



I have been doing a lot of reading about brain fitness recently. Our brain is like our muscles – if we don't use it we'll lose it. Using means learning something new or doing logic puzzles like Sudoku. I think our computers also help us out. At least I'm often wondering how to do something or trying to figure why unexpected results happened. Installing and learning new software is definitely a brain stretching exercise. Pinnacle has some great new video editing software – Studio 12 – that has easy to learn and use basics with enough depth to keep your projects and mind fresh for quite a while.

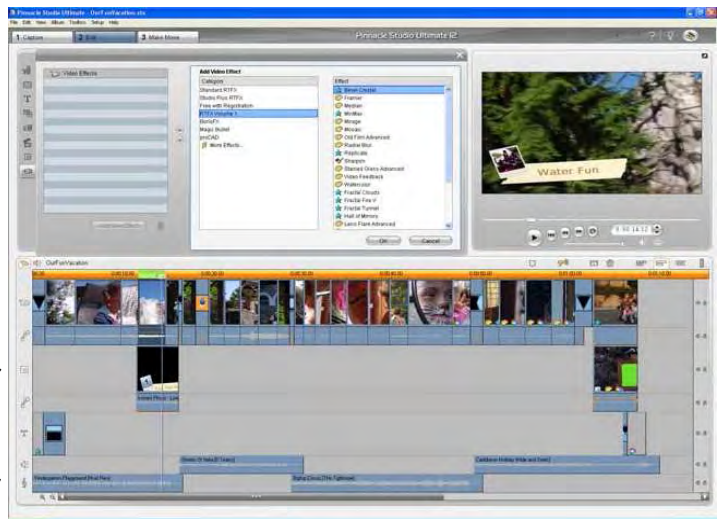


Pinnacle is a big supporter of computer user groups. I first became acquainted with their products by attending user group conferences where Pinnacle sponsored meals and had speakers give presentations. They also took part in the vendor fairs. I was impressed with how fast and easy their products worked. With a little research I discovered that Pinnacle's software is made by AVID – the standard editing system for films and television. Many of Studio 12's features really are things the "big boys" use.

You can mix video from many sources and even use still picture as pictures or add some movement to make them seem more like video. Everything is drag and drop. The hardest part is deciding which features to use – especially the transitions. It is even easy to tell where you are editing – that area of the timeline will



have a green highlight. Your finished movie can



easily include many features that the "big boys" use. Your choices are huge and the special effects are awesome. You can import and use your favorite music, or use "Scorefitter" to generate original background music for you – just like the "big boys". All you have to do is pick the mood you want. When you are through editing your newly made movie there are lots of output options – including just audio and uploading to YouTube and Yahoo Video.

With such a wide range of mind blowing features you would expect a high price, but Studio 12 is also amazingly affordable. The standard version is \$50, while Studio 12 Ultimate, with ALL its bells and whistles, is just \$130.

To learn more, come to our next meeting on Saturday, September 13th at 10:30 am in Sonoma Valley Library's De Long room.



Windows XP Expires

By Sandy Berger, CompuKISS
sandy(at)compukiss.com

www.compukiss.com

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

On June 30th, 2008, Microsoft started the death march for Windows XP. As of that date, Microsoft stopped shipments of Windows XP as a stand-alone shrink-wrapped product. So after supplies are exhausted, you won't be able to go into a store and purchase Windows XP. Microsoft also stopped most sales to PC manufacturers. So Dell, Lenovo, HP and others will not get any new copies of Windows XP to install on their mainstream computers. However, Windows XP, Microsoft's longest-lived and best-loved operating system, isn't going to vanish overnight. You will still see copies of the XP software and/or computers with Windows XP in stores until inventories and depleted.

Microsoft has made four important concessions that will also keep XP alive:

1. Microsoft will support Windows XP until April 2014. They will offer updates, security patches, and technical support until that time.
2. Smaller local PC makers can continue to sell PCs with Windows XP until January 2009.
3. Computers with limited hardware capabilities which are sometimes called ultra-low cost PCs (ULCPC) can sell with Windows XP Home until June 2010.
4. With the purchase of Windows Vista Business or Windows Vista Ultimate, the two most expensive versions of Vista, a customer will be able to move back to Windows XP Professional via what Microsoft is calling "downgrade rights." Details on how this will be handled have not been clearly defined to the public at this time. It is even possible that different manufacturers will handle this in different ways.

To the home users, this all means very little, unless you need a new computer and are violently opposed to Windows Vista. To business users, these new policies and extensions mean that they will be able to keep their fleets of Windows XP computers running for several more years. Microsoft has announced that Windows 7, the next version of Windows, will be available in 2010 so many businesses will be able to skip Vista entirely [moving] instead to Windows 7. Intel has al-

ready announced that they will do just that.

What this means for everyone is that Microsoft, while not writing off Vista, has made it an "interim" operating system. Microsoft is still pushing Windows Vista. They recently announced that Vista now supports 77,000 printers, cameras, speakers and other devices and components. They also brag that more than 140 million copies of Windows Vista have already been sold, making it the fastest selling operating system in Microsoft history. So Windows Vista is not a flash-in-the-pan like Windows ME which was quickly replaced by Windows XP.

