabilities, is the ability to encrypt a drive to protect all data and files contained on that drive from unauthorized access. An administrator can select a drive from the File Explorer app and turn on the BitLocker option from the right mouse button option list. The user must then select an encryption key using any combination of uppercase and lowercase letters, numbers or symbols up to 64 characters long. It is critical to record this password as it will be impossible to access the files afterwards without this key. Windows will prompt you to save this key on your cloud account, or in a file or by printing it before encrypting the drive.

I recently had a customer who had a broken Surface PC and needed to recover some business files from the drive. The first place they'd taken it to had told them that it was not possible to access the data, not because it was encrypted, but because the drive was a solid-state circuit board, as is usually found in tablets and many Macs, and did not have the usual SATA drive connector. Having used many drives of this type before, I had the correct adapter to convert it to a SATA type connector. That was when we discovered that it had been locked using BitLocker. It prompted us to enter the key and the owner had no idea what that key may be. I told them that without the key I could not access the data for them. They were advised to check all of their paperwork to see if it was recorded somewhere. Fortunately, when the PC was purchased, the BitLocker key was written on their bill of sale by BestBuy! When they returned later with the key, we were able to access the data and transfer the files to a USB stick.

If you need to encrypt just specific files or folders and not a complete drive, there are several alternatives available. For example, Word and Excel provides for the ability to protect a document by applying the 'protect document' option to the file through the Word or Excel options.

Adobe Acrobat can also be used to protect PDF type files. In certain versions of Windows, namely Windows 10 Pro, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro or Windows 8 Enterprise also come with an Encrypting File System (EFS), which lets you encrypt any kind of file, as well as whole folders and subfolders.

Users with a Home edition of Windows will need to use either the Office Suite encryption or a third-party solution, such as TrueCrypt, VeraCrypt or 7-Zip.

EFS is applied by selecting the folder or file, select the properties/advanced through a right button click, and then select the 'encrypt contents to secure data' option. This encryption is applied using the logon ID and password so it is not as secure as that used by the BitLocker and I'm not sure what would happen if the password used by that ID was removed using a password removal tool. Possibly the data would stay encrypted and still require the original password to allow the files/directories to be accessed.

Many USB drives also offer their own encryption system for the files on that drive, but I would be hesitant to use these as the proprietary nature of the program may cause problems later.

Interesting Internet Finds March 2019

By Steve Costello -- scostello (at) sefcug.com

In the course of going through the more than 300 RSS feeds, I often run across things I think might be interesting to other user group members. The following are some items I found interesting during the month of February 2019.

What is Google Voice and How Do I Use it?
https://www.groovypost.com/howto/what-is-google-voice-how-to-use/

I have been using Google Voice for years and am always surprised by people I meet knowing nothing about it. It started out as the designated phone number for user group contacts so no matter where I was the calls forward to my house and cell numbers and, if still missed, the voice mails get transcribed to text. Google Voice was free then and is still free now.

How to Protect Your Accounts with Two-Factor Authentication
https://www.techlicious.com/tip/best-practices-for-using-2-factor-authenication/

Do you keep hearing about two-factor authentication and want to learn more about protecting your accounts with it? If so check out this post. (Note: If you are not using two-factor authentication, you really should.)

Search Images with Creative Commons License: Free Tool by Creative Commons
http://www.ilovefreesoftware.com/22/webware/search-images-creative-commons-license-free-tool-by-creative-commons.html

As a blogger I look to use creative commons licensed images a lot. Sometimes I will even use tools such as this one to browse a broad group for images serving as inspiration. Free stock photos are also good, but I feel they don't work as well and it is harder to properly use them without copyright concerns.

Which Wifi Channels Should I Use for My Wireless Network?
https://lifehacker.com/which-wifi-channels-should-i-use-for-my-wireless-networ-1832788063

Are you having trouble with your wifi speed? If so, check out this posting to see how to find out which channels you are using and which you should be using.

5 GHz Wi-Fi Isn't Always Better Than 2.4 GHz Wi-Fi
https://www.howtogeek.com/405105/5ghz-wi-fi-isnt-always-better-than-2.4ghz-wi-fi/

This post explains why sometimes one band is better than the other for dual band wifi. Something else to check if you are having wifi speed issues.

How I Write on My Phone … WITHOUT Typing on a Fiddly Touchscreen
https://www.aliventures.com/writing-on-phone/

I have been thinking about only taking only my smartphone and maybe my tablet on vacation, instead of lugging a laptop around. I do have a Bluetooth foldable keyboard that I only used to use at meetings with my tablet. After reading this post I am actually going to do it next vacation. Check it out for yourself to see if it might be right for you too.

Is There a Real Alternative to Windows?
https://askleo.com/is-there-a-real-alternative-to-windows/

With support for Windows 7 ending soon many who don't want to move to Windows 10 are asking this question. Leo Notenboom explains that there is no direct replacement, but there are alternatives that may

or may not work for you. (Note: I have experimented with several distributions of Linux, and probably will go with Linux Mint. If I need a laptop my top choice will be a Chromebook.)

