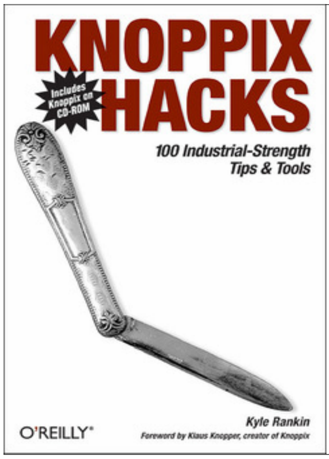
PACC TALK

Official Newsletter of the Pittsburgh Area Computer Club April 2011

MEETING SCHEDULE

Sunday, April 17, 2011

11:00 -11:25 am ROOM # 311	**Sign In, Pay Dues, Greet visitors, Purchase 50/50 tickets (Optional), Setup Computers, Connect to Internet , Prep for Meetings**
11:00 - 11:25 pm ROOM # 301	**PACC BOD Meeting**
11:35 - 12:00 pm ROOM # 301	**Windows New Users Can we help you? V. Agrawala**
12:00 - 12:30 pm ROOM # 301	**General Meeting, Raffle. (pg. 1)**
12:35 - 2:00 pm ROOM # 301	**System Information for Windows, TestDisk, WinHotKey …. (pg. 1)**
2:05 - 3:30 pm ROOM # 301	**More programs and utilities ….. (pg. 1)**
2:05 - 3:30 pm ROOM # 311	**Hardware SIG Users Helping Users - guests included**
1:00 - 3:30 pm ROOM # 311	**Linux SIG, Members Helping Members, Computer troubleshooting, Info Exchange**
3:30 - 4:00 pm	**Pack Up Equipment, Doors Close**



*** RAFFLE ***

Knoppix Hacks is an invaluable collection of one hundred industrial-strength hacks for new Linux users, power users, and system administrators using--or considering using--the Knoppix Live CD. These tips and tools show how to use the enormous amount of software on this live CD to troubleshoot, repair, upgrade, disinfect, and generally be productive without Windows--without the difficulty of installing Linux itself.

PJK

What is inside....

Windows SIG

As always, my intent is free software wherever it can be found. So…

System Information for Windows written by a superb programmer Gabriel Topala can be found at the following web site:

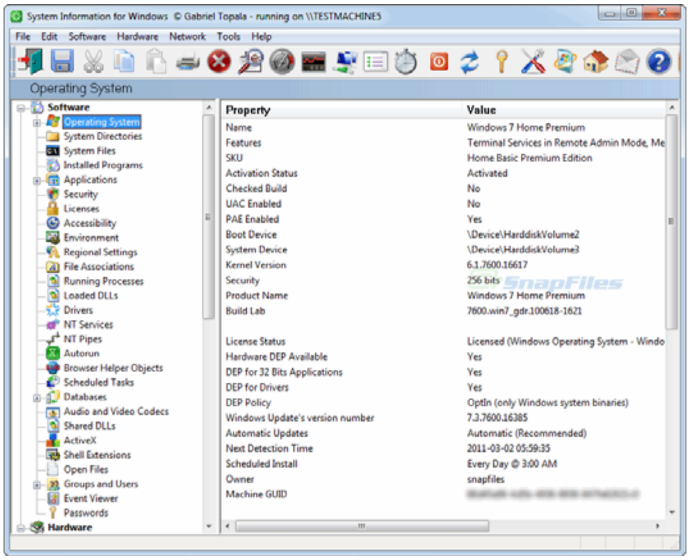
http://www.gtopala.com/

The program produces so much information, it is possible you may not need other of its type. Here are some excerpts from the site, and mind you they are not an exaggerations:

"SIW is an advanced System Information for Windows tool that gathers detailed information about your system properties and settings and displays it in an extremely comprehensible manner.

SIW can create a report file (CSV, HTML, TXT or XML), and is able to run in batch mode (for Computer Software and Hardware Inventory, Asset Inventory Tracking, Audit Software Licenses, Software License Compliance)…..

"SIW is a standalone utility that does not require installation (Portable Freeware) - one less installed program on your PC as well the fact that



Property	Value
Name	Windows 7 Home Premium
Features	Terminal Services in Remote Admin Mode, Me
SKU	Home Basic Premium Edition
Activation Status	Activated
Checked Build	No
UAC Enabled	No
PAE Enabled	Yes
Boot Device	\Device\HarddiskVolume2
System Device	\Device\HarddiskVolume3
Kernel Version	6.1.7600.16617
Security	256 bits
Product Name	Windows 7 Home Premium
Build Lab	7600.win7_gdr.100618-1621
License Status	Licensed (Windows Operating System - Windo
Hardware DEP Available	Yes
DEP for 32 Bits Applications	Yes
DEP for Drivers	Yes
DEP Policy	OptIn (only Windows system binaries)
Windows Update's version number	7.3.7600.16385
Automatic Updates	Automatic (Recommended)
Next Detection Time	2011-03-02 05:59:35
Scheduled Install	Every Day @ 3:00 AM
Owner	snapfiles
Machine GUID	[redacted]

(Continued on page 2)

(Continued from page 1)

you can run the program directly from an USB flash drive, from a network drive or from a domain login script. SIW can be distributed freely (ftp, archives, CD-ROMs ...).

Client Platform: Windows 7 / Vista / Windows XP / 2000 / NT4 / Me / 98 / Media Center / Tablet PC / WinRE / Bart PE / Winternals ERD Commander

Server Platform: Windows Server 2008 (R2) / Windows Server 2003 (R2) / Windows Server 2000 / NT4 "

One would do well to get this program, at only a 2.2 MB download at: **http://www.gtopala.com/siw-download.html**

Just go to the lower portion of the page and click on the one saying:

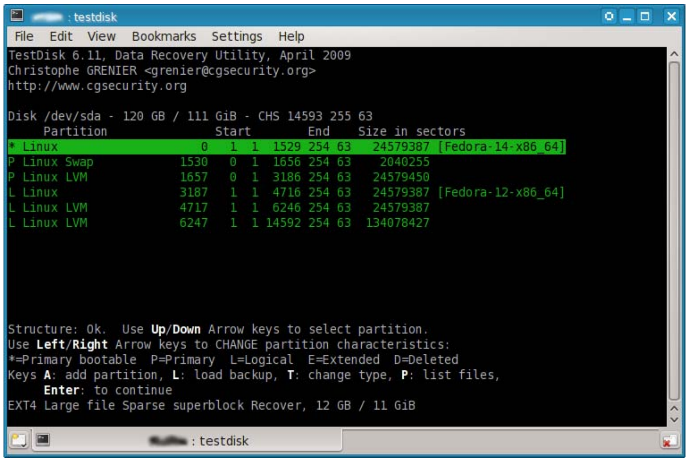
SIW Without Installer (English-Only)

———————————————————————————-

Yet another great freeware program to include in your toolbox is TestDisk. Only a 1.5 MB, character based, but it packs a punch!

