THE BUG REPORT

A Publication of the Greater South Bay PC Users Group

May 2012

INSIDE

It's spring fever. That is what the name of it is. And when you've got it, you want - oh, you don't quite know what it is you do want, but it just fairly makes your heart ache, you want it so!

~Mark Twain

Meeting — May 7

President's Thoughts

By U. A. Garred Sexton

At our last **general** meeting, Phil Cohen from the South Bay Camera Club demonstrated how he develops a web site. Examples that he showed were from the South Bay Camera Club http://www.sbccphoto.org/ and the Southern California Live Steamers Club http://www.southerncalifornialivesteamers.com.

Phil developed these websites and programmed them with unique capabilities that were very impressive. Each page is kept up to date by a club member who is assigned to the particular area. To update the pages is very simple so that almost no training is required for the updaters. For the general membership, there is access to a 'blog' page that can be used by any club member to ask questions or make comments to which any other members may respond. (Shades of the Bulletin Board days for you old-timers.) Also another area is provided on the website for members to post useful information, including videos. You may check some of this out by visiting the URLs noted above.

Phil's presentation will help us re-design and modernize our present site. Please give any Board Member your thoughts and feedback so we can include them in our planning.

Greg Neumann and Lou Little, our program co-chairs, are planning some interesting meetings for the future. They will let you know as far in advance as possible about each program's details.

**Greater
South Bay
PC Users Group**

A member of
Association of Personal Computer User Groups

MEMBERSHIP

Membership is available for twelve months from the date of joining. Membership rates:

Individual	$36.00
Student	$18.00
Family	$48.00
Newsletter Subscription	$18.00

Checks payable to GS-BUG, Inc.
Mail to:
GS-BUG, Inc. — Membership
635 W. 61st St.
Los Angeles, CA 90044

THE BUG REPORT

A monthly publication of GS-BUG, Inc. Reproduction of any material herein by any means is expressly prohibited unless written permission is granted. Exception: Articles may be reprinted by other user groups in unaltered form if credit is given to the author and the original publication.

SUBMISSIONS

All submissions to the GS-BUG Report must be unformatted on PC disk or e-mail (no hardcopy). Limit formatting to bold or italicizing. We reserve the right to edit as necessary for space consideration. Art work submitted must be in a common graphics format (.jpg, .tif, etc.)

DISCLAIMER

All opinions herein are those of the individual authors only, and do not reflect the opinions of GS-BUG, Inc. The group does not intend to endorse, rate or otherwise officially comment on products available and readers are cautioned to rely on the opinions presented at their own risk.

Articles are compiled without verification of accuracy or application to a special task or computer. GS-BUG, Inc., its contributors and the editor do not assume any liability for damage arising out of the publication or non-publication of any advertisement, article, or any other item in this newsletter.

GENERAL MEETING

General meetings are held at 7:00 p.m. on the first Monday of the month at the Torrance Airport Zamperini Field, 3301 Airport Drive (intersection of Airport Drive & Zamperini Way), Torrance.

BOARD OF DIRECTORS

President	Garry Sexton	310-373-3989
		uags@aol.com
Vice-President	Tom Tucknott	310-530-4992
		ttucknott@socal.rr.com
Secretary	Joyce Oliver	323-778-6256
		oliver_joyce@hotmail.com
Treasurer	George Porter	310-373-5416
		g19porter@verizon.net
Membership	Joyce Oliver	323-778-6256
		oliver_joyce@hotmail.com
Program	Greg Neumann	
		Gbugcaller@aol.com
	Lou Little	310-546-1274
		loulittle182@yahoo.com
Web Master	Shelley Miller	310-541-6796
		seamil19@verizon.net

Directors at Large

Virginia Pfiffner	310-374-2410
	vpfiffne@elcamino.edu
Greg Neumann	Gbugcaller@aol.com

Newsletter Staff

Editor	Marian Radcliffe	818-249-1629
		Marian2Rad@att.net
Proofreader		Virginia Pfiffner

Article

What the Heck are 'hiberfil' and 'pagefile'

By Linda Gonse
Orange County PCUG, California
www.orcopug.org
editor@orcopug.org

One day while purging unnecessary and unused files on my *Windows XP* computer, I spotted two massive files on the C:\ drive that perplexed me. One was hiberfil.sys at nearly 3.5 gigabytes! And, the other was pagefile.sys at 2 gigabytes!

