Midland Computer Club

BITS AND BYTES

The Newsletter of the Midland Computer Club

April 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: April 25th

THIS MONTH'S TOPIC: Larry Piper will be giving a presentation on "How to run Ubuntu Linux on your PC ".

PROGRAM COORDINATORS
Contact :

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

What You Missed

The **March** meeting had Howard Lewis demonstrating the new Microsoft Office 2007. There are many new enhancements to Office, one of which is a new interface. While it may take some time for a seasoned Office user to make the migration, most people seem to find the new interface much more efficient.

Upcoming Activities

There has been a change in the plans for the **April** meeting. Larry Piper will be giving a presentation on "How to run Ubuntu Linux on your PC." Many people are becoming disillusioned with Microsoft Windows and are looking for some alternatives. This is an opportunity to see one of those alternatives and be able to compare it to the interface with which we are so familiar.

In **May**, Howard Lewis will demonstrate the new Microsoft Windows Vista. The presentation will include the new interface and some of the advantages and disadvantages of move from Windows XP toWindows Vista.

The President's Corner

Two weeks ago, one of my favorite "old world" (i.e., print) rags (InfoWorld) announced that it would no longer produce a printed copy of their weekly magazine. All of their content would be available online at www.infoworld.com. This sort of surprised me as I had not thought much about the future of print media. However (no matter how full your "snail" mailbox is on a daily basis), the trend for years has been to move to electronic distribution of most newsworthy items. Most of my technical information is picked up online as well as local and world news. Last October, when I was visiting my son in the Seattle area, I received an e-mail telling me about the death of someone I knew. I immediately went online to the Midland Daily News website and read that person's obituary. I still subscribe to a number of magazines, but I also subscribe to several times that quantity of electronic newsletters. I probably read the local newspaper in less than five minutes each day because I've already picked up more current news online. Once I reflected on this fact, it does not surprise me that many magazines are now significantly thinner than they used to be (take a look at a current issue of PC Magazine compared to 10 years ago). Even the club went to electronic distribution of our monthly newsletter because of the cost of printing, copying and mailing the paper version. Some people will say that they don't like doing extensive reading on a monitor or they can't take their computer with them wherever they go. In those cases, the simple answer is to print off what you WANT to read instead of taking the whole thing (including ads) with you. And if you are one who likes to do their reading in the bathroom, please feel free to print off what you want to read and take it with you. Some people have been known to take their laptops or PDAs with them with dire results. After all water and computers do not coexist very well!

If you have any comments on this, please feel free to let me know. — Howard Lewis

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

MCC OFFICERS

POSITION		EMAIL:
President	Howard Lewis	lewis3ha@chartermi.net
Vice Pres.	Bill Tower	stressed@tir.com
Treasurer	Bob Miller	barloshelties@sbcglobal.net
Membership	Gary Ensing	gensing@juno.com
Editor	Jan Ensing	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

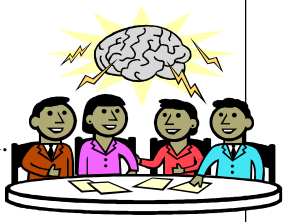
Terry Brown	t_bbrown@yahoo.com

PUBLICITY

Kathy Bohl	kbohl30265@aol.com

Board Meeting

The next board meeting will be 7 p.m., April 10, 2007, at Chapel Lane Presbyterian Church, 5501 Jefferson Ave., Midland.



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

http://grist.org/ – Grist is a web site that feels news about green issues and sustainable living doesn't have to be predictable, demoralizing, or dull. If you have always thought that environmental news and commentary have been dry and boring, think again and visit this site. We should all be environmentalists!

Http://www.loons.com/ – If you've been living under a rock and haven't read or heard any news lately, our Great Lake Loons are here. This is the official site for the Loons. Be sure to check it out. It has all sorts of information on the team, their schedule, their players, the store and of course, Lou E. Loon.

http://mikeshea.com/ – On the subject of baseball, Fenway Park is probably the oldest park in Major League Baseball. There is a move on to replace the park with a new modern park. This site presents the new park and what can be done to save the old one. Now if action had been taken sooner, perhaps Briggs Stadium could have been preserved.

http://www.bootdisk.com/ – Has your hard disk crashed and your boot disk backup failed? Here is a site where you can download a boot disk that will allow you to get your system back up and running so you can figure out what went wrong.

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

Tips, Tricks & Techniques

Browse Multiple Websites Using Internet Explorer 7

Windows Internet Explorer 7 enables you to run a single copy of Internet Explorer with multiple pages in one window (called Tabs). When you use multiple tabs you can:

Open a new page by clicking the empty tab on the toolbar (next to the current tab) or by right-clicking any hyperlink and choosing *Open in New Tab*.
Refresh individual pages or refresh pages as a group by right-clicking tabs and selecting *Refresh*.
Close either individual tabs (by clicking the "X" on the right side of the tab) or an entire group.
Save tabs as a group under *Favorites*.
View thumbnail images of all open tabs in a single view using the Quick Tabs feature (under *View/Quick Tabs*).

