

Official Newsletter  
SouthEastern Michigan  
Computer Organization, Inc.

# DATA BUS

---

Volume 33

June 2008

Number 6

---

## IN THIS ISSUE

Deals Column, by Bob (The Cheapskate) Click .....	3
Secure Your Wireless Network, by Ira Wilsker .....	6
Internet Security iFrame Attacks, by Brian K. Lewis .....	8
Google Releases Updated Version of "Google Earth," by Ira Wilsker .....	11
Scotty, I Need More Power, by Alan Mildwurm .....	13
Meeting Pictures .....	16
Board Meeting Minutes, by Carol Sanzi .....	18
Geohashing!, by Warner Mach .....	18
SIGS: IBM, IBM Intermediate, Advanced, & Novice IBM Group .....	19
DATA BUS Deadline .....	19
Other Groups Calendar of Events .....	20
Computer Resource People .....	21
SEMCO Calendar .....	22
Map & Directions to SEMCO Meeting at ArvinMeritor Building .....	23

## SEMCO OFFICERS

President	Mike Bader	(586) 573-7330
Vice-President	Richard Jackson	(248) 546-3694
Secretary	Carol Sanzi	(586) 739-7256
Treasurer	Bette Gay	(248) 641-7799
Members-at-Large of the Board of Directors	Bob Clyne	(810) 387-3101
	Charles Moery E-Mail	< <a href="mailto:keypounder2@aol.com">keypounder2@aol.com</a> >

## NEWSLETTER STAFF

Publications Committee Chair	Warner Mach	(734) 326-0733
Editor	Warner Mach	(734) 326-0733
Proofreader	Beth Fordyce	(734) 453-0349
Proofreader	Fred Acerri	E-Mail < <a href="mailto:acerri@att.net">acerri@att.net</a> >

## SIG (SPECIAL INTEREST GROUP) CHAIRPERSONS

SIG-IBM: Chairman	Tom Callow	(248) 642-5770 (9-5)
SIG-IBM INTERMEDIATE	Open Position	
NOVICE-IBM GROUP	Rotating Hosts	
SIG-ADVANCED	Franz Breidenich	(248) 398-3359

The SouthEastern Michigan Computer Organization, Inc. (SEMCO) is a non-profit, 501(c)(3), group dedicated to providing information, education and a forum to computer users (professional and amateur) and other interested individuals. Membership in SEMCO is open to all individuals 18 years or older. Persons under 18 years may become members through the sponsorship of a parent or guardian. Dues of \$30/year include monthly DATA BUS and free personal ads.

**All SEMCO correspondence should be addressed to**

**SEMCO - P.O. Box 707 - Bloomfield Hills, MI 48303-0707**

Web site: <http://www.semco.org>

E-mail: [semco@semco.org](mailto:semco@semco.org)

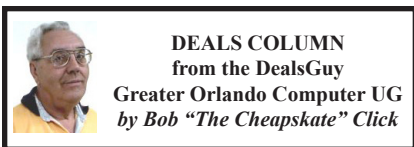
General information: (voice) answering device in Royal Oak **(248) 398-7560**

DATA BUS is published monthly by SouthEastern Michigan Computer Organization, Inc. (SEMCO) as its official newsletter. **Mail DATA BUS newsletter copy to: Warner Mach, 1360 N. Hix Rd., Westland, MI 48185; or e-mail: [machw@att.net](mailto:machw@att.net).** The Editor is responsible for contents and control of the DATA BUS. Materials published herein may be used for non-commercial purposes only, without further permission of SEMCO or the authors, except as noted, providing credit is given to the author and source, i.e. DATA BUS, and issue date. Entire contents copyright © 2008 SouthEastern Michigan Computer Organization, Inc.

SEMCO does not condone in any way the illegal copying of copyrighted material and will not tolerate such practice at any SEMCO function.

Your mailing label and membership card list the month and year your membership expires. Newsletters will not be sent after the month of expiration. Back issues may not be available. Renew your membership as early as possible.

This publication was created using Adobe InDesign CS2  
donated by Adobe Systems, Inc.



### **Friends Helping Friends!**

A friend uses his computer a lot, but doesn't belong to any computer organization. I gave him a couple of PC Magazines I had read and he enjoyed them enough that he subscribed. He mentioned that he had a problem with his laptop not connecting to the router and I told him about the tech support included with the PC Magazine subscription he had just purchased. He called them and they helped him fix the problem quickly. His words later were "Boy; I've already gotten my subscription money back in just one day."

### **Eat Or Be Eaten**

I saw where EMC will acquire Iomega. Although it is taking much longer than he said, Ralph Nader said years ago that in 20 years most of the business in the US will be controlled by 20 or so large corporations, and it looks like that prediction is gradually taking place. Small startups that have a unique product are quickly scooped up by the big guys who also buy their competition to close it down. That's certainly a good way for a smart programmer to become a millionaire; just come up with a great idea that works. As for being bought up, foreign countries will soon own the US by repossessing us if we keep borrowing money from them.

The items below are announcements I received, but I have necessarily edited the wording. I have not tried any of the products.

### **Free Tutoring For The Uninformed**

Output I/S has launched HTML.net, a free HTML and CSS tutorial site that

makes it easy to learn how to design and develop web sites. In about an hour, novice computer users can learn the essential information needed to build a web site using nothing more than an ordinary text editor. The Hypertext Markup Language (HTML) tutorial begins with the basics and introduces you to links, images and tables. You'll learn how to develop a site that can be viewed by all web browsers on all platforms. There are tips and tricks to make your web site attractive, fast loading, and effective.

The Cascading Style Sheets (CSS) tutorial teaches you to separate your web site content from your design, enabling you to quickly change the look and feel of your web site. CSS-based web sites improve your search engine rankings by making it easier for search engines to find and index your content. CSS is slowly replacing table-based HTML as the design tool of choice. The HTML.net tutorials are available 24/7, without charge. Tutorials are in English, German, Spanish, French, Italian, Russian, Chinese, and more.

For more information, visit <http://www.html.net/>, or contact Output I/S, Kaj Munks Vej 10, 3.th, 2300 Copenhagen S, Denmark. Phone: (+45) 5194 5001. E-mail: [info@output.dk](mailto:info@output.dk).

### **Free Screensaver**

DealsGuy note: I am always suspicious of screensavers and I don't even use them myself, but my proofreader found some decent reviews of the companion game from the same author, so this screensaver is probably OK.

A sweet and adorable fairy soars across a beautiful fantasy landscape. Along the way, she uses dazzling spells to defend herself against evil goblins and

blazing firebirds. This delightful visual feast is the free Feyruna Fairy Forest screensaver from Jochen Kaercher Gamedesign, creator of premium games for casual players.

Fairy Forest screensaver includes the option to turn on atmospheric music and sound effects. As viewers listen to the soothing audio, they're treated to smoothly animated scenes featuring the otherworldly artwork of Feyruna Fairy Forest, a casual game created by Jochen Kaercher Gamedesign. Visit <<http://www.feyruna.com>> to download the 13 MB installation file and begin enjoying the free Feyruna Fairy Forest screensaver. Windows 95 or later is required.

