Appendix G

Preservation of Digital Crime Scene Related Photographs and Checklist for Processing Computer Forensic Data and Evidence

Introduction

Photographs are one of the most important clues in crime investigation. When it comes to investigation of an incident location, the objective of the digital camera and digital photography used is to capture evidence in a manner that would be admissible in court. Crime scene photography is not a new field; it has been around almost as long as the camera itself. In the modern world, almost all photography is done digitally and that presents a few challenges from evidence perspective. Forensic photography is also known as "forensic imaging" or "crime scene photography." It is the art of making an accurate replica of a crime scene with use of photography for the benefit of a court or to help an investigation. It is part of the process of evidence collecting (more about it is discussed in Chapter 7). Forensic photography makes photos of victims, places and items involved in the crime available to investigators.

Forensic data and evidence need to be handled with great care given the requirements of "evidential integrity" when the evidence is presented in the court. When digital imaging is viewed in law enforcement perspective, there is a major concern and that comes from the admissibility of digital photographic evidence in court. It is known that digital photographs are more amenable for alteration than the traditional film-based photographs. There are people who believe digital photographs are not admissible in court.

This appendix serves as extended material for Chapters 7 and 8. In particular, it is to be used with reference to the "chain of evidence" concept explained in Chapter 7 (Box 7.12). Recall the discussion in Section 7.8, Chapter 7, about "chain of custody" concept and the discussion about evidential integrity, that is, forensic integrity of data need to be preserved as mentioned in Boxes 7.2 and 7.3 in Chapter 7. While using this appendix, do visit Chapters 7 and 9 and keep in mind Figs. 7.3, 7.6, 7.7 and 7.9. A number of SEDONA Conference items are provided in Refs. #2, #4–8, Additional Useful Web References, Further Reading. These references will be useful for cyberforensic investigation professionals as additional guidance. From the perspective of "evidence" do refer to Appendix Q. Legal professionals and law students can refer to Ref. #3, Additional Useful Web References, Further Reading.

This appendix is presented in two parts:

Part I: Guidance on digital crime scene photographs preservation.
Part II: Checklist for processing computer forensic data and evidence.

While reading Part I, it will be useful to refer to Figs. 8.13, 8.14 and 8.15 in Chapter 8. You may also like to revisit the discussion in Section 8.3.7 in Chapter 8. Information presented in this appendix is based on the opinions of the authors' research and study in forensic field. Authors believe that the information presented is accurate at the time of preparing this appendix; however, authors disclaim any responsibility or liability for any information contained herein. In Part I, first a few challenges are explained with regard to digital images as the evidence and then a procedure is recommended. It is to be noted that although most digital evidence comes from the Electronically Stored Information (ESI) inside a computer system, digital photograph as crime scene evidence should not be ignored – that is why this appendix is important.

Part I: Guidance on Digital Crime Scene Photographs Preservation

The Law Enforcement Community engages into extensive discussion regarding "evidence admissibility" issues concerning photographs captured with digital cameras – refer to discussion in Section 8.3.7, Chapter 8. Essentially, such discussions focus on some primary issues:

1. No film negative to testify the original photograph.
2. The potential for alteration of photographic evidence.
3. The lack of clear case law clarifying admissibility.
4. The quality of the photographic image.
5. Storage, retrieval and management of crime scene photographs – you can refer to the SEDONA guidelines provided in Refs. #4 and #5, Additional Useful Web References, Further Reading.

The purpose of this part is to discuss these issues to help Law Enforcement Officers about the usability of digital cameras within their jurisdictions. Note, however, that it is in the best interest of a concerned forensic investigation case to refer to experts having significant experience with digital technology. Readers are strongly advised to discuss the issues mentioned above with the appropriate legal professionals and law enforcement agencies in their jurisdiction. The legal professionals/law enforcements need to be comfortable with this technology and be prepared to handle any potential challenges. With regard to this we draw readers' attention to Ref. #3, Additional Useful Web References, Further Reading.

The Issue of "No Film Negative"

Digital cameras come with different types of sensors: charge-coupled device (CCD) is one of the sensors (refer to Ref. #9, Additional Useful Web References, Further Reading). CCD-based digital cameras use CCD sensor to "capture" the photograph electronically. A digital camera that uses CCD sensor creates a digital file of this image and that image is recorded onto the storage media. An image can be printed when this image file is read into the computer. Owing to this, there is no film that exists with the "original" image of the photograph. The real issue, however, is not the film but about the possibility of that the photograph that is presented as evidence can be altered being digital in nature.