In my opinion, Vista is both better and safer than Windows XP and if you are already using Vista or plan to make the move, it is not a bad choice. Yet Vista has become a lame duck. Microsoft definitely has a dilemma on their hands. The only way they will come out of this is if they can get Windows 7 out quickly while making it faster, safer, and easier to use. They also need to give it a good name and get the members of the press behind it. I'm not sure if the lumbering giant can pull that off – especially if Apple and/or Linux find a way to take advantage of this Microsoft predicament!

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Smart Computing Tip Of The Day

Put On Your Editor's Hat

Even the most captivating video footage can benefit from a little ruthless editing. Use your favorite video editing program to weed out the less-interesting bits. You can help your kids rearrange scenes to create a better story and add titles, audio, music, and special effects. Keep in mind that special effects, including transitions, can be as overused as they can be effective. Focus on content, not flash. While you're in the video editing program, capture a collection of interesting still images and save them for later. You can take the stills from several movies and turn them into a slide show based on a common theme, such as birthdays, holidays, or home-improvement projects.

The New, the Best AND, the Worst

Collected BY Pim Borman, Webmaster
SW Indiana PC Users Group
<http://swipcug.apcug.org>

[swipcug\(at\)gmail.com](mailto:swipcug(at)gmail.com)

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

Picasa web album

In June I took a brief vacation with son mike and cocker spaniel bonnie, touring scenic central West Virginia. We visited the stark rock outcropping known as Seneca rocks, admired the amazing 110-meter steerable radio telescope at the green bank national radio astronomy observatory, and found carnivorous plants in their natural habitat in the cranberry glades botanic area. Together we took over 400 pictures along the way that we culled down to 60-some upon our return. It is often said that the secret of great photographers is that they take hundreds of pictures but save only the one or two best ones. Nobody ever mentions how hard it is to pick out those few winners!

I decided to try and upload the best pictures to one of the online free photo albums. I was already somewhat familiar with Flick'r, but I decided to try the Google-Picasa web album instead. Picasa is an excellent simple photo editor and it gives direct access to the online web album. The album allows 1gb of storage, enough for some 4000 pictures, and you can get even more than that for a small fee.

Since I already had a Google email account, setting up the web album was easy, using the same user name and password. On the web site you can set up separate albums (folders, really) to store pictures in separate categories. I created a new album for my vacation pictures and prepared to upload them. After some trial and error I found it easiest to first assemble the captioned pictures in a Picasa album on my pc and then to upload them all at once to the web album. Once the pictures are uploaded you can add more or delete mistakes, move them around into the desired order, and add or change captions. By default, the photos are automatically converted to the optimum size for display on a computer screen, but there are options for larger (up to 20mb) or smaller file sizes.

Once the album has been installed it is ready to be shared with the rest of the world. You may choose to make your photos public, available to anyone, or keep them private, only accessible to

those you share the URL with. The view album page shows large thumbnails of the photos. They can be viewed individually or as a slide show. The view map button brings up Google maps where you can indicate where you took your pictures. The Organize and Edit captions buttons are self-explanatory. A new features link at the top of the page leads to the latest features added. It is now also possible to upload videos from Picasa to your web album. That might be preferable to using YouTube, unless you want the whole world to admire your movie.

The web album displays the URL of your album site either as the address itself or as a short paragraph of html code that you can insert on your web site. Either way, it is best to copy and paste the information since the URL tends to be lengthy and confusing. My vacation pictures are located at [http://picasaweb.google.com/swipcug/westvirginiavacationjune2008?](http://picasaweb.google.com/swipcug/westvirginiavacationjune2008?Authkey=kovcoyrboay)
[Authkey=kovcoyrboay](http://picasaweb.google.com/swipcug/westvirginiavacationjune2008?Authkey=kovcoyrboay).

To do your correspondents a favor you should convert the URL with SNIPURL (<http://snipurl.com>) or TINYURL (<http://tinyurl.com>) to a simpler address, such as <http://snipurl.com/pimpspix>. If you have never done that before, you'll find it easy to do. Just go to <http://snipurl.com> (or the TINYURL site) and paste the URL of your album in the box. Specify an easy-to-remember nickname (such as "Pimpspix," but only available in SNIPURL) and "snip it!" the shortened URL (<http://snipurl.com/pimpspix>) will be shown and also copied to your clipboard, ready to be pasted in your message.

Gathering CLOUDS

My experience with setting up a photo album "somewhere up there" is a typical example of the current trend towards "cloud" computing. Almost since the beginning of the world wide web we have been using online search engines that access indexed information stored "somewhere up there." many of us have changed from our pc-based email programs to online programs, such as Yahoo or Google Mail, that store our email correspondence on computers "somewhere up there." somewhere up there in the clouds, as it were.

The push is now to extend cloud computing to of-

office suites. Instead of using expensive ms office we can choose to use Google docs and conduct all our administrative activities online, with the option of sharing our work with colleagues far away if necessary. Microsoft, always ready to recognize good ideas after others first thought of them, is moving versions of its office suite online under the "live" banner. Others are jostling to join the crowd.

