



# SANE and the Hydra Privacy Card® Digital Attaché

## Confidentiality and Legal Admissibility in a Sexual Assault Nurse Examiner Program

In cases of sexual assault or domestic violence, it is vitally important to satisfy two potentially conflicting goals. The patient's urgent medical needs must be attended to, but at the same time a physical examination must be conducted and evidence gathered for possible prosecution. To a woman who has already been violated, the collection of the most intimate photographs and physical evidence can cause her to feel violated again. It is important to respect the patient's privacy while at the same time ensuring that any evidence collected will withstand a legal challenge if the case is ever taken to court.

Because a sexual assault examination typically takes place within a healthcare facility, the strict confidentiality requirements of the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and HHS Breach Notification Rules must be satisfied. One of the best ways to ensure that Protected Health Information (PHI) is protected is through the use of encryption to limit access.

In recent years, the importance of this task has been widely recognized, and programs have been instituted to train selected nurses and other medical staff in forensic skills. Many hospitals throughout

the country are now creating Sexual Assault Nurse Examiner (SANE) units to deal with these issues.

SPYRUS, Inc., is a manufacturer of cryptographic products originally designed and marketed to the US military. Protecting the confidentiality and integrity of digital data is a SPYRUS core competency that fits nicely with evidence-handling requirements. This match led to a partnership with the SANE program at Holy Cross Hospital in Taos, New Mexico, which began in January, 2011.

This effort is the first-ever field trial of the SPYRUS Hydra Privacy Card® (Hydra PC™) Digital Attaché™ USB encryption and authentication device in a clinical setting. The Hydra PC Digital Attaché can act like an encrypting USB flash drive to provide both confidentiality and integrity, but it is also much more.

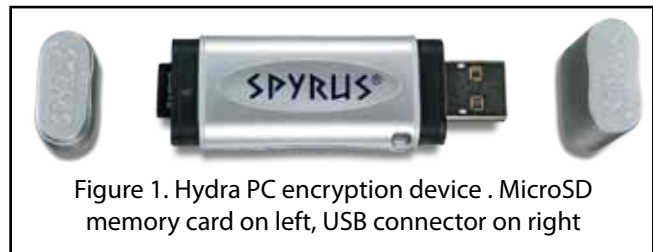


Figure 1. Hydra PC encryption device . MicroSD memory card on left, USB connector on right

*"The innovative SPYRUS solution ensures HIPAA compliance, provides outstanding protection for a victim's privacy, and guarantees an air-tight chain of custody to ensure the evidence is admissible in court once it is turned over to law enforcement. Holy Cross Hospital is pleased to partner with SPYRUS in the first clinical deployment of this very cost-effective technology."*

**Peter Hofstetter, CEO, Holy Cross Hospital, Taos, New Mexico**

The solution recommended by SPYRUS uses a camera that is connected, or "tethered," to a computer via a USB connection and a Digital Attaché. Photographic images are written directly to the Digital Attaché's encrypted partition so that no unencrypted copies of the image ever exist, except for those that have been explicitly decrypted.

While Digital Attaché can store data like any USB flash drive, it can also protect information stored anywhere, not only on the device itself. Just as a Microsoft Windows file can be emailed by right-clicking it, Digital Attaché protection can be invoked in a similar manner. The nurse examiner collects the photographic images into a folder, and then right-

clicks the folder to encrypt it. Once encrypted by Digital Attaché, the images can be transmitted and or stored anywhere without fear that unauthorized individuals, including IT administrators, can access them. Public key infrastructure (PKI) allows encrypted files to be shared with other authorized individuals, including law enforcement personnel, who have their own Digital Attaché devices.

Many nurse examiners report that they are using ordinary digital camera storage cards and then moving the images to a PC before burning them to CD. Even when using a packaged solution that encrypts the PC hard drive, this can expose the images to unauthorized access, because images are present in so many different locations. These systems may fail to satisfy the HITECH and HHS Breach Notification rules for protecting PHI, and to the best of our knowledge, none provides the kind of hardware-based integrity and nonrepudiation controls necessary to ensure that the information will stand up in court as evidence.

The SPYRUS solution offers enhanced confidentiality, integrity, and nonrepudiation while significantly limiting possible insider threats. Even better, the SPYRUS solutions cost approximately one-fourth as much as competing solutions to equip a six-person SANE unit, including a budget for photographic equipment.

Although SPYRUS does not sell photographic equipment, the author of this paper has done substantial research on it and includes an appendix discussing photographic equipment recommendations for this solution

### **Confidentiality, Integrity, and Nonrepudiation**

The most significant difference between competing solutions is the use of the Hydra PC Digital Attaché, which was designed for secure military storage.

According to the HHS Interim Breach Notification Rule, PHI must be preserved and protected for the life of the patient plus fifty years. Because a baby born today might live to be 110, any system designed to protect Personal Health Information must (securely) preserve the information for up to 160 years.

In the case of SANE programs, additional standards must be met concerning the admissibility of evidence under the Federal Rules of Evidence and any state or tribal rules.

Traditional chain-of-custody (lock box) controls are inadequate for preserving digital evidence, which must be backed up to ensure availability, and yet must be protected against unauthorized access, viewing, or possible manipulation by using Photoshop or similar programs.

Although such evidence can be written or “burned” to a CD, knowledgeable experts contend that burned CDs (as opposed to the pressed CDs sold for music distribution) have a relatively short life span of only two to five years, because of the breakdown of the layer of dye that is modified by heat during the recording process.

A better approach to preserving such information is the kind of long-term data storage routinely used to preserve digital data. The information is copied to enterprise-class storage, such as a RAID array, and backed up to one or more off-site facilities to protect against fire, flood, and other disasters.

However, off-site storage facilities may not be as secure as on-site facilities, and as a consequence, both the confidentiality and the integrity of the information could be compromised, which violates HIPAA requirements. In addition, information must be protected while it is being transferred from one site to another.

Another problem is proving that images were not altered between the time that they were collected and when they are presented in court.

