Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXIV | May 2014 | Issue 5

The Prez Sez

by John Pearce, President, P*PCompAS

Bob Blackledge, our Vice President, has a selection of videos for the May meeting. It looks like the topic of faster home WiFi performance made the top of the list.

My thanks to Bob for presiding at the May meeting in my absence. ☺

Meeting Minutes

by Toni Logan, Secretary, P*PCompAS

The 5 April 2014 meeting was called to order at 9 am by President John Pearce. Coffee and donuts are free to first-time visitors and a donation for all others. The coffee is from Laura at Starbucks at the Citadel Crossing.

Vice-President Bob Blackledge reported that the presentation for this meeting will be a video on XP after Microsoft stops supporting it. The stop date for XP is April 8, 2014. There was some discussion as to whether Microsoft will rescind the end of support, but the consensus was that they will stop supporting XP except for the server product.

There was a motion and a second to approve the minutes as printed in the newsletter. The motion passed.

Next P*PCompAS meeting: Saturday, 3 May 2014
VP Bob Blackledge will show a selection of Lynda.com video tutorials.

OFFICER REPORTS

Vice-President Bob Blackledge reported on the presentation today and for next month.

Secretary Toni Logan had nothing to report.

The Treasurer's report was as follows: savings account balance is $5813.04, and the checking account balance is $1226.18, for a grand total of $7039.22 in the treasury.

Newsletter Editor Greg Lenihan reported that the next deadline is April 19, 2014, which is the same date as the breakfast.

Media Rep Ilene Steinkruger reported that she sent the latest newsletter to the members via e-mail. There is a large selection of books from Taylor and O'Reilly, but she doesn't want to order unless there is an interest. If you have any questions about the books, or if you want a certain one to review, let her know.

Membership Chair Ann Titus reported that only eleven of our past members have not renewed. She has sent them reminders.

The one guest was the daughter of Ann Titus, Beverly Kurtz, who works for IBM.

OLD BUSINESS

The President reported that the church had three needs: a Kitchen Aid Mixer, the entrance painted, and a new entrance mat. After some discussion, a motion to buy the Kitchen Aid Mixer was made by Pat Krieger and seconded by Warren Hill. The motion passed.

The next meeting is Saturday, May 3, 2014. If you are doing your spring cleaning and have anything to donate to the drawing, please bring it to the meeting.

The meeting then broke for a recess and refreshment. The business meeting was called to order again and a motion was made by Jeff Towne and seconded by Chuck Kinsley to purchase the Professional Kitchen Aid Mixer for $299 plus tax. The motion passed.

NOTE: The mixer was purchased at Sam's club by a member and was shown during the meeting.

AROUND THE ROOM

Some of the discussion in Around the Room was on uninstalling software; virus programs; Windows 8; the end of support for Windows XP, and radio programming on KVOR. The audio of the meeting is on our website.

PROGRAM

The program was a video on XP after Microsoft stops supporting it.

Continued on page 6

In This Issue

Articles

P*PCompAS

Officers

President: John Pearce
jlpnet@comcast.net

Vice President: Bob Blackledge
ms5mjkk49z@snkmail.com

Secretary: Toni Logan
bradtonilogan@gmail.com

Treasurer: Dennis Conroy
dennisconroy@comcast.net

Staff

APCUG Rep/Webmaster: Joe Nuvolini
Editor: Greg Lenihan
Librarian: Paul Major
Membership: Ann Titus

Committees

Hospitality: Pat Krieger
Programs: Bob Blackledge
Publicity: Bob Blackledge
Nominating: Frank Fraser

Board of Directors

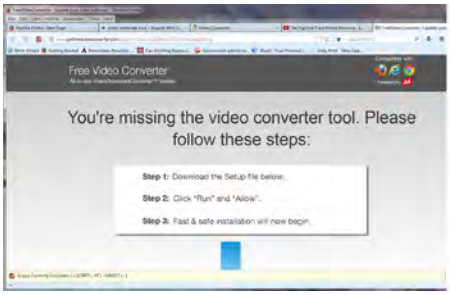
Bill Berkman
Toni Logan
Norm Miller
Bob Blackledge
Warren Hill

