

Paul Inks/ Stacy Norcross
Instructor Mike Brooks
Forensic Photography III
January 29, 2007

Choosing a Digital Imaging Storage System

With more law enforcement agencies converting to digital imaging, the storage and retrieval of digital assets is becoming a primary concern. Information can now be captured and stored in an electronic format, allowing agencies greater access and the ability to share and distribute information endlessly. This electronic format can be recorded from a variety of devices, and in many formats giving the user an array of options to record information. Today, digital cameras are capable of recording still images, video images, and audio files on a single camera. Although there are many types of media that can be captured and stored digitally, this paper will only address digital photographic images. The ease of capturing and sharing information and the variety of format options has led to greater implementation of digital imaging in law enforcement, and has increased the need for storage and maintenance of this information. As the volume of digital information grows, the need for a well designed system that meets the needs of security, accuracy, and reliability must be addressed. Police departments are forced to make tough decisions in choosing a storage system, usually with budget being the driving factor. Being knowledgeable in all variables, pros and cons of each type of system, and future capabilities of computer systems will assist law enforcement in making educated decisions in a digital media storage system that will be fully operational and adaptable for many years.

In discussing a digital storage system, one must first define the parameters of a “storage system”. For the purpose of this paper, a storage system is defined as any means utilized to permanently record and preserve any data captured in a digital format. This loose definition allows the maximum range of systems addressing all departments’ needs, budgets, and configurations. The purpose of preservation is to ensure protection of information of enduring value for access by present and future generations. (Conway, 1990:206) In law enforcement terms, preservation is necessary to ensure the ability to investigate crime and prosecute the offenders. To understand the different storage systems we must first know the pros and cons of each possible component of the system.

While tape is the one of the oldest storage mediums, it is still thriving. Affordability is the number one factor in its longevity; the proven storage length is also a strong reason. Stored correctly, data on a tape has been proven to be readable for at least 30 years (Marks, 2006). The drawback to magnetic tape is being able to maintain a compatible drive and its long retrieval times. Along this avenue, it also requires a considerable amount of time to write to the tape. Depending on the amount of data to store, the read and write times could extend into days.

Optical media is possibly the most popular storage solution today. With its reasonable storage capacity, portability, and accessibility, it seems to provide a cure-all for most storage dilemmas. However, the manufacturers' claims of a shelf life of 50 years or more have yet to be sustained. It has been found that information stored on either a CD or DVD has been defective after only 3-5 years depending on the quality of the media and storage environment. Many in the imaging community believe CD and DVD storage is too risky. It can pose problems such as disk failures, incomplete files due to multiple updates, and wasted time searching for files assets spread across multiple CD's just to name a few. Compatibility issues are also a concern. In the DVD format, manufacturers have created two main types of formats, DVD+R and DVD-R. While both perform the same functions, not all computers are compatible with both formats which can lead to confusion. Blu-Ray, UDO, and other products on the horizon are offering greatly expanded data storage capabilities, but are still relatively new and may not be recognized or accepted.

With the questionable reliability of optical media as a major downfall, one would think a removable hard drive could be a remedy. With its storage capacity being much larger than an optical disk, a department may be tempted to invest in many removable hard drives and then storing each one after its capacity has been reached. Its downside is the fact that no true long-term research has been conducted on how long one can store a removable hard drive on a shelf. After time, the information stored on the disk just fades away, caused by thermal magnetic decay. Even vendors will not guarantee their product beyond a maximum of ten years. Also, when trying to replace the hard drive, obsolescence becomes the challenge. Vendors often produce new and improved versions of hardware and discontinue parts for the older items. This makes maintaining a fully operational system difficult, especially when working within the confines of a law enforcement agency's budget.

A server system seems to be the ultimate resolution to all of the above problems. Being adaptable to meet almost any need, more reliable, and able to expand to meet storage needs, a server is appealing. However, appeal is costly; to the point of being prohibitive to a department with a small budget.

In every solution examined above there are still overall issues that need to be addressed. Complete system failure, the human factor, progression of technology, budget, and poor planning all need to be addressed and strategies must be implemented to avoid loss of important digital assets.

With so many advances in technology, law enforcement agencies are struggling to keep pace with the cost of storage systems. Budgetary concerns are usually the biggest driving factor in the choice between systems. Smaller departments which are limited in their purchasing power usually choose a smaller storage system comprised of a hard drive with DVD backups. The instability of this system is a trade off for a more stable, but expensive system. A larger department needs to be concerned with a larger storage capacity which, in turn, costs more.