It has been possible for crime scene technicians, forensic specialists and attorneys to show a judge, jury and defense attorney a film negative (or "Polaroid") that is obtained at the scene and processed chemically. Conventionally, courts considered that such evidence, along with simultaneous investigation notes, is admissible. This is because they believe that a film coming out of a camera can be treated as solid evidence. After all, the court can understand technology of camera and has confidence that evidence is not altered. A film that can be held in your hand cannot be doubted; however, it seems that this is far from true!

The "Alterability" Issue

It is known that one can alter film-based photographs. There are professional's services available to retouch photographs – they can do just about anything to a piece of film. Using relatively inexpensive scanners and film recorders, it is possible to scan the negatives into a computer and get them manipulated, that is, altered. Once scanning is done, negatives can be recorded onto 35 mm film. Thus, a "new" manipulated a.k.a. altered piece of film can be shown to the jury. Although such a crafty work is detectable by forensic professionals, it is certainly not detectable to the eyes of average defense attorney, judge or jury!

Besides the issue mentioned above, a film is not always "secure," especially when the print development work is outsourced to any local agency. For example, before even a confidential film is presented at the court, there could be others at the development shop who could have looked at it! On the other hand, although "digital" cameras are "filmless," they offer features that can actually help the investigator to keep the evidence secure provided proper procedures are followed.

Expectation for Case Laws for Digital Images

"Case law" is the collection of available case rulings to explain the verdicts in a case. Most often than not, case law is formed by judges based on their rulings when they make their decisions along with the

reasoning behind them. Case law also comes forth when statutes and precedents in other cases are citied – judges do this when there is a bearing on their decision. A single case may generate almost no written interpretations or opinions. These collective viewpoints/interpretations/opinions can be referred to in the future by other judges when they make their rulings on similar cases, allowing the law to remain relatively consistent.

Thus, a "case law" is the reported decision of selected appellate and other courts (also known as "courts of first impression"). The purpose of case laws is to make new interpretations of the law and, therefore, case laws can be cited as "precedents" in a process known as "stare decisis." The interpretations (from case laws) are differentiated from "Statutory Laws" which are the "Statutes and Codes" as per enactment of legislative bodies. When it comes to "crime scene photography," clear case laws may not be available to directly address them. However, the courts, in general, have held that photographic, video and audio evidence as admissible, provided documentary or testimonial supporting evidence is available to support it. The fact that no direct case law is in existence does not necessarily work as a negative because worldwide there are millions of digital cameras in use, and it appears that there have been no serious challenges.

Concerns for Picture Quality

Digital technology is changing rapidly – until recent years, digital cameras were not capable of producing picture that would compare in quality with film. Even with the lateset digital cameras, 35 mm film still captures a photograph with more "image information." This, therefore, raises the question: "Can digital cameras capture a picture of adequate quality to document the crime scene?" and the answer is absolutely yes!

First and foremost, sound methods must be used for crime scene documentation. Some of the good methods involve photographing the overall crime scene, perhaps from several locations. As with any camera, the photographer should then be gradually taking closer photographs of items of interest, with the last photos being macros or close-ups of detailed evidence. By adhering to the standard crime scene analysis techniques, digital cameras will produce 8×10 photographs that are almost indistinguishable from film-based prints. Second critical factor is the choice of a digital camera (refer to Ref. #13, Additional Useful Web References, Further Reading). Also read white paper titled *Considerations on Digital Cameras for Crime Scene Investigations* quoted in Ref. #14, Additional Useful Web References, Further Reading.

Third, it should be noted that digital printers greatly influence the overall picture quality. Photographs reside inside the computer and many types of printers can be used. For example, if Windows is the environment where the PC operates, almost any printer can be used to prepare the printed photograph – either monochrome or laser printers. For getting the true "photo" quality prints, many vendors recommend "Dye Sublimation" printers or true silver halide printers, however, they are higher priced. These printers can produce photographic quality clear enough for presenting in the court.

Last but not the least, the digital world offers to crime scene technician certain tools for use in the processing of the photograph. Some of these tools are comparable to chemical adjustments that can be used on film to lighten or darken the image. However, standard PC tools such as Adobe Photoshop offer several enhancement features. To summarize, using a proper combination of the right type of digital camera and right printer, one will be able to produce 8×10 photographs that are most acceptable as evidence in the court.

Best Practices for Preservation of Photographs as Digital Evidence

Assuming that the investigator has selected a PC computer, digital camera and printer, let us understand how these components work together to ensure admissibility of the photographs.

First, it is important to note that the camera itself cannot alter a captured image once it is stored inside the PCMCIA card. Thus, the image stored on the PC card by definition is in an "original state."

