

Midland
CComputer
Club

BITS AND BYTES

The Newsletter of the Midland Computer Club

May 2007

GENERAL CLUB MEETING 7:00 P.M.

Meets 4th Wednesday of the month at the Midland Community Center
2001 George St., Midland, MI
<http://mcc.apcug.org/>

This month's date: May 23rd

THIS MONTH'S TOPIC: Howard Lewis demonstrating the new Microsoft Windows Vista Operating System

PROGRAM COORDINATORS

Contact :

Frank Koenig frankkoenig@charter.net
Co-Chairman-Larry Piper larryP56@chartermi.net

What You Missed

At the **April** club meeting, Larry Piper have a very informative presentation on the various distros (distributions) of Linux, with the primary thrust on Ubuntu. Ubuntu is frequently considered to be the most "user-friendly" distro and (as with most of the other Linux distros) is freely downloadable from the Internet. If your PC can be booted from the CD drive, you can give Ubuntu a try without disturbing your Windows setup. This will allow you to determine first hand whether you are interested in joining the flock migrating to Linux.

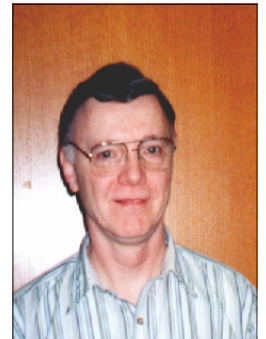
Upcoming Activities

The **May** meeting will have Howard Lewis demonstrating the new Microsoft Windows Vista. The presentation will include the new interface and some of the advantages and disadvantages of moving from Windows XP to Windows Vista.

In **June**, Bill Tower will demonstrate how to set your system to utilize two monitors. When working with

The President's Corner

How much do you spend on tech gadgets on a yearly basis? A recent report in Information Week (informationweek.com/1137/gadgets.htm) said "U.S. households are spending an average of \$1,200 a year on electronic gadgets". I don't know about you, but I'm definitely not keeping up my end of that bargain! I did build my own computer this year and have exceeded that number for this year. But in the last several years I have hardly spent any thing on "electronic gadgets." Now their definition of "electronic gadgets" is quite broad. It includes cell phones, PDAs, computers, MP3 players, DVD players, TVs, digital cameras, etc. Most of those gadget are not included in my household. I currently have 3 computers (one is 3 months old, one is 5 years old and the third is 9 years old — although my wife is after me to get rid of one of them), a 3 year old digital camera, and a 15 year old TV (but only one). But with flat-panel TVs running \$3,000 to \$5,000 each (and selling like crazy), it's easy to see what has caused this large average. So the question that I pose to you is: Are you keeping up your end of the bargain? Let's get out there and buy those "electronic gadgets!"



After all, we have to keep that average up!

Feed me your comments. They are always welcome.

— Howard Lewis

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

multiple applications, there can be many instances where it is convenient to have two (or more) applications visible at a time.

There will be **no meeting in July** and August will feature our annual club picnic.

MCC OFFICERS

POSITION

President Howard Lewis
 Vice Pres. Bill Tower
 Treasurer Bob Miller
 Membership Gary Ensing
 Editor Jan Ensing

EMAIL:

lewis3ha@chartermi.net
 stressed@tir.com
 barloshelties@sbcglobal.net
 gensing@juno.com
 btiger6@juno.com

<http://mcc.apcug.org/>

Special Interest Groups:

CLUB PROGRAM COORDINATORS

Co-Chairman Frank Koenig frankkoenig@charter.net
 Co-Chairman Larry Piper larryP56@chartermi.net

BOARD MEMBER

Mary Branson molly688@chartermi.net
 Robert Hughes MIDItunez@yahoo.com

INTERNET SIG

Terry Brown t_bbrown@yahoo.com

PUBLICITY

Kathy Bohl kbohl30265@aol.com

Strange, useful, and useless (in no particular order) Web Sites:

<http://tinyurl.com/335f8q> – Terry Brown has shared his pictures on Snapfish from their trip to Mexico this past January. Travel along with Terry as he traverses Mexico from coast to coast via train on his RV. There are some great pictures there.

Free registration to Snapfish is required to be able to see these pictures.

[Http://www.1-click.jp/](http://www.1-click.jp/) – Have you ever wondered how that little cursor moves across the screen when using the mouse on your computer? The Japanese have delved into this issue and, through the power of magnification, can show you exactly what's going on every time you move your mouse. Even though this is a Japanese site, you can still see what is going on by moving your pointer around on the magnifying glass (the gray circle located in the middle of the screen).

