Digital Image Security - Backup, Backup, Backup

Avoid A single Point Failure

By Bill Wight, Staff Instructor, Mountain High Workshops

-DRAFT-5/18/11-

What is the single most important concept in digital photography that you as a photographer must know and probably don't?

It is that every digital storage device and media--removable magnetic disks; optical disks [CDs and DVDs]; magnetic tapes; internal hard drives; external hard drives, USB hard drives, solid-state hard drives, thumb drives and memory cards cannot only fail, but **WILL** fail at some point in time.

Rule Number One In Digital Image Data Security.

Digital Image Data Should Never Be Lost.

It is basic computer knowledge to back up data. Computer users must also know that regular backups must be performed and that the integrity and availability of the backed up data must be periodically verified to ensure it can be restored when necessary.

Rule Number Two.

Read rule Number One.

There is not much worse in the life of a serious photographer than to lose digital images when a computer storage device or storage media fails or image are lost. Digital storage devices and

media can fail for a variety of reasons. Here is a list of some of the ways they can fail and you can lose your digital images:

- A mechanical or electronic problem in the drive or storage device.
- Degradation of the storage information.
- Damage to the magnetic or optical properties of the media.
- A software problem--bug in a program, data corruption, a virus or other malware.
- Malicious hacking by persons unknown into your system and erasure of data.
- Errors that you make--accidental erasure, errors while making a backup set, inadvertently overwriting data, etc.
- Accidental or intentional damage or erasure of your files by someone else--a small child, an angry teenager, a malicious co-worker or a vengeful ex.
- A fire, a flood, an electrical surge, a hurricane, a tornado, an earthquake or a tsunami.
- Theft of computer and backup equipment by a break-in to your home, office, vehicle or hotel room.

Compared to film, digital images have many advantages and a few disadvantages in storing the images. With film, you had only a single original negative or transparency. The film or transparency was somewhat rugged. It was not something that disappeared with the touch of a key. To get a duplicate of a negative or transparency meant taking or sending the original to a photo lab. Making a copy resulted is a slight degradation of the original image quality. You could also keep printed enlargements, but these were not as good as the original film and it was cumbersome to go from a print to a negative again. With digital images, we have the ability to make an unlimited number of exact copies of the original without any degradation, and store them on a variety of digital storage media. The cost of making a digital copy is essentially zero after you have purchased the digital device or media.

As digital photographers and personal computer users, most likely we have all experienced a hard drive or other media failure. I began my personal computer career in 1982 and personally have had just about every kind of media and drive failure possible--failure of analog tapes, digital tapes, floppy disks, Zip disks, CDs, DVD's, and hard drives of all types and brands.

During my career, part of my job in our small division of a Fortune 500-sized corporation was as the IT manager. We had over one hundred PCs and several servers in our facility. After I retired from that job, I worked as a PC consultant for several years for a number of small businesses. So I've seen just about every type of computer failure and data loss imaginable, including accidental erasure, sabotage, fire and water damage (a roof leak poured water onto a client's server), malware damage, and break-ins where the thieves stripped the offices of all computers and accessories.

So our goal should be in light of the above, to design a data storage and backup system that minimizes a catastrophic loss of our digital images and other computer data.

Over the years, I have also seen many back-up systems fail when I or other users went to restore data. This is more common than most people believe. So even when you have a backup system in place, you must be diligent in making sure that the backup system is doing its job. These backup failures can have many causes, from failed hardware, corrupted data, poor operation or incorrect set-up of the backup system. All one needs to do is to go to www.newegg.com and search for a RAID backup system and then read the horror stories from

users who had primary drive failures in the computers and then found that their expensive backup system failed to perform its function of restoring their data files. Or do a Web search for "backup software review" and read the posts of users who's backup software failed to restore their systems and files. The most common restore problem in non-RAID systems appears to be that a disk-image backup failed to restore correctly. It is less common for individual folder and files to be not restored.

You need to ask yourself, "What is my digital data worth to me?"