Today there are cameras available to print images directly to their companion printer. If an investigator is using such camera/printer, after going to the crime scene laboratory, he/she should print the photos immediately and should label them as "original camera prints," along with the date, time and technician's initials. Later on, during the testimony it can be demonstrated that these photographs were directly printed, prior to any viewing on a computer system. In case the investigator's equipment does not have the facility for direct printing, then the original file should be maintained in an ineffaceable format. Recordable CDs are one of the approaches for this.

A file recorded on CD cannot be "re-recorded"; it means when a file is stored on CD it is indelible, that is, cannot be wiped out. Furthermore, as part of file format the date and time stamp will get automatically created inside the PC. However, there is still the risk that the file could be read into a PC and enhanced/altered. The enhanced/altered photograph can be recorded back onto the same (or different) CD. When the photograph is recorded on the same CD, it must have a new filename because the original file name is indelible. Moreover, the file would carry a new date and timestamp. Following are suggested guidelines for secure processing of digital photographs:

1. Choose a digital camera that has the capability of producing the output directly through a photo quality printer. Print and label original photos upon return to the crime scene laboratory. Have a form that testifies to this transaction.
2. Use a PC to record the digital files directly to a CD before viewing any image on the PC screen. Have a form that verifies this transaction.
3. Use evidence forms that record the minimum of the following information:
   - Case report number, date and time of recording.
   - Number of photographs.
   - ID number of the CD-ROM.
   - Name and signature of photo technician.
   - Legend such as or similar to "*This is to certify that the digital photographs stored on CD Number <xxxx> were captured directly from the digital camera card prior to viewing on a computer system. The technician (whose name appears on this form) certifies that such digital photographs are the same as the digital photographs taken at the crime scene*."
4. The digital files on the CD can then be viewed safely, can be enhanced, annotated and entered into a database of crime scene. If the digital file is recorded from the PC card directly onto a non-erasable CD-ROM, then the original photographic file is always obtainable. Although it is true that the photograph can be read into the PC and can later be tampered with, it is not possible to record it back on to the CD with the same file name. It must carry a new file name and matching date and timestamp from the computer.

In case the court challenges the photograph, the technicians can testify and produce the supporting paperwork, along with the computer-generated date and timestamps. This should demonstrate to the court a strong audit trail. It is recommended that the above-stated basic procedures be followed with digital photographic files. These standard operating procedures (SOPs), available from the authority, should be rigorously followed – recall the SOPs mentioned in Appendix F. The checklist presented in Table F.2 in Appendix F is relevant for what is mentioned here. A key aspect of this discussion is, however, the "credibility/competence" of the technician (refer to Table F.4 in Appendix F). There is no doubt that the strongest factor in admissibility is direct testimony harping on the "true and accurate" nature of the photographs in question when it comes to presentation of evidence in the court. Another related issue is about considerations for photographs that require special lighting and night-time exposures – it is briefly explained below.

There may be several crime scenes that call for photography at night. If traditional film cameras and a "bulb" (open lens) are used on such occasions, then appropriate setting can be selected for timed exposures. On most digital cameras, however, such a setting is not available – the longest exposures being in the half-second range. Many digital cameras have an effective ISO rating of 800 while some cameras have ISO 3200 rating. Even when these faster speeds are used, conventional "paint with light" techniques are not possible with digital cameras. It is recommended, therefore, that the most powerful external flash units be used for long night-time shots. There is another alternative and that involves having a couple of subordinate flash units placed at the crime scene. When the main flash is fired, the subordinates will also flash, thereby illuminating multiple points at the crime scene location.

Occasionally, there are situations where special lighting, that is ultraviolet (UV), needs to be used. In such situations, it is crucial to fully test the camera before using it. There are cameras that will shoot UV; also there are some special cameras that claim they are capable of infrared shooting. Also available are digital cameras with special lens coatings for effectively blocking UV and infrared – they are not usable in these situations. It is emphasized that the camera to be used should be thoroughly tested before the actual use at the crime scene. Next, we explain the advantages of digital photography from crime scene investigator's perspective.