I did not delete them right then and there. First, I checked them out on Google. As it turns out, both of the system files serve a purpose.

Hiberfil.sys is a file the system creates when the computer goes into hibernation mode. *Windows* uses the file when it is turned back on. If you don't need hibernation mode and want to delete the file you need to turn the hibernation option off before *Windows* will allow you to delete the file.

The file size depends largely on the size of active RAM in the computer as the contents of the file are basically a RAM image. That explains why the file was so large. My computer has 4G of RAM — although it only recognizes 3.25 gigabytes.

I couldn't see a need to have hibernate enabled on my computer so I disabled it by unchecking the 'Enable Hibernation' box in 'Power Options' in the Control Panel. (The procedure for turning hibernation off is significantly different between *Windows XP* and *Vista*.)

The next time I rebooted, though, my UPS scolded me for not having hibernation enabled. The UPS unit used that as storage space in case the power goes out and battery power has to kick in.

I was careful to research **pagefile.sys** before taking any kind of action that might compromise it.

Good thing, too. **Pagefile.sys** is the virtual memory file *Windows* uses. Typically, when installed, *Windows* sets the size of the file at around 1-1/2 times the physical memory size. However, the size may vary depending on the amount of free disk space when the file is created and other factors. The default size generally works fine but it can be changed. *Windows* uses this file for its normal operation, but if you really need the space you can delete it after turning the virtual memory option off. Just be aware that this can cause extreme instability in *Windows* — even causing it to stop working. Yikes!

Time is rapidly approaching June 21 to 24, 2012, when the Southwest Computer Conference will be held in San Diego.

This is an interesting get-together for computer club members from computer clubs all over Southern California. One person even comes from Australia. The people are wonderful and the Town & Country Resort provides a beautiful location.

We were most fortunate to convince the Town & Country Resort to reduce their nightly rate for the

conference to $99, which can include up to four in a room. It includes days prior to and following the conference if you want to enjoy some extra time in and around San Diego.

If you are interested, you can sign up for tours to be held on Thursday and Friday through The Microsoft Store and The Apple Store both of which are located in the Fashion Square Shopping Mall adjacent to the Town & Country Resort.

For further details, see page 7 and check out the conference website: www.theswcc.org.

Article

FBI: Hundreds of Thousands of Computers May Lose Internet on July 9

By Ira Wilsker
iwilsker@sbcglobal.net

In case you have not heard the news, on July 9, 2012, hundreds of thousands of computers will lose access to the Internet. This is not some hoax or urban legend, but a fact announced by the FBI. Following the arrest of an Estonian hacker group which had made millions of dollars from a fraud scheme that infected millions of computers worldwide with a "DNS Changer" malware that redirected legitimate commercial transactions to a series of scam websites. These cyber crooks created a sham company called "Rove Digital" to receive the revenues of the scam. DNS is an acronym for a Domain Name Server, which serves somewhat like an internet phone book, which converts web addresses, also known as domain names (such as www.theexaminer.com), into an IP (Internet Protocol) address (theexaminer.com is really 50.116.108.205). By changing the Domain Name Server accessed by an infected computer, it is like replacing an authentic phonebook with a purloined one that has the correct names, but intentionally different phone numbers. Dialing a correct phone number will intentionally connect you to someone who pretends to be the person whom you called, and that person is a crook; this is what the DNS Changer malware does to an infected computer. As many as

500,000 American computers may have been infected by this DNS Changer malware, as were an estimated 4 million other computers around the world. In addition to modifying the computer's DNS, the malware also made the infected computers vulnerable to a variety of other malware. The rogue servers were hosted in Estonia, New York, and Chicago.