Nybbles and Bits

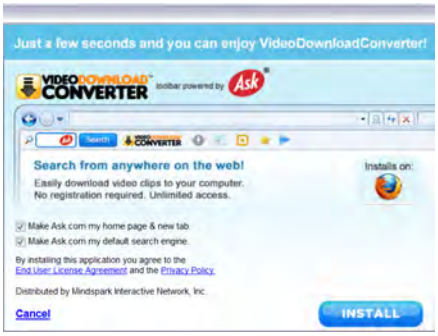
by John Pearce, P*PCompAS

Below is a screen snip showing the pop-up I described at the April meeting. It randomly appears when I'm watching YouTube videos. It does not look like the typical YouTube advertising because it does not go the full width of the window and there is no "x" to close the pop-up.

Clicking on the link "Click here" takes you to www.videoconverter.com.



If you click the link to get the free converter, you get this popup.



Mindspark Interactive Network seems to be a reputable company. It is part of IAC Corp. I didn't click "Install" so I still don't know if this in legitimate or malware. ☺

The Pikes Peak Computer Application Society newsletter is a monthly electronic publication. Any material contained within may be reproduced by a nonprofit user group, provided proper credit is given to the authors and this publication, and notification of publication is sent to the editor. Any opinions contained in this newsletter are made solely by the individual authors and do not necessarily reflect or represent the opinions of P*PCompAS, its officers, or the membership. P*PCompAS disclaims any liability for damages resulting from articles, opinions, statements, representations or warranties expressed or implied in this publication.

P*PCompas welcomes any comments, letters, or articles from members and non-members alike. Please send any articles to the editor (see last page for address). The editor reserves the right to reject, postpone, or edit for space, style, grammar, and clarity of any material submitted.

I picked up a Lepow Moonstone 6000 Power Bank at CES. It is a portable power bank used to charge your cell phone, bluetooth device, tablet, etc. The unit comes with a cable with a USB connector at one end and a micro-USB connector at the other that can be used to charge the Moonstone 6000, as well as charge your device. The unit has one micro-USB input port for charging the Moonstone and two USB output ports for charging your device(s). One has a 1200mA common mode output, the second a 2100mA quick charge output. The capacity of its Li-Polymer battery is 6000mAh. The current sale price at the Lepow Website is $19.99. For more information, visit: **http://lepowglobal.com/products/moonstone/**.

Nuggets from Nuvo

*by Joe Nuvolini, P*PCompAS*

ChargerLeash is a device that was not shown at CES this year but was sent to me after the show by its promoter. It can be seen at their **http://www.chargerleash.com** Website. It is a 3-foot long cable that will charge and/or sync devices. The cable has a USB connector at one end and a micro-USB connector at the other suitable for charging cell phones, blue tooth devices, and tablets.

In the middle of the cable is a device that contains an LED and beeper. If the device you are charging is disconnected from the cable, the LED turns red and shortly thereafter, the device beeps. This is supposed to remind you not to leave the cable behind when leaving your hotel, or to alert you if someone disconnects your device while its charging in a public charging area. The device works as advertised if you disconnect the device from the charging cable, but it does not if you unplug the cable from the charging supply. I have an issue with the pricing. The model I have is $22.99, There are two Apple models at $26.99 and $34.99. There is another model with multiple charging tips for $34,99. You can buy a USB-to-micro-USB charging cable from Amazon for under $2.00. I found one ad that offered 10 three foot USB-to-micro-USB cables along with a 110 VAC to 5 VDC USB charging device for $9.95 plus shipping. It doesn't seem like a very cost effective solution to me, even though it came with a gift of a mono hands-free phone headset, a $4.39 value on Amazon. ☺

It was the day before Easter when the digerati filled the Country Buffet meeting room with good humor and good food, and everyone felt blessed to be able to rise from their chairs.

Surviving Microsoft's Decision to Cease Updates to Windows XP

*by Bob Blackledge, P*PCompAS*

The presentation for the April P*PCompAS meeting included:

I) TWiT episode 1068 from: http://TWiT.tv/ttg. Note that TWiT is primarily a call-in talk show by Leo LaPorte, "The Tech Guy".

II) SecurityNow episode 445 from http://twit.tv/show/security-now/445, which has a talking heads interview/discussion format between Leo and Steve Gibson (a well-known security expert).

