CAEUG

Computers Are Easy User Group

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers **A**re **E**asy **U**ser **G**roup

March
2014
Volume XXXI Issue 3

Confirmed meeting dates

March 22
4th Saturday

April 26
4th Saturday

May 24
4th Saturday

Check
www.caeug.net
for confirmed
meeting dates

MEETING
PLACE
is the
Glenside Public
Library
*** ***

Visitors
Welcome
HOPE TO SEE
YOU THERE!!

* * * March 2014 meeting * * *

March meeting -- March 22 4th Saturday

Our presenter: Mike Goldberg will present an
Eli the Computer Guy video on backups

New year reminder to all members: Dues are due every January!

For just $20.00 a year you receive ten informative presentations. The bonus is all presentations is accompained by coffee, donuts & bagels, your choice. Don't forget our wonderfully relaxing annual CAEUG picnic.

THIS YEAR ANNUAL PICNIC ON
SATURDAY JUNE 21, 3RD SATURDAY.

Also, you will have the opportunity to bring your computer related problems to the Members forum at every meeting. You could have your computer problem solved with the wealth of knowledge of other members. That means a huge savings to you not having to call a heldesk that could charge you big bucks. You also will continue to receive the ARI CAEUG monthly newsletter.

To renew your membership see John St. Clair, Treasurer, at the third Saturday, March 22 meeting and pay your annual dues.

Table of Contents

Backups and Disk Cloning

Recap of October 2013 Meeting by Anne Moss
Secretary, Northern Neck Computer Users' Group, NJ
October 2013 issue, The Computer Link
www.nncug.org
mcmillan (at) va.metrocast.net

Brian Riley, Vice President of the NNCUG, gave a Membership Meeting presentation on computer backups and cloning of hard drives. Most of his presentation centered on what you can do to get your computer working quickly after a virus infestation or hard drive failure.

He explained that while backing up is necessary, the problem is that you have to have a working operating system and backup software to restore the backup you made. This may entail having to reinstall the operating system and backup software before you can even start to get your computer back.

He then explained the difference between cloning a disk and making a disk image. With cloning a disk, you get an exact copy of the disk, that if inserted into your machine, will allow you to resume work from the point the clone was made. Disk imaging on the other hand, which is how backups work, makes a copy of the contents of the disk in some kind of compressed format (zipped), which then has to be restored by a program that can read that format.

Usually this is done with a "restore" disk, which is a bootable CD or DVD that contains enough of an operating system to run the backup software that can restore your drive, but requires you to make that disk ahead of time. If you haven't done that (and most backup software, including what comes with Windows 7, has utilities to make one of those disks), you need to restore from the original Operating System Install disks. This is a time consuming process!

Brian showed us what he called a "toaster" drive, which is a USB or ESATA device that allows you to put a regular 3 ½ " (desktop hard drive) or 2 ½" (laptop drive) in a slot, and run your backup or clone to it.

Tiger Direct has a listing of toaster drives here (NewEgg and Amazon have them also)
http://www.tigerdirect.com/applications/category/category_slc.asp?MfrId=0&CatId=2785

He then explained that if you have chosen a computer that has your C: accessible from the outside of the machine, you can take that disk and easily and quickly replace the damaged or infected drive with it.

Brian explained he had made a clone of the laptop drive he was giving the presentation on the night before, he simulated the computer becoming infected with a virus, shut it down, replaced the hard drive, and rebooted continuing the demonstration, all within three minutes.

He pointed out making a clone is not the complete answer to backups: clones do not do versioning of your files for example, and it is still important to do a regular backup.

Con't pg 3

There are two key questions you have to ask yourself in choosing a backup method:
How important is my data? Is merely having a second copy of it enough, or does it have to survive a catastrophic event like a fire? If it is the latter, you must have an offsite backup, if it isn't then just a backup copy will do.

How much important data do I generate in what period of time? If you spend all day working on a project, then you probably want a backup on a daily basis. If redoing everything you have done for a week isn't a problem, then a weekly one will do. If all you do is play games on your computer and answer e-mails on line, then you probably don't need more than a clone – your data isn't changing.

Things that cause data loss come in many forms: from "happy clicking", where you accidently overwrite something you have been working on all day with an inappropriate up-date; virus infestation that makes your machine unusable and may scramble the contents of your hard drive; hard drive failure (sooner or later they all fail); or catastrophic event such as a fire or burglary.