"**TestDisk** is *powerful* free data recovery software! It was primarily designed to help **recover lost partitions** and/or **make non-booting disks bootable again** *when* these symptoms are caused by *faulty software*, certain types of *viruses* or *human error* (such as *accidentally* deleting a Partition Table). Partition table recovery using TestDisk is really easy."

TestDisk can: Fix partition table, recover deleted partition. Recover FAT32 boot sector from its backup. Rebuild FAT12/FAT16/FAT32 boot sector. Fix FAT tables. Rebuild NTFS boot sector. Recover NTFS boot sector from its backup. Fix MFT using MFT mirror. Locate ext2/ext3/ext4 Backup SuperBlock. Undelete files from FAT, NTFS and ext2 filesystem. Copy files from deleted FAT, NTFS and ext2/ext3/ext4 partitions. TestDisk has features for both novices and experts. ……" TestDisk can ***run*** under DOS (either *real* or in a Windows 9x DOS-box), Windows (NT4, 2000, XP, 2003, Vista, 2008, Windows 7 (x86 & x64), Linux, FreeBSD, NetBSD, OpenBSD, SunOS and MacOS X." Worth getting it, only 1.5 MB, get it from here:



```
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
     Partition               Start        End    Size in sectors
* Linux                    0   1  1  1529 254 63   24579387 [Fedora-14-x86_64]
P Linux Swap            1530   0  1  1656 254 63    2040255
P Linux LVM             1657   0  1  3186 254 63   24579450
L Linux                 3187   1  1  4716 254 63   24579387 [Fedora-12-x86_64]
L Linux LVM             4717   1  1  6246 254 63   24579387
L Linux LVM             6247   1  1 14592 254 63  134078427




Structure: Ok.  Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
     Enter: to continue
EXT4 Large file Sparse superblock Recover, 12 GB / 11 GiB
```

http://www.cgsecurity.org/wiki/TestDisk_Download

———————————————————————————

Increasingly I get annoyed having to look through Program Menu for a particular program I like to use. As many of you know there are a many shortcut Icons on my PC Desktop. Yeah.. Laugh! So I may have found at least a partial solution.

"WinHotKey allows you to assign "hot keys" that do various things. Actions that can be done with a hotkey are: 1. Launch a Program 2. Open a document 3. Open a folder 4. Automatically type something 5. Control other windows on the screen. …..The main goal of this tool is to be easy to use. There are many other hotkey programs out there, but most of them do not provide a sufficient level of "ease of use". This walks the user through the options, while remaining a

(Continued on page 7)

THIS AND THAT

By Elizabeth B. Wright, Member,
Computer Club of Oklahoma City
February 2011 issue, CCOKC eMonitor
www.ccok.org wright599new(at)sbcglobal.net

Last Fall my husband and I were part of a tour group which visited several countries. The most amazing part of the trip was how many of our fellow passengers had brought laptop computers and Kindle book readers. Since nearly all of us had digital cameras, we used our computers to download the images after each day's adventure. That gave us some reassurance that even if our cameras had been lost or stolen, the downloaded images would be safe on the computer. We were able to leave our computers in the care of the tour company while visiting the various sites of interest. Then we would have them with us later in our hotel rooms. The smartest thing I did was take with me a very small ACER Netbook and a very small Seagate 500G external drive. Also several USB flash drives for extra storage. The netbook computer was so much easier to carry than a full sized laptop, and all I needed it for was photo downloading and email. I did not try to do any photo enhancing or editing while still on the road. That was saved for my return home. And here it is January, and I still haven't finished!!

It is a bit difficult to explain how I nearly lost some of my pictures, but here goes. We took four cheap point and shoot cameras with us on the trip. Three of them used SD memory cards. At some point during the trip at least one card was interchanged between two of the cameras. In addition to that confusion, somehow the numbering system was duplicated in two of them, causing pictures with the same numbers appearing on two memory cards. Somehow, almost surely because of the daily downloading procedure, both sets of numbered images were salvaged. It took me quite a while after we returned home to figure out the problem and actually retrieve all of my images. At least I think they are all accounted for.

My personal accessories included, in addition to the still cameras, a newly purchased FLIP video camera. It has limited memory, so each day I not only downloaded the videos but also erased them in the camera. This was a bit risky, and I am not too sure some videos were not lost. I don't remember taking any that I can't find, but it is possible. In my defense, most of my videos were not any good anyway. Word of advice: If you are going to travel with a new device, purchase it far enough in advance to learn how to use it. If I could do it over again, a small hand-held tripod would have been very useful for stabilizing the camera as well as keeping my clumsy fingers off of the very sensitive controls. Amazingly, the videos are of very high quality for such a small device, so even though mine are not particularly good, it should be possible to lift some still shots from them to use with the rest of the still pictures we took.

Upon returning home, I copied all of our pictures, even the bad ones, to flash drives and gave them to our son. Not only will that give us a backup if something happens to our computers, but he actually wants to look at them. That is the greatest compliment of all.

HOVER CRAFT

I recently received one of the slickest SPAM emails I have ever seen. The website was made to resemble a Microsoft offering, complete with pictures of products that looked like Microsoft Office programs. But when you hovered over the link, it did not go directly to Microsoft.

(Continued on page 3)

(Continued from page 2)

Hovering is NOT clicking. Remember this. When you hover the mouse pointer over the link, i.e. placing the mouse over the link on the screen but not pressing any buttons, it should produce the actual link at the bottom of the screen. Using our club webpage as an example, pretend the fancy arrow is your mouse pointer and that it is hovering over the option to view details for Randy’s study group. (The real mouse arrow does not show in a “printscreen” image.) At the bottom of the page, under the curved arrow, is the actual web URL which will transfer you to the page containing the information for the group. It is in very small print and hard to read, but it is there. It says: “Go to http://www.ccokc.org/documents/Win7_Resources.pdf (http://bit.ly/h2TmCh)”, and the quotes are included in the URL.