Jochen Kaercher is an experienced game developer based in Germany. After launching his company in 1999, he created several freeware and shareware offerings for the PC. Kaercher is now developing more ambitious titles aimed at casual gamers. All offerings can be downloaded from <<http://www.jochenkaercher.com>>.

### **Free USB Protection**

A.C. Element Company has made available the free version of MyUSBOnly for individual users. MyUSBOnly Free 2007 is a Windows security application that prevents data theft through your computer's USB ports. While USB ports have made computing much more convenient, they also introduce a security threat that could subject many computer users to identity theft and data theft. MyUSBOnly thwarts attempts to gain access to your computer via your USB ports.

New features for MyUSBOnly Free 2007 are:

- Syslog entries for copied, modified, deleted files/folders

- Firewall-like feature to allow/deny inserted USB devices

It acts as something similar to a firewall that monitors the USB ports for any storage device connected to the protected computer. Simply create a whitelist of all of the USB devices you want to allow on your computer. The program will recognize each of your flash drives, external disk drives, MP3 players, and other USB devices and add them to its list of accepted hardware once they are authorized by the user. When your list is complete, the software will then check the whitelist of allowed devices by USB brand (if you want to allow a certain USB brand) or by serial number (for specific USB devices you want to allow) depending on the settings desired by the user.

The software also has reporting features, such as e-mail notifications, each time somebody attaches a USB device to your desktop or laptop. MyUSBOnly also maintains a security log of all attempts to gain access to your computer via USB flash drives, iPods, card-readers, or any USB hardware. Modified and copied files are now included in the log entries and can be configured to send all log information to syslog. Use syslog viewers such as Kiwi Syslog Daemon TM to view all the log entries from one or more computers in the network, allowing administrators to be able to manage and audit security.

There is an option to hide the software from the user, by not displaying any tray icons at all, so it silently works in the background without the user even knowing it's there. MyUSBOnly makes it easy to lock down your USB ports to protect this critical vulnerability on your desktop or laptop.

MyUSBOnly runs under Windows 2000/XP/2003/Vista/Server 2008, Download the software from the website <<http://www.myusbonly.com/usb/free.php>>. DealsGuy note: My proofreader noted some contradictions in the Web site information so look closely and clarify what you don't understand by trying the trial version before buying.

### **Jigsaw Puzzles**

Like Jigsaw Puzzles? Try This One! They claim, "It is even possible to see and feel the cardboard thickness," but I am skeptical about feeling the cardboard thickness on the screen.

Gaia Dream Creation Inc. released its new 3D jigsaw puzzle game, and a puzzle screensaver named "Gaia 3D Puzzle" and "Gaia 3D Puzzle Screensaver." This 3D jigsaw puzzle game allows players to play jigsaw puzzles on their computer by selecting their favorite images and the number of pieces. The 3D view creates a totally immersive playing experience like a real puzzle game.

Gaia 3D Puzzle allows players to play with almost any images found on the Internet. Unlike other computer puzzle games, Gaia 3D Puzzle is in 3D. Players can see their puzzle as a real jigsaw puzzle and the pieces are as real as true jigsaw pieces. The pieces are not pre-cut image shapes. They are generated from advanced mathematical procedures to show the exact look and feel of true jigsaw pieces. It is even possible to see and feel the cardboard thickness. Players are able to play puzzles from 9 to 2000 pieces. Children can play and enjoy the same puzzles that adults play, but with less pieces.

A selection of 4 different piece shapes is available which increases or decreases the difficulty level. It's

also possible to modify the degree of distortion in the pieces, meaning the pieces can all look the same, which is harder to play, or all look different, which is easier to play.

The puzzle game and screensaver are available in English and French for Windows 2000/XP/Vista. The puzzle game (Gaia 3D Puzzle) is \$29.95 USD and the screensaver (Gaia 3D Puzzle Screensaver) is \$14.95 USD. 20% is offered to DealsGuy readers with coupon code GAIA-XAKB-USAV. This code is valid until June 30th, 2008. You must download the trial version to make sure it works well on your system and that you are satisfied, then follow the URL in the product to pay using the discount code.

Website: <<http://www.gaiadreamcreation.com/games/gaia-3d-puzzle/>>. Screensaver: <<http://www.gaiadreamcreation.com/screensavers/gaia-3d-puzzle-screensaver/>>.

*That's it for this month. I'll soon have some new product announcements on my Web site. 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](mailto:bobclick@mindspring.com)>. Visit my Web site at <<http://www.dealsguy.com>>.*





## **Secure Your Wireless Network**

**By Ira Wilsker**

Many of us have wireless networks (Wi-Fi) at home, and often use other wireless networks at the office, coffee shops, restaurants, hotels, airports, and a variety of other places. Many of us blissfully connect to whatever network is available, either free or pay networks, oblivious to the security threats we will likely encounter. We may feel safe behind the locked doors of our homes while we leisurely surf the net on our home Wi-Fi, unaware that our wireless signal can be picked up, without the use of any sophisticated hardware, a few hundred feet from the security of our home. When traveling, and using a hotel or restaurant wireless network, we may feel safe because we are in somewhat secure surroundings, with lots of innocent looking people all around us doing the same as we are. The problem is that unless we have implemented proper security precautions with out Wi-Fi, we are open to attack by electronic eavesdroppers, identity thieves, and an assortment of hackers, crackers, and other miscreants, many of which may be bent on doing us harm. According to the FBI, "... odds are there's a hacker nearby, with his own laptop, attempting to "eavesdrop" on your computer to obtain personal data that will provide access to your money or even to your company's sensitive information."

Several years ago, while working on a cyber security grant, I took the liberty of driving down the major thoroughfares in town, including the downtown area, equipped with my notebook computer with wireless adapter, and my Garmin

EMap GPS, carefully logging the many wireless networks I was receiving. About 80% of the networks that I received on my computer did not have adequate security, and could have been easily accessed from the road. This practice of driving around a city looking for open wireless networks is known in hacker circles as "war driving," and there are many illicit websites that have detailed city street maps that accurately show the locations of these vulnerable networks. On a trip to New York City, one of my daughters asked me what the chalked symbols on the sides of buildings meant; I explained that "war chalking" was the practice of labeling the buildings themselves that housed inadequately protected wireless networks. Anyone with a little larceny in his heart who was aware of the symbolism could easily penetrate the wireless networks thus disclosed. There is a large group of hobbyist hackers who delight in seeing how many wireless networks that they can penetrate in a given period of time. What the Wi-Fi hacker can do to the computer infrastructure and data of a vulnerable wireless network is only limited by his conscience.

Wireless hotspots, now common in fast food restaurants, coffee shops, airport waiting areas, and hotel lobbies, are other places that the innocent web surfer can be attacked while accessing the Internet. Many of these business locations actively advertise their Wi-Fi hotspot status and availability. Again, according to the FBI, "...there are 68,000 Wi-Fi "hot spots" in the U.S., at airports, coffee shops, hotels, bookstores, schools, and other locations where hundreds or thousands of people pass through every day. While many of these hot spots have secure networks,

some do not, according to Supervisory Special Agent Donna Peterson of our Cyber Division. And connecting to an unsecured network can leave you vulnerable to attacks from hackers.”