Even if you are using anti-virus software, your machine can become infected by a virus that was built to get around that software. Often the first thing these viruses will do if they manage to get a foot-hold on your machine is turn off your anti-virus software.

Brian suggested a simple step: since many viruses work on the account level, you should always create a second account on your machine with administrative privileges.
This may allow you to log in as that other user and run your anti-virus software that has been disabled under your main account.

He also suggested you should hover over any link with your mouse to see where it is sending you. Depending on the application, the address the link is sending you to will be displayed in a tool-tip or on the bottom of the screen. If that address goes somewhere unexpected, don't click on it!

What backup software should you use?
Windows 7 ships with backup software, and allows you to make a restore disk. It doesn't do cloning, it isn't easy to tell what it is backing up, and the backup requires a disk larger, sometimes double the size, of the drive you are using as your C: In other words you would need a one terabyte drive to back up a 500 gigabyte one.

It was suggested using Macrium Reflect, which is available as either free or paid software. The major difference for the home user between the two is the free version can't do incremental backups (that is, only backup the files that have changed since your last full backup). You can read more about it on their website:
www.macrium.com/reflectfree.aspx

Along with the free version, the Standard version costs $49.99, and the Pro version costs $58.99.

There is cloning and backup software available from other vendors also.

Con't Page 4

Acronis is another backup/cloning program. Brian and Rob stated it is much more
Bloated but not as user friendly as Macrium.

If you are interested, reviews of 10 of the top contenders for 2013 can be found here:
http://data-backup-softwarereview.toptenreviews.com/

Brian emphasized that if your concern is getting your computer up and operating as quickly as possible from a simple hard drive failure or virus infestation, then cloning is the way to go.

He also made the point that one does NOT have a backup UNTIL it is confirmed that the data can be RESTORED from the backup!

Cloud Storage - Are You Concerned?

By Bill Armstrong, Treasurer
Lehigh Valley Computer Group, PA
November 2013 issue, The LVCG Journal
https://sites.google.com/site/lvcgsite/
Bill (at) yahoo.com

There has been discussion at our Lehigh Valley Computer Group meetings about cloud storage. Concerns include not being able to retrieve your data without an internet connection, and the safety of your sensitive data. Who is looking at it? Is it encrypted? Can the government get at it and see all your data? Can the company hosting the data read it?

These are legitimate concerns, especially since the recent revelation about the NSA spying on our domestic phone calls, emails, and cloud stored data.

In today's Morning Call, I found an ad for Best Buy. It offers a solution to this concern that is very practical.

Western Digital offers their My Book Live Personal Cloud Storage external hard drive (HD). This unit attaches to your wireless router. That makes it available to every connected device that you own, both in your house, and when away from it (via the internet). That means your smart phone, tablet, and laptop, whatever. There are apps for both Android and iOS. You can store movies, photos, and all kinds of data, and access them anywhere you have an internet connection. It also makes a good place to share files with other family members, no matter where they are located. Public and Private shared accounts can be created.

Because the data resides on your personal hard drive in your home, the worries about others (government, hackers, etc.) getting that data is greatly reduced, if not eliminated. Your data is safely stored behind your user ID and password (as well as your router's security), which is as safe as you choose to make it (long, complex passwords are recommended).

The cost is not excessive. Best Buy offers the Western Digital 2 terabyte (TB) version for about $130, and the 3 TB version for about $150. The included software makes backup of your computer very easy.

Con't pg 5

Online backup services, such as Carbonite and iDrive cost about $60 per year. This unit would pay for itself quickly, and offer the added privacy of local storage.

One drawback that I can see is that if my house should burn down, or thieves should steal the HD, your data is gone. Cloud storage is safer in that respect. Any very safe storage system should include off-site storage in some manner. It could be as simple as burning DVDs and storing them in another location.

So, to summarize, it is an interesting solution with many positives, but not a perfect one.

Lamp Post 156
March 2014

Last month I reported a problem with my Microcenter **(1)** 128GB flash drive. I went to the Westmont Microcenter **(2)** service department to see if they would be able to reformat the drive. A supervisor was at the desk and asked if I wanted to recover data from the drive. I told him that I back up the drive and that recovery would not be necessary. He then replaced the drive with a new one. I was delighted with that solution to the problem. I recommend shopping a Microcenter.