<http://www.geekologie.com/> – The Geekologie website says that they are “dedicated to the scientific study of gadgets, gizmos, and awesome.” Whether you are into geek or not, this site has some pretty amazing videos and pictures. They range from a dog playing tennis on a Wii to the detonation of 100 tons of munitions (looks like it might be Iraq). You can also see a man holding ten eggs in one hand!

<http://www.evite.com/> – Planning a party for Memorial Day or graduation or some other festive event? Evite will help you with many ideas to incorporate into your planning. You can also send electronic invitations to make sure everyone gets included in your special event.



Board Meeting

The next board meeting will be 7 p.m., June 12, 2007, at Chapel Lane Presbyterian Church, 5501 Jefferson Ave., Midland.

Membership Enrollment form

NAME _____ PHONE _____
 ADDRESS _____ CITY _____
 ZIP _____ EMAIL ADDRESS _____

Membership dues FAMILY (\$20) STUDENT (\$15) NEW Member ____ renewal ____

Please fill out the above form and mail it along with payment of check or money order to :

MIDLAND COMPUTER CLUB Attn: membership chairman
 P.O. box 132
 Midland, MI 48640-0132

you may also pay for membership at a regular club meeting

Recovering Files from a Hard Drive

By Vinny La Bash, a Member of the Sarasota PCUG, Florida
www.spacug.org
labash(at)spcug.org

Obtained from APCUG with the author's permission for publication by APCUG member groups.

Have you deleted a file that you need and you don't know how to get it back? The first step is to make absolutely sure that it has been deleted. Open your Windows Recycle Bin and double-check. Is it in there? If so, simply right-click on the file and choose Restore.

If you have emptied the Recycle Bin the next step is to restore the file from your latest backup. You do back up your data regularly, don't you?

Unfortunately, there is no native "Undelete" command in Windows XP. This is a mystery because Microsoft had a nifty undelete feature in Windows 3.1 which somehow disappeared in Windows 95 and subsequent versions of the operating system. This is abysmal for Windows users, but profitable for third party software developers.

It's important to understand that when a file is deleted it is not actually removed from your system. Windows deletes only the first letter of the file's name and replaces it with a marked for deletion character. This makes the file "invisible" to windows, and if Windows needs the space for something else, it has no qualms about overwriting your valuable data.

What this means is that if you accidentally delete a file, you have a limited amount of time to recover it before windows stores something else over the same space. It may not happen right away, but it will happen eventually.

Since there is no way within XP to recover a lost file, you have to turn to a third party solution. The good news is that there are several excellent programs that will do the job easily. The even better news is that these programs are free. Isn't that nice?

Use Google or your favorite search engine to find FreeUndelet, PC Inspector File Recovery, or Undelete Plus. All of them work well though you may find one easier to use than another. That's a matter of personal preference.

You need to be cautious about this. If you download the utility directly to your hard drive, you run the risk of storing the undelete program over the very data you are trying to recover. If you have a second hard drive, you can download to that or better yet, download directly to a thumb drive. That avoids all danger of losing important data, and it has the additional advantage of immediate portability.

The programs all work similarly. Direct any of the programs to a specific disk and you will get a list of all deleted recoverable files on the drive. You may also get a description alerting you that the file(s) may be wholly or partially recoverable. That's good to know.

Direct any recovered files to an external hard drive if you have one. Don't save anything to your hard drive until you have recovered everything you need. Use Windows Explorer to manage the recovered files. Group them into categories to sort or group the files so you can easily determine if they are program files, data files or something else. Some files may have data missing if Windows overwrote some of the sectors where it was stored.

(Continued from page 3)

If after all this you haven't been successful, your best alternative is to consider a data recovery service. These can be a devastating drain on your wallet, so don't use these services to recover saved game files.

Do some comparison shopping as rates can vary considerably. Good luck and watch those sticky fingers when they hover near the delete key.

+++++

Why You Need A Firewall

By Brian K. Lewis, Ph.D., Member of the Sarasota PCUG, Florida

www.spcug.org

bwsail at yahoo dot com

Obtained from APCUG with the author's permission for publication by APCUG member groups.

When you connect your computer to the Internet, you have opened a door which invites any other computer in the world to come in. Actually, you have more than 65,000 doors into your computer, any one of which may be open. That is, unless you have taken steps to keep these doors closed. That is the purpose of a firewall. The firewall filters the information packets that show up at your "door" or computer port as we usually refer to it, and can either prevent them from entering or pass them through.

When your computer connects to the Internet, it is assigned a numeric address or IP (internet protocol) address. These addresses are a 32 bit number. They usually written out in four groups with periods between each group as follows: 111.11.11.111. Traveling over the Internet are many programs that simply look for unprotected IP addresses. The IP address of any unprotected computer is sent back to the originator who can then upload a trojan or spyware package to that address. The originator can then take control of the computer or the application will record keystrokes and send all recorded information back to the program originator.