Digital Photography Presents Advantages to the Crime Scene Investigator

Following are some of the advantages of digital photography:

1. **Cost reduction:** A simple analysis of the direct amounts of money currently spent for film-based photographs. You can sum up the costs involved for polaroids, 35 mm film, developing and prints for court. In most jurisdictions, the investments in digital technology, including the PC, digital camera, printer, software and training, need financial support.
2. **Secure chain of evidence:** All photographs will be maintained and printed by authorized law enforcement staff. Recall the "chain of evidence" concept explained in Box 7.12 and "chain of custody" concept explained in Section 7.8 in Chapter 7.
3. **Time/date stamping of digital files:** Investigator will be able to produce an audit trail that is not available with the conventional films.
4. **Indelibility of CD:** Opportunity to work with solid evidence, that is, secure, unalterable/inerasable digital files.
5. **Image processing for clarity and annotation:** Images can be brightened, darkened, sharpened and otherwise processed for clarity of detail. Refer to Figs. 8.13, 8.14 and 8.15 in Chapter 8.
6. **Accessibility:** Photographs can be sited on a secure computer network and made available to investigators, digital media analysts, medical examiner, Defense Attorneys or other appropriate parties.
7. **Review of photos at crime scene:** Most modern digital cameras make it possible for the investigator to review photographs on a display prior to leaving the crime scene. This gives an assurance to the investigator that all photographs are well exposed and that they contain the most wanted details. There are lesser possibilities for lost, spoilt or poorly exposed photographs.

Guidelines to Ensure Admissibility of Digital Photographs as Evidence

Recall the SOPs mentioned in Appendix F. Develop an SOP, Department Policy or General Order on the use of digital imaging. The SOP should include when digital imaging, chain of custody, image security, image enhancement, and release and availability of digital images are used. The SOP should not apply only to digital cameras, but should also include film-based and video applications as well.

1. Preserving the original digital image is important. This can be done in a number of ways including saving the image file to a hard drive or recording the image file to a CD. Some agencies prefer to use image security software.
2. It is best to preserve digital images in their original file formats. The saving of a file in some other file formats results in loss during image compression. If such compression is used, one may lose critical image information as a result of the compression process.
3. Providing "need-to-know" basis access is important when images are stored on a computer workstation or server, and several individuals get access to those image files. One good way is to make the files read-only for all, except for your evidence or photo laboratory staff. As an advantage, consider this – investigators could view any image files but they would not have rights to delete or overwrite those files.
4. When an image is to be analyzed or when it is enhanced, new image files get created – these should be saved with new file names. In no circumstances, the original file should be replaced (overwritten) with a new file.

Part I: Summary and Recommendations

For crime scene documentation, digital technology has become a strong option to film-based photography. Good SOPs in place assure proper evidence handling.

It is important to design a system and to incorporate the features that are important for photograph preservation. The challenge is to ensure that there is an integrated system with proper procedures. Even though forensic investigation agencies may have capable staff, it is advisable to use commercial systems

integration companies along with law enforcement background for assistance in developing integrated forensic solutions.

Part II: Checklist for Processing Computer Forensic Data and Evidence

Finally, we present the checklist for processing computer forensic data and evidence. The checklist presented in Table G.1 is a due diligence/best practice checklist; it can be considered in alliance with "Evidence Control Checklist" presented in Table F.2 of Appendix F. The purpose of this checklist is to provide a basic guideline to computer forensic technicians working with laboratory units so that a uniform working style can be adopted while working on a forensic case either with an investigator from their own agency or per request from another agency. This section serves as a recommended guide and not an instruction.

Table G.1 Checklist for processing computer forensic data and evidence

Aspect to be Considered	***Remarks***
Basics	
1. Track the person-hours expended into media analysis and administrative work.	
2. Verify search authority, consent, warrant and subpoena/warrant for exact legal level of analysis. Determine the level of analysis and the files to examine (i.e., does the warrant address E-Mail, unopened E-Mail, etc.). Get a copy of this document and put it in your analysis case file.	
3. Place master of the case documentation file in the analysis case file.	
4. Prepare a modified boot disk for the forensic software. Make sure it is of the current version existing on the forensic machine.	Refer to list of forensic software tools in Appendix I.
Best Method Determination	
Establish the best method to process any computer-related evidence. If the laboratory unit forensic examiner cannot process the evidence in custody due to lack of experience, paucity of training, or non-availability of equipment, the officer submitting the evidence or the forensic examiner will fill in a "request for assistance" form and will submit the evidence to the forensic laboratory.	

