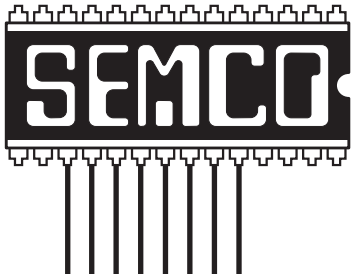


Official Newsletter
SouthEastern Michigan
Computer Organization, Inc.

DATA BUS

Volume 38 December 2013 Number 12

IN THIS ISSUE

SEMCO OFFICERS

President	Mike Bader	(586) 447-6683
Vice-President	Richard Jackson	(248) 546-3694
Secretary	Carol Sanzi	(586) 739-7256
Treasurer	Brian Brodsky	(248) 391-9125
Members-at-Large of the Board of Directors		
	Bob Clyne	(810) 387-3101
	Richard Fink	(248) 752-6762

NEWSLETTER STAFF

Publications Committee Chair	Position Open	
Interim Editor	Bob Clyne	(810) 387-3101
Events Research	Betty MacKenzie	(586) 254-0677
Proofreaders	Beth Fordyce	(248) 573-5321
	Ken Phillips	(734) 654-3679
	Paul Baecker	

SIG (SPECIAL INTEREST GROUP) CHAIRPERSONS

SIG-Computing	Tom Callow	(248) 642-5770 (9–5)
SIG-Techniques	Position Open	
SIG-Advice	Bob Clyne	(810) 387-3101
SIG-Linux	Brian Brodsky	(248) 391-9125
SIG-Programming	Richard Jackson	(248) 546-3694

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**

DATA BUS is published monthly by SouthEastern Michigan Computer Organization, Inc. (SEMCO) as its official newsletter. **Mail DATA BUS newsletter copy to: Bob Clyne, 130 First Street, Yale, MI 48097; or e-mail: clyne@mich.com.** The Editor is responsible for contents and control of the DATA BUS.

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 CS6
donated by Adobe Systems, Inc.

NOTICE OF ANNUAL MEETING AND ELECTION

The annual meeting of the members of the SouthEastern Michigan Computer Organization, Inc., will be held Sunday, January 12, 2014 at 1:30 p.m. at Engineering Society of Detroit, 20700 Civic Center Drive, Suite 450, Southfield, Michigan. The election of Officers and Members-at-Large of the Board of Directors of the Corporation will take place at the annual meeting.

NOTICE OF NOMINATIONS

Please take notice that under the Bylaws of the SouthEastern Michigan Computer Organization, Inc., nominations for officers will be taken at the general meeting to be held Sunday, December 8, 2013 at 1:30 p.m., with the election of officers to be held at the January general meeting. The following offices will be open for nominations:

1) President
2) Vice President
3) Secretary
4) Treasurer
5) Two Members-at-Large of the Board of Directors

Do Not Fall Prey to the Vicious CryptoLocker Extortion

By Ira Wilsker

October was the tenth anniversary of National Cyber Security Awareness Month (NCSAM). According to a statement on the FBI website, "(National Cyber Security Awareness Month) Established by presidential directive in 2004, the initiative—administered by the Department of Homeland Security—raises cyber security awareness across the nation by engaging and educating public and private sector partners through a variety of events and programs. The ultimate goal is to protect the country from cyber incidents and respond to them effectively if they do occur."

Around the country, at K-12 schools, colleges, universities, and private businesses, thousands of seminars and events took place during NCSAM in order to educate computer users at all levels on cyber security. I had the honor and privilege of presenting two citizen awareness sessions for the city of Port Arthur, Texas. I discussed several of the contemporary online threats and how users could effectively protect themselves from those threats. One of the warnings that I repeated several times was to never open e-mail attachments, as they are a common

vector used to bypass much of the security software that we (should) have installed on our computers.

Now that the National Cyber Security Awareness Month is behind us, we should not forget the lessons learned about clicking on e-mail attachments. Unlike our New Years' resolutions that many of us make, but quickly forget to implement, cyber security threats are continuing, and in many cases becoming more threatening. One recent example is a new version of an old Russian cybercriminal extortion scam; in the original versions, which took over countless millions of computers worldwide (and is still showing up in large numbers), the purloined computer displayed a window after boot that had an official looking logo of the FBI or other law enforcement agency, along with an official looking criminal complaint that child pornography (or other illicit content) was found on the computer. Nothing else could be done on the computer, as it was effectively locked by the "FBI." The computer user was told that if they did not pay the fine, typically $200, within 24 or 48 hours, they would be subject to arrest, charged with a felony, and face 10 years in federal prison, plus a $10,000 fine. Detailed instructions were provided on where to purchase a specific prepaid debit card, and then entering the cards 16 digit number into the payment box on the warning screen. After payment was received, the "FBI" would drop the charges and (hopefully) release control of the computer.

The especially nasty new type of ransom ware, also likely from Russia, goes a step further than the other recent ransom ware; the new version contains a version of a vicious piece of malware called "CryptoLocker." Some variants contain a version of the well-know Zeus trojan, which is used to install and run CryptoLocker. Typically spread via an e-mail attachment, often apparently sent from a known acquaintance or company, the attachment appears to contain a ZIP file with a disguised file that looks like an innocent PDF file. I have personally received dozens of these e-mails, and I will admit that they do look like they are from a legitimate source, but I know not to open e-mail attachments that have any vestige of being suspicious. Once opened, the attachment executes, installing itself in the Documents and Settings folder with a random file name, adding a startup command key to the registry which causes CryptoLocker to load when the computer is booted. CryptoLocker then goes through a series of servers, making it difficult to trace, eventually connecting to a command and control server. This remote server generates a very sophisticated 2048-bit RSA encryption key pair using the public key to encrypt Microsoft Office and Open Document files, as well as some common graphics file formats. CryptoLocker will not just encrypt the computer of the user unfortunate enough to open the e-mail attachment, but can also encrypt those file types on any mapped network drive, including USB drives, network file shares, and even cloud storage folders that are made to appear as a drive letter (like "G:\" drive), which may effectively shut down a business, school, hospital, or government agency that uses mapped network drives; it only takes one infected computer to possibly compromise the targeted files on an entire network.

Once the files are encrypted using the 2048-bit RSA public encryption

key, a warning is displayed on the computer that critical data files have been encrypted, and that the ransom (extortion) payment must be made in a specified time, often 72 or 100 hours, or else the private encryption key on the command and control server will be destroyed and "nobody and never [sic] will be able to restore files." The extortion demand is, "…a payment of either 100 or 300 USD or Euro through an anonymous pre-paid cash voucher (i.e. MoneyPak or Ukash), or 2 Bitcoin in order to decrypt the files." Anecdotally, some published reports have claimed that some businesses have received cyber extortion demands of $10,000 or $20,000 dollars, or equivalent amounts in Euros or Bitcoins (private currency). In order to add a sense of urgency, a countdown timer is displayed indicating the deadline to pay the ransom, or the files will forever become unrecoverable (Image: <http://blog.emsisoft.com/wp-content/uploads/2013/09/crilock.png>). The 2048-bit encryption keys used by CryptoLocker are considered in the security industry as extremely secure and virtually unbreakable, and can be expected to meet security requirements until the year 2030 (source: <http://en.wikipedia.org/wiki/Key_size#Asymmetric_algorithm_key_lengths>).