****

Security Tips - March

By David Shulman, WPCUG Weekly Update editor, intergroup liaison, and a co-organizer of WPCUG's Meetup
March 2019 issue, Westchester PC News -- www.wpcug.org / intergroupliaison (at) wpcug.org

We'll gather links and published info from various sources and post them here for your investigation and education. We have secured permission to use all of this material in this fashion. Please do NOT otherwise post or circulate without getting your own permission.

This article from The Verge caught my attention: "ji32k7au4a83 is a surprisingly bad password." How bad could that be, I thought? See for yourself--

https://www.theverge.com/tldr/2019/3/5/18252150/bad-password-security-data-breach-taiwan-ji32k7au4a83-have-i-been-pwned

"Smart" homes are both a new challenge and a new opportunity for those who can commit the resources to update to this technology. The security concerns that come along are often overlooked in the process. A smart home is SO TEMPTING! Imagine telling your bedroom lights to turn off as you get drowsy in your bed. How convenient! There ARE security challenges that tag along. One is the poaching of your security protocols by an outsider. Your physical keys are under your control and likely cannot be copied unless they are stolen, lost, or brought to a licensed locksmith. Your wireless world is another story. The media has stories of "hacked" cars. Any wireless communication between devices is subject to interception. Unless extraordinary steps are taken to encrypt these signals, they are subject to theft and use by another.

One aspect of this is your smart TV. If it sends back info as to what you watch, companies find value and others find invaded privacy. Kim Komando writes about this and TV spying court settlements: https://www.komando.com/tips/544540/stop-your-smart-tv-from-spying-on-you

Another aspect is the use of a smart home hub that is not manufacturer supported, or out of date, or from a company that is defunct. In particular, the Securify Almond router, demoed at one of our workshops and which has some really interesting features, is mentioned in this article as a potential issue. See this: https://www.howtogeek.com/405197/4-smarthome-hubs-youve-never-heard-of-and-why-you-shouldnt-use-them/

On the malware front, PC Mag has this article which Check Point says can affect 500 million users at risk: https://www.pcmag.com/news/366678/winrar-has-serious-flaw-that-can-load-malware-to-pcs
Credit to David Lerner.

On the PUP (potentially unwanted programs) front, see this article from Popular Science Mag on your PC installing PUPs, also from David L.- https://www.popsci.com/stop-laptop-installing-software

On the iOS front, certain apps are collecting info from you and, unknown to you, sharing them with Facebook and others. NOTE: This article is behind a paywall but may be accessed by subscribers and other sources. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?ns=prod/accounts-wsj

PLEASE—CHANGE YOUR PASSWORDS AND MAKE THEM LONG AND UNIQUE

President's Corner - **To Discern the Truth**

By Greg Skalka, President, Under the Computer Hood User Group, CA
www.uchug.org - president (at) uchug.org

In the TV game show To Tell the Truth, three contestants all claim to be the same person. Each segment starts with the three lined up next to each other, each claiming to be the described character ("I am John Smith," for example). A panel of four celebrities was tasked with determining which of the three was the real 'John Smith' by asking each contestant (numbered one through three) a set of questions. They knew the authentic 'John Smith' was obliged to tell the truth, while the two imposters may lie. After the period of questioning, the celebrity panelists each record their votes for which contestant they believe is the real 'John Smith', and the real central character is then asked to stand and reveal themselves. The show first aired in 1956, was popular from the 1950's through 1970's, and a revived version has been produced in recent years.

Today we are all unwitting participants in a game played out on the internet to discern the true identities of those we communicate with. Unfortunately, the stakes are higher than some cash divided among the contestants that is proportional to the number of celebrity panelists deceived by the imposters, as in To Tell the Truth. In our game, our confidential personal information, our identities and possibly our finances are at risk.

On the internet, there is a lot of information available, but a lot of it is suspect. Every email, Facebook post, tweet and blog entry could be the absolute truth, totally false or something in between. Even Wikipedia entries could contain biased or even false information, as though they are supposed to be written and reviewed by experts, it is a "crowd-sourced"; encyclopedia. Email is a particularly problematic communications medium for determining the truth of information. The accuracy of statements made in individual emails is obviously subject to the credibility of the sender, and this is usually only judged by the recipient of the email. Unfortunately, it is often difficult to truly know who the real sender of an email is. For some emails, it is pretty obvious the sender is not the IRS, the Director of the FBI or a Nigerian prince. In other cases, it can be more difficult to verify that the sender is who the email claims. That email from a bank you don't do business with is probably suspect, but what about the emails from banks, utilities, credit cards and other businesses you do expect dealings with?

How do you determine if the email sender is who they claim to be? How do you get them to tell the truth? There are a lot of checks you can make to help discern if an email is authentic and from the source they claim. Look carefully at the sender's email address listed; if the email is from wellsfargo@gmail.com, it is probably not really from Wells Fargo Bank. Even if it looks legitimate, hovering over the address by placing your mouse cursor over the text in the email header may reveal that the actual address is different.

Corporate emails that contain misspellings or grammar issues are probably fake. Emails sent at an unusual time of day for the sender (like the middle of the night) could be suspect. A lot of these are phishing emails, sent by bad people with the hope that you won't notice these inconsistencies and will click on the link included, or open the file attached, actions that will put malware on your device or trick you into entering your real passwords into their fake sites.