Case File Preparation	
1. Fill out all the necessary details of the case and place all preliminary case documentation in this file. **2.** This will help you to keep track of vital details from the start of the forensic examination. **3.** Before opening a case file, make sure you have a search warrant or an approval to search. **4.** Ask the submitting officer to fill out the "Official Request for Laboratory Examination." **5.** The purpose of this form is for the officer to indicate the keywords that will be used to search the computer during forensic investigation.	
Worksheet for Media Analysis	
1. The purpose of "Media Analysis Worksheet" is to track the flow and process of media analysis support. **2.** Use this worksheet to record important information on the support provided. **3.** The sheet can also be used to track information that needs to go in the periodic report sent to all concerned agencies connected with the case or reports to internal units supported forensically for the assistance provided by the forensic laboratory.	
Preparation of Report (for Attaching to the "Media Analysis Worksheet")	
Throughout your work on the forensic case, maintain notes and provide as much information as you can – such as the aspects mentioned below: **1.** Date and time of CPU evidence. **2.** Current date and time (along with applicable time zone). **3.** Significant problems/broken items. **4.** Limitations in forensic analysis. **5.** Forensic findings/evidence obtained – this belongs to your final report in more detail; these are "working notes" (mentioned previously) so that anyone (i.e., a forensic colleague, an investigating officer or a manager/supervisor) can refer to the file and can find out exactly where you left off in your evaluation of the captured computer and media. **6.** Special techniques required or used over and above standard processes (e.g., password cracker, etc.). **7.** External sources used (e.g., commercial organizations/agencies that provided assistance, information provided by other trained crime investigation officers, etc.).	

Visual Inspection and Inventory (Evidence Shut Out)	
1. Shut out all computer media and machines captured for analysis.	
Media comes in so many different varieties. Make sure that all the media are labeled sequentially (e.g., N1–N3, etc.). Also ensure that same labeling system is used as you acquire this evidence into imaging tools – refer to Appendix I for list of forensic software and equipment.	To see different types of media, refer to Figs. 7.2, 7.6 and 7.7 in Chapter 7 as well as Figs. 3.1 and 3.12 in Chapter 3.
Note: As soon as you receive evidence, make sure that the evidence is tagged correctly to reflect the items taken in custody. Note any damage that may have gone undocumented on the evidence tag, take pictures of the damage and prepare a supplemental report to document what you found.	Revisit/recall Section 8.7.6.
2. Additionally, also carry out a visual inspection of the physical makeup of the seized computer and maintain inventory. It is crucial that you systematically document the computer condition.	Refer to Chapter 1 (Section 1.5.13) and Chapter 6 (section 6.2.2) about COPPA and Child Pornography.
3. Open/remove the CPU case to examine its internal circuitry, make a note of all media (hard drives, removable media drives, floppy drives, etc.).	
4. If appropriate, note down all internal expansion cards (e.g., where unusual cards are located, where the interior devices that could be pertinent to the investigation). Look for presence of a video capture card board in a child pornography case, and other details pertinent to this type of investigation (e.g., amount of RAM, CPU speed, etc.). Be sure to look for optional storage devices such as flash memory, disconnected hard drives, etc. Verify that the system is configured to boot from floppy diskette, and record which floppy drive is the boot disk.	
5. Decide if the CPU holds potentially valuable information to justify analysis. Check if the CPU is functional, or at least contains some form of media. You might also want to look for any hardware that could be used in the alleged crime (e.g., a video capture board in a pornography case, etc.).	
6. Note down the position of all inside devices including hard drives, floppy drives (if any), expansion cards, etc. Pay special attention to also note down jumpers, cabling and other items that are likely to get altered in the course of analysis.	

7. Take photograph of the system to document its condition upon its entry at the media analysis laboratory. **8.** Inspect all items in custody for evidence of mishandling or other damage. Look for out-of-place or broken cards, drives, etc. **9.** Compare any damage with any damage noted on the evidence tag and record any changes noted. **10.** Photograph ALL damage to evidence, regardless of severity. **11**. If the damage is likely hindering analysis, let this be known to the requesting official or case officer.	
Label Procedures (Split Evidence)	
1. Sometimes, a hard drive needs to be removed from the computer system for forensic data analysis. If the hard drive is detached from the original evidence, it must be labeled separately or some indelible marker must be used to record the case number, suspect name, machine number, etc. on the hard drive that has been removed from the computer system. **2.** The new evidence identifier, that is, label will be the same as the original, however, it will be followed by an "I," "II" or similar designator. In order to identify them separately, you can number the hard drives found in the machine. **3.** A description on the hard drive evidence label might read like this: "This hard drive (serial number, model, etc.) was removed from Label II for purposes of analysis. This is a continuation of Label I and completed by Officer <name of the investigating officer>. **4.** Note down the name of the person receiving the evidence artifact originally and the name of the forensic examiner who removed the hard drive from the machine. **5.** Maintain the chain of custody of the hard drive using this new label till the time the forensic analysis is completed and the hard drive is connected back to the original CPU. **6.** If you return the CPU without the hard drive back to the evidence custodian, then note the original label in the "chain of custody" report as follows: • Released by: <name of the forensic examiner>. • Purpose of releasing the artifact to evidence custodian.	*Note:* When a series of images are created in chunks (typically 2 GB chunks), they are said to be in "*split raw* format." There are issues associated with evidence in "split" format because although commercial forensic tools will typically be able to handle evidence easily in conventional format, split raw images can present challenges for examiners when they use open-source utilities and Linux command-line tools. Remember the "chain of custody" (see Section 7.8) and "chain of evidence" concepts (see Box 7.12) are explained in Chapter 7. *Note:* The analysis can be commenced after visually inspecting. Take photographs (digital pictures are even better) of media and place them in the case file.