Hackers have a variety of tools and methods that they can use to penetrate your wireless computer. One that I have personally experienced (but did not fall for) is the phony “free wireless access” or inexpensive wireless connection that often appears on the list of wireless networks at airports and other areas. Hackers set up these hotspots in areas where there are likely to be many potential users (victims). Last January, in the Las Vegas airport (LAS), I picked up a very strong wireless signal from a source using the name (SSID) of “Free LAS Internet.” I happened to know as a fact that in the area and terminal I was in, there was no free Wi-Fi access provided by the airport. What this most likely represented was a hacker trolling for nearby victims in the terminal. They commonly dangle the bait of free or cheap Internet access, and wait for the hapless user to connect. Once connected, unless proper security precautions are in place and functional, the hacker may have access to any data that is on the victim’s computer. Popular items to steal are user ID’s, passwords, credit card numbers, and other personal information; this may also be used for sophisticated identity theft. Some hackers will install keylogging Trojans to record all of the victims’ keystrokes. Other hackers may redirect the user to counterfeit websites for the purpose of stealing information. “Another thing to remember,” said (FBI) Agent Peterson, “is that the connection between your laptop and the attacker’s laptop runs both ways: while he’s taking info

from you, you may be unknowingly downloading viruses, worms, and other malware from him.”

There are several tips on wireless security that the FBI has published; they are mostly common sense precautions that we should all be doing anyway. First, try not to connect to an unknown Wi-Fi network; just because an available network carries the name of the hotel, restaurant, or airport does not necessarily mean that it is legitimate, as the SSID (name) can be easily forged. Other recommendations from the FBI include, “Make sure your laptop security is up to date, with current versions of your operating system, web browser, firewalls, and antivirus and anti-spyware software; don’t conduct financial transactions or use applications like e-mail and instant messaging; change the default setting on your laptop so you have to manually select the Wi-Fi network you’re connecting to; turn off your laptop’s Wi-Fi capabilities when you’re not using them.”

Our home wireless networks are every bit as vulnerable to attack as is the road-warrior. One of my acquaintances has periodically used the wireless network of his neighbor (without his knowledge or consent) for broadband Internet access, rather than subscribing to an Internet service himself. This home user who had the open wireless system did not have any of the protective security features, like encryption, activated. It should be noted that firewalls generally do not provide any significant protection against unscrupulous wireless access. Virtually all home and office wireless systems utilize a router of some type to broadcast the signal. Wireless routers offer some encryption, which should be utilized;



many models turn off encryption by default, while others require it. It should be noted here that an encrypted signal is difficult for unauthorized users to utilize, and a very necessary security implementation. The two most common types of encryption available are the older and less secure WEP (Wired Equivalent Privacy), and the newer and more secure WPA2 (Wi-Fi Protected Access). Vista supports both forms of encryption, but XP generally only supports the older and less secure WEP. In setting up the encryption the user will initially be required to create a passphrase used to create the encryption key. Never use a default key if it is offered, and never use easy to guess phrases, words, family names, phone numbers, or other readily determinable passphrases. Instead, be sure to use a combination of random appearing upper and lower case letters and numbers, which will be harder for a hacker to crack. Security experts recommend that the encryption key and passphrase be changed on a regular basis, often every month or two. When the passphrases are changed, the keys on any computers connected to the wireless router must also be changed or they will lose their access.

Wireless connectivity is a great convenience, and I use it frequently both at home and when traveling. Just be very careful when using wireless wherever you are.

#### **WEBSITES**

[http://www.fbi.gov/page2/may08/wifi\\_050608.html](http://www.fbi.gov/page2/may08/wifi_050608.html).

<http://www.pcmag.com/article2/0,2817,2293406,00.asp>.

[http://www.fbi.gov/cyberinvest/protect\\_online.htm](http://www.fbi.gov/cyberinvest/protect_online.htm).

*Ira Wilsker is an APCUG director; Columnist, The Examiner, Beaumont TX; Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX; and a radio and TV show host. Contact him at <[iwilsker@apcug.net](mailto:iwilsker@apcug.net)>.*



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

I'm sure that most of you reading the title of this article are asking "What is an iFrame?" Well, sit back, get comfortable and I'll tell you about the latest method hackers are using to steal information from you.

First the definition of an iFrame, which is shorthand for inline frame. That clears it up doesn't it? I guess I'd better add some more to that. An inline frame is code within a web page that permits a second page to be imbedded inside the first page. For example, they can be used to imbed an ad that is located on a different web site. One example is the clickable scrolling ad you frequently find on web sites. IFrames generally load after the main page and may sometimes have their own scroll bar. The iFrame may contain Javascript programming code which can permit interactive content. Some iFrames may be invisible and may contain code which can redirect the user to another page or download trojans or viruses.

Whenever your Internet browser sees an "iFrame tag" in the web page code it sets aside the space requested in the tag. It also goes out to the web page



specified in the code to download the requested information.

So is this something new? I thought it was until I read a report in a tech newsletter (Windows Secrets) about an attack on the AskWoody web site. It turns out that iFrame attacks have been recorded since 2004. The first exploit implanted a worm on thousands of computers. The only thing that stopped it was a patch that Microsoft had to apply to Internet Explorer 6. In June 2007 over 10,000 pages were infected in Italy. In November 2007 Monster.com had to shut down as a result of an iFrame attack. Then, this year the AskWoody site had iFrame code added to its main web page. His research indicated that the code originated on a Russian web site, which subsequently disappeared. The code placed on the AskWoody web page linked to a web site in China and subsequently to the Russian web site. This was all done by a short length of code that setup a single, invisible pixel on the web page. The code was designed to load data from the Chinese web site. Anyone with an unpatched IE 6 that visited the AskWoody web site would probably have been infected. However, it was never determined just what was being delivered by the offshore web site.

The worst part of this scenario is that the owner of the AskWoody web site did not find out about the iFrame exploit until he started receiving messages from someone who advised him that their AVG Resident Shield said his site was infected. That was followed by Google advising him that his site was infected and down rating the site. Google also provided a warning to anyone attempting to link to AskWoody

warning them that visiting the site might infect their computer.