If this trend continues and spreads to other computer activities, our operating systems, whether windows, Mac, or Linux, will become less and less important. The functions of the operating system will be taken over by browsers. To those of us using multiple operating systems, such as windows and Linux, we already find that it makes no difference if we use Firefox in windows or Linux. Similarly, Picasa is Picasa and my new web album is the same no matter how i access it.

So far, that all sounds good. But gathering clouds threaten to bring rain. If everybody is going to use the Internet almost all the time, the current Internet infrastructure will not be able to keep up. There will be a need for millions of additional servers and drastically increased connection speeds.

The computer industry is aware of that. Accord-

ing to the Economist (May 24, 2008) Microsoft is building a new \$500 million data center near Chicago. It will require 3 electrical substations with a total capacity of almost 200 megawatts. Google is said to have 3 dozen data centers with an estimated million individual servers. More and more these extensive data centers are being built in out-of-the-way places near sources of low-cost power, even in Iceland with cheap geothermal power. With all this power consumption computers are becoming a major source of global warming.

To increase transmission speeds the industry is eyeing the airwave bands that will be freed up in February 2009 when analog TV will be phased out. There are so-called white spaces between the frequency bands assigned to TV broadcasts, and tech companies want to use those buffer zones for lightning-fast data transmissions. Initial tests show that it might wipe out nearby HDTV broadcasts, but they keep working at it. (Scientific American, June 2008)

The computer revolution has just begun!

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Security and Deleting Files: A Common Misconception

By Bob Schwartz, a member of HAL-PC, Texas,
bobx(at)hal-pc.org www.hal-pc.org

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

You have just deleted a file from your hard drive. It's gone, isn't it? Sorry! It is still there. You want to clean up your hard drive, so you format it. It is now clean. Nothing is on it anymore, right? Nope! Everything is still there, except for the file directory.

How can this be? Doesn't Delete mean remove? Doesn't Format clean the disk? Each file system - has a file directory which records the file name and it's location.

To delete a file, the disk system only alters the file's name in the file directory, usually by changing the first letter of the name. Formatting goes one step further, it just empties the file directory. Neither does anything to the files on the disk! They remain.

To clean a drive, either overwrite the whole drive or the unused space. The most common way to

clean drives, especially older drives, is to write fixed or random data obliterate the old files.

Fortunately, all ATA drives over 15-20 GB produced since 2001 have an internal drive command that will clean the drive sufficiently that it will meet DOD requirements. At the University of California at San Diego's Center for Magnetic Recording Research (CMRR) you can download their free program for Secure Erase, entitled "HDDerase.exe". Its use meets U.S. Government requirements for disk erasure. Secure Erase should provide the greatest peace of mind. Internet Commentary suggests it is even better than mechanically shredding the disks.

If you have a good machine with good software that you would like to pass on to some else, and you don't have all the original disks - remove personal information. I suggest this approach:

1. "Delete" the contents of: all the "My" fold-

ers - My Documents, My Pictures, My Music; Recent; Temp or Temporary folders; Recycle Bin; Cookies; Downloads; and the entire folders for Quicken and Tax preparation software.

2. Clean your Registry of all personal data. For XP, go to Start/Run, type regedit and press Enter. Go to edit and click on find. Enter your last name, click on find next. When the first entry is found, go to edit and select modify. Delete your name (it should be in color). Depressing the space bar may clear it. Go back to edit and click on find next, etc. Keep on until you get a message that you have reached the end. Then repeat the above with your first name, then your street, your phone number, bank name, broker name, and anything else of a personal nature that you used.
3. Find and download a registry cleaner. Use it to remove unnecessary items from the registry. Ccleaner is an example.
4. Defragment the drive. This condenses the files and moves them toward the beginning of the drive.
5. Locate and download a wipe application such as bcwipe. Use it to wipe (overwrite) all unused space.

IMPORTANT NOTE: Before editing your "registry", back it up first, please.

This should effectively sanitize your disk, leaving it clean, safe and usable.

Loss of personal information and the risk of identity theft is a risk for you. For a business, the loss of personal, financial, or medical data may subject it to risk from recent laws, both federal and state.

I have been repairing or rehabilitating older machines as a hobby to give them a second life. There are many good machines and plenty of worthy recipients. If there is good software worth keeping, remove all personal data. If the software is not worth keeping, then wipe the disk clean to install an operating system and applications.

Removing the hard drive before you dispose of an old machine is not a solution, unless you plan to use it in your new machine, or store it permanently - you still ultimately have to sanitize it.

Programs available, free or fee, include: Secure

Erase (mentioned above), Secure Delete, Wipe Drive, Acronis Privacy Expert, East-Tec Eraser, East-Tec Dispose Secure, Eraser, SysInternals SDelete, Darik's Boot and Nuke (dban), OverWrite, Wipe, Kill Disk, BCWipe, and Autoclave. This list is NOT exhaustive. And, you have to determine which is suitable to (1) wipe the entire drive or (2) wipe only the unused space.

Bottom line is, when you give away or dispose of a used computer, either clean the hard drive yourself or give the machine to someone you can trust who will do it for you. The comments and opinions here are wholly mine. I welcome alternative perspectives.