Although your computer has one IP address there are many different ports on your address. There are different ports for different purposes on your computer. Your connection to the Internet is usually through port 80. This is referred to as the HTTP (hypertext transfer protocol) port. It is used when you connect to a web page. The web page data is downloaded to your computer through this port. Another commonly used port is 25. This is used for the SMTP (standard mail transfer protocol) or e-mail transfer. Another port is used for incoming mail or POP3 transfer is port 110. These are all part of the port series from 0 to 1024 that are the most common ports. Many applications use ports in this region including PC Anywhere, Internet telephones, MSN messenger, Net Meeting, and all AOL operations. Ports 1024 to 49451 are referred to as registered ports. There are many Internet games that use ports in this region. There are also other specific functions assigned to these ports and some may duplicate functions in the common port region. The final group of ports are dynamic and have no specific functions registered. However, the point is that all of these ports can be accessed by remote computers somewhere out on the Internet and use them to connect to your computer if you have not protected them.

Automated port scanning software is available free on the Internet from many "hacker sites". Its use is very common on the Internet. There are various types of scans. Some scanners will look for any of the 65,535 possible ports. Another type looks for open UDP (user data protocol) ports or may use an FTP (file transfer protocol) bounce to hide the origin of the scan. If an open port is located, software can be downloaded that will open a "backdoor" on your computer. This allows remote input and output. Such access can be used to record and transmit out information from your computer. It can also be used to

(Continued on page 5)

(Continued from page 4)

attack other computers to produce a “zombie” network. Such networks have been used to attack large computer servers in attempts to bring them down or to produce a “denial of service” attack.

Many users believe that a router with a firewall is adequate protection. Most routers use either network address translation (NAT) or a packet filter. Information on the Internet is transmitted in packets which contain the IP address of the sender and the address of the receiver in addition to the data. The routers firewall uses filters that look at the sending and receiving addresses of incoming packets on port 80 (HTTP). Only those packets that are a response to an outgoing request are allowed through. If your router uses a packet filter it can be penetrated by a fragmented scan. This type of scan breaks up packets into fragments which can easily get through the simple packet filter found in most router firewalls. Routers using NAT either alone or in combination with a packet filter can also be easily thwarted. NAT is not successful when the packet is an FTP packet or is sent by Microsoft's Netmeeting or similar audio/video applications that bury the address in the body of the packet. Only when the address is in the header of the packet can the router use address substitution. So packet filtering and NAT, although useful, do not provide complete firewall protection for all Internet connections.

Another method for preventing intrusions is “stateful” packet inspection. This is the method used by most software firewalls and is found in some of the newer routers. When your web browser opens a connection to the Internet, the firewall software records that connection and keeps a record of its status. Whenever a packet arrives at your computer, the data in the packet can be compared to the information in the firewall state table. The firewall software can also make decisions based on the data content of the packet, not just the sender's address. Because this examination does require some time there may be a slight slowdown of your system. However, in most cases, there will not be a long enough delay for most users to notice.

So inbound packets can be filtered and examined for dangerous content. However, when the user connects to a web server, the page requested is downloaded to the users computer. It is possible for that web page to contain a small program or a link to a dangerous site in a one pixel unit on the page. When this is downloaded the program is run or the link activated. This results in an outgoing packet to some Internet address through a non-standard port so the user is not aware of the activity. This type of activity would not be stopped by a hardware firewall in a router. It can only be blocked by a software firewall which recognizes that this activity is coming from a new application that has not previously made an Internet connection. In this case the software will query the computer user to determine if this new application should be allowed to connect. Hopefully, the user would recognize that this was not an application that the user was running and the outbound packet would then be blocked. It is absolutely necessary for the firewall to process both incoming and outgoing packets. Only a software firewall can establish the necessary tables for comparing the incoming/outgoing packets to allowed activity and request user interaction when necessary.

This leads us to the Windows firewall. This firewall, as used with Windows XP, does not have any control of outbound packets. Any application is allowed to connect to the Internet without any filtering or other checking of source or content. Windows Vista was supposed to come with both inbound and outbound filtering. However, as it is delivered it provides only inbound protection just as did XP. The outbound protection is turned off by default. So, if it is there, how do you turn on the outbound protection. To change this you have to use the Microsoft Management Console. Then you have to write a rule to block each “malware” application you anticipate might get on your computer. You can not create a general rule for all malware. Creating rules that would cover all possible malware applications is an impossible task. Microsoft has been quoted as saying “outbound filtering isn't really needed, and the key is making sure that malware doesn't infect the PC in the first place.” Also they have stated that large enterprises had requested that it be turned off by default. Microsoft does say that “core Windows Services have specific behaviors which are monitored by the firewall”. Instead of using outbound filtering Microsoft recommends that you buy “Windows Live OneCare”, a product and subscription service. My rec-

(Continued on page 6)

(Continued from page 5)

ommendation is that you obtain a free two-way firewall like ZoneAlarm and ignore the Windows firewall completely.