Organize Your Files into Groups

The files and folders listed in Windows Explorer can be organized by Group to make it easier to find a specific file. To organize your files into groups try this:

Open a folder containing several different folders and/or file types.
Right-Click on an empty space on the window's contents pane and click *Arrange Icons By*
Next Click *Show in Groups*.
To arrange the window's contents (by Type for example), right-click again in any empty space on the window's contents pane, point to *Arrange Icons By*, and click *Type*.

The list can be modified by *Name*, *Size*, *Type*, or last *Modified*.

Experience the Windows Vista Aero Interface

If your PC supports the new Windows Aero interface, you can open multiple files and see how easy it is to locate the right open window using **Windows Flip** or **Flip 3D**.

To use **Windows Flip**, press *Alt+Tab*.
To use **Flip 3D**, press the *Start menu key+Tab*.

Rename Many Files at Once

If you import digital photos into your computer, you have probably gotten frustrated at the fact that they end up as just sequentially numbered files. To rename a series of pictures there is a simple way to rename a group of pictures:

1. Open the folder where you've saved your pictures.
2. Click on the first picture of a group of pictures to be renamed.
3. Shift-Click on the last picture of the group (which highlights the whole group).
2. Right-Click the first picture selected and then click *Rename*.
3. Rename the first picture to whatever you like (for example, "Dow Gardens"), then *Click* any empty space within the window to deselect the pictures.

Your pictures will automatically be renamed ("Dow Gardens (1)," "Dow Gardens (2)," etc.). This tip also works to rename any collection of files.

Countdown to the Digital Deadline

By Jim Sanders, Editor, North Orange County Computer Club, California
www.noccc.org
editor(at)noccc.org
Obtained from APCUG with the author's permission for publication by APCUG member groups.

Television, as most of us know it, has barely two years of life left in it. Congress has set a deadline of February 17, 2009 for analog broadcasts to end. That means that the faithful television that you have had, for I don't know how many years, will cease functioning on that date. Well, cease functioning may be too strong of a description, but there will no longer be an over the air broadcast of the analog type of signal that it knows how to interpret.

Starting on that date, all of the over the air television broadcasting stations have been mandated to transmit the digital television format signal only. Old faithful, or maybe not so old, can still be used as long as there is some device that can feed it the analog signal that it knows how to deal with. This could be your VCR or DVD player for instance. Or, it could be one of the set top boxes that millions of people are going to have to purchase if they wish to continue using their analog television to receive over the air television broadcasts. The purpose of the set top box is to tune in the digital television frequency and convert it to the NTSB analog signal that your television knows how to deal with.

The set top boxes contain an ATSC tuner. This stands for Advanced Television Systems Committee. They are an international organization setting the standards for digital television. In time, they will replace the NTSC, which is an American organization overseeing analog TV transmissions. There is considerable talk about Congress passing legislation to subsidize, or provide free of charge, set top boxes to low income families. At this time there is no requirement that the recipients be United States citizens.

When you purchase a digital television, ATSC is a term that will be listed on the specifications showing that the television has a built-in digital tuner. There are eighteen formats in the DTV spectrum, 12 SDTV formats and 6 HDTV formats.

The Federal Communications Commission (FCC) is the regulating organization in the United States that controls conversion from analog to digital. The Federal Communications Commission has set deadlines that mandate all manufacturers include digital tuners in their televisions. These are the dates that have been mandated:

July 1, 2005: all TVs with screen sizes over 36 in. must include built-in ATSC tuner.
July 1, 2006: 100% of 25 to 35in. TVs must include ATSC DTV tuner.
July 1, 2007: 100% of 13 to 24in. TVs must include ATSC DTV tuner.
July 1, 2007 100% of all interface device's must have ATSC DTV tuner. That includes equipment such as VHS VCRs, DVD player/recorders, and DVRs.

These deadlines only apply to new televisions and do not include the huge inventory of existing units. That is why you may see a number of television's larger than 36in. still being sold without built-in digital tuners.

Definition of television; a television is a viewing device that includes a tuner. A device without a tuner is called a monitor. There is a loophole in the FCC regulations that allows manufacturers to build TVs without any tuner which would technically make it a monitor.

Most cable subscribers and all satellite subscribers use their service provider's set top box to receive and decode the digital signals instead of using the television's built-in ATSC tuner. One exception to

(Continued on page 5)

(Continued from page 4)

that rule is a small credit card type of chip that takes the place of the set top box and is called a Cable-CARD.

