



Nybbles & Bytes



www.neopc.org

Voice: 216-521-2907

May, 2009 Volume 25 Issue 8

A day in June

A day in December

A day in July

A day in September

Never, ever forget

Always Remember

Memorial Day

Letter from the Editor -
David A. Vydra



Good news! After much discussion by the powers that be (10 – 15 seconds), it has been decided to discontinue the last page of the Nybbles and Bytes Newsletter. Thus, commencing with this current issue, we will no longer have a last page.

The format of the last page was primarily to facilitate postal mailing back in the days when this was done. And horse feed was aplenty. Now, as we no longer mail the newsletter, the last page is just wasting paper. It will be easier, for those who prefer to print it out at home, to not have to be concerned with a printer setting to eliminate printing this unneeded page.

Through the Gates:



Enter to the Trove of Bills Treasures and Travails

A monthly column dedicated to revealing some of the unknown or lesser known features or foibles of the Microsoft line of products.

By: David A. Vydra

Lots and lots of interesting stuff this month! It will be like a marriage. Some things from the old column and a few things from the new column. Perhaps even a bit borrowed.

Some Word Tricks:

Selecting text is a common task in Word[®]. Holding down the Shift key while maneuvering the cursor to cover the text you want with the arrow keys is a long used method. You can also use the mouse to highlight text by dragging the cursor over it, but that can be tedious and a bit cumbersome — and fortunately, unnecessary. Here are a few easy selection techniques for mouse lovers:

To select a word, double-click it.

To select a single line of text, click in the left margin next to the line.

To select a sentence, hold down [Ctrl] and then click anywhere in the sentence.

To select a paragraph, click three times in the paragraph. Alternatively, click twice in the left margin next to the paragraph.

To select the entire document, click three times in the left margin.

By golly! It really is that easy. The hard part is remembering which function calls which action. These should work with all versions of Word[®]. If not, I hope someone will let me know. You have done your selection, then what?

Word's[®] Smart Cut and Paste

You have copied a selected block of text to somewhere else and been disappointed with the results? Perhaps you lost leading or trailing spaces or paragraph spacing. If so, you're a victim of Word's[®] Smart Cut and Paste feature. This feature enables Word to automatically adjust formatting when you paste text. The problem is, you might not want Word[®] to adjust a thing.

This feature is enabled by default, and it works well for most people, most of the time. However, if you're very specific with your editing, you might find this feature annoying. This will sometimes happen as I do a newsletter article using data from another source. If that's the case, simply turn it off – or better yet, customize it. To disable this feature, do the following:

Choose Options from the Tools menu.

Click the Edit tab.

Uncheck "Smart Cut And Paste" in the Cut And Paste section.

Be careful though by disabling this feature, you'll lose its good points as well as its bad.

That is why customizing it might be more efficient. Instead of un-checking the Smart Cut And Paste option in step 3, click the “Settings” button to display the options you can control. Then, uncheck the behaviors you want to lose and check those you want to keep. For instance, if you don’t want to lose leading or trailing spaces, just uncheck the Adjust Sentence And Word Spacing Automatically option. As always, you should make a note of the default settings prior to making any changes.

The “Options” available in Word[®] under the “Tools” menu are quite extensive. Many of us just accept the “Default” settings and go with it. However, why not explore your options? Spend some time making yourself familiar with what is there. Experiment with changes after noting which settings are currently in force. At the least, you will have a better understanding of where some settings are and how to adjust them should it be necessary.

Windows7[®]

The RC (Release Candidate) of Windows7[®] was released to certain Microsoft subscribers at the end of April. A release to the general public is expected on or about May 5. I would not be surprised to have this delayed because of overwhelming response similar to what occurred with the release of the first Beta. Each passing week there seem to be more revelations of “What is new and good” with this latest version. You will no doubt hear and read much from the skeptics and naysayers. Microsoft bashers are in it for the long haul and they tend to be quite vocal. With that in mind, I will attempt to “go over lightly” some of what I have unearthed.