You probably have on your computer(s), in addition to digital images, other files, documents and email messages that you would not care to lose. I know people who have had un-backed up data on a failed hard drive unit that was so valuable to them that they spent several thousand dollars to have it recovered by a data recovery company. Even if you are willing to pay this much, there is no guarantee that any of your data can be retrieved from a failed hard drive. It all depends on how the unit failed.

It is a lot cheaper, and you will worry a lot less, if you take some of that recovery money and invest in a backup system that can survive a **single-point-failure**.

What is a 'single-point-failure'?

In the field of reliability or systems engineering, a 'single-point-failure' is where the entire system fails due to the failure of an individual part. Your vehicle has dual independent hydraulic breaking systems. An airliner has multiple backup systems for the flight control actuators. These systems protect against the system failing because of a single point of failure in a part or subsystem. I use the term 'system' to include everything that is associated with the safety of your digital data. Not just equipment and media.

Let me give you several real-life examples of single-point-failures that resulted in a catastrophic loss of digital image data.

- A famous movie producer lost 15 years of his video and images and other personal data when his home was burglarized. The thieves not only stole his computers, they also included in their haul his RAID backup drive system. His expensive digital backup system failed him when it was stolen along with his computers.
- A professional landscape photographer just completed a month-long photo trip. On his way home, he stopped for dinner. While eating, thieves broke into his vehicle (parked a block away and out of sight) and stole everything of value, including all his camera gear and his computer and backup hard disk. He lost all the images he'd taken on the trip. His entire system failed due to a single event.
- An advanced amateur photographer had a good backup system in his home office. A wind-driven wildfire in Southern California came upon his neighborhood with almost no notice. The fire burned his home to the foundation. He and his family barely escaped with their lives and they lost everything--all his computer equipment and all his backup disks and drives and all his prints and negatives. A single event resulted in the loss of all his digital information.
- A professional landscape photographer was on a several-month long photo trip. He had all of his images from the trip on the hard drive of his laptop. His backup set was also on the hard drive of his laptop. As he was traveling over a bumpy dirt road, his laptop went

airborne and hit the floor of his vehicle. The hard drive was ruined and he lost all of his images from his trip. He relied upon a single device for his images and the failure of that single device resulted in data loss.

- Another professional landscape photographer was on an extended photo trip. His backup system consisted of a 1TB external 120 volt-powered hard drive. He took so many images on this longer trip that he filled his laptop hard drive. So he copied his images from his laptop to his external hard drive to free up space. He deleted the digital images from his laptop to make room for more new images. He now had no backup of the images he removed from his laptop hard drive. Sometime later in an internet cafe, he was backing up new images from his laptop to the external hard drive when he got tangled up in the 120 volt power cord for the external hard drive and it fell to the floor. The external 1TB drive was damaged and he lost most the images from his trip.

The above examples do not include the most common way image data is lost--due to equipment or media failure--but illustrate how easy it is to have a single-point-failure that results in the loss of irreplaceable digital images.

How do we protect our valuable and irreplaceable digital images and data?

Here are a few guidelines and tips for minimizing the possibility of losing your data:

1. Do not allow a single-point-failure to result in data loss.
2. Have a reliable automatic data backup system in place.
3. Have three separate sets of your data and images.
4. Keep one copy of your backup set in a separate physical location.
5. Keep your software products--OS, security, applications, and utilities--up to date.
6. Keep a robust two-way firewall in place and active.
7. Periodically check the integrity of your backup sets.
8. Your data is only as safe as your latest backup.
9. Make sure your backup copy is the same as your original, verify it.
10. Do not create a chain of corrupted backup sets.

Let's talk about these points one by one.

1. Do not allow a single-point-failure to result in data loss.

Let's put on our 'reliability engineer' hats and go through an analysis of our computer backup system and look for all ways that a single-point-failure can result in a catastrophic loss of our valuable digital images and other data. What we engineers do is to create a failure analysis and list all the ways that our system can fail. We make a list of all the failure modes we can think of. Then we develop means of preventing any of the failure modes from causing a loss of data.