The question becomes, how did the iFrame code become attached to the web page? The code pages on web sites are generally password protected. Access to these pages for the purpose of making changes is controlled by the web site host and the hosting software. However, there are several programs available which enable hackers to take advantage of holes in web site security. Some of these are described as “kiddie scripts,” indicating their ease of use. Others, such as Mpack, require a more sophisticated knowledge of programming. The problem is that thousands of respectable sites have been infected. The following are only a few that were reported in March 2008 by Dancho Danev’s blog (a security information web site):

- \* eHawaii Portal - ehawaii.gov - 992 pages
- \* The World Clock - timeanddate.com - 944 pages
- \* Boise State University - boisestate.edu - 471 pages
- \* The U.S. Administration on Aging (AoA) - aoa.gov - 425 pages
- \* Gustavus Adolphus College - gustavus.edu - 312 pages
- \* Internet Archive - archive.org - 261 pages
- \* Stanford Business School Alumni Association - gsbapps.stanford.edu - 157 pages
- \* BushTorrent - bushtorrent.com - 147 pages
- \* ChildCareExchange - ccie.com - 131 pages
- \* The University of Vermont - uvm.edu - 120 pages
- \* Hippodrome State Theatre - Gainesville, FL - thehipp.org - 112 pages

\* Minnesota State University  
Mankato - [mnsu.edu](http://mnsu.edu) - 94 pages

\* Medicare – [medicare.gov](http://medicare.gov) – 12  
pages

In many instances it appears that the hackers were able to “harvest” passwords which gave them access to these sites. Then, if the site did not have current input validation patches, the iFrame could be added to web pages. In some cases, home users may have been the source of the initial password theft. By use of a keylogger a hacker can obtain passwords to any protected site visited by the user. In other cases clicking on a banner ad that attracts you can result in the download of a bot, a trojan or other spyware. This is especially true if you are still running an unpatched Internet Explorer 6. It appears that Firefox is less vulnerable to these types of exploits. Also, clicking on an executable file in IE 6 generally results in running the file. In Firefox you are usually only given the option to download the file. Obviously you should never download or run any file that you don’t know or don’t recognize. This is especially true when the site tells you that you need some kind of add-on or special viewer to see the information you want. This is the type of social engineering being used to tempt users into downloading spyware.

There is also a danger related to the firewall you are using on your computer. A keylogger or other trojan needs to be able to report “home” without the user being aware that information is being sent out. This is done by opening a “back door” to the Internet; an outgoing port in one of the thousands on every computer. If your firewall doesn’t check on all outgoing data and requests permission for new unknown activity,

then you will not be able to block the trojans back door connection. So it is very important that your firewall check both incoming and outgoing data. Then, anytime your firewall requests permission for a program, one you don’t recognize, to connect to the Internet, just say NO.

There is one other recognized method for obtaining the information needed to get into web page code. Hackers can purchase web site administrator information on the black market. One software application used to hack web sites, Mpack, sells for about \$1,000 US. The person behind this software is known as \$ash in the Russian underground. The software exploits six flaws in Windows and Internet Explorer. Thus for not a lot of money, hackers can obtain everything they need to exploit weaknesses in web pages.

As you can see, the iFrame attack is a real danger for those who surf the Internet. If you want to read more about these attacks, a Google search will provide you with tons of information. If you want to protect yourself from these attacks, your ability is limited. It is really up to your ISP and the web hosts to provide the security needed to prevent the web page intrusion of an iFrame. So what can a home user do? The following will help, but are no guarantee of protection.

1. Beware of pages that require software installation. Do not allow new software installation from your browser unless you absolutely trust both the Web page and the provider of the software.
2. Scan with an updated antivirus and anti-spyware software any program downloaded through the Internet. This includes any downloads from

P2P networks, through the Web and any FTP server regardless of the source.

3. Use only a firewall that checks both incoming and outgoing data.

4. Beware of unexpected strange-looking e-mails, regardless of their sender.

5. Never open attachments or click on links contained in these e-mail messages

6. Enable the "Automatic Update" feature in your Windows operating system and apply new updates as soon as they are available

7. Always have an antivirus real-time scan service. Monitor regularly that it is being updated and that the service is running.

8. OR another option would be to verify that the address is safe before going to it. You can do this by checking it at: <<http://linkscanner.explabs.com/linkscanner/default.asp>>.

As you can see, for Windows users, the Internet is becoming more of a hazard to navigation. You, as a user, must always be cautious about clicking on links or accepting downloads. If in doubt, don't do it! If everyone practiced safe-surfing, it would be harder for the hackers to succeed.

***Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years; teaching, developing software and assembling systems. Dr. Lewis is a member and contributing columnist of the Sarasota PCUG, Florida. <<http://www.spcug.org>>. He can be reached at [bwsail \(at\) yahoo.com](mailto:bwsail@yahoo.com).***

***This article has been provided to APCUG by the author solely for***

***publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).***



**Google Releases  
Updated Version of  
"Google Earth."  
By Ira Wilsker**

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

It has been nearly two years since I first (and last) discussed Google Earth in this column. In the ensuing time since the last review, Google has been busy updating and improving the product, adding new features, and improving the graphics. For those who may not be aware, Google Earth is a program that allows the immense Google database of terrestrial and satellite images of the earth, along with amazing images of space, to be utilized and manipulated on the computer.

What is new and improved in the recently released Google Earth 4.3 (beta) is demonstrated in an interactive video tour online at <<http://earth.google.com/tour.html>>. One of the new features in version 4.3 include what Google calls "Photo-realistic Buildings," where hundreds of buildings in many of the world's major cities are shown in three dimensions (3D). If a building that is displayed "turns purple" when cursoring over it, clicking anywhere on the building will open up a smaller window giving details of the building, and the moniker of the person who created or updated the digital image. The images displayed can be manipulated to zoom in or around them from any angle, effectively creating a dynamic 360 degree panoramic view. These 3D views

are not just of cities and buildings, but there are also spectacular images of natural beauties such as mountains, rivers, waterfalls, and canyons. Another new feature on this version is what Google calls “Swoop Navigation” where the user can virtually “Fly seamlessly through the landscape with new navigation controls. Swoop from outer space to street level and leap from one building top to another. Use the look joystick to view buildings as if you were standing right in front of them.”

Another aspect of the new version is the “Light and Shadow” feature where many of the images can be shown in selected or sequential times of the day, such as displaying a mountain top from sunrise to sunset. On the top of the screen is an optional slider which can be moved with the mouse to display the simulated or realistic image at any chosen time. In some of the more scenic images it appears to show the path of the sun across the sky with the corresponding light and shadows. The new and improved “Street View” that has been previously available online with Google Maps (<<http://maps.google.com>>) is now integrated into Google earth. Google has a fleet of vehicles which cruise major cities taking high resolution 360 degree digital photos as they drive down the streets. With “Street View” the user can virtually visit a city and virtually walk or drive the streets using the mouse instead of a vehicle. Views are literally from the street level showing cars, people, store fronts, intersections, and any other features visible from street level. Using the mouse, the user can cruise the streets just as if he was navigating the city for real. While not yet available for every city, a camera icon, when

displayed on a map, will zoom in to a 360 degree panoramic image from street level. Many street level images contain additional camera icons which allow the user to travel seamlessly up a selected street, and the mouse can be used to turn in any direction.

The popular features that were in earlier versions of Google Earth have been retained. One that I periodically use is the “Directions” feature, which does not just give traditional driving directions and maps, but also animates the drive by clicking on the play button at the bottom of the driving directions listing. When animated, a detailed sequential zoomed-in satellite image is displayed, with the directions overlaid on the image. For example, when I requested driving directions from the Examiner offices on Willow Street in Beaumont, to the Bush Airport (IAH) in Houston, the seamless animation in Google Earth showed the street images including real pictures of the highway showing which lane to be in, detailed images of each turn or exit, and high resolution images of the airport. The images are actual photographs, not computer generated images. By seeing the route in exquisite detail prior to a journey may help ease the anxieties of the drive.