Most cable and satellite providers charge in the neighborhood of $9.95 a month to receive HD channels. Over the air High Definition channels are “free” in the same sense that current analog channels are free, that is you pay the price of watching the commercials but don’t actually have to shell out money. So if you spend the extra bucks up front to buy an HD television that includes the ATSC tuner, you are not forced to pay that additional monthly charge. By purchasing an antenna from an electronics store for in the neighborhood of $25.00 to $100.00, a person that owns a set with a built-in ATSC tuner can enjoy the over the air broadcasts for free.

When the analog signals are turned off and digital becomes the standard, cable and satellite providers will probably provide the local networks for free if they don’t do so already. But you will still have to buy or lease the cable box which right now costs in the neighborhood of $199.00. In addition to that, you’ll still have to purchase the programming from the provider.

So if you are a person that currently relies on getting all of your television through a rooftop antenna, in less than two years you will be faced with the choice of spending money for some new equipment or no longer being able to watch television.

One method of dealing with the problem would be to purchase one of the new DVD VCR combos that include the ATSC tuner. A number of VCR manufacturers, including Panasonic, have announced that when the new regulations go into effect, they will simply stop manufacturing that class of equipment. JVC has announced a new DVD/VCR/ATSC tuner model that will be available in May, the DRMV99 at $329.95. If you already own a good VCR and a good DVD player, it might make more sense to go ahead and purchase just the ATSC set top tuner.

In addition to dealing with all of the high definition signal acquisition problems, a whole lot of people are already trying to deal with the somewhat confusing array of HDTV offerings. The terminology which is frequently observed in the papers can be very confusing. The phrase “HD ready” is usually an indicator that the unit is a monitor that does not include a tuner. A lot of advertisements conveniently do not include what version of high definition a particular offering is. It is simply referred to as HD without saying whether it is 720i, 720p, 1080i or 1080p. The actual pixel resolution is often omitted as well. The 720i or p sets need to have a resolution of 1280 pixels by 720 pixels. The real 1080i or p sets need to have a resolution of 1920 pixels by 1080 pixels. Just like the older VGA computer monitors the 720i refers to an interlaced display and the 720p refers to a progressive scan display. The progressive display is the better quality.

Then you have to decide which display technology you are going to pick. The Plasma flat panel, the LCD flat panel, the rear projection DLP television, the rear projection LCD television, the wall projection unit in either DLP or LCD. What is the brightness level? What is the viewing angle? What is the life expectancy of the projector bulb? What is the cost of the projector bulb? Does the unit have a VGA, a DVI and an HDMI video connector?

At the moment, I think the best bang for the buck is to purchase a projector that will do 720p, and if you can afford the extra cost, one that will do 1080p. If you have never seen even an older 800x600 projector displaying a movie from a standard DVD on an eight foot diagonal screen, I think you will find it impressive and I think you should do that before you spend money on anything.

Some selected FAQs from your http://www.dtv.gov/ site.

What is the digital TV transition?
The switch from analog TV (the traditional TV system using

(Continued on page 6)

(Continued from page 5)

magnetic waves to transmit and display TV pictures and sound) to digital television (the new TV system using information transmit-ted as “data bits” -- like a computer -- to display movie-quality pictures and sound), is referred to at the digital TV (DTV) transi-tion. In 1996, the U.S. Congress authorized the distribution of an additional broadcast channel to each TV broadcaster so that they could introduce DTV service while simultaneously continuing their analog TV broadcasts. In addition to improved picture and sound quality, an important benefit of DTV is that it will free up parts of the broadcast spectrum for public safety as well as other valuable uses. This is possible because the modern technology of DTV is more efficient than analog TV technology. DTV allows the same number of stations to broadcast using fewer total channels (less of the broadcast spectrum) which will free up scarce and valuable spectrum for public safety and new wireless services.

What is the February 17th, 2009 DTV deadline date?
Congress passed a law on February 1, 2006, setting a final deadline for the DTV transition of February 17, 2009. Most television stations will continue broadcasting both analog and digital programming until February 17, 2009, when all analog broadcasting will stop. Analog TVs receiving over-the-air pro-gramming will still work after that date, but owners of these TVs will need to buy converter boxes to change digital broadcasts into analog format. Converter boxes will be available from consumer electronic products retailers at that time. Cable and satellite sub-scribers with analog TVs should contact their service providers about obtaining converter boxes for the DTV transition.

