

The Bridge

The Journal of the Memphis PC Users Group

Volume 19 Number 8

August 2003

For group information
please visit our Web site:
www.mpcug.org

The Bridge Staff:

Editor
Gil Hennon

Review Editor
Rick Fischer

Publisher Emeritus
Les Owen

In This Issue

The School Bell	Page 2
Easy Create CDs & DVDs	Page 4
Outlook Pocket Guide	Page 5
Out for Review	Page 6
Review Editor's Notebook	Page 6
A Whole Lotta' Hackin'	Page 7
SIG News	Page 10
Please Help	Page 10
Wizard's Tips	Page 11
Event Calendar	Page 12

Main Meeting Wednesday, August 27 Southwest Tennessee Community College

5983 Macon Cove, Memphis

MEETING LOCATION Farris Auditorium

First Floor - Farris Building

New Users & Wizards 6:30 p.m. Main Meeting 7:30 p.m.

We went to press without firm plans for the August meeting. Something interesting always turns up, so come on out and see what happens!



Bring a friend along!



The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

I finally broke down and bought a big hard drive. 120 gigabytes. It almost boggles the mind to consider that the thing is capable of holding 128,849,018,880 individual characters. Only ten years ago, hard drive sizes were in the hundreds of megabytes, and most operating systems couldn't yet address storage beyond 200 megabytes without the help of tricky boot sector utilities.

The big drive replaced three smaller ones, eight, fifteen, and thirteen gigabytes each, that had been respectively my C:, D:, and E: volumes. The changeover wasn't quick and easy, but more about that later. Increasing my storage capacity by about five times got me thinking about how we measure computer-related capacities, and what size hard drives we would probably be using ten years from now.

A gigabyte is nominally 10 raised to the ninth power and most of us consider it to be a billion bytes. But because the base measurement is a kilobyte, which is 1,024 bytes and a power of two, multiplying by tens isn't quite accurate. Calculating a gigabyte as two raised to the 30th power is accurate, and yields the correct number of bytes: 1,073,741,824. The next iteration in size past a gigabyte is a terabyte. Again, it's easier to think of it as a trillion bytes than to try to remember that a terabyte is actually 1,099, 511,627,776 bytes. Here's a table that covers several magnitudes.

<u>Prefix</u>	<u>Symbol</u>	<u>Power of 10</u>	<u>Power of 2</u>	<u>bytes</u>
kilo-	k	10 ³	2 ¹⁰	1,024
mega-	M	10 ⁶	2 ²⁰	1,048,576
giga-	G	10 ⁹	2 ³⁰	1,073,741,824
tera-	T	10 ¹²	2 ⁴⁰	1,099,511,627,776
peta-	P	10 ¹⁵	2 ⁵⁰	1,125,899,906,842,624
exa-	E	10 ¹⁸	2 ⁶⁰	My calculator coughed and died!
zetta-	Z	10 ²¹	2 ⁷⁰	
yotta-	Y	10 ²⁴	2 ⁸⁰	

Beyond a yottabyte the terms are undefined until we reach a google (10¹⁰⁰ or 10 with 100 zeroes behind it) and then a googleplex ((10¹⁰)¹⁰⁰). You can figure out that number for yourself. My brain is starting to ache. I would probably be safe in predicting that I probably won't see a googleplexbyte hard drive in my lifetime, but I'm not going to do that. After all, Bill Gates once said that 256k of memory was more than enough for any task that could ever be done on a computer.

Now, about that big hard drive—I had a few problems installing it. The drive specification was "Ultra ATA," and my computer was just old enough to not recognize the spec or the large size. It is a Pentium III 500MHz, which is still speedy enough for anything that I do, but

the BIOS was about three years old. So I went to the ASUS Web site, downloaded the most recent BIOS, and flashed it into my machine. It had an improvement that speeds up the boot process and a couple of other enhancements, but support for Ultra ATA and big storage devices was not in there. My computer could see the new drive, but it believed that the capacity was 7.8 gigabytes.

The drive manufacturer knew this was going to happen. There is a page on the Web site addressing the exact problem I was having. It suggested a BIOS upgrade, which already hadn't worked, and then some creative jumpering on the drive, which also made no big difference. Next to try was installing the Ultra ATA Management utility furnished by the drive manufacturer on a diskette. The utility made a noble effort, but my operating system didn't like that solution.