• Condition of the evidence artifact: Changed. Removed hard drive for analysis – see label no. <label number>. • Received by: <name of the evidence custodian>. **7.** After completing the analysis of the hard drive, connect the drive into the original CPU. Identify Label II-A in the "chain of custody" report as follows: • Released by: <name of the forensic examiner>. • Purpose of releasing the artifact to evidence custodian. • Condition: Changed. Connected the hard drive into CPU. • Received by: <name of the evidence custodian>. **8.** After the hard drive is re-connected and Label II-A is annotated appropriately, attach Label #II-A to the original tag II.	
Creating Directory of Forensic Analysis	
Having completed the evidence labeling process, create a directory for the analysis on the forensic examination computer. This is the directory under use during the analysis to deposit potential evidence, keyword files and disk images.	
Keyword Listing	
Next, you carry out an assessment of all case data for taking up a potential analysis process, that is, to determine what kind of cybercrime it is (child pornography, murder, credit card fraud, online banking fraud, etc.). Prepare a list of keywords to be searched or get the list from the officer engaged in the case investigation. Put a copy of this in your analysis case file. *Note:* You will understand the importance of "key word search" in computer forensic when you study Chapter 11 (see Section 11.6.2).	In Chapter 8, a real-life example involving use of Internet for murder was sited (see Section 8.6). Also refer to Chapter 11 (in CD) where a number of Credit Card Frauds are explained (see Illustration 4: Understanding Credit Card Fraud Scenarios in Section 11.4.2). A number of video links related to use of keyword searches in computer forensic and topics of evidence acquisition are provided in Ref. #1, Video Clips, Further Reading.

Checking Data Subject's Computer	
Data subject or "suspect" is an individual whose data is being analyzed for forensic investigation. A number of important steps are explained below (this is under the assumption that EnCase is used – refer to Table I.1 of Appendix I).	To understand the difference between CCD and CMOS image sensors in a digital camera, refer to: http://electronics.howstuffworks.com/cameras-photography/digital/question362.htm (26 January 2011).
1. Verify the computer's CMOS settings to make sure that the computer is configured to boot from floppy diskette and to boot the machine from the modified EnCase boot disk.	CMOS is complementary metal–oxide–semiconductor.
2. Verify that the system clock shows the actual date and time. Record in your analysis the correct date, time and time zone reported by the data subject's computer and note down the time difference.	
3. Identify all hard drives, that is, know their make, model, capacity and condition. Document this information and also whether the device is internal or external. Where required, photograph individual hard disks to document damage or other unusual condition.	There are either IDE hard disks or SCSI hard disks. IDE and SCSI are types of hard drive connections/interfaces. SCSI is "Small Computer System Interface" and IDE is "Integrated Drive Electronics."
4. Shutdown the power of computer and identify the hard drive master/slave settings (if IDE) or SCSI ID settings (if SCSI). Note down these settings, and any changes made if necessary to mount the disks into computer used for forensic examination. Make sure that you note any and all changes to evidentiary media.	To understand the working of hard disks, visit the following URLs: http://en.wikipedia.org/wiki/Hard_disk_drive and http://www.buzzle.com/editorials/7-21-2006-103059.asp (25 January 2011).
5. Find the parameters of the hard drive itself by going to the manufacturer's home page (e.g., http://www.seagate.com). If required, modify the computer's CMOS settings manually to get the correct settings for the particular drive under forensic analysis.	
Things to Do on Workstation for Computer Media Analysis	
The following checklist points will help you ensure that media analysis work takes place properly.	
1. Depending on the type of media you have, the size of the suspect evidentiary media and the like decide on the most appropriate backup utility. If possible, use a hard disk of equal size and interface (EIDE, SCSI, etc.). For drives larger than the available media, use 8 mm DAT (Digital Audio	EIDE is Enhanced Integrated Drive Electronics.