2. Have a reliable automatic data backup system in place.

Face it, trying to have a backup system that relies on us to do it manually is just asking for trouble. You need to have a software backup program in place and working that can automatically schedule a backup of changed files each night.

3. Have four separate sets of your data and images.

Assuming that your computer has two internal hard drives.

Keep one set of your images and other computer data on your primary hard drive in your computer. That is set one, your working set.

Have a backup set that is on a secondary hard drive within your computer. This is set two.

Have a third backup set that is separate from the computer but can be in the same area, like an external hard drive. This is set three.

4. **Keep the fourth set of your backup set in a separate physical location.**

To have a single-point failure-proof system, you must keep one set of your data separate from your computer, like at work. If that is not possible, keep a copy at a relative or friend's home. If that is not practical keep one copy in another part of your home, away from your computer and out of sight. If you must keep your fourth data set at home, try to find a place that will not suffer the same fate as your computer in the event of a catastrophe. Here are some pointers:

a) keep it high enough above the floor so it will not be damaged by a flood;

b) keep it safe from a fire, like in a fireproof file cabinet;

c) keep it safe from an earthquake, someplace it cannot fall or have anything fall on it;

d) keep it hidden so a thief who comes into your home is unlikely to steal your backup drive. A lockable, 4-drawer, heavy, fire-proof file cabinet is a good storage choice. You can also store all our important papers there too.

And don't forget to refresh this drive so it has as recent a backup set as is practical. The longer between times of rotation, the more data loss is possible if your other backup sets are lost.

5. **Keep your software products--OS, security, applications, and utilities--up to date.**

It should be fairly obvious to personal computer users these days of the need to have a good security program. Newer forms of attack by malware comes in many ways, with the most popular now being the drive-by web page infection. So to help protect your valuable data, make sure that you do have this protection. Also, make sure that your operating system and application programs are current with all security updates. It is possible to lose data on a computer due to a software bug.

6. **Keep a robust two-way firewall in place and active.**

To minimize the possibility of a remote intruder from getting into your computer from the Internet, you need to maintain a robust firewall that keeps intruders out. You should have a firewall that blocks both incoming and outgoing unwanted messages or data. A firewall is usually included in an anti-virus or security program.

7. **Periodically check the integrity of your backup sets**.

It's a fact of computer life, data can become corrupted, in a variety of ways. So for your backup data, you need to periodically check to make sure you can do a restore from you backup sets. I simply go into the restore feature and select a temporary folder on my primary internal hard drive and select a few backed up folders and let the backup program restore them to the temporary folder. Then I check them to make sure that the data is valid. I do this about once a

month. For a disk image, this is not possible, so you must rely on the reputation of the company that made the software you use. Again, a disk image backup should not be your only backup set. In addition, you should have several non-disk image backup sets.

8. **Your data is only as safe as your latest backup.**

This is a bit of an exaggeration. But what this means is that if you have created new content on your primary hard drive and you have not backed up that data, then it will be lost in the case of the failure of or data corruption on your primary hard drive. Your backup software cannot restore data that was not backed up. So if you have your backup system set to run automatically every night at midnight and you download a bunch of new digital photos to your primary hard drive or you are working in Photoshop and creating your masterpieces, none of those files are protected because your backup will not run until midnight. So if these files are important to you, need to back up the files manually as soon as they are on your primary hard drive. Yes, this is a lot of work. But it is absolutely necessary to minimize the possibility of data loss.

9. **Remember to make sure your backup copy is the same as your original, verify it.**

There are occasions when the backup software writes corrupted data to your backup hard drive. You can make sure that the data that is written by the backup program is the same as that on your primary hard drive by turning on the '**Verify**' feature. This feature compares the just-written backup data with the original data. Not all backup software has this feature. Doing this takes almost twice as long but it is necessary to insure against data loss.