So, what do you do now? What follows is derived from the TWiT tip of the week from TechGuyLabs 'Securing Windows XP' and Security Now. These steps are things that you should already have been doing, but it is now more crucial to be "Security Aware." Importantly, WindowsXP will not suddenly crumble without frequent updates, but you should use it with (more) discretion!

1) Install Windows XP's final updates:
On my WinXPsp3 sytem, this consisted of:

- KB2936068 MS14-018 Security Cumulative iE8/XP
- KB2878236 MS14-017 Security MicroSoft Office '07
- KB2922229 MS14-019 Security Spuninst.exe and Kernel32.dll
- KB2878304 MS14-017 Security MicroSoft Word Viewer
- KB890830 Windows Malicious s/w Removal Tool (also known as MRT)

2) Use Windows XP with a "limited user" account, not Administrator.

a) Consult www.wikihow.com/Create-a-New-User-Account-in-Windows-XP.
b) Create a (new) Administrator account and specify a password.
c) Log out of your current account, log in as the Adminstrator.
d) Go into Control Panel, User Accounts again and change your normal account's privilege to be a "Limited User" (my default was "Owner")
e) From now on, any new software you install, and any significant changes to system settings will have to be done from the Administrator account, so don't lose the password! When you do an install something, specify it for "All Users" (or your specific default account) so that you can use it!

TIPS #2 and #3 alone would have avoided most/all security problems reported in the last year!

3) Use the Google Chrome [or Firefox] browser instead of Internet Explorer IE/XP, currently at version 8 (vs 11). It will no longer be updated at all! Go to www.google.com/chrome/ or www.mozilla.org/en-US/firefox/new/. Chrome includes their own PDF viewer which they maintain. Both Chrome and Firefox can be automatically updated!

4) Make sure ALL programs are patched and up to date, check regularly. Certainly patch Microsoft Office '07 (and earlier) programs! Any program that allows scripting should be considered dangerous!

5) Download software only from original vendors, or at least really trusted sources!

6) Don't click on links in e-mail at all...ever! If you get e-mail with an important looking link, go to the relevent base Website on your own to view or interact.

7) Keep antivirus software up to date, and run scans regularly. Note that Microsoft's "Security Essentials" will continue to be updated for the foreseeable future.

8) Connect to the internet through a router, even with only one computer! Any recent router includes a NAT firewall which is invaluable protection!

9) Disconnect Windows XP from the Internet. While this statement is a little overly strong, certainly disconnect when not in use!

Additional advice from me:

10) De-install (or at least disable) Java, Flash, Shockwave, Adobe Acrobat and Adobe Reader (use Foxit or another program for PDF files). These programs have had numerous problems in the past, and shouldn't be trusted any further with XP!

11) If you have a software firewall (such as in XP), enable it! ☺

Heartbleed Vulnerability and Your Passwords

Published with permission from Ira Wilsker, Golden Triangle PC Club, columnist for The Examiner, Beaumont, TX

WEBSITES:

http://krebsonsecurity.com/2014/04/heartbleed-bug-what-can-you-do/
https://lastpass.com/heartbleed/
http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/
http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/
http://www.cnet.com/news/heartbleed-bug-undoes-web-encryption-reveals-user-passwords/
http://www.techsupportalert.com/content/how-check-if-website-has-been-affected-heartbleed.htm
http://www.infoworld.com/t/security/5-no-bull-facts-you-need-know-about-heartbleed-right-now-240269
http://consumerist.com/2014/04/11/regulators-warn-banks-to-plug-any-heartbleed-security-holes-asap/
https://addons.mozilla.org/en-us/firefox/addon/heartbleed-checker/
https://ssl-tools.net/heartbleed-test

In recent days, the media has been heavily reporting a bug in the code that is supposed to encrypt our personal information as it travels between our browsers and its intended destination. This coding error, now known as the Heartbleed encryption bug might allow hackers to access the encryption keys or “Secure Sockets Layer - SSL” or “HTTPS” used on supposedly secure Internet links, potentially giving hackers access to the personal information being transmitted. Despite media hyperbole, as of this typing, there have been no documented and confirmed cases of hackers obtaining passwords and other personal data through this security hole in the commonly used encryption software utilized by most of the globe’s commercial servers. What the mass media has done with its extensive publicity of this programming bug is to alert miscreants of a potential security vulnerability in our Internet connections, giving them a virtual invitation to “come and take it!”