	Tape). Make sure that the target media is large enough to hold the image of the evidence media. If a hard drive is to be used as the target media, mount it so that it is accessible to the analysis computer, without being subject to the drive write-protect software.	
2.	Connect the data subject's hard drive to forensic laboratory's computer for analysis or connect the drive into the suspect machine with a parallel port cable for parallel-to-parallel imaging.	
3.	Check the computer's CMOS settings to ensure that the computer is configured to boot from a floppy diskette. Boot the computer using the modified boot disk following instructions as per the instructions in the manual of forensic software you are using.	Appendix I has the list of forensic equipment and forensic software tools.
4.	As you proceed with the analysis to obtain an image, compare the reported information with the information seen on the suspect's machine to make sure that the forensic computer has correctly identified the drive.	Refer to "chain of custody" and "chain of evidence" concepts explained in Chapter 7.
5.	Create an image using suitable forensic software with the suspect's hard drive.	
6.	Store evidence in a secure storage. Where appropriate, return the evidence to the evidence custodian for safe-keeping.	
7.	Use a suitable forensic software tool, study the file structure and look through directories and subdirectories searching for evidentiary files. Also do image searching based on keywords of the investigation.	Refer to D.II.13 in Appendix D.
8.	Look for all files with extensions that would indicate the file requiring special handling. These typically are .zip, .arc, .tar, .gz, etc. Also examine application files that might be password-protected (e.g., MS Word, Excel, Quicken, etc.). If there is any contention (computer intrusion, etc.), or if any allegation is specifically addressed in the request for support, it may call for a review of the file headers. Where found, decompress all compressed files and review their contents.	
9.	Inspect the file structure for applications that could be pertinent to the investigation (e.g., a file conversion utility/viewer in a pornography case).	
10.	Execute any applications that you believe could provide valuable clue for the analysis.	
11.	Write down any log files/configuration settings or other potential sources of information. Note down the names of those applications executed and any important data	

collected during runtime. **12.** Create an "Analysis and Findings" directory on government-owned media (i.e., zip disk, hard drive, Jaz disk, etc.). **13.** Report and transfer all findings to a separate directory under your findings directory that indicates the original location to which the files belong.	
Analysis of Floppy Diskettes	
Although floppy disks are almost out of use, some old data may reside on this media and therefore following items in this checklist: **1.** In order to make the analysis simple, keep all floppy diskettes separate and make sure that each diskette is write-protected. **2.** Using a suitable forensic software tool (here we are assuming EnCase), prepare an image copy of each diskette, and then add these individual evidence file to your case. **3.** Before any acquisition, scrutinize each diskette using a trusted virus protection utility. If the virus scan shows presence of a virus, put a label to indicate that data subject's diskette as infected – this will prevent inadvertent corruption of other media. Note down the virus' presence (name, infected files, etc.) in your working notes.	For an example, refer to Section 11.6.2 in Chapter 11. Hold a 3.5" floppy diskette facing you, and the write-protect slot (if present) is found on the upper right-hand corner – it should be in "covered" state. Appendix I has the list of forensic equipment and forensic software tools.
Findings and Analysis CD	
1. Copy evidence containing files from your "save" subdirectory on the evidence-processing computer to a CD-ROM. Be sure to take in the appropriate utilities on the CD-ROM for reconstruction of the original files by the end-user (lawyer, investigator and defense). **2.** Also make an additional copy of this evidentiary CD to place in evidence. Also have the final report that includes keyword listing, logical file listings, search results and a detailed listing of physical image files, free space, slack space and deleted files where appropriate.	
Case Report and Documentation (Making Sure You Have Everything That Is Needed)	
This is the final step and is very important. The	Remember that case documentation is