10. **Do not create a chain of corrupted backup sets.**

In a backup structure where sequential backup sets are created, I have seen this problem occur many times in the past. A primary data set exists (a file, a folder or an entire volume) and somehow it becomes corrupted. A backup of this data occurs and the backup set now contains the same corrupted data as the original. A third backup occurs and now there is a chain of corrupted backup data sets. This situation usually occurs in a sequential backup system. A sequential backup set works like this: day 1, a backup copy of the data is made, and is named "backup(1).dat". The next day a new backup set is created, named "backup(2).dat". This process continues for say five days. Then the oldest backup set is replaced by a new one and named "backup(1).dat" again. So if data were to become corrupted in the primary data set, in five days all the backup sets will contain copies of the corrupted data and the backup scheme has failed.

How to Establish A Backup System

There are many ways to create a backup system for your images and data. Some are better than others and some methods are more expensive than others. Just make sure that any system you put into place meets the guidelines mentioned above. In some ways, your backup system will be dependent on the number of images you have. If you have terabytes of images, your system will be more complex and expensive than one that backs up tens or a hundred gigabytes of data.

Where to make your backups:

You can elect to have your backup set created on a variety of storage devices. My recommendation is to keep it simple.

On-Line Backup:

A new way to do backups is to use an on-line backup service. I don't advocate using one of these services for several reasons. First, they will cost you at least $50 per year. For $50, you can now buy an external hard drive of 320GB capacity. Second, the uploading of your backup files is limited by the speed of your internet uplink connection. It can take weeks for you to upload a full backup of five hundred gigabytes. Further, it can take weeks to download your files in case you need to do a full backup or you must ship the on-line backup company a blank hard drive and pay an extra fee to have them copy all of your files onto the hard drive and ship it back to you. For me, this does not seem like a very workable system. In addition, several on-line backup companies recently went out of business and did not give users enough time for many of them to download all their stored data. This is also known as 'cloud' data storage. Meaning that your data is in the 'clouds' somewhere.

Before you decide to put your valuable data in the hands of an on-line data backup service, be sure the read the fine print. An example is below:

"Our systems are vulnerable to damage or interruption from earthquakes, terrorist attacks, floods, fires, power loss, telecommunications failures, computer viruses, computer denial of service attacks, or other attempts to harm our systems. Some of our data centers are located in areas with a high risk of major earthquakes. Our data centers are also subject to break-ins, sabotage, and intentional acts of vandalism, and to potential disruptions if the operators of these facilities have financial difficulties. Some of our systems are not fully redundant, and our disaster recovery planning cannot account for all eventualities. The occurrence of a natural disaster, a decision to close a facility we are using without adequate notice for financial reasons, or other unanticipated problems at our data centers could result in lengthy interruptions in our service."

I hope that makes you feel really secure about on-line data backup services.

At Home:

RAID Hard Drive Systems:

RAID stands for **R**edundant **A**rray of **I**nexpensive **D**isks. This method uses a system of at least two hard drives and it stores copies of your data across multiple disks. In theory, if one drive fails, you can still access all of your data, because a redundant copy (a mirrored copy) is stored

on another disk in the RAID. This process is controlled by a RAID controller, which can be either hardware or software. The RAID system automatically maintains the duplicate data sets in real time. The user is unaware that there are multiple copies of the data.

Advantages: when it works is a very easy and secure way to have multiple sets of your data. In some RAID systems you can 'hot swap' a failed hard drive and the system will recreate the data on the newly-inserted drive.

Disadvantages: First, the RAID systems require more hardware and are more expensive per GB of data backed up. Second, the RAID controller manufacturers use a company proprietary system for controlling the RAID system and the data is usually written to the hard drive in a proprietary format. In other words, the data cannot be directly read by your operating system. Third, they are more complicated. Fourth, they do not provide for a fourth backup set that can be taken off-site or stored somewhere separate from your computer. Fifth, when a RIAD system fails, you lose all the data on the RAID system. From user forums, this happen much more often than the RAID systems manufacturers would like to admit. When a RAID system fails, you are at the mercy of the tech support of the company who made the RAID system. Horror stories of poor tech support abound in the user forums of failed RAID system from all the manufacturers.