Almost all of the common security suites, including Kaspersky, Symantec, Sophos, Emsisoft, and others, can detect and remove the CryptoLocker malware and the Zeus trojan, but no one (yet) has been able to come up with a practical method to crack the encryption key and recover the encrypted files; effectively they are gone forever. Removing the infection is a moot point, as the encrypted files will remain unusable. While some experts claim that paying the extortion prior to the expiration, hoping that the cyber criminal will send the private key necessary to decrypt the files, many others, including most law enforcement agencies do not condone paying ransom under the theory that it will only encourage more criminal behavior. Cited by Wikipedia, "Symantec estimated that 3% of users infected by CryptoLocker chose to pay the ransom." Do some simple arithmetic; if a million computers are hijacked by these criminals, and only 3% pay a $200 ransom, the crook receives a cool $6 million in illicit proceeds. Since multiple millions of computers have been held for ransom by CryptoLocker, the proceeds to the criminal enterprise may be staggering.

As is typical, prevention is the best method to avoid being taken over by CryptoLocker or any of the other cyber threats. Sophos, a well respected multinational security company headquartered in the UK has published "Five "top tips" for keeping safe against malware in general, and cyberblackmailers in particular" <http://nakedsecurity.sophos.com/2013/10/18/>. The first of the five tips is common sense, and a task incumbent on all computer users, "Keep regular backups of your important files." After cleaning the CryptoLocker and any other malware that infected the computer, the encrypted files can be safely deleted and replaced by their backup copies. One strong warning about the backup copies and the devices that the backups are stored on; do not leave the backup devices, such as external hard drives, attached to the computer or the network, as they will likely have a drive letter that

can be identified by CryptoLocker. If CryptoLocker can see it, it will also encrypt the files on those devices, making the backup copies as useless as the encrypted files on the primary hard drive. Good practice is to frequently rotate through multiple backup devices, creating redundant backup copies, and never allowing more than one device to be attached and running at any given time. The other backup devices should be stored securely, and only connected in rotation, never having more than one backup device connected at a time. While CryptoLocker may also encrypt the files on an attached backup device, it cannot attack any unattached devices.

The second tip from Sophos is the often stated, "Use an anti-virus, and keep it up to date." I would add to that rule that it should also be required to do frequent and periodic security scans for malware using alternate third-party security software such as Emsisoft, SuperAntiSpyware, and MalwareBytes. My rationale for this secondary scanning by alternative scanning utilities is that prior infections may have either slipped through the primary security software, or rendered itself immune to detection by it. There are documented cases of CryptoLocker being downloaded and installed by Zeus or other malware that was already present on an infected computer, without a user opening an e-mail attachment.

"Keep your operating system and software up to date with patches" is Sophos' third tip. Software publishers often release patches and updates to close newly detected security vulnerabilities. According to Sophos, "This lessens the chance of malware sneaking onto your computer unnoticed through security holes."

Number four on the Sophos list of tips is, "Review the access control settings on any network shares you have, whether at home or at work. Don't grant yourself or anyone else write access to files that you only need to read. Don't grant yourself any access at all to files that you don't need to see—that stops malware seeing and stealing them, too."

Sophos concludes its list of five tips with, "Don't give administrative privileges to your user accounts. Privileged accounts can "reach out" much further and more destructively both on your own hard disk and across the network. Malware that runs as administrator can do much more damage, and be much harder to get rid of, than malware running as a regular user."

Using the lessons learned during National Cyber Security Awareness Month, such as "don't click on and open e-mail attachments," being aware of the tremendous threat and damage that the rapidly spreading CryptoLocker Ransomware can wreak, and following the five safety tips recommended by Sophos, our computing safety and security may be much improved. Remember that in computers, as well as in other aspects of life, prevention is far better than the alternatives.

WEBSITES

<bibliography>
<http://www.dhs.gov/national-cyber-security-awareness-month>.

<http://www.fbi.gov/news/news_blog/national-cyber-security-awareness-month-2013>.

<https://en.wikipedia.org/wiki/Cryptolocker>.

<http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/>.
</bibliography>

<http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>.

<http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/>.

<https://en.wikipedia.org/wiki/Key_size>.

<https://www.us-cert.gov/ncas/alerts/TA13-309A> This link is provided for informational purposes only and does not represent an endorsement by or affiliation with the US-CERT (DHS).

GRAPHICS

<http://blog.emsisoft.com/wp-content/uploads/2013/09/crilock.png>.

<http://blog.hotspotshield.com/wp-content/uploads/2013/07/who-is-spying-on-you.png>.

Ira Wilsker is a Columnist for The Examiner, Beaumont TX and Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX. Contact him at <iwilsker@sbcglobal.net>.

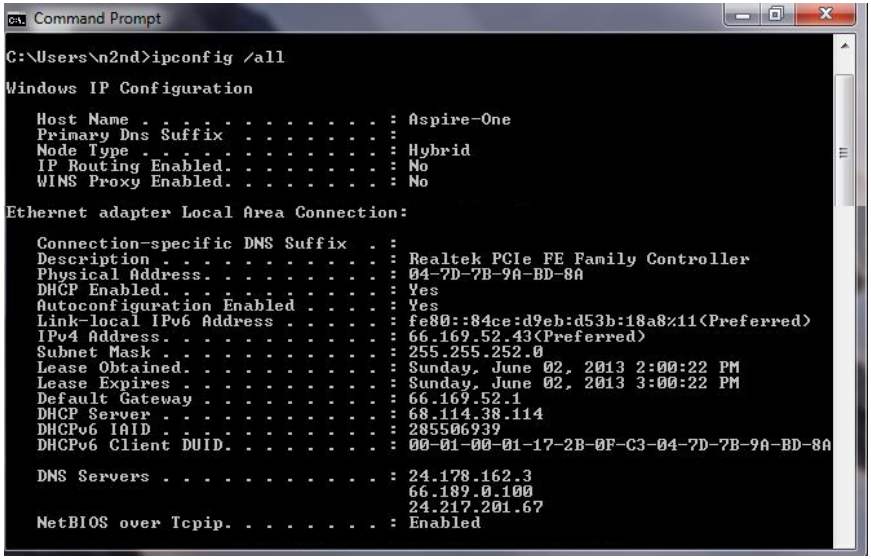
Home Networks
By Dick Maybach

Learning about networks, especially the Internet, can easily become mind-numbing, largely because the field is so full of jargon and acronyms. While it is not possible to escape this morass completely, we can make it somewhat more manageable by approaching the topic in two stages: (1) a single computer connected to the Internet and (2) a home network connected to the Internet.

Every device connected to the Internet, no matter its location in the world, has a unique Internet Protocol (IP) Address. This is usually written as four three-digit numbers separated by periods, where the value of each number varies from 0 to 255. Although we usually think of a site's address as being its Uniform Resource Locator (URL), this is just a convenient representation. When you send a message to a URL, your computer uses a Domain Name System (DNS) server, usually a service provided by your Internet Service Provider (ISP), to find the associated IP address. For example, *http://www.google.com* is assigned the IP address 74.125.140.105. You, of course, must have your own IP address so that you can receive data. (You can find it by browsing the site <http://whatismyipaddress.com/>.) Your ISP assigns an IP address to your computer when you connect it to the Internet using a Dynamic Host Configuration Protocol (DHCP) service. This means that your ISP must own enough IP addresses to supply a unique one to each user, and normally each home user has only one. If you have only one computer and you plug it directly into the ISP's modem, this is sufficient.