According to a report on the popular online technology news source cNet, “‘Heartbleed’ bug undoes Web encryption, reveals Yahoo passwords” dated April 8, “ “The problem, disclosed Monday night (April 7), is in open-source software called OpenSSL that’s widely used to encrypt Web communications. Heartbleed can reveal the contents of a server’s memory, where the most sensitive of data is stored. That includes private data such as usernames, passwords, and credit card numbers. It also means an attacker can get copies of a server’s digital keys then use that to impersonate servers or to decrypt communications from the past or potentially the future, too.” In this cNet story there were some allegations that some Yahoo! users were tricked into logging on to bogus websites, disclosing their usernames and passwords, but there is some debate as to whether or not this was due to the Heartbleed vulnerability or another identity theft technique.

Some of the pundits interviewed in the media warned that it was imperative for all users to immediately change all of their online passwords, and possibly even their usernames, or face imminent peril of identity theft. While it is a good security practice for users to periodically change passwords, and not use the same password on multiple online accounts, this immediacy may be premature. If a web server is currently insecure, and your password has already been compromised through this Heartbleed vulnerability (unlikely), changing your password may only give you a false sense of security as the potential hacker will likely also get your new password as well. If a particular web server where the user has an account has not been compromised by Heartbleed, there is no immediate need to change passwords, other than as a routine and regular security procedure. If a web server that had been vulnerable to Heartbleed has already been patched to close this security hole, then it may indeed be appropriate to change passwords. In fact, many of the major web services, banks, and online merchants have already announced that users should change passwords after they are notified that the Heartbleed vulnerability has been rectified.

It is fairly easy for users to determine if the websites that they visit are vulnerable to the Heartbleed bug; a variety of free utilities and browser plug-ins have been quickly developed that will alert the user of any potential risks. I have predominately been using the Firefox browser on all of my computers, and now there are add-ons that will instantly alert Firefox users if a website being loaded is vulnerable to the Heartbleed bug. I am currently using “Heartbleed-Ext 3.0”, published by proactiveRISK as a

Continued on page 6

Meeting (Cont. from page 1)

DRAWING

Bluetooth speaker—Toni Logan
TShirt—David George ☺

Bob Blackledge introducing our presentation topic in April

At the April meeting, we voted to give the Church a Kitchen Aid mixer as a gift. The Church was very appreciative of our generosity and sent these pictures of "Toni" putting it to good use.

Heartbleed (Continued from page 5)

Firefox plug-in. According to its author, "Whilst some servers have been patched already, many remain that have not been patched. Heartbleed uses a web service developed by Filippo Valsorda and checks the URL of the page you have just loaded. If it is affected by <sic> a Firefox notification will be displayed. It's as simple as that GREEN GOOD / RED BAD" (addons.mozilla.org/en-us/firefox/addon/heartbleed-checker).

There are also several free utilities that can inform the user if a website is subject to the Heartbleed bug. Gizmo's TechSupportAlert.com has posted an updated directory of web services (techsupportalert.com/content/how-check-if-website-has-been-affected-heartbleed.htm) that can inform the user if a particular website is safe or insecure, in terms of the Heartbleed vulnerability.

I used the utility provided by my password manager, LastPass Heartbleed Checker (lastpass.com/heartbleed) to check the merchant and banking websites that I frequently access; I was surprised to learn that my credit union server is "Probably" vulnerable. LastPass Heartbleed Checker reported, "Probably (known use OpenSSL, but might be using a safe version). SSL Certificate: Possibly Unsafe (created 4 months ago at Dec 20 17:49:52 2013 GMT). Assessment: It's not clear if it was vulnerable so wait for the company to say something publicly, if you used the same password on any other sites, update it now." I then used the LastPass utility to check my primary e-mail server, and found that it was vulnerable, but has since been fixed. Specifically, LastPass Heartbleed Checker reported, "Site: mail.yahoo.com;Server software: ATS; Was vulnerable: Possibly (might use OpenSSL, but we can't tell); SSL Certificate: Now Safe (created 5 days ago at Apr 9 00:00:00 2014 GMT); Assessment: Change your password on this site if your last password change was more than 5 days ago." In consideration of this information, I immediately changed my e-mail password, but will wait to change my credit union password until the credit union updates its online security. Unlike Yahoo! or my credit union, I will not be promptly changing my Microsoft related passwords, as, according to LastPass, "Was Vulnerable: No (does not use OpenSSL)," but routine password changes are still recommended. Registered users of the LastPass Password Manager (lastpass.com) can automatically check all of their frequently visited websites for the Heartbleed vulnerability," LastPass users can do this by running the Security Check tool from their icon menu. LastPass will not only alert you to which sites are vulnerable, but also tell you the last time you updated your password for the site, when that site last updated their certificates and what action we recommend taking at this time." A similar website checker is Qualsys SSL Server test at ssllabs.com/ssltest/index.html.

