Vol XXV No. 11 ISSN: 1076 089X

Member of the Florida Association of Computer Users Groups

Brevard Users Group

apcug Member of The Association of Personal Computer User Groups

November 2006

Prez Sez

By Larry French

The October BUG meeting was characterized by being held in the wrong Library, on the wrong day and in the wrong room which was way too small. The cause of this was a communication SNAFU with the Library.

As luck would have it, the meeting was well attended by our membership, the Space Coast User's Group and the public.

The featured speaker for the evening was Jen Clausen of Smart Computing. Jen did her usual great job of entrancing the group, even under the stress of the crowded venue.

Bob Schmidt is still interested in regaining members for the Tinkers SIG. He would like people interested in tinkering under the hood of their machines to contact him at; ***hardware@bugclub.org.***

Several of us are interested in forming a Linux SIG. Anyone interested please drop me an E-mail at president@bugclub.org.

November's meeting will feature Jim Howes of Data Doctors, a local computer shop.

This became effective in Florida October 2006:

You may have two emergency contacts attached to your Florida driver's license. If you are in an accident or otherwise incapacitated and the authorities run your drivers license, two emergency contacts will pop up so they do not have to search for relatives.

Go to **www.hsmv.state.fl.us.** Click on Emergency Contacts (the cell phone), enter your drivers license number. You will be asked for the name, address and phone number of the two persons you want to have contacted. Try to have the information ready when you start the process as there seems to be a time limit. Save and you are done.

Take care of each other,
Larry French, President

Moving South ?

Be sure to change your address.
Send to the Editor at: **newsletter@bugclub.org**
And also to the Treasurer at:
treasurer@bugclub.org

Table of Contents

Brevard Users Group

Managing Editor	Jim Townsend
Assistant Editors	Ed McEwen, Jack Nash
Contributing Editor	Jim Hally
Newsletter Volunteers:	Dan Wadler
Distribution:	John Williams
Home Page:	http://bugclub.org

The BUG Newsletter is created on a AMD Athlon XP 2400 Mhz computer using PageMaker 6.01.

Articles, Reports, and new Advertisements should reach the Managing Editor or Desk Top Publishing SIG by 5:00 p.m the Friday before the second Wednesday of the month. Items received after the deadline will be held for the following month's issue.

The articles contained in this Newletter do not necessarily represent the opinion of the Group, Editor, or Publisher or any other person other than the author of the article. The Brevard Users Group does not support or condone illegal copying of software.

Permission is granted to copy articles, provided the source is disclosed and proper credit is given to the author.

All questions, correspondence, and other items pertaining to the Newsletter should be directed to one of the Editors.

Questions involving advertising should be directed to **Advertising** at the address below.

Articles or items of interest for inclusion in the newsletter should be sent to **The Editor** at:

Brevard User's Group
PO Box 2456
Melbourne, Fl. 32902-2456 or
Jim Townsend 728-5979
E-mail to: newsletter@bugclub.org

THE NEXT MEETING OF THE BREVARD USERS GROUP WILL BE ON
November, 15th, 2006
At 7:00 pm
IN
The Melbourne Library
Visitors welcome!

Visit the BUG CLUB web site for the latest schedule.
http://bugclub.org

There will be a drawing for Door Prizes!
You must be a member and present to win!

Secretary's Report

By: Erich Dalton, Secretary

BUG October Monthly Meeting
Oct 19, 2006

The meeting was opened at 7 pm by club president Larry French.

Guests were welcomed and included members of the Space Coast PC Users Group.

The swap table was absent due to a shortage of space. Don't ask.

Announcements were that the Tinkers SIG has resumed, and that we need 3 volunteers for the Nominating Committee.

Our speaker was Jen Clausen of Smart Computing magazine. She gave an overview of the magazine itself and an introduction plus live tour of the Smart Computing web site. Some highlights are:

1) A paid subscriber has access to 4 different magazines. They are Smart Computing, PC Today, First Glimpse, and Computer Power User. The online versions contain all articles from every issue.

2) The biggest news was subscribers have FREE TECH SUPPORT! This is available M - F, 9a to 9p Eastern time. Even more incredible is the phones are answered by Americans.

Part of the on-line tour was directed at the Tech Support center features and the User Group area, which connects you to all participating User Groups.

The program ended by a drawing of prizes provided by Ms. Clausen. There were 2 collections of Smart Computing Reference Series and a one year subscription to Smart Computing magazine.

The meeting was then adjourned at 8:43 pm.

Respectfully submitted, Erich Dalton, Secretary

Treasurer's Report

By Tom Butler

October 2006

EXPENSES

Newsletter Mailing	$82.53
Newsletter Printing	$63.63
Total	$146.16

INCOME

Dues	$250.00
Total	$250.00

ASSETS

Checking*	$ 743.60
Savings	$2,210.37
Total	$2,953.97

New Members:

Cordova, Harold #1275
Manthey, Clifford #1273
Waltz, Allen #1276

Renewals:

Rymer, George #0982
Allen, Beth #1274
Bechtel, Paul #1237
Gundlach, William #1219
Buchanan, Albert #1023
Gillis, Knox #0955
Nash, Jack #0845
Adams, Doris #1078

Web 2.0 & Portable Computing.

By John Abbott, member of the Bentsen Grove Resort Computer Club, Mission Texas

Portable Computing has always lagged behind the rest of the computing market. This is probably because there are currently less mobile devices than computers. But that is about to change. According to Steve Rupel (leading PR company on the planet) billions of mobile devices will reach the market this year and by 2010 there will be 50 million of them sold quarterly.