1) http://www.microcenter.com/
2) http://bit.ly/1qJ0TdB

Security Alert for Apple **(1)** products iOS **(2)** and OS X **(3)**
Secure Sockets Layer (SSL **(4)**) authentication did not work in iOS or in OS X. It did not work because of a software 'error'. Wired Magazine **(5)** has in depth explanation of the error in Apple software and what it means. In short, SSL is the protocol that provides secure communications between a server and your browser which displays the https **(6)** in the address box (the browser may also display a padlock). You see the https and padlock on banking sites, retailing sites, and donation sites. Generally, any site where money is transferred. If the https and padlock are not displayed, the communication is not secure and subject to easy cracking. Sophos **(7)**, the anti virus company, has a page **(8)** that describes the code and why it is called the Goto-Fail error. The program was written in C **(9)**. Here is the C code 'error';

```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0) <=== this is the 1st if statement
    goto fail;                    <=== this is the instruction if the if statement evaluates to true
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;                    <============== this line is the 'error'
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

Each if statement is ended with a semi-colon. Each line is evaluated one at a time in order. If the

if statement evaluates to true the goto fail statement is executed. What appears to be the fifth line of code is goto fail;. It is actually the third line because each line is ended with a semi-colon. The fourth line of code will never be executed because the third line will always execute first. When the third line of code is executed (goto fail;), the SSL authentication fails. The page will be displayed, but no secure communication is possible. What this means to you is that if you did banking, purchased something, or donated money, your user name, password, and / or credit card data could have been compromised. Pundits and others are calling this an error. I do not think it is. Companies that develop software (programming) like Apple use software development kits (SDK **(10)**) and version control software. These tools help in the writing of software by preventing simple errors like this one. These tools would also tell management which programmer committed the error and what date and time it happened. Apple management had to have known about this, but shipped the product anyway. If this is the case, I would wonder how many other 'errors' were shipped. ZDNet has an article **(11)** about the 'culture' at Apple and what it means to Apple users.

1) https://www.apple.com/
2) http://bit.ly/1gqUpXP
3) http://bit.ly/Ola1Gp
4) http://bit.ly/1kyUMoD
5) http://wrd.cm/1iRZH6u
6) http://bit.ly/1qJ19Jz
7) http://www.sophos.com/en-us.aspx
8) http://bit.ly/1kV6PiA
9) http://bit.ly/1eHGOvR
10) http://bit.ly/1od7eMb
11) http://zd.net/1gwlmOs

Security Alert a Cryptolocker (**(1), (2)**) derivative is now available
SecureWorks **(3)** reported that Powerlocker **(4)**, a derivative of Cyroptolocker, is being sold to anyone with $100 US in Bitcoin **(5)**. SecureWorks has analyzed Powerlocker and said it is a re-engineered version of CryptoLocker. They found it not nearly as capable as Cyrptolocker. The seller reports that 'updates' will be available for $25 US in Bitcoin.

1) http://bit.ly/1fBfgHY
2) https://en.wikipedia.org/wiki/CryptoLocker
3) http://www.secureworks.com/
4) http://ubm.io/1gCP1lb
5) https://bitcoin.org/

Security Alert on WeMo **(1)** devices
WeMo home control devices similar to X-10 **(2)** are made by Belkin **(3)**. Just so you know where I stand, I stopped buying Belkin products about 17 years ago because I found them inferior to other brands. The trouble with WeMo was discovered a few weeks ago **(4)**. Because a private key was released **(5)**, hackers could take control of the devices controlled by WeMo and perhaps the local area network (LAN) in a victim's home **(6)**. Belkin announced that they had fixed a few of the problems **(7)**. If you use WeMo remote control, you may want to disconnect it until all the problems are solved.

Con't pg 7

1) http://bit.ly/1isLpXm
2) http://www.x10.com/x10-home-automation.html
3) http://www.belkin.com/us/
4) http://www.kb.cert.org/vuls/id/656302
5) http://bit.ly/1ibxwfj
6) http://zd.net/1eHHcdO
7) http://zd.net/1kV7b8U