The final resort, which did the trick, was to purchase and install an Ultra ATA controller card. This added \$30 to my cost for the drive, but it works perfectly. The card has its own BIOS that handles the addressing of the large drive, and as an added bonus, it has a large cache, so the drive reads ahead and puts a very noticeable zip into data retrieval intense tasks. I'm very happy with the final solution.

If your computer is two years old or less, it will probably install a large Ultra ATA hard drive without any complaints. Otherwise, I wouldn't bother with weird combinations of jumpers or diskette utilities. Get a controller card that handles the drive without any tricks. If you have a choice between 100 and 133 bus speed on the controller card, take the 133. It is backward compatible, so it can handle any ATA drive and costs only a couple of bucks more.

We may not have a googleplex of tips for computing at MPCUG Education Services, but the ones we have got are tried, tested, and successful. Join the Wizard Session each month immediately before the main meeting. You'll save yourself yotta-yotta-problems!

*The two most abundant
things in the universe are
Hydrogen and stupidity.
- Harlan Ellison*

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.
P.O. Box 241756
Memphis, TN 38124-1756
Internet: www.mpcug.org
Information Line: 901-375-4316

Easy Creating CDs & DVDs

Book Review

Reviewed by John Schuster

Generally, Que publishes very informative, adult oriented computer books. In this case, my first impression is that the word "Primer" ought to be in the title.

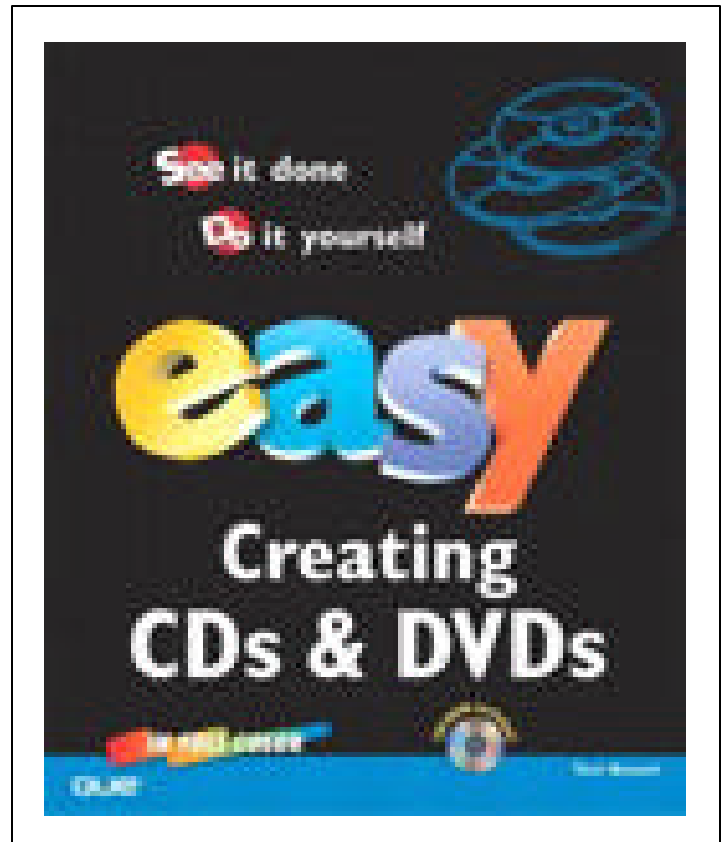
This is a step-by-step guide to creating all the various types of projects available for CDs and DVDs. It is heavy on pictures and light on text (See Dick click. See Jane drag.).

There are, also, holes in the coverage. On page 40, in the section on creating enhanced CD with *Easy CD Creator*, it states, "Notice the two blank folders ready to accept CD Plus data or Pictures (we'll cover those shortly)." Shortly must be in the next volume, because, they never do address these issues. A quick Google search found the following information from a Roxio PDF file: "**Note** The CDPLUS and PICTURES folders in the Data Project are automatically created and are required for making an Enhanced CD." This promise of a follow-up, with no fulfillment, shows me that this book has been written with insufficient attention to detail.

In defense of this book, I must say that the topics are covered in a detailed fashion and, where it is important, with full detail. There is also coverage of both Roxio's *Easy CD Creator* and Ahead's *Nero Burning ROM*, as well as Ulead's *Movie Factory 2.0*.

One of the best chapters is the "Hints and Tips," which includes using *Windows Media Player* to manage audio playlists, how to make an autoplay CD and many several other useful tidbits.