### **Proving That Images Are Secure**

Because camera memory cards are still relatively expensive in the large sizes required to hold many high-resolution images, it is a common practice to continually erase, format, and reuse the compact flash memory cards. Unlike computer hard drives, memory cards and USB flash drives incorporate “wear-leveling” technology. After a certain number of write cycles, individual memory cells wear out, and older cells are swapped out for new, unused cells,

under the control of the on-board memory controller chip.

The problem is that when the old cells are swapped out, they are not erased, and the data is recoverable using forensic tools.

Some memory erasure applications destroy only the file directory, leaving the actual data (photographs in this case) fully recoverable by a sector-by-sector examination, as demonstrated by many commercial “photo-recovery” services. Disassembly of the device to access the memory cells directly is also possible.

A paper presented at the 2010 Silicon Valley Flash Memory conference reported that EVERY flash erasing tool that they examined (15 or more, including US Department of Defense and Russian tools) failed completely. In other words, a compact flash memory card can be a potential time bomb of latent images from previous examinations, unless the card is used only one time and then physically destroyed after the evidence has been turned over to law enforcement. This may be too expensive a proposition to be considered for routine use.

### ***Proving Who, What, and When***

At least one vendor claims that the vendor-proprietary RAW digital camera image format is impervious to modification. Unfortunately, this is not quite true.

The Canon RAW (CR2) format is well known within the industry. Adobe supports it in Photoshop and Lightroom, and Apple, Microsoft, and other vendors support it within various viewers and editors. The CR2 format is based on the TIFF file format, and since TIFF files can be produced as output from Photoshop, it is relatively straightforward to modify an image along with the relevant data verification information embedded in the CR2 file format.

Canon sells an Original Decision Data Verification Kit, which is widely used by news organizations, law enforcement, and even realtors to provide protection against image manipulation. Unfortunately, the notorious Russian hacker Dmitry Sklyarov of ElcomSoft, showed in a presentation entitled “Forging Canon Original Decision Data” presented in

Prague on November 29-30, 2010, that Canon image verification could be broken.

Although juries may not be experts in such matters, most jurors have heard of and may have used Photoshop or similar image editing programs, and they have probably seen the results of such manipulated images in magazines or elsewhere. A jury could perhaps be persuaded that something like that might have occurred—especially in a high-profile trial. It is certainly not beyond the realm of possibility, or a defense attorney’s imaginative argument, that the result of such manipulation could be converted back to the original RAW format.

Even if the camera RAW files were secure and impenetrable, that would not satisfy the second part of the requirement: nonrepudiation or, in other words, who created the photograph or other documentation, when, and under what circumstances. Without nonrepudiation, anyone could easily photograph a person other than the alleged victim of an assault and then substitute that image for the real one.

The camera RAW file would be completely genuine in that case, but the photograph itself would be a fake.

Digital Attaché can prevent the authenticity of evidence from being questioned when the case goes to trial. When files are encrypted, Digital Attaché performs several actions. The unencrypted files are “hashed” or signed using a government-approved algorithm, the data is encrypted, the time of encryption and Digital Attaché serial number are injected, and then the entire file is hashed again. SPYRUS calls this “sealing” the file, because sealed data cannot be altered in any way without detection. When data must be presented in court, the Digital Attaché that encrypted the images, when they were encrypted, and the fact that the images were not altered in any way can be mathematically proven.

Although this does not eliminate the need for a SANE examiner to provide multiple photographs to establish the scene, and if necessary testify in court as to how, when, and of whom the pictures were taken, Digital Attaché encrypt-and-seal technology provides an unbreakable chain of custody that does not depend on human control.

**SPYRUS Hydra PC Digital Attaché**

SPYRUS believes that the only proven way to ensure confidentiality, integrity, and nonrepudiation is to record the image directly onto an encrypted device such as the Hydra PC Digital Attaché, using a camera that is tethered directly to a standalone, dedicated PC. In this application, the camera’s memory card should be removed completely and the removal verified before the beginning of the examination.

Digital Attaché is a small USB device, similar to a conventional USB flash drive, that uses replaceable microSD memory cards. For the SANE application, the memory card is divided into one encrypted and one unencrypted partition.

The encrypted partition contains the original camera RAW images. Upon completion of the SANE exam, all images and other documents can be moved into a single folder or zipped file, using the case number as the name. The file or folder is then encrypted, and the encrypted files can be shared with other

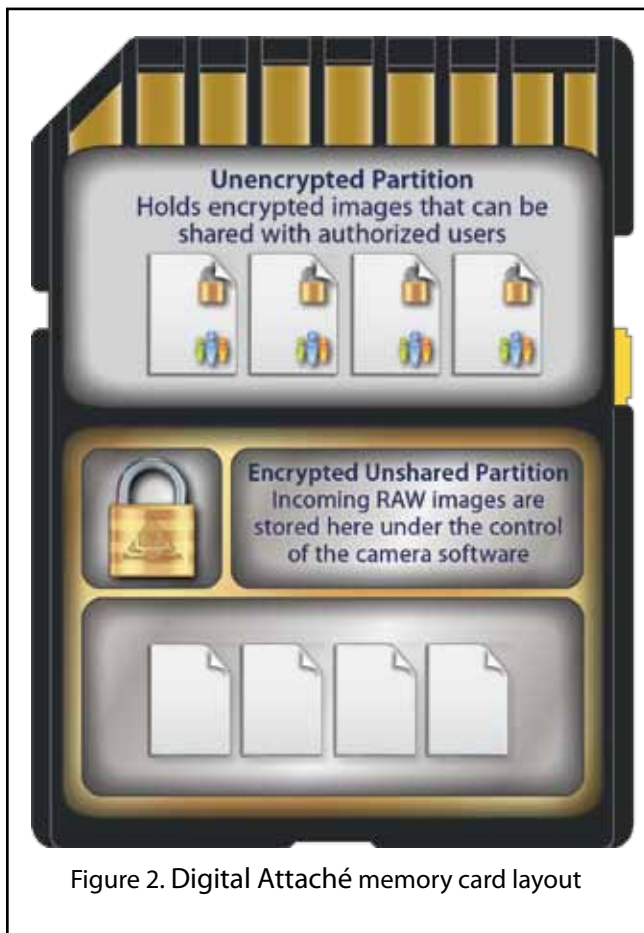


Figure 2. Digital Attaché memory card layout

authorized recipients or stored in the unencrypted partition.