This scam was very lucrative to the Estonian hackers who made an estimated $14 million in illicit fees. According to the FBI, this cyber-gang started infecting computers with the DNS Changer malware in 2007, successfully infiltrating millions of computers owned by individuals, businesses, schools and colleges, and government agencies, including NASA. The malware was able to penetrate many of the anti-virus products in use, and prevented the installed anti-virus and operating system software from updating, which would have likely enabled the anti-virus software to detect and kill the DNS Changer. Since the security software would not be updated, there would be no protection from the thousands of new viruses, worms, and Trojans that appear every day, which allowed those computers to become infected with countless additional malware programs and other threats. According to the FBI,

"They were organized and operating as a traditional business but profiting illegally as the result of the malware. There was a level of complexity here that we haven't seen before." Since DNS Changer redirected the unsuspecting victims to rogue internet servers, the crooks were able to manipulate the destination of the web connections. In one example of how this scam worked, the FBI said, "When users of infected computers clicked on the link for the official website of iTunes, for example, they were instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software. Not only did the cyber thieves make money from these schemes, they deprived legitimate website operators and advertisers of substantial revenue." The FBI announced the arrest of the "Rove Digital" Estonian hackers on November 9, 2011.

Since there are likely millions of computers still infected with the DNS Changer malware, the sudden shutdown of those rogue servers would have prevented the victims from accessing many of their favorite web sites. In order to allow the infected computers to continue to access the Internet, but actually reach their intended web sites, the FBI arranged for the

rogue servers to be temporarily replaced with legitimate servers, such that the victims' Internet access is not disrupted. It is these temporary replacement internet servers that will be shut down on July 9, meaning that anyone who still has a computer infected with DNS Changer as of that date may lose Internet access.

In order for users around the world to determine if their computers are infected with the DNS Changer malware, a consortium of academic, governmental, and private organizations created the DNS Changer Working Group (DCWG), which initially administered the servers that replaced the illicit Rove Digital servers. The DCWG consists of representatives from Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, and the University of Alabama at Birmingham. The website for the DCWG, www.dcwg.org, is hosted at the Georgia Institute of Technology, under a research grant provided by the Office of Naval Research. The DCWG provides a quick method for users to determine whether or not their computers are infected with the DNS Changer malware. According to the DCWG, there are still 350,000 computers infected by the DNS Changer malware that are using the clean servers maintained by the DCWG which replaced the Rove Digital servers.

In order to quickly and safely test

if a computer has been hijacked by the DNS Changer malware, the DCWG has created 11 international servers which will report back to the user if his computer is indeed hijacked by DNS Changer; in the U.S. the link for this test is www.dns-ok.us. The test can be run from any browser, and nothing is downloaded or installed on the computer during the test; it is simply a test to see if the computer is connecting to a correct IP address. The results are almost instantaneous, with a "DNS Changer Check Up" result displayed in an IP graphic; if it is

green, the user is possibly free of the DNS Changer malware, but the green graphic does not certainly prove that the computer is clean. When the green display appears, it also says, "Your computer appears to be looking up IP addresses correctly! Had your computer been infected with DNS changer malware you would have seen a red background. Please note, however, that if your ISP is redirecting DNS traffic for its customers you would have reached this site even though you are infected."

DNS Changer Check-Up

DNS Resolution = GREEN

Your computer appears to be looking up IP addresses correctly!

Had your computer been infected with DNS changer malware you would have seen a red background. Please note, however, that if your ISP is redirecting DNS traffic for its customers you would have reached this site even though you are infected. For additional information regarding the DNS changer malware, please visit the FBI's website at:
http://www.fbi.gov/news/stories/2011/november/malware_110911

If the display is red, then it is likely that the computer is one of the many that have been compromised by DNS Changer.