Once at a destination, it may be helpful to find nearby “points of interest,” such as restaurants. By simply entering the word “restaurants” in the “What?” box, and the current address in the “Where?” box, restaurants will be displayed on the Google map. By clicking on the icon displayed for each restaurant, details will be displayed for the selected restaurant in a window overlay. Typical information displayed included the name, address, phone,

a hyperlink (if any) to the restaurant website, any reviews that may be available and driving directions “to” and “from” the restaurant.

Google Earth does not just provide maps and images of terrestrial and earthly locations, but also includes celestial maps and images. Clicking on the Saturn-looking icon on the top of the screen will open a “Search the Sky” search box. By entering a celestial body or location, such as “Mars,” Google Earth will display a sky map with an image of the heavenly body, and also display the current geometric coordinates for those using sophisticated telescopes.

The basic version of Google Earth 4.3 (beta) is a free download from [earth.google.com](http://earth.google.com). For those desiring more features, Google offers Google Earth Plus for \$20, which adds support for a variety of GPS devices (verified support for Magellan and Garmin GPS devices, but can not upload to those devices), improved network performance, and improved high resolution printing. For professional and commercial use Google offers the Pro version for \$400.

Google Earth is a fascinating utility, and will run on Windows 2000 or XP (Vista is not mentioned), and requires a minimum of 400MB hard drive space, and a video card capable of 1024x768 resolution with a 16bit color depth. An Internet connection of at least 128Kb/sec is required. I suggest that readers of this column at least download the free version of Google Earth and simply play with it. Click on the icons at the top of the page, and check and uncheck some of the boxes on the left margin, and experiment with it; do not worry, you can not hurt anything by experimenting

with it. Google Earth is one of my favorite “fun” programs.

#### WEBSITES

[<http://earth.google.com>](http://earth.google.com).

[<http://earth.google.com/download-earth.html>](http://earth.google.com/download-earth.html)—FREE Version.

[<http://earth.google.com/tour.html>](http://earth.google.com/tour.html).

[<http://earth.google.com/enterprise/earth\\_plus.html>](http://earth.google.com/enterprise/earth_plus.html)—\$20 Plus Version.

[<http://earth.google.com/enterprise/earth\\_pro.html>](http://earth.google.com/enterprise/earth_pro.html)—\$400 Pro Version.

*Ira Wilsker is an APCUG director; Columnist, The Examiner, Beaumont TX; Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX; and a radio and TV show host. Contact him at [<iwilsker@apcug.net>](mailto:iwilsker@apcug.net).*

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

**Scotty, I Need More Power  
By Alan Mildwurm**

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

When my kids were young, I bought batteries by the bushel. All of their toys required some batteries. The phrase “batteries not included” raised almost as much terror as “some assembly required.” I still recall going out one Xmas morning in search of “C” size batteries because we missed the warning on the box. One very cool pool toy took 16 batteries - in 3 sizes.

In those days, rechargeable batteries were garbage. Most rechargeables were nickel-cadmium and with a memory

that made them useless after a few charges. Shelf life was a joke and power output dismal. For several years, I bought throw away alkaline batteries at Costco because they were cheaper than those clever bunny batteries. Not environmentally friendly, but definitely kid toy friendly. As the kids grew up, their needs for batteries diminished (actually they now buy their own), but my need for batteries is increasing. Wireless keyboards, wireless mice, gps, wireless game controllers (the Wii-mote takes 4 batteries per controller and there are 4 controllers), iPod external power units, camera accessories and on and on. I am going through more batteries now with my toys than I ever did with the kids! Luckily, rechargeable battery technology has come a long way.

Sanyo produces the eneloop <<http://www.eneloop.info>>. According to their spec sheet, the AA battery is rated at 1.2 volts and 2000 mAh. Not bad for a rechargeable. (A disposable usually is 1.5 volts.)

There are two sizes of eneloop batteries, AA and AAA. They also produce C and D size cylinders in which you insert AA batteries. From their site: "...eneloop is a totally new type of battery, which satisfies in a unique way the needs and expectations of the consumers."

**Consumers would like to have a battery, which:**

- \* Can be used right after the purchase
- \* Has a high performance
- \* Has a long shelf life with no loss of energy:
- \* Can be used everywhere
- \* Is cheap in purchase and usage
- \* Is environmental friendly
- \* Is easy to use

So far these requirements could not be satisfied by a single type of battery. The consumer had the choice between disposable batteries or rechargeable batteries.

Disposable batteries have several advantages:

- \* They can be used immediately
- \* They have a long shelf life with low loss of energy
- \* They are rather cheap in purchase
- \* They are easy to use and no charger is required

These advantages of disposable batteries however, had to be seen alongside several clear disadvantages:

- \* Can be used only once and therefore mean substantial waste and risk for the environment.
- \* Have to be purchased over and over again and are therefore expensive considering the life-time of your equipment.
- \* Are not quite powerful enough in certain applications (like digital cameras)
- \* Are being offered in many varieties and special application-specific types, which confuses the consumer.

**The classical advantages of rechargeable batteries are:**

- \* High performance, especially if high discharge currents are required ( like in digital cameras)
- \* Cheap in use, because they can be recharged many times.
- \* Environmental friendly, because one rechargeable battery replaces 1000 disposable batteries.
- \* Good performance at low temps.

Given these advantages, rechargeable batteries also have some disadvantages, which made consumers reluctant to exchange disposable batteries for rechargeable batteries:



\* After purchase, rechargeable batteries have to be charged before they can be used.

\* Rechargeable batteries lose the stored energy rather fast.

\* The state of the charge is hard to determine.

\* Continuous charging or frequent charge (without complete discharge ) can destroy the battery.

\* Proper charging is complicated for an average consumer

\* The charging takes quite long and rapid chargers are expensive.

All these negative attributes have one root-cause: self discharge.

Self-discharge means, that a charged battery slowly discharges itself without any equipment consuming any current. This is the reason for rechargeable batteries being sold in discharged state. And this is the reason that keeping charged batteries for some time did not make any sense. When you needed them, the energy was gone.

### **How was the self-discharge reduced? (For you techy folks!)**

Modern Ni-MH batteries consist of two metal stripes (anode and cathode), which are separated by a non-conductive porous plastic foil (separator). These three stripes are laid on top of each other and are wound to a coil. This coil is put in a metal can and immersed with a liquid (electrolyte). Then the metal can is closed with a cap.

The self discharge of Ni-MH batteries is caused by three main reasons:

\* The chemical decomposition of the cathode,

\* The natural disaggregation of the anode,

\* Impurities of the anode.

Now, how could the self-discharge in the eneloop have been reduced?

The chemical decomposition of the cathode has been reduced substantially by the use of a new superlattice alloy. As an additional benefit the superlattice alloy increases the electrical capacity of the battery and reduces the internal resistance, which allows higher discharge currents. Another advantage of the reduced decomposition of this alloy is the fact that less Cobalt is needed to stabilize the alloy. The anode has been strengthened by another new material, which reduces the natural disaggregation. Additionally the separator and the used electrolyte have been optimized for low self discharge of the eneloop.