Also included is a CD containing trials versions of *Nero 5.5*, Ulead *MovieFactory 2.0* and Ulead *Cool 3D* as well as examples



to be used with the later parts of the book.

I would recommend this book to any 8-14 year-old **novice** to the art of creating CDs and DVDs (Que's website does state that this is a **beginner's** guide). Anyone older than that can, probably, manage quite well from the help files, which accompany each program and save the \$19.99 (plus tax) which is the suggested retail price of this book (I found it as low as \$13.99 on the Web).

Easy Creating CDs & DVDs
by Tom Bunzel.
Que Publishing.
www.quepublishing.com

Outlook Pocket Guide

Book Review

Reviewed by Rick Fischer

Can you believe it? I read the Pocket Guide from cover to cover. The plot was thin and I already knew the ending.

But, the characters (*Outlook* functions and features) are rich and complex. And, I had forgotten much of what those functions and features could do.

A good bit of the book has highlighter marks. Now, I'll come back with *Outlook* running to see for myself what I have been missing.

The pocket guide series is designed for the person on the go. The book is small. It could easily fit in a carrying case with your laptop, or out of the way on your desk. It is NOT a coffee table book.

What's inside?

After the overview you step through the functions, e.g., e-mail, contacts, calendar, notes and so on one by one. Chapters focusing on the functions and features are organized around a central theme: "How do I . . ."

So the organizing structure is topical and functional. When you are

busy you want answers to your questions – fast. That's what you get.

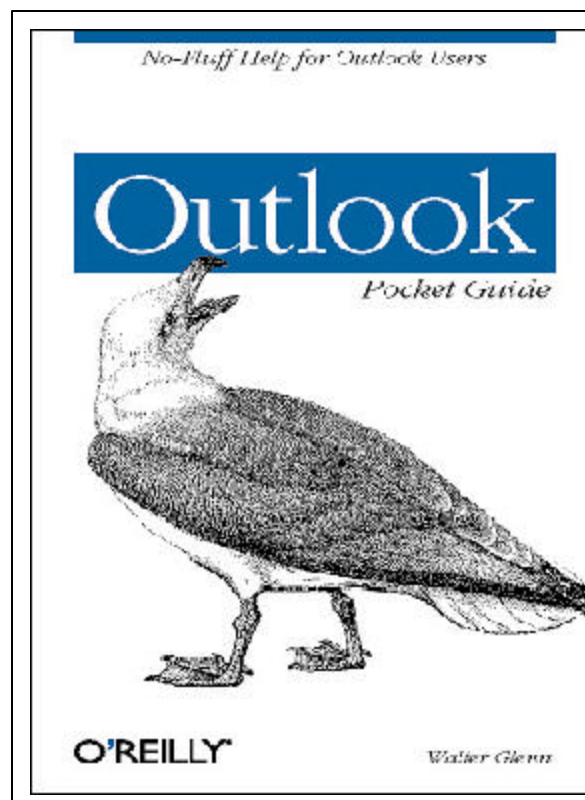
Will your question be in here? It's highly likely. I got answers to questions I didn't know I should ask. And, I have leads on getting the answer as to why I have some buttons on my toolbar at home while, so far, have been unable to find them to customize *Outlook* at work.

The last chapter is worth your attention. It outlines Web sites and newsletters (including Wood's Watch) where you can get more information

on *Outlook*. Glenn also reviews nine add-on tools for *Outlook*, describing what each does and offering the URL where you can download it. That's real added value.

Outlook Pocket Guide by Walter Glenn. O'Reilly. 2003. 186 pp. \$13.

O'Reilly User Group Discount. 20% on all O'Reilly books and conferences when you order direct. Include your User Group code: **DSUG**
www.oreilly.com



Out for review

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
Teach Yourself GoLive 5 in 24 Hours
Spell Catcher
Civilization: Call to Power
Microsoft Personal Collection 2002
Links 2003
Microsoft Office 2000 8 in 1
Windows Security Handbook
The Little Web Cam Book
Microsoft Works 7.0
How to Use Microsoft FrontPage 2002
The Complete Idiot's Guide to Starting
 A Business Online
Space Bunnies Must Die (game)
Sin (game)
X-Wing vs Tie Fighter
Star Wars: Behind the Magic
Extreme Tennis
Photoshop Type Effects
Teach Yourself ASP.net in 24 Hours
Sportsman's Challenge
Top Shot
Using MS Windows 2000 Prof
FrontPage for Win 2000 (book)
Microsoft Money 2002 Deluxe
Windows XP Pro (book)
FrontPage 2002 Unleashed
Macromedia (book)
Image Broadway
Windows XP (book)