To overlook the possibility of massive storage failure could literally prove to be disastrous. When addressing a hardware/software failure or a natural catastrophic event such as a hurricane, earth quake, flood or fire it is imperative to have a back-up system in place to preserve the digital assets that are so instrumental in proving a case in a court of law. Not only does a department have to decide on what type of storage system to install, but how to back up all of the information stored should that system fail. A single hard drive on a single computer is the poorest system for storing vital information. Agencies have lost valuable information when it was stored on a single computer. As a protection against unfortunate incidents such as fire, tornados, floods, etc., store one of your backups in a different secure location (Bockaert). The most likely solution would be offsite storage in another secure facility. Some image management systems incorporate a duplicate system or storage area in another location. This is called redundancy. Systems capable of redundancy range from a few thousand dollars to over a hundred thousand dollars depending on the needs and configuration of the system. The demands of an individual agency will vary greatly; so flexible, customized systems are a necessity for law enforcement agencies. If a few thousand dollars is prohibitive the companies offer backup services. Companies such as Linear Systems and Iron Mountain offer data backup and recovery. With continuous, automated backup and a reasonable monthly subscription fee, it seems to be a reliable way to ensure the safety of digital assets. There is no initial capital investment, so almost any department's financial office can easily incorporate the subscription fee into its budget. This also provides a fail safe should the department's hardware/software should be lost. However, in law enforcement the issues of image integrity, controlled access, and chain of custody may be forfeited with the use of a non law enforcement agency storing sensitive information. Having graphic images displayed on the internet as in the California Highway Patrol case involving Nikki Catsouras could result in law suits costing millions more than a secure imaging system (Hardesty). A secure system providing instant access to only individuals involved with the case, and system administrators would reduce the possible of information being compromised. Additionally, the ability to track and log all activities to the individual file and the action taken should be recorded and easily accessible by the system administrators. Systems are available to control information sent out on CD. Images can be placed in a password protected package and burned on to the CD to prevent the release of information to an unauthorized person.

Another issue that must be addressed is the human factor. Any time the human factor is introduced into a system the chance for problems to surface multiplies infinitely. Whether an innocently or maliciously, people tend to create fatal errors in any computer system. An angry employee or computer hacker can bring a computer system to its knees within minutes by introducing a virus. An employee unfamiliar with a system may also unknowingly crash it with just a few keystrokes. This is another reason why constant, continual backup of the system is necessary and can provide a seamless transition to the backup information should the primary system fail.

The ability to transfer data from a system close to becoming obsolete to a newer more updated system is called the migration of data. For instance, when 3.5" disks were being phased out, most computer systems still offer the 3.5" drive and the newer CD

drive together. Today, most systems offer a combination CD/DVD drive with read and write capabilities. If this were not offered, a system would become outdated with no ability to be updated with the newest hardware available. So to avoid incompatibility issues, it is advisable to migrate your data to newer media (Bockaert). The time frame for decision making also becomes a challenge since hardware changes so rapidly, it is necessary to make educated decisions quickly before the storage system becomes completely outdated.

Migration is more complex than simply transferring a stream of bits from old to new media or from one generation of system to the next. Complex and expensive transformations of digital objects often are necessary to preserve digital materials so that they remain authentic representations of the original versions and useful resources for analysis and research. (Task Force on Archiving of Digital Information)

In this sense, keeping a system up-to-date becomes a continual battle and constant expense. Planning becomes of primary concern to ensure that any digital images stored are retrievable in the near future and beyond. Proprietary systems and obscure formats can hinder an agencies ability to migrate its information from one system to another.

The dependence on one type or manufacturer of a system can lead to unexpected problems in the future if an alternative more adaptive storage system is not purchased. For instance, if a system's manufacturer goes out of business or discontinues service for a particular system how does the department continue to store assets? What if the system needs maintenance or repair? A system that is compatible with common open standards and recognized brands may be a wise investment. This alleviates the problem of a storage system becoming instantly obsolete should the company go bankrupt.

