



# The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 10

October 2005

For group information  
please visit our Web site:  
[www.mpcug.org](http://www.mpcug.org)

## *The Bridge Staff:*

Editor  
Gil Hennon

Review Editor  
Rick Fischer

Publisher Emeritus  
Les Owen

## Main Meeting Wednesday, Oct. 26 Southwest Tennessee Community College

5983 Macon Cove, Memphis

### **MEETING LOCATION**

## Thornton Room 104

First Floor - Thornton Hall

Wizards Session 6:30 p.m.  
Main Meeting 7:30 p.m.

## *In This Issue*

The School Bell	Page 2
WipeDrive 3.0	Page 4
Congratulations Rick!	Page 5
Too Many Wrongs . . .	Page 6
September Meeting Report	Page 10
Out for Review	Page 11
Event Calendar	Page 12

## October Main Meeting

The temperature is cooler, the wind is gusty, the days are getting shorter, and the leaves are falling. But none of this is going on at our meetings.



Escape those Autumn chores at the MPCUG. Relax and join in the fun. Bring along a friend.



# The School Bell

## News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Americans tend to believe that the United States is a technologically advanced country. We see ourselves as on, or at least near, the cutting edge of modern life. Other cultures know better, especially those of Europe and Asia, where Americans are ranked about five on a scale of one to ten for embracing and using new technology. We are followers, waiting for someone else to take the risks and expense of early adoption. Our vehicles, homes, businesses, phones, and even televisions are only starting to take advantage of technological improvements many other countries have had for years.

Among all of the geeky gadget lovers in the world, the Japanese are without peer. It's not just a stereotype. Whether it's a camera, car, or appliance, the more complicated it is, the better it will sell in the Japanese marketplace. Japan was the first country with an optical interface between vending machines and cell phones, where you can point your phone at a Coke box and have a cold drink delivered and charged to your monthly telephone bill.

Brian Lam, an editor at Wired magazine, travels regularly to Japan. He noticed that fads such as Pokemon, Beyblades, and other Japanese novelties experienced a lag of several months to a year before catching on in the United States. He began keeping track of what he saw in Japan and pretty soon had built a reputation for accurately predicting the next big fad to sweep America. Brian's observations became a monthly Wired column: Japanese Schoolgirl Watch.

His first posting, in the April 2003 issue, wasn't all that high-tech. It was about socks—the high top kind that Japanese Schoolgirls wear. Since the style and

color of their clothing is decreed by their school dress code, the girls were faddish on socks with tiny, almost unnoticeable embroidered logos designating the fashion design house that sold the socks. Top brands at the time were Arnold Palmer, Polo, and East Bay. The photo below, taken sometime afterward, shows some of the school girls checking out the issue with the story about their socks.

Since then, several different Wired journalists have contributed to the column, and Japanese Schoolgirl Watch has been noticed and quoted in USA Today, the MIT Technology Review, and the New York Times. Here are some highlights from recent issues:

May 2005: Brian Ashcraft took note of many schoolgirls with giant, inky black eye pupils. Influenced by the manga and anime art in their culture, they were purchasing black tinted contact lenses. "The bigger the character's eyes, the cuter they look," explained 15-year-old Yumi Koba about her "Sailor Moon" inspired gigantic orbs. The contact lenses are non-prescription, so schoolgirls can order them through their cell phones.

July 2005: Todd Jatras discovered that the best-selling confectionary among



Japanese schoolgirls is a chewing gum named Bust-Up. The gum is fortified with phytoestrogens and it's claimed that regular usage will enhance the size, shape, and firmness of breasts, as well as improve the condition of hair and skin. So far, the manufacturers have been unable to keep up with demand in Japan, limiting their plans to introduce Bust-Up in the United States, where they expect a 100-piece package will sell for \$50.

August 2005: Brian Ashcraft sneaked over to China to find that schoolgirls there are just as faddish as their Japanese counterparts. The big deal on the mainland is finger-nail printers. A company in Zhengzhou manufactures a digital 4,800 dpi printer that prints directly on fingers or on salon press-on fake nails. Quick and easy, the customer just sticks a hand under the inkjet for photo perfect nails. The printer contains a stock of over 3,000 images and also accepts any JPEG file. A company spokesperson remarked that, "now high school girls can change their nails as easily as switching the faceplate on their mobile phones."