The Digital Attaché is then connected to a networked PC, where the encrypted data is copied from the unencrypted partition to a secure location for backup. After the encrypted data has been protected from accidental deletion, the Digital Attaché is reconnected to the original, dedicated PC and the encrypted partition is securely erased. After this, only encrypted images exist.

Unlike competing solutions, Digital Attaché immediately protects the images as they are captured using XTS-AES 256-bit encryption implemented in a hardware security module. After all images are captured, they are encrypted and shared solely with authorized individuals, again

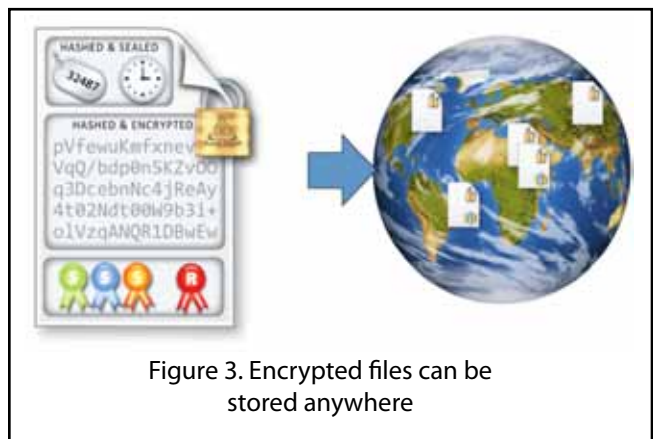


Figure 3. Encrypted files can be stored anywhere

using hardware-based encryption, to minimize the possibility of an unauthorized individual gaining access to the data.

**Securely Sharing Evidence**

Digital Attaché uses public key infrastructure to enable secure sharing of the images taken by a nurse examiner. The originator’s and authorized recipient’s identities are confirmed by a “sharing certificate” that is exported from each authorized individual’s device.

Because it is always possible that a Digital Attaché might be lost, stolen, or damaged, SPYRUS recommends that at least one Digital Attaché be designated as a Recovery Agent. The Recovery Agent Digital Attaché should be locked up in a

secure location, and the password stored in another location, preferably under two-person control.

The Digital Attaché can be set up by policy to automatically add the Recovery Agent’s sharing certificate as a designated recipient for all encrypted files as a safeguard against the loss of the encrypting Digital Attaché.

If the healthcare institution has already set up a PKI; for example, for encrypted email, and can issue X.509 certificates, those certificates can be incorporated into the sharing certificate. If no PKI is available, the user’s name by itself can be used when policy allows. In a small SANE unit, where everyone knows everyone else, this may be sufficient.

The originator’s sharing certificate is included in the digitally signed file, thereby providing technical nonrepudiation of the origin of the file. The device ID and a timestamp are also included, and a strong ECDSA signature is applied. Other relevant data can also be collected and processed similarly, including voice recordings, digital documents, and annotations.

If a sexual assault case goes to trial, the conventional practice is for the prosecuting attorney to show the nurse evidential photographs and ask under oath whether the nurse did in fact take those photographs and whether they are an accurate

representation of the victim’s condition at the time. The defense attorney will attempt to impeach the nurse’s testimony by questioning how many such examinations the nurse might have conducted during the intervening years or how the nurse could possibly remember every detail of every photograph. Effectively, the nurse is being expected to be able to prove that no manipulation of the photographs could possibly have taken place, even though the photographs were not in the nurse’s custody. Needless to say, this is not a very sustainable position.

In the Digital Attaché solution, it may be necessary for the SANE nurse to testify about who performed the examination, took the pictures, and gathered other evidence. But once the file is digitally signed and sealed, there can be no question as to its authenticity from that point forward. Any attempt to modify the encrypted file, even by as little as a single bit, would cause the decryption process to fail. This could easily be demonstrated in court. Any allegation by the defense that the photographs had been altered or enhanced can be easily refuted.

**Preventing Data Leakage**

Encrypted and sealed files can be transmitted or stored anywhere, even insecure facilities, with complete security.

