The PULP

HUGE this month:

General Meeting: Dec. 20th

Gifts for Geeks

See you there!

East Hartford Public Library
Main St. & Central Ave., E. Hartford, CT.

Q&A Session: 7:00PM–7:30PM
Meeting starts at: 7:30PM

Contents:

Member of
Association of Personal Computer User Groups
APCUG

UGC

Apple User Group

H.U.G.E.

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATIONS
East Hartford Public Library
Main & Central Avenue
in the Lion's Room
(downstairs)

Editor's Corner

The annual December meeting for holiday gift suggestions is now upon us.

As you may have noticed, hard drive prices have started to rise due to the flooding in Thailand. Prices have already started upward, the price of some drives has tripled since Oct. 2011. The reason, Western Digital, which makes about 30% of all hard drives, has 60% of its capacity under water. Toshiba with 10% of the market has lost 50%. The estimates are that 25% of the worlds hard drive manufacturing is under water and will be for awhile, some estimates are as long as a year.

In the news, there is a bug (which maybe patched by the time you get this) in OSX 10.7 (Lion) which could let a hacker view, change local user passwords.

For those who are really paranoid (are you paranoid if they really are after you?), a service called FootPath Technology has teamed with several shopping malls to deploy a method of tracking shopper movement using cellphones. Using receivers attached to walls the devices then track anyone in the vicinity with a switched-on cell phone. The person-specific tracking allows the system to determine which stores get the most traffic, and which areas within the stores attract the largest crowds. No idea how much personal info is collected. There appears to be no practical method to opt-out except switching off your phone, which sort of defeats the reason for having a cell phone.

According to an AP report, the CIA monitors up to 5 million tweets daily.

Is there an Apple TV set in your future?

Stuart Rabinowitz, Editor

A Little Computer Quiz

by Stuart Rabinowitz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

1 One of the current computing buzzwords is 'Cloud Computing', but where & when did the concept of shared resources originate?

2 I'm sure that many of you have used 'Google Street View', but was the first use of that type of virtual reality/mapping technology?

3 Recently, Google disclosed its fleet of self-driving (without human intervention) cars (http://www.pcmag.com/article2/0,2817,2395049,00.asp), but it was not the first to develop one. Who was first?

4 The 'Tor' network provides a method to ensure privacy & security on the internet. What does 'Tor' stand for?

5 What do all these questions have in common?

Answers to Nov., 2011 Quiz

1 Comdex had its first show in 1979, can you name who created it?
A Shelley Adelson
2 Where was it held?
A Las Vegas
3 IBM is in the process of celebrating the 100th anniversary of its creation, but that was not its original name. What was the original name of "international Business Machines"?
A Computing Tabulating and Recording Company. It did not become IBM until 1924
4 What was IBM's first product?
A Meat grinders, Cheese slicers, & Clocks. The punch card came a little later.
5 Donkey Kong turns 30 this year, what was the name of the little guy in the game that did all the jumping and tried to rescue the princess?
A No it was not Mario (he got that name in the sequel), he was officially called 'Jumpman'

ABC's of Digital Photography
Review of a meeting presented by Gary Stanley at the Quad Cities Computer Society, IA
www.gary.stanley.net
www.qcs.org
joseph85_us (at) yahoo.com

Gary Stanley returned to the QCS to share his lifelong interest in Photography and the tips to help make our photography more useful, and endearing. Photos tell a story. He was here to help us tell ours. His first digital camera was a 1/3 megapixel one that used a 3.5 disk for storage. Today he uses a wide range of digital cameras on his travels around the world.

He has wonderfully condensed some photographic principles that we all can use. First off he related that sales people will emphasize megapixels. Some of today's point and shoot cameras have 14 megapixels. A 5 megapixel camera is all you need. The large capacity megapixels cameras are needed only for large size blowups of your photos. Most of us will never need this resolution. We usually will print 8 x 10 prints at the most and 5 megapixels will sustain that quality. In fact, the Flixr photo web storage site highlights that the most used camera for its site is the iPhone4 which has a 5 megapixel lens.

Point and shoot digital cameras have automatic settings by default. Gary explained that these settings will give you OK pictures. But for a better outcome, it is preferable to select the program mode so that you can fine tune the camera to fit your photographic perspective.

One of the essential features of creating a good photo is to understand and manage the white balance in it. Note the lighting conditions before you take your shot. Is it outdoors in the sun or indoors under incandescent or florescent light. Select the appropriate setting. If you take an outdoor shot with an incandescent setting the picture will turn out blue. If you pick the florescent setting in an outdoor shot the picture will have a purple cast. Make sure that your camera is set properly.