September 2005: Tony McNichol found the Japanese schoolgirls writing tiny notes between the lines of their textbooks. Back in 1994, they went crazy for Pilot pens with a fine point ink ball of 0.3 mm. The recent revival of tiny writing came after Mitsubishi introduced a new pen with a ball diameter of 0.18 mm. Special, friction reducing ink is required to produce a fine line about the thickness of two human hairs. The pens come in eight colors for \$1.75 each, and Mitsubishi is selling about 4 million of them each month. Most schoolgirls have as many different colors as their allowance can afford.

October 2005: Brian Ashcraft returned to Japan this month and discovered that the schoolgirls are finding new ways to keep from putting down their cell phones. The infrared ports on DoCoMo handsets can be programmed to function as a remote control for television sets and DVD players. If that doesn't keep the phone in hand, Japanese manufacturer Quixun plans to release by the end of the year a \$20 USB device that lets the phone function as keyboard and mouse for a computer. Girls can type, move the cursor, and click from 30 feet away, streamlining the transfer to hard drive of those secret pictures they took of the cute boys in their classrooms.

When will all of these fads reach the United States? Nobody knows for sure, but the Japanese Schoolgirl Watch crew at Wired magazine bets that we'll be seeing some of these novelties pretty soon. In the meantime, come to the Wizard session immediately prior to the main meeting each month. The Wizards don't make too many predictions, but they can rescue you when that faddish new hardware or software you installed starts to misbehave.

-0-

This newsletter is a monthly publication of the Memphis PC Users Group, Inc. (MPCUG) Copyright ©1998 MPCUG. Unless otherwise indicated, articles may be reprinted in other non-profit publications without express permission, subject to the following conditions. Full acknowledgement must be given to the MPCUG, The Bridge, and the author. The article must be reproduced in its entirety from magnetic media, without editorial changes, deletions or additions. Two copies of the entire publication containing the reprinted article should be sent to The Bridge within 30 days of publication. All other rights reserved. Any changes to the article require the written permission of the author. All articles are made available through the APCUG BBS and on disk to qualified non-profit organizations.

Any opinions expressed belong to the author and not the Memphis PC Users Group, Inc. Articles in this newsletter may contain trademarks of various companies. Any proprietary right those companies have in those names is hereby acknowledged.

Unless otherwise indicated, all submissions to this newsletter become the property of Memphis PC Users Group, Inc., and are subject to editing by the staff. The MPCUG reserves the right to determine the suitability for publication of all items received.

Members are encouraged to submit articles for publication. By submitting articles, the author gives permission for publication in this newsletter and for publication by other user groups. The editor cannot guarantee that all submissions will be used.

The information contained in this newsletter is believed to be correct and accurate; however, the Memphis PC Users Group, Inc., cannot and will not assume responsibility for the consequences or errors contained in articles or misapplication of any information provided. Any information used from these articles is at the user's own risk. If a review of any hardware or software contains errors or inaccuracies, upon notification of these errors or inaccuracies by the manufacturer in writing, a correction will be printed in the subsequent issue following receipt of these corrections.

The Memphis PC Users Group, Inc., makes no warranty, expressed or implied, as to the suitability of any advertised product. You must determine that yourself. The Memphis PC Users Group, Inc., also expressly declines to assume liability for any use of any published software, and your use of same constitutes your agreement to hold us blameless.

Memphis PC Users Group, Inc.  
4746 Spottswood Ave. PMB 178  
Memphis, TN 38117-4815  
[www.mpcug.org](http://www.mpcug.org)