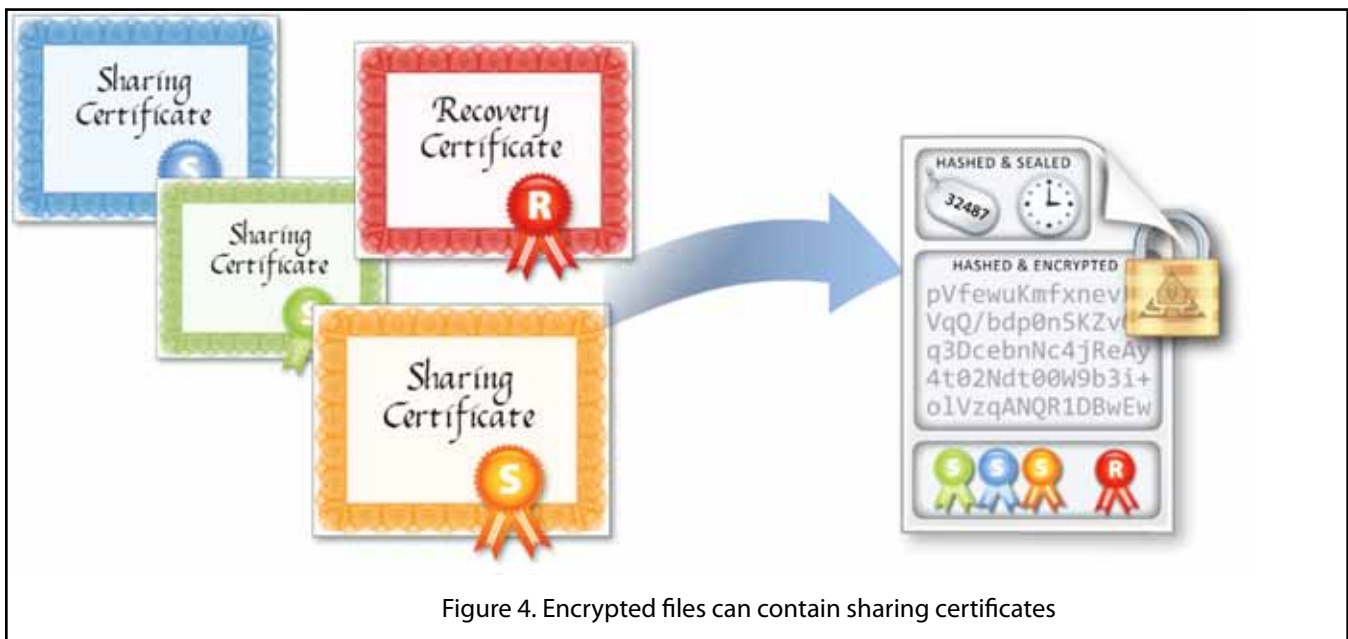


Figure 4. Encrypted files can contain sharing certificates

In some competing solutions, encrypted files are posted to a file server so that they can be downloaded by law enforcement. In such a system, anyone who knows or can guess the password required to access the file server could download those images at any time. Worse yet, someone on the inside could divulge the password, perhaps even to a tabloid or someone who would post the images on the Internet.

The SPYRUS solution completely prevents this possibility, because a unique feature of Hydra PC encrypting USB flash drives limits their use to one or more specifically authorized computers. Files on the Hydra PC cannot be accessed on unauthorized computers, even if you know the Hydra PC logon password.

Without going into technical detail, one or more secret values called an Enclave Authentication Value (EAV) is installed on one or more computers that are specifically authorized for SANE evidence collection. This value is encrypted and stored in the registry under system administrator control, so that only the system administrator has access to or knowledge of that value.

In nontechnical terms, this means that even if you have a device and know the password for that device, you cannot use it except on an authorized computer containing the EAV. If you take the device home, you cannot log on to the device or access any of the encrypted data.

The computer used to process the SANE images should be secured with a cable to prevent it from being borrowed or stolen by someone who could take it outside of a secure area and then decrypt protected evidence.

### **Medical Device Data Systems Implications**

The Food and Drug Administration has recently released a Final Rule dictating that manufacturers of medical device data systems that are manufactured and sold for the diagnosis and treatment of a disease condition, and which are used to collect, process, store, transmit, or display data from medical devices are required to register with the FDA. The FDA has assured SPYRUS that this registration

requirement does not apply to the SANE solution described in this paper. The equipment is designed to securely process sensitive information, and to do so accurately, but the data being collected and processed is forensic data and not medical data per se, even though it may be collected in a healthcare setting.

### **Summary and Conclusions**

There are two fundamental aspects to forensic digital evidence collection in a Sexual Assault Nurse Examiner program.

The first is photographic, which requires a camera capable of being tethered so that the photographic images are saved only onto an encrypted partition on the Digital Attaché microSD card. Part of the operational procedure should be to examine and document the fact that the camera's memory card has been removed prior to taking any photographs. The camera should be a semiprofessional version, preferably with interchangeable lenses capable of close-up or macro shots and equipped with a flash, preferably a ring flash for close-ups. Unless the camera is always hand held, a tripod or studio stand should be used to steady the camera.

The second aspect concerns the confidentiality required to comply with HIPAA, HITECH, and the HHS Breach Notification rules and the integrity and nonrepudiation controls required to comply with the Federal Rules of Evidence and various state and tribal laws and regulations. Confidentiality, integrity, and nonrepudiation are also required to meet the standard of "beyond reasonable doubt" imposed in a criminal trial.

To ensure confidentiality, the Hydra PC Digital Attaché uses the same file encryption technology found in the Hydra PC Personal Encryption Device, which is FIPS 140-2 Level 3 validated and used by the USA Federal government and by governments of other countries to protect highly sensitive information. Digital Attaché also provides a secure location for the original images with an encrypted partition that uses two AES-256 keys in the superior XTS-AES encryption mode. With this method, the image is always encrypted and never recorded

anywhere, not even on the camera's memory card, where it could be accessed by unauthorized individuals, including the IT staff and any backup facility personnel.

After the image is recorded on the Digital Attaché, the individual files or a complete folder can be encrypted and shared only with designated individuals. Each file is also sealed with a digital signature to detect any possible modification and to provide proof of origin (nonrepudiation).

The collection and encryption of the digital photographic evidence must be supplemented with encrypted documentation of important details of the examination, including the SANE examiner's notes and observations, regardless of whether it is a voice recording or computer document. Physical evidence such as DNA swabs must be annotated in the same manner.

According to respected experts, the combination of AES-256 and elliptic curve cryptography with P-384 keys is expected to be secure for at least 176 years. This more than satisfies the HHS Interim Rule, which requires that Protected Health Information be protected for the patient's lifetime plus 50 years.

*“Sexual assault and domestic violence are crimes that are devastating and dehumanizing, and require the utmost in discretion to preserve the victim's often fragile sense of privacy and self worth. But at the same time, if the incidence of such crimes is to be reduced, then it is important that they be prosecuted fairly, yet effectively.*

*SPYRUS salutes the efforts of Holy Cross Hospital and all of the other SANE units throughout the world in addressing these problems, and we are proud to be able to make a contribution to this effort.”*

**Sue Pontius, CEO, SPYRUS, Inc.**

The equally strong ECDSA digital signature technique provides mathematically provable integrity (protection against undetected modification) and nonrepudiation (strong assurance as to who created the encrypted document) that can stand up in any court of law.

Although some competitive approaches cost as much as \$25,000 per installation, the SPYRUS solution costs about one fourth of that to equip a six-nurse SANE unit, even with a generous budget for photographic equipment, while providing unparalleled confidentiality, integrity, and nonrepudiation protection. See the table on the next page for a recommended configuration.

The SPYRUS budget includes \$5,037 for photographic equipment, the most expensive component being a camera stand, and \$1393 for seven Digital Attachés purchased at retail (quantity one) from Amazon. For larger nursing staffs, all nurses, SANE administrative staffers, law enforcement officials, and prosecutors need their own Digital Attaché, for approximately \$199 per person.

These figures do not include shipping and handling costs or a host computer (most facilities already have at least one computer). Training and consultation costs are also excluded, as they depend on the location, the relative experience of the staff, and the extent to which detailed policies and procedures must be developed. The cost of Digital Attachés for law enforcement or other agencies will be additional.