He suggested that you take your photos at a 90 degree angle to the sun; this will add depth to your subject. Also view your subject through the lens. Will it look better in a vertical or horizontal mode? Conform to your subject and it will improve the quality of your shot. For example: get down on the same level of kids and animals. Enter their world and your pictures will come to life.

One of the more interesting settings is the camera timer which is usually prefigured at 2 seconds and 10 seconds. The 2 second mode allows for a perfect shot with a tripod. Press the shutter button down half way to allow the camera to calculate all of the configurations. Now you can lift your finger from the trigger and walk away from the camera as the still camera takes the shot a second later. The 10 second mode allows one to take the picture and also be a part of it.

On the photo walk in LeClaire, he reminded the participants to always check their settings before they began their work. Also take many pictures, unlike the old days they are free. Professional photographers usually get a good photo with a 200 to 1 ratio. Let creativity be your guide.

When we are finished with our photo set we need to transfer them, edit them and store them. Gary recommended that we transfer our photos by removing the memory card from the camera and placing it in a card reader or your computer. This saves the battery life of your digital camera. Using a USB inadvertently with a low battery can risk losing your photos entirely.

When you transfer them it is important to select them all on the memory card with a

Control-A, then right click on a photo, select COPY from the menu. Next, on your computer create a folder for your images, right click in that folder and select PASTE from the drop down menu. This method places your photos in three places until the process is finished: on the memory card, the computer memory clipboard and the hard drive. Always a good fail safe method.

There are many free photo editing software packages on the Internet, however Gary recommended Windows Live Photo Gallery from Microsoft. Paid image editing software offers more advanced options. Good choices in this category are : Photoshop Elements, and Paint Shop Pro Photo X3.

Gary emphasized that we need to back up our precious photographic moments to an external hard drive. He mentioned they are very reasonably priced, as low as $49. There are several brands: Seagate, Western Digital, and Maxtor. He has a Western Digital MyBook external drive that has a feature that he likes. It backs up your data as soon as it is created on your computer. For him photographic backups are essential as he has over 70,000 photos that he has taken over the years and doesn't want to lose them. Likewise, we wouldn't want to lose those memories either.

Gary offered a delightful presentation filled with humor, insight and detail. An enjoyable evening and learning experience all in one. Be sure to visit his Blog:
gary-stanley.blogspot.com as it will have many of the presentation details on the internet from this meeting. Also visit his fine photo gallery online, a wonderful collection:
www.pbase.com/gary_stanley

He ended the night with a "special" Internet photographic slide show which featured creative pictures of Paula Sands holding one of his landscape pictures in a photo gallery as well as a Time magazine cover featuring himself. These were created with three clicks on the Internet. Go to **www.writeonit.org** or **www.loonapix.com.** On these fake picture sites, you create the picture display, browse your computer to select your own image, then right click the finished product to save it to your computer.

He said:
"Birth Certificates show you were born."
Death Certificates show you died."
Photos show that you lived."

Tech Tip: How to Recover Data from a Dead Hard Drive

By Bryan Lambert, Geeks.com
www.geeks.com

One of the most dreadful feelings that you can have is having a pc computer or laptop die that hasn't been backed up recently; especially if you have valuable pictures, music, videos, documents or other files on it.

One of the most dreadful feelings that you can have is having a pc computer or laptop die that hadn't been backed up recently; especially if you have valuable pictures, music, videos, documents or other files on it.

In this Tech Tip we'll take a look at how to recover your valuable pictures from a dead computer.

Where to start

Computers are complex machines and when they work right, they are fun to use – but when something goes drastically wrong, it can feel as if your world crashed down around you. If your hard drive is still in working order, there is a very good chance that you'll be able to recover your pictures, music, videos and valuable documents (and other data) simply with another computer; a specialized cable, a screwdriver; and a little time.

To start off, your best bet it to get a specialized USB cable that can plug directly into your hard drive that you'll recover from the dead computer. There are several types, and I'd recommend getting one that can handle both PATA (IDE) and SATA hard drives (the two most common used in consumer computers) as well as 2.5" (laptop) and 3.5" (desktop) hard drives (Geeks.com sells several that run in the $13-16 range). You can also use a hard drive dock or external drive cases as well - but personally I find the specialized USB cable to be the easiest and most flexible option.

Next, remove the hard drive from the dead computer. On desktops it is usually held in with four Philips screwdrivers and on laptops it is usually under an access panel on the bottom of the computer. Remove any cables and caddies that the drive may have – all you need is the bare drive. Then plug in the USB cable into the hard drive (and a power cable if it is a desktop drive – also provided with the USB cable kit) and then plug the other end of the USB cable into a working computer. The computer will then set up the drive ad an external storage device and voilà! you'll now have access to the files on that drive (provided that the drive is not encrypted or using some type of security feature).