### **They really are good batteries!**

I have been using eneloops for several months. They work fine. I have both a wall charger and two-battery (AA or AAA) USB charger. Both chargers work very well. I like the USB charger and I love the fact that they come charged and ready to go.

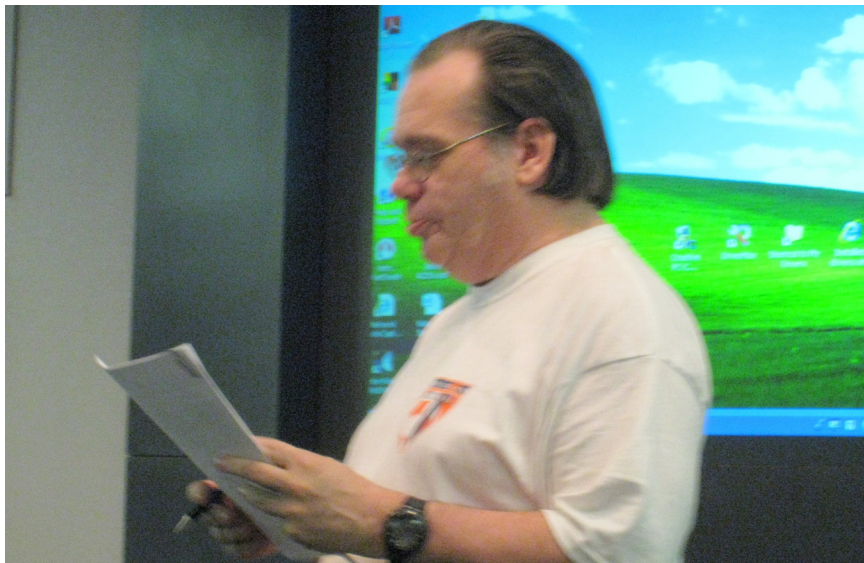
The kit lists for \$50.00 but is available at Amazon for \$32.00. It comes with 4 AA, 2 AAA, and 2 spacers each for C and D plus a charger. I have found even better deals with more batteries at Costco!!

*Alan Mildwurm is President of the Diablo Valley PC Group of California. <<http://www.dvpc.org>>. E-mail: [avn\(at\)mildwurm.com](mailto:avn(at)mildwurm.com).*

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



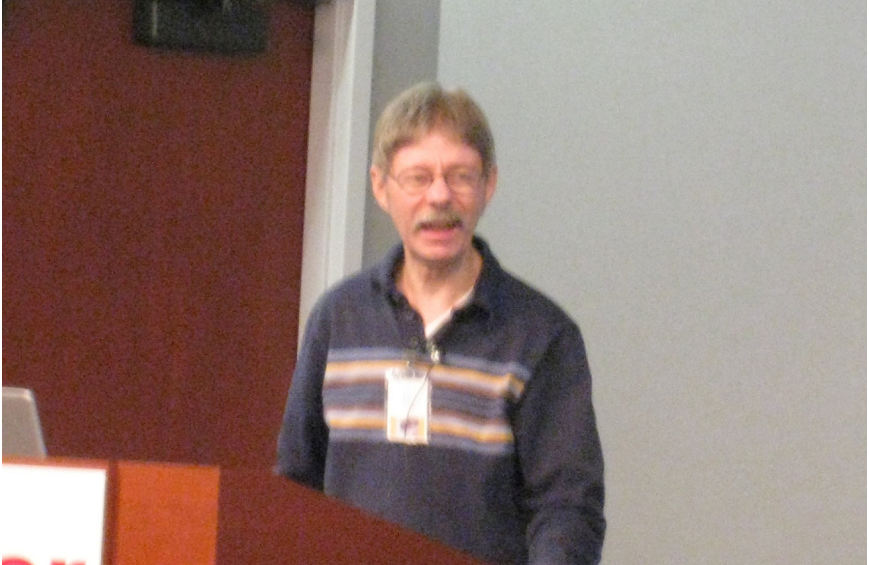
## *Meeting Pictures*



**(Above) Mike Bader addresses the group at the May meeting. (Below) Paul Cervero and Charles Moery at the April meeting.**



## *Meeting Pictures*



**Richard Jackson discusses "Crossloop" at the May meeting.**





**BOARD MEETING**  
**5/11/2008**  
**Carol Sanzi**

**BOARD MEMBERS PRESENT**

President Mike Bader, Vice President Richard Jackson, Treasurer Bette Gay, Secretary Carol Sanzi, SIG-Advanced Chairman Franz Breidenich, SIG-IBM Chairman Tom Callow, Publications Committee Chairman Warner Mach, and Members-at-Large Bob Clyne and Chuck Moery. The meeting was called to order at 12:06 p.m.

**OLD BUSINESS**

Bette Gay reported that the amount in the treasury equaled \$9,065.41 with \$4,405.41 in the bank account and \$4,660.00 invested in three Certificates of Deposit. The membership stands at 74.

It is time for John Samarian to renew his membership.

**NEW BUSINESS**

Mike Bader reported that the Yahoo on-line user group has grown to 44 members. Activity continues to grow.

Mike Bader reported that SEMCO could use Constant Contact's service to send out text and html announcements to members, but the sign-up fee is \$100 and the monthly fee is \$30. Jack Vander-Schrier, however, is offering text only List Server at no charge. Bob Clyne moved that SEMCO use Jack Vander-Schrier's List Server to send announcements only. Tom Callow seconded the motion and it was carried.

Richard Jackson moved to include the complimentary DATA BUS recipients to this mailing list. Franz Breidenich seconded the motion. After a discussion took place, Richard Jackson

restated his motion to send e-mail announcements to those members and complimentary DATA BUS recipients whose e-mail addresses are available. Bob Clyne seconded the motion, but it was not passed.

Warner Mach moved that the person handling the list mailing would have the discretion to send e-mails to complimentary DATA BUS recipients and Honorary Members. Bob Clyne seconded the motion and it was carried.

Warner Mach will work with Mike Bader to create the e-mail announcements to be sent out at least once a month. More communications would be optional as needed.

Bob Clyne moved to adjourn. Tom Callow seconded the motion and it was carried. The meeting adjourned at 12:44 p.m.



**Geohashing!**  
**By Warner Mach**

You have probably heard of "Geocaching" where a "treasure" is hidden at some location and the GPS coordinates are given out on a web site.

Now Randall Monroe, the artist who publishes cartoons on the xkcd web site <<http://xkcd.com>> has come out with the concept of "Geohashing."

The way it works is that, on a given day, you take the date and the opening value of Dow Jones for that day. This combined number is then run through the MD5 (Message Digest Algorithm 5) algorithm which produces a 32 byte hex number. Take the left 16 bytes of

[Continued on Page 21](#)

## SPECIAL INTEREST GROUPS (SIGS)



**SIG-IBM**  
Tom Callow

**June 8: 1:45 p.m. Screen Shots and More with Snagit by TechSmith:** Rick Schummer, President and Owner of White Light Computing, Inc. will demonstrate Techsmith's Snagit, screen capture program and Camtasia Studio screen recording program.