Whatever you do, don't connect your computer to the Internet without using a firewall and an antivirus application. I have come across too many computers recently that are attached to constant on Internet connections and had no protection. The cost of removing the malware from these systems was more than the cost of premium protection. So don't get caught short!

Dr. Lewis is a former university & medical school professor. He has been working with personal computers for more than thirty years. He can be reached via e-mail: bwsail at yahoo dot com.

+++++

VistaVexes

The Windows Vista Pains'n'Gains Page

By Jan Fagerholm, Associate Editor, PC Community, Hayward, California

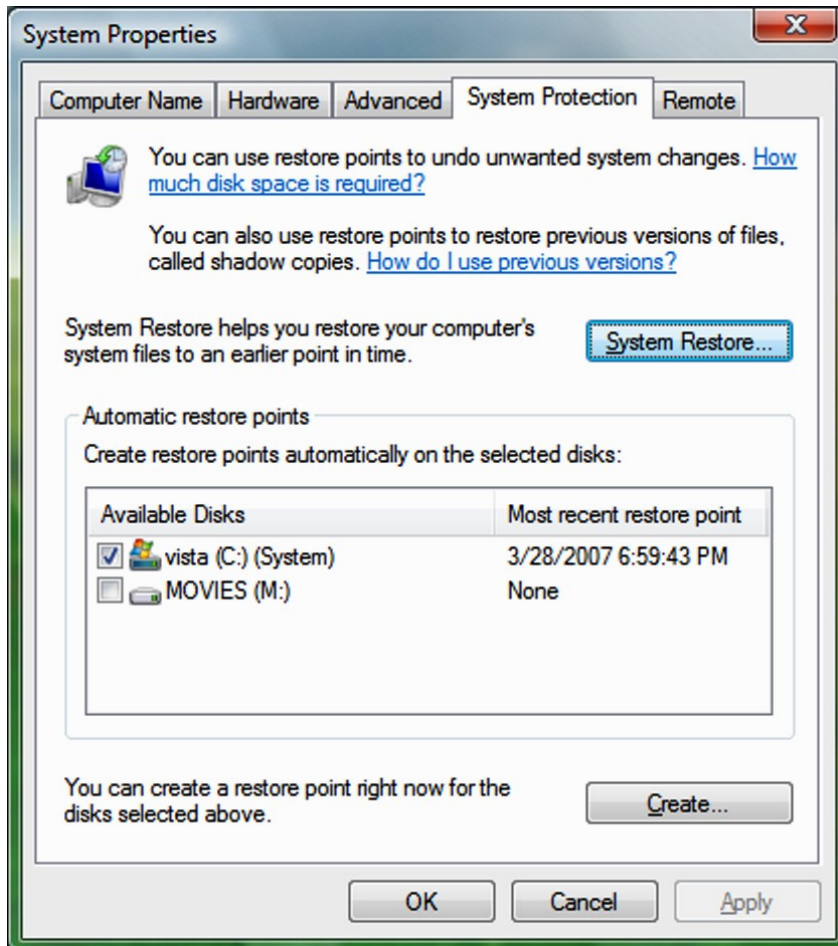
http://www.pcc.org

jan-f(at)pacbell.net

Obtained from APCUG with the author's permission for publication by APCUG member groups.

I've been transitioning to Vista cautiously with a dual boot system with both Vista and Windows XP for several months now. This has not been as painless as I might have expected because of the changes that Microsoft made in NTFS and the System Restore feature. Before delving into diatribe,

though, I need to explain how this system is set up.