What is digital television (DTV)?
Digital television (DTV) is a new type of broadcasting tech-nology that will transform television as we now know it. By transmitting the information used to make a TV picture and sound as “data bits” (like a computer), a digital broadcaster can carry more information than is currently possible with analog broadcast technology. For example, the technology allows the transmission of pictures with higher resolution for dramatically better picture and sound quality than currently available – called High Definition Television (HDTV) - or the transmission of several “standard definition” TV programs at once – called “multicasting.” “Standard definition” digital TV pictures would be similar in clarity and detail to the best TV pictures being received and displayed today using the current analog broadcast system and TV receivers. DTV technology can also be used to provide interactive video and data services that are not possible with “analog” technology.

Is HDTV the same thing as DTV?
HDTV is the highest quality of DTV, but it is only one of many formats. In addition to HDTV, the most common formats are Standard Definition Television (SDTV) and Enhanced Defini-tion Television (EDTV).

SDTV is the baseline display and resolution for both analog and digital. Transmission of SDTV may be in either the tradi-tional (4:3) or wide-screen (16:9) format. EDTV is a step up from Analog Television. EDTV comes in widescreen (16:9) or traditional (4:3) format and provides better picture quality than SDTV, but not as high as HDTV.

VistaVexes
The Windows Vista Pains’n’Gains Page
By Jan Fagerholm, Assistant 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.

Applications compatibility is still slow coming in Vista. Since Vista came out, Microsoft has released one update aimed at improving applications compatibility (KB929427). While it is not unreasonable to expect vendors to update their applications, Microsoft has not been forthcoming with information that vendors need. Both Symantec and McAfee (70% of the anti-virus market) are at open war with Microsoft over the lack of kernel information on Vista. Microsoft says this is for “security reasons”. This reasoning seems specious in view of That Other Operating System

(Continued on page 12)

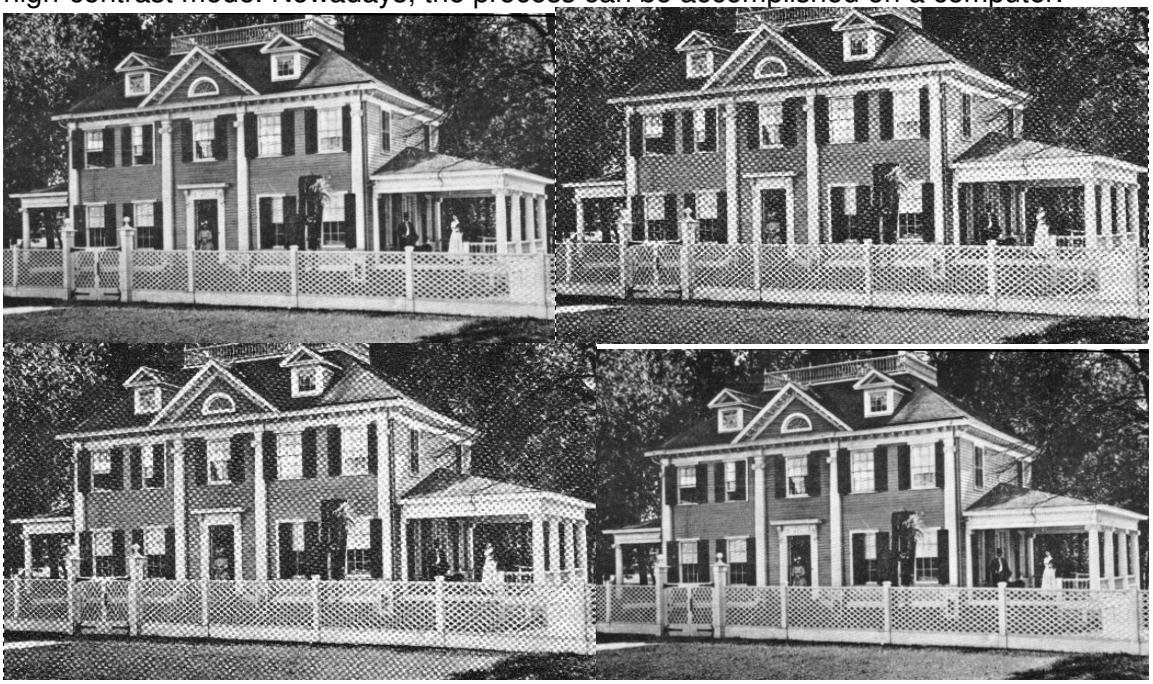
Scanning Published Photos

By Irving Elliott, Twin Cities PC User Group, Minnesota
www.tcpc.com/
irving.elliott(at)att.net

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

If you scan a photo from a newspaper or magazine, then examine the results on your computer screen, you may see a criss-cross pattern of fuzzy lines over the entire print. If you print the scanned photo, you may also see such a pattern. This happens because pictures in newspapers and magazines are printed in a “halftone” mode.