ITEM	UNIT COST	TOTAL COST
Canon 60D	\$999	\$999
Canon 17-85mm IS USM lens	\$449	\$449
Canon 100mm macro USM lens	\$509	\$509
Hoya 58mm UV high-definition multi-coated UV filter	\$58	\$58
Hoya 67mm DMC PRO1 Digital multi-coated UV	\$52	\$52
Hoya 67mm multi-coated #58 green filter	\$39	\$39
Canon MR-14EX Ring Light	\$487	\$487
Canon Macrolite Adapter 67	\$35	\$35
Calumet 7' Monopro camera stand w. accessory tray	\$1500	\$1500
Manfrotto 400 tripod head	\$742	\$742
Wimberley C-12 Quick Release Clamp	\$79	\$79
Kirk Enterprises KBA-1 USB/AC Spacer Block	\$60	\$60
PocketWizard CM-N3 Remote release cord	\$63	\$63
Boss FS-5U Footswitch (unlatching)	\$25	\$25
Seven Hydra PC Digital Attachés	\$199	\$1393
<b>TOTAL</b>		<b>\$6490</b>

For further details regarding the SPYRUS Digital Attaché solution to the problem of maintaining proper confidentiality, integrity, and nonrepudiation controls over SANE digital evidence, please visit <http://www.spyrus.com/company/literature.asp> and look for these SPYRUS white papers:

- Hydra Privacy Card Digital Attaché
- Solving the Digital Chain of Custody Problem

## Appendix A: Photographic Quality and Ease of Use Issues

Because of the importance of photographic evidence in a SANE examination, this appendix outlines the photographic requirements and how to meet them with the minimum necessary equipment.

SPYRUS does not sell photographic equipment and has no vested interest in one kind or brand of equipment versus another. SPYRUS acknowledges that other camera systems on the market that might perform equally well as those discussed below. The information is provided purely to assist those who may be setting up a SANE unit for the first time and might appreciate some guidance regarding some of the more esoteric photographic details for this application.

There are many camera brands on the market that are suitable for use in a SANE unit, but because of technical issues involved in the use of a tethered camera and the author's extensive personal experience with the Canon line of digital cameras and lenses, this discussion concentrates on that series.

The Canon 30D used by the Holy Cross program was introduced in 2006 and has an 8-megapixel image capture system. Newer models have 15-megapixel and larger image capture systems. Although more megapixels are generally better, the difference is subtle unless you are making extremely large, poster-sized prints. Even eight megapixels is four times the resolution of a very high resolution high-definition TV, and that degree of resolution would certainly be considered adequate for presentation in court or elsewhere. Because new camera models come out at least every two years, future upgrades are always possible. For example, the new Canon 5D Mk II boasts 21-megapixel resolution, and there is no end in sight. In this case, "good enough is good enough."

For these reasons, this paper recommends the current model Canon 60D as representative of a reasonably priced yet very capable camera for SANE evidence collection.

### Lens Selection

The Canon 30D system that was donated to Holy Cross Hospital includes an EF-S 17-85mm 1:4-5.6 IS USM medium-view zoom lens of above-average quality. The Canon 60D normally comes with an 18-135mm zoom "kit" lens, which provides significantly better magnification, but several reviews have panned it as being unacceptably soft and having significant chromatic aberrations, especially when used wide open.

The 17-85mm zoom can focus to about 4 inches at the 85 mm setting with decent magnification, as shown in Figure 5 showing a nickel (approximately the same size as a woman's cervix), taken through a full-size speculum.

The 17-85mm lens can be used in combination with an EF 25 II extension tube to provide closer focusing and a larger image, but manual focusing is generally needed at that magnification, and the distance from the front of the lens to the subject is inconveniently short.

The Canon macro lens EF 100mm 1:2.8 L IS USM provides a substantially larger image of the nickel, but it requires an EF 12 II extension tube to focus from the outer edge of the speculum to the tip. However, it not obvious that this extreme degree of magnification is really required, as shown in Figure 6.

Without the extension tube, at maximum magnification (greater than 1:1 on the Canon 30D and similar cameras, including the 60D), the lens is 5 inches from the subject, or 4.5 inches from a ring light to the subject. Because the camera and lens is normally used on a camera stand or tripod, the 100mm macro lens IS (Internal Stabilization) L USM lens is not essential — the older 100mm Macro USM performs nearly as well, and is less expensive (\$509 versus \$839 new).

The reason why the image from the 100mm lens (Figure 7) is so much larger relative to the focal length compared to the 17-85mm lens is that the sensor on the Canon 30D (and others in the series



Figure 5. Canon 17-85mm at 85mm, through speculum



Figure 6. Canon 100mm macro 1:2.8 L IS USM plus EF 12 II extension tube, through speculum

of so-called APS-C size sensors) is not a full-frame sensor, but the 100mm lens is intended for full-frame cameras. The 100mm lens, when used on a 30D or similar camera, becomes the equivalent of a 160mm lens on a full-frame camera because of the 1.6 cropping factor, whereas the 17-85mm lens is an EF-S lens that is appropriately scaled for the smaller sensor in cameras that support the EF-S series of lenses.

The Canon Macro Lens EF 180mm 1:2.8 L USM is another alternative (Figure 8). Like the 100mm macro, the 180mm can record a 1:1 image on a full-frame camera and can more than fill the frame on a camera with an APS-C sized sensor, such as the 30D or 60D. Although considerably larger and heavier than the 100mm, with a 72mm filter size compared to 58mm on the 100mm macro, or the 67mm filter on the 100mm macro IS L lens (which may cause some vignetting when used with the Canon ring light with its 58mm opening, when focused

at infinity), the 180mm provides a much greater working distance from the subject—9.5 inches from the lens, or 8.75" from the ring light to the subject, even at the 1:1 minimum focusing distance. The lens is more expensive, at \$1279, and may be overkill for this application where there is usually no problem getting close enough to the subject.

An acceptable alternative to using a longer lens is to crop and digitally magnify the image produced by the 17-85mm lens.