Before introducing any more complexity, let's see what we can learn about our Internet connection. Use an Ethernet cable to connect your PC directly to the Wide Area Network (WAN) modem provided by your ISP. You will have to reboot your PC and probably the WAN modem to establish an Internet connection. If you use Windows, navigate through *All Programs* and *Accessories* to *Command Prompt* and type "ipconfig /all". (The equivalent Linux and OS-X command

is "ifconfig" or "ip".) There are graphical programs that show the same information, but ipconfig puts it all on one screen. (The screenshot shows only the first portion the command's output.)



Fortunately, not all of the displayed data is important, but note the following items.

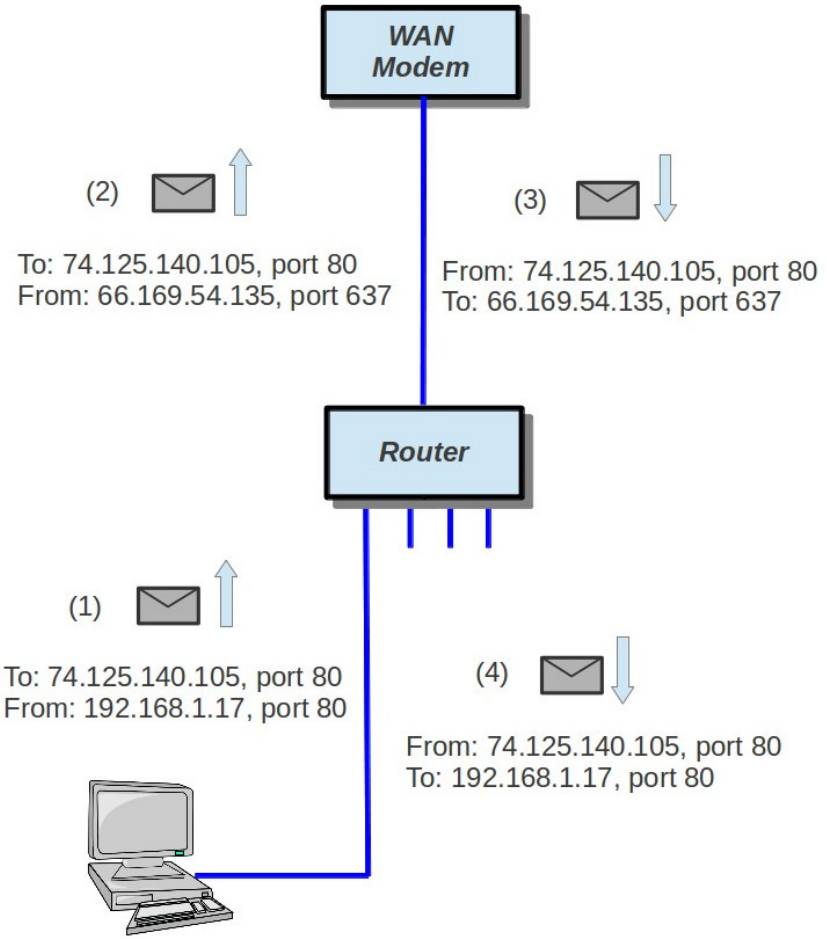
- DHCP is enabled and its server is located at 68.114.38.114, and the ISP used it to assign the IP address 66.169.52.43 to this particular PC.
- This address is valid for one hour (as shown by the Lease Obtained and Lease Expires times). Before the IP address lease expires, your PC will automatically request a renewal.
- The hard-wired address of the Ethernet interface in our PC is 04-7D-B-9A-BD-8A.
- One of the DNS servers at 24.178.162.3, 66.189.0.67, or 24.217.201.67 translates URL to IP addresses.

If ever you lose your Internet access, a good first step would be to repeat the above procedure to see whether the problem is in your home network or within your ISP.

However, many of us want to connect several devices to the Internet. How can we do this with only one IP address? There are blocks of IP addresses which never appear on the Internet, but are reserved for local use. The devices on most home networks use the addresses 192.168.1.x, where where x varies from 0 to 255. (The 1 in the third group could be replaced with any number from 0 to 255.) If your network is using the 192.168.1.x plan, it knows that any IP address in this range belongs to a local device and any IP address outside this range resides on the Internet. To make use of this, we purchase a router and connect our local network devices to it. [*Editor's note: frequently the modem and router are in the same case.*] It has a separate connector for a cable to our ISP's modem. The router, as its name suggests, directs any local messages to internal addresses and sends all others to the ISP, but first it changes their

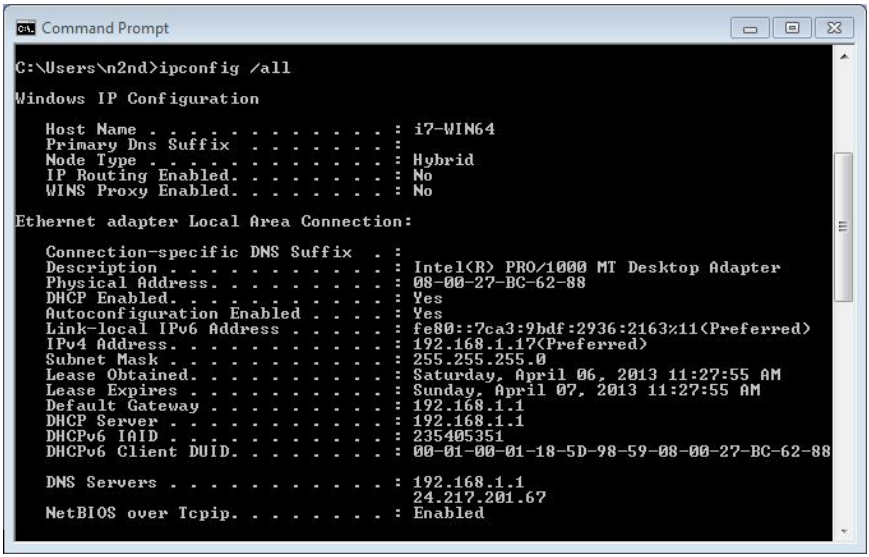
return address to the IP address the ISP has assigned. But this means that all incoming messages have the same IP address; how does the router get them to the correct local device? Each message has not only an IP address, but also a 16-bit port number, and the router changes the port numbers of the return addresses of outgoing messages. It keeps track of these and when an incoming message appears, changes its address to the appropriate local device and restores the original port number. This process is called Network Address Translation (NAT).

In the figure, our PC generates a message (1) to Google at 74.125.140.105 using Port 80. (It probably consulted an DNS server to obtain Google's IP address.) In this case, the ISP has assigned us the IP address 66.169.54.135, and the router changes the return address to this (2) and changes the port to 637. When Google replies (3) to the only address and port it knows, the router consults its records and sees (4) that messages from Google to port 637 should be routed to local IP address 192.168.1.17 and Port 80. Your neighbor may also be using 192.169.1.17 as the local IP address for



one of her PCs, but since her Internet IP address is not 66.169.54.135, she won't get your messages from Google.

If your home network includes a router, you should now reconnect it to the WAN modem and restore the original network connection for your PC. Again, use *ipconfig /all* (or *ifconfig*, as appropriate) and compare the results with those you obtained with the PC connected directly to the WAN modem. Again, the screenshot shows only the first portion of ipconfig's output.