I have received my share of phishing emails and think I can spot them in most cases. I know enough to be suspicious and never click on links or open files sent to me, unless I am expecting them or have verified their authenticity. Last week, however, I was part of a fake email scheme that I had not seen before. I was not the target; the fake emails were sent to others I have corresponded with. Fortunately, these were savvy tech users and it does not appear anyone was taken in by the scam.

I first became aware that something was wrong when I got up on the morning of Monday, April 15 (which was tax day, but I don't think that had any significance). My son sent me a text while I was eating breakfast; he said my UCHUG email address had sent him a strange email at 3 AM and might be hacked. He attached screen shots of the email. The email he had received appeared to come from my president@uchug.org address, and appeared to have two parts, as in an email chain. The first, current part was a generic message characteristic of phishing emails. It had a zip file attached,

Greg_Skalka_UCHUG.zip. The second part of the email, as if it were a prior part of the email chain, was what I recognized as an actual email that I had sent from a work email to my son over a year ago.

I had my son confirm that he believed the email he received was sent from my UCHUG president email address. I found this to be unusual, as I never send emails from that address. Our group's web hosting and email services are through 1&1 Ionos, and since I am not fond of their email web interface, I have the three uchug.org email address; all are forwarded by the 1&1 email account to my personal email address.

I wondered if someone had actually hacked into my UCHUG president email account but didn't think too much more about it until I started getting more warning emails. Over the course of the morning I received emails from eleven people that had received a similar email from president@uchug.org with the mystery zip file attachment. These included a few of our UCHUG members and officers, a number of APCUG officers and member group officers, and even Bob Gostischa (our March meeting presenter). Most people replied back to me (the UCHUG president email) questioning why I had sent the zip file. A few tried to open the zip but their security software flagged it as infected. In each case, the emails they received contained the same generic 'Good Morning' message with the same zip file attached. The second part was unique in each email, as were the email subject lines. In most cases that second part was an email that the recipient had received previously, either from me, our editor or another APCUG member.

When I received the first reply at around 7:30 AM, I realized this was likely to be more than just an errant email my son received. I quickly wrote back to the first recipient:

> Unfortunately, I did not send you any emails recently. It appears others have been receiving the same email, appearing to come from our president@uchug.org email address. Either that UCHUG email address has been hacked (I'm copying our webmaster so he can look into it) or someone is spoofing that address. In either case, that email is suspect; please don't open its attachment. I don't actually send from the president email address (emails sent to it are forwarded to my personal email), so anything sent from it is not from UCHUG. Sorry - it is sad we live in such a world.

As I received additional replies, I copied that first response and sent it to each, to explain what had happened.

Bob Woods, our webmaster, soon let me know that he could find no evidence that our email account had been hacked, or that these bad emails were being sent from our account. As a precaution, he changed the passwords on my three group email accounts. It appeared that someone was spoofing our UCHUG email address when sending these out. Since there was nothing we could do to stop that, all I could do was continue sending my warning response to all replies I received.

By early afternoon, the replies to the bad email had stopped. The 'infection' had apparently run its course, with only about a dozen of these impersonating emails sent out, and no one appeared to be the worse for it. Most of the recipients were sufficiently suspicious to not try to open the attachment, and those that did try were protected by their device's security software.

A few days later, Bob Woods sent me an email with a link describing a situation very similar to mine: https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/ This ZDNet article describes how the Emotet malware gang has stolen old email threads (probably getting them from a PC previously infected with their malware), attached an infected document and sent it out to others in the thread. This is possibly what happened with the UCHUG president emails on April 15.

Thus it appears there are bad actors out there, trying to impersonate email users, using old email chains to try to deceive other users into opening their infected attachments. Just like in To Tell the Truth, they are imposters, saying "I am the president of UCHUG," trying to win the game by infecting computers. We all need to be wary and make sure we are certain we know the sender before trusting the message. We all need to ask the equivalent of "Will the real president of UCHUG (or the real email sender) please stand up!"

Audacity and digital audio noise reduction

by John Krout, Member, Potomac Area Technology and Computer Society, VA
www.patacs.org - jkrout75 (at) yahoo.com

This article describes the use of a feature of Audacity, the popular digital audio editor application, called noise reduction.

Noise is audible all around us. When we make an audio recording, usually some noise is included. I dictate memos to my tablet audio recording application while in my car or hiking in the woods. Outdoors, wind is almost always a part of the background noise, and in the car there is engine noise, HVAC fan noise, and sometimes surrounding traffic noise included. Your ears might not notice noise, but that is a part of human audio perception: we filter out the noise and pay attention to other, possibly more important sounds. It goes all the way back to the ancient time when the more important sounds might, to paraphrase a famous rock musician, potentially become our lunch or might try to make lunch out of us.

If you do not believe your live recording includes noise, then listen to it using earmuff-type headphones that exclude the sounds around you. Listen especially to the quiet parts.

Personal computer applications have been available to reduce noise in audio recordings for quite some time, 20 years or more. The Adobe application called Audition, a competitor for Audacity, includes a variety of noise reduction capabilities. BIAS Corporation, until it went bankrupt, offered an application called SoundSoap that did only audio noise reduction, and nothing else. I used SoundSoap in the 2000s for audio noise reduction on self-produced DVDs of high school music concerts and plays produced by The Children's Theater in Arlington VA.