The halftone process was invented when it was desired to print black-gray-white photographs using a printing press that used only single-color black ink. In this process, the photo is divided into a pattern of small squares, then each square is replaced with a black “blob” of a size proportional to the average shade of black in the square. For example: a white square remains white; a light gray square becomes a small black blob; a dark gray square becomes a larger black blob; a black square remains black. The gray shades were called “half-tones”, which explains the name of the process. Originally, the conversion was done by re-photographing the picture with a camera that contained a wire screen. then developing the picture in a high-contrast mode. Nowadays, the process can be accomplished on a computer.



If the density (squares per inch) of the scanned picture is not an exact multiple of the pixel density of the scanner, computer screen, or printer, an interference pattern occurs. They may also appear if the original photo is slightly rotated after scanning.

Colored pictures from publications may also give you interference patterns. For these, the halftone process uses filters to split the image into more than one black-gray-white photo, with each photo representing the intensities for each color. In each resulting halftone, the blob pattern is slightly offset from that of the other halftones. The picture is reproduced by printing the same paper once for each halftone, in the corresponding color. The printing press does not print one color on top of another because of the slight offset of the halftones.

You can get rid of the interference pattern by processing the picture with any photo software package that has a “blur” or “soften” selection. For example, in Paint Shop Pro, the IMAGE/SOFTEN menu selection spreads the black blobs so that the fuzzy bars magically disappear.

Vista Alternatives – Part II

By Brian K. Lewis, Ph.D., a 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.

This article is being written in the Linux version of Open Office 2.0 on a computer that uses Ubuntu as the operating system (OS). Since this system is now networked with my Windows XP computers, both desktop and laptop, I can easily transfer files between the computers. I am also able to print from this Linux computer to my laser printer over the Windows network. So what did I have to do to accomplish this?

The first thing I had to do was to install a copy of Samba on this Linux computer. Ubuntu has an Add/ Remove graphic interface for the Synaptic Package Manager. This has a one-click download install for new applications. The Samba package that was installed had a GsambaD graphic front end. This turned out to be very frustrating as it insisted I had to be logged in as Root to run the application. Now with most Linux versions this would be a simple change of user. Root is usually the designated Administrator and is the only user allowed to alter system files and add/remove software. There is also a user that has fewer privileges. (Sounds somewhat like Vista doesn't it?) However, in Ubuntu, the user is also the administrator. To carry out any functions that require administrator privilege, the OS asks for the password. The idea being that only one password is required for the user to remember. Anyway, the GsambaD software refused to acknowledge that I was the administrator and didn't ask for a password, it simply shut down after presenting me with the error message.

The next step was to manually edit the samba configuration file. I did have to do some searching through the Ubuntu on-line forum in order to find some help on the lines I needed to edit. It also required some facility with the command line mode (terminal) in Ubuntu. Obviously, if you are not comfortable making these types of changes, this OS is not for you. Until Ubuntu is able to install peripherals and local networking functions as easily as does Windows, it will not attract a truly large following.

So after making the configuration changes and re-booting the system, I went to the Places-Connect to Server menu. Immediately on clicking on that line, an icon was placed on the desktop and a window opened up showing the shared folders on my WinXP computer. I had no problem pulling up data files or PDF files and reading them. On my Windows computer I also found a new icon in the “My Network Places” folder. This was the icon for the Ubuntu computer. Here I was also able to read the folders and located data files that could be opened on the Windows computer. So the file sharing was successful.

My next complication was to setup a network printer. This had not worked in any of my previous attempts. Now that I was definitely connected to the Windows network I tried again. Going to System – Administration – Printing brought up a window with an Add Printer icon. This time by following the instructions in each window I was able to install my networked laser printer. When I indicated that I wanted install a networked printer there were a series of windows to go through. I had to change the designation from a CUPS printer to a Windows (SMB) printer. Then using the drop-down list I was able to select the name of the Windows computer. The next line also had a drop down list and I was able to select the name of the laser printer. The list did show both of the networked printers. The most difficult part of the printer install was locating the device driver file. First I had to select the manufacturer and the printer model. Then I was asked to locate the PPD driver file. I had to go back to the file management search function to find the folder where the driver files are located. Search is located at the bottom of the Places menu. The folder turned out to be at the end of this path: File system-usr - share – ppd. Yes, the folders in Linux have names that are not always straightforward. It takes some getting used to the differences. Once that was done, the last window asked for a description and a location. For the location I typed in the name of the Windows computer. Once back at the Add Printer window the laser printer icon appeared. Then I right-clicked, opened Properties and did a test print. The test print came through much

(Continued on page 9)

(Continued from page 8)

faster than it did when I had tried printing from Windows Vista. So at least I had one printer that I could use with the Ubuntu OS.