Poor planning on the department's behalf is often a precursor to an expensive failure. Not conducting a proper needs assessment can be disastrous. Purchasing a system before knowing exactly how much storage is required and whether or not it can be expanded to accommodate a department's growing needs can lead to dead ends in productivity, sometimes in just a couple of years. The purchaser should understand the department's needs and the equipment currently being used. Different cameras turn images into different sized files. It may take 500 photos to fully document a homicide, sometimes more. In large agencies, cases have been turned in where thousands of Raw format images must be loaded to a storage area. Storage capacity can be difficult to estimate if the stored data is to be stored in a variety of formats or resolutions. Compressed and uncompressed images will vary greatly in their storage requirements. Each frame captured will differ slightly in composition, color, and lighting. This variance will cause the compression algorithm to create a variety of file sizes despite very similar images. This difference maybe small, but when multiplied by hundreds, thousands, or millions of images, it will make a substantial difference. If the purchaser knows approximately how many photos are taken each month and year, the type of

equipment used, and the size of the files created for each type of image, then a rough approximation of storage needs can be ascertained.

Several variables contribute to the file size issue and the purchaser must be educated as to all the possibilities. Vertical and horizontal resolution, the color bit depth, pixels per inch, and compression algorithms are just a few of the factors that determine file size. Using color bit depth as an example, an 8 inch by 10 inch image will create an image size of 20.6 megabytes with 8 bit color. The same file with a 16 bit color will increase to 41.2 megabytes.

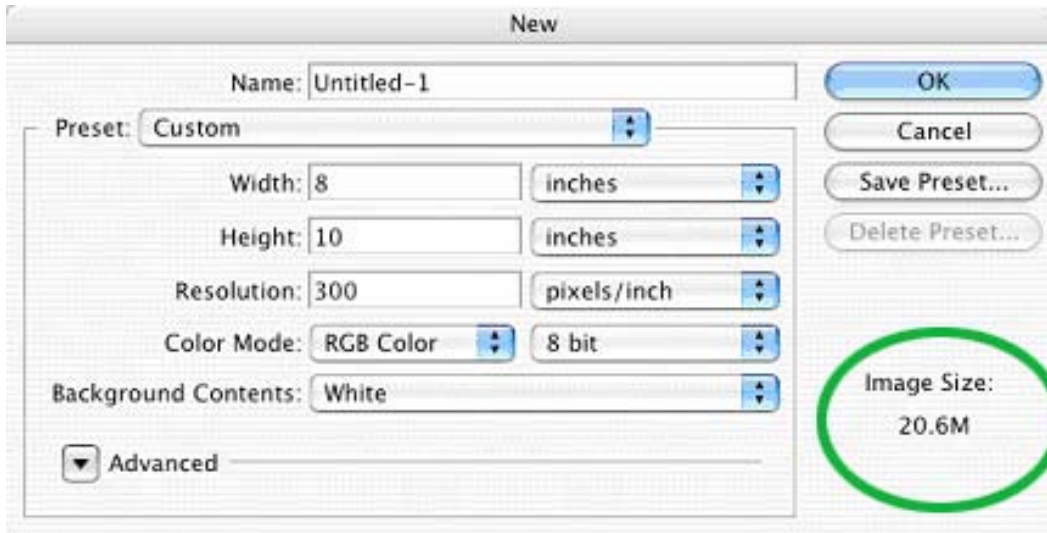


Image of Photoshop screen with 8 bit color mode selected. (Above)