Greg Adams
Allison Banks
Deborah Hart-Curtis
Morgan Curtis
John Dodson
Mike Dudas
Dorothy Drum
Dorothy Drum
Mike Heinrich
Jim Ingram
David Levine
David Levine

Adam Locke
Adam Locke
Adam Locke
Adam Locke
Adam Locke
Bill Luber
Jim McGee
Kim McNeil
Paul Merz
Eric Miles
Lee Mouring
Vanessa Muldrow
Daniel Notowitz
Carl Osborne
David Stowell
George Stringham
Terry Thomas

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

Review Editor's Notebook

Congratulations to John Schuster who will complete 51 reviews with this issue. One of the great benefits of membership is being able to read the latest computer books and try out new software — for free.

Gil Hennon now had 44 completed reviews and Jack Merrill has 16. Bill Luber is active with 11. Thad Craig is a new reviewer with three already this year.

We have published 1,022 reviews in The Bridge since it was launched in 1987.

Rick Fischer
Reviews Editor

(Editor's addition: Rick didn't mention how many reviews he has done. As the Reviews Editor, he not only coordinates the efforts of all of the other reviewers, but also reviews many books and products himself. Often these are ones not taken by any other reviewer. I'm sure his numbers are as impressive as those he congratulates! If you haven't reviewed any software lately, take a look at what Rick has to offer. You get to keep the software, you perform a service for your fellow members, and you get a break from seeing the same old stuff day after day. It's a really good deal!)

A Whole Lotta Hackin' Goin' On!

Editorial

by Gil Hennon

One of the rituals of summer in Las Vegas is the annual DEFCON hacker convention. Maybe it should be called an information security convention. The hackers are not the majority of attendees anymore. One of the reporters covering the event remarked that there are four distinct groups at a DEFCON convention. Some hackers still attend. They are the ones wearing suits and ties. The largest group now are security professionals, mostly corporate, but a handful also from government and military organizations. They are the ones wearing Dockers and Land's End casual wear. A growing group each year are the investigators—FBI agents, U. S. Marshals, and probably this year, a few from Homeland Security. They are the ones wearing tie-dyes, cutoffs, and bandana headbands. The last group is his own, the journalists. They don't dress in any particular manner, but can still be recognized by their blank expressions. They don't understand a word that is spoken in the conferences and speeches, but they get a kick out of watching the other three groups try to avoid each other.

DEFCON, you may remember, was where Dmitry Sklyrov, the Russian programmer, delivered the keynote address, then was arrested by the U. S. Justice Department for violating the Digital Millennium Copyright Act. After our Federal Government spent a couple million in tax dollars prosecuting Dmitry, a San Francisco jury acquitted him of all charges. They said the case against him was so disorganized and confusing, that even the Federal Prosecutors contradicted themselves trying to explain to the jury why Dmitry was on trial.



Another notable DEFCON of the past was when the hacker community "Cult of the Mad Cow" dropped a news bombshell announcing that they were reorganizing into a security consulting business and their *Back Orifice* software product would henceforth be offered on the commercial market. Back Orifice was, at the time, one of the best tools for remotely managing distant computers from across a network. It may still be one of the best, but it has not achieved popularity. Information security professionals, aware of the product's sinister origin, are still skittish about using it.

DEFCON number 11 in 2003 had all of the fun that hackers love. For the first three days of August, individuals and teams competed to see who could come up with the best slogan, who could rack up the highest wardriving score, and who could break into a firewalled and fortified server the quickest. There were lots of other challenges too, including an old fashioned scavenger hunt through the neighborhoods of Las Vegas, but along with the fun and entertainment, DEFCON also has a serious side. Several security and computer "self defense" organizations hold their sessions and technical

briefings during the DEFCON event.

This year I received an invitation to attend the Black Hat 2003 Briefings, several days of educational sessions dealing with serious hacking and the technical aspects of computer security threats. I didn't go. It wasn't a travel and expense paid invitation; they wanted money before they would put up with me. Our household was also sawing and hauling fallen trees out of the yard about that time, so a trip to Las Vegas would have sounded more like an excuse than a necessity. But I was intrigued by the electronic brochure they sent via email. The course list sounded like graduate studies at the University of the Underworld. Here are some examples:

- Infrastructure attacks
- Ultimate hacking
- Hacking by the numbers: Combat edition
- Forensic tools for opening Windows XP platforms
- Steganography training
- Offensive rootkit technology
- Hacking Cisco networks

Some security professionals have complained about Black Hat offering training in these and other shady endeavors. The DEFCON associated group that provides the curriculum emphasizes that these courses are intended for security professionals to understand the threats they will face, but they do not limit attendance to those who work in computer security related jobs. The Black Hat instructors took some criticism because there were obviously some hackers in their classes.