As Figure 9 shows, the image quality holds up perfectly well, even at this magnification, and there is good depth of field. These images were taken from the JPEG shot in the camera—the CR2 RAW image (a digital image format that is proprietary to each camera vendor) would hold up even better.

Note, however, that this type of manipulation should NOT be done prior to encrypting and sealing the photograph, because it might compromise



Figure 7. Canon 100mm macro 1:2.8 L IS USM at maximum magnification, without extension tube



Figure 8. Canon Macro Lens EF 180mm 1:2.8 L USM, maximum magnification

the evidential aspect of the photograph. Instead, the original image should be captured, and any enlargement for the purpose of presentation should be performed at the time the images are to be presented in court, either by law enforcement, or by someone from the SANE unit who could testify as to the accuracy and provenance of the images.

Another low-cost option is the Canon 250D or 500D close-up lens, which attaches to the front of the main lens, although such attachments are generally considered inferior to a prime lens or a good zoom lens.

To summarize, SPYRUS suggests that the Canon 17-85mm EF-S zoom on one of the APS-C size semi-pro cameras such as the 60D provides excellent value and is sufficient for nearly all SANE photographic purposes. However, for very detailed macro photographs or to gain additional working distance for high magnification, the 100mm macro USM (non-IS version) is recommended as a secondary lens.

### Photographic Lighting

A ring flash setup is especially useful for close-up pictures. Ring flash setups are readily available online and elsewhere, and the Canon MR-14EX Ring Light (\$494) is highly recommended.

These units are routinely used by dentists and oral surgeons to photograph teeth, the inside of the mouth, cheek, tongue, and so on, and by dermatologists to photograph various skin lesions and diseases. Figures 5 through 9 were all taken with the MR-14EX.

The Canon Twin Light flash, MT-24EX, uses basically the same hardware as the ring light, but instead of surrounding the lens with a ring of light, the Twin Light provides two mini shoe-mount boxes that can be tilted and rotated in various configurations. The MT-24EX offers much more creative control of light, but at some increased risk of operator



flashlight that emits UV from a ring of LEDs, and costs only \$18 plus shipping. It may be useful in performing screening exams. However, just because a substance fluoresces doesn't necessarily mean that it is semen or even a body fluid—it could be nasal secretions, liquid soap, salad dressing, or a host of other substances that also fluoresce. For that reason, the services of a forensic laboratory may be required to determine exactly what the suspect stain is, but identification of stains that might not be apparent under normal light could be helpful.

Once a suspect area has been identified, various other tests, including Acid Phosphatase (AP), the



Figure 11. ProofPronto Forensic UV Flashlight reveals otherwise undetectable stains.



Figure 12. Stain revealed by ProofPronto Forensic UV Flashlight.

more specific Prostate Specific Antigen (PSA), and DNA tests may be used to narrow down the list of possibilities. These tests can get results even on semen stains up to 30 years old. Figures 11 and 12 illustrate the fluorescence that the Proof Pronto can reveal.

**Camera Stands and Tripod Heads**

Deciding which tripod or support stand to use is another issue. Colposcopes typically used for gynecological exams and surgical procedures are quite expensive, ranging from \$2,700 to well over \$14,000. Most come equipped with binocular microscopes, which may or may not have remote viewing or screen capture capabilities and may not be particularly useful for a SANE examination. Colposcopes invariably offer a stand-mounted apparatus that is sturdy, easily positioned, and stable. Some offer an articulated arm and an overhead suspension system, said to be suitable for an operating environment. Other options include a foot-controlled power zoom and power focus, which could be essential in a sterile operating environment.

Such features seem like overkill for a SANE unit, and SPYRUS instead recommends a sturdy studio camera stand, plus a good tripod head, at a substantially lower cost. A conventional tripod is more likely to cause a trip hazard, is less easily repositioned, and offers only limited vertical movement.

The Calumet 7-foot Monopro Camera Stand with accessory tray (#CC20075K1), shown in Figure 13, features a cast iron base with three swivel casters. It offers quick height adjustment, 360° panning, and a geared cross arm for lateral adjustment. If necessary, the stand and the interior counterweight cable can be cut down to fit through a lower doorway. The



Figure 13. Calumet 7-foot Monopro Camera Stand.

included 11" accessory tray (Figure 14) can be used to provide convenient access to a laptop computer or recording device. The cost is \$1500. Order from the manufacturer at <http://www.calumetphoto.com/1/1/18983-7-monopro-camera-stand-accessory-tray-calumet.html>.

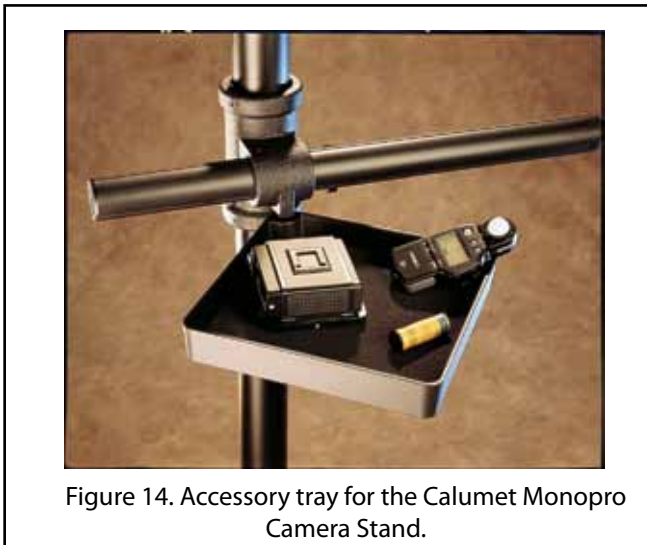


Figure 14. Accessory tray for the Calumet Monopro Camera Stand.

Many suitable tripod heads are also available for use with this stand (Figure 15). The Manfrotto 3263 (\$742) (now replaced by the apparently identical Manfrotto 400) is a sturdy, heavy, top-of-the-line geared tripod head with separate foldaway rotating handles for pan, tilt, and side-to-side leveling. It is ideal for the most precise composition and extreme close-up shots. In practical operation it might be a little slow compared to some other tripod heads, but it has the significant advantage of staying put once it is adjusted, with no sag or drift—an important consideration when the nurse may have to use both hands to adjust the speculum or spread the labia.