Some well-known companies that make RAID systems and controller are: Drobo, Rosewill, Netgear, Adaptec.

I do not personally use a RAID backup system but I know several photographers who do and they are happy with them.

Internal and External Hard Drives

The most common way for home and small office computer uses to backup their data is to use internal and external hard drives. The amount of data we now store on our systems, most notably digital images and video files, are very large and so that makes copying these files to a tape magnetic or optical disk (CD and DVD) medium impractical. So we are left with backing up a hard drive onto another hard drive. Fortunately, the cost of both internal and external hard drives have come down so that you can now purchase a hard disk of 1TB capacity for less than $100US.

Here is what I recommend: equip your desktop computer with at least two high-capacity internal hard drives. The drive capacity should be as large as you can get, 750GB or 1TB. Use the primary hard drive for your primary, original, data and the secondary internal hard disk for your second set of data. Having your data backed up on just one internal hard drive does not satisfy the requirements set forth above. Since you only have one backup set, and it is inside your desktop computer, you are not protected from a single-point-failure. A third internal hard drive, if your computer will accommodate one, will give you another backup set, but you are still not protected from a single-point-failure, as the third disk is inside your computer. Theft, catastrophic damage or viciously-destructive malware can all render all three backup sets useless.

You can purchase 1TB external hard disks for around $120US. The full-sized drive are powered by USB or 120 volts in the USA and connect to your computer via USB or Firewire. The prices

for these drives seem to fall every month. I recommend that you buy two of these external hard drives with a capacity of 1TB. One of the external drives will become your third backup set and the other will become your fourth backup set that you keep separate from your computer.

Digital Tape Drives:

In the past, the only practical way to copy large amounts of data for backups was to use digital tape drive systems. However, with the low cost of today's high-capacity hard drives, that is no longer the case. I do not recommend the use of tape drive systems for backup. My personal experience is that these are the most unreliable of all ways to backup data.

Compression and Encryption

When hard disks were more expensive, it made sense to compress the backup data to be able to store more of it on an individual device. However, with today's terabyte plus capacity hard drives, I don't find this necessary. Compression of the backup data tacks on another layer of something that can go wrong. The only compression scheme I recommend or use anymore is the Zip format. This is a common format and does not rely on a specific company's propriety compression algorithm.

You may feel it necessary to employ an encryption algorithm to your data but I suggest you limit this to personal data that you would not want to fall into the hands of the bad guys if your computer was hacked or stolen. I would not use an encryption scheme for your digital images. Lose the encryption key and you lose the data!

For my digital images, here is what I do:

1. I use 8 and 16GB memory cards in my Nikon DSLR cameras. After downloading the images from my camera memory card to a folder on my secondary internal hard drive, I do a check to make sure all the files are readable.

2. I then copy the newly created image folder from my secondary internal hard drive to both my 2 TB external hard drives. So now I have three identical hard drive copies of my newly-downloaded master images files--one on my internal secondary hard drive, and a copy on my two #1 and #2 external 2TB hard drives.

3. I take my #2 external 2TB hard drive to my daughter's office and put it in one of her file cabinets. This gives me an off-site storage of all my digital images.

4. My automatic backup software created a first-time copy of all the data on my primary and secondary internal hard drives onto my #3 2TB external hard drive. Each night, it automatically creates an incremental backup of all the files on my internal hard drives that have changed. So when I've added new digital images to my secondary internal hard drive, that night the backup software makes an incremental copy of that data.

5. Once a month, I bring my #2 2TB external hard drive home from my daughter's office and update all the images files using the free Microsoft tool 'Sync Toy'.