Mobile device? You won't be calling them Pocket PC or Cell Phone long; maybe PCC for Personal Communication Center. The merger of all forms of digital communications is rapidly taking shape. Cell phones now contain very limited access to the web, receive very limited email, and take limited resolution pictures – oh and they work as phones too. With smaller and more low powered devices quickly coming on scene these limits will expand exponentially.

My project over the past month has been the installation of an Operating System on a USB Flash-memory Device (UFD). I started with a full blown Linux distribution on a USB 80 gigabyte micro hard drive. Well after some real torture and lots and lots of reading I managed to get it operational. However, in editing the boot file I managed to misspell something and now I've got to start all over again.

But I did find a couple of small Linux distributions: Damn Small Linux and Puppy Linux. I downloaded the ISO files for each and started working on a flash drive. Today I managed to get the thumb drive fully functional. Along the way I've learned a lot about what I still need to learn about executing from a CD or a UFD. But DSL in a tube really works.

Why do this? Well because I know that Web 2.0 is going to dominate the future of the web. With more and more of the platform being located on the Internet, less and less will be required on your local computer. The computer will take on more and more of the role of thin client (from a client/server relationship where all the applications are on the server). This in turn will have a direct impact on the cost of computers which will no longer have to come with expensive 3rd party software. So I created a portable thin client.

Web 2.0 (platform on the web) will take away a great deal of the chest thumping over O/S because the web interacts with all operating systems. The feature rich web already offers on-line mail processing that works perfectly with thin client or host computer. I am an advocate of Google's Gmail. I can access it on the web where it neatly threads my messages and stores up to 2.5 Gigabytes of mail in the in-basket or in the search - able archive. From within that mail system I can also originate chats with my friends and maintain my calendar. I can make my calendar or part of it accessible to colleagues for event coordination.

I can use Zohowriter.com for my word processor. Zoho is a full strength word processor with all the power you find in Works, Word or Open Office (or any of the dozen or so word processors available. I am able to store my documents on-line, download them to my computer, publish them on the site so they can be collaborated by associates whom I have previously arranged access. I can upload files from remote files (my computer or yours) and modify and store or simply store them online. And as an added feature I can use Zoho as a mail client; sending, receiving and originating email. Zoho automatically assigns you an email account when you register (free).

There will be some who say: "well I can have several programs open at once on my desktop." And my response would be, fine, I have multiple web pages open on my computer as I use Zoho to write this. I have a page set up with Wikipedia to check facts, the weather, my Google mail, my personal mail web ac-count, XM radio playing great jazz. And in a few moments I'll open another and watch the news on TV – all from my thumb drive. I sure hope my Gizmo or Skype phones don't ring during the news!

Are You Concerned About Loss of Personal Data?

By Carlisle Barnes, Newsletter Editor, Bowling Green Area Microcomputer User Group, KY
Newcarlislebarnes(at)insightbb.com
http://www.bgamug.org/

The advanced state of Information Technology is one of the great blessings of modern times. Today it is built into our economy, and it would be hard for both individuals and corporate America to do without it. However, along with the blessings to us have come curses. These curses are going to get considerably worse unless some dramatic changes are made in the way stored information is handled by the majority of organizations.

Computer spam, pfisheng/phishing schemes and other e-mail con games, as well as a multitude of ever changing computer viruses are obvious curses to everyone using a computer on-line. Great effort is being expended to get these curses under control. Very good and still improving anti-virus programs are available. Bill Gates said recently that spam will be completely under control within two years. (It will be interesting to see if Bill is right about that.) The point is that something positive is being done to correct those Internet curses.

However, one of the worst of current IT curses is identity theft, and very few positive things are being done to stop it. Identity theft is not associated with the Internet as are many other IT curses, but it has become very much associated with computers because of the casual way in which CD's, laptop computers, and portable hard drives are often handled. People who would never ever consider leaving a collection of gold coins laying in the back seat of a car, or leaving a thousand dollar bill on a table while going to get another cup of coffee, seem to have developed very little concern about leaving a portable computer, a container of CD's, or even a portable hard drive in all sorts of places where they can be easily stolen. (Home?)

Unlike sensitive data handled by military or military contractor organizations, the personal data stored in files of civilian Government organizations, major universities, insurance companies, credit card companies, and etc. are often treated as casually as advertising material. A recent extreme example is shocking and deserves examination.

Not long ago, a Veteran's Administration senior analyst took home electronic data from the office to do after-hours work on his personal computer. He had done this numerous times before. The data included names, Social Security numbers, and dates of birth on 26.5 million veterans. These data list essentially all military personal who have served following the Second World War. The analyst's laptop and a Government owned external hard drive (along with all the data under discussion on it of course,) were stolen in a May 3 burglary of his home. He reported the theft within an hour of discovering it. VA Secretary of Veterans Affairs Jim Nicholson made a public announcement of the theft on May 22.

Jim Nicholson appeared before the House Committee on Veterans Affairs to explain the situation. While accepting a certain amount of personal responsibility for the data breach, Nicholson expressed anger toward the analyst who took the data home "without permission." Further, he said "As a veteran myself, I have to tell you I'm outraged. Frankly, I'm mad as hell." Afterward, he fired the analyst involved. For what appear to be justifiable reasons, the analyst is now suing to be reinstated.

What Nicholson did not report, and later insisted that he did not know, was that the analyst had been taking data home as part of his regular work routine since 2003. (Is the VA a good place to work?) Furthermore, existing documents dated September 5, 2002 show that the analyst — lead programmer within the Policy Analysis Service — was officially permitted to take the external hard drive home for "work-related projects." Specifically, he had a property pass allowing the laptop and accessories to be removed from the building and also a permit allowing him to access any Social Security numbers on the hard drive. It later turned out that there was yet a third document allowing him to remove various materials from the VA building.