An alternative to the Manfrotto head is a fluid head of the type used for camcorders. The Manfrotto 128RC costs only \$90. The major drawback is that once the head is adjusted, another hand is required to tighten the vertical adjustment knob, and even then there may be some sag. As with the other heads, a clamp that can interface with an I-bracket, such as those made by Kirk Enterprises, Wimberley, Really Right Stuff, or Novoflex Arca-Swiss is needed.

A "joy-stick" head, such as the Manfrotto 322RC2 (\$140), is also worth considering. Although it permits relatively unconstrained tilt, pan, and elevation controls, this is all under the control of a single trigger grip, permitting one-hand operation so that the user can zoom with one hand, while controlling the orientation of the camera with the other, and then reach up and press the shutter release or use a foot controller. Although this head is convenient for one-hand operation, it requires a strong grip—otherwise, the camera and lens may flop forward. Again, an Arca-Swiss clamp is recommended to support an L-bracket.

Most ball-heads would not be optimal for the intended application. They tend to flop over and lose the horizontal and vertical orientation whenever a small adjustment is made.

After reviewing and handling these heads and several more that are not listed, the unanimous choice of five SANE nurses was for the Manfrotto 3263 or equivalent Manfrotto 400. Of course the camera could be hand-held, and this would be perfectly adequate for torso and facial shots, especially when equipped with a ring light flash, but for a gynecological exam this would require



Figure 15. Tripod heads.

holding the speculum with one hand and the camera with the other, at least if only one nurse is conducting the examination. Although auto-focus normally eliminates the need to focus manually (except perhaps at high magnifications), it might be necessary to adjust the zoom, requiring yet another hand.

The Manfrotto tripod head tilts back and forth, enough to level the picture right and left, but it does not tilt to a 90° angle. Instead, most professional photographers use an L-bracket in combination with an ARCA-Swiss compatible quick-release clamp from Wimberley, Really Right Stuff, or Kirk Enterprises so that the camera can be moved quickly from a horizontal to a vertical orientation.

A foot-operated controller can be improvised by connecting a PocketWizard CM-N3 Remote release cord (which has the Canon three-pin connector) to a momentary type foot switch, such as the Boss FS-5U (unlatching) (<http://www.zzounds.com/item--ROLFS5U>), if necessary through an adapter plug or with some cable splicing. It should be noted that most foot controllers use a simple on/off switch and do not have a middle position that allows focus and lighting tests or confirmation without taking a picture. Most foot controllers are of the latching type, which require the pedal to be pressed twice—once to take the picture and once to reset the switch.

Although the adapter cable that connects the foot pedal uses an offset connector, the USB cable connecting the camera to the computer uses a straight-on connector, which would interfere with using an L-bracket to mount the camera in a vertical orientation. Fortunately, the Kirk LBA-1 USB-AC Spacer Block screws onto the side of an L-bracket and allows the cables to be routed out of way of the quick-release clamp.

### Proper Exposure and Color Balance

The Canon ring light is normally used in Electronic Through The Lens (ETTL) mode, so that the right amount of light is delivered to the subject. However, if it appears that the subject is too light or too dark, a compensation can be entered on the flash head itself

by pressing the SEL/SET button and then pressing the + or – buttons.

Normally, when taking flash pictures, the Picture Mode dial on the upper left of the camera is set to Manual (M), with a shutter speed of 1/60 second and an aperture of around f/8. This avoids any possibility of room lighting causing a blur or trail after the flash has gone off. However, if a UV light is used or if an overhead examination light is preferred instead of a flash, the Aperture-Preferred (Av) setting is a better choice, using the camera stand for any long exposures.

The “normal” lighting condition for most cameras is specified in terms of a so-called Kelvin color temperature of 5500°K—the mean noon daylight color temperature at the old National Bureau of Standards in Washington, DC. However, although flash units fairly good in terms of matching that color temperature, most of them run around 6000°K to 6500°K, which causes the pictures to look overly blue. This problem can be corrected by either of the following methods:

- With the Canon 30D, press the <AF-WB> button, and then, looking at the top LCD screen, turn the multi-function wheel on the rear of the camera and select the flash (lightning bolt) icon. This sets the white balance to 6000°K.
- A more accurate way is to photograph an 18% gray card. Set the focusing switch on the lens to MF (Manual Focus) and take a picture of the gray card (or a white piece of paper if a gray card isn't available). Then press the Menu button and use the multi-function wheel to select [Custom WB]. Press the > button, turn the multi-function wheel to select the previous image, and press Set. The image's white balance is imported and the menu reappears. Exit that menu, press the <AF-WB> button, and this time select the Custom icon (two little triangles with a dot above them).

Regardless of which method is chosen, it is a good practice to always take a reference color picture before each examination, preferably holding a color chart against the victim's clothing and skin.

The universal standard in this case is the x-rite ColorChecker® 24 Patch target (Figure 16). It is important that the difference in brightness between the white and nearly white squares on the chart

be distinguishable. It should also be possible to differentiate between the black borders used between patches and the dark black patch.

SPYRUS, Inc. does not endorse any of the photographic products and accessories recommended in this paper. Always try before buying.



Figure 16. x-rite ColorChecker® 24 Patch target.

## Appendix B: Tips and Tricks to Implement a Secure Evidence-Gathering Environment

Consider the following procedures when using Digital Attaché for SANE applications:

Include a case number or similar reference in the filename, but never display the victim's or alleged assailant's name for privacy reasons. Canon Utility software allows the user to specify file naming conventions, and a convention such as prefix + shooting date + file number can uniquely identify each photo as it is captured. For example, a photo from the Holy Cross Hospital SANE unit in Taos, New Mexico, might have the filename HCH\_SANE\_Taos\_20101129\_0022.cr2.

The correlation between the case number and other relevant information such as the victim's name; the SANE examiner's name, credentials, and affiliation; evidence label numbers for relevant physical evidence; and so on should be recorded separately, as a text, MS Word, or PDF document, and then encrypted in the same manner as the photographs.

Original images and other documents relevant to a single case can be placed in the same folder or zipped into a single file before being encrypted and sealed. As an added precaution, change the operating system permission of the encrypted and sealed file to read-only, so that it cannot be deleted by accident.