There are a couple of key concepts when using any audio noise reduction application. First of all, noise reduction applications require you to identify in your audio recording file a segment of at least four or five seconds during which the noise *and only the noise* is heard. Sometimes the noise-only portion is at the beginning of the audio recording, but it could be anywhere in the audio recording. What the noise reduction applications do is analyze that noise segment so that the same noise can be subtracted from the overall recording.

What I suggest you do when making any live audio recording is tap the Start button at least five seconds before the first spoken words or sounds occur. That leader portion becomes your noise sample for noise reduction.

Second, often the noise reduction is especially useful where the audio you want to use is recorded at a relatively low level. With modern entry-level recording apps lacking Automatic Gain Control (AGC), this can happen when the audio source is distant from your microphone. I ran into two examples recently, both involving animals. Typically, then, to make the sound recording louder, and therefore useful as a ringtone, we use an application like Audacity to increase the audio level of the recording.

When you combine the two, amplification and noise reduction, it makes the most sense to amplify your entire recording *first*, then select the audio noise segment, and do the noise reduction on the entire audio recording.

Illustration 1 accompanying this article is a screen capture of Audacity displaying a short recording that I made in Yosemite National Park on the evening of September 5, 2018. This is a recording of a howling animal. I had heard howling on the hillside to the north of the Old Faithful Village for four straight nights and, on September 5, I was outside with my smart phone at the time the howling started up, so I made a recording.

The next day I played the audio recording for a National Park Service Ranger, and she said the animal was a coyote.

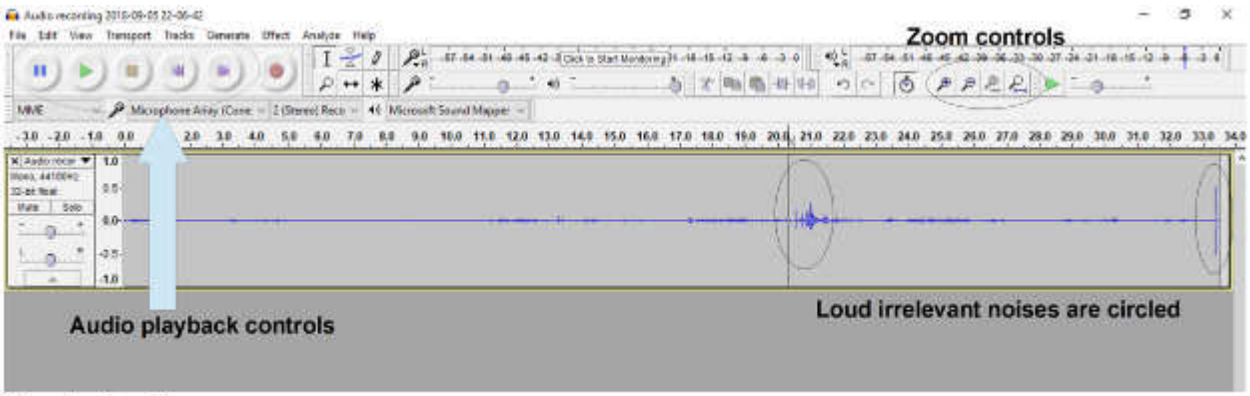

Illustration 1

In Audacity, the recording graph is very low level, quite minimal, because the coyote was far away from my smart phone. I had no desire to get any closer, stumbling through unfamiliar terrain at night, and I would have scared the animal into running away. Below you will learn how I improved the recording and ultimately made a ringtone. An important part of the process is amplification.

CLIPPING: THE UPPER LIMIT OF AMPLIFICATION

To understand amplification and its limits, you need to learn a recording concept called clipping. This concept is a part not just of digital recordings but also of all analog tape recorders, plastic records, stereo amps, and every guitar amp ever made, so it is a very old concept. All of these devices have limits of how loud they can record or reproduce sound. Amps often are rated based on wattage. A small amp might use 25 watts, and a big one might use 200 watts. Essentially that wattage rating defines the level at which clipping is done.

When using any audio editor app, the editor displays the recording just like it would look on an oscilloscope, with ups and downs. The loudest portions have peaks that stand out, looking bigger in both the up and down direction.

Audacity and similar apps have a limit on loudness, just like the analog media. In recording devices, the limit is usually called zero decibels, or decibels abbreviated as dB. When a peak literally exceeds that limit, its top is clipped off at the limit. And that effect radically changes the sound. Sounds at lower levels are expressed as negative decibels, because zero dB is the loudest.

In fact, clipping is how guitarists introduce fuzzy distortion of a guitar sound. Please refer to the **Illustration 2**. This is a photo of an oscilloscope on which a clipped sine wave is depicted. I borrowed this from a Wikipedia article on audio clipping. You might remember the smooth curves of a sine function from high school trigonometry. In this example, the peaks have been clipped and are replaced with flat areas.