Continued on Page 6

Lost of Personal Data ... Continued from Page5

A certain amount of security could have been provided for these "take home" documents, by encrypting them. However, a reasonable up-front cost for the systems, services, processes, and procedures to encrypt 100,000 or more customer records is estimated to be about $500,000. VA working personnel probably couldn't justify that sort of expense to their budget group.

Once files have been stolen, it is difficult to determine if the data have been used illegally. The computer and VA hard disk have now been returned, apparently without data loss, but if it is eventually considered necessary to contact all affected veterans and to provide them with credit-checking services, then there will be an estimated taxpayer cost of at least $100 million.

The fiasco was not quite finished when Nicholson appeared at the congressional hearing. It was revealed at that hearing that Pedeo Cadenas, the VA's chief information security officer, had resigned by e-mail 30 minutes before the proceedings began. Nicholson said he was completely unaware of Cadenas' intentions. Evidently, Nicholson has learned many things rather late.

On June 28th, not quite two months after they were stolen, the computer and external hard drive were turned in to the FBI Office in Baltimore, Maryland. A tipster, in response to the $50,000 reward being offered, had let a US Park official know that the equipment might be recovered. Quickly then, the stolen items were turned in to the FBI. The tipster was not identified, nor was it clear if either he or anyone else would receive the $50,000 reward. Furthermore, no one has been arrested for stealing the equipment, unless that particular information is being held secret for some reason.

Inspection of the hard drive by the FBI does not indicate access to the data during the time that the drive was in the possession of the thief. Superficially then, no data were compromised and there is perhaps nothing to worry about.

Unfortunately, if the thief was a computer expert, knew what he had, and wanted to make illicit use of the data, then he could have transferred everything on the external hard drive to another hard drive without leaving a record. While that is possible, it seems improbable and it seems unlikely that there is reason for continued concern. However, can we be absolutely sure?

Those of us who served in the military, or worked for military contractors are quite well aware of the way in which sensitive intellectual material is handled by these organizations. While current practices are unknown to the author, not very many years ago, there were at least five security levels. Restricted meant that the information was not to be given to unauthorized people, was certainly not to be made available to newspapers or to other media, and was not to be left anywhere where it might be stolen. The only people allowed to see the material were those with a need to know about it. Confidential material classification, one step up from Restricted meant that the material was not to be made available to anyone not having appropriate clearance i.e., clearance by appropriate investigators. Except when being used in a cleared area by cleared personal, the material was to be locked in a desk or file cabinet with a safety bar and a combination lock. All desks and cabinets were to be regularly checked by guards. Secret material was to be handled in somewhat the same way, but clearance was more difficult to obtain, storage was in a secure safe, not in cabinets or desks, and material was to be guarded twenty four hours a day, and seven days a week. Top secret material was of course even more closely guarded, and investigations for personal clearance were carried out by FBI personnel; in general all security was substantially tightened. . Then there was "Special Clearance" which need not be discussed here, but which was very tight indeed.

It is absolutely shocking to note that as serious as identity theft can be, hardly anyone handling social security numbers, driver's license numbers, medical history facts, educational information, and etc., etc. is required to treat personal information in their possession with a level as high as military Restricted. As this article was being written, yet another security breach occurred at Ohio University, Athens, Ohio. There were several resignations from the school staff as a result, but it is one more case of "locking the barn door after the horse is gone."

Continued on Page 7

Loss of Personal Data ... Continued from Page 6

If current sloppy handling of private data continues, then it is only a matter of time until identity theft becomes a disaster.

This article by your newsletter editor is as close as you will get to a BGA-Bytes editorial. However, your editor considers the matter to be a lot more serious than it is being treated by many people and particularly by most public officials.

If you would like to encourage your congressmen or other public officials to put some teeth into privacy laws and into laws concerning the handling of private information, then may I encourage you to write and let them know how you feel.

To help you get started in sending letters, here are three addresses of interest. There are numerous others on the Internet.

U. S. Senator Mitch McConnell, 361A Russell Senate Office Building, Washington D. C . 20510

U. S. Senator Jim Bunning, 316 Hart Senate Office Building, Washington D. C. 20510 U. S. Representative Ron Lewis, 2418 Rayburn House Office Building, Washington D. C. 20515

Basic DVD Recording

By Bob Elgines, Editor, Colorado River Computer Club, Arizona
Elginesz(at)rraz.net
http://www.crccaz.com/

DVDs are like CDs, but with greater capacity; you can record sound, video, or data. The latest CDs allow 700MB of data, or 80 minutes of sound or video (mpeg1 format) whereas the DVDs allow 4.7 GB or 120 minutes of sound or video (mpeg2 format). Then you have Double Layer DVDs which allow 9.6 GB or approximately 3.7 hours of video. As we probe into the basics you will find approximately 10% of the room on your disk is used by Titles, Menus, and Directories.

First, what do we need to accomplish the recording of data, and sound:

A computer with a minimum of 1 Ghz, 512 MB of RAM, 40 GB hard drive, CDR optical drive, video with 32 MB RAM for 1024 x 768 screen mode, and recording software such as "NERO" by Ahead Software.

Second, we need all the above plus the items below for Video:

A DVDR optical drive, an input device such as ADS' InstantDVD (USB input) or equivalent for recording from VHS tape, and a VCR. A firewire input card can be used if you are recording from a digital camcorder (DV).