For the computer that is 'red,' it will be necessary to clean the DNS Changer malware and then reset your DNS. Most of the current anti-spyware products such as the free versions of SuperAntiSpyware (www.superantispyware.com) and the free version of MalwareBytes (malwarebytes.org/products/ malwarebytes_free) can detect and remove the DNS Changer malware, but it will still be necessary to reset your DNS in order for the Internet to properly function on your computer.

Almost all ISP's (Internet Service Providers) offer telephone support that will help the user reset the DNS to the ISP's preferred DNS server. Gizmo's TechSupportAlert has instructions and links on how to find the best DNS server for you (techsupportalert.com/ content/how-find-best-dns-server.htm), as well as detailed instructions on how to change or reset the DNS settings on your computer (techsupportalert.com/ content/how-change-dns-server.htm).

Google has a free DNS utility "Namebench" at code.google.com/p/namebench that can help the user find the fastest free DNS, with instructions on how to change your DNS at developers.google.com/speed/public-dns/docs/using. Another excellent DNS service, OpenDNS, has simple but detailed instructions on how to change your DNS at

use.opendns.com. If you use Google's Namebench to find the best combination of DNS for your computer and connection, you can use those DNS on your computer by following the instructions given on Google or OpenDNS on how to change your DNS settings; while the default DNS listed on the Google and OpenDNS instructions are excellent and totally adequate, there may be some performance improvement by using the DNS recommended by Namebench. You can always change them again later.

If you enjoy or depend on the Internet, it is imperative that you go to www.dcwg.org/detect and see if your browser is connecting to a legitimate DNS. If the results are 'green' you are likely (but not certainly) safe from the DNS Changer Trojan, and can probably continue to use the Internet after July 9. If you are 'red' you must clean your computer of the DNS Changer malware and reset your DNS as instructed above. Regardless of 'green' or 'red' results, it is always a good practice to periodically scan your computer with a good third-party utility such as SuperAntiSpyware or MalwareBytes to verify that nothing slipped by your security software. Failure to check your computer prior to July 9 may mean no internet for you on July 10.

Secondary screens are becoming commonplace. It is an option you probably should try.

BE BRAVE, GO FOR THE BIG SCREENS!

Tip

Skip A Bullet Or Number

There can be times when you're working with a bulleted or numbered list when you want to add a new line without tacking on a number or bullet. Perhaps you want to add a parenthetical note below an entry without making it part of your list.

If you hold 'Shift' and press 'Enter,' *Word* will add a new line to your list without a bullet a number. When you want to resume numbering or bulleting, don't hold the 'Shift' key any longer.

Back in the old 3.11 *Windows* days, a file like this was called a swap file. *Windows* used the hard disk space even then to simulate extra memory. A swap file helped when printing large documents, among other uses.

Not surprisingly, experts advise leaving **pagefile.sys** alone and to look elsewhere for files to delete!

about computer and telecommunication security. But for personal home use, I think you can be much less paranoid.

But remember -- If your computer is repaired or replaced, or if you use another computer, you will need to have your passwords!

Southwest Technology & Computer Conference
Enhance Your Life with Technology

Where:
***Town and Country Resort & Convention Center
500 Hotel Circle North
San Diego, CA 92108
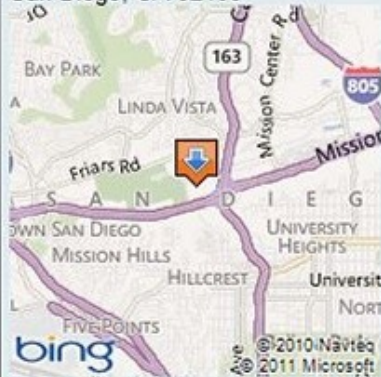
Driving Directions
Add to my calendar

Visit Our Website!

Thank you to everyone who has already registered for the conference; I've also received entries for the Digital Photo contest.

We're planning some new activities this year: bring your laptop for mini hands-on sessions and join Judy Clarke for early morning walks around the property on Saturday and Sunday.