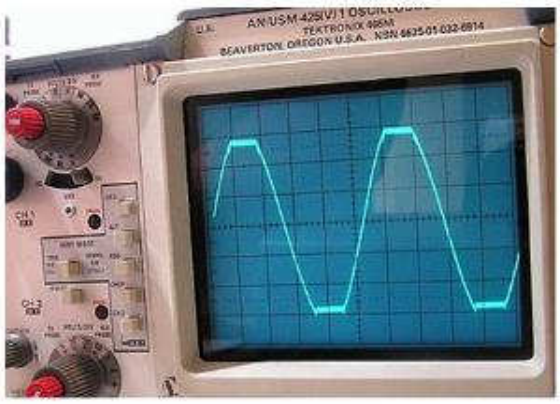

Illustration 2

To put it diplomatically, clipping is bad news when you want your amplified audio recording to sound just like you heard it. In short, you want to avoid clipping.

Audacity has a convenient amplification tool. It is found in the Audacity Tools menu. The menu choice is Amplify... as shown in **Illustration 3**. When you select that choice, it will suggest the amplification amount, in decibels. This suggestion is based on Audacity's analysis of the loudest peaks in the audio recording; it will amplify the recording so that the loudest peaks just barely reach -1 dB, precisely so that no peak is clipped.

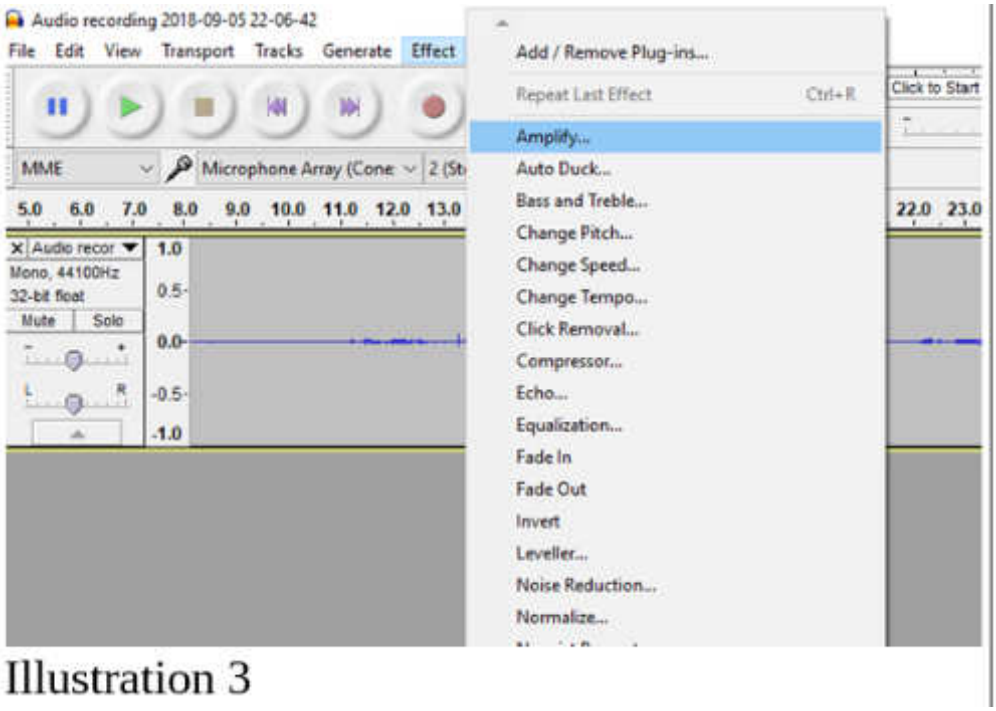

Illustration 3

The dialog box allows you to override that goal and amplify even more, but I strongly recommend not going beyond zero DB. Just beyond that level, clipping happens, and I strongly urge you to avoid doing so.

Although I am an advocate of using good quality microphones, for the same reasons that good lenses are a must on cameras, I did not have good microphones with me, plus the animal probably would have quit sounding off and departed before I hooked up microphones. I used the smart phone's built-in microphone.

I decided that the coyote sounds would make good ringtones. Ringtones have two important characteristics: they must be short, ideally less than say 5 seconds, and they must be loud. So I wanted to amplify the audio recordings, and remove the audio noise, and choose one good short sound occurrence of the animal sound, the yip-yip-howl pattern.

I also did that for a recording I made while on vacation in West Virginia during the first week of August. One night at about 11 pm, outside of our rental home, we heard an owl hooting away, conversing with a more distant owl. I think the closer owl was maybe 50 or so feet from our door, but I never did see the animal in the trees. That time, too, I made a recording of the animal using my smart phone. I used Audacity to turn that recording into a ringtone I call Two Hoots.

All of these audio recording modifications are easily done using Audacity.

REMOVE LOUD IRRELEVANT SOUNDS

Now, what happens if the loudest sound in your audio recording is irrelevant? Maybe a door slammed, or a car drove by, or a jet flew overhead. As a practical matter, if that loud irrelevant sound is included, then the Amplify... feature will suggest an amplification factor that avoids clipping the loudest sound but, at the same time, *does not adequately amplify the sound segments you care about*.

To work around that limit on amplification due to those loud irrelevant sounds, you have some choices. All of them start with you selecting the loud and irrelevant sound. Listen to the audio recording of that loud and irrelevant sound using Audacity playback. As depicted in **Illustration 1**, the Audacity playback control buttons appear in the upper left of the Audacity window, and look like CD player controls, including pause, start and stop buttons.