To record data and sound on DVDs is very similar to CDs, but video is different only because we use a different format. A CD may be used with this format and would hold approximately 30 minutes of mpeg2 (MP2) video. This CD would be called a "VCD" (Video CD) and would be played on a DVD Player.

There are several different video formats such as WMV, MPE, MPG, MP1, MP2, MP4, etc. MP1 (352x480) is fine for B&W video, but size and quality is too low for color. MP2 (720x480) is the most common format used at this time for doing video DVDs. MP2 can be recorded in low (3382Kbits per sec), medium (5073Kbits per sec), and high (9716Kbits per sec) quality.

Continued on Page 8

DVD Recording ... Continued from page 7

Before you start recording video, you may want to shut down all the programs running in the background to gain the maximum amount of System Resources in order to acquire the greatest performance when recording video. You will use 4 to 20 GB of your hard drive for recording a two hour video depending on the format you use.

"NERO" (Version 6 or 7) is the cheapest way to go for software. This program will do just about everything for you (two hours plus on DVD, some editing, excellent recording). I also have used "MyDVD v4 or5" by Sonic (easy to use, some editing, up to 1.9 hours on a DVD), "MyDVD v6" by Sonic (up to 3.5 hours on a DVD, but SONY players do not like the recording format), "Premiere Elements" by Adobe (easy editing is great, but recording is only good for one hour, jumps around with movement and going more than one hour really destroys it by also getting choppy), "Movie Factory2" by Ulead (not bad, but very time consuming and hard to use, 1.9 hours on DVD) and "Studio Plus 10" by Pinnacle (very demanding, needs more memory and high quality video card; very hard to use!).

I am using an INTEL P4, 3.06 Ghz, 512 MB RAM @ 800 MHz, GeForce FX5200 128 MB RAM video card, and a Digital Research model DDVD116DL (DVD Recorder with NERO software), an ADS Instant DVD VHS input device, which converts the antilog video to digital Mpeg2 format via a USB port, and an IEEE firewire port for my DV Digital Camcorder.

The Deals Guy

by Bob (The Cheapskate) Click
Greater Orlando Computer User's Group

Last month I published an announcement for a product that could copy DVDs.

We included what we found about downloading an additional product that was necessary to accomplish certain tasks, and I was accused of encouraging illegal activities.

Maybe I should have worded it differently, but the fact is, I simply published the announcement for a free product, along with our findings, and made the information available so an editor, or reader, could use it, or not use it, however they wished. I had two complaints (from the same UG) and that group chose not to make the column available to their members, which is their choice. This is not an apology because there has been tremendous interest in such products; I simply reported the facts and people are responsible for their own actions. I have read a number of articles in UG newsletters containing opinions concerning the law and the tactics of publishing companies. By the way, since last month's column, ShrinkTo5's product pricing and lineup has changed.

There are also those who would argue that a gun shop encourages murder, and I could use other similar issues that might be said to imply illegal activity. Recently I published an announcement for a product that recovers passwords. That could also be used for an illegal activity if used on a stolen computer. With all the write-ups and notoriety about new and controversial copyright laws, I wouldn't even try to explain the legalities of anything.

Is it legal, or illegal to make a backup copy? Do you know for sure? Also, ShrinkTo5 has other uses and we did not include a link for Machinist2.dll. My proof reader suggested that car companies must encourage a long list of illegal activities, including manslaughter, since they sell cars that can do such things.

Actually, I am not a fan of publishing companies' tactics and the UCITA or DCMA laws. If those officials

Continued on Page 9

The Deals Guy ... Continued from Page 8

have their way, you would not be able to give, or even lend, anything published after you have read or listened to it. From what I read, they want all used book stores shut down as well as all libraries, and you would even be arrested if you were caught lending, or giving, a book or CD to a friend. Who knows where it all might end when it comes to the pockets of some corporate bigwigs.

However, I have no interest in any of this copying stuff. I have no time and have not bought a music CD in years, nor do I rent videos or go to a movie. The performers and executives involved with that industry are grossly overpaid, but they don't make any money from me. I don't watch much TV now, but if they keep adding commercials, I'll shut that off too.

While I'm on my soapbox; if I am paying for cable TV, why should I have to put up with all those commercials? People are much too tolerant of being taken advantage of, and about what they are paying for.

Do Your Homework

The announcements below have been edited to shorten them so be sure to check their Web sites for better information. Remember, I have not tried any of these and have no knowledge about their reliability.

Check That Malware, And For Free!

Put an end to all types of Malware, at no cost: The a-squared Web Malware Scanner 2.0 hunts undesired Spyware modules and dangerous Trojans, Backdoors, Keyloggers, Worms, Dialers, Rootkits, Hacking Tools, Riskware and TrackingCookies; all from within the Web browser and no software must be installed.

All users having Internet Explorer and a fast Internet connection, such as DSL, can make optimum use of the scanner.

The a-squared Web Malware Scanner 2.0 uses over 350,000 signatures and an ingenious heuristic algorithm for detecting pests on the local computer, and this scanner can be used directly from the Web browser. The user can choose from four different scan functions depending on the time available for a scan. The quick test provides rapid results, while a detailed analysis of the entire computer can take a while. A Riskware recognition system can also be enabled that informs the user of programs that are usually harmless, but are often used by Malware for specific tasks. There is also a paid version that they recommend as quicker and better with a 30-day free trial.

a-squared Web Malware Scanner 2.0:
http://malwarescan.emsisoft.com
a-squared Anti-Malware:
http://www.emsisoft.com/en/software/personal
Product details Malware-IDS:
http://www.emsisoft.com/en/software/ids
Order a-squared Anti-Malware:
http://www.emsisoft.com/en/order/homeuser
Phone: +43-664-3446068 (German)
Fax: +43-6272-73083
Email: <info@emsisoft.com
Web: <www.emsisoft.com

Lets Compare Data

ZsCompare allows users to efficiently synchronize computers, backup data, compare different versions of files, verify that CDs have been copied correctly, manage Zip files, review changes to source code, and more. Users can easily run comparisons on local directories, networked computers, or removable media, such as CDs, DVDs, and flash drives.