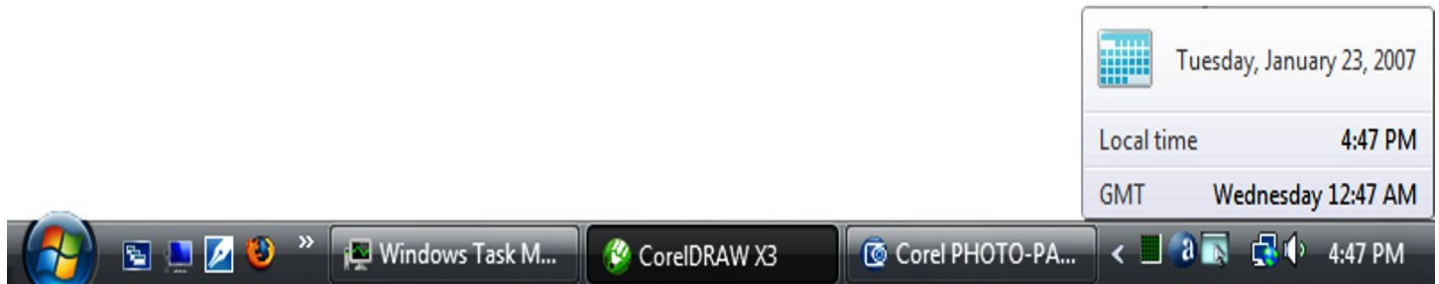
I use conventional IT practices for installing the OS, programs, and data on separate partitions on the hard drive. This is useful for preserving data in case the OS fails. (That's "when", not "if" in the case of Windows.) So, installing another operating system is a simple matter of creating a new partition for it, then installing the OS on that partition. You can boot into either OS at startup, then access the data, which is on its own partition. (Incidentally, this also makes backup chores easier, as you can simply back up the partition with the data on it, which is what you really want to keep.)

The problem comes when running Vista and XP on the same drive, because of the changes Microsoft made in System Restore. They are not compatible between Vista and XP. If you have System Restore set to monitor all partitions (the default), XP will wipe out Vista's restore points when it starts, and Vista will wipe out XP's restore

(Continued from page 6)

points when it starts, so if you have a problem with, oh, let's say Vista, which you will because it's barely out of beta, then you boot into XP to recover something, guess what! – you cannot restore any of your drives in XP because Vista wiped out all of XP's restore points! (Ask me how I know . . .)

There is a solution to this, though it does require you to commit to one system or the other. In my case, I took the plunge and gave System Restore responsibilities to Vista by turning off System Restore in Windows XP. This way I can still use both XP and Vista without losing the much-needed functionality of System Restore. I am committed to moving to Vista on the Windows side (though I spend most of my constructive time in the *nix systems of Linux and OS X.) At least this way I am able to use System Restore where I need it most, namely in Vista.



Looking beyond the gloom and doom view, there have been a couple of nice additions to Vista since it came out. I'm running Vista Ultimate, which offers something called "Windows Ultimate Extras". These are some fluff pieces offered from time to time that are similar to what the old Plus Pack used to offer. In the case of Windows Ultimate Extras, these additions are offered as downloads and you receive notification of them through Windows Update, where you can download them. A recent addition is a wallpaper feature called DreamScenes, which provides animated displays as wallpaper on the desktop. Microsoft has turned some thoughtful people loose on this concept, so while my first reaction to things that wiggle on the desktop is that it is just distracting, there are some very pleasant and gentle animations that I find pleasing without being disquieting. There are a couple of nature scenes that I like to activate while I am writing, as the effect is similar to gazing out the window when you sit back seeking inspiration.

The last month has seen two of my must-have applications come out with Vista compatible versions; Corel Graphics Suite X3 and ABBYY FineReader Pro (OCR program). I'm still recommending that you wait for Vista SP-1 before upgrading from XP, unless you are adventurous enough to try some alternatives to what you may be using now.

So this month I found out that dual booting XP with Vista will trash my system recovery options while soothing my jangled nerves with moving wallpaper. What next?

+++++

Secure Your Flash Drive Cap

By Fran Damratowski. Refurbishing SIG Leader, Chesapeake PC Users Group, MD
www.chesapeakepcusersgroup.org
[refurbishing\(at\)chesapeakepcusersgroup.org](mailto:refurbishing(at)chesapeakepcusersgroup.org)

Obtained from APCUG with the author's permission for publication by APCUG member groups.

Have you ever misplaced your flash drive cap? No need to ever do that again. Secure it with a button. You will need
 --a shirt button,
 --some heavy thread such as carpet thread,

(Continued on page 8)

(Continued from page 7)

- double sided self-sticking adhesive mounting foam,
- double sided sticky tape, and
- some colorless nail polish.

1. Run the thread diagonally through two of the buttonholes and secure with a square knot.
 2. Place the knot on the top of the button not on the flat bottom of the button.
 3. Cut the thread long enough to secure it with enough play to remove the cap.
 4. Cut a small piece of the double-sided self-sticking adhesive mounting foam about the size of the button.
 5. Remove the backing from one side of the double-sided self-sticking adhesive mounting foam and place a small piece of the double-sided sticky tape on the sticky side of the double-sided self-sticking adhesive mounting foam. (The double-sided self-sticking adhesive mounting foam does not hold well without the sticky tape. The tape alone does not hold well either.)
 6. Securely attach the flat side of the button to the sticky tape.
 7. Trim the excess tape and foam using an x-acto knife.
 8. Remove the backing from the other side of the double-sided self-sticking adhesive mounting foam and place another piece of double sided sticky tape on the foam.
 9. Securely attach the button foam and tape to the flash drive cap.
 10. Secure the other end of the thread to the flash drive or lanyard.
 11. Leave enough play to easily remove the cap, but not get tangled.
 12. Use the colorless nail polish to secure the knots so they don't become undone.
- After the nail polish dries trim the thread.