In the case of the suspicious website, the URL address contained some words after the initial part of the link, including “Microsoft,” which would again lead you to believe it was a legitimate Microsoft offering. If this had been truly from MS, I think that company’s web address would have been in the first part of the link, in other words “microsoft.com”. Since the Golden Rule is to never click on links incorporated in unsolicited email, I decided the offering was SPAM and deleted the email from my web server, never to be seen again (hopefully).

the end of the story

The Other Side of the Street

By Bill Hart, Member, The PCUG of Connecticut
March 2011 issue, The Program
www.tpcug-ct.org
adrabinowitz (at) ieee.org

When IBM and Microsoft first released OS/2 in the late 1980s I was keen to try it, and even signed up as a Beta tester. I really wanted to be able to run more than one application at a time, and this seemed to offer a chance.

OS/2 could be described as a GUI-based system supporting any number of virtual machines. Open an application and you opened a virtual machine to run it. It accepted both DOS and Windows 3.0 applications. At last I could run more than one application at a time on one machine; I could run long-running simulation runs in one virtual machine while sending and receiving messages and writing documents in two others, Fantastic!

And then Microsoft, who had left the project, struck in their inimitable way. Windows 3.1 subtly changed the interfaces needed for applications to talk to Windows, so when OS/2 users tried to run the new Windows apps they failed – until IBM was able to catch up. Redmond is still doing this; they have not accepted internationally-agreed document formats, but have invented their own, ignoring the rest of the world. Windows Office apps like Excel or Word will still not accept those formats, and Windows does not recognize any other disk format than those developed by TBOR (The Beast Of Redmond).

So I just LOVE Micros**t (supply your own two letters). When OS/2 faded I looked around for a substitute that was not from Redmond – and chose Linux.

Linux is also fantastic, though, being derived from UNIX (so to speak), it has a somewhat different philosophy from OS/2 or DOS. But I can run many applications at once, as I did with OS/2. AND it has a feature that the miser in me loves – it is free. You can download applications without charge; you can, if you are Guru enough, download the source code for applications and modify them to fit your own needs.

Another nice thing: Linux applications used on the Internet are safer than Windows ones. Steve Gibson of Gibson Research Corporation, makers of SpinRite http://www.grc.com -- take a look) many years ago fell afoul of a hacker who didn't like something he had said and retaliated by putting a "Denial of Service" attack on his site. (That's when you visit a site with an invalid request which takes time to analyze, but you do it so often so quickly that the site is overwhelmed.) During his (successful) exploration to find the perpetrator he discovered that Windows leaves all the ports on the computer CPU open by default -- which is why you need something like ZoneAlarm or some other firewall-type product to keep you safe. When he told Redmond about it they just shrugged their shoulders and said they knew, but it didn't matter.

Linux only opens to the outside world those ports on the CPU which are absolutely essential. So I rarely use Windows to surf the Web any more. I said “so far” because I suppose hackers would be more likely to work at attacking Linux if more people were using it. It’s much easier to go after Windows users, who are the vast majority.

There are many varieties of Linux. I usually run OpenSuSE on my desktop. A lot of people like Ubuntu. I have tried it more than once, but it has yet to recognize the Wi-Fi equipment built into my laptop. I finally settled on a variety called PCLinuxOS. (http://www.pclinuxos.com/). Go to download it, and you are immediately faced with another decision: there are many varieties of desktop available.

Like, say, Windows 95, Linux runs a GUI on top of a basic DOS-type machine. And this means that a number of people, having different ideas of what constitutes a really nice GUI, have made, and offer, their own designs. The two most used are probably KDE and Gnome, but there are, as you can see on the PCLinux site, several others, and you can read a description of each before you choose. But if you want to start somewhere familiar, probably the best to start with is the KDE desktop. It is most like Windows in its appearance and behavior. Its descriptive page on the website says of it:

Features:
Kernel 2.6.33.7bfs kernel for maximum desktop performance
Full KDE 4.5.4 Desktop
Nvidia and ATI fglrx driver support
Multimedia playback support for many popular formats
Wireless support for many network devices
Printer support for many local and networked printer devices
Addlocale allows you to convert PCLinuxOS into over 60 languages
GetOpenOffice can install Open Office supporting over 100 languages
MyLiveCD allows you to take a snapshot of your installation and burn it to a LiveCD/DVD
PCLinuxOS-liveusb – allows you to install PCLinuxOS on a USB key disk

----

Sounds a pretty good deal, despite some of the Version Number flack. "Kernel" is the basic Linux system on which this version of PCLinuxOS is founded, "KDE", of course, are supplying the GUI portion and GetOpenOffice will add the free Office Suite to your system. Well worth the price! Anyway, you can experiment if you wish. Download more than one. But make sure they are described as 'LIVE CD'. Those will run entirely from the CD without disturbing your hard disks at all.

(Continued on page 5)

Your Computer's Health, Part 1

By Art Gresham, Editor,
UCHUG (Under the Computer Hood User Group), CA
January 2001 issue, UCHUG Drive Light
www.uchug.org
1editor101 (at) uchug.org

At the start of this new year the UCHUG Drive Light is going to present a series of articles on the general topic of Your Computer's Health.

You say you are doing most of those things recommended to keep your body healthy: annual physical, dental checkups, good diet, bathe regularly, stay physically active. And you do what you must do to keep your auto healthy like oil changes, tune ups, check the tire inflation and tread depth, wash it occasionally, and use good quality gasoline. Even in your home you take out the trash, wash the dishes, vacuum the carpet, change the heater air filter, flush the toilet.

But are you as regular about the same kinds of things with your computer? Like other areas your life, your computer has several facets that you should care for with some regularity, from weekly, or monthly. Some areas are software, or data based, to help keep the computer running at full speed. Others like simply opening the case and removing the dust accumulated on the cooling fins and fans that will help it stay cool and functional for more years.

Maybe you already have a plan, and actually do make data backups (we all do have Acronis don't we?) but what are you doing to be sure your computer stays alive so that you never have to actually use one of those backups? Have you actually complained recently about how much slower your computer seems to run than it used to do?

We want to present some ideas to help you form a plan, or get started. We each have a wide variety of things that we do, some are very common and widely known. Others may be very unique, much deeper, or something you simply never thought of doing. What you choose to do will, of course, depend on how you use your computer. But the important thing is that you know that your computer's health is your responsibility and if you “take out the trash” occasionally then something is likely to become, well.... trashed!