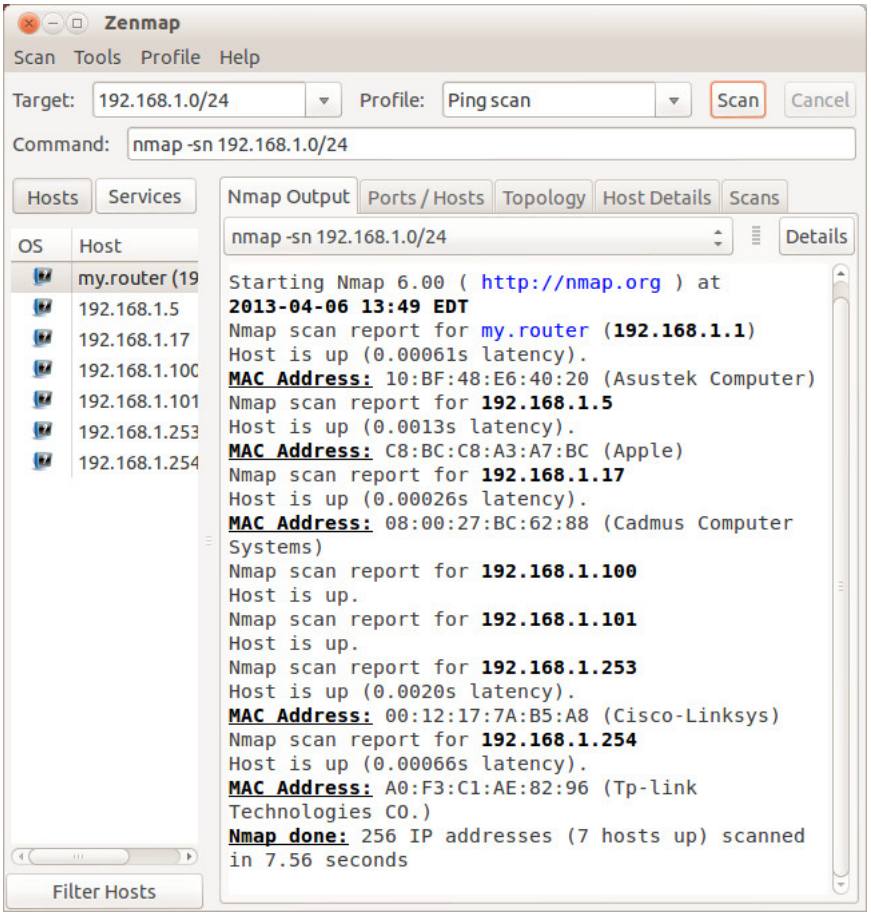


Note the changes. (Ignore the change of Host Name and physical address; this is for a different PC.)

- The IP address now begins with 192.168.1, which is a local one, as is the default gateway.
- The DHCP server is now our router, which assigns all the devices with IP addresses of the form 192.168.1.x.
- There are two DNS servers, one in the router for local devices and one at the ISP for the Internet. (Note that the latter is one of the three we saw when connected directly.)

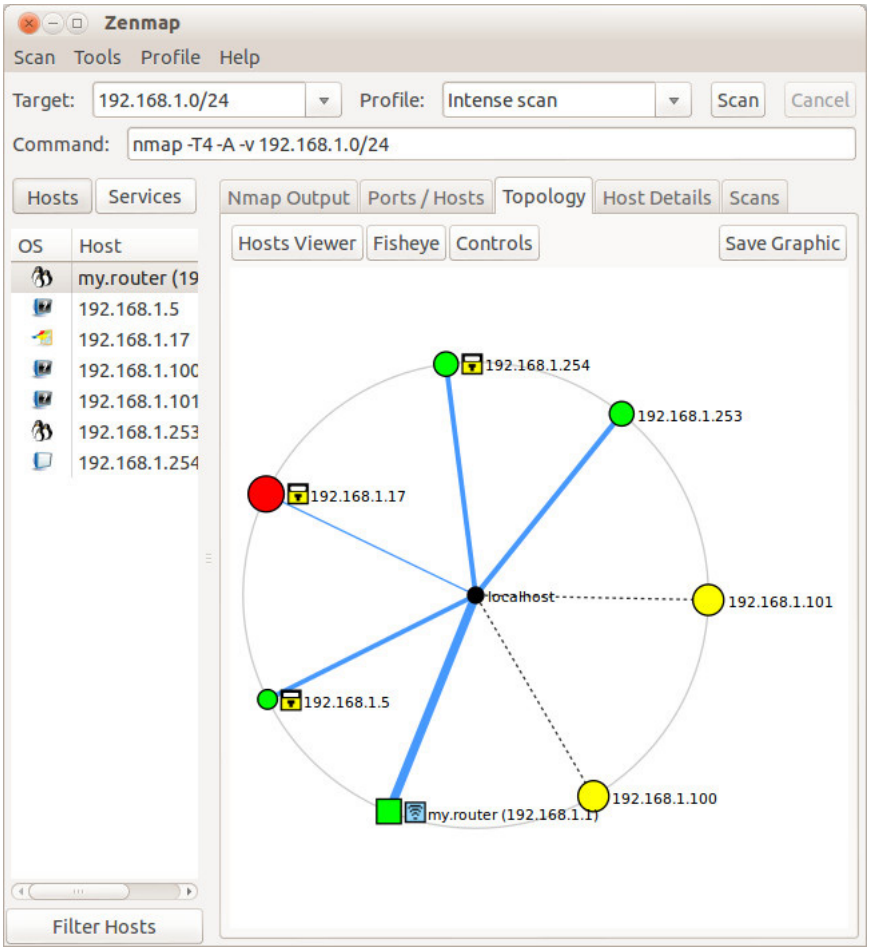
Zenmap <http://nmap.org/zenmap/>, available for Linux, OS X, and Windows, is a very valuable tool for exploring your local network. Pay special attention in the following discussion of how you can limit its probes to your local network, as its activities can look like you are trying to hack any computer it probes. Some system administrators are quite sensitive to these, and using them could result in unpleasant conversations with your ISP or legal authorities. The screenshot on the next page shows the results of a simple ping scan of my local network. Note that the target was 192.168.1.0/24. My network uses the addresses 192.168.1.x, where x varies from 0 to 255. Each field in the IP address is actually an 8-bit number, and the /24 tells Zenmap that it should not change the first three fields. (Three fields times 8 bits equals 24.) Thus it probes all the addresses from 192.168.1.0 through 192.168.1.255. If we had specified 192.168.0.0/16, Zenmap would have probed 192.168.0.0 through 192.168.255.255, and while

this wouldn't probe outside your local network, it could take a long time. The result is shown below.



Seven devices are operating; since the first three fields of their IP addresses are the same, I'll designate them by only the last field. Our router is located at 1; 5 is a PC with an Asustek motherboard; 17 is a Windows 7 PC, 100 is the Ethernet adapter and 101 the wireless card of my desktop PC; 253 is a wireless access point; and 254 a network switch. A ping scan is quite simple; we are just looking for an answer from each address. We can learn much more by performing an intense scan, which takes several minutes, compared to the few seconds for a ping scan, and the results fill several screens. Fortunately, Zenmap can sumarize its results graphically.

In the graphic on the next page circles indicate computers, and squares indicate routers. The colors and sizes of the nodes indicate how many ports are open; a greater number of open ports implies a greater vulnerability to outside hacking. (Green is good, yellow less so, and red could be something to be concerned about.) The thickness of the line to localhost indicates the round-trip delay; thick means slow.