Bob Schwartz is a HAL-PC member, retired EE, 14 patents, technical writer, active in civic affairs: President, Brays Bayou Association; Vice President, Marilyn Estates Civic Association; Correspondence Secretary with the Willow Waterhole Greenspace Conservancy.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Smart Computing Tip Of The Day

Screen Savers

Over the years, you may have received email messages warning of viruses that lurked inside popular screen savers. Such warnings are, in some cases, hoaxes. Nevertheless, you should treat all screen savers as if they actually were contaminated with viruses, spyware, or adware. A screen saver is an executable file and, as such, has the potential to carry dirty code into your system.

You should take the opportunity to scan any screen saver file you download for viruses and spyware before loading it into your system. When you're satisfied that a file is safe for installation on your PC, you can install it in one of two ways. If the screen saver bears an .EXE file extension, double-click the file and follow the on-screen installation instructions. If the file has an .SCR extension, however, then simply move it to the WINDOWS\SYSTEM32 (in WinXP) or WINDOWS\SYSTEM (in Win98/Me) folder and select it as your screen saver in the Display Properties dialog box. (You can access Display Properties in any version of Windows by right-clicking your Desktop and selecting Properties from the pop-up menu.)

Rootkits - A continuing Security Problem

by Brian K. Lewis, Ph.D., Member of the Sarasota Personal Computer Users Group, Inc., Florida
bwsail at yahoo.com www.spcug.

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

By now I suspect everyone reading this article is familiar with most malware: viruses, botnets, Trojans, etc. These are becoming less of a problem because of the efforts of the security companies to provide software solutions. More and more users are also becoming aware of the need to have some means of protecting their computer. As a result, hackers are turning to a more effective method of controlling your computer – rootkits. Although these have been around more than ten years, like other malware, their numbers seem to be increasing.

Probably the most dangerous form of the rootkit is the "kernel mode Trojan". This is a program that inserts itself into the "kernel" of the operating system. The kernel is the central component of the operating system – its heart or brain to put it in more common terms. It manages the communication between the operating system, the hardware and the software applications.

Most viruses operate as applications and can be readily found in memory or in the file system. Rootkits, however, can hide themselves in such a way that it is very difficult to find them. In order for a rootkit to alter the normal execution path of the operating system, one of the techniques it may employ is "hooking". In modern operating systems, there are many places to hook because the system was designed to be flexible, extendable, and backward compatible. For example, a rootkit can "hook" itself into the Application Programming Interface (API) which allows it to intercept the system calls that other programs use to perform basic functions, like accessing files on the computer's hard drive. If an application tries to list the contents of a directory containing one of the root kit's files, the rootkit will censor its filename from the list. It'll do the same thing with the system registry and the list of running processes.

A rootkit is a collection of tools an intruder brings along to a victim computer after gaining initial access. A rootkit may contain network sniffers, log-cleaning scripts, key-loggers and trojaned replacements of core system utilities. Although the intruders still need to break into a victim system before they can install their rootkits, the ease-of-use and

the amount of destruction they cause make rootkits a considerable threat. One main purpose of a rootkit is to allow the intruder to come back to the compromised system later and access it without being detected. A rootkit makes this very easy by installing a remote-access backdoor. A rootkit can also allow the intruder to use the compromised computer as part of a botnet (see Botnets, SPCUG Monitor, January, 2008).

Another mechanism for hiding a rootkit is to add it to a system driver file. Windows XP and Vista store driver files in the System32/drivers folder. Many of these system files load early in the boot process. These files have boot or system flags in the registry and load before any of the malware-prevention software. That means they are very difficult to find. Although the file size for the driver will be increased, the rootkit may report the original file size to any query, not the infected file size. All of this means that once a rootkit has been installed and activated on your computer, it is difficult to find by any of the usual malware prevention software.

Rootkits do not require large software applications to carry out their function. We are accustomed to commercial applications that are many megabytes in size. Even the anti-virus software may be 40-50 megabytes in size. In 2003 a rootkit was identified that required only 7 kilobytes for its cloaking routine and 27 kilobytes for maintaining the open backdoor.

Anti-malware programs depend on two main means of identifying malware. One is the signature method and the other is heuristics. The signature method requires that the malware be identified and reverse engineered to determine a code sequence which can be used to identify the application in the wild. This code sequence is referred to as the signature and is used by the anti-virus database. This signature is then compared to code sequences in applications to determine if they are malware. This method is of no value when dealing with new or unreported malware.

So the next option is heuristic signatures. Their primary advantage lies in their ability to identify new, previously unidentified malware. The heuristics technique assumes that malware will display

certain characteristics or attributes. They also attempt to recognize deviations in "normal" system patterns or behaviors. Using these predicted patterns, the anti-malware application will attempt to determine if the target application is malware. This has been a successful approach for identifying viruses, but it is less successful for active rootkits.

The April 2008 Virus Bulletin (www.virusbtn.com) reported the results of testing a number of popular commercial A-V programs, Internet security suites, web-based scanners and specialized anti-rootkit tools. The testing involved 30 known rootkits. The testing categories were detection of: (1) inactive rootkits; (2) active rootkits; and (3) malware hidden by rootkits. Then they tested removal of (1) inactive rootkits; (2) malware hidden by rootkits; and (3) active rootkits. The results were not encouraging.