The next thing I wanted to test was using a dual boot setup. I had Windows Vista installed on this computer but the changes to the boot menu to allow a choice of booting Vista didn't work. So I tried another tactic. I installed the latest version of Linspire. After its installation I rebooted the system and ended up back in Ubuntu. So after using the Linspire CD to force the boot from the Linspire partition I printed out the Linspire loader file. Then I used that information to edit the Ubuntu loader. I added five lines of code that I had copied from the Linspire loader file. After saving the file I rebooted the computer and brought up the boot menu. Linspire was listed as the first application in the list. Pressing return selected this item and Linspire loaded. So now I had a dual boot system with Linspire and Ubuntu.

One of the first things I accomplished in Linspire was installing the network printer. Linspire automatically installed Samba so I didn't have that to do. In the graphic printer installation I was able to select a network printer as the type. Next I provided the network name; the server name and the application found my networked printers. After that it was simply a process of letting the installer find and install the printer driver and run a test print. I still don't have my inkjet connected to either Linspire or Ubuntu. That will be another project.

Finally, I checked on the networking ability of Linspire. It found my Windows XP computer with no problems. Then I had to figure out how to list the Windows folders I wanted to show in the Linspire file manager. Every time I tried to bring up the Windows “My Document” folder, it would appear to be empty. Since I knew that wasn't correct I went back into the Linspire Network Share Manager and tried to figure out the problem. When I would put in the folder name I would get a bad share name error. So then I made the entire Windows C drive shareable. That worked but I still couldn't get any files or folders listed under my user name. I tried using the Windows user name and password but that didn't work either. Finally I used the Admin user name and password and that worked! Now I can browse all of the folders and files in the Windows “My Documents” folder. The Linspire “My Documents” folder also shows in the “My Network Places” on the Windows computer. So, I can now move files and folders either direction on my local network. The final network setup was to connect my laptop to the wireless network and see if it was visible in Linspire. The laptop immediately found the Linspire computer and I was able to transfer a number of files with no difficulty. However, I did have to first provide the Administrator name and password.

After playing with Linspire for a time I went back to Ubuntu. Most Linux distributions don't come with any anti-virus software. Both Linspire and Ubuntu do include a built-in firewall. So I wanted to add an anti-virus. Since my Windows anti-virus of choice is Avast I checked their web page first. They do have a Linux version of their free home edition and it was a Debian package. Both Linspire and Ubuntu are Debian based versions of Linux. This, again, is one of my preferences as I find it easier to obtain and install software packages based on Debian. So I downloaded the Debian version of Avast. Clicking the install package Ubuntu brought up a menu asking if I wanted to install the package using “Gdebi Package Installer” and I clicked on OK. The installation took no time at all, but I couldn't find Avast on any of the menus. So I went to the Avast forum on the web and looked through some of the Linux questions. Not surprisingly there were a number of questions related to installation on Ubuntu systems. I found a command line entry fairly quickly. So I copied it and pasted it into a Terminal window. That put an Avast icon in the Applications – Accessories menu. The next problem was when I clicked the icon it immediately asked me for a license key. I had found a comment in the forum that you could use a Windows Avast key for the Linux installation. Since I had a license key that I obtained for Vista that I was no longer using, I typed it in, pressed Enter and Avast came up in the graphic interface. With one click I did an update on the virus database. Then with another I started a full system scan. So Avast is now protecting my Ubuntu installation.

There was another application that I wanted to install on the Linux systems. This is Picasa, a photo editing

(Continued on page 10)

(Continued from page 9)

and organizing application. It is produced by Google and is another example of quality freeware. I use it for downloads from my digital camera, for photo editing and for e-mailing photos. Picasa automatically compresses photos for e-mailing. For Linspire I was able to find Picasa in the Click-n-Run (CNR) warehouse. So that was a single click to have it downloaded and installed on the hard drive. In Ubuntu I had to go to the Picasa web site and find the download page and select a Debian version. Once it was downloaded I double-clicked it and Gdebi installed it just as had been the Avast. In both OS's I found that Picasa worked just as cleanly as it did under Windows. Incidently, both Linux OS's identified and installed my USB card reader as soon as I plugged it into a USB port. That will make downloading photos from my camera as easy as it is in Windows.

So why have I spent so much time playing with these Linux systems? It is mainly because I see them as viable competition for Windows. Granted there is a learning curve to getting these systems running on a computer. But that is true whenever you install any new software application. However I believe that Linspire and Ubuntu have come a long way toward meeting the needs of Windows users. There is a wide variety of software available for these Debian versions of Linux and the download-install functions have been quite simplified. In some respects adding software to either Linspire or Ubuntu is simpler that installing software under Windows. It is only in rare instances that you have to reboot your Linux system after installing a new application. The graphic interface of both of these Linux versions has improved to the point that most Windows users would have no difficulty in making the transition. The major problem is finding drivers for peripherals. I think this is a real stumbling block for some users who might like to change from Windows. Because of this problem I can't recommend either OS for novice users, only for those willing to do some web searching when they can't find drivers for their printers, scanners or other devices directly through the OS software.