Let's start with the basics. Here in Part 1 we want to look at basic hard drive-OS-data cleaning. For this article I am using XP, so your newer Vista/Win7 will have some slight differences. Windows includes a number of good basic tools that you can, and should be aware of and using. For starters, how full is your hard drive (or hard drives) and how much space can you free up so you can download more of the great utilities (more ideas about those soon) and photos from all the holiday parties and family gatherings. I always like to start by noting the free space, and after all finished I can see a measurable improvement there. Other areas will be a lot harder to note accurately (did the system start/shut down faster this time? Did that program seem to load faster?). So to start Open My Computer, Right Click your hard drive (usually labeled "Local Disk (C:)"), and click Properties. Note how much space is used and free, then close the dialogue box. Repeat for each hard drive. Note that you can probably run the Defragmentation program from the Tool tab on this dialog window, but resist the urge for now, we have miles to drive before we are ready to do that step.

Before defragmenting you should delete as much of the unneeded, unwanted, unused files and programs as you are comfortable removing. While I am primarily thinking of temporary internet files, useless log files, and other truly worthless stuff, you may also have duplicate copies of data (photos, important files) that have been leftover from other activities. While there are a number of tools for finding and deleting those 'clones' we will leave that to a much later discussion. But you say your drive is so large you don't even know where to begin?

Well, start with the 'biggies' first. Why waste 20 minutes hunting and deleting 50 tiny files that save you two megabytes of disk space when there may be two or three directories you can delete in 30 seconds and save 5 gigabytes of space. But how do you find them? Use a tool!!

My first tool choice is OverDisk (Freeware) http://users.forthnet.gr/pat/efotinis/programs/overdisk.html which was featured in the January 2007 Drive Light. Open a disk letter and see the folders and files as a series of concentric rings, as if you were looking down onto the disk itself and seeing the files laid out below. The neat thing is that the biggest folders and files are graphically displayed and you can quickly zero in on the folders that are the biggest. It may be your email folders that have grown out of control and need to be archived. Perhaps you will see a folder for a program you have long since forgotten about and no longer use. By starting here you will have an idea where the big fish are hiding. Check each drive letter or partition and see what sticks out.

Now that you know a little more, generally, about what and how much is on your drive let’s get down to getting rid of those pesky junk, temp, trash and other files. The problem is that they are tucked away in folders nested 6 levels deep, or under names that appear self-important, or downright mysterious. Don't be tempted to just dive in with Explorer and manually delete them helter-skelter. Use a Tool!! Actually for this I use several different tools because each seems to catch a few files that the others miss. You may want to try these and then just use the one that gives you the best results. I recommend, and use these the end of every month (usually after I finish the Drive Light as that is one of my major monthly milestones - sorta like smoke detector batteries and DST!

First, and one of the fastest is CCleaner (Freeware) from **http://www.piriform.com/** which was mentioned in the August 2009 Drive Light. In addition to quickly finding all those useless files, it contains a very good registry cleaner.

My next tool is very similar, called CM Disk Cleaner. Although it does not appear to be being updated it is available on several download sites including

HYPERLINK "http://www.scanwith.com/download/CM_DiskCleaner.htm" http://www.scanwith.com/download/CM_DiskCleaner.htm

Next is the very advanced Advanced System Care (Freeware) from IOBit. This is probably one of the most complete, and easy-to-use tools. A very good review and download is available from download.cnet.com

Now that you have a nearly automated way to find all those files, deleted many, cleaned up the registry, and feel you have made some good progress, go back and look at those drive properties and see if you have saved any space. You probably have, especially on your C: drive and perhaps your primary data drive. NOW is when you can run your defragger. Either use the one supplied with Windows, or use a free tool also from IOBIT called Smart Defrag. But you say defragmenting takes so long and your time is so valuable.

Well, I have mine setup to automatically begin defragging each time my computer is inactive for five minutes, and Deep Optimize every weekday at 7PM (which is when I am usually eating supper, or watch-

(Continued on page 5)

(Continued from page 4)

ing TV). Now I can relax knowing I have cleaned up and defragged with very little effort.

the end of the story

Your Computer's Health
The “Oh Oh” Moment, Part 2

By Art Gresham, Editor,
Under the Computer Hood User Group, CA
February 2011 issue, UCHUG Drive Light
www.uchug.org
1editor101 (at) uchug.org

Oops. Darn, What The....? You know the feeling. Yesterday everything was fine. Today you are wondering what happened overnight. What can you do if your computer seems to have suddenly gotten sick? Perhaps it was caused by that neat new application, or game, you installed yesterday, or maybe something got installed when you visited that website that promised to speed your computer's internet access, but when you the page opened it ran a moment and then seemed to hang up with no sense that it really did what was expected. Maybe you should not have installed that app/game/utility because it was some kind of rogue or worthless program, or worse, and you are now stuck with a sick system.

Don't you wish you could go back in time to last weekend when everything seemed to be running fine? Well, you can. Probably.

If you are running a Microsoft Windows ME, XP, Vista or 7 then the System Restore is available to offer you protection for many of these kinds of illness, and might be worth checking to see if you can regain your computer’s health.

System Restore allows you to roll back most system files, registry keys, and installed programs, the DLL Cache folder, local user profiles, and more. When installed, and not disabled (more about that later) you may manually create a restore point, or use one of the automatically created points. And it does this without affecting your personal files, or data such as e-mail, documents, or photos. We will discuss full backups that include your data in a future article.

Also note that in Vista and later versions it has been improved and now uses “Shadow Copy” Technology with even more backup capabilities.

So where do you look to see if you have any restore points? You should do this today to be sure it is not disabled. Open System Restore by clicking the Start button, clicking All Programs, clicking Accessories, clicking System Tools, and then clicking System Restore. Be sure to select “Restore my computer to an earlier time,” then click Next.

You will see a calendar of the current month, and several of the dates should be marked in Bold. These dates have restore points available, and some may have more than one as shown below. You may have multiple restore points for several reasons.

Wikipedia lists the Restore points that are created:

- When software is installed using the Windows Installer, Package Installer or other installers which are aware of System Restore. [note]
- When Windows Update installs new updates to Windows.
- When the user installs a driver that is not digitally signed by Windows Hardware Quality Labs.
- Every 24 hours of computer use (10 hours in Windows Me), or every 24 hours of calendar time, whichever happens first.