We're pleased to announce a tour and presentation at the Apple store in the mall behind the Town and Country on Friday morning from 9-10am. If you have already registered for the conference, just send me an e-mail at judytaylour@theswcc.org and let me know you will be going on the tour.

This year, SW will be held in the Regency conference area on the eastside of the property; we have a block of rooms reserved in the Regency Tower.

Jerry Clarke is requesting that conference attendees send him one of their favorite recipes to share with others. He plans to put them on the Conference CD. We've all made good friends over the years and make new ones each year....this is a way to remember them throughout the year. jerryclarke@theswcc.org

Important Dates

Digital Photo Contest Deadline - 5/11/12
Early Bird Registration Ends - 5/21/12
Hotel Conference Rate Through - 5/26/12
Microsoft, Sony Store Tours - 6/21/12
Apple Store Tour - 6/22/12

We look forward to seeing you

Article

Undeliverable E-mail Messages

By Gini Pedersen
Seniors Computer Group, CA
www.scgsd.org
http://www.iteachyou.com

Reasons E-mail Messages You Send out May Be Returned as 'Undeliverable'

Reason #1
You mistyped the intended recipient's e-mail address. This also happens if you include a space in the address or fail to add the .com, .net, or other ending to the e-mail address.

Possible Solution -- Send the message again after correcting the e-mail address.

Reason #2
The intended recipient's ISP's (Internet Service Provider's) e-mail system may be offline (usually temporary).

Possible Solution -- Send the message again perhaps hours or days later.

Reason #3
The intended recipient's e-mail mailbox may be "full" or "over quota" (or similar wording).

Possible Solution -- Send the message again perhaps days later after the intended recipient's e-mail mailbox is no longer full.

Reason #4
The intended recipient's e-mail address is no longer valid.

Possible Solution -- Contact the intended recipient to get a new e-mail address.

Reason #5
The intended recipient's ISP's e-mail system (more common with Yahoo) deems that everything sent to multiple recipients at once MAY be spam. I notice this with my Net Happenings newsletter that I send out once a month. The only way around this is to individually (by e-mail) let the intended recipient know that they may need to check their Spam or Trash folder, click on a message from your e-mail address and click on a "Not Spam" (or similar) button or link on their screen. Exact wording varies with different ISP'S e-mail systems.

Possible Solution -- Send messages one at a time to each intended recipient -- painful unless you have an automated program for accomplishing this.

Reason #6
Some of the intended recipients use the 'white list' concept to control e-mail spam. This means that if the exact address of the sender (example: abc@xyz.com) isn't **already** in their contact list/address book, the message will be rejected. This message never even makes it into the intended recipient's e-mail Inbox.
Possible Solution -- Tell each rejected intended recipient to add your exact e-mail address to their Contact/Address list so it won't be rejected in the future.

Reason #7
Next, an outgoing or incoming e-mail server **may** have a limit on how many intended recipients may be included in the BCC field at one time. This happens to me if I try to send my newsletter out to too many e-mail addresses at the same time using either gmail.com or cox.net -- even though all recipients e-mail addresses are listed in the BCC field. That is why I now send them out through my school's e-mail server -- after I've asked permission to send so many at one time.

Possible Solution -- Call your ISP or check the 'Help' file in your e-mail to find out why these messages are being rejected.

Reason #8
And, finally, if the intended recipient has (even accidentally) in the past tagged a message from you as Spam, it will thereafter automatically go into their Spam folder.

Possible Solution -- Personally contact the rejected intended recipient's explaining that they may have to 'untag' messages from your e-mail address as 'Spam.' Again this was often done accidentally sometime in the past.