I do have several remaining questions on my use of Linspire and Ubuntu. The first is solving my problem with a driver for my Canon printer, possibly replacing it. The second is seeing if some of my Windows software can be run on either system. There are several applications that allow Windows software to be run under a Linux OS. One is called WINE and the other is CrossOver Linux sold by CodeWeavers (www.codeweavers.com). WINE is a free application (winehq.org) and CrossOver Linux sells for either $39.95 or $69.95. So in the next few months I will continue my adventures with both Linspire and Ubuntu. You will see an occasional Linux article whenever I come across something that I think might be of interest to Windows users looking for alternatives. As for me, I intend to gradually transition all of my rk to Linux.

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.

Real Digital Forensics

Review by Jim DuWaldt, a member of the North Orange County Computer Club, California
www.noccc.org
editor(at)noccc.org
Obtained from APCUG with the author's permission for publication by APCUG member groups.

About the authors: Keith L. Jones leads the computer forensics and electronic evidence discovery practices at Red Cliff Consulting. Richard Bejtlich is the founder of TaoSecurity, a network security monitoring consultancy. Curtis W. Rose provides support to criminal investigations and civil litigation as an executive vice president at Red Cliff Consulting.

This book (with included DVD) intends to teach Computer Forensics for both Windows and Linux systems, that is, gathering evidence from infected machines and the network they operate in so that the intended victim can effectively react to a successful penetration.

Or, to quote the book: "...give new forensic investigators more than words to learn new skills." "We use the same

(Continued on page 11)

(Continued from page 10)

tools attackers use... the same methods rouge employees make... [collect] the same media we typically collect...this book takes a practical, hands-on approach to solving problems...[with] techniques you can employ immediately." The clear implication is that the book is aimed at the inexperienced practitioner. As usual, TCP/IP knowledge is a good idea. There is one staring oddity: to use one of the tools you need to alter your kernel! From pg 208: "Please download and install the NASA-enhanced kernel..." This takes more than just a beginner's skill!

The context for the procedures is provided by five scenarios which are a mix of internal and external threats as seen from the point of view of admins or law enforcement. As the techniques are presented, it is explained how they might be applied to these scenarios, as opposed to stepping through the scenarios and describing the methods.
Richard Bejtlich's books usually focus on evidence gathered by network monitoring. Instead, Part I ("Live Incidence Response") begins with host-focused procedures for both Windows and Linux (one chapter for each). Live Response techniques invoke a series of programs on the suspect machine in order to gather "volatile data," that is, system state that will not survive a reboot or shutdown. This explanation is entirely suitable for creating your own Live Response software and procedures.

Networks return to the center of attention in Part II ("Network-Based Forensics"). There is a brief but well-done review of the types of data (Full Context, Session, Statistical, and Alert Data) that should be collected and the software to collect them (Tcpdump, Snort, and many others) as well as the five steps of intrusion (recon, exploitation, reinforcement, consolidation, and "pillage"). A Cop/Drug Ring analogy is employed to describe these four data types which, given the popularity of CSI, might be good for rank beginners but will be less useful to anyone with more experienced. This section also has separate chapters on analysis of the information for Windows and *NIX machines.

Part III ("Acquiring a Forensic Duplication") presents open and closed tools for the forensic cloning of a suspect disk, regardless of the operating system. Its chapter on legal paperwork is very efficient but it would be great if the authors had photos or illustrations of what they use, if only as an example. The material on disk duplication, on the other hand, had lots of excellent photos and screen shots for both the commercial (EnCase and FTK) and open source products (DD, DD_resume, DCFLDD and NED).

Part IV (Forensic Analysis Techniques) shows you what to do with your new disk image. Methods for disk analysis begin with looking for and recovering deleted files, what to do when that is not possible, discerning strings of interest from NBE (Network-Based Evidence) and Live Response findings (like the name of an executable) and searching the disk for them.

This is followed by techniques for reconstructing emails (even Outlook and Outlook Express proprietary formats can be analyzed by open source tools), pages visited while web browsing including reconstructing emails sent with web clients, and the examination of the Windows Registry (good for finding recently-accessed documents or evidence of programs subsequently deleted).

(Currently only commercial applications are available for analyzing the Registry which is odd, considering that scripting languages, like Python for example, have Registry access libraries.)

Multiple chapters focus on examining unknown files to determine their use, with an emphasis on Microsoft-formatted documents and on the examination of unknown Windows and *NIX executables. This includes static analysis with tools like strings.exe and hexWorkshop and disassemblers like IDA to discover system calls or modify a binary file in order to, for example, bypass password security. Missing are instructions on using a product like VMware to set up a virtual machine environment for protecting the rest of the system from the foreign executable; they only mention that you *should* use something like VMware when in fact it is vitally important to do so or you could wind up with yet another infected computer!