Where to look

OK, so the drive is now plugged into your computer and seen as an external drive, now what? You have several options. **One option is to simply look for the files on the drive from the dead computer that you plugged into the USB port and copy them onto the working computer. This is my preferred method personally**. I like to "brute force" my way through the drive with Windows Explorer (or a similar file browsing tool) and manually copy/paste the data from one computer to the other. Another option is to follow a Windows dialog box (that usually pops up when you plug in an external drive) and have it help you copy your data from one computer to the other. If you are manually choosing to "brute force it" personal data is usually stored by default in the computers operating systems "home directory" for users.

Common Locations

for home directories *(where <root> takes the place of the drive letter)*:

1. **Microsoft Windows 95-Me** *<root>\My Documents*
2. **Microsoft Windows 2000/XP/2003** *<root>\Documents and* Settings\<username>
3. **Microsoft Windows Vista / Windows 7** *<root>\Users\<username>*

cont. on pg. 9

TrueCrypt

Free open-source data encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

By John Langill, Newsletter Co-editor, Southern Tier Personal Computing Club, NY
August 2011 issue, Rare Bits, STPCC Newsletter
jlangil1 (at) stny.rr.com

The May 2011 issue of *Rare Bits* contained an article by Dick Maybach titled "Cloud Computing" in which he pointed out the necessity of securing your data via encryption when it "...is stored on the same disks, uses the same memory, and passes through the same processors as everybody else's." And I recall Dave Bilcik voicing a similar warning at the May meeting and also mentioning the program TrueCrypt. It just so happens that I am currently using TrueCrypt and I believe it to be very satisfactory solution whether you need relatively modest security or very tight and sophisticated protection.

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). "On-the-fly" encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. The entire file system is encrypted; e.g., filenames, folder-names, contents of every file, free space, meta-data, etc. No data stored on an encrypted volume can be read (decrypted) without using the correct password and/or key file(s), or correct encryption keys.

I'm not sure how unique TrueCrypt's approach is but I was nevertheless intrigued by it. The first step is to create a "container;" otherwise known as a TrueCrypt "encrypted volume." To my mind, this is somewhat like obtaining a safety-deposit box at a bank.

TrueCrypt provides a "wizard" to assist with the task. As at a bank where safety-deposit boxes of various sizes can be rented, the encrypted volume can be created to have as much capacity as you need. For example, it can be a specific portion of a hard-disk, or an entire flash drive or other storage device. Unlike a safety-deposit box, however, you hold the only key... so you need to remember and protect it. And, into the container (the volume) you can store any number of files. If the capacity of the volume is exceeded, you simply create a bigger container.

One of the interesting facets of a TrueCrypt volume is that it has most of the characteristics of an ordinary file. That is, the volume can be moved or copied within the storage areas of a given PC, or to a different PC. The name of the volume can be changed; and the volume can be included in routine backups. It can be transmitted across the Internet; and even into the wild-blue yonder, if you're so inclined. And, even if you have no intention of salting "the cloud" with your personal data, what about that minuscule 8- or 32GB flash-drive you carry around in your pocket. The smaller they get, the easier they are to lose. Wouldn't it be reassuring to have made it an encrypted volume so that whoever finds it won't have an easy time of it when they try to discover the contents of your personal data?

The downside of the file-like characteristics is that, like any file, an encrypted volume can also be deleted and all its content lost (...thank goodness for the Recycle Bin). That would be very bad if done unwittingly. But that's why we do back-ups! Yes? Once a TrueCrypt volume is mounted, the data files it contains can be copied to and from the volume just like they are copied to or from any normal disk; for example, by simple drag-and-drop operations.

Files are automatically decrypted on-the-fly in RAM (Random Access Memory) while they are being read or copied from an encrypted TrueCrypt volume. Similarly, files that are being written or copied to a TrueCrypt volume are automatically encrypted on-the-fly in RAM right before they are written to the volume. Note, however, this does not mean the whole file that is to be encrypted/decrypted must reside in RAM before it can be encrypted/decrypted. That is, there are no extra RAM requirements for TrueCrypt. The following paragraph explains how this is accomplished.

Let's suppose that there is an .avi video file stored on a TrueCrypt volume; that is, the entire video file is encrypted. The user provides the correct password and/or key file and mounts (opens) the TrueCrypt volume. When the user double-clicks the icon of the video file, the operating system launches the application associated with the file type ? typically a media player. The media player then begins loading a small initial portion of the video file from the TrueCrypt-encrypted volume to RAM in order to play it. While the portion is being loaded, TrueCrypt is automatically decrypting it in RAM. The decrypted portion of the video in RAM is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the TrueCrypt-encrypted volume to RAM and the process repeats. This process is called "on-the-fly" encryption/decryption and it works for all file types, not just for video files. The process also ensures minimal impact on processing performance.