This setting is configurable through the registry or using the deployment tools. Such a restore point is known as a system checkpoint. System Restore requires Task Scheduler to create system checkpoints. Moreover, system checkpoints are only created if the system is idle for a certain amount of time.

- When the operating system starts after being off for more than 24 hours.
- When the user requests it. On Windows Vista, shadow copies created during File Backup and Complete PC Backup can also be used as restore points.

Older restore points are deleted as per the configured space constraint on a First In, First Out basis. [Wikipedia] To begin a restore simply click on the date you want, and then click Next a couple times. Your system will restart and hopefully you have healed the patient.

If you do not see any restore points, you might want to check that the process is not disabled. To do this in XP you can right click My Computer, open the Properties, and click on the System Restore Tab. There you will see a checkbox where you can “Turn of System Restore on all drives. Be sure that is un-checked. For Win 7 see the FAQ How do I turn System Restore on or off?

References:
http://en.wikipedia.org/wiki/System_Restore

http://windows.microsoft.com/en-US/windows-vista/What-is-System-Restore

http://windows.microsoft.com/en-US/windows-vista/What-types-of-files-does-System-Restore-change

the end of the story

(Continued from page 3)

Each will come as an ISO file -- a CD image which you can burn with Nero or Roxio or whatever you have. You will end with a bootable CD. Insert it in your drive and reboot the computer. It will provide you with a menu of choices of which the top one is usually the one to pick and the bottom is probably 'boot from the hard disk", which will allow you to chicken out if you wish.

And now you are running Linux, without having disturbed anything on your present computer. Reboot and remove the CD, or choose the "Hard Disk" option, and you are back to Redmond's product. But I hope that you will have found, if you explore a bit before doing that, that you have a wide range of applications -- an Office Suite, Multimedia players, editors, a few games, and Internet applications like Firefox. Try Firefox and you should find that your Web connection has been recognized and you are able to surf -- without bothering about special software to keep you safe from Hacker Harm.

the end of the story

Tor, Anonymity On-line

By Dick Maybach
Brookdale Computer Users Group
Lincroft, NJ February 2011
n2nd (at) charter.net

Tor protects your privacy when you are on-line in two ways:

(1) it prevents other users of the network you use to reach the Internet (for example a public Wi-Fi hotspot) from seeing the data you exchange and with whom you communicate and
(2) it hides your identity from those with whom you communicate. For most of us, item (1) is more important.

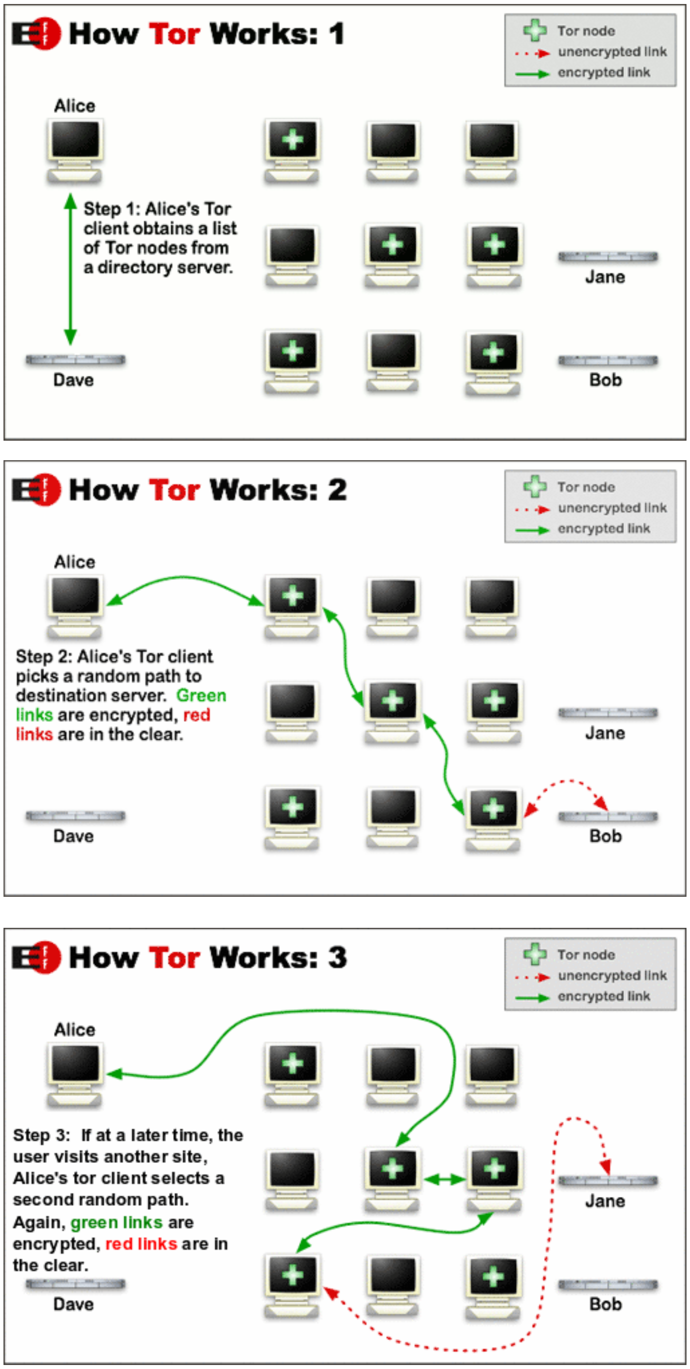
For example, when we use a Wi-Fi hotspot to access the Internet, every byte we send and every one we receive is accessible to all its other users. One defense would be to add a separate defensive tool for every offensive one, which is the approach taken to foil Windows viruses. The result will surely be the same – an ever-increasing kit of defensive programs to counter the never-ending supply of offensive programs. A much sounder approach is to run Tor, which defends against all such attacks; as a result you need install only one tool. Item (2) is probably less important to you; it prevents sites you visit from knowing who you are or what other sites you've visited. We are seeing ever more intrusions into our privacy by governments and businesses, and Tor was developed to help us preserve our privacy, safety, and dignity in the face of this. Although Tor is legal in all countries, you can do illegal things using it. In this way, it's similar to the gas pedal on your car, which is essential if you want to go someplace, but must be used with restraint to avoid awkward and expensive discussions with the law.