Was that bad? Although the majority opinion seems to believe so, I personally don't think we need to worry about any hackers who are open enough about what they do to attend public classes under the

noses of several law enforcement agencies. They also paid a respectable amount of tuition, travel, and living expenses, even if we don't count what they left in the Vegas casinos. That indicates that they probably don't entertain intentions of using their new knowledge frivolously. Most likely they are about to make the jump into the legitimate occupation of security consultant.

Hackers might be annoying, and the less mature ones can be destructive, but we owe a lot of the conveniences we use everyday to them. For instance, we all know that worms are bad little programs that travel around on networks to collect passwords and credit card account numbers. But when we call a worm a "search engine," it doesn't sound like such a threat, and we all use this type of worm regularly and with complete confidence. Likewise, viruses are bad. They are semi-intelligent, capable of entering systems secretly, and possibly can cause a lot of mischief or destruction. Viruses have useful cousins, though, called "agents." If you hang out around Ebay or Yahoo auctions, you have probably used one of their agents to notify you when a higher bid has been placed on an item you want. Other agents can be set to recognize a specific event, like a package you shipped being delivered, and the agent will notify you when that happens. Worms and viruses are bad. Search engines and agents are good. All of them are the result of hacker research and development.

There are also good hackers. I used to say I was a hacker until the media put a bad spin on the term. Back in the sixties and seventies, someone would stop and look over a programmer's shoulder and ask, "What are you doing?" Fairly often the answer would be, "I'm hacking out a program that will . . ." and a discourse on the value of having that done by a computer would begin. In the mid-seventies,

Byte Magazine observed that those involved in many technical pastimes were known by nicknames. Radio enthusiasts were called "hams," and so on. They ran a contest to find a nickname for computer enthusiasts, and the overwhelming preference was "hackers." It wasn't until an uninformed news reporter called a computer criminal a "hacker" that the term got an undeserved bad reputation. Journalists love new buzz-words, and the misuse of "hacker" moved at the speed of light across the media.

In spite of the term's current unsavory connotation, there are hackers who use their talents to keep all of us out of big trouble. They pick apart the code and architecture of operating systems and applications, searching for vulnerabilities that a bad hacker can exploit. The big software development houses have been less than appreciative most of the times when a "white hat" hacker informs them of a fault in their code. That's understandable, since no one likes being told that their baby is ugly. Fault notification gives the software developer a chance to plug code holes before they cause big problems. When the "white hat" hackers were ignored, users became victims to malicious intrusions such as *Code Red* and *Nimda*. I'd like to see more "white hat" hackers taking Black Hat training courses, and I'd like to see the "white hat" hackers' discoveries taken seriously.

Obviously, there could be a bad hacker taking the Black Hat classes. There might be a terrorist at the airport and a Unabomber at the Post Office too. I hope we are not ready to deny information to someone based on nothing but suspicion. Of the hackers (according to the current definition) that I know, most tired quickly of coding pranks and malware. These are smart people with a hunger for knowledge. They tend to mature into responsible innovators and make worthwhile

contributions to the computing community. If anything, let's help the immature pranksters to get through that phase of their existence more quickly!

One of the courses in the Black Hat list addressed a technology that is getting lots of attention lately. Rootkits have been known to UNIX and Linux system programmers for quite some time, but only in the last year have become interesting to Windows hackers. Rootkits are programs that modify important system files so that they can run invisibly. A rootkit can, theoretically, perform any function that the operating system can perform. It hooks system calls and interrupts. It can hide directories, files, registry entries, or processes, and can change the privileges that a process, user, or group normally inherits.

Rootkits use a complex technology called "Direct kernel object manipulation," which is a long-winded way of saying that the basic component of the operating system is being modified or impersonated. Since they place themselves in a position to watch everything that goes on inside a computer, rootkits are very good at hiding. Scan engines of the sort used to detect viruses and spybot software are seldom useful against rootkits. When the rootkit observes that something is looking around, it hooks the searching call and returns a message to the scanner that "no rootkits are around here!"