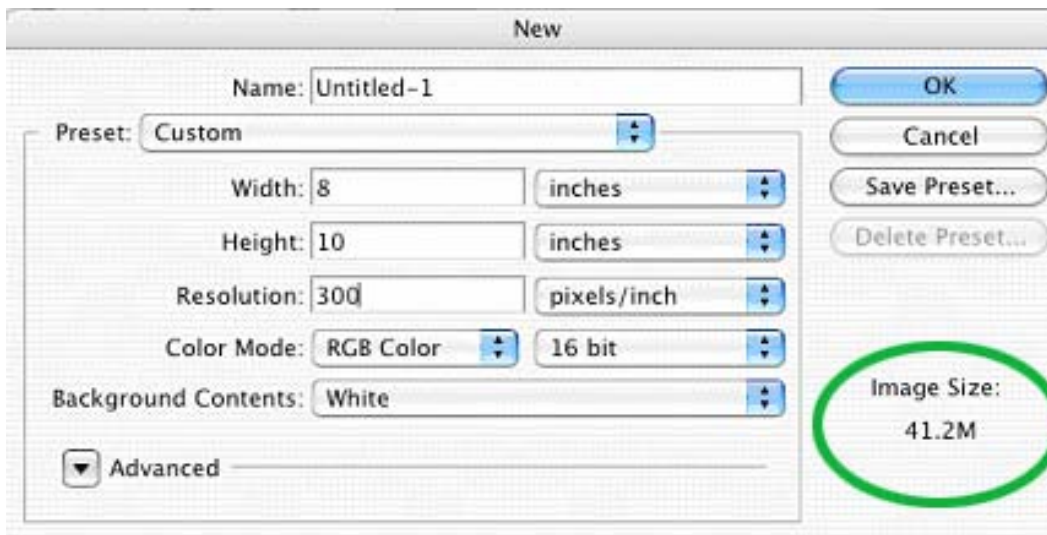


Image of Photoshop screen with 16 bit color mode selected. (Above)

What appears to be a small change can have drastic results in the storage requirements. Stored files from scanners or images created in image editing software may be

substantially larger than images from a digital camera and need to be accounted for when estimating storage needs.

Most images stored by a law enforcement agency are from digital cameras and understanding the amount of storage required to maintain electronic data will depend on the equipment used and the configuration of the equipment. Below are samples from a couple popular digital cameras. The RAW, Tiff, and JPG fine formats were considered because these are the preferred formats of law enforcement. Not all camera manufactures offer the Tiff feature, and Fuji offers a Wide and Narrow dynamic range in their Raw format.

	<u>RAW</u>	<u>Tiff</u>	<u>L</u>	<u>M1</u>	<u>M2</u>	<u>S</u>
Canon 1Ds Mark II	12.6Mb	N/A	9.16Mb	2.38 Mb	1.90Mb	1.16Mb
Nikon D100	4.28Mb	17.71 (L)	1.93Mb	1.03Mb	N/A	582Kb
Fuji S3	25.0 Mb W 13.0Mb N	N/A	4.10Mb	2.20Mb	1.45Mb	691Kb
Fuji S9000	18.71Mb	N/A	4.33Mb	1.14Mb	714Kb	616Kb

If an agency chooses to capture all crime scene images in a lossless format, such as RAW or Tiff, the amount of storage space will greatly increase and the ability to work with the information will become time consuming if the computer infrastructure is not able to handle the larger file sizes. Because of this many agencies are choosing to capture the majority of images in a JPG format and use the larger files for images where the high quality capture is required. This allows them to store, transfer, back up, and print the information much quicker. The demands from using all RAW or Tiff files placed on the computer infrastructure are significant and should be considered when designing a system. Some management schemes store the Raw or Tiff file as a secure master and then create a high quality Jpg for use over the network. This allows much faster access to the information, and will free up the system to handle other tasks. This also follows the guidelines posted by the Scientific Working Groups on Digital Evidence and Imaging Technology from November 2004.

The increase in the quantity of images, variety of formats and the special requirements of law enforcement are creating a new market for software and hardware companies. The data management systems have been in law enforcement agencies for years, however Digital Image Management Systems (DIMS), or Digital Asset Management systems (DAMS) are new to law enforcement. A few companies are leading the way into the management of digital assets for law enforcement. Understanding and meeting the special needs of each law enforcement agency will require modification of the system. Some companies specialize in modifying their system to meet the needs of individual agencies. The chart below shows a comparison of

three of the more popular companies: Linear Systems, Veri-Pic, and Data Works.