While you listen, Audacity not only moves its cursor through the recording graph, but also displays the timepoint measured in seconds from the start of the audio recording. You can identify the playback timepoint when the irrelevant sound occurs, then stop playback and select the irrelevant sound.

To determine the *precise* start and end of the irrelevant sound, you can magnify the graph display. The buttons for magnification are on the upper right of the Audacity window.

See Illustration 1 in which the Audacity playback control buttons and the magnify buttons are shown. The magnification buttons, from left to right, are: + (zoom in), - (zoom out), zoom to selection, and zoom out to show the entire recording.

In the coyote recording, I found two places where irrelevant loud sounds were recorded. One was at the very end; it is a loud snap, and I am not sure what made that sound. The other was in mid-recording, and was not quite so loud, some conversation in the background as park visitors were returning from dinner at the Old Faithful Lodge. These two irrelevant sections are also circled and pointed out in Illustration 1.

The Audacity selection method for audio is a lot like selecting a paragraph in a word processor. Click at the beginning of the audio segment, hold the mouse button down, and drag to the end of the audio segment. Then, at the end of the segment, you can let go of the mouse button. Magnification lets you play back, identify and select the irrelevant loud sounds very precisely.

The three methods of eliminating the effect of a selected irrelevant audio recording segment are:

- Delete the unwanted sound (like deleting a paragraph out of a Word doc)
- Blank the unwanted sound (replace it with zero sound)
- Reduce audio level of the unwanted sound (the opposite of increasing the audio level)
- Deleting is perhaps the easiest. After selecting the unwanted sound precisely, tap the Delete key on your keyboard. Voila! The loud sound disappears.

I do not recommend either of the latter two methods. Blanking will possibly disrupt noise reduction. Reducing audio level requires you to know the audio level in the remainder of your recording; you need to reduce the level in the loud irrelevant segment so that it is no louder than the relevant portions.

THE AMPLIFY TASK

After eliminating the loud irrelevant loud sound, you can amplify the entire audio file. Choose the Amplify... feature in the Effect menu. Illustration 3 shows that menu and the Amplify choice is highlighted.

When you choose Amplify, Audacity automatically selects your entire recording, analyzes it, and presents a dialog box in which it suggests the amplification factor, in decibels, that is sufficient to maximize the peaks of your audio recording. As I recommended above, simply click on OK to accept the recommended amplification level.

Illustration 4 shows the dialog box with the amplification factor suggested by Audacity for my coyote recording after I deleted the two irrelevant loud segments. The new decibel level is shown as zero dB, which is the maximum possible level without clipping.

After listening to my coyote recording a few times, I decided the best coyote sounds were in the first 6 seconds, and the best sample of noise alone was in seconds 6.5 to 11. I deleted the remainder of the audio recording beyond second 11.

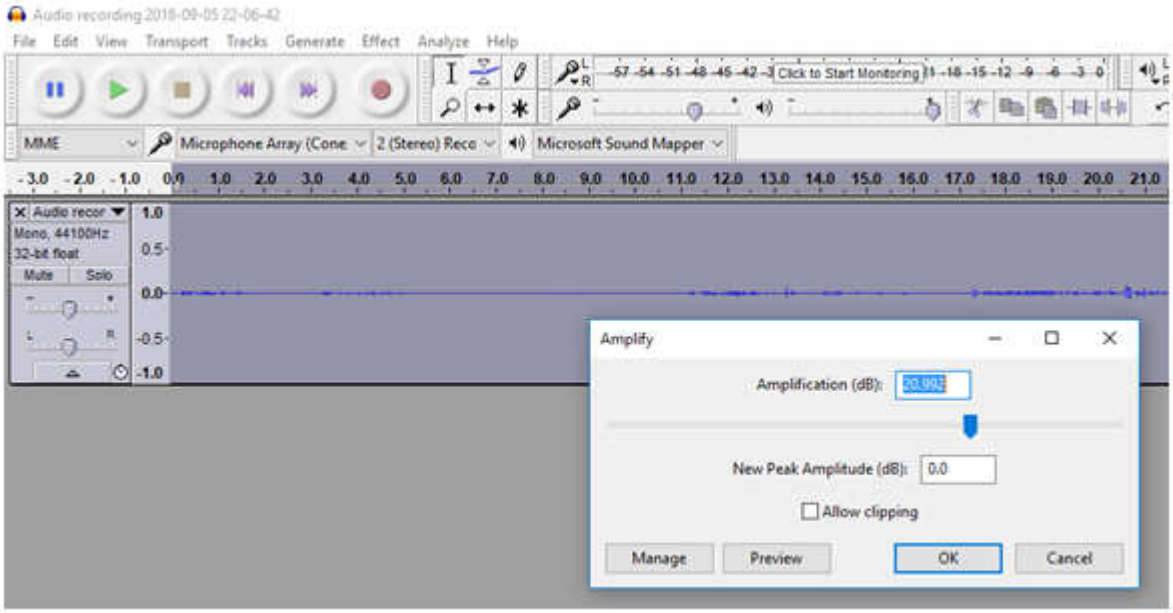

Illustration 4

The noise in the coyote recording included the Firehole River nearby (I thought the coyote was on the other side of the river), the wind in the trees, and possibly the background noises of the Old Faithful Village complex at night.