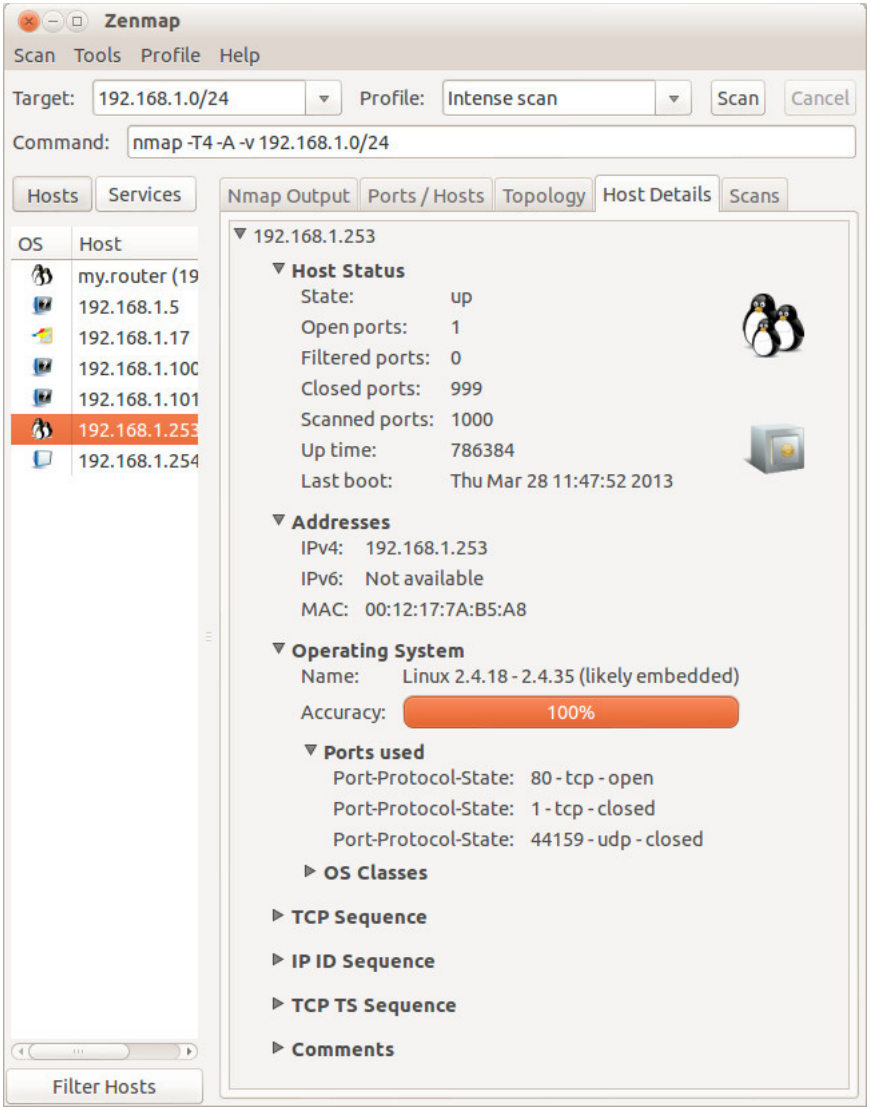
(I made this probe from the PC with addresses 100 and 101, so delays can't be measured here.) The square yellow icon is a padlock indicating that some of the ports are filtered, which lessens the vulnerability to hacking. Finally, the square blue icon indicates a wireless access point. (Clearly, the detection isn't perfect, because 253 is also a WAP.)

The host details tab shows what Zenmap has found about a particular computer (graphic on next page).

In this case (the WAP), the operating system is Linux and the one open port is 80.

Zenmap can also show you the route your data takes as it travels to its final destination. For example, let's again use www.google.com at 74.125.140.105. We enter this into the target box and select *Quick traceroute* as the scan. The screenshots on pages 13 and 14 show both the text and graphic results.

In this case, our test message made 16 hops on its way to Google, although other tests would provide slightly different results. You can also view these results graphically, but I find the text output easier to understand and to be more complete. There are other

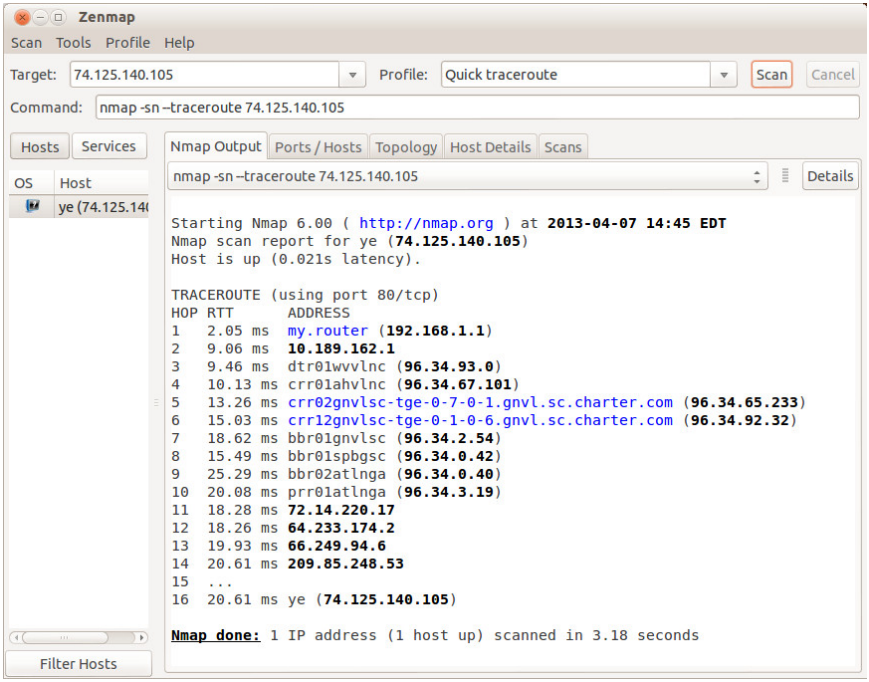


network tools, but Zenmap is included in the Parted Image toolkit (discussed in my April 2012 article, available at <http://www.bcug.com>), which I always have with me. There is extensive documentation for this useful program on the Zenmap Web site, accessible through the Help menu button visible in the screen-shots.

Taking a few minutes to explore your home network will remove much of its mystery and could prove valuable in solving future problems.

Dick Maybach <n2nd (at) charter.net> is a member of the Brookdale Computer Users' Group, NJ <http://www.bcug.com>.

This article first appeared in the July 2013 issue of BUG Bytes.



End of article from preceding page.

Free and Deeply Discounted Software at SharewareOnSale.com By Ira Wilsker

For several years, one of the best sources of objective software reviews, evaluations, and tips has been on dotTech.org <http://dotTech.org>. Under the active leadership of the well respected "Ashraf," dotTech.org has developed an impeccable reputation for honesty when evaluating software and related computer components. For many PC users, Ashraf has become the resident guru on software, and they loyally and faithfully follow his evaluations and recommendations. On an unaffiliated software giveaway website, GiveawayOfTheDay.com (GOTD) <http://Giveaway OfTheDay.com>, best known for its free daily giveaway of one legally licensed commercial software product, Ashraf's comments and review of the day's single software offering are strongly considered by many of the GOTD users before deciding whether or not to download and install the day's offering. Ashraf's opinion appears to influence the daily volume of downloads.