Finding a rootkit on your computer could be done by comparing the checksum or CRC of a system file before and after it has been modified by the rootkit. Some rootkits don't modify system files, though, and may only be noticed because a little bit less memory is available than ought to be there. When it doesn't want to be found, a rootkit hides extremely well.

Fortunately, a rootkit has to be in-

stalled on a system before it can compromise it. Like many viruses and worms, it could arrive as an attachment to an email message. We all know not to fall for that one, don't we? More dangerously, the rootkit could be present in software that we install intentionally. Most software manufacturers have safeguards in place to keep tag-along malware from showing up in packaged commercial software, but there is always the exception. Even more likely would be a rootkit embedded in software we download or install across the Internet. In this case, knowing and trusting the software source is all-important.

Chances are that if you have the proper safeguards to protect you from viruses, Trojans, worms, spy-bots, and scumware, you are probably reasonably safe from rootkits. Don't be surprised if you hear more about them though. The bad hacker community has noticed rootkits and found them fascinating.

For more information about DEFCON and the "post event" synopsis, go to <http://www.defcon.org>. If you plan to spend much time there, you need to find yourself a name like "rotbottom" or "weaselboy." The Black Hat site is a bit more dignified and intensely technical at <http://www.blackhat.com>. Finally, if rootkits intrigue you, download a few at <http://www.rootkit.com>. Just be sure you understand what you are getting and what they are supposed to do before installing any of them.

On the lighter side of DEFCON, the slogan contest was one of several events in which every attendee could participate, regardless of the level of hacking expertise. Two of the three winners were "Plead the First!" and "Don't hack the best. Be the best!" For those of you into wardriving, the other winner was "216.231.63.34 36.10778N 115.15717W 20030801 ANY QUESTIONS?"

SIG News

Word Perfect SIG News

by Maury Ellis

The Word Perfect SIG held its regular meeting July 21 at the White Station Library. Several short cuts and procedural tips were demonstrated. There were several operating questions discussed. Several of the members met for dinner at the New Hunan Restaurant.

What's your SIG doing?

Let us know!

Just send a couple of lines about each month's meeting. There may be folks who would attend if they knew the kind of interesting things your SIG does!

Please Help

The MPCUG receives requests from local organizations looking for used computers and printers that individuals are willing to donate. We get requests from churches, schools, communities, and charities. If you have an old Pentium 300MHz or higher in operating condition or a working laser/ink jet printer that you no longer use and are willing to donate, we will try to match you with a recipient in need of equipment.

Currently we have requests from two churches and the Collierville Food Pantry.

Please contact:

Gil Hennon gil@ahls.us

or

Jim McGee jim_mac@bellsouth.net

The WIZARD's Font Tips



1. Windows has a limit of 1,000 fonts.
2. Users can manage fonts by clicking FONTS in the CONTROL PANEL.
3. If you remove a font, it goes to the Recycle Bin. If you expect you will put a font back into the system later, copy it in another directory before removing it.
4. To install a new font, choose Install New Font from the FILE menu. In the Add Fonts box, browse to find the new font file location. Leave the "Copy Fonts to Fonts Folder" box checked. Keeping fonts anywhere other than the default folder causes the path to be stored with the font name, possibly reducing the number of fonts that can be installed below 1000.
5. Double click any font name to see the font's catalog sample page. You can print these pages for fonts you use often and make your own typesetting book.
6. If you have a lot of fonts in the Fonts Folder, select VIEW and HIDE VARIATIONS. This causes the list to show only font family names, such as ARIAL, but not all the different varieties of ARIAL, such as Black, Narrow, etc.
7. Select VIEW and LIST FONTS BY SIMILARITY to get a list of fonts that are close in appearance to the font currently highlighted. This works only for fonts that have a "PANOSE" number, which is calculated from the font's characteristics.
8. All of the above works for True Type fonts. If you have third-party fonts, manage them using the font utility that came with them.

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: _____

**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
AUG 2003	4	5 DOT.NET	6	7	8	9 WEB WRITERS MS OFFICE
AUG 2003	11	12	13	14 VISUAL STUDIO	15	16
AUG 2003	18 WORD PERFECT	19	20	21	22	23 INVESTMENTS
AUG 2003	25 CLIPPER	26	27 MAIN MEETING	28	29	30
SEP 2003	1	2 DOT.NET	3	4	5	6 INTERNET HARDWARE
SEP 2003	8	9	10	11 VISUAL STUDIO	12	13 WEB WRITERS MS OFFICE