OR

You could go to your local photo shop and buy a \$2+ button size lens cap keeper (or cap retainer) and modify it as needed. Most of them appear to come with elastic bands that are placed around the lens barrel as opposed to a leash that can be attached to another part of the camera.

+++++

Live CD-ROMs

By Dick Maybach. a Member of the Brookdale Computer User Group, New Jersey

<http://www.bcug.com/>

N2nd(at)att.net

Obtained from APCUG with the author's permission for publication by APCUG member groups.

In the early days of PCs, we did much more experimenting than we do now. The only long-term storage was on diskettes, and when we removed the diskette holding the operating system, we also removed

(Continued on page 9)

(Continued from page 8)

any problems that resulted from our experiments. Now, our hard disks hold large, complex operating systems, and if they are damaged by our errors or by malware such viruses, the recovery process can be long and painful. Those who still like to experiment should consider live CD-ROMs.

A live CD-ROM contains an operating system and applications and can be run without using the hard disk at all. When you remove the CD-ROM, your old operating system (probably Windows) takes over. In fact, since the hard disk was not accessed while the live CD-ROM was running, Windows is no more aware that the PC has been used than if you had never switched on the power.

To use a live CD-ROM, you must set up your PC so that if a CD-ROM is present, it will try to boot from it, rather than the hard disk. Watch carefully as your PC boots, and you should see a message telling you how to start the BIOS set-up program. Often, the procedure is to press the F2 key repeatedly during booting. Don't just hold it down, as the PC will think your keyboard has a stuck key and will refuse to start. Once the set-up program has started, read each screen carefully before changing anything. If you think you've made a mistake, exit without changing anything (often done by pressing the escape key) and start again. You are looking for the screen that lets you change the boot order, which is the order in which the PC checks devices for an operating system. It always includes the hard disk, diskette, and CD-ROM, and (on newer machines) USB devices. In our case we want the CD-ROM checked before the hard disk. Once you are satisfied that everything is ok, save your changes and exit the program, often done by pressing F10.

You can download live CD-ROM programs free from the Internet. However, you will now have what's called an ISO image; this is not a file, and if you write it to a CD-ROM as a file, it won't be bootable. Unfortunately, the free versions of CD-ROM burner programs included with many PCs won't burn ISO images. However, a suitable program, *ISO Recorder*, is available, free over the internet from <http://isorecorder.alexfeinman.com/isorecorder.htm>. Many live CD-ROMs are also available as pre-recorded CD-ROMs; see the referenced Web sites for information.

A good place to start is with the *Ultimate Boot CD*, available at <http://www.ultimatebootcd.com/>. This provides four versions of DOS and five of Linux, plus tools for motherboard, hard disk, and file system maintenance, in addition to four virus scanners.

If you long for the simpler days of DOS, see <http://www.freedos.org/> to obtain an open-source clone of DOS. This will allow you to get acquainted with the command line, BAT files, BASIC programming, and run those old programs that no longer work under Windows. The full version contains some extras, FreeGEM (a clone of the old Digital Research graphical user interface), BWBasic (Bywater Basic), and several games.

If you would like to experiment with Linux, but aren't ready yet to install it on your hard disk, look at Ubuntu, <http://www.ubuntu.com/>, which provides a Windows-like interface, or Knoppix, <http://www.knoppix.org/>, which is known for being very adaptable to different PC hardware. Several tutorial books are available for each; check your local Barnes & Noble or Borders.

For Linux, Windows, and, to a limited extent, Macintosh maintenance and recovery, my favorite is INSERT, available at http://www.inside-security.de/insert_en.html. This is worth a complete article, and I'll discuss it next month's column.

Security Tools Distribution (STD), <http://s-t-d.org/>, is a variant of Knoppix, customized for those in computer security. It includes tools for encryption and code-breaking, for finding evidence of computer

(Continued on page 10)

(Continued from page 9)

break-ins, for working with firewalls, for building honey pots (traps for ensnaring hackers), for analyzing and breaking passwords, for analyzing network traffic, and for assessing computer vulnerability.

You can see a long list of available live CD-ROMs at <http://www.frozentech.com/content/livecd.php>. Most of these are versions of Linux, because its source code is available and free, and because it's modular. Windows, by comparison, is proprietary and monolithic; at one point, Microsoft claimed that you couldn't remove even its Internet browser without disabling the operating system.