Article

Computer Password Tips and Strategies

By Jim Cerny
Sarasota PCUG, Florida
www.spcug.org
jimcerny123@gmail.com

Most of us have several computer or Internet "accounts" which provide us with many free services such as e-mail, movies (Netflix), video communications (Skype), photo printing (at Wal-Mart, Walgreens, etc.), music (I-Tunes), banking, shopping, games, entertainment, books, and many more. In fact, your computer is the perfect window to the world and all the people and services in it! But each account you set up requires some sort of "ID" and a password. For example, your email account is your email address and it requires a password to access your email. Many other accounts will use your email address as your ID (so they can email you notices and ads) but will require another password. How do you handle all your accounts and passwords? Here are some helpful tips:

1. **Always Write down Every Account and Password You Have.**
I cannot emphasize this enough. Review this list every few months and make sure it is current. **Keep it with you when you travel**. Keeping them on a small portable "jump" drive is a good idea too. You may have set up your computer at home to easily access your e-mail, perhaps telling the computer to "remember me" or your password for you, but when

you travel or use another computer you will need your passwords! Personally, I do not ever allow my computer to "remember" any of my passwords – I enter the password from the keyboard each time I "log in" any account. That way, no matter what computer I am using, the way I access my account stays the same – I always enter my account and password.

2. **Write down the Internet address of the web page where you enter your account and password.**
Many people use a "favorite" or an icon on the desktop to quickly get to the "log in" screen for their account. This is ok, but if you use another computer you will not have your shortcuts! So write down the web page address needed for each account.

3. **The longer and more complex a password is, the safer it is.**
In fact, many services now require a password of 8 or more characters with some digits or other "non-letter" characters. Some accounts may require you to periodically change your password. But, hey, we are not spies guarding government secrets. Keep your passwords simple. Use unusual combinations which are easy for you but would be diffi-

cult for someone else to guess. Children's names, birth dates, and home address numbers are too easy for someone to guess since such information can be obtained without too much effort. Instead, try the make and model of your first car, a childhood favorite game or toy, the name of your super hero, the nickname you gave to your worst in-law, etc. Get the idea? Easy for you but hard for someone else to guess, and impossible to find out without knowing you personally.

4. **Yes, you can use the same password for multiple accounts.** Now if someone really wanted to use your Skype account or read your e-mail and they had a hint to one of your passwords, it would be much easier for them to guess your other passwords. So your security is reduced. But, honestly now, who would really want to steal your passwords anyway? Who would care? Well, ok, maybe for banking or credit card accounts I would be more careful, but for most other accounts I do not feel the need for a super secure password, so I do use the same password or a variation of it for several accounts.

In business, things are different. Most companies are very careful

Article

Pass It On

By Elizabeth B. Wright
Computer Club of Oklahoma City
www.ccokc.org
wright599new@sbcglobal.net

In my beginning days of computing - 1982, Ms. E. Arly Bird was my mentor. (Not her real name of course.) She was a mathematical prodigy who became a computer expert in the very early days of personal computers. We were friends from another association and when she heard our daughter needed help doing some freelance PR work using a computer, she stepped in to get her up to speed.

Ms. Bird's mastery of the new machines was awesome. She later became a computer professional with clients in industry and offices in many locations. She and I both were members of the original IBM OKC PCUG, but she soon outgrew what the club had to offer. As my abilities leveled off, the club remained my source of new information, but whenever I needed immediate help she was always willing. Everyone should have such a friend.

Mentorship is the "new" catch phrase, approaching networking in importance. Since mentors can help people of all ages, they are becoming highly esteemed. Think about what you have to offer a young person, or even an older friend who really needs encouragement. While the young people know enough about computers to do about anything they want, they don't really know about life yet. They need to be encouraged to

make that knowledge count for something other than texting their friends or looking at a social network site. If you have the chance to become a mentor, regard it as a golden opportunity to hopefully make the world a better place.

In the past, parents sometimes punished their children (mostly boys??) for taking their toys apart. Then the world realized that the same curiosity which prompted such behavior resulted in adults who were much sought after for their engineering skills. Especially the ones who not only took their toys apart, but put them back together again. Since girls were usually given dolls for toys, there certainly wasn't much incentive to see how they worked (except for Betsy-Wetsy® of course). The world has made some progress in that area. Ms. E. Arly Bird must have had great parents. I know she had an outstanding mentor.