Some websites have posted updated susceptibility assessments for the most widely used web services. The website Mashable (mashable.com/2014/04/09/heartbleed-bug-

Continued on page 7

Live CD-ROMs

by Dick Mayback, Member, Brookdale Computer Users' Group, NJ, www.bug.com, n2nd (at) att.net

A live CD-ROM contains all the files normally stored on a computer's hard disk, and when booted, acts exactly the same as a hard disk, except of course that it can't store data. Although these media are normally called "live CD-ROMs," because they were available first, DVD-ROMs and USB memory sticks now can fulfill the same role. The hard disk plays no part when the PC boots from such a medium, and your PC will run fine even when its hard disk is malfunctioning or even absent. Moreover, the system leaves no traces on the PC of anything that occurred while it was running. However, the PC's hard disk is available as a storage medium, and, if it is operable, you can read from and write to it if you wish. Likewise, all the peripherals and ports are available; for example, you usually can access networks, including the Internet, use any USB devices, and do printing. There are several applications for live CD-ROMs:

- trial or installation of a new operating system,
- file system repair, backup, and restore, file recovery from corrupted hard disks, running diagnostics, disk cloning, and cleanup of malware, such as viruses and root kits,
- anonymous Internet browsing, and
- temporarily using other computers without risking making unwanted changes to them or leaving your passwords.

The overwhelming majority of portable operating systems are based on Linux, as both Microsoft and Apple require a separate purchase for each computer, and transferring one of their operating systems among several computers violates their terms of service. There are a few based on DOS, but they are quite limited compared to their Linux counterparts.

Live CD-ROMs are most often available in the form of ISO images. These aren't files; instead they are bit-for-bit copies of the contents of a CD-ROM or DVD-ROM. Many media burners can write these; if yours can't, make an Internet search for "iso image

Continued on page 8

Heartbleed (Continued from page 6)

websites-affected) has posted an extensive list of popular websites and their respective Heartbleed related security vulnerability. According to this frequently updates listing, while some of the popular websites were not vulnerable to this bug, others were, and most have patched their SSL software; those who have patched their software mostly are asking users to change their passwords. Mashable broke down its extensive list into categories such as Social networks, Financial, and others. Among the major web presences that were vulnerable, but now indicate that the security holes have been patched include Facebook, Instagram, Pinterest, Tunblr, Google, Yahoo!, Gmail, Yahoo! Mail (and its affiliates such as AT&T mail and SBCGlobal email), some Amazon Web Services

(but not the Amazon.com shopping service), Etsy, GoDaddy, Flickr, Minecraft, Netflix, SoundCloud, YouTube (Google says that YouTube users do not need to change YouTube passwords), USAA, Box, Dropbox, GitHub, IFTTT, OKCupid, Wikipedia (registered users only must change passwords), and Wunderlist. None of the major online financial services, stockbrokers, or password managers were ever threatened by Heartbleed, as they did not use the Open SSL software as a primary security tool.

While it is a good practice to periodically change passwords to hard to guess passwords which are alphanumeric, and incorporate upper and lower case letters, as well as some allowable punctuation characters, it is only imperative now to change passwords to those websites that were vulnerable, but which have been recently patched. The Mashable listing referenced above is a good source as to the Heartbleed status of the largest websites, but free Heartbleed checkers such as LastPass Heartbleed Checker can give the likely status of individual websites. If in doubt, go ahead and change your passwords, but be aware that changing a password on a website subject to Heartbleed that has not yet been patched will necessitate another password change as soon as the patch is implemented. Better safe than sorry. ☺

Live CD-ROMs (Cont. from page 7)

burners" to find a suitable application. You may prefer to use a live memory stick which is faster, more convenient to carry, and can also store data. If so, I recommend the free program *unetbootin*, which converts an ISO image to a suitable form and writes it to a stick. It's available for Linux, OS X, and Windows. Finally, if you have virtualization software, such as Oracle's VirtualBox, you can boot directly from the ISO image file without burning anything.