There is a scam that is primarily affecting Europe but has the potential of spreading to the United States (if it hasn't already). Italian police in Genoa are investigating **(1)** four attractive young women who, with the use of social media, strike up online friendships and then entice the victim into increasingly explicit sexual behavior to be recorded by webcam on Skype **(2)**. They then demand payment of 500 Euros so that the video is not put on the Internet. Sometimes the contact list is stolen from the victim's social network sites. StaySmartOnline **(3)** has an explanation of this type of blackmail and what to do about it **(4)**. StaySmartOnline reported that sometimes the images are altered to make them seem worse than they actually are. This was reported last August (2013) in the London Telegraph **(5)**. More recently, Tom's Guide reported a more sophisticated extortion **(6)**. Microsoft (MS **(7)**) acquired Skype in 2011. MS cannot be blamed for this criminal activity although they might offer to cut off accounts that are linked to this activity. They may be helping the police, but there are no reports of this. Facebook **(8)** is the social media mentioned the most in these reports. Evaer software **(9)** seems to be the software used to record the Skype phone calls. It cost $20 US. Information Week Magazine and StaySmartOnline both have pages dedicated to helping people avoid social networking scams (**(10), (11)**).

1) http://bit.ly/1kV7cd3
2) http://www.skype.com/en/
3) http://www.staysmartonline.gov.au/
4) http://bit.ly/PG3KpX
5) http://bit.ly/1qJ1DPU
6) http://bit.ly/1cNru5z
7) http://bit.ly/1lGxpJD
8) https://www.facebook.com/
9) http://www.evaer.com/
10) http://ubm.io/1isLKJz
11) http://bit.ly/Ou6C7Z

Yahoo **(1)** webcam chats were recorded by Government Communications Headquarters (GCHQ **(2)**) with the aid of the National Security Agency (NSA **(3)**) according to The Guardian **(4)**. GCHQ is the british equivalent of the NSA with a focus of computers and communication. Per their web site, "Everything we do is governed by law, and overseen by the Foreign Secretary and other Ministers." Sounds similar to the NSA malarkey, "We will protect national security interests by adhering to the highest standards of behavior. **(5)**" Notice its just behavior and not ethical behavior. The GCHQ program is called Optic Nerve. Because GCHQ does not have the resources or funding of the NSA, they were only able to collect one still frame (photo) for every five minutes of webcam chat (video). These pictures were collected in a giant fishing expedition - no warrents, not looking for anyone specifically (sound familiar?). At least in the U.K., they are not

Con't pg 8

plagued by The Constitution. Many of the photos were of non-British english speakers including U.S. citizens. The Guardian says, "... legal authorisations are required before analysts can search for the data of individuals likely to be in the British Isles at the time of the search. There are no such legal safeguards for searches on people believed to be in the US or the other allied "Five Eyes" nations - Australia, New Zealand and Canada." Yahoo told The Guardian, "Yahoo strongly condemned the Optic Nerve program, and said it had no awareness of or involvement with the GCHQ collection." I do not know whether to believe that or not. It really depends on how sneaky GCHQ is as opposed to NSA. GCHQ said that three to eleven percent of the photos contained "undesirable nudity". I wonder how they would know that without looking at every picture. That is a lot of pictures when they collected 1.8 million pictures every six months. Another thing to remember is that in the U.K., you have no rights. I suggest covering the web cam when you are not using it and try not to use it for any reason unless you do not value privacy.

1) https://www.yahoo.com/
2) http://www.gchq.gov.uk/Pages/homepage.aspx
3) http://www.nsa.gov/
4) http://bit.ly/1iSDfG7
5) http://www.nsa.gov/about/values/index.shtml

Speaking of the NSA and social media, The New American Magazine reported **(1)** that the NSA created web site(s) that looked and acted like Facebook servers. The article was covering the most recent revelations by Edward Snowden **(2)** through Glenn Greenwald **(3)** at the Intercept **(4)**. The release also told of broadcast e-mails that were rife with malware. In previous Snowden released documents MS, Facebook, Yahoo, Google, PalTalk, AOL, Skype, YouTube, and Apple all had given access to federal agents to snoop on their users. That line up of companies gives me a sick, creeped out feeling, because I have used some of those services in the past. The article quotes Mikko Hypponen, from the Finnish computer security firm F-Secure **(5)**. He said the revelations were disturbing and that the NSA's deployment of malware create potentially new vulnerabilities, making them more vulnerable for attacks by third parties. He thought that