	<u>Linear Systems DIMS</u>	<u>Veri-Pic</u>	<u>Data Works</u>
Cost (Entry Level)	495.00 Core Software \$16,000 entry Server	License Based \$5000.00 ea. user	\$14,000-\$275,000
Proprietary Format	Linear OS/Linux	Windows - SQL	Windows-SQL
Still Images	Yes	Yes	Yes
Video Support	Yes/fees vary	Yes/Add-On Module	Yes- 3 rd party app.
Audio Support	Yes/fees vary	Yes/Add-On Module	Yes- 3 rd party app.
Adobe PDF Support	Beta Testing	2007/summer	Yes- 3 rd party app.
Camera RAW Formats	Yes/Virtually All DNG-in beta	All Major Brands DNG-No	Yes- 3 rd party app. DNG- No
Download Stations/ #	Unlimited	Unlimited	Unlimited
Remote/Offsite backup systems	Yes / multiple options	Yes	Yes
Backup Type(s)	Tape/CD/DVD/Blu-Ray/UDO/Jukebox/	Tape/Optical/ RAIDs	Tape/Optical/ RAIDs
Software Update Costs	No	16 % based SMA	With SMA-14% of install cost
Onsite Service/ Fees	Yes /Fees vary	Yes	Free w/ SMA, or \$180 hr. plus expenses
Onsite Training	Yes / Fees vary	Yes/ \$2299 per day	3 days incl. w/ install
Online Training	Yes / Go to Meeting	Yes/ Web-X/ 10 people	Yes/Web-X, Multimedia
Chain of Custody to the indiv. file level?	Yes/File and Function	Yes/file and function	Yes/File and function
File renaming	Yes/8 digit numbering system	No Original Name	Yes/SQL guid#
Image Enhancement Capability	Yes / Forensic Pro	Yes	Yes/3 rd party app.
# of Users per Hr./Day	Unlimited	Unlimited	Unlimited
Image Authentication	Yes	Yes	Yes
Biometric Access control	Yes / No fee	Yes/Additional Fee	Not standard, but avail
Dynamic Network Monitoring	Monitors network bandwidth, makes adjustment	No	No
Real Time Adjustments	Yes	No	No
Workflow Manager	Yes	No	Yes
# of Active Installations	400+	Confidential	40

This chart is not a comprehensive list of the issues involved with storage of law enforcement data. For example, John Kwan from Veri-Pic states that, “Another very important feature that we have is a hardware clock. Our audit trails do not rely on the computer or the server's clock. We actually ship a trusted time source in hardware form with our system. This is a standout feature because often the computer's clock is improperly set. This also prevents tampering because the trusted time source can not be set to a time that isn't the real time.” Other companies also have specialized features they have included to satisfy the needs of their clients. Each law enforcement agency will require different features depending on their procedures, personal, and resources. First, an agency should have a digital imaging policy in place and then begin researching the features necessary to meet their agencies needs. In federal government agencies budgets have dramatic influence over the ability to manage resources, but resources are also available to assist very small agencies to very large departments. Finding a company that is willing to modify or customize their system to meet your department’s needs is critical to create a smooth work flow, save time, and maintain the legal requirements for digital evidence.

In summary, choosing a digital storage system is such an individualized decision it is difficult to blindly recommend one system over another, but because of this issue data management companies are becoming more adaptive and scalable to meet the needs of police agencies that are constantly updating and improving their systems. It is important certain questions be asked by the actual users within the police agency to determine which system’s strong points would benefit the agency the most. Such questions may be as broad as “Which system is easily adapted to what we already use?” or as restrictive as “What size image file is produced by our current camera equipment?” Most often the decision is made by weighing the benefits and drawbacks of a system, whether it is multiple hard drives, DVD backup, in house redundant servers or independent storage corporations; always keeping in mind the confines of the agency’s budget. The purchaser should remember to hold the digital storage system to the same high standards to which other types of evidence are held, since photographs are possibly the most important evidence investigators are armed with when walking into the courtroom.

Works Cited

Baker, M., Keeton, K., and Martin, S. Why Traditional Storage Systems Don't Help Us Save Stuff Forever. 1/22/07 from <http://www>.

Bockaert, Vincent. (1998-2007). Storing your Digital Images. 1/22/07 from <http://www.dpreview.com>

Cardinal, David. (2001). Digital Image Storage. 1/22/07 from <http://www.nikondigital.org>

Conway, Paul. (1990). "Archival Preservation in a Nationwide Context," *American Archivist*, 53, No. 2: 204-22.

Hardesty, G. (2007). (2007, January 9). Lasting Images. *The Orange County Register* Task Force on Archiving of Digital Information. (1995).

Hedstrom, Margaret. Digital Preservation: A Time Bomb for Digital Libraries. 1/22/07 from <http://www.uky.edu/~kiernan/DL/hedstrom.html>

Marks, Howard. (2006). Strategic Info Management: Long-Term Storage. 1/22/07 from <http://www.networkcomputing.com>

Kwan, John. Veri-Pic. Personal Interview. 23 Jan 2007.

Parsons, Chris. Linear Systems. Personal Interview. 24 Jan 2007.

"Preserving Digital Information," report of the Task Force on Archiving of Digital Information, commissioned by the Commission on Preservation and Access and The Research Libraries Group 1.0, August 24, 1995.