6. Every 90 days or so, I delete all of the backup sets created by my backup software and that night let the backup program create a new first-time backup set on the 2TB external hard drive. This may take more than 16 hours, so I just let it run in the background until it is finished.

Now, I have a fresh set of all the files on my two internal hard drives. Then on the following nights, new or changed files will be added to the backup set.

A successful backup strategy needs to take into account how you use your computer and what type of data files you need backed up. For example, if you are a digital photographer, you are basically copying files from a memory card to your hard drive. Or you are scanning in negatives, transparencies or prints to a digital file. First off, you should never edit or modify an original digital image file. All of your image editing should be with a copy of your original. You will use an image editing program to modify a copy of an original digital image. So you have two types of digital image files. One is your original digital image master file, and another is the edited version. Your original image file should be archived. It never changes. If you are saving your digital images in your camera as a RAW file, then the file is never edited. An edited image file can and does change. You may have multiple versions of the same digital image. So these two types of files must be backed up in different ways. When I edit a digital image in Photoshop, the image will start with a name like this: Mammoth-2009-3-0341. When I'm finished editing, I save it as Mammoth-2009-3-0341-b. If I make another version it is named Mammoth-2009-3-0341-c, etc.

If you are writing a textbook, or creating the Great American Detective Novel, or the script for the next hit TV show, you will be making additions and changes to your text file and you need to make backup copies in a different manner than for digital images. For example, you may have a novel in the works. You could name it **My Great Mystery.doc**. Every time you finish adding to it or editing it, you would save your work to a sequential file. That way, you will have a series of files that have all your changes. **My Great Mystery-bak-001.doc,** then **My Great Mystery-bak-002.doc, and My Great Mystery-bak-003.doc**. This way if in a recent edit you delete a section and then someday want to get that section back, you can find it in one of your sequential backups.

If you use email and Instant Messaging on your computer, and if those message files are important, they too must be backed up. But doing that is not as clear-cut as copying your digital images or document files. You need to find the folder where your email client keeps the files and then copy that folder and sub-folder to your backup hard drive.

Backup Strategies

When making a backup of the files on your computer, there are two main ways to accomplish this. One is to make what is called a 'disk image'.

Disk Image Backups

The backup or Ghosting software creates an exact image of the primary hard drive onto a backup hard drive. The reason to do this is so that if the main system hard drive fails, a disk swap or a copy of the image can restore the system to the point the last backup image was created. This will save all your operating system, your system registry, all your programs and settings and all of your data files.

Advantages: In theory, it is easy to restore a complete image of the system and have it as it was at the time the image backup was made.

Disadvantages: the main problem with this method is that when a restore is needed, the user sometimes discovers that the backup system will not restore their drive image correctly and they find that the backup system they relied upon has failed them. From what I've read in user forums, this may happen as much as 30% of the time.

Non-Image Backup

There are three main ways most people backup computer files.

I Full and Incremental Backup Method

This the most common method that backup software uses. It consists of making a full backup of all the files on the computer. Then each time the backup software runs, it creates an incremental backup of all new or changed files. The way the backup software knows which files to include in the incremental backup is that on computer file systems, there is a bit in the file header called the 'archive bit'. If the archive bit is set to binary zero, the file has not been backed up. If the archive bit is set to a binary one, the file was backed up. A new file when it is created by the Operating System [or a user program like Photoshop that tells the OS to create a new file] the archive bit is set to a binary zero. When a file is changed, the OS checks to see the state of the archive bit. If it is zero it leaves it as zero, if it a binary one, it resets it to a binary zero. When the backup software runs the next time, that file will get backed up. The backup program will use some type of library or database to keep track of the main backup files and all of the incremental backup files. When you use the backup software to recover a file, the program will look up the file backup history in its catalog on the backup hard drive and then replace the latest copy of the file to its original location or a folder you have designated for the recovery.

Advantages: low disk space usage for the backed up files. All files selected by the backup program are copied to the backup device. This is usually done by scheduling the backup program to run automatically each night at a given time.