ZsCompare 3.0 adds many new file and freeform text comparison features, including the ability to compare text from Microsoft Word documents and PDF documents. Also, zsCompare provides additional control over how the comparison is performed with predefined options for common comparisons. Finally, the new version of zsCompare permits direct editing of the contents of a file from the results. ZsCompare 3.0 operates on Windows, Mac OS X, and Linux. It runs on the Java platform, a copy of which is included with the ZsCompare installation. ZsCompare 3.0 is available in three editions: Professional ($199.95), Standard ($99.95), and Lite ($35.00). For a 20% discount, my readers should enter the coupon code "DealsGuy" when purchasing a license at https://www.zizasoft.com/store/order.shtml. The Lite Edition contains basic comparison and synchronization functionality. With the Lite Edition, users can compare directories, zip files, text files, and freeform text. All versions include free lifetime upgrades and free technical support.

More information, including a complete list of enhancements and a fully functional 30 day trial version, is available at http://www.zizasoft.com/products/zsCompare/index.shtml.

Sales: sales@zizasoft.com
Telephone: 1 (303) 638-9235

Continued on Page 10

The Deals Guy ... Continued from Page 9

The Arnold Schwarzenegger Of Windows?

Tame Windows with Actual Window Manager 4.01. Microsoft Windows is the most widely used operating system today and its window architecture is a brilliant invention. However, this architecture comes with a bit of baggage and a degree of frustration, especially when you work with several windows simultaneously. With many applications open at once Windows becomes heavily cluttered, which in turn cuts down on your computational productivity. The more windows you open, the more time you spend to manage them and less focus is on the job. Monotonous clicking, window clutter in the taskbar, switching between windows, their positioning and resizing may double and even triple the time you need to concentrate on your job.

Actual Window Manager adds its buttons to each window in your system and allows you to navigate them in new ways. Instead of the taskbar, you will be able to minimize windows to the task tray or to the edge of the desktop, or roll them up or unroll, like blinds. If you need to multitask in several applications at once, you can simply pin all necessary windows on top without the need to bring up each one several times a day. In fact, you have over 40 other controls to automate routines related to windows. You can apply a predefined level of transparency to any window, automate positioning of windows, resize them and change priory from the title bar menu and more.

Over 450 suggestions were carefully considered and reflected in a more intuitive user interface.

The customization of options has become much simpler, and the choice of options wider. In addition to subtle customization abilities, the program has a list of presets for most popular applications that allow you to use Actual Window Manager in the "install-and-go" style.

Read the complete description of features at
http://www.ActualTools.com/windowmanager/
Download a no-cost evaluation copy from
http://www.ActualTools.com/files/aimsetup.exe
Pricing and Availability

Actual Window Manager 4.0 runs under all Windows platforms and costs $39.95 (USD) for a single-user license. Registered customers are entitled to the unlimited functionality, free updates and lifetime technical support. Additional information on Actual Window Manager, a collection of tutorial articles and success stories, as well as a 60-day evaluation copy is available from http://www.ActualTools.com/. UG members should visit our User Groups Support page http://www.actualtools.com/usergroups/ and click the "Get 20% discount" Link, then follow the instructions.

E-mail: info@actualtools.com

That's it for this month. Meet me here again next month if your editor permits. This column is written to make user group members aware of special offers or freebies I have found or arranged, and my comments should not be interpreted to encourage, or discourage, the purchase of any products, no matter how enthused I might sound. Bob (The Cheapskate) Click bobclick@mindspring.com. Visit my Web site at http://www.dealsguy.com

From the Editor:
Following is the article Bob Click is referring to at the start of this column.

DVD Copying Anyone?

ShrinkTo5 has released version 2.02 of ShrinkTo5 GUI, a new DVD copying engine distributed at no cost to anyone. This application lets you copy and shrink your favorite DVD disks in brilliant quality, which is complemented by a surprisingly high processing speed. You can copy an entire DVD, copy the main movie only, or copy its content elements selectively. The output can be saved to the hard disk drive as an ISO image or compressed and burned onto one DVD disk. The best thing in copying DVD disks with ShrinkTo5 is that it no longer involves tedious and sometimes confusing configuration. ShrinkTo5's AI chooses the perfect balance automatically.

DealsGuy Note: **Bob Clyne says the free version contains Adware; WhenU to be specific and recommends against it.**

He also says the $19.95 version, containing no adware, is available from Download.com and you can try it for three days before you have to buy it. He suggests getting the Machinist2.dll before getting ShrinkTo5 if you intend to copy encrypted DVDs. The program will not work on encrypted/copy protected DVDs i.e. most commercial DVDs, without the Machinist2.dll, which for legal reasons, they don't supply. The Machinist2.dll can be challenging to find, but he did find it a few places, some of which were Warez sites.

Continued on Page 11

Deals Guy ... Continued from Page 10

Some of the features for ShrinkTo5 GUI are:

• - Support for Machinist2.dll. The program has been modified to support new Machinist2.dll. Now, ShrinkTo5 has a unique ability to make DVD backups that cannot be handled by other DVD copying software like DVDShrink.