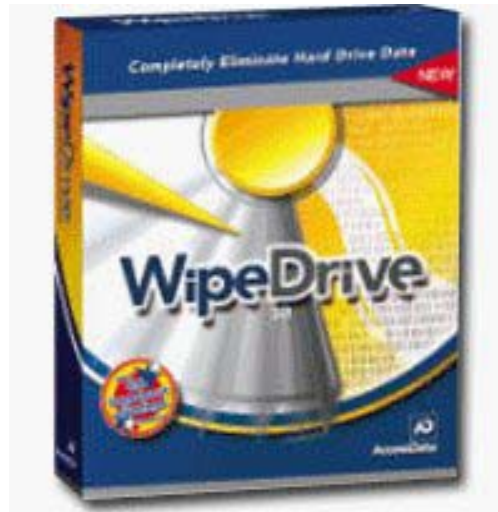
# WipeDrive 3.0

## Software Review

Reviewed by John Dodson

Over the last two or three years, many of the security-based organizations have brought to our attention that the data left on our hard drives when the drives and/or machines are passed on to others or even recycled or sold can leave us vulnerable to ID theft. *WipeDrive* 3.0 by White Canyon Software is one of the several products available to permanently overwrite the data on a computer's hard drive. The overwriting process removes everything on the hard disk including operating systems, program files and personal (i.e., private) information. White Canyon's *WipeDrive* was introduced in 1999, and is listed in the top five disk sanitizing tools approved by the U.S. Department of Defense.

Many computer users aren't aware that when a data or system file is deleted, that only the marker for the particular fat table entries only are changed to indicate that they are not currently being used. The data, in fact, remains on the hard drive until overwritten by new data. This



leaves the need to protect users from the potential retrieval and misuse of confidential and/or possibly embarrassing information.

Quoted from the *WipeDrive* 3.0 package:  
"Selling, rebuilding or donating a computer? Make sure your personal data has been removed first! Your computer contains online banking information, credit card numbers, email messages - basically any data entered on your PC. Reformatting your drive will not erase it! *WipeDrive* securely overwrites ALL hard drive data giving you the peace of mind you deserve."

*WipeDrive* does not run from within *Windows*. The *WipeDrive* program is

started by booting either from the bootable program CD or from a bootable floppy disk into its easily understood menu. The booting software is DR-DOS which may be changed to one of the MS-DOS programs if so desired. The floppy disk is created from the *WipeDrive* program CD in *Windows* format - a bootable *WipeDrive* floppy disk is not included in the package.

Once the *WipeDrive* program is booted it autoexec's to an intuitive, easy-to-use interface that allows users to:

- permanently overwrite hard drives and generate a log report;
- perform an unlimited number of disk wipes per license;
- configure custom overwriting patterns;
- overwrite hard drives as many times as needed according to organizational requirements and/or DoD standards;
- verify that 100 percent of the disk has been cleaned;
- erases all partition tables and drive formats - FAT16, FAT32, NTFS, and Linux.

The main menu gives you several choices including wiping drive(s), slow and fast verification for any remaining data, identification of the drives connected - drive manufacturer and serial number.

I had occasion to use the *WipeDrive* 3.0 program recently to erase several small hard drives that I was contributing to the local amnesty dumpster day project. All of the tested drives were smaller than 540 MB so took a relatively short amount of time to process (i.e., wipe) and gave me the opportunity to try several of the menu selections. In all it was a good experience and only one of the drives was uncooperative in

being cleaned (quite possibly my fault).

Additionally, I ran the *WipeDrive* program on a Maxtor 20GB (19.42GB net) 7200 rpm drive with times to accomplish the various wipe and verify functions listed as detailed below. Time and function info is from the log: (see table box below).

I did not attempt to run the 7 or 13 time pass as available from the standard menu for obvious time reasons.

As you can see from the above results, to wipe a 20GB drive three times and verify that data is nonexistent on all sectors takes approximately 6 hours. Wiping and verifying a larger drive could be an extended amount of

time.

WhiteCanyon's *WipeDrive* 3.0 software is available at \$39.95 for the individual user.

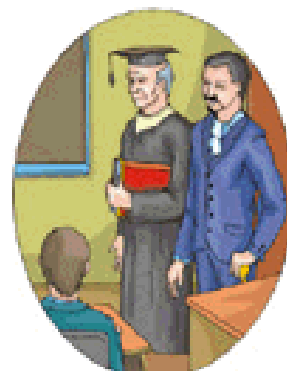
Note: the uncooperative drive was disassembled with the body, motor, heads and magnets going in one container and the circuit board and disks being held for disposition at a later time.