Tor hides not only what you say, but also who you say it to. You could use it to communicate back home from a location where disclosing your country of origin or religion might expose you to unpleasantness or risk. This feature also allows you to circumvent restrictions that your ISP has placed on the Web sites you visit. It's used by individuals, businesses, activists, reporters, the military, and law enforcement for investigations and to protect themselves, their organizations, and those with whom they communicate. Using it, you can surf the Web, exchange e-mail, use instant messaging, and transfer files. However, please don't just install it and assume you're safe. You need to change some of your habits, and reconfigure your software. Tor by itself is NOT all you need to maintain your anonymity.

Tor consists of two parts – a public, secure virtual private network (VPN) and the software to access it. The software is free and available for Windows, Mac OS X, Linux, and some smart phones at:

"http://www.torproject.org/"

Most PC and Mac users will want the ***<u>Tor Browser Bundle</u>***, which includes the Firefox browser. (For reasons you can read on the Tor Web site, neither Internet Explorer nor Safari is suitable for secure browsing.) The Tor VPN is distributed and accessible worldwide, is free, and is provided and maintained by volunteers. Because the network consists of thousands of independent Web sites, it's quite robust; there is no single point of failure.


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob
How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob
How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Images downloaded from the Tor Project website

These diagrams explain how Tor software, when configured correctly, creates a secure connection over the internet.

How does Tor work? When you access the Internet with it, you first communicate with a Tor Directory Server over an encrypted link (one with a URL beginning https;//). Here, you obtain a list of available Tor Nodes. The Tor software on your computer selects at least three of these; call them Node 1, Node 2, and Node 3. It then sets up a secure link to Node 1, which forwards your traffic to Node 2, which forwards it to Node 3. All these links are secure, and only Node 3 can decrypt your packets. Finally Node 3 sends your packets to your desired end site. Note that if the end site is secure (indicated by a URL beginning with https://), even Node 3 can't read your data. Packets coming to you follow the reverse path, Node 3 encrypts them in such a way that only you can do the decryption. As far as the end site knows, it is communicating with Node 3; it has no way of finding your computer's URL. An observer on your local network knows only the URL of the Tor Directory Server and Node 1; he can't find the location of the end site or read any of your packets. Only Node 1 knows your location, and only Node 3 knows that of the end site. Note that Node 3 can also see

(Continued on page 7)

(Continued from page 6)

the data you exchange, unless you're using end-to-end encryption, i.e., talking to a site with a URL beginning https://.

When you install Tor, you will also install the Torbutton add-on for Firefox, which allows you to turn Tor anonymous browsing on and off. Turning Tor on changes some of Firefox's operation.

None of the cookies you acquired during normal browsing will be available. This is because cookies can tell the site you are communicating with a lot about you and which sites you've visited. As a result, you will have to reenter passwords where they are required. These cookies will return when you toggle Tor off.

Some sites will be displayed in a foreign language. Since they don't know where you are, they assume you are located in the same country as Node 3. See the Tor site for work-arounds.

You will see moderate delays while surfing the Web. There are at least three intermediate sites on the path to your final destination, and several layers of encryption are involved. While the delays are noticeable, I haven't found them to be obnoxious, and I consider it a good trade-off to achieve better security.

Many users need only browser access to the Internet when away from home, since through it they can also exchange e-mail and transfer files. (I've found that the FireFTP add-on is convenient for the latter, but see the Tor site for instructions on how to configure it and follow these exactly.) If you want to use secure instant messaging, use Pidgin, which Windows and OS X users can obtain by installing the Tor IM Bundle, available on the Web site. (Pidgin is in most Linux repositories.) You can't use Tor for file sharing, i.e., using BitTorrent; instead use the I2P network, **"http://www.i2p2.de/"**. See the Tor site for how to configure other Internet access programs, including some that provide access to your home computer. However, if you really need access to files on your home computer, it would be better to transfer them to your laptop or to a cloud service before you go. Otherwise, a power transient or other failure could disable your computer until you return home to restore it.

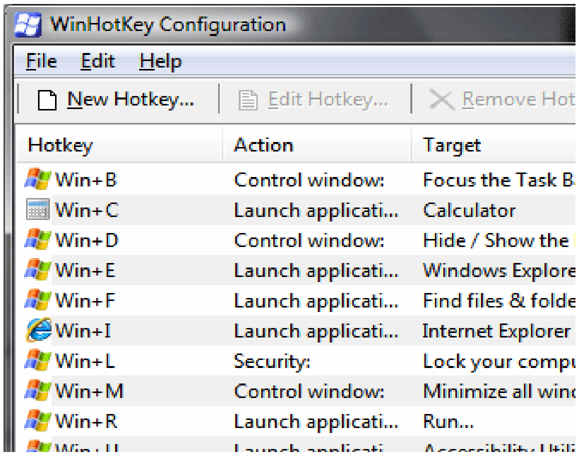
Accessing the Internet away from home without Tor is like driving without insurance, you can almost always get away with it. That doesn't mean it's a smart thing to do.

the end of the story

(Continued from page 2)

powerful tool. When running, the program sits in the system tray. Double-clicking on the system tray icon will bring up the main window." I will give it a try. We will see…. Just a small download of 826 KB. You can get it here:

http://directedge.us/content/winhotkey



Hotkey	Action	Target
Win+B	Control window:	Focus the Task B
Win+C	Launch applicati...	Calculator
Win+D	Control window:	Hide / Show the
Win+E	Launch applicati...	Windows Explore
Win+F	Launch applicati...	Find files & folde
Win+I	Launch applicati...	Internet Explorer
Win+L	Security:	Lock your compu
Win+M	Control window:	Minimize all winc
Win+R	Launch applicati...	Run...
Win+U	Launch applicati...	Accessibility Utili

the end of the story

Malware, Viruses, Trojans Defined

By Ira Wilsker
Columnist, The Examiner, Beaumont TX;
Program Director of Management Development
at the Lamar Institute of Technology, Beaumont TX;
and a radio and TV show host.
iwilsker@apcug.net

In the past week, I was called upon four more times to clean malware off of infected computers. One user had a major name brand antivirus program installed, running, and updated and could not understand how the malware had penetrated his antivirus software and contaminated his computer. He had purchased the antivirus software last fall from a big box electronics store based on the recommendations of a salesperson. He had been told that this particular brand of security software was the best as it was their top seller, and that antivirus software was all that he really needed. Based on that recommendation he plopped his hard earned money on the counter, went home, installed it, updated it, and blissfully surfed the internet, opened email attachments, downloaded software and music, and had just a jolly good time online until his computer gradually slowed to a crawl, and friends informed him that they were receiving spam emails from him. This user was perplexed, as his antivirus software was running, and indicated that it was updating several times a day. He just could not understand how 90 different malware programs had infected his computer. His problem started when he purchased inadequate security software; while the product he bought was excellent at protecting his computer from viruses, and some Trojans and spyware, it did not offer the all-inclusive protection of the comprehensive security suite offered by that publisher (and others as well) that would have only cost him a few dollars more.