After the file is encrypted, delete and overwrite the original images on the encrypted partition to prevent possible confusion with a subsequent case, even if no one other than the authorized user of that Digital Attaché can access them. The freeware program Eraser works well for this purpose, and it can be configured to use a single pass of random data to overwrite the image. If an attempt is made to access the images, even using national laboratory tools, only the encrypted data could be recovered, which is useless without the encryption keys.

To protect against fire, flood, accidental or even deliberate destruction or deletion, and virus or malware attacks, hand carry the Digital Attaché

containing the encrypted and sealed files to another computer that is connected to the network, read the encrypted files read from the unencrypted partition, and then back the encrypted files up to multiple off-site locations. If the networked computer does not have the proper Enclave Authentication Value (EAV) installed on it, no one can access the encrypted data on that computer, either to read it or to alter it.

To validate the integrity and completeness of the backups, create a manifest of backed-up files at the local repository using the Digital Attaché sealing keys, create another manifest at the backup facility, and then compare the two manifests to ensure that they are identical. This process also rehashes the files and compares them to the digital signature associated with each file, ensuring that no undetected modifications have occurred. This process synchronizes the backup database and facilitates the continuing availability of the data. Using this process, there is absolutely no chance that anyone inside or outside the facility can decrypt the data, even if they have access to the encrypted files, so long as they do not have both a designated recipient's Digital Attaché and its logon password.

Digital Attaché's secure file sharing relieves anyone who copies or prints from having to testify as to exactly how the images were conveyed to law enforcement or the prosecuting attorney. If a SANE unit is processing multiple incidents per month and a case takes a year or more to go to trial, it would strain credibility to claim that a person could remember all of the pertinent details of every photograph taken or all of the circumstances of the incident and the original scene well enough to testify truthfully that a photograph was in fact an accurate depiction of what occurred. A digitally signed document, whose provenance cannot be challenged, provides a much stronger case.

By equipping local law enforcement and district attorneys with at least one Digital Attaché per office, encrypted images could be transmitted to them

electronically. This ensures that no paper documents can be mishandled and compromise the victim's privacy and also ensure the admissibility of the evidence in court. Law enforcement or the district attorney can apply post-processing techniques such as negative inversion, enhanced contrast to highlight particular features without contaminating the original evidence.

If a network-connected computer used to process evidence can also contact the file server where the information is stored, that computer is at risk of compromise. If the server is ever corrupted with a virus, as happens all too frequently, the virus could also infect the SANE computer. Some viruses inject software that can record key strokes, exposing encryption passwords and providing access the original unencrypted images.

Digital Attaché allows the data collection computer to be fully functional in an offline environment. Because the only input to that computer is from a camera and the only output is to a Digital Attaché, there is virtually no possibility that a virus could ever be spread to that computer.

For extra protection, Digital Attaché can block all read and write access to USB flash drives and portable hard drives connected to the computer, preventing data from being removed from the computer and blocking all access to data stored on those drives.

After the various images pertaining to a particular case have been encrypted and sealed, the Digital Attaché should be removed from the SANE computer and moved to another computer which is connected to the network but which does not have an EAV installed, to prevent unauthorized users from logging on to the Digital Attaché or encrypting or decrypting any files. Because the partition containing the encrypted and sealed files is itself unencrypted (only the individual files are encrypted), it encrypted files on the network computer can be copied securely to various backup sites for safe keeping and ultimately transmitted electronically to law enforcement or district attorney's offices, assuming that those offices are authorized file-sharing recipients of the encrypted files.

When the encrypted and shared files are securely and properly backed up, the Digital Attaché should be returned to the SANE evidence computer, where Eraser is used to erase all of the contents of the encrypted partition.

# Appendix C: Computer System Requirements

Most desktop or laptop computers running Microsoft Windows XP or later can host the Hydra PC Digital Attaché and Canon software. The only requirement is at least two available USB ports, preferably USB 2.0 (one for the interface to the camera, and one for the Digital Attaché).

SPYRUS recommends Microsoft Windows 7 Enterprise or Ultimate editions, or Windows Vista Enterprise or Ultimate. Both Windows 7 and Vista support Microsoft BitLocker software disk encryption, which provides added protection against accidental file “spillage” to a swap file if the computer is lost, stolen, or accessed surreptitiously.

Windows XP systems can use the freeware TrueCrypt disk encryption package instead of BitLocker.

The Canon EOS Digital Solution Disk software, including the EOS Utility 2.8, can control the 30D and all later cameras.

## About The Author

### ROBERT R. JUENEMAN, CHIEF SCIENTIST, SPYRUS, INC.

Member, ABA Science and Technology Section, Information Security Committee

Member, ABA Health Law Section, eHealth Committee

Member, American Telemedicine Association

Associate Member, International Association of Forensic Nurses

### DISCLAIMER

This document is provided for informational purposes only and is subject to change without notice. SPYRUS, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Nothing in this document should be construed as providing legal advice or advice as to compliance with applicable laws or regulations.



For more information about SPYRUS products, visit [www.spyrus.com](http://www.spyrus.com) or contact us by email or phone.

#### Corporate Headquarters

1860 Hartog Drive  
San Jose, CA 95131-2203  
+1 (408) 392-9131 phone  
+1 (408) 392-0319 fax  
info@spyrus.com

#### East Coast Office

+1 (732) 329-6006 phone  
+1 (732) 329-6211 fax

#### Australia Office

Level 7, 333 Adelaide Street  
Brisbane QLD 4000, Australia  
+61 7 3220-1133 phone  
+61 7 3220-2233 fax  
[www.spyrus.com.au](http://www.spyrus.com.au)  
info@spyrus.com.au



© Copyright 2011 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, Hydra PC, Hydra PC Digital Attaché, Hydra PC Secure Pocket Drive, Rosetta, LYNKS, En-Sign, and SPYCOS are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries. All other trademarks are the property of their respective owners. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications:  
U.S. Pat. Nos. 7,380,140; 6,088,802; 6,003,135; 6,981,149;  
U.S. Pat. Appl. Ser. Nos. 12/018,094; 12/126,759.