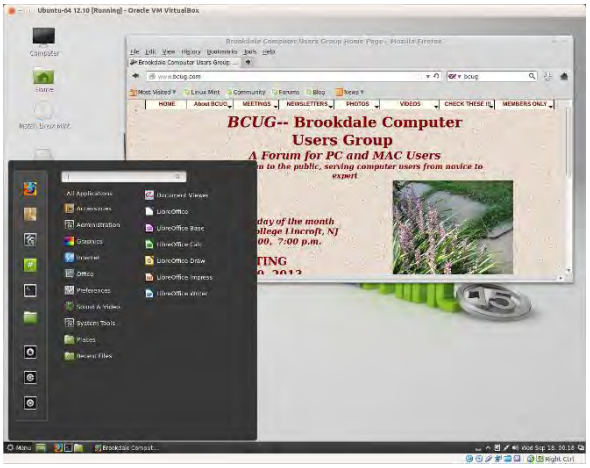
To use a portable operating system, a computer must be configured so that it checks its CD-ROM drive and USB ports for bootable media before it checks the hard disk. Most computers check for CD- and DVD-ROMs, but you may have to set up your ROM BIOS to check for bootable USB memory sticks. Owners of new machines will also have to disable the safe boot feature on Macs and secure boot on PCs. Secure boot is a new "feature" of PCs that prevents software from running unless it has been approved by Microsoft. You should be able to disable it, but not all PCs allow this. It will make running live CDs more difficult, and may prevent them from running on some machines altogether. Finally, the use of live CDs on Macs can be problematic; you may have to do some reconfiguration or even replace your wireless keyboard and mouse, as these can have proprietary drivers.

Using a live CD-ROM to try out Linux on a Mac or PC is a common application, but a Windows installation disk is also an example, although it's limited to installing and repairing Windows. Regardless of what is on the hard disk, your computer will boot the live CD-ROM system; the hard disk has nothing to say about this. So long as you don't write to the hard disk, you can do whatever you like without affecting the installed system, which won't even know a session has taken place. CD- and DVD-ROMs and even memory sticks are much slower than hard disks, so don't expect speed. Aside from this, operation should be the same as though the system on the live CD-ROM were installed on your hard disk. If you have enough RAM, some light versions of Linux will transfer themselves to a RAM-disk, and these will be quite fast.

There are far too many portable operating systems to cover in this short article; see **https://en.wikipedia.org/wiki/List_of_live_CDs** for very brief descriptions of many of them. Instead, I'll introduce some examples that you can use as starting points for the applications listed above.

Trying out a new operating system

Which operating system you try out depends on the age of your hardware. (The critical feature that older computers lack is Physical Address Extension or PAE.) If your PC is modern enough to run Windows Vista or later, you should consider Ubuntu (840 Mbytes) or Linux Mint (960 Mbytes). (See the following two screen-shots.) Both have complete office suites and all the other applications you are used to, and both have full-service user interfaces with more bling available than you really need.



If your hardware dates from the XP era, it may lack PAE or a modern display controller and you'll have to be more careful. Something like Xubuntu (840 Mbytes) runs fine on older machines, but includes all the modern Linux applications found in the top-of-the line systems. However, its user interface is more Spartan.

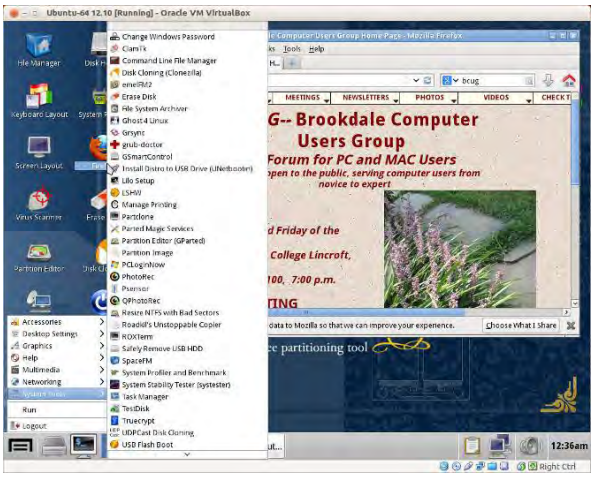
Diagnostic and Repair

For hardware and software maintenance and repair, I prefer Parted Magic (327 Mbytes), which