The “Upgrade” path has not changed. Nor, is it likely to do so, even with the XP[®] lobby clamoring for some relief. As has happened with previous releases of the latest and greatest, an upgrade path is available from the current version to the new release version. Consider these more like a “Migration” to the new version wherein the new replaces the old and retains all of the settings of the old. And, in addition, the unclean processes and habits of the “Registry” are migrated to the greatest extent possible. There will be “Upgrade” versions of Windows 7[®] sold just as there has been for all previous versions of Windows[®]. The upgrade license requires proof of a previous version before it will install. Whereas, all previous upgrade versions of Windows[®] would install after examining the media for an older version or performing a migration, this is no longer the case since the advent of Vista[®]. From my testing, of the “Beta” we found that it was necessary to have Vista and not XP[®] installed in order to do a “Migration Upgrade” to Windows7[®]. You may expect this to be a “for sure” with the other versions as well. Even a clean install will require Vista[®] to be actively installed if you are using the “Upgrade” and not the full version. (Stay tuned!)

There will be changes and enhancements to how things are done and which defaults are retained. One recent change is the ability of the RC to support the ability to drag and drop folders into Windows7[®] Libraries, which you previously could do to create a new library. Since libraries are virtual folders, Microsoft said that it feared users might delete the original folder, supposing that it now existed in the library. Microsoft also appended a clarification about the Windows Easy Transfer feature for synchronizing data between PCs, saying that it would work only on PCs running Windows7[®], or the Windows7[®] version of Windows Easy Transfer (which has to be installed manually on Vista[®] and XP[®] PCs). A Windows7[®] PC will now be able to stream media from your home to any Internet-connected Windows7[®] PC through an upgraded Windows media player and login with your Live ID[®]. The Windows Live ID[®] is the latest incarnation of the Hotmail[®] or Passport ID[®]. Hope you still have yours.

Microsoft is building a small but important change into Windows7[®] to help slow the spread of malware. According to Microsoft, the company is changing the way the AutoPlay feature operates to prevent it from enabling the AutoRun task for USB devices. The move, Microsoft officials said, was done in response to malware-most notably Conficker-taking advantage of the functionality to spread.

"The reason we're making this change is that we've seen an increase, since the start of 2009, in malicious software abusing the current default AutoRun settings to propagate through removable media like USB devices." "The best-known malicious software abusing AutoRun is Conficker, but it's not alone in that regard: There is other malicious software that abuses this feature." The growth of malware spreading via USB devices was well-publicized in 2008. In fact, a report by Symantec found that self-copying to removable media was among the most common means of malware propagation in the second half of 2007. "Because we've seen such a marked increase in malicious software abusing AutoRun to propagate, we've decided that it makes sense to adjust the balance between security and usability around removable media". "We've tried to be very measured in this adjustment to maximize both customer convenience and protection." With this change, Windows will no longer display the AutoRun task in the AutoPlay dialog except for removable optical media such as CDs and DVDs. ***NOTE: The modification is slated for the Release Candidate build of Windows7[®], but officials at Microsoft said they plan to also release an update in the future to fix the issue in Windows Vista[®] and Windows XP[®] as well.*** The change is one of a number of security enhancements to Windows7[®] Microsoft has already announced, including the Windows Biometric Framework and improvements to the BitLocker full-encryption solution first introduced in Vista. There are also improvements slated for UAC (User Account Control) to reduce user prompts. As you might imagine, this has been applauded on many fronts.