+++++

Buying an HDTV – Recap of the SWIPCUG February 2007 Meeting

By Pim Borman, Webmaster, with notes by Kay Anne Peake, Member of SW Indiana PC Users Group, Inc.

<http://swipcug.apcug.org/>

swipcug(at)sigecom.net

Obtained from APCUG with the author's permission for publication by APCUG member groups.

Robert D. Covington was the featured presenter. He explained that he does not sell TVs but learned a lot about them while advising a variety of companies as CTO of Rhysome, a provider of Enterprise Software.

Bob explained how TV broadcasters are in the process of changing from analog to digital technology. The change will result in more efficient use of the available transmission frequencies and improved image quality. The US Government also had a \$14 billion windfall from auctioning off the available frequency bands to interested parties. As long as there is adequate signal strength digital TV presents a sharp picture, free of snow and distortions. When there is poor reception an analog TV might still present a recognizable picture, but the digital TV won't show any picture at all. It is easier to manipulate digital transmissions, and to make and store perfect copies. The downside is that digital data can be compressed to reduce bandwidth requirements, resulting in loss of quality, and that they are wide open to all sorts of Digital Rights Management (DRM) restrictions that so far have caused problems and demonstrations.

February 17, 2009 is the currently expected date when broadcasters will stop sending analog signals. TV sets will continue to receive programs from cable and satellite providers who will supply conversion boxes to their customers. TV receivers connected to an antenna will no longer work, unless provided with a converter box and a suitable antenna to receive the digital signals. Starting in 2008, the National Telecommunications and Information Administration (NTIA) will provide up to 2 coupons per household, worth \$40 each, towards the purchase of the converter boxes. The required antennas are similar to those used for UHF reception on analog TVs, but they are more sensitive and can be placed almost anywhere in the house. For more details see <http://www.ntia.doc.gov> .

Concurrent with the change to digital broadcasting, the aspect ratio of the picture is being changed from the current 4:3 to 16:9. The 4:3 ratio was originally chosen because it was similar to the 35 mm slide format. The 16:9 ratio is the format used for most current Hollywood movies and is therefore preferred for the best display of movies on a TV screen. Many TV programs and commercials are already being produced in the new format and show up on current televisions as a "letterbox" across the screen, unless the receiver has the new, wider format.

(Continued from page 10)

Digital broadcasts will use different protocols depending on the transmission medium. Over-the-air transmissions to antennas will use ATSC (8VSB), satellite broadcasts use QPSK, and cable systems use QAM ("kwam"). When buying a converter box it is important to make sure it supports the correct protocol. Cable and satellite providers are likely to provide the correct boxes, but over-the-air (antenna-based) receivers will need an ATSC-capable converter. Newer TVs may also have built-in QAM conversion. In that case the cable provider only has to install a circuit card to configure the connection.

As with all things digital, what used to be simple and good for a lifetime of use gets complicated and subject to early obsolescence with digital TVs. The buyer will be faced with many choices to make in addition to the screen size he prefers and can afford. The next most important choice involves the type of display. Bob described 3 kinds, current Standard Definition TV (SDTV), Enhanced Definition TV (EDTV), and High Definition TV (HDTV).

SDTV and EDTV both use a screen with 480 lines of 640 pixels wide, but EDTV also provides a choice in screen dimensions with 4:3 ratio or 16:9 ratio, and progressive or interlaced scanning. As Bob explained, with interlaced scanning as currently used each frame is generated in 2 steps, first painting the odd-numbered lines followed by the even-numbered lines. If each step takes 1/60th of a second, the resulting frame rate is 30 fps. In progressive scanning all the lines of each frame are painted in a single step. In fast-moving scenes, such as sports broadcasts, interlaced scanning can result in a slightly distorted picture on large monitors and the (more expensive) progressive method is then preferred.

HDTV is available in 2 screen resolutions, 720 lines of 1280 pixels progressive only, or 1080 lines of 1920 pixels with a choice of interlaced or progressive. How's your headache so far? But wait, there's more! With EDTV and HDTV you also have a choice of frame rates, usually 24, 30, or 60, depending on the other parameters chosen. Not many broadcasts are of the highest possible quality, as the broadcasters may prefer instead to use their allotted bandwidth to transmit several different programs at the same time, using various compression levels and display parameters. The difference in quality may not even be noticeable except on the largest displays. But there is no point in paying for the best quality if no matching broadcasts are available.

Bob discussed what to look for when you buy a digital TV. One of the specifications is the luminance (brightness) of the display in candelas per square meter (cd/m²). An LCD or plasma screen should have a minimum of 250 cd/m² while a projection system should have at least 1200 cd/m². The other display specification is the contrast ratio between white and black areas, at least 800:1.