An additional source of information and software product links for drive wiping is: <http://dban.sourceforge.net/>

WhiteCanyon URL: [www.whitecanyon.com/wipedrive-erase-hard-drive.php](http://www.whitecanyon.com/wipedrive-erase-hard-drive.php)

Function:	Specification:	Total Elapsed Time: (HH:MM:SS)
Overwrite Disk	1 time	00:45:21
Overwrite Disk	3 times with verification (DoD 5220.22-M)	04:40:18
Quick Verify	Not all sectors examined	00:02:17

**Congratulations**  
to our own **Dr. Rick Fischer**  
on receiving national recognition as  
**Educator of the Year**  
by the Public Relations Society of America.



**Way to go, Rick!**

# Too Many Wrongs in Digital Rights

*Editorial*

by Gil Hennon

David Berlind is an editor at ZDNet.com. David is also a serious audiophile. He has, in round numbers so far, invested about \$20,000.00 in a state-of-the-art home music system that, when complete, should allow him to listen to his music collection in every room of his home. His plans include a central MP3 server that can send any song in his collection to any room in the house. David can listen to his favorite tunes as he moves between the den and his office while other family members listen to their own selections wherever they are in the home. That's a serious system, and David is serious about having the music he wants wherever he wants it. His plans include adding video distribution sometime in the future. And, for the kind of money he's investing, he certainly should get nothing less than excellent audio and video quality.

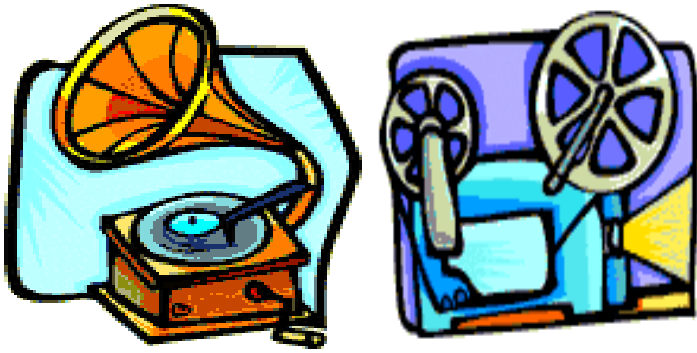
About a month ago, David found out that the sophisticated music system he has been working on for several years may already be obsolete. It doesn't conform to the new Digital Rights Management (DRM) requirements being imposed upon customers by the music industry. Even a simple 99 cent song from the Apple iTunes Music Store has a DRM "wrapper" that the equipment he has or plans to use can't decode. His research into how to accommodate the DRM encoded music and video files first appeared to be a matter of adding adapters for about \$500 per room. Besides being a very expensive solution that he preferred to avoid, David also found out that the decoding process can interfere with the quality of the music

or video. DRM is a very immature technology still plagued by problems for which there are currently no solutions.

DRM would not have inspired David Berlind to post several rants on his blog if it was only one of several alternatives for acquiring the music he wants. As long as he can find tapes, vinyl records, or CDs, he can convert songs to MP3 and preserve the quality level that the media allows. What bothers him, though, is that the entire music industry appears to be leaning toward DRM for all future products. He sees several serious consumer disadvantages in this direction.

There are many proprietary "versions" of DRM already being distributed. Apple iTunes is probably the best known and most popular. Several other vendors have their own DRM schemes, and none of these are compatible with each other. Until one of them emerges as a standard, the music market will be embroiled in a "Betamax vs. VHS" type of competition. What happens to the consumers who unluckily bet on the wrong DRM encoding? Very likely whatever they purchase today will not be supported as the losing vendors drop product lines or go bankrupt. DRM encoding is tightly bonded with specific playback equipment. If that equipment stops being manufactured, the music being sold today becomes worth about as much as an 8 track tape.

Similar thinking is going on in the video industry. Regional encoding (the CSS wrapper that prevents viewing a European DVD on an American player) was hacked by a fifteen-year-old several years ago, and some of the DVD player manufacturers no longer bother to install the regional filters in their equipment.



Since some movies have appeared available for download on fast, high-volume services such as BitTorrent, DRM has attracted the attention of Hollywood. An independent investigation found that over ten-thousand copies of the blockbuster movie, "Return of the King" had been downloaded in the several days before the movie opened in theaters. The piracy was too blatant to be overlooked, even though the same investigators concluded that the stolen copy of the finished movie was sneaked out of the distribution chain and onto the Internet by an insider employee of the studio. DRM or any other sort of encryption technology would have been useless to prevent this theft and piracy.