### SIG-IBM INTERMEDIATE

**June 8: 3:45 p.m. Using Yahoo Groups:** Mike Bader will present "Using Yahoo Groups," by highlighting our own SEMCOUG Yahoo group, as well as showing several favorite links and web sites listed there. Also he will give a demonstration of a two-pound, touchscreen computer and a PC fingerprint reader

### NOVICE-IBM GROUP Rotating Volunteer Hosts

**June 8: 3:45 p.m.:Help Q & A:** Discussion directed by the audience. No question is too simple! Note: The Novice-IBM Group is 'by request.' If you have special questions for this group then speak to one of the officers to schedule the session.



**SIG-ADVANCED**  
Franz Breidenich

**July 7, 2008: . 6:45 p.m,** at the Oak Park Library. The library is located at 14200 Oak Park Blvd., Oak Park, MI. Phone: (248) 691-7480. Topic: Wide ranging discussion of computers and computing.

---

### July 2008 DATA BUS DEADLINE (7th day after 2nd Sunday in month)

**SEMCO Input and Members' Ads—Deadline: Sun., June 15, 11:59 p.m.** Members' personal ads are free. To mail, use Editor [address on Page 2](#); e-mail address: <[machw@att.net](mailto:machw@att.net)>. PLEASE send to arrive sooner than deadline.

**Business Ads - Deadline: Second Friday monthly.** Contact Editor ([address Page 2](#)).



**Warner Mach**[machw@att.net](mailto:machw@att.net)

(to post monthly computer group info)

**CALENDAR-OF-EVENTS  
OTHER GROUPS****COMP (Computer Operators of Marysville & Port Huron)**

(No meeting), 7 p.m., (1<sup>st</sup> Wednesday); St. Clair County RE&SA, 499 Range Rd., Marysville, Admin. Building. Jane Wheatly 810-982-1187 or Pam Raisanen <[compinfo@hughes.net](mailto:compinfo@hughes.net)>. <<http://www.bwcomp.org>>. No meetings in July & August.

**DCOM Computer Club**

June 13, 6:30–8:30 p.m., (2<sup>nd</sup> Friday); Henry Ford C.C., Patterson Tech Bldg, Ford Rd/Evergreen, Rm T143, Parking Lot C. Info: Doug Piazza 313-582-2602. Topic: TBA.

**HUG (Holly User Group)**

June 14, 9:00 a.m., (2<sup>nd</sup> Sat.); Groveland Twp. Fire Hall, 3085 Grange Hall Rd. & Dixie Hwy., Ortonville. Topic: TBA.

**MacGroup- Detroit**

June 22, 3:00 p.m., Birmingham Temple, 28611 West 12 Mile Rd., Farmington Hills. Info: Terry White, <[terry@macgroup.org](mailto:terry@macgroup.org)> or 248-569-4933. <<http://www.macgroup.org>>. Topic: "Jon Rutherford from Macprofessionals will show the latest developments in professional digital video using Apple's Final Cut Studio."

**MacTechnics, (MAC User Group)**

June 21, 11:00 a.m., (3<sup>rd</sup> Saturday); (SIGs at 9:30); See web site for meeting location. <<http://www.mactechnics.org>>. JoAnn Olson at 248-478-4300. Topic: "Applescript," with Dave Ginby from the Briarwood Apple Store.

**MDLUG (Metro Detroit Linux User Group)**

June 21, 12:30–2:30 p.m., (3<sup>rd</sup> Saturday); MDLUG meetings will be at The Gaudior Academy located at 27100 Avondale Avenue in Inkster. Web: <<http://www.mdlug.org>>. Info: Raymond McLaughlin 248-960-1864. Topic: TBA.

**MUG (Michigan User Group)**

June 10, 6:00 p.m., (2<sup>nd</sup> Tuesday); MUG meetings are at The Farmington Community Library–Main Branch, 32737 W. 12 Mile Rd., Farmington Hills, MI. 48334. <<http://www.mug.org>>. Topic: TBA.

**Michigan Apple Computer User Group**

June 12, 7:30 p.m., (2<sup>nd</sup> Thur.); General meeting; Fraternal Order of Eagles Hall in Clawson, 174 Bowers St. (one block North of 14-Mile and one block East of Main). Avi Drissman 248-232-7865. Web: <<http://www.themichiganapple.com>>. Topic: TBA.

**Oak Park Computer Club**

Every Fri., 10:15 a.m. at Oak Park Recreation Bldg, Oak Park Blvd. west of Coolidge.

**Royal Oak Computer Club**

Every Wed., 12:30 to 2:30 PM at Mahany/Meininger Senior Community Center, 3500 Marais Ave., Royal Oak, 48073. Near Crooks & 13 Mile. Guest speakers & regular monthly speakers. <<http://www.geocities.com/royaloakcomputerclub/ourpage.html>>

**SHCC (Sterling Heights Computer Club)**

(No meeting), 7:30 p.m. (1<sup>st</sup> Tues); Macomb Community College South Campus, Bldg. K, 14500 E. 12 Mile Rd. Don VanSyckel <[Don@VanSyckel.net](mailto:Don@VanSyckel.net)>, 586-731-9232; Web: <<http://www.SterlingHeightsComputerClub.org>>. No meetings in July & August.

**Wayne State University Mac User Group**

June 14, 10:00 a.m.–Noon, (2<sup>nd</sup> Saturday); at 21042 Laurelwood, Farmington. Information: JoAnn Olsen 248-478-4300. Topic: TBA.

## Continued from Page 18

that number and convert it to decimal and attach the first six digits (after the decimal point) to the value of the latitude in your part of the country. Take the right 16 digits and convert them and attach the first six digits to the longitude.

The values that you come up with determine where you should go for that day.

Misc: (1) The MD5 algorithm is widely available in the Unix/Linux world. For Windows, check “MD5” under Google. (2) If the location that you come up with is over water or on a military base or in some inaccessible place, then give up. (3) The opening value for Dow Jones is available around 9:30 AM EDT. The value for Friday is good for Saturday and Sunday. (4) If you want to attempt to meet other geeky folks in your area who are doing the same thing then go to the designated

location at 4 PM on Saturday. (5) The Detroit latitude/longitude is (42,-83).

References: (1) Example of the calculation at: <<http://xkcd.com/426>>. (2) Wiki entry: <[http://wiki.xkcd.com/geohashing/Main\\_Page](http://wiki.xkcd.com/geohashing/Main_Page)>. (3) To get latitude/longitude for given address: <<http://itouchmap.com/latlong.html>>. (4) To get address at given latitude/longitude: <<http://stevemorse.org/jcal/latlon.php>>.



### COMPUTER RESOURCE PEOPLE

This is a list of members willing to be resources for other members to call when they have hardware or software questions.

Are you willing to help members learn?

Which software programs are you familiar enough with?

It is not necessary to be an expert, but just have some familiarity with the program and be willing to help someone starting to learn it. Please give this some thought and volunteer at the next group meeting.