The seven Internet Security Suites used in the test were able to detect 95% of the inactive rootkits. (Remember, these were known samples that had already been identified and their signatures incorporated into the anti-malware applications.) These suites were also able to remove 95% of the inactive rootkits. However, when it came to active rootkits the story was very different. The Internet Security Suites detected only 65% of the active rootkits and were able to remove only 48%. They also were able to remove only 48% of the hidden malware. All of the versions of the Internet Security Suites were the latest available at the time of the test.

There were fourteen specialized anti-rootkit tools tested using the same thirty rootkits. They were not tested against the inactive rootkits, only the active rootkits and the hidden malware. Again, the results were anything but satisfying. These tools detected 83% of the active rootkits and 80% of the hidden malware. The anti-rootkit tools removed only 60% of the active rootkits and 67% of the hidden malware.

The web-based scanners did a far poorer job of identification of the rootkits. They also were uniformly unsuccessful in removing rootkits. The detection rate was 53% and the removal was around 32%.

In reviewing these tests it is obvious that successful detection and removal of rootkits depends on their being inactivated. This can be done by running the computer in "SAFE" mode which does not allow the rootkit to load from the hard drive.

However, it would be expected that if detection/removal tools were developed for this specific purpose, then rootkits would appear that would load in "SAFE" mode. Another alternative would be to develop rootkit scanning software that would run from a CD. The computer would boot from the CD and the operating system for the scan would load from the CD. This should improve the detection and removal rates considerably. However, it then depends on the user running the CD application periodically to scan the entire computer. Considering how few users backup their hard drives on a regular basis, this CD system might be less than universally successful.

Given the current difficulty of detecting and removing rootkits from your computer, what is a user to do for protection? The only answer to this is to prevent the rootkit from getting access to your computer. That means using every tool you have available to prevent the malware from gaining access to your system. Your firewall is the first line of defense, followed by your anti-virus, then your anti-spyware. Also, when you are surfing the web, make sure you aren't your own worst enemy. Be careful and check out links before you click on them. It just like getting spam in your e-mail. Check where the link will take you before you click on it. Social engineering techniques are also used to propagate everything from viruses to rootkits. These are techniques that encourage the user to take some action which allows the malware to be downloaded and installed on the users computer. A very interesting analysis on these techniques is contained in this article from the University of Cambridge (U.K.); <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-666.pdf>. Although this is written specifically about virus propagation, similar techniques are used to gain entry for rootkits. This paper illustrates many of the "carrot & stick" methods used by malware to gain access to computer systems. Microsoft has also published a paper detailing many of the common methods used to trick users into installing malware. These can be found in the paper "Behavioral Modeling of Social Engineering-Based Malicious Software" on the Microsoft web site.

So to all of you reading this paper, I would suggest that "caution is the watchword" when it comes to using your computer. I'm afraid that the situation will only get worse when it comes to new forms of malware.

Update Note: In my article on iFrame attacks

(SPCUG Monitor, May 2008), I listed a number of portals that had been affected by iFrame attacks. One of these was the eHawaii.gov portal. I have received information from the site manager that the problem has been corrected (removal of the iFrame) and actually only affected one page on their site. Thanks to Russell Castagnaro for correcting this problem and notifying me.

Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years, developing software and assembling systems.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Window Pains – Task Manager

By Bob Balogh, President, Boca Raton Computer Society, Florida
helpbrcs(at)yahoo.com www.brsc.org



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

TASK MANAGER

Task Manager is a helpful application that is part of the Windows Operating System (2000, XP & Vista). You can open it with the three fingered salute – Ctrl/Alt/Delete, or more easily, my preferred way, by a right click on an open space on your Taskbar, and clicking on Task Manager. You may also open Task Manager by going to Start-Run and entering "taskmgr" (without the quotes).

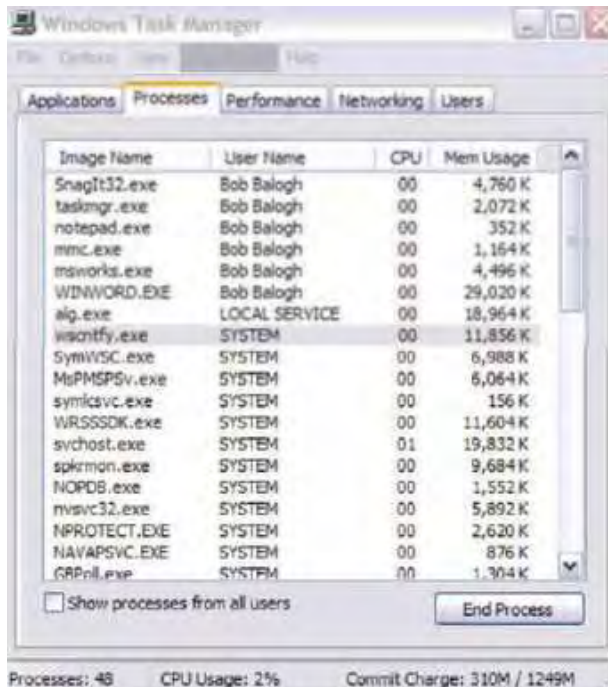
Most of us have only experienced dealing with the Task Manager when a program no longer seems to be functioning. We then open the Task Manager and click on the Applications Tab, see the list of running programs, and highlight the program we are having difficulty with, then click on "End Task" at the bottom of the page. Voila, the program is shutdown and is no longer causing you a problem. Of course, you still will want to find out why the problem began or why the program froze in the first place. However, that is for another time.