To support digital connections between digital devices, new cable standards have been developed to make connections between units of a digital home system. The new Direct Video Interface (DVI) standards are labeled DVI-D for carrying digital signals only, and DVI-I for carrying digital-to-digital and analog-to-analog signals. A DVI-D plug will fit in a DVI-I socket, but not the other way around. Converter boxes usually carry a complete set of outlets compatible with DVI as well as the older RGB, 3-wire composite, and S-video connections. A more recent standard, High Definition Multimedia Interface (HDMI), carries both digital video and sound but is only useful if your whole home theater is newly digital and supports the cables.

CRT displays are rapidly disappearing because of their bulk and difficulty in forming a sharp color image across a large screen. Liquid Crystal Displays (LCD) are currently the most economical but suffer from limited contrast, brightness, color depth, slow refresh rates, and fixed screen resolution. Plasma displays depend on micro fluorescent light sources to provide bright images with excellent color, a wide viewing angle, and high contrast. They are still expensive and limited in size and have a limited lifetime.

(Continued on page 12)

[However, when they burn out they have probably become obsolete already anyway, and a new unit of higher quality may be available at lower cost – Pim.] Finally, for large sizes projection displays have been used. They are based on Texas Instrument Digital Light Processing (DLP) technology that uses a chip with thousands of tiny mirrors that can flip up and down to direct light beams to the screen. They use an expensive, bright light bulb of limited lifetime.

+++++

Guilty!

By Berry F. Phillips, a Member of the Computer Club of Oklahoma City and a monthly contributor to the e-Monitor

www.ccokc.org

bfpdata(at)laccess.net

Obtained from APCUG with the author's permission for publication by APCUG member groups.

Guilty, the strange judge shouted as he banged the gavel. The defendant will rise and receive his sentence. You have been found guilty of dirty deeds done to your computer and are sentenced to electrocution!" I thought to myself, with my knees shaking, there must be some kind of an appeal process since the judge and jury all had heads that looked like monitors and bodies like upright computers and could easily be biased and not in my human favor!

I did find the testimony at my trial to be informative. A clean environment does not require computer cleaning usually more than once a year. Many computer users like to do the cleaning when they are doing their annual spring house cleaning. The dirtier the environment the greater frequency of cleaning needed. A clean computer cuts down on downtime, repair bills, and minimizes health risks. **DO NOT EAT, DRINK, SMOKE, OR USE MAGNETS NEAR YOUR COMPUTER AFTER ALL IT IS NOT A FAST FOOD JOINT!**

Here are some tips: (1) shut your computer down properly, (2) run scan disk and defragmenter at least monthly, (3) Delete files and programs you no longer need, (4) use antivirus, anti spyware programs and a good hard drive cleaner like the freeware CCleaner and a registry cleaner like the freeware RegClean to keep your hard drive healthy, (5) **BACK UP YOUR DATA IN CASE OF AN EMERGENCY!**

When cleaning your computer case, use a damp lint free cloth. **NEVER SPRAY WATER ON A COMPUTER OR OTHER ELECTRICAL DEVICES.** Place liquid on the cloth not directly on the system and normally 100% alcohol which has no water content. Use a pencil eraser on hard to remove marks. The monitor can be cleaned with a commercial glass cleaner using a damp clean lint free cloth. Using an anti static wipe or a dry cloth with anti-static fabric softener will reduce the dust attracted by static discharge. The keyboard can be cleaned by turning the keyboard upside down and shaking the gunk out of it while singing, "There is a whole lot of shaking going on." Clean the keyboard surface with a damp lint free cloth with 100% alcohol. **DO NOT TAKE THE KEYBOARD APART OR YOU MIGHT NOT GET IT BACK TOGETHER AGAIN!** Clean the mouse by taking it apart using a damp lint free cloth and clean the rollers inside of the mouse (be sure to rotate them) with a clean cotton swab with 100% alcohol solution. After the mouse has dried put it back together reversing the steps you did when taking it apart. The inside of your computer is a dust magnet. An annual cleaning in a normal computer environment is a good idea. **YOU MUST BE VERY CAREFUL IF YOU DECIDE TO CLEAN THE INSIDE OF YOUR COMPUTER OR YOU COULD DO DAMAGE TO YOUR SYSTEM!** Whenever, you go into the case of your computer it is a good idea to wear a grounding strap to reduce the risk of a static discharge. Blow out dust with compressed air or a vacuum cleaner. Avoid touching chips or electronic components on your system. Electronic components run hotter when covered with dust blankets, and it shortens their normal life span which is why your computer needs to be cleaned internally periodically.

I have to go now to get a human attorney to appeal my case so I can avoid electrical execution so there will be another article in the Computer Hysteria Column for next month. However, I do have one final question for you, **"Are you guilty?"**