There is a common misconception in user circles that viruses are the primary computing threat, as users have had heard about viruses for several years. Today, viruses are present, but a relatively minor threat in terms of prevalence. I did a quick analysis of the most common new threats recently listed by TrendMicro, and found that viruses only made up 4% of the new significant threats to our computing security. On the other end of the spectrum, Trojans made up 42% of the commonly seen new threats, worms were at 14%, backdoors at 14%, web based threats were at 6%, java script malware was at 6%, 4% were hacking utilities, 2% adware, and about 8% other threats. It is obvious that protective software that protects the computer primarily from viruses is failing to protect the user from the majority of contemporary threats; it is precisely this fact that led to this user's infected computer, despite his premium quality antivirus software. A lot of users have a misconception about the common threats in circulation, believing that they are generically all viruses, but, as I saw in this case, this blissful ignorance may lead to a computing nightmare.

While not necessary to use a computer, it would likely be beneficial for computer users to be aware of the different threat groups that can impact our computing. According to Wikipedia, "A computer virus is a computer program that can copy itself and infect a computer." Many viruses attach themselves to legitimate programs or data files on the infected computer. The fact that a computer virus can copy itself to infect other computers is what makes it different from other types of malware, for which viruses are commonly confused. Viruses can be spread through digital media (USB drives, CD or DVD discs, and floppy discs) or through network connections that the virus can use to copy itself to other attached computers. Once a virus has infected a computer it may perform a variety of tasks as

(Continued on page 8)

(Continued from page 7)

programmed by its author. Viruses may damage the data on a hard drive or degrade the performance of the computer. Some of the viruses are stealthy and their effect may not be noticeable by the user, as the viruses do their damage in the background. Some viruses are functionally benign, other than they reproduce themselves countless times on the infected hard drive, until they consume all of the free space on the hard drive.

Computer worms are a malicious computer program that wriggles through computer networks sending copies of itself to other computers attached to the network. Most worms are free standing programs, and are commonly programmed to spread themselves through the network without any action by the user. Most worms have an explicit nefarious function such as deleting files on the infected computer, or encrypting critical files, only releasing them after an extortion payment is made to the cyber criminal. Some worms open a backdoor into the computer that will enable the creator of the worm to take remote control of the computer, converting the computer into a "zombie" under his control, which can be used to generate revenue for the originator of the worm by sending spam mail from the infected computer, with the spam fees collected going to the author of the worm. Some worms are used to create a zombie network of computers, also called a "botnet", where the compromised computers can be used to launch directed cyber attacks on other computers or networks, in an act of cyber terrorism.

For those who are aware of the epic "Helen of Troy" of Greek mythology, the term "Trojan Horse" means an object looks like it serves one purpose, but really has an unobvious, usually nefarious, purpose. Cisco, the networking company, describes a Trojan as, "It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems". In cyber speak, a Trojan Horse, typically shortened to the simple moniker "Trojan" is a program that appears to have a useful function, but after being installed by the user, the Trojan may be used to perform other undesirable functions. Some Trojans are money makers for their authors because they place paid (and usually unwanted) pop up advertisements (Adware) on the infected computer, redirect web searches, or shift online purchases to a seller not of the buyer's choice without his knowledge. Some Trojans are keyloggers, which are commonly used for identity theft, or to give unauthorized users access to a computer system. Trojans are often spread through intentionally downloaded software, surreptitiously bundled with another often legitimate program, from email attachments, and purloined websites with executable contact (ActiveX is sometimes used for this). Some Trojans can be installed on the target computer by way of code written in Java, or a Java script, that when executed, implants the harmful content on the victim computer.

One of the more recent and costly types of malware to attack our computers is generically referred to as "Rogue Antivirus Software", which is usually implanted on the victim's computer by a Trojan. There are thousands of these rogue programs in current circulation, infecting millions of computers at any given time. Rogue antivirus is sometimes installed by the user using "social engineering" tactics, which tricks the user into clicking on something that installs the rogue software. Some of the common lures to ensnare the user into loading rogue software on the computer are offers for free screen savers, toolbars, utilities to play specific video formats (often attached to an email), sham online security scanners, contaminated PDF files, insecure web browsers, and other vectors. The common thread of this rogue software is an authentic looking popup that informs the user that his computer is (falsely) infected with hundreds of viruses and Trojans, and for a fee it will clean the computer. These popups which will not permanently close will typically hijack the computer, destroy the installed legitimate security software, prevent access to online services that can kill it, prevent cleaning utilities from executing, and otherwise take control of the computer until the user pays a fee, typically $30 to $70. This fee is to be paid by credit card or other online payment service to a website that looks legitimate, but is really a complete scam. Not just will the rogue software not clean the computer of the pseudo infections after the fee is paid, but now a cyber criminal, often in Russia, has the user's credit card information. it is not uncommon for that same credit card information to promptly be sold on illicit websites, and to have substantial unauthorized charges appear on the compromised credit card account.

While there are many other cyber threats out there, those listed above are among the most commonly encountered by users. The traditional antivirus software will protect from some of the threats listed, but not all of them; this enhanced security capability is in the purview of the comprehensive security suite, or a combination of different types of individual security utilities, and not the free standing antivirus program. this is explicitly why I currently recommend a high quality integrated security suite, rather than an antivirus program. There are several good commercial security suites available, as well as a few free security suites. Just be aware that antivirus software by itself is inadequate to protect against today's contemporary cyber security threats.

the end of the story

From the President ...
... Editor's desk

Hi PACCsters!

Required reading list:
THIS AND THAT …... by Elizabeth B. Wright
The Other Side of the Street …… by Bill Hart
Your Computer's Health, Part 1
The "Oh Oh" Moment, Part 2 …. by Art Gresham
Tor, Anonymity On-line …..… by Dick Maybach
Malware, Viruses, Trojans Defined …. by Ira Wilsker

ATTENTION PACCSTERS:
For some time we have been trying to reach members to confirm their e-mail address, for the PACC TALK notification, which goes out to let you know the newsletter is at the PACC web site ready to download. Some members did not yet confirm getting the notice. Please do so! Thank you,
PJK

Also, the results of the March 2011 election retained all the same PACC BOD officers. We thank you again! PJK

IMPORTANT NOTICE

Finally!!! The PITTSBURGH AREA COMPUTER CLUB web site is accessible and working.
It needs updating in many areas, but it is functional.
You are again able to get your copy of PACC TALK there. If you have a problem with viewing it with adobe reader, use another PDF reader, such as Nitro. It is much smaller and faster to open, to view the PACC TALK.