the NSA could justify using malware in a small number of cases against known adversaries, but millions of malware implants is 'out of control'. Forbes Magazine reported on the Facebook posting by Mark Zuckerberg **(6)**, founder and owner of Facebook. The posting **(7)** reported that Zuckerberg called (on the telephone) President Obama to complain about the NSA. The comments in response to that article used the word posturing and hypocrisy quite a bit. I agree inasmuch as a previously released NSA document has already implicated Facebook's complicity in government spying. The Electronic Frontier Foundation (EFF **(8)**) participated in the Office of the Director of National Intelligence Review Group which wanted comments. The EFF provided a four page document **(9)** which calls for a dismantling of the NSA due to a culture of rights violations. Specifically, the document says that the NSA is 'out of control'. Jimmy Wales, founder of Wikipedia **(10)**, told CNBC **(11)** that, "... recent revelations have shown a government that's completely out of control, lying to Congress, doing things that are blatantly unconstitutional...". The spying has not stopped. Using Windows on a regular basis as well as Google, Facebook, Yahoo, PalTalk, AOL, Skype, YouTube, or Apple services or products puts your rights at risk (even if you have nothing to hide).

1) http://bit.ly/1gCPHqN
2) http://bit.ly/1eHHNMp

Con't pg 9

3) http://bit.ly/1malkzr
4) http://bit.ly/1dbdxJj
5) http://home.f-secure.com/en_US/
6) http://bit.ly/1ibxPHf
7) https://www.facebook.com/zuck
8) https://www.eff.org/
9) http://bit.ly/1e8iOoF
10) https://www.wikipedia.org/
11) http://www.cnbc.com/id/101494036

The Decorah bald eagles **(1)** have three eggs this year. The new nest is now equipped with a camera for a close up look at the hatching which should take place around the beginning of April. The camera is supplied and operated by the Raptor Resource Project **(2)**. Decorah **(3)** is in northeastern Iowa.

1) http://www.ustream.tv/decoraheagles
2) http://www.raptorresource.org/
3) http://www.decorahia.org/decorah.asp

Mark your calendar for April fifth. WGN's **(1)** Tom Skilling **(2)** is hosting the 33rd annual tornado seminar (**(3), (4)**) at Fermi National Accelerator Lab **(5)**.

1) http://wgntv.com/
2) http://bit.ly/1gqW8fY
3) http://1.usa.gov/1g12WXi
4) http://bit.ly/1malC9z
5) http://www.fnal.gov/

Between you, me and the LampPost, that's all for now.

Now for something completly different

Magic - Pick a number, any number. Now double that number. Now add 10 to it. Then, subtract 4....Divide that number you now have by 2. OK, now subtract the number you orginally picked. Add 49 to it...Your number is 52!

1. "It was a cold, bright day in April, and the clocks were striking 13" So begins what novel by George Orwell?

2. What state capital is the southernmost among the 48 contiguous states?

3. National Pi Day falls on what day in March?

Answers: 1. "1984" 2. Austin, Texas 3. March 14 - The real "Pi" moments occur March 14, at 1:59 a.m. and p.m. (314159.....)

March DVD of the Month

Adapter - Media converter
ARI - March newsletter
AuslogicsDefrag - Updated HD defrag program

cCleaner - Updated HD cleaner
CDBurnerXP - Updated CD DVD burning program
CDOMlists - Lists of past CDOMs and DVDOMs
CoreTemp - System monitor program

F-SecureKEY - Password and User name secure storage
FormatFactory - Media converter
FreeAudioEditor - The name says it all
FreePortScanner - Scans network ports for activity
FreeTrimMP3 - Trims MP3 files

GPUShark - Monitors the graphics card

Jarte - Free word processor

KFKfileSplitter - Slits large files into smaller ones

Liberkey - Free office suite

MaxthonCloudBrowser - Internet browser
MemberContributions - Things e-mailed to me from members

NADetector - Monitors and analyzes the network traffic

OldTimeRadio - Old time radio broadcasts

PasswordUncover - Reveals passwords under the dots
Photoimp - Updated photo editor
PicEdit - Photo editor program

ShouldIRemoveIt - Malicious process remover
StartMenuReviver - Win 7/8 start menu
StartW8 - Win 7/8 start menu

UltraVirusKiller - Free virus killer

WebOfTrust - Web site to install WOT
WindowsFirewallControl - Configure Win 7/8 firewall
WindowsHotfixDownloader - Find the updates needed for your Windows

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at
. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg at, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline
- Billy Douglas

Beginner hardware problems
- Dick Fergus

Hardware problems, XP, Win 7 & Linux
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter Ed	Kathy Groce
Board Member	Billy Douglas
Webmaster	John Spizzirri