THE NOISE REDUCTION TASK

- It is time to apply noise reduction. In Audacity, noise reduction is a two-part process.
- Step 1 requires you to identify a noise-only segment of the audio recording. Audacity analyzes the noise and remembers how to subtract it from the entire audio recording.
- Step 2 does the work of subtracting the noise from the entire audio recording.

Noise reduction is one area where Audacity could use a bit of user interface improvement to avoid some ambiguity. Here, in a nutshell, is how to use it.

- Select the noise-only segment of your audio recording.
- In the case of the coyote audio recording, that starts at second 6.5 and ends at second 11.
- That selection is shown in **Illustration 5**.
- Remember, this is *after* amplification, so that the sound graph appears much bigger than before.

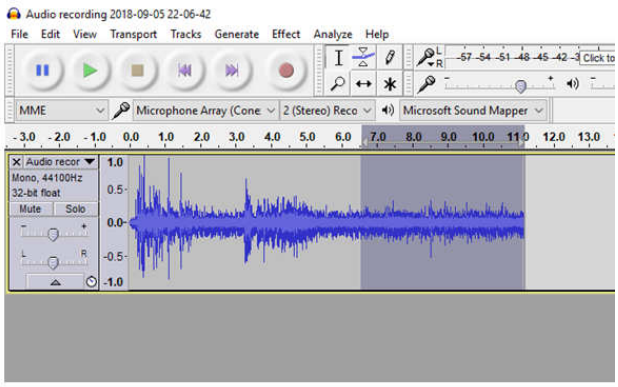

Illustration 5

After selecting the noise-only segment, in the Audacity Effect menu, choose Noise reduction. **Illustration 6** shows the Audacity Effect menu with the Noise reduction choice highlighted.

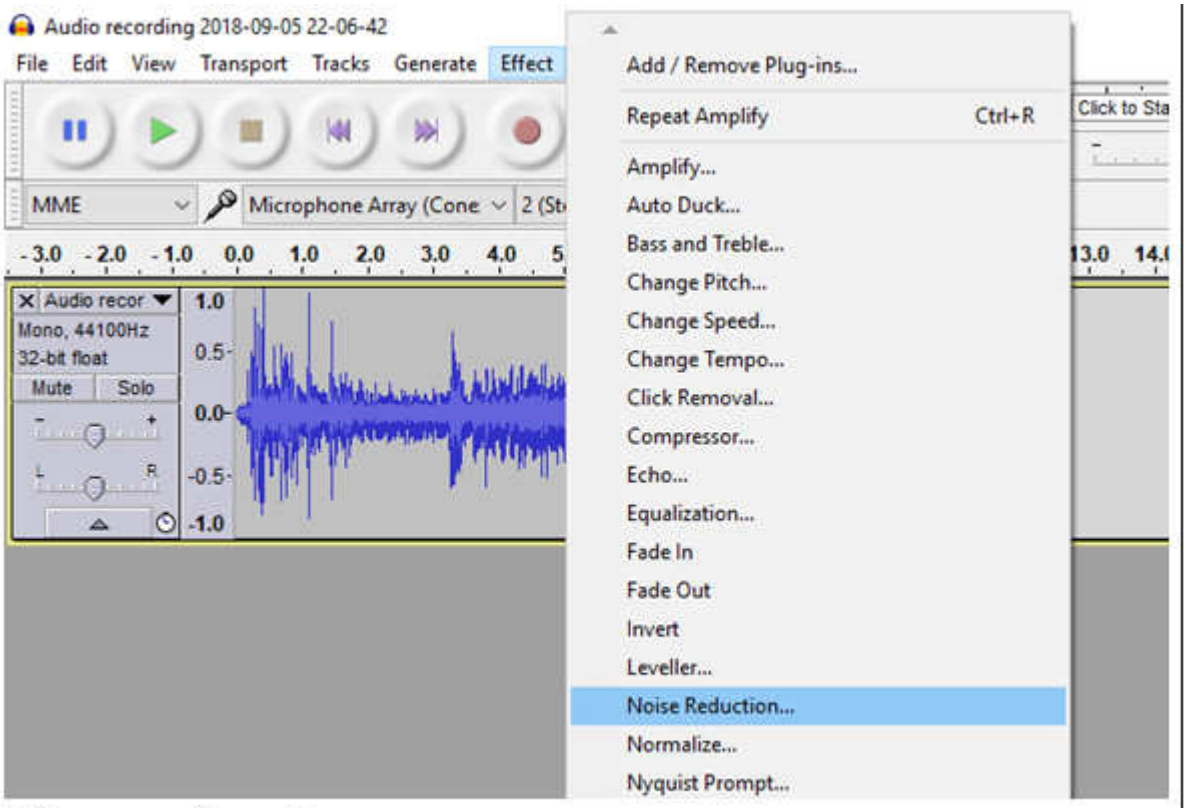

Illustration 6

Illustration 7 shows the Noise reduction dialog box which appears when you choose Noise Reduction in the Effect menu.