Another shortcoming of DRM that concerns David Berlind and many other music and video collectors is the likelihood that something in the complicated encryption-decryption process will go wrong and render purchased media worthless. Bugs and incompatibilities occur in every type of software and hardware that prevent legally purchased products from working correctly. At best, the vendor may refund the price of returned goods, but often the honest customer's equipment or other software is blamed for the glitch and the vendor accepts no responsibility. Equally unfair is the DRM scheme that intentionally sabotages the user's equipment or files without warning. TiVo added "content protection" to their units without any

notice to purchasers, then sold this protection to television studios. Most TiVo users had no idea what was going on when their unit failed to record some programs or automatically deleted previously recorded shows like "King of the Hill." Consumer advocacy Web sites have heard complaints about both unintentional and intentional vendor abuse too often to try to keep count. They cite these complaints as a primary reason for many former customers learning to deal with pirates.

Getting back to David's DRM rants, he makes a good case that DRM, in whatever form and from whatever vendor it comes, is actually Trojan Horse software, and in many cases it is also spyware. Like a Trojan program, DRM gives a vendor access into systems and equipment in your home and sometimes informs those vendors of what a user is doing. The rationale used to justify this behavior is the "license agreement" between the music or video vendor and the customer. Following the software industry's very successful use of End User License Agreements (EULAs) to limit their responsibility for defective products and usurp control of the product from the customer who bought and paid for it, entertainment media is now more often "licensed" than sold. By opening the package containing music or video media, the purchaser agrees to a variety of restrictions in return for a "license" to view or listen to the product. Typically these restrictions limit the kind of equipment that can be used to play the product, prohibit copying, even for archival purposes, and prohibit giving or selling the product to anyone else. Some licensing agreements contain clauses preventing the product from being inherited after the death of the owner. This restriction is unusual, but it is occasionally included in the license. More common is a clause in the license allow-

ing the vendor to retain control over the product and even to take the product back without compensation to the purchaser if the vendor believes the purchaser has violated any provision of the license. Like DRM, the license agreement is just another way to take control of the product away from the person who paid for it.

David Berlind also examines the long-term marketing implications of DRM. He notes that vendors use their licensing agreements to establish their right to change anything about the deal anytime they want. Already Apple has reduced from ten to seven the number of playlist installs a customer is allowed. Napster doesn't limit the playlist, but since it is a continuing subscription, rather than a single purchase service, access to all of the songs downloaded from Napster ends if the subscription fee is not paid. Close examination of the agreements of each online music provider reveal that many of the consumer rights we have come to expect are limited by DRM and license agreements. Since every online music provider's songs typically can be played only on a few proprietary devices, the sale of these songs practically guarantees the vendor future sales of devices and upgrades for those devices. In return for the privilege of listening to a song, customers usually must buy a special device and voluntarily agree to restrictions on their consumer rights. The vendors have figured out how to get the money and most of the benefits of the sale while incurring very little responsibility.

Probably very few online music and video customers consider these drawbacks when contemplating a purchase or service subscription. The prime consideration at that point is the desire for a song or movie, and not what is being given up in return for the opportunity to listen or watch. From January to June of 2005, digital music customers spent \$790 mil-

lion buying songs, more than three times the dollar amount of similar sales in the same period a year ago. So there isn't much customer concern. The DRM advocates, most of whom have ties to the recording and movie industries, also don't publicize what the customer is giving up. Instead, any advertising or press releases relating to DRM emphasize their efforts to prevent piracy. They also don't tell anyone that most of their anti-piracy schemes violate federal consumer protection laws, federal copyright laws, and occasionally the first amendment of the U. S. Constitution.