The web address of PACC Web Site:
http://pacc.apcug.org/

MEMBERSHIP APPLICATION FOR PACC: (Please print in CAPS)

NAME..DATE...............................

ADDRESS..COMPANY............................

CITY...STATE............ZIP+4..........................

PHONE.................................E-MAIL..

OCCUPATION..

INTERESTS...

RECOMMENDED BY PACC MEMBER..

Dues: $25 per year.
Make your check out to: PACC and send it with your application to:

Treasurer, PACC, P.O. Box 6435, Pittsburgh, PA 15212-6435

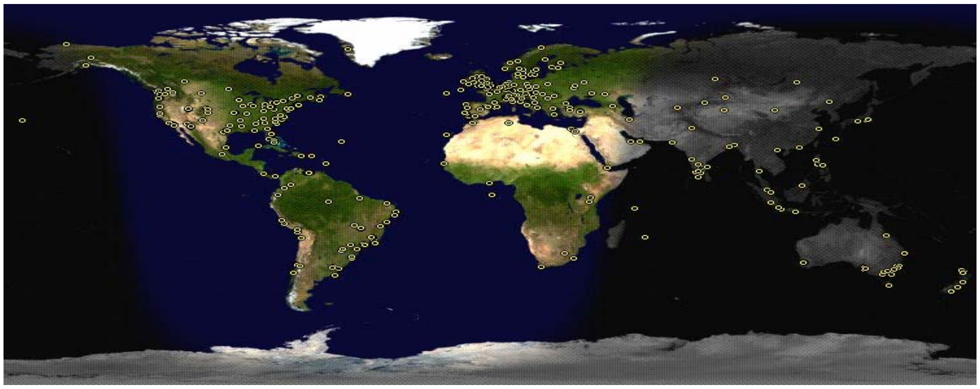
cut here...cut here

PACC HELP LINE

Help is available to PACC members on various computer topics by contacting one of those listed below. It is recommended that the initial contact with any of these experts should be made via the PACC WEB SITE. In this way others can benefit from the questions and responses. Be courteous and call only during the listed times.

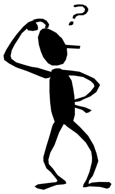
NAME	COMPUTER AREA	PHONE	TIME
Agrawala, Vishnu	Hardware	724-553-8051	3 - 6:00 pm
Cutrara, Phil	Geoworks	766-0274	
Fisher, Bill	Cobol, Word Perfect	367-8996	7 - 9:00 pm
Konecny, P.	Windows, DOS 6.2x, MS IE,, Hardware	795-6075	8 - 9:00 pm

If you would like to become PACC HELP LINE volunteer inform the editor by sending e-mail to: pacccomm@aol.com



FOR SALE

Your ads PACCsters?



Classified ads. Buy, Sell, Trade. Members may place free ads (up to 5 lines).
For commercial ads send a inquiry to:
PACCCOMM@Aol.com

ATTENTION:
IF YOU HAVE NOTICED THAT THE EXPIRATION DATE ON YOUR LABEL DOES NOT REFLECT CORRECTLY YOUR MEMBERSHIP STATUS OR HAVE AN ADDITIONAL INFORMATION YOU WANT TO SHARE SEND E-MAIL DIRECTLY TO: pacccomm@aol.com

Reprint Policy.

Permission to reprint articles from PACC TALK is given to school, personal computer club, and nonprofit organization publications, provided that: (a) PACC Inc. receives a copy of the publication; (b) credit is given to PACC TALK as the source; (c) the original author is given full credit; and (d) the article author has not expressly copyrighted the article. Recognition is one means of compensating our valued contributors. Arrangements can be made to receive copy on magnetic media; for details, contact the editor.

PITTSBURGH AREA COMPUTER CLUB
P.O. BOX 6435
PITTSBURGH PA 15212-6435

E-mail: pacccomm@aol.com

NEXT PACC MEETING IS ON APRIL 17, 2011

PACC 1975 - 2011
IN ITS THIRTY-SIXTH YEAR

PACC TALK

OFFICIAL NEWSLETTER OF THE PITTSBURGH AREA COMPUTER CLUB
P.O. BOX 6435, PITTSBURGH PA 15212-6435
NOT RESPONSIBLE FOR TYPOGRAPHICAL ERRORS OR WRITERS ACCURACY

NEXT MEETING: April 17, 2011

The Pittsburgh Area Computer Club (PACC) holds its meetings the THIRD Sunday of each month. The next meeting will be in room 311 at Point Park University, Wood St. and Blvd. of the Allies. The doors open at 11:00 am and close at 4:30 pm. Bring your PC!
NOTICE THE EXPIRATION DATE ON THE MAILING LABEL OF YOUR NEWSLETTER. You won't get your newsletter if you let your membership expire. Renew your Memberships !!! Send a check or money order for $25 made out to 'PACC' and addressed to Treasurer, PACC, P.O. Box 6435, Pittsburgh, PA 15212-6435.
Classified ads. Buy, Sell, Trade. Members may place free ads (up to 5 lines). Articles should be prepared in plain ASCII text. WITHOUT formatting. Deadline for articles is the 25th of the month. Send them to P.J. Konecny, P.O. Box 557, Monroeville, PA 15146.
PACC homepage can be found at: **http://pacc.apcug.org**

PACC OFFICERS AND VIPs

Pres. – P J. Konecny	795-6075	Editor - Pavel J. Konecny	795-6075
Exec VP – J. Duda	367-0392	VP Edu. Bud Kittle	821-5807
Treas. - Vishnu Agrawala	724-553-8051	MAL - Anil Rodrigues	521-4096
VP Comm. Homer James	341-0252	MAL - Bill Fisher	367-8996
VP Prog. - Lori Cislon	367-0392	MAL - Rich Springer	655-2883

PACC SIG LEADERS

Hardware-Vishnu Agrawala	724-612-1443	Windows - P. J. Konecny	795-6075
MS Publisher - P. J. Konecny	795-075	Internet - Bill Didycz	884-6225