Part V ("Creating a Complete Forensic Toolkit") succinctly describes creating CDs for a Live Response toolkit. (But, why not do this in the first part of the book?) It also describes the use of a Knoppix disk which allows you to examine a suspect system without having to boot it from its (possibly) contaminated disk or be concerned about your 'clean' OS being cleverly contaminated by a suspect hard drive.

Part VI ("Mobile Device Forensics") describes gleaning and examining data from PDAs like Palms and iPaqs (with additional information about how they manage memory and how to access internal debugging consoles), USB and CF drives. Forensic examination of USB/CF devices using a loopback is well illustrated and an example of recovering a

(Continued on page 12)

(Continued from page 11)
deleted file is shown. The chapters also illustrate that, while some PDAs have good forensic tools available (like later Palms and iPaqs), the earlier ones do not: sifting through evidence on a Palm III, for example, is limited to hex and string searches.

Part VII ("Online-Based Forensics") presents methods for determining where an email originated from via header examination, and how determined users could cover their tracks. Finally, they leverage searching for DNS records into a lesson on manipulating the entire VeriSign TLD (Top Level Domain) file in a large (100GB+) Postgres database, allowing them to find all DNS names owned by, in their example, the company Foundstone.

My only complaints about the book are the sudden request to change the kernel and a failure to put front and center the necessity of using a virtual machine environment before executing potentially hazardous code.

Otherwise it was a typical Bejtlich security book (no offense to the other authors), containing the basis for immediately creating Standard Operating Procedures, in particular for Live Response, proper forensic documentation, and creating forensic-compliant duplicate drives. It definitely has a place on my security bookshelf, alongside The Tao of Network Security and Extrusion Detection.

The book is published by Addison-Wesley (http://www.awprofessional.com/bookstore/product.asp?isbn=0321240693&rl=1), ISBN 0-321-24069-3, and lists for $55. User group members can get a 30% discount if their group belongs to the UG program.; it sells for $34.64 at Amazon.com (new).

(Continued from page 6)
(Linux), which is Open Source. Anyone can download the kernel source code and study how it works, and Linux has far better security than Windows for just that reason. Everybody knows how it works; they also know just how to prevent intrusion.

So, compatibility for lots of applications has been slow coming. The Big Kahuna application vendor, Adobe, is an example. While CS2 installs and runs on Vista, they have released about 300 MB worth of patches to address "compatibility issues" in Vista. These range from visual anomalies to outright crashes. If reliability is foremost, you may be stuck in Windows XP for several months. Don't give up that dual-boot configuration just yet. . .

ReadyBoost is a new feature of Vista that lets you use a USB flash drive as part of system memory, improving what Microsoft characterizes as "system responsiveness". It serves as storage for the system cache that gets paged to the hard drive in a low RAM machine. Computers with less than 1 GB of RAM benefit most from ReadyBoost; Vista moves a lot of the system cache to the flash drive, where it is accessed much faster than if it were paged to the hard drive.

I tested ReadyBoost by reducing the RAM on my Vista machine to 512 MB and running Vista over several sessions to get a feel of the system's responsiveness, then adding a SanDisk Cruzer 2 GB ReadyBoost-capable flash drive to see the difference. Leaving the flash drive in the computer during startup actually lengthened boot times. (Same thing happens if you add RAM: Windows simply spends more time filling the added RAM with more system components.) The speed difference shows up while you are running applications. Vista caches system and application pieces in memory, but lacking memory, it will simply page these off to the hard drive, which is the slowest component in the computer. When it can page these pieces to the flash drive instead, system response improves markedly. If you do something like load Adobe Photoshop, Adobe InDesign, and CorelDRAW, and switch between the applications, there is a definite improvement in system response. Crude stopwatch testing on my part suggest 25% - 50% improvements whenever Vista works the cache. Even Flight Simulator X was faster, with less delay between scenery changes while in flight. Noted from other sources, performance improvements are best in machines with the RAM configured single-channel and barely noticeable in machines that have paired modules running in dual-channel mode.

Note that the flash drive must be ReadyBoost capable. It must meet minimum speed tests before Vista will use it. Every other flash drive I own fails this test. When you go to the store, make sure the package says the flash drive is ReadyBoost capable. A side benefit of ReadyBoost is that if you don't want the flash drive for ReadyBoost, you can get an ordinary 2 GB drive for as low as $14.

So, this month, I found out how much faster I can't run my incompatible applications using ReadyBoost in Vista; the Microsoft version of Catch-22. Stay tuned for more misadventures.