Coming Soon: Windows XP[®] Mode and Windows Virtual PC[®]

Last week, Microsoft announced that it would offer an add-on called "Windows XP Mode" (XPM) to users of Windows7[®] *Professional, Ultimate and Enterprise* when the new operating system ships. Professional and Ultimate are the two highest-priced versions of Windows7[®], while Enterprise is sold only through volume licensing agreements. Microsoft was clear about XPM's purpose. "WindowsXP Mode is specifically designed to help small businesses move to Windows7[®]," Scott Woodgate, the director of Windows enterprise and virtualization strategy, said in a blog entry last Friday. "I think that this will help the uptake for Windows7[®], because it removes one more 'gotcha, and that's never a bad thing to do," said Michael Cherry, an analyst with Directions on Microsoft. The idea of using virtualization to provide backward compatibility for older applications is neither novel nor surprising, Cherry continued. He called it a nice "safety net" for users concerned about abandoning XP[®] who don't have access to the centrally-managed MED-V (Microsoft Enterprise Desktop Virtualization). XPM is a smart, if necessary, move, given the reception users gave to Windows Vista[®], Cherry said. "Because of the way Vista[®] was received -- it's got enough baggage already -- the more they can do to address all those things [Vista[®] was criticized for] up front with Windows7[®], the more likely that people will go to the new OS," said Cherry.

If you are familiar with the use of a "Virtual PC" it is important to note that you require two OS's and their license. I did a demo last year using Vista[®] as the Host OS and then running Windows3.1[®], Windows95[®] and 9[®]8 as client systems. XPM is not "Virtual PC". Microsoft will include a fully licensed copy of Windows XP Service Pack 3 (SP3)[®] with the add-on. That, in effect, gives Windows7[®] users a way to run older applications without having to pay for another operating system license. This will create the ability to run Windows XP[®] applications directly from the Windows7 desktop without having to first open a separate virtual machine window as you would in a Virtual PC environment. The one sort of "fly in the ointment" is the fact that XP[®] has been "End of Life" for several weeks now and the only support from Microsoft will be extended.

Portions of this column may have been garnered from several publicly available sources, verified and edited for content. Where an article is used in its entirety without editing, the author and source are acknowledged.

Members Podium - All Members



Submitted by: David Vydra

I have been using a browser called “Maxthon” for many, many years. At the time I first discovered it in 2003 this browser it was called “MyIE2”. This became my initial introduction to “Tabbed Browsing. In addition, there were several neat features with regard to annoying ads. Popup ads were a thing of the past. In 2004 MyIE2 was renamed Maxthon Browser. Maxthon is a powerful tabbed browser built for all users. Besides basic browsing functionality, Maxthon Browser provides a rich set of features to improve your surfing experience. I have listed a few of the available features here. The coolest feature is: “It’s Free”! Check it out for yourself at www.maxthon.com.

To give you a small idea of what is available in Maxthon I have listed a few of the features that are most recommended by users;

Tabbed Browsing

All the web pages are arranged as tabs inside main window to ease your navigation.

You can find almost all common operations in the Right-click Menu of tabs.

Mouse Gestures

Hold right mouse button and perform the gestures to access common features such as Back, Forward, Refresh and Close Tab.

You can set up your own mouse gestures in Setup Center.

Maxthon Smart Acceleration

Boost the browsing speed of your frequent visit websites.

And the Super Acceleration Mode can improve your browse speed even more.

Ad Hunter

Ad Hunter can efficiently clean up the web pages by stopping Popup Windows and removing Ad Content Blocks.

You can add content block to the filter with the "Block Page Content..." command in the Right-click Menu.

Super Drag&Drop

Type the keywords in Address Bar then press Enter to perform a search. Or simply drag & drop a keyword with your mouse.

Click on images when holding the Ctrl key, the image you clicked will be saved to specified folder.

Screen Capture

Capture Full Screen, Selected Area, Selected Window and Page Content as an image.

You can set copy the image to Clipboard or save it as a file.