PROCESSES

You can also click on the "Processes" tab, to see exactly which programs are running in the background.

Of course all these programs do not have to run. In fact while many of these programs are useful and are needed others are not needed and may at times cause problems. The problem is what determining what these programs do. Even if you are not inclined to stop any of these programs it is a step forward to know what these programs do so at least you have an idea as to what may be causing a particular problem when it arises.

To see a list of most of the possible programs



Go on open yours up and see what is running.

that are running in the background just go to this web site http://www.answersthatwork.com/Tasklist_pages/tasklist.htm and peruse the programs from A-Z. Well, you don't have to look at all of them, just the ones you have listed in your Task Manager.

Remember, all the programs, that are listed in your Task Manager, may not be listed at "Answers that Work". Why you might ask? Well, just look at my list and you will see a program listed called Snagit32.exe. That is a program that I added to my computer, and use often.

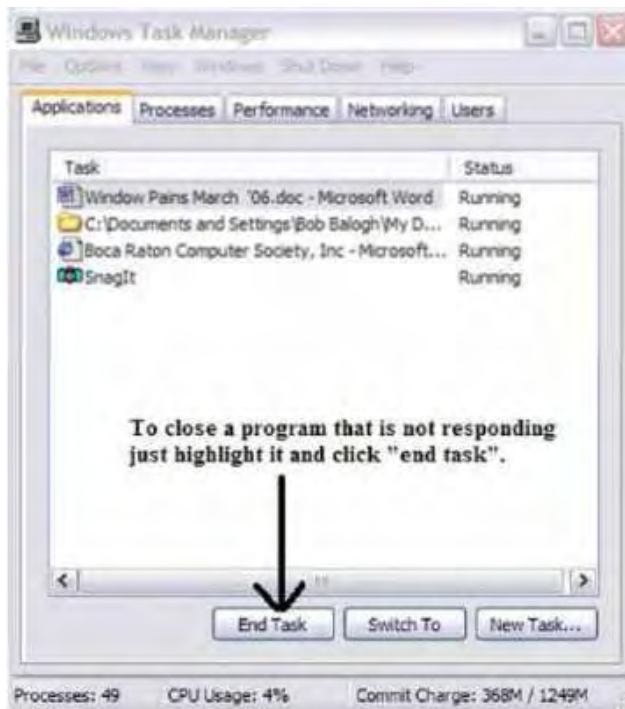
Actually, it is the program I used to create the picture of the Task Manager above. So it is listed,

since it was still “running”, when I made the screen capture. Could I turn it off? Sure, all I have to do is close the program.

If you want to turn off a program that is running in Task Manager, don't change, or disable it in the Windows Task Manager. Instead, go to the Control Panel | Administrative Tools | Services, and change them there.

Double click on the entry, and change it from the dropdown list where it says "Startup Type". Carefully read what it does, and what it is related to, before making a decision. Write down what you changed, in the event you wish to change it back.

If you have System Restore or Go Back operating, write down the date and time, in case you want to return to an earlier time, when all was well. Additionally, set a new restore point, prior to doing anything. If the service isn't listed in there, then more than likely it was added by an application you added after the install. You'll need to decide if it's necessary, or if you only want it running when you decide. There also comes a time when a particular program “freezes” and is not functioning as we mentioned at the outset of the article. What should you do? Simply use Ctrl+Alt+Delete, open the Task Manager, and simply close down the program by selecting it and clicking on “End Task”. The following figure demonstrates it for you:



Smart Computing Tip Of The Day

Use the Magnifier Utility in Windows XP

Microsoft offers a number of accessibility-oriented tools, including a screen magnifier. This utility displays an enlarged version of part of your screen in a user-customizable viewing area. The Magnifier tool features several options:

- *Magnification level. From 1 (no magnification), to 2 (allowing about 10 words across the top of the page), to 9 (about three words, highly pixelized).
- *Follow mouse cursor. Self-explanatory. Works in all programs.
- *Follow keyboard focus. Follows along as you type. Moving the input point using the arrow keys does not move the focus. Works only in WordPad and Notepad.
- *Follow text editing. Follows the input point as you move it around a block of text.
- *Invert colors. May make text or images stand out better.
- *Start minimized.
- *Show Magnifier. Toggles it on and off.

You can click the edges of the Magnifier window to enlarge or reduce it, move it around your screen, or drag it to an edge of your screen to dock it.

The Performance tab displays an overview of your computer's performance, including graphs for CPU and memory usage as well as the total number of processes running. Google such other items displayed if you are interested in the purpose they serve. I do not wish to get too technical here.

The remaining tabs, Networking and Users are basically self explanatory. If you are running a home network it will show up under Networking and inform you of it function ability. As far as Users is concerned you will see a list of those using your computer.