• - Free burner plug-in. The ShrinkTo5 GUI package comes with FoxBurner, a shell plug-in that allows you to burn directly from the Windows Explorer. You don't have to donate or download a burner separately.

• - ISO Image. Along with burning onto DVD disks, copied images can now be saved as ISO images on the hard disk drive and burned onto disks later if the need arises.

• - Auto-Repair. New ShrinkTo5 lets you automatically restore scratched and defective DVD disks so that their content can be accessed and copied.

• - Dynamic Compression. The code of the dynamic compression rate has been enhanced, which now allows users to get an even sharper picture.

• - Built-in Player. New ShrinkTo5 features a built-in player that allows the user to view selected video tracks. This gives you more control over the copying process.

Read more information about ShrinkTo5 GUI at http://www.shrinkto5.com/software.asp

Watch the online tutorial demo at http://www.shrinkto5.com/gTour.as>

ShrinkTo5 is available as Basic and Professional. Both versions run under Windows 2000/XP. The Basic version is available as a free download from http://www.shrinkto5.com/software.asp>.

The Professional is available as a three day trial. The price of the Professional version is $19.95 download, or $24.95 plus S&H box USD. Both versions are compiled without DeCSS. To enable ShrinkTo5 to decrypt CSS, users should download "Machinist2.dll" from the Internet.

Product page link: http://www.shrinkto5.com

Download link: http://www.shrinkto5.com/_data/ShrinkTo5AdFree.exe (4.77 Mb)

E-mail: <info@shrinkto5.com>

Ram & Reason: Erasing a Dead Hard Drive

By Rob Rice August 2006
Reprint from; Computer Club of Oklahoma City

You will have a hard drive fail. If you have been around computers for any length of time, you probably know this already. Nothing in this world lasts forever and hard drives are no exception. But let's say you have a hard drive keel over unexpectedly with all of your data still on it. Lots of folks dutifully take the computer back to Best Buy, CompUSA, or wherever for repairs, trusting that they will keep your personal information secure. Yes, the hard drive is dead, but the data isn't! Hank Gerbus found this out in a most alarming way.

According to an article at MSNBC,

One year ago, Hank Gerbus had his hard drive replaced at a Best Buy store in Cincinnati. Six months ago, he received one of the most disturbing phone calls of his life.

"Mr. Gerbus," Gerbus recalls a stranger named Ed telling him. "I just bought your hard drive in Chicago."

In June 2005, when Gerbus took his computer to Best Buy for repairs after a hard drive crash, he knew the drive was a potential hot potato. So when a clerk there told him it had to be replaced, he asked for the damaged hardware back.

No dice. The replacement was done for free, under warranty, and Gerbus was told the old drive had to be sent to a repair center in Chicago to fulfill warranty terms.

"I asked in the store on two or three occasions. ... I was very concerned," he said. "But they said 'we can't give you the old one because it's under warranty.'"

Gerbus said he was assured that, after verifying the warranty, workers in Chicago would drill holes through the drive and make it unusable. . .

The Best Buy service center did not destroy the drive but instead sold it. A fellow named Ed bought it at a flea market for $25. Social Security numbers, account numbers, and retirement/ investment information was on

Continued on Page 12

Ram & Reason ... Continued from Page 11
the drive. Ed tracked down Mr. Gerbus at his winter home in Florida (from information obtained on the hard drive) and fortunately returned the drive. Best Buy is said to be investigating and has offered Mr. Gerbus a $250 Best Buy Gift Certificate for his troubles.

I have seen for myself the information left on hard drives. I have gone to computer shows and bought used hard drives, never paying more than $7 a piece. I recovered data on 5 out of seven drives during one such show; however, none of the drives that I bought had sensitive or personally identifiable information on them. All of the drives were erased and were used for data storage.

In 2002-2003 Simson Garfinkel, an MIT researcher picked up a number of used hard drives from various sources. He examined 129 drives; only 12 had been completely cleared of data. One drive had 3,722 credit card numbers on it! http://www.computer.org/portal/cms_docs_security/security/v1n1/garfinkel.pdf

So how do you deal with a dead hard drive? We will assume that the drive has very sensitive data that you do not want others to have access to.

If taking it back to the retailer or in to a shop for repair, call them first. Explain the situation. Hopefully, they will have a more realistic policy than Best Buy. Some manufacturers will allow you to keep the drive in your possession, but require you to sign a form stating that you have physically destroyed the drive. They will then replace or send you another hard disk. But don't look for this policy on their website, for obvious reasons they do not advertise it.

You could also ask the repair shop or retailer to destroy it on the spot and in your presence. Drilling holes through it would work, so will smashing it with a heavy hammer.

The best way to destroy the drive is to melt the discs that contain the data located inside the drive, but this is not always possible, again for obvious reasons. I prefer to take the drive apart and physically remove the platters and file the surface or run a powerful magnet over both sides of each platter or disc. Hard drives typically have strong magnets located inside of them. These may be able to do the job.

Of course the problem with taking the drive apart is that you void the warranty. But it may be worth it if it means protecting your data.

If the company insists having the drive intact and the warranty seal unbroken then you can avoid Mr. Gerbus' situation with a powerful magnet, like the ones found in some hard drives. Rubbing it over both sides of the drive, top and bottom, at least ten times should hopefully do it. But beware, MOST magnets people have available to them are not strong enough to penetrate the shielding of the hard drive case. Simple iron magnets, including the big ones, just cannot do it. Electro magnets used for erasing floppy disks and video tapes are also too weak. As a loose rule of thumb: if you can, without much difficulty, move the magnet over the drive in a circular motion, it is too weak. The proper magnet should be VERY difficult to move in a circular motion over the drive because it is forcibly sticking to it.