DotTech.org has now been online for five years (October, 2008), and is viewed on a daily basis by thousands of visitors. Ashraf has expanded the online services that he offers with the creation of his Azadi Network, which he describes as, "…a web-based company that provides solutions for the digital age." Azadi is an Urdu word which means "freedom," a concept that Ashraf apparently encourages on his websites. Recently (August, 2013), Ashraf expanded his Azadi Network to include a

second website, SharewareOnSale.com <http://SharewareOnSale.com>. Again, according to Ashraf, "SharewareOnSale connects software developers with users, offering daily software deals of free and heavily discounted programs. Although it is a relatively new service, SharewareOnSale has already garnered much attention around the world."

I first found out about SharewareOnSale.com while researching a particular software product on dotTech, and noticed a banner promoting SharewareOnSale. Now, SharewareOnSale is one of the first websites that I visit every day. In order to be better informed about new bargains offered on the site, I chose to sign up for the once daily e-mail that lists that day's offerings; it is important to check the website frequently as the offerings are very dynamic, and frequently changing. Product offerings that may appear on the site early in the day may possibly "expire" before the end of the day as a limited time offer may expire, or a finite quantity of available product may be downloaded, completing the offering prior to a stated expiration of the offer. On two excellent recent offers, both now expired, the offers quickly became unavailable prior to their stated expiration. One was a free, one-year "extended trial" of a newly released and updated, fully functional, comprehensive security suite, AVG Internet Security 2014. On SharewareOnSale.com it was a legitimate free download, rather than paying the $55 charged on the AVG website for the same product. I registered on the SharewareOnSale website (one time, simple and free), put the program in my shopping cart, and checked-out with a zero balance due, with no credit card or PayPal necessary to pay for the free item. On the following screen were download links for both the 32- and 64-bit versions, which were pre-registered and fully activated when installed. Even though the AVG Internet Suite 2014 was labeled as a fully functional, not crippled in any way, trial version, the expiration date of the trial was a full year in the future. All services and updates would be available for a year, no different than any other program with an annual license. When I downloaded the AVG Internet Security 2014, SharewareOnSale said that the offer was still good for five more days, but just two days later this particular offer was listed as "expired" <http://sharewareonsale.com/s/free-avg-internet-security-2014-54-99-value>.

Another offer that I was fortunate enough to take prompt advantage of, prior to its quick expiration, was a free download of the $40 Wondershare Video Converter Pro <http://sharewareonsale.com/s/free-wondershare-video-converter-pro-39-95-value>, an excellent program for converting videos in almost any video format to almost any other video format, including dozens of formats for PC, Mac, online, YouTube, and individual smart devices. I told one of my neighbors about it the day that I downloaded and installed Wondershare Video Converter Pro, but by the next day, when he went to download it, the offer had already expired. The important object lesson here is to frequently check the SharewareOnSale.com website, and download (or purchase) any desired item right away, as tomorrow may be too late.

On the positive side, as mentioned above, is that the content on the site is

very dynamic, as new software items are very frequently added, and other offers expire. As I type this, there are several interesting deals posted, which may likely expire before readers of this column have a chance to get them, but new offers will inevitably replace the expired ones after this column is published. Some of the items currently available (which will likely expire soon and be replaced with new offers) are:

SoftOrbits Sketch Drawer Pro, a $79.95 value, available free for a very limited time; this product can, "turn your digital photos into works of art! SoftOrbits Sketch Drawer Pro converts photos/images to sketches in just a few clicks."

SoftOrbits Photo Digital Suite Personal on sale for $4.99 ($349.95 value if each component purchased individually, or $99.95 if purchased together as a suite). According to the posting, "SoftOrbits Digital Photo Suite Personal is a software pack of 10 software titles: Batch Picture Resizer, Photo Stamp Remover, Batch Picture Protector, Html Web Gallery Creator, Red Eye Removal, Private Photo Album, Flash Drive Recovery, SoftOrbits Photo Retoucher, SoftSkin Photo Makeup, and Sketch Drawer."

GiliSoft #1 Video Tools on sale for $4.99 ($380 value). "GiliSoft #1 Video Tools is a 7 + 2 software bundle of nine different programs: seven programs by GiliSoft (Video Converter, Screen Recorder, Video Editor, Slideshow Movie Creator, Movie DVD to Video, Movie DVD Backup, Movie DVD Creator) and two bonus gifts by EaseUS (Data Recovery Wizard and Partition Master Pro)."

Tenorshare Data Recovery WinPE on sale for $2.99 ($39.95 value). One of my personal favorites for recovering deleted or damaged files, "Tenorshare Data Recovery WinPE lets you recover lost, damaged, formatted or deleted data from a bootable/recovery CD/DVD/USB without booting into Windows."

Free BlazeVideo SmartShow ($49.95 value). " BlazeVideo SmartShow offers you the easiest way to create a unique movie with your favorite pictures, video clips, music and voice-over."

While it is somewhat inevitable that many, if not all of these offers will expire prior to publication, Ashraf has been very good at keeping SharewareOnSale.com well stocked with an assortment of free and deeply discounted software products. Examples of some of the other now expired offerings include Wondershare PDF Converter, a $60 utility given away for free, that can convert PDF files in a large variety of other editable formats including Word; RoboForm Everywhere, a very popular $20 password manager, that was also available for free for a limited time; Process Lasso Pro, an excellent $15 system and memory manager, that was available for free; Paragon Partition Manager 12, a very popular $40 hard drive partition manager, that was available for $2.99; Ashampoo Burning Studio 2013, a comprehensive $40 CD and DVD burning utility, that was given away for free; and dozens of other utilities that were either given away for free or sold for very nominal prices. As each of these offers expired, they were replaced by newer offers, a cycle that has been repeating since the inception and availability of the service.

It is somewhat amazing that Ashraf has been able to compile and make available several dozen decent utilities of various types, during the two months

that SharewareOnSale.com has been in existence. For those who may like notice of the free or bargain software available, I recommend signing up for the free, once daily e-mail announcing the offerings, using the form on the top right of each SharewareonSale.com web page. Just like our local weather, if you do not see anything that you like, just come back in a few minutes or tomorrow, and the offerings will likely be different.

WEBSITES

<http://sharewareonsale.com>.
<http://dottech.org>.
<http://azadinetwork.com>.
<http://giveawayoftheday.com>.
<http://sharewareonsale.com/s/free-softorbits-sketch-drawer-pro-79-95-value>.
<http://sharewareonsale.com/s/free-avg-internet-security-2014-54-99-value>.

Ira Wilsker is a Columnist, The Examiner, Beaumont TX; Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX. Contact him at <iwilsker@sbcglobal.net>.

The Mac Corner—July 2013
By Danny Uff

Because OS X sits on another operating system called Unix, it handles files differently than a Windows computer. This is because each file on that computer has what we call Permissions. Permissions tell Unix what it can do with the file—if it can read it, or write data to it, etc. But sometimes (for whatever reason) those permissions get changed around. So, let's say that a data file that had permission to be written to the day before, does not have that same access the next day—yes, it does upset you—believe me, I know!

All Macs come with a utility called Disk Utility. It is located in the Finder in the Utilities Folder. From this app, one can "repair" the file permissions of all files on a Mac. Here's how to use Disk Utility to verify and/or repair permissions:

1. Go in to Disk Utility: Finder → Utilities → Disk Utility.
2. Click on the Mac's hard drive icon (upper-left).
3. Now, go down one space to the name of your hard drive (usually named Macintosh).
4. On the lower-left of the second window panel is a button that says Verify Disk Permissions. Click it.
5. Disk Utility will now verify and repair any permissions that may have gotten changed.