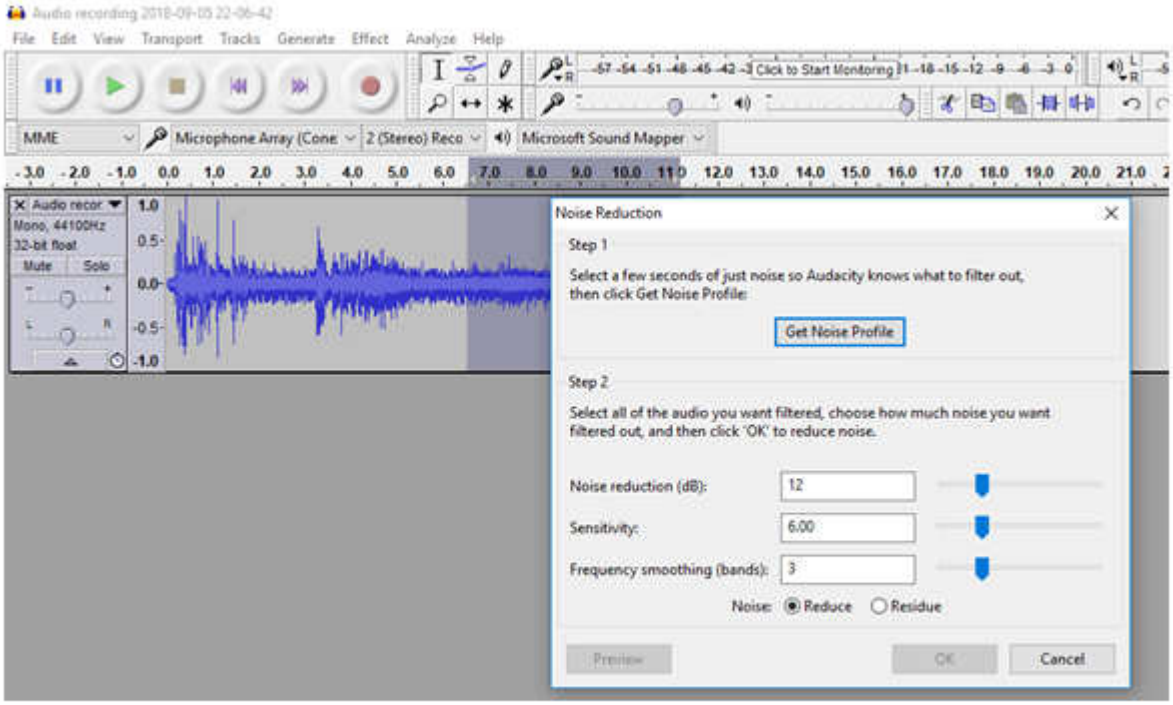

Illustration 7

The dialog box had two parts, labeled Step 1 and Step 2. Notice that initially the OK button at the bottom of Step 2 in the dialog box is inactive, grayed out.

- To complete Step 1, click on the button labeled **Get Noise Profile**.
- When you click that button, Audacity analyzes the selected noise-only segment. Then Audacity closes the Noise Reduction dialog box.
- Your next task is to select the entire audio recording. In Windows you can do that by tapping the CTRL-A key combination.
- To complete Step 2, use the Effect menu to re-select Noise Reduction. The noise reduction dialog box re-appears.
- This time in the dialog box, *the OK button is active*, because you have already completed Step 1 and Audacity remembers the noise profile it created in Step 1.
- All you have to do is tap the OK button.

There are some noise reduction parameters you can adjust in Step 2 of the dialog box. I have not tried that so I cannot give you any advice about that.

EXPORT AND CONTINUE EDITING

At this point, with noise reduction completed, I strongly suggest exporting the recording under a new name, maybe by adding the suffix noise free.

Why not Save? In Audacity, Save is for storing a Project, a combination of the name of the open audio recording file and a description of effects applied to the file. *Save does not save the edited audio file itself.* Export does that.

After exporting, you can edit the file to delete the noise-only segment, so that you have only the precise audio segment that you want.

I applied one more Effect menu item, called Fade Out, for the last quarter second or so of the recording.

I displayed the Audacity File menu and selected Export Audio. Then I exported the six second ringtone as an M4A file, and again as an MP3 file. The MP3 file is now ready to use as an Android ringtone. I changed the M4A file suffix to M4R, so iPhones will recognize the file as a ringtone file.

If you have not done sound exports previously to M4A or MP3 with Audacity, it will first prompt you to download and install third-party libraries for file types MP3 and M4A.

I applied Audacity amplification three times overall to the Coyote recording, for a total of more than 32 decibels. That is a very substantial amount of amplification. I think the ringtone sounds pretty good.

Enjoy!

About the author:

John Krout is a former president of the Washington Area Computer User Group, a predecessor of PATACS. He is a frequent contributor to the PATACS Posts newsletter and occasionally demonstrates various interesting tech at PATACS meetings. He began working with audio recording tech in high school, worked as a DJ and news reader in college radio and television, and began working with personal computer digital audio in the 1980s. In July 2018 at a joint meeting of PATACS and OLLI OPCUG in Fairfax City VA, he demonstrated ways to use personal computers to create do-it-yourself ringtones. A software developer for major multi-server computer systems for many years, he is now a tech writer for a major maker of automated fingerprint identification hardware, supporting a federal agency’s system in which that hardware plays a major role.