Sanitizing Your Hard Drive

User data is left on disk drives removed from computers and storage systems, creating a data security vulnerability that many users are unaware of. Recent Federal and state laws requiring secure erasure of user data expose companies to fines of \$250,000 and responsible parties to imprisonment for 10 years. Of course you are not a company, corporation or enterprise. However, if you have personal or business data on your computer, it is your responsibility to secure it. As you would protect data of your own, you are obligated to protect the data of others. Complete eradication of user data off drives can be accomplished by running data Secure Erasure utilities such as the free-ware "HDDerase". It executes the Federally-approved (NIST 800-88) Secure Erase command in the ATA ANSI standard, which is implemented in all recent ATA drives greater than 15-20 GB. Normal Secure Erase takes 30-60 minutes to complete. Some ATA drives also implement the standard Enhanced Secure Erase command that takes only milliseconds to complete. Data security has risen to be one of the highest concerns of computer professionals. Tighter legal requirements now exist for protecting user data from unauthorized use, and for both preserving and erasing (sanitizing) records to meet legal compliance requirements. The cardinal rule of computer storage design has been to protect user data at all costs. Disk drives supply primary mass storage for computer systems, designed to prevent accidental erasure of data. Techniques such as "recycle" folders and "Unerase" commands are common ways that operating systems try to prevent accidental sanitization of user data. Deletion of file pointers is standard to speed data writing, because actual overwriting of file data is far slower. Drives use elaborate error detection and correction techniques to make sure that they don't return incorrect user data. All this, means that true computer data erasure is an abnormal event. These measures taken to protect and speed access to user data can make that data vulnerable to recovery by unauthorized persons. When a computer is lost or disposed of, active and discarded data typically remains stored on its hard disk drive. Even if users "delete" all their files, they can be recovered from "recycling" folders or by special utility programs such as Norton Unerase.

If data is not erased beyond recovery, data on disk drives that leave the physical control of owners can and often does fall into the hands of others. Data can be recovered with little effort, from discarded, warranty repaired, or resold disk drives. Many reports have been written on data recovered from discarded disk drives. Each year hundreds of thousands of hard disk drives are retired. Some of these hard disk drives find their way back into the market and their data can be recovered unless it is erased securely. There is an urgent need for a capability to reliably erase data and prevent access to data from retired computer hard disk drives for security and privacy reasons. Data sanitization needs arise differently depending upon the user application. Even consumer drives could use data sanitization to protect user privacy or for DRM purposes.

Data Sanitization in Hard Disk Drives

Four basic sanitization security levels can be defined: weak erase (deleting files), block erase (overwrite by external software), normal secure erase (current drives), and enhanced secure erase (see below). The CMRR at UCSD has established test protocols for software secure erase. Block erase is most commonly used. While it significantly better than no erase, or file deletion, or drive formatting, it is vulnerable to malware and incomplete erasure of all data blocks. Examples are data blocks reassigned by drives, multiple drive partitions, host protected areas, device configuration overlays, and drive faults. Normal secure erase is approved by NIST 800-88 for legal sanitization of user data up to Confidential, and enhanced secure erase for higher levels. Enhanced level has only recently been implemented, initially in Seagate drives, and these drives are under evaluation by the CMRR.

These four erasure protocols exist because users make tradeoffs between sanitization security level and the time required. A high security protocol that requires special software and days to accomplish will be avoided by most users, making it little used and of limited practical value. For example, the old data overwrite document DoD 5220 calls for multiple block overwrites of Confidential data, which can take more than a day to complete in today's large capacity drives. So users make tradeoffs between the time required to erase data and the risk that the next drive user may know and use recovery techniques which can access weakly erased data.

To positively prevent data from recovery, disks can be removed from disk drives and broken up, or even ground to microscopic pieces. (Actually, simple disk bending is highly effective, particularly in emergency situations.) Obsolete government document DoD 5220.22M required physical destruction of the storage medium (the magnetic disks) for data classified higher than Secret. Even such physical destruction is not absolute if any remaining disk pieces are larger than a single 512-byte record block in size, about 1/125" in today's drives. As linear and track densities increases, the maximum allowable size of disk fragments become ever smaller. Destroyed disk fragments of this size have been studied by the CMRR. Magnetic microscopy is used to image stored recorded media bits. Some storage products are more easily destroyed than hard disk drives, such as magnetic disk data cartridges, tape cartridges, secure USB drives, and optical media.

Sanitizing Your Hard Drive Cont.

So what's the magic?