Mentoring can start at home. The recent computer breakdown at our office resulted in a temporary fix. My husband is closing the office gradually, so investment in new hardware was hardly feasible. We had a monitor, so we decided to hook it up to a laptop computer. The result is slightly less than satisfactory, but as he seems to be getting the "hang" of flipping his word processing program from the small laptop screen to the lar-

ger monitor, we will probably stay with this configuration until he closes the office for good. I think he has done pretty well for being a non-computer-literate 81 year old man.

For the type of setup mentioned above, the primary computer must be configured to accept the satellite monitor. We used a laptop computer, but a desktop machine can be used instead. For major business computing a desktop would be preferable. If you are planning to try this type of configuration, by all means call for help. Yes, you can get information online, but it will go faster if you have an expert set it up for you. As for "flipping"- also referred to as dragging - the physical movement of the cursor or program from screen to screen is not easy for some people.

Whether you use a regular desktop mouse, rollerball type or a touch pad, the use of a mouse has historically been difficult for adults, especially older people. The cursor changes screens just by moving the mouse, but other data requires holding down the left mouse button while moving the item. If you are left handed, you might have switched the mouse buttons, so if you decide to try this added convenience, be aware which button to keep depressed while moving the mouse.

SIG MEETINGS

Bob Hudak   rsh532@aol.com
Call for Appointment   310-323-0579

Digital Imaging   First Three Tuesdays
9—12 noon   Torrance Airport
Greg Neumann   Gbugcaller@aol.com

Beginning *Windows XP/7*   3rd Thursday
7:00 p.m.   Garry Sexton's
Virginia Pfiffner   310-374-2410
                                      vpfiffne@elcamino.edu

Internet   4th Thursday
7:00 p.m.   Garry Sexton's
Tom Tucknott   310-530-4992
                                      ttucknott@socal.rr.com

SIG Meeting Addresses

Torrance Scout Center
2375 Plaza Del Amo, Torrance

                            Garry Sexton's
                    3623 W. 227th St., Torrance
Torrance Airport
3301 Airport Drive, Torrance.

Tips from *Smart Comoputing*

No RAID For You

If your computer won't boot after you add or remove a non-bootable hard drive, you might need to get your priorities straight. Some motherboards will change their boot drive priority list every time a hard drive has been added or removed from the system since the last bootup. A motherboard with a bootable RAID and a few single drives might automatically drop the RAID to the bottom of the boot priority list if there is one of the other drives has just been added or disconnected. Enter the BIOS Setup, restore the boot drive or RAID to the top of the priority list, save your changes, and exit.

Get A Better Screen Shot

Taking a screen shot with your *Windows* PC has always been easy: simply press the 'Print Screen' key, open Paint (which comes with *Windows*), right-click on the white canvas, and click 'Paste.' Once the image appears, you can use the 'Crop' feature to cut out the parts of the image that you don't want. With *Windows 7*, this process is even quicker, thanks to the 'Snipping Tool.' To start it, click 'Start' and then enter 'Snip' in the search field. When 'Snipping Tool' appears, click it. When your screen gets cloudy, use the cursor to select the part of the screen you'd like to grab.

Alternative Copy

When you want to copy a file or folder, you don't necessarily have to use the left mouse button. You can click and drag the file using the right mouse button, too. When you release the button you'll see a small context menu prompting you to perform an action. You can 'Copy Here,' 'Move Here,' or 'Create Shortcut Here.'

May 2012

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1 **SIG Meeting** Digital Imaging	2	3	4	5
6	7 **General Meeting**	8 **SIG Meetings** Digital Imaging	9 **Board Meeting**	10	11	12
13	14	15 **SIG Meeting** Digital Imaging	16	17 **SIG Meeting** *Windows XP / 7*	18	19 Newsletter Deadline
20	21	22	23	24 **SIG Meeting** Internet	25	26
27	28	29	30	31		