By accepting a licensing agreement (or a software EULA), a purchaser voluntarily gives up the right to the safeguards of most federal, state, and local consumer protection statutes, including the rights to return defective or unusable goods, to receive a refund of money paid, or hold the seller liable for damages and losses that are caused by the product or its use. If a similar contract were required for the purchase of most other goods, such as an automobile or food product, its doubtful any customer would be willing to continue with the transaction. Similarly, licenses or EULAs, including all DRM restrictions, completely ignore the "fair use" rights that have been an integral part of U. S. Copyright law for nearly 100 years, "Fair use" is a term the vendors hate. As a doctrine of law, it states that a person who honestly buys and pays for a product becomes the owner of that product. He or she has the right to complete use of that product and may dispose of the product when it is no longer needed. In other words, fair use" says that I own any copyrighted product that I paid for. I can make one or more copies as long as it is for my own use. I can give away or sell the product to someone else as long as I don't keep any copies for myself. You can bet that you won't be told that you are

being robbed of these “fair use” rights by any sellers of online digital music or video, but it’s still out-and-out thievery.

DRM grew out of the Digital Millennium Copyright Act (DMCA), an even less subtle affront to the rights of honest citizens. The law was passed by congress without any discussion, the result of extensive lobbying efforts by the movie and record industries. Having been almost entirely written by media industry lawyers, the DMCA is one-sided to the point of being perhaps the most abusive bill ever passed. It has, however, been almost completely ineffectual in securing the stranglehold on copyright law sought by the media moguls. Instead, the DMCA has been used to:

- Stop third-party ink cartridge fillers from competing with printer manufacturers
- Prevent game console users from making modifications to the circuitry
- Stop the reading out loud of books (specifically *Alice in Wonderland*)
- Prevent researchers who discover flaws in software from making those flaws public (especially the flaws in electronic voting software)
- Force dental school students to purchase textbooks on DVD that expire and become unreadable after a set period of time
- Stop libraries from making archival copies of difficult to obtain or no longer available content
- Restrict doctors and hospitals from “copying and forwarding” patient records
- Prevent the sharing of bankruptcy and credit fraud data between financial institutions
- Allow movie companies to use the “unskippable track” on DVDs for paid advertising (the track was intended for required copyright and legal notices)

Despite the diversity of situations to which the DMCA has been applied, most of the copyright related lawsuits based on the act failed to attain a judgment favorable to the media industry. DRM is only the latest incarnation of many years of effort to gut the copyright and consumer protection laws. There are currently more than fifteen different DRM schemes in use. Amazingly, only a couple were created by the media industry. In most instances, the industry took on a partner or become a content supplier to a large, powerful Internet provider or software development company where the song or video is packaged (put in an encoded wrapper) for online delivery. The very interesting twist in these arrangements is that the recording and movie industries, whose ultimate goal has always been to regain control of their content products, are now cheerfully handing that control over to companies who are their direct competitors in many other markets.

Hopefully the purchasing public will catch on that it is getting burned by DRM and voluntary licensing agreements. Hopefully “fair use” will survive the media industry onslaught and consumers will someday re-educate vendors that “the customer is always right.” Until then, DRM will make getting a fair and honest deal in the marketplace difficult for those who still care about ethical treatment. And somewhere along the line, perhaps the big music and movie moguls will get a taste of being on the receiving end of a raw deal. After all, the online providers and software development companies who are taking over the control and distribution of songs and video have many more years of experience with licensing and content restrictions. Hollywood and the record companies have put themselves in the hands of folks who are experts at sticking it to everyone else. If for no other reason, this will be an interesting farce to watch!

# September Meeting Report

## Windows Genuine Advantage



Microsoft Mindshare User Group support provided the presentation for the September meeting explaining how to participate in the Microsoft Genuine Advantage program and detailing the benefits participants can expect. At first glance, the Genuine Advantage program appears to be just another software anti-piracy scheme, but after ten months of testing and improving the process, Genuine Advantage achieves Microsoft's goal of reducing software piracy while enhancing the value of Genuine Microsoft products to the users.

The Genuine Advantage validation process is required when a user goes to the Microsoft download site, Windows Update, or the new Microsoft Update site. Validation is necessary in order to receive free, premium software add-ons, such as Media Player, Anti-Spyware, or Photo Story. Before the download begins, the validation process determines whether or not the user's system is Genuine Microsoft software.

The process does not collect any user identification data. In fact, Microsoft does not want to know the identity of users with pirated software. Individual users are not the targets Microsoft wants to prosecute. They have found that the majority of users with pirated software are unaware that they do not own genuine Microsoft products. They may have bought a computer with the software already loaded, or purchased a product through a channel that normally provides genuine software, and have been victimized, along with Microsoft, by the software pirates. It is those pirates, the thieves who sell thousands of copies of fake products, that Microsoft wants to identify and prosecute.