The only magnet I have seen that worked (after trying many!) is a Neodymium magnet. These are the strongest magnets made. They come in various grades such as N28, N35, N38 and N40. An N40 of sufficient size, say 1" W x 3/4" thick x 2" long, would probably work. A 1-1/2" Diameter x 3/4" ring might also, which may be easier to handle. These will cost around $25 from an industrial supply, hobby store, or specialty store. Using one of these magnets should render the hard drive data very difficult if not practically impossible to recover. You can then pop the drive back in the computer and ship it off for warranty repair with reasonable confidence.

I have verified that they work. After taking a Neodymium magnet that was roughly 2" x 2" x 1/4" to a working hard drive I was unable to recover any data afterwards. Unfortunately, it also wrecked the drive, rendering it useless.

My company is actually using neodymium iron-boron magnets in its development work on a magnet powerful enough to erase U.S. intelligence-gathering aircraft's hard drives in emergency situations - like that
Continued on Page 13

Ram & Reason ... Continued from Page 12
which took place near China several years ago, http://gtresearchnews.gatech.edu/newsrelease/erase.htm.

A note of caution: these magnets are not for kids to play with. They are very strong, even the small ones, and should be kept away from all electronic devices including pacemakers, security badges, monitors etc. Size matters! Two magnets in the same proximity can slam together and splinter or shatter. Larger examples, such as 2" x 1" disk, can crush fingers if in the presence of another. And do not stick the magnet anywhere near your computer! Remove the hard drive first.

Of course, this method has its disadvantages. You have to remove the hard drive, you have to find or buy a magnet that is sufficiently powerful, there is no easy way to verify that the data is erased and because of the magnets strength, it can be an irritation to work with. Still, you can sweat it out like Mr. Gerbus did, only to find out that your sensitive information was sold at a flea market, or you can have some measure of confidence that your data is safe. It's up to you.

Rob Rice is a member computer specialist in Anchorage, Alaska and a graduate of the Candler School of Theology, at Emory University, Atlanta GA. Rob can be contacted at articles@isp.com.

How To Allow Email Attachments

A fairly common problem people run into is the inability to save attached files to their PCs. This may happen to you if your email client is configured-for security reasons-to prevent you from opening file attachments of a certain size, content, or type. You can disable this setting in Outlook Express by opening the Tools menu and selecting Options. Click the Security tab, deselect the Do Not Allow Attachments To Be Saved Or Opened That Could Potentially Be A Virus option, and click OK. To avoid viruses, worms, spyware, and other types of nasty code, be sure to scan the saved file for malware before opening it.

Legal Bytes: What is the Real ID Act of 2005?

By John Brewer - August 2006
Reprint from:
The Computer Club of Oklahoma City

Almost everyone is unaware that a national ID card is on the way. In 2005, the Real ID Act was enacted as federal law. The Act was attached to a 2005 military spending bill.

The Act establishes national standards for state-issued driver's licenses and non-driver's identification cards; waives laws that interfere with the construction of physical barriers at the borders; updates and tightens the laws on application for asylum and deportation of aliens for terrorist activity; introduces rules covering "delivery bonds" (rather like bail bonds, but for foreign nationals that have been released pending hearings); funds some reports and pilot projects related to border security; and changes visa limits for temporary workers, nurses, and Australians.

The vehicle for implementation of the Act will be State driver licenses (and substitute identity cards for non-drivers). After May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements specified in the Real ID Act." States may also issue non-complying licenses and IDs, so long as they have a unique design and a clear statement that they cannot be accepted for any Federal identification purpose. The federal Transportation Security Administration is responsible for security check-in at airports, so bearers of non-compliant documents would no longer be able to travel on common carrier aircraft.

Each card must include, at a minimum: the person's full legal name; the person's date of birth; the person's gender; the person's driver's license or identification card number; a digital photograph of the person's face; the person's address of principal residence; and, the person's signature.

The card must have physical security features designed to prevent tampering, counterfeiting, or

Continued on Page 14

Legal Bytes ... Continued from Page 13
duplication of the document for fraudulent purposes. It must also have a common machine-readable technology, with defined minimum data elements. The details have not been spelled out, but are the responsibility of the Secretary of Homeland Security, in consultation with the Secretary of Transportation and the States.

There are specifications for the States stating the documentation required before issuing a license or ID card. Before a card can be issued, the applicant must provide the following documentation: a photo ID, or a non-photo ID that includes full legal name and birth date; documentation of birth date; proof of Social Security Number or verification that the applicant is not eligible for one; and documentation showing name and principal residence address.

In addition, the Act requires documentation showing that the applicant is legally present in the US. For example, that the applicant is a US citizen or national, is an alien with permanent or temporary residence status or a valid visa, has applied for or been granted asylum, or is a refugee. The State must verify each of the above documents with the issuing agency. The only foreign document that may be accepted for any of the above items is an official passport.

Each State must agree to share its motor vehicle database with all other States. This database must include, at a minimum, all the data printed on the State drivers' licenses and ID cards, plus drivers' histories (including motor vehicle violations, suspensions, and points on licenses). Any State that does not link its database, containing records on all drivers and ID holders, to the database of the other States loses its federal funding.

The ID provisions of the Act are not without controversy. One website, realnightmare.org, summarizes the negative aspects as follows:

1) The Act was not passed through a true democratic process. It was slipped through Congress in May, 2005, in a "must-pass" Iraq War/Tsunami relief supplemental bill, as part of a deal reached between the powerful Rep. James Sensenbrenner (R, Wis.) and the Congressional leadership. There was no time for sufficient consideration of the Act and its sweeping implications; in the Senate, there was not even a single hearing held on the Act. The result is that Real ID lacks the legitimacy that comes from having been studied, debated, considered, and directly voted upon by Congress.