Peruse the headings in the toolbar (top), just to get an idea of what they are and do. Of course the Help tab, as usual, is the most important in explaining the program at hand. Use it and you will learn much

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Prepare for Hard Drive Recovery

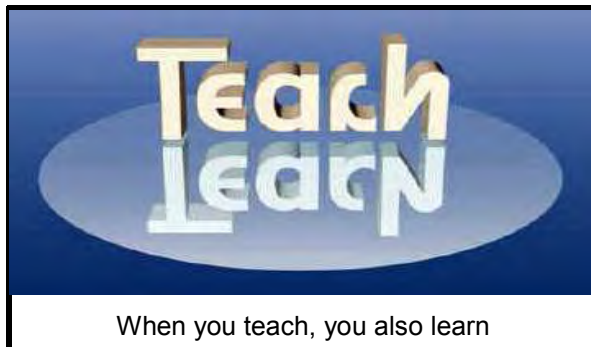
by Bob Hudak, Greater South Bay User Group Hardware SIG Leader (California)
uags(at)aol.com

<http://gsbug.apcug.org>

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

When you lose control of your computer due to a virus or some sort of malware, or your O.S. becomes corrupted for one reason or another, be ready to fix the problem.

1. Start by setting up your hard drive with 2 partitions at least. Put all programs on 'C:' & all Data on 'D:'
2. When hard drive is clean and all programs are loaded, it is time to make an image file of 'C:.' Use Acronis *True Image* to do this or whatever program you like. Put it on 'D:' drive in the root. Name it using date. Remember you do not have a backup till you have two copies in two different places. So now copy this image file to an external USB drive. The reason is if "C:" goes bad you can reformat it and start over without losing any data. If your computer will not boot and you did not put all your data on another drive or partition, you will want to save your data before reinstalling your operating system. What can you do?
 - A. Open computer case and remove drive. Install drive as a slave drive in another computer. Now you can copy and paste your data or burn to a CD. This means opening two computers and moving the drive in and out and resetting the jumpers.
 - B. Hook up the drive you removed from your computer to a second computer using a USB adapter, like the one we have at the Hardware SIG, to another computer and copy and paste or burn the data you want to keep.
 - C. Here is my first choice in a case like this.



Use a Live Linux CD to boot up. Plug in a USB drive before booting. After booting, mount your 'C:' drive and your USB drive. Copy your data from 'C:' drive to the USB drive. With this option there is no case to open and drive to remove.

3. Backup your data as necessary to a CD or another drive. Use a USB drive. This drive can also fail so putting backup on a CD or DVD is better way to go. Also, there is an on-line service at Carbinite.com that will automatically back up your data. This service costs \$50.00 a year for unlimited backups. How important is your data?

Here are a few key folders to have on 'D:.' drive:

Data — In this folder make sub folders for each application you use. Include one called Pictures. Under this folder have another sub folders for different events. Like: Christmas07, Vacation08, Dog, etc.

D/L — Use this folder for all your downloads. Then you will always know where your downloads are. Set it up so the last thing you downloaded is on top.

E-Mail. If possible. You wanted your e-mail off the 'C' drive

My Stuff. Cut and paste from 'My Documents' on 'C' items that were sent there without asking you where to send. Documents that you want to keep.

Using Acronis *True Image*

Use Acronis *True Image* to backup to your USB drive. Make a full backup the first time.

This is going to be pretty easy because all your data is in one folder on 'D:.' called **DATA**. If you want to backup your downloaded items, back up the 'D/L' folder. E-Mail is not something I backup but you may want to. Once again it should all be in the 'E-MAIL' folder.

You already loaded the Acronis program and made a rescue CD that is bootable. Right?

Now open your CD drive and insert the CD. Do

not close the drive. Shut down your computer. Close the CD drive. Wait a minute and then re-boot.

If you have your BIOS set to boot from a CD first, you are good to go. If not you will need to enter into your setup screen at boot-up and change the boot order.

After booting up with Acronis, follow the prompts to select what you want backed up. Practice this before you need to use it.

Make notes on how to select each step. Acronis will not do anything until you give it the final OK.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Uniblue Registry Booster 2

By Terry Currier, Vice President & Webmaster, WINDOWS users (WINNERS), CA
Tcurrier(at)jao1.com www.windowsusers.org/

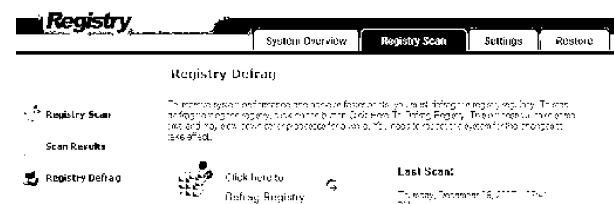
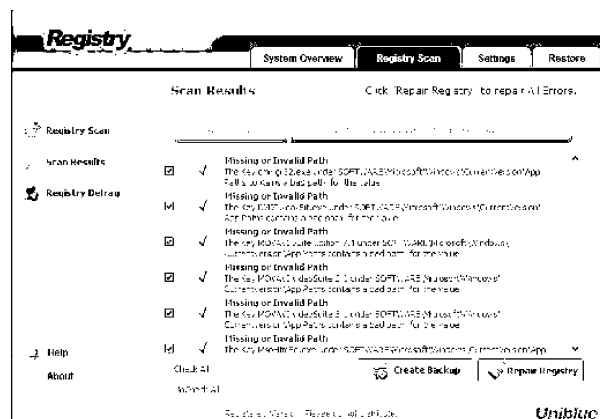
Obtained from APCUG with the author's permission for publication by APCUG member groups.