The Genuine Advantage validation process takes several minutes the first time it is done. Thereafter, when a user returns to a Microsoft site for another patch or add-on, the confirmation that the system has already been validated is nearly instantaneous.

Extensive testing has eliminated the chance for "false positives" in the validation process. If the system is found to have pirated software, Genuine Advantage displays a short explanation for why the software failed. The user has several options at that point. First would be to go back to the seller of the software and demand it be replaced with a genuine product. If that

### Memphis PC Users Group Membership Application

Date: \_\_\_/\_\_\_/\_\_\_ Membership # \_\_\_

Name: (Last) \_\_\_\_\_ (First) \_\_\_\_\_ M.I.) \_\_\_\_\_

Mailing Address: \_\_\_\_\_ Birth Date: \_\_\_/\_\_\_/\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_ - \_\_\_\_\_

Home Phone: (\_\_\_\_) \_\_\_\_\_ Business Phone: (\_\_\_\_) \_\_\_\_\_

Fax Number: (\_\_\_\_) \_\_\_\_\_ E-mail: \_\_\_\_\_

Employer: \_\_\_\_\_ Position: \_\_\_\_\_

Dues: \$35 per year

For office use only

Check#: \_\_\_\_\_ Amount: \_\_\_\_\_ Date: \_\_\_/\_\_\_/\_\_\_ Initials: \_\_\_\_\_

# Out for Review

can't be done, then the user can show Microsoft the install media, a store receipt, and give the details of how the software was obtained. If the user qualifies, Microsoft may assist the user in obtaining a license key or replacement software. As a final resort, the user can purchase and replace the pirated software with a genuine product from a Microsoft reseller. In any event, Microsoft will not prosecute any end users for having illegal software.

Microsoft has also decided that it will not withhold critical security patches from any user, whether or not the software on the system is genuine. Non-critical patches and free add-ons, however, will only be available to owners of Genuine Advantage validated PCs.

Microsoft Genuine Advantage is a no-risk opportunity for every user to know that a genuine copy of Windows is running on his or her computer. Once validated, the user can download Microsoft premium content add-ons that are available in no other way. Even if a PC fails the validation test, the process was anonymous and there will be no follow-up by Microsoft. There is plenty to gain and nothing to lose by participating in Microsoft's Genuine Advantage program. For more information and a FAQ about software piracy, visit <http://howtotell.com/windows>



Here is a list of software, books, or other products you can expect to see reviewed here in the coming months. These members checked out items to review for the benefit of all.

Windows Me: The Missing Manual	Greg Adams
Teach Yourself GoLive 5 in 24 Hours	Allison Banks
Teach Yourself Adobe Photoshop CS in 24 Hours	Judith Bogan
TIVO Hacks	Jacob Burke
Home Theater Hacks	Osborne Burks
Windows XP in a Snap	Vicki Dabney
Windows Security Handbook	Dorothy Drum
Smart Home Hacks	Megan Hefner
The Little Web Cam Book	Mike Heinrich
Microsoft Works 7.0	Jim Ingram
How to Use Microsoft FrontPage 2002	David Levine
The Complete Idiot's Guide to Starting A Business Online	David Levine
User Interface in C#	Jim McGee
Maximum PC 2005 Buyers Guide	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
Create Your Own Website	Jesse Strauch
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas
Using FileMaker 7	Tommy Towery

Thanks to all who checked out products for review. Let's keep the Group vital and provide value for membership.

For up to the minute information and special updates  
 be sure to check our Web site at:  
***www.mpcug.org***

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
Oct 2004	10  COLUMBUS DAY	11	12 	13	14	15
Oct 2005	17	18	19	20	21	22 INVESTMENT
Oct 2005	24 CLIPPER 	25	26 MAIN MEETING	27	28	29
Oct- Nov 2005	31 	1	2	3	4	5 INTERNET HARDWARE
Nov 2005	7	8	9	10	11 	12 WEB WRITERS MS OFFICE
Nov 2005	14	15	16	17	18	19