Note that TrueCrypt never saves any decrypted data to a disk – it only stores it temporarily in RAM. Even when the volume is mounted, data stored in the volume remains encrypted. When you restart Windows or turn off your computer, the volume will be automatically dismounted and files stored in it will be inaccessible and encrypted. Even when power is suddenly interrupted (i.e., without a proper system shut-down), files stored in the volume are inaccessible and encrypted. To make them accessible again, you have to mount the volume by providing the correct password and/or key file.

Of course, as with any unintended power interruption or shut-down, unsaved changes to files are lost because re-encryption of changes occurs only when files are saved to the volume in a normal fashion.

I've only touched on a few of the main facets of TrueCrypt. In addition, TrueCrypt offers a choice of encryption algorithms from which you can select one that will give the degree of security you feel you need. This and other aspects of TrueCrypt are fully documented in an excellent User Guide. The latest version of the free software, Release 7.0a, can be downloaded from the product's home Website at http://www.truecrypt.org,
as well as from CNET's
http://www.download.com, and other sites on the Web.
The User Guide PDF and a more detailed description of TrueCrypt can be found at the product's home web-site.

TrueCrypt is one free program that is, in my opinion, an exception to my general perception of the breed. Of course, the developers gratefully accept donations. In this case, I think they are well deserved.

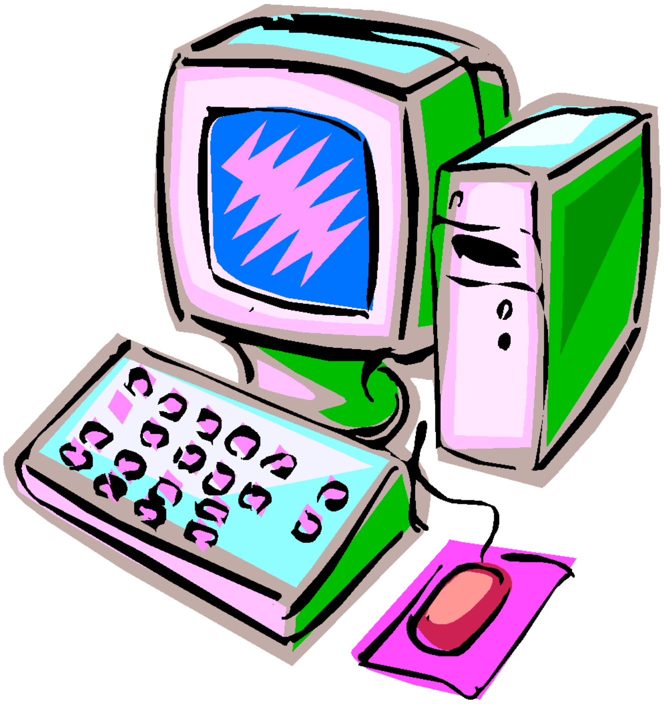
from pg.6

Other "What ifs"
What if the files on the drives are erased? If they are, you can use a free recovery program such as Piriform's Recuva to look for and (hopefully) restore the files. This simple, easy-to-use tool is terrific for recovering pictures from a camera's memory card that have accidentally been erased as well!

What if the hard drive is the reason that the computer died (actual hardware failure)? If the hard drive is the part that caused the computer failure, then you may be out of luck. Yes, there are specialty recovery services that will pull apart the drives data platters and attempt to recover data (and they are usually successful - such services were used, for example, to recover data from the hard drives that were used on computers from the space shuttle Columbia after it broke apart in 2003) but such services are usually very expensive.

A word to the wise
Backup, backup, backup! Whether using one of the Internet based cloud services or a separate external hard drive – if you make it a habit of backing up regularly, chances are good that you'll keep the loss of such a failure to a minimum if a computer fails. Of course one of the benefits of using cloud-based backup services is that you can have access to your pictures anywhere you have Internet access.

Summing it up
A computer that dies can be a loss – but don't lose hope that your valuable pictures (and other stuff) are gone forever. With a little work, you can retrieve your data off the hard drives from a dead computer!



PULP Staff

Editor	Stuart Rabinowitz
Distribution	George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President:	George Carbonell	860.568–0492	george.carbonell@comcast.net
Vice President	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net
Secretary:	Ted Bade	860.643–0430	tbade@cox.net
Treasurer:	Charles Gagliardi	860.233–6054	epencil@att.net
Director at Large:	Richard Sztaba		richer1@aol.com
Web Manager:	Bob Bonato		wmaster@huge.org

Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net

December 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1	2	3
4	5	6	7	8	9 1909 Grace Hopper born	10
11	12 1980 Apple goes public	13	14	15	16	17
18	19	20 General Meeting 7 PM	21	22	23	24
25	26 1951 DPMA founded	27	28	29	30	31