**Almost Anything:** Vander-Schrier

**AutoCAD:** Comptois

**Genealogy:** Cook

**IBM PC Hardware Issues:** Clyne, Yuhasz

**Operating Systems:** Callow, Clyne, Yuhasz

**MAC Hardware and OS Issues:** Yuhasz

**Security:** Bader

**MS Office for Windows:** Callow

**MS Word:** Clyne

**Networking:** Callow

**Novell Network:** Yuhasz

**Quicken:** Clyne

**Geocaching:** Cook

Bader, Mike—586-573-7330, 9am–8pm.....	<a href="mailto:mdbader@flash.net">mdbader@flash.net</a>
Callow, Tom—248-642-5770 9am–5pm.....	<a href="mailto:tcallow@monaghanpc.com">tcallow@monaghanpc.com</a>
Clyne, Bob—810-387-3101, 9am–10pm.....	<a href="mailto:clyne@mich.com">clyne@mich.com</a>
Comptois, Jerry—248-651-2504, anytime	
Cook, Stephen—313-272-7594, eves.....	<a href="mailto:scook48227@ameritech.net">scook48227@ameritech.net</a>
Vander-Schrier, Jack—586-739-7720, 12–8pm.....	<a href="mailto:jvanders@myself.com">jvanders@myself.com</a>
Yuhasz, Steve.....	<a href="mailto:Help@yuhasz.org">Help@yuhasz.org</a>



**SOUTHEASTERN MICHIGAN  
COMPUTER ORGANIZATION, INC.**

## **SEMCO CALENDAR**

**ArvinMeritor Building  
2135 West Maple Road  
Troy, Michigan**

**June 8–SUNDAY (Meet 2nd Sunday)**

**SEMCO Board Meeting at 12:00 noon. For Officers and SIG Chairpersons.  
Other members are invited to attend.**

**SEMCO General Meeting at 1:30 p.m.**

### **Special Interest Groups (SIGs)**

**SIG-IBM** 1:45 p.m. **Program: Screen Shots and More with SnagIt by TechSmith:** Rick Schummer, President and Owner of White Light Computing, Inc. will demonstrate Techsmith's Snagit, screen capture program and Camtasia Studio screen recording program.

**SOCIAL PERIOD** 3:15 p.m. Refreshments! (Reminder: We must continue to maintain a neat environment.)

**NOVICE-IBM GROUP** 3:45 p.m. **Program:** Help From An Expert With Discussion Directed By The Audience.

**SIG-IBM Intermediate** 3:45 p.m. **Program: Using Yahoo Groups:** Mike Bader will present "Using Yahoo Groups," by highlighting our own SEMCOUG Yahoo group, as well as showing several favorite links and web sites listed there. Also, he will give a demonstration of a two-pound, touchscreen computer and a PC fingerprint reader.

**SIG-ADVANCED, July 7, 2008–MONDAY, 6:45 p.m.,** Oak Park Public Library, 14200 Oak Park Blvd., Oak Park, MI. Phone: (248) 691-7480. Directions: Oak Park Blvd. is 9 1/2 mile Road; library is west of Coolidge. Info: Franz Breidenich 248-398-3359. TOPIC: Wide-Ranging Discussion Of Computers & Computing.

**July 13–SEMCO Sunday**

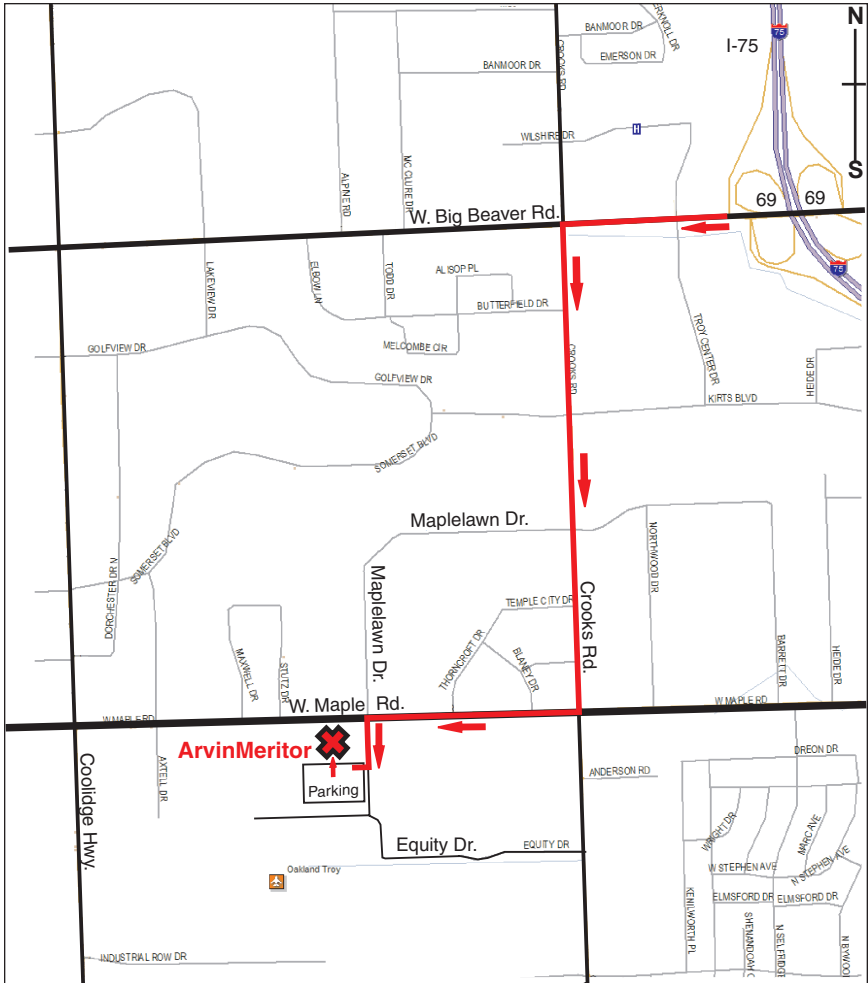
**<http://www.semco.org>**

**PUBLIC INVITED**

**(Please copy this and the next page to post on your bulletin board)**



**SEMCO Meetings at [ArvinMeritor](#)  
2135 West Maple Road, Troy, MI 48064**



**DIRECTIONS**

From I-75, take Exit 69 to westbound Big Beaver Rd. (16 Mile). Turn left (South) on Crooks Rd. Turn right (West) on Maple Rd. (15 Mile). Turn left (South) on Maplelawn Dr. Turn right into the parking lot at the rear of the ArvinMeritor building. The building is shaped like an X. Enter the building thru the South entrance at the center of the rear of the building. Follow the SEMCO signs.

SEMCO thanks the [ArvinMeritor](#) Corporation for their hospitality in providing their facility for our meetings.



**SouthEastern Michigan  
Computer Organization, Inc.  
P.O. Box 707  
Bloomfield Hills, MI 48303-0707**

**SEMCO (future meetings)**

**June 8**

**July 13**

**FIRST CLASS MAIL  
Dated Material**

**SEMCO: A Community Organization  
Helping People for the 21st Century**