Disadvantages: It is necessary to have a copy of the backup software to do a restore of the lost or damaged files. For the loss of individual files or folders, you would use the backup software to do a partial recovery of the lost or corrupted files. In the case of a completely corrupted or damaged hard drive, you must have a copy of the backup software available to restore the files. Depending on the software this can be easy to recreate, if one using the built-in backup program supplied with MS Windows or Apple Mac OS's. For most third-party backup programs, a restore cannot be accomplished until the backup software has been reinstalled on the computer.

There are also some third-party file manager programs that will copy files from the primary hard drive folders to a backup hard drive folder and if the file already exists on the backup hard drive, will compare the Date Modified field. If the file to be copied is newer than the file on the backup drive, then the program replaces that file. If the date modified is the same or older, the file is not replaced.

II Sequential Backup Method

In this method, a complete copy of the selected files, or all the files on the system, is made on a backup device. The first copy is called Backup-A, the next Backup-B, the next Backup-C and so

on. At some point, Backup-A is erased, and replaced by a new set, then Backup-B is erased as new backup sets are created on the backup device.

Advantages: No backup software is required to copy the backed up files from the backup device to the main computer hard drive(s). You use a file manager program, like the Windows Explorer to do the copying.

Disadvantages: It is possible with this method to corrupt an entire chain of backup files. This method also takes more hard drive space than the Incremental method. Also, since there is no software program, all backups must be done manually.

III. Replacement Method

In this method, a backup set is created. Then when another backup set is created, the original is deleted and is replaced with a new copy.

On The Road Image Downloading and Backup and Tips

We have been asked how the Mountain High instructors handle our image downloading and backup when we are on a photography trip. Here is my rule for image data while I'm on a trip. I never delete images from my storage cards until I have two separate copies of the images.

We all use laptop PCs and we remove the memory card from the camera and put the card in the card reader slot or use a USB 2.0 port card adapter.

James and Kevin use Photoshop Bridge to download their images from the memory cards to the laptop. Bill Uses Photoshop Elements 7. Jeff uses Adobe Photoshop Lightroom 2.0.

Bill's Dell laptop has a 160 GB internal hard drive and he purchased two Western Digital My Passport compact external USB 2.0 hard drive with 320 GB of storage. James has two of these at 500GB capacity. Jeff uses two 1TB external 120 volt-powered hard drives for archiving and backup. Kevin uses a 500GB external hard drive for backup.

When you download images from the card to your laptop, you should check the downloaded files to make sure they are not corrupt. Each time Bill downloads his images to his laptop, he makes sure that the same number of files were downloaded as there were on the memory card. Then he does a random check of the images with the Vista Windows Photo Gallery. He then copies all the downloaded files to one of his WD Passport external hard drive. He then does another random check of the backup images. He then stores the Passport drive away from the laptop. Bill then uses the Windows Vista, Windows Explorer to burn the downloaded images to DVD disks. One 4GB memory card fills one DVD -R or +R disk. He then checks a few of the burned files to make sure they are OK. Then and only then does Bill put the memory card back in his camera, delete all the files and then do a Format of the card.

The SD and CF card experts tell us to never delete the images or format a memory card using your computer. These tasks should be done in your camera. The experts also say that to minimize data corruption in your memory cards never let your camera battery get below 25% and keep shooting. A low camera battery is said to be the major cause of data corruption in memory cards. Also, make sure that your camera is turned off when you insert or remove a

memory card. Keep your fingers off the contacts on an SD card as the oil and sweat from your fingers can corrode the contacts.

There are also on the market several devices that you can use to download your memory cards to and some allow you to view the images. The Epson P-6000 and P-7000 are good devices as is the Jobo Giga Vu Pro. However, the prices of these devices are about the same or more than for several brands of Netbook computers. Acer sells several models with 160GB hard disks for less than $350US on www.amazon.com. These offer the same features as a full-sized laptop computer but in a smaller form factor that are great for traveling. In fact, if you are doing any extended foreign travel where access to the net and computer parts or services are not available, buying one of these Netbooks for a laptop backup is a smart move. Remember to purchase a power adapter for foreign travel.