I've tested a number of programs on my secondary test computer over the years. I've also installed and uninstalled a number of programs. At start up the computer loads up my anti-virus, anti-spyware, firewall, UPS monitor, motherboard monitor, QuickTime, Intel graphics monitor, Maxtor storage monitor, printer software, TV software, and others. It takes a while for it to boot up. I turn it on when I need it, go away to do other things, and come back after it's ready.

Rebooting is even longer with it shutting down everything and restarting. So I thought Uniblue RegistryBooster 2 would be something good to try. Rebooting took 4 minutes 45 seconds. When I first ran RegistryBooster it found 459 Problems/Errors. The vast majority being Missing or Invalid Path.

things associated with the software, right? Well it does uninstall the programs, removing it from the hard drive. Most really do very little removal from the registry. So the software is removed, but the settings are still in the registry and you have a bunch of orphan links.

Even before I installed RegistryBooster 2 I did a backup, for safety sake. It also can create a backup of the registry before you have it do any repairs. It can create up to eight backups, keeping the most recent. Before running it my reboot time was 4 minutes 45 seconds. After running and fixing what it said were problems I also used it to defrag the registry. Using RegistryBooster 2 (twice)



The Windows Registry in a broad sense is a database of the hardware and software on your computer. It contains all your settings for windows and other software. Whenever you install new software it creates new settings in the registry. When you uninstall software it removes all those registry set-

my reboot time was down to 3 minutes 39 seconds, saving 66 seconds. Okay that's great, but for a program like this you want to make sure there are no problems later. So I've used this for two months now and I can say I've had no problems. I've run it about ten times total. Each time I chose to trust the program with what it said was a problem.

Conclusion

RegistryBooster 2 is very easy to use, and at \$29.95 it is a good value.

<http://www.liutilities.com/products/registrybooster/>
Supported Systems
Windows 2000 Windows XP
Windows Vista 32-Bit

Recommended Requirements:

Intel Pentium 4 1GHz or Equivalent processor
512 MB RAM
200 MB free hard disk space
Graphics mode 1024x768 true color (highest 32-bit)
Microsoft Windows 2000 / XP / Vista (32-bit)
Internet Explorer 6

Terry Currier is currently Vice-President & Editor of WINNERS – WINdows usERS which meets in Fountain Valley, California. He has been a member of computer user groups since 1984 (months before he even brought a computer.)

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

When to Turn Off Personal Computers

www.energy.gov/forconsumers.htm

U.S. Department of Energy - Energy Efficiency and Renewable Energy.
A Consumer's Guide to Energy Efficiency and Renewable Energy

If you're wondering when you should turn off your personal computer for energy savings, here are some general guidelines to help you make that decision.

Though there is a small surge in energy when a computer starts up, this small amount of energy is still less than the energy used when a computer is running for long periods of time. For energy savings and convenience, consider turning off the monitor if you aren't going to use your PC for more than 20 minutes both the CPU and monitor if you're not going to use your PC for more than 2 hours.

Make sure your monitors, printers, and other accessories are on a power strip/surge protector. When this equipment is not in use for extended periods, turn off the switch on the power strip to prevent them from drawing power even when shut off. If you don't use a power strip, unplug extra equipment when it's not in use.

Most PCs reach the end of their "useful" life due to advances in technology long before the effects of being switched on and off multiple times have a negative impact on their service life. The less time a PC is on, the longer it will "last." PCs also produce heat, so turning them off reduces building cooling loads. For cost effectiveness, you also need to consider how much your time is worth. If it takes a long time to shut down the computer and then restart it later, the value of your time will probably be much greater than the value of the amount of electricity you will save by turning off the computer.

Power-Down or Sleep Mode Features

Many PCs available today come with a power-down or sleep mode feature for the CPU and monitor. ENERGY STAR® computers power down to a sleep mode that consume 15 Watts or less power, which is around 70% less electricity than a computer without power management features. ENERGY STAR monitors have the capability to power down into two successive "sleep" modes. In the first, the monitor energy consumption is less than or equal to 15 Watts, and in the second, power consumption reduces to 8 Watts, which is less than 10% of its operating power consumption.

Make sure you have the power-down feature set up on your PC through your operating system software. This has to be done by you, otherwise the PC will not power down. If your PC and monitor do not have power-down features, and even if they do, follow the guidelines below about when to turn the CPU and monitor off.

Note: Screen savers are not energy savers. Using a screen saver may in fact use more energy than not using one and the power-down feature may not work if you have a screen saver activated. In fact, modern LCD color monitors do not need screen savers at all.

Smart Computing Tip Of The Day

Smart Computing Magazine sends these tips via e mail. They also have them archived on their website:

www.smartcomputing.com