Some tips:

- Make sure all data files are closed (such as a text document) so Disk Utility can repair the file correctly. This should be done with hard drives and SSDD drives as well.
- Although Apple says you do not have to, reboot the Mac after Disk Utility is finished. This will guarantee you're using the newly repaired permissions.
- You should do the above at least once a month to help your Mac run as smoothly as it can.

Well, that's it for this month. Thanks for reading.

Danny Uff <danny.uff@gmail.com> is a member of Lehigh Valley Computer Group, Pennsylvania <http:// www.lvcg.org>

This article first appeared in the July 2013 issue The LVCG Journal.

What To Do If You Think Your E-mail Has Been Hacked By John King

The first thing to do if you worry about e-mail hacking is to change your e-mail account password to something more complex than 123456. For best security, use a password such as Q*93im#&qrR-57$. You'll never remember it and won't have any more e-mail problems [insert snicker].

My Hotmail account was hacked a while ago. A human hacker or automated bot was indeed sending spam from my account on Hotmail. My local computer wasn't involved. Everything was happening on the Hotmail computers.

Spammers like to use other people's e-mail accounts to send spam because it's free and makes the spam harder to block. After I changed my weak Hotmail password to a stronger one, the spammer/bot couldn't access my account; and the problem ended.

Alternatively, a spammer may be simply spoofing the return address of the spam using your e-mail address to make the message less likely to be blocked. There's nothing that you can do to stop that. You could stop using that e-mail address, but the spammer can keep using it as the return address anyway.

Fortunately, spam with your spoofed return address usually stops in a few days or weeks at the most. The spammer probably found your address without hacking your account, for example, from the address book of a friend, an intercepted e-mail, etc. Nonetheless, changing your e-mail password is still a good idea.

If your e-mail is a POP account, as opposed to a web mail account such as Hotmail or Gmail, the odds are higher that your computer has been hacked, which is a much larger problem. The best solution is to restore a backup system image made well before the hacking was suspected. The chance that you have a backup image to restore is as likely as the intruder putting money into your bank account, but this instance is when you want backups. Lacking a backup, you can thoroughly scan your system with several anti-malware products in addition to your normal anti-virus product.

Again, you should change the passwords for your Internet Service Provider, router, and e-mail, and be sure that your Wi-Fi network is protected with the highest level of security possible. People often hate passwords on computers; but if any computer on the network was hacked, all computers on the network should have logon passwords. Fortunately, protecting the network is enough in most cases.

Personally, I'd suggest you change your e-mail password, scan your computer with your up-to-date anti-virus software, and wait to see what happens. If possible, do not do any online shopping or banking until some time has passed to confirm that only your e-mail was hacked. Also watch for any suspicious activity on credit card and bank accounts.

John King <editor (at) ggcs.org> is a Contributing Editor for the Golden Gate Computer Society <http://www.ggcs.org>.

This article first appeared in the July 2013 issue of GGCS Newsletter.

The November 10, 2013 SEMCO Board Meeting minutes had not been received by the deadline.

SPECIAL INTEREST GROUPS (SIGS)

SIG-COMPUTING
Tom Callow

December 8 1:45 p.m.: Bitcoin—The Future of Money: David Smith will introduce Bitcoin and then discuss it from a practical point of view. Answering questions such as: What is Bitcoin? How can I get Bitcoin? Can I create Bitcoins? What can I use Bitcoin for today? What are the legal issues surrounding Bitcoin? Why is Bitcoin valuable? How can I learn more?

SIG-PROGRAMMING
Richard Jackson

December 21 (Sat.) 2:00 p.m.: Visual Basic 2010 Express: Chapter 9 including the associated programming exercises of the book "Microsoft® Visual Basic® 2010 Step by Step." **Where:** Richard Jackson's home. Call Richard at 248-546-3694 for directions.

SIG-LINUX
Brian Brodsky

January 28 (Tues.) 6:45 p.m.: SIG-Linux will not meet in December due to the holidays. Where: Richard Jackson's home, 10495 Kingston, Huntington Woods, MI 48070. Call Richard at 248-546-3694 for directions.

SIG-TECHNIQUES

December 8 3:45 p.m.: Learn your way around Excel: SEMCO member Jean Blievernicht will cover essential worksheet operations such as moving around, adding, deleting, hiding columns, naming ranges, filling in a series, manipulating data, and more. Some of the functions will be introduced with examples. You'll be shown how to work with several sheets simultaneously. There will be an example of a real world problem and the steps taken to get the solution. Other topics will be introduced if time permits.

SIG-ADVICE
Bob Clyne

December 3 (Tues.): 5:30 p.m.: General discussion. If you have computer related questions or problems, come to the meeting and we will discuss possible solutions. **Where:** At the Madison Heights Library, 240 West 13-Mile Rd. one block west of John R. The parking lot and entrance to the library are located on the north side of the library off Brush St.

January DATA BUS DEADLINE (7th day after 2nd Sunday in month)

SEMCO Input and Members' Ads—Deadline: Sun., December 15, 11:59 p.m.

Members' personal ads are free. To mail, use Editor address on Page 2; e-mail address: <clyne@mich.com>. PLEASE send to arrive sooner than deadline.

COMP (Computer Operators of Marysville & Port Huron)
December 4, 8 p.m. The Dorsey House, 6008 Beard Rd., Clyde, MI 48049. Jane Wheatly 810-982-1187 or Pam Raisanen E-mail: <bwcompinfo@gmail.com>. Web: <http://www.bwcomp.org>. Topic: Christmas Dinner (see web site for details).

DITUG: Detroit IT User Group (Formerly Focus: Hope IT User Group)
1400 Oakman, Detroit, MI. 48238. Web info <http://www.ditug.org/>. See web sites for details. Pre-registration required.

HUG (Holly User Group)
December 14, 9 a.m.–noon (2nd Saturday) Groveland Twp. Fire Hall, 3085 Grange Hall Rd. & Dixie Hwy., Holly, MI. 48442. Ron McCauley 810-629-9683. Topic: TBA.

MacGroup-Detroit
December 15, 3:00 p.m., Birmingham Temple, 28611 West 12 Mile Rd., Farmington Hills. Info: Terry White, <terry@macgroup.org> or 248-569-4933 <http://www.macgroup.org>. SIGs: 2:00 PM. Topic: How to take advantage of cloud storage.

MacTechnics, (MAC User Group)
December 14, 9 a.m.,See web site for details and location <http://www.mactechnics.org>. JoAnn Olson at 248-478-4300. Topic: Holiday Party.

MDLUG (Metro Detroit Linux User Group)
December 14, 12:30 p.m., (2nd Saturday); Michigan Network Services, 1677 W. Hamlin Rd., Rochester Hills, MI 48309. Web: <http://www.mdlug.org>. Topic: TBA.

Motor City Free Geek
Every Saturday 1 p.m. to 5 p.m. 1511 Jarvis St. Suite #10, Ferndale, MI 48220 <http://www.motorcityfreegeek.net>. E-mail: <MotorCityFreeGeek@gmail.com>. Recycling & Open Source.

MUG (Michigan User Group)
December 10, 6:30 p.m., (2nd Tuesday): Farmington Community Library-Main Branch, 32737 W. 12 Mile Rd., Farmington Hills, MI. 48334. <http://www.mug.org>. Topic: TBA.

Oak Park Computer Club
Every Fri., 10:30 a.m. at Panera Bread—in the Cornerstone Mall (on the west side of Greenfield, south of Mt. Vernon) just north of Kroger. Including Q&A.

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://tinyurl.com/royaloakcc>.