There is always the possibility that you will be in the field and your laptop computer will fail, get dropped or stolen. In that case you will need to have with you enough memory cards to be able to keep shooting on your trip. You should have your external USB backup hard drive separate from your laptop and hopefully you have burned your images to DVD disks. Your DVD disks should also be kept separate from your laptop computer case or bag.

Keeping your images safe

Kevin uses a series of 4GB cards in case one fails he does do not lose too many images. He owns some 16Gb cards but he does worry about using those if the card becomes corrupt. In terms of backup on the road he always carries a laptop and a 500GB portable external drive to backup on two sources. He also tries not to use the CF cards again until he returns home in case of a failure of his backups so he essentially has three backups upon returning from photo trips. When he returns home, he downloads the Raw images to two different 1 TB external drives and does a backup on his Mac Pro so again he has three copies. He learned the hard way--when he went to Colorado two years ago for a fall season trip for a whole month. He downloaded his memory cards to his laptop and then reused the CF cards. He made no backup of the files. While driving the rough back-roads, his laptop bounced off the seat and onto the floor of his vehicle and destroyed his laptop's internal drive. He lost 21 of his 29 days of images. So he learned from that experience to backup multiple times.

Jeff recently lost many images when he found himself on an extended trip that resulted in the filling up of his laptop internal hard drive. As he was copying images to an external hard drive, it fell to the floor and was damaged beyond recovery. That drive contained the only copy of many images from that trip. So even us 'experts' sometimes foul up and lose data that can't ever be replaced.

While traveling, if your image files are of value to you, and we all think ours are, then you need to be aware of some of the things that can happen. First, memory cards sometimes do become corrupt. If you are shooting with 8, 16 GB, 32GB or 64BG cards and one of those cards becomes unreadable, you stand to lose a lot of images. Before you toss the cards, try the manufacturer's recovery program or one from a 3rd party. A set of 4GB SD or CF cards might be a better bet than higher-capacity cards. You can now get 4 GB high-speed SD and CF cards for very reasonable price.

If you are fortunate to have a pro-level camera like the Canon 1Ds Mark III or the Nikon D3, or the Nikon D300s then your camera has two card slots. We advise that you use one card for images and the second for a backup.

You can put your laptop computer with your external hard drive in your computer case or bag. Everything is nice and organized and handy and then someone steals your entire computer bag or case, including your precious images and the backup drive. Computer theft happens all the time, from vehicles, from RV's, from hotel rooms, checked baggage on airlines, and even grabbed from your person. Take all the precautions you can but be prepared if someone does steal your laptop. Keep your laptop and your external backup drive in separate places, in different areas of your vehicle, hotel room or RV or in a separate checked bag or better yet, carry it on with you. We recommend to never put your laptop computer or camera gear in checked baggage on an airline. Baggage handlers can now see into your checked luggage with the x-ray machines and the crooks have ways of signaling their cohorts which baggage is worth opening. Carry them on with you and put up a fight if the airline says you have to check them.

If you travel in an RV, put your external backup drive in a hidden place, somewhere not likely to be searched by a thief in a hurry. Someplace like your sock drawer or a cabinet behind a box of cereal. Do not leave your computer out on a table or desk when you leave the RV in a campground for a day trip. Close the shades and put the laptop away in a place that is not visible. When in a hotel, put your laptop out of sight in a drawer and your external hard drive somewhere separate or in the room safe if available.

Don't Forget That Your Smart Phone Is A computer too

Many of us use smart phones, some of them with many gigabytes of data storage capacity, including data, music, images, video and photographs. The data on these smart phones is even more at risk than the data on your home computer. You are a hundred times more likely to lose your smart phone than your home computer or even your laptop computer. So if the data on your smart phone is important, you must learn how to transfer that data to your home computer's hard disk and include it in your backup system.