Something called Secure Erase, a set of commands embedded in most ATA drives built since 2001. If this is so wonderful, why haven't you heard of it before? Because it's been disabled by most motherboard Bios'. Secure Erase is a loaded gun aimed right at all your data. And Murphy's Law is still in force. But hey, if you're smart enough to format a drive, you're smart enough to not play with Secure Erase until you need to.

How does Secure Erase work?

Secure Erase overwrites every single track on the hard drive. That includes the data on "bad blocks", the data left at the end of partly overwritten blocks, directories, everything. There is no data recovery from Secure Erase.

Says who?

The National Security Agency, for one. And the National Institute for Standards and Testing (NIST), who give it a higher security rating than external block overwrite software that you'd have to buy.

Update: There is an open source external block overwrite utility called Boot and Nuke that is free. If you have this, use it. However, HDerase is rated more secure as well as quicker.

Secure Erase is approved for complying with the legal requirements noted above.

UCSD's CMRR to the rescue

The University of California at San Diego hosts the Center for Magnetic Recording Research. Dr. Gordon Hughes of CMRR helped develop the Secure Erase standard.

Download this Freeware Secure Erase Utility, read the ReadMe file and you're good to go. <http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>

What is Secure Erase?

HDerase.exe accesses an ATA disk drive's internal Secure Erase commands to wipe a disk clean. Merely deleting a file doesn't delete your data: the data is still on the disk and can be recovered by anyone with a few readily available tools. Credit card numbers, passwords, emails, medical info, anything on your hard disk is liable to be recovered. Secure Erase is built into all ATA-compliant disks drives since 2001. This functionality is recognized by the US Government's National Institute of Standards and Technologies (NIST) as equivalent to magnetically wiping a drive (degaussing) or physically destroying it. NIST also rates the secure erase commands as more secure than external host-based drive wiping utilities such as Boot and Nuke. Secure Erase complies with HIPAA, Personal Information Protection and Electronic Documents Act (PIPEDA), the Gramm-Leach-Bliley Act (GLBA), and California Senate Bill 1386 for data destruction.

There is no data recovery after running HDerase.exe!

Don't mess with it if you don't know what to do with a blank drive.



 Coming Events
May 2009

Event Date	Event
05/12	*** Computer Fundamentals Open Forum *** MORNING session. Northeast Ohio PC Club (NEOPC) - 9:30am Fairview Park Senior Center -Fundamentals of computer use - Any and all topics discussed - Bring a question, bring a topic - Guests always welcome - Always coffee - Free and open to the public. Second Tuesday of the month.
05/13	Northeast Ohio PC Club (NEOPC)-General Meeting- Porter Public Library, 27333 Center Ridge Road, Westlake, OH. 6:30pm Social (pastries and beverages); 7:00pm Club announcements; 7:15pm main program for the evening will be "Investments" by Ian Abbott. Ian's talk covers the Mood of the Market and Indicators to forecast the Market; 8:30 pm Raffle and Door Prizes.
05/20	May 20, 2009 PLEASE NOTE: THE MEETING DATES FOR THIS GROUP HAVE BEEN CHANGED FROM THURSDAY TO WEDNESDAY. Ladies Only Special Interest Group at Westlake Porter Public Library from 2:00 p.m. to 3:30 p.m. The Library is located at 27333 Center Ridge Road, Westlake, Ohio. All ladies are invited, whether or not members of NEOPC. Come with your questions and/or comments about software you have.
05/25	Final day to submit your article for inclusion in the next "Members Podium" column for the June 2009 issue of Nybbles & Bytes. We had no entries for the month of May. Be sure to send your article to info@neopc.net and include the phrase "Members Podium" in the Subject line.
05/26	Northeast Ohio PC Club ***Fundamentals Special Interest Group*** (SIG). Fairview Park Library (lower level) 7:00 - 8:30pm. Fundamentals of computer use - Any and all topics discussed - Bring a question, bring a topic - Guests always welcome - Free and open to the public. Fourth Tuesday of the month.