SHCC (Sterling Heights Computer Club)
December 3, 7:30 p.m. (1st Tues); Macomb Community College South Campus, Bldg. K, 14500 E. 12 Mile Rd. Don VanSyckel <Don@VanSyckel.net>, 586-731-9232; Web: <http://www.SterlingHeightsComputerClub.org>. Topic: Finding Great Deals on Tech Stuff.

SEMCO

Serving the needs of professionals, hobbyists, novices, and prospective computer users since 1976.

* Learn more about computing in an informal, non-academic setting.
* Get honest answers to computer questions without commercial bias.
* Meet and interact with other computer users. Personal and electronic networking.
* Gain access to members willing to provide help in response to a phone call or e-mail.
* Receive monthly newsletter with informative articles.

Help Wanted–Presenters

SEMCO needs members to do meeting presentations. We have meeting presentation slots that we need to fill and there is probably some aspect of computing that you could do a presentation on, whether it's hardware or software; PC, Mac, tablet, smartphone or some other electronic device; Windows, Mac, iOS, Android, Linux or some other OS; an 'app,' utility or other program. Contact Richard Jackson 248-546-3694 or Tom Callow 248-642-5770 9–5 if you can help.

COMPUTER RESOURCE PEOPLE

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

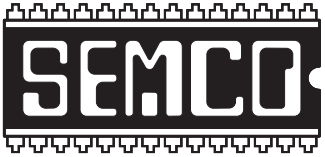
Are you willing to help members learn?

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
Geocaching: Cook
IBM PC Hardware Issues: Clyne, Yuhasz
Linux: Brodsky
Mac Hardware and OS Issues: Yuhasz
MS Office for Windows: Callow
MS Word: Clyne
Networking: Callow
Novell Netware: Yuhasz
Operating Systems: Callow, Clyne, Yuhasz
Quicken: Clyne
Security: Bader

Bader, Mike—586-447-6683, 9 am–8 pm..... mdbader@flash.net
Brodsky, Brian— 248-391-9125, 5–7 pm+weekends .. brianbrodsky@ameritech.net
Callow, Tom—248-642-5770, 9 am–5 pm..... tcallow@monaghanpc.com
Clyne, Bob—810-387-3101, 9 am–10 pm ..... clyne@mich.com
Comptois, Jerry—248-651-2504, anytime
Cook, Stephen—313-272-7594, eves..... scook48227@ameritech.net
Lis, Bernie—248-669-0101, 10 am–8 pm..... BerlLis@comcast.net
Vander-Schrier, Jack—586-739-7720,12–8 pm ..... jvanders@comcast.net
Yuhasz, Steve..... Help@yuhasz.org



SOUTHEASTERN MICHIGAN COMPUTER ORGANIZATION, INC.

SEMCO CALENDAR

Engineering Society of Detroit
20700 Civic Center Dr., Suite 450, 4th Floor
Southfield, MI. 48076

December 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-COMPUTING, 1:45 p.m.: Bitcoin—The Future of Money: David Smith will introduce Bitcoin and then discuss it from a practical point of view. Answering questions such as: What is Bitcoin? How can I get Bitcoin? Can I create Bitcoins? What can I use Bitcoin for today? What are the legal issues surrounding Bitcoin? Why is Bitcoin valuable? How can I learn more?

SOCIAL PERIOD, 3:15 p.m.: Refreshments! (Reminder: Keep it neat & tidy.)

SIG-TECHNIQUES, 3:45 p.m.: Learn your way around Excel: SEMCO member Jean Blievernicht will cover essential worksheet operations such as moving around, adding, deleting, hiding columns, naming ranges, filling in a series, manipulating data, and more. Some of the functions will be introduced with examples. You'll be shown how to work with several sheets simultaneously.

SIG-PROGRAMMING, December 21 (Sat.) 2:00 p.m.: Visual BASIC 2010 Express: Chapter 9 including the associated programming exercises of the book "Microsoft® Visual Basic® 2010 Step by Step." **Where:** Richard Jackson's home at 10495 Kingston, Huntington Woods, MI 48070. Call Richard at 248-546-3694 for directions.

SIG-ADVICE, December 3 (Tues.) 5:30 p.m.: General discussion. At the Madison Heights Library located at 240 West 13 Mile Rd. one block West of John R. The parking lot entrance is off Brush St. The lot and entrance to the library are located on the north side of the library.

SIG-LINUX, January 28 (Tues.) 6:45 p.m.: No meeting in December due to the holidays. Where: Richard Jackson's home at 10495 Kingston, Huntington Woods, MI 48070. Call Richard at 248-546-3694 for directions.

December 8—SEMCO Sunday.

http://www.semco.org

PUBLIC INVITED

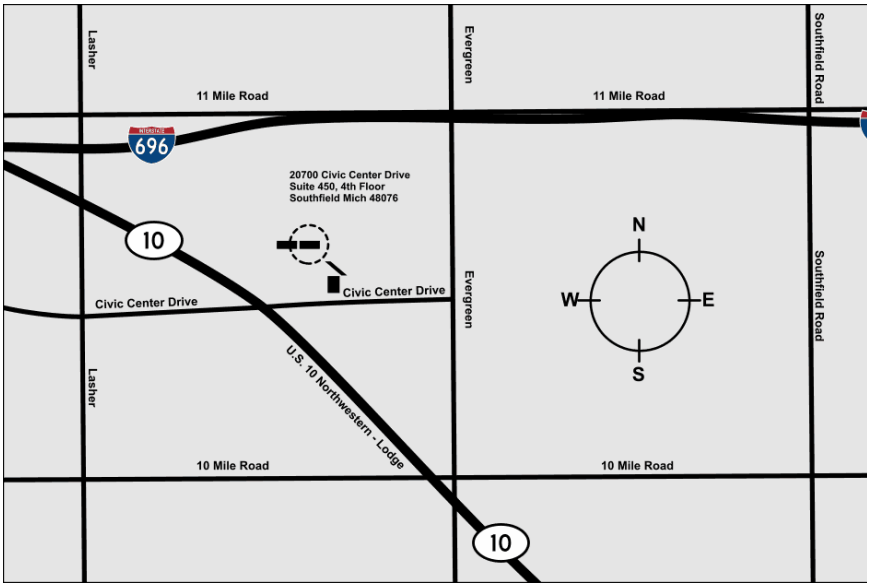
(Please copy this and the next page to post on your bulletin board.)

SEMCO Meetings at [Engineering Society of Detroit](#)

20700 Civic Center Drive, Suite 450, 4th Floor

Southfield MI 48076.

42°29'7" N by 83°14'29" W



From I-696 exit at Evergreen. Take Evergreen south to Civic Center Drive. Civic Center Drive is about halfway between I-696/Eleven Mile Rd. and 10 Mile Rd. Turn west, right if you are coming from the north, onto Civic Center Drive. Follow Civic Center Drive, watching the number signs on the right. When you get to the 20700 sign turn right, north, and follow the drive until you arrive at the southwest corner of the brown building with the Engineering Society of Detroit sign near the top. Turn right, east, and go past the front of the building. When you reach the end of the building, turn left, north and go to the back of the building and turn left, west, again. The parking lot will be on your right. The entrance is in the center of the building. Park in back of building. Enter the rear door. The ESD office is on the fourth floor.

ESD
THE ENGINEERING SOCIETY OF DETROIT®
FOUNDED IN 1895
Affiliate Society

GITCA

Member of
apcug
An International
Association of Technology
& Computer User Groups

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

SEMCO (future meetings)
December 8
January 12

FIRST CLASS MAIL
Dated Material

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