Continued on page 9

Live CD-ROMs (Cont. from page 8)

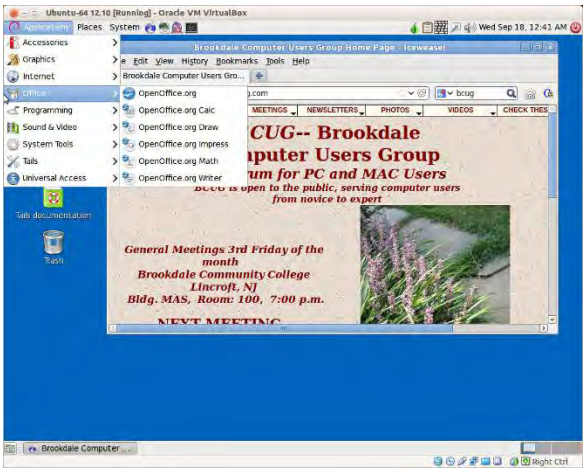
I discussed in my April, June, July, and August 2012 articles, available at http://www.bcug.com. (See the screen-shot below.) The standard version of Parted Magic requires PAE; for computers without this, look the version with “586” in its ISO filename. Unfortunately this valuable tool is no longer free, but its $5 cost is quite reasonable, and your can still find an older free version with a little searching. You may prefer SystemRescueCD, which also has a good reputation and is still free.



I haven’t found DOS and Windows portable systems, such as Ultimate Boot CD or BartPE, to be effective. There are also some specialized tools, such as Network Security Toolkit and BackTrack, for penetration testing, i.e., computer and network hacking, but they require substantial expertise and are interesting only to network professionals.

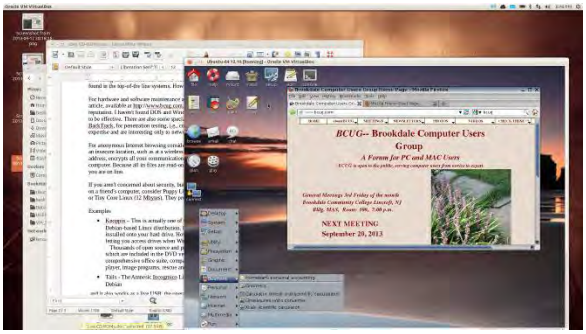
Anonymous Browsing

For anonymous Internet browsing consider Tails (897 Mbytes). (See the screen-shot below.) You would use this for doing Internet banking from an insecure location, such as at a wireless hot spot or while using a borrowed computer. (It also provides added security when doing on-line banking from home.) It hides your IP address, encrypts all your communications, and leaves no traces (such as passwords) on the host computer. Because all its files are read-only, it can’t be infected with malware, no matter how careless you are on line. If you operate Tails from a USB memory stick, you can create an encrypted directory on it to securely move files, so if you lose the stick, the finder can’t access your data. It does not require PAE and so should run on almost any PC.



Portable Computing.

If you aren’t concerned about security, but just want the convenience of having a familiar environment on a friend’s computer, consider Puppy Linux (173 Mbytes). It provides only the basics, but probably everything you need. (See the screen-shot below.) Like Tails, if you use a live memory stick, you can create a partition on it to store your files, but they won’t be encrypted, so don’t lose the stick.



Damn Small Linux (52 Mbytes) and Tiny Core Linux (15 Mbytes) are even smaller, but of course they provide more modest capabilities.

I’ve introduced only a few of the hundreds of available live operating systems and suggested only a few uses. If none of them suit your needs, check the Internet. ☺

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 3 May, beginning at 9 am (see directions below)
Next Breakfast Meeting: 17 May @ 8 am, Country Buffet, 801 N. Academy Blvd.
Newsletter Deadline: 24 May.

Check out our Web page at: http://ppcompas.apcug.org