2) The game is not over, it has just moved into the States. Although the Act was passed by Congress, Real ID cannot go into effect without a multitude of actions in the States. State legislatures must appropriate money and, in most cases, change State laws. State executives must remake or build anew all the administrative machinery required to comply with the Act's numerous mandates. A lot of people at the State level do not like what they see.

3) Opponents range from privacy and civil liberties organizations to conservative groups and immigration groups.

4) It is a bad Act. Most fundamentally, the Real ID Act has sparked opposition because it would not be good for our country.

In addition, Homeland Security has become a windfall for certain areas of the county. Harold Rogers is a Kentucky congressman who is the chair of the subcommittee that controls the appropriations for Homeland Security. His district has profited from his position in terms of government contracts including the production of identification cards. Congressman Rogers represents an economically depressed area and has exercised his control to influence technology decisions. Industry experts say his interference has been detrimental to the development of identity cards using state-of-the-art technology. It is a safe assumption that Congressman Rogers will seek to influence the Real ID card technology so that it benefits his home district.

Regardless of whether the Real ID card is a good idea or a politician's dream in term of "pork" projects, this is a topic that is worthy of attention and investigation. The motivation for this project may be more complicated than just national security.

John Brewer practices law in Oklahoma City, is a member of the Governor's and Legislative Task Force for E-Commerce, and enjoys issues relating to eBusiness and cyberspace. Comments and questions are welcome and can be emailed to johnb@jnbrewer.com.

Brevard Users Group Membership Application

First Name _____ Last Name _____

Address _____ City _____

Home Phone _____ State _____ Zip + 4 _____

Family Membership $25.00 E-mail Address _____

Special Interest Groups

Afternoon Meeting

A daytime meeting is held on the first Monday of the month at 2pm, in One Senior Place, 8085 Spyglass Hill Rd in Viera.

http://oneseniorplace.com

WINDOWS SIG

Meets 7:00 PM Thursdays

1st & 3rd Thursday at Eau Gallie Library.

All Other Thursdays at Melbourne Library on Fee Avenue.

BEGINNERS SIG (Newbies)

Meets at 6:30 pm. The 2nd and 4th Thursdays, in the Fee Ave Library, before the Windows SIG

IMAGING SIG

Meets at 7:30 PM the second and fourth Thursdays, after the Windows SIG, at the Fee Ave Library in Melbourne.

NEWSLETTER SIG

Meets twice a month on the Saturdays before and after the BUG monthly meeting.

Place is Jim Townsend's home

call 728-5979 for directions.

TINKERS SIG

Meets on most Sundays at Bob Schmidt's house.

Call 952-0199 to verify meeting and directions.

E-mail: rschmidt@cfl.rr.com

BUG Club Information

BUG E-MAIL LIST

To be included in the BUG E-Mail roster, send an E-Mail to Larry French at: president@bugclub.org.

We will need your full name, E-Mail address and your BUG membership number. You will then receive notices and updates on BUG activities, special events, changes to schedules, etc.

BUG Officers

Meets the second Wednesday of the month at the Fee Ave. Library, in Study room 1

Time 7:00 pm to 8:00pm

Sponsorship Rates

	4 Months	8 Months	12 Months
Full Page	$160.00	$ 305.00	$ 440.00
Half Page	$ 85.00	$ 162.00	$ 232.00
Qtr Page	$ 45.00	$ 86.00	$ 123.00
Bus Card	$ 25.00	$ 48.00	$ 68.00

Moving ?

Don't miss out on any issues of the BUG Newsletter
Send your new address to:
Brevard Users Group Att: Treasurer
PO Box 2456
Melbourne, FL 32902-2456
And e-mail to the Newsletter and Treasurer at:
newsletter@bugclub.org
treasurer@bugclub.org

Brevard Users' Group
Incorporated
P. O. Box 2456
Melbourne, FL 32902-2456

Meetings:
Are held at the Melbourne Library on Fee Ave. the third Wednesday of the month at 7:00 PM.

Membership:
Is by application and payment of $25.00 annual dues. Membership is for 12 months from receipt of dues and includes a year's subscription to the newsletter.

Your membership expires on the date indicated in the upper left of your address label (YYYY\MM). Please allow six weeks for processing the renewal.

BUG Officers

President:
Larry French 837-0962
president@bugclub.org

Vice President
Lester Cassel
vicepresident@bugclub.org

Treasurer:
Tom Butler 242-9869
treasurer@bugclub.org

Secretary:
Erich Dalton
secretary@bugclub.org

Member at Large:
Dan Wadler

Committee Chairperson

Beginners Help:
Tom Butler 242-9869
geotbutler@juno.com

FACUG Representative:
Dan Wadler

Program Director:
Dan Wadler

Webmaster:
Eric Arnold
webmaster@bugclub.org

BUG Web Page:
http://bugclub.org

Special Interest Groups

Beginners' SIG:
Larry French 837-0962
beginners@bugclub.org

Hardware (Tinkers) SIG:
Bob Schmidt 952-0199
hardware@bugclub.org

Newsletter Publishing SIG:
Jim Townsend 728-5979
newsletter@bugclub.org

Win 9x/XP SIG:
George Rymer 724-6715
Chuck Boring 454-9455
Bob Staples 255-2623

Imaging SIG:
Ed McEwen imaging@bugclub.org