following items in this checklist are for investigation manager's utmost attention: **1.** Document the complete computer media analysis and your conclusions in an "Investigative Analysis Report." **2.** Provide this report directly to the Case Officer/Investigation Leader. Include the following artifacts: • Original "Computer Forensic Investigative Analysis Report" duly signed. • All forms used during forensic analysis. • Working notes made during analysis, if available. • Work products produced as a result of the analysis (CDs created, printouts, etc.). • Search authorization copies (consent, search warrant, etc.). • Listing of all evidences. • Worksheet containing media analysis. • Keyword lists used in the forensic analysis. • Documented copies support requests to ancillary agencies as appropriate depending on the nature of the case. • Any other forms, documentation or important correspondence/E-Mail communication copies. **3.** Categorize any files pertinent to the investigation and print them out for inclusion as attachments to analysis report. **4.** If there are too many files that are relevant to the forensic investigation, coordinate with the concerned lawyer to know if print-outs are required. If it turns out that such files are too many, consider taking a print-out of only representative samples and attach them to the case file.	very important especially from the perspective of presenting it in the court. Consider an example of case involving child pornography – there would be several hundred child pornography pictures on a suspect's hard drive. In such situation about 20/30 representative sample images could be printed and included as a hard-copy attachment. 1 GB of information on a hard drive would be 150,000 pages of printed material. The purpose of including the CD findings is to eliminate the need for a printed material.
Important Notes	
While you prepare the final report, it is important to keep in mind the following; although it sounds like common sense, often it is overlooked: **1.** Never make any assumptions. If you discover an E-Mail, do not assume you know the recipient's name from the E-Mail address alone. An E-Mail addressed to "Andrew Wilson," whose E-Mail address is awilson@iex.net does not necessarily mean that the recipient's name is Andrew. E-Mail	In Chapter 2, it is explained how criminals can create fake E-Mails (see Box 2.7 in Chapter 2). Forensic Analysis of E-Mail is explained in Section 7.6 in Chapter 7.

addressed can be faked easily. **2.** Act within your scope – do not go overboard to spot any leads. The report is meant for the Case Officer, and it is his/her job to identify the leads. If you discover something important during your analysis, note it down so that it helps the officer without you providing a lead. **3.** Make sure your report is taken through spellcheck. Do not expect a supervisor or lawyer to proofread your report! Before it leaves your office, make sure all spelling errors are fixed. **4.** Double-check your media findings. If you create a CD finding, make sure that the data is indeed contained in it before you hand it over to your case officer.	

Further Reading

Additional Useful Web References

1. A collection of guidelines to *Crime Scene Investigation* are available at: http://www.homesecurity.us/articles/guide-to-crime-scene-investigation.html (22 January 2011).
2. All publications of SEDONA Conference can be accessed at: http://www.thesedonaconference.org/publications_html (20 January 2011). If you have a general comment, you can E-Mail them at: tsc@sedona.net The link mentioned above is useful because there you can access a number of documents devoted to various topics on digital evidence and questions about them such as preservation of evidence, evidential integrity, etc.
3. Read article *What Judges Should Know about Computer Forensics* is available at: http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf (28 February 2010).
4. The *SEDONA GUIDELINES: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* can be downloaded from the Conference documents repository at: http://www.thesedonaconference.org/publications_html (20 January 2011). Refer to item No. 21. 11/2007 in the link.
5. Legal professionals and law students would like to take a look at item no. 17. 03/2008 at: http://www.thesedonaconference.org/publications_html (22 January 2011). It is The Sedona Conference® Commentary on ESI EvidenCe and Admissibility (ESI is Electronically Stored Information).
6. THE SEDONA CONFERENCE® GLOSSARY: E-Discovery & Digital Information Management (2nd edn) is available at: http://www.thesedonaconference.org/publications_html (20 January 2011). Refer to item no. 20. 12/2007 in the link.
7. The SEDONA Conference Journal containing many useful articles is available at: http://www.thesedonaconference.org/publications_html (20 January 2011). Refer to item no. 23. 08/2007 in the link.
8. The Sedona Conference® Commentary on Email Management (August 2007) is available at: http://www.thesedonaconference.org/publications_html (23 January 2011). Refer to item no. 22.08/2007 in the link. Recall discussion about Forensic Analysis of E-Mail in Section 7.6 and Boxes 7.6, 7.7 in Chapter 7.
9. To understand about CCD and other sensors in digital cameras, you can refer to http://www.digicamhelp.com/camera-features/camera-parts/sensors/ (14 January 2011). http://www.ccdcamera.in/index.htm (14 January 2011). http://sawaal.ibibo.com/search/sensors (14 January 2011).

10. Read article *How to take Crime Scene Photographs* at: http://www.ehow.com/how_2156835_take-crime-scene-photographs.html (12 January 2011).
11. Information about *Forensic Photography for the Crime Scene Technician* is available at: http://www.crime-scene-investigator.net/fet-ol.html (22 January 2011).
12. For information on *Crime Scene and Evidence Photography*, visit: http://www.crime-scene-investigator.net/csi-photo.html (19 January 2011).
13. For advice about choosing the right weapon for crime scene investigation, visit: http://www.crime-scene.blogspot.com/2007/04/choosing-right-weapon.html (24 January 2011).
    To understand Digital Photography and its Importance in Crime Scene Investigation, visit: http://www.bukisa.com/articles/75450_digital-photography-and-its-importance-in-a-crime-scene-investigation (24 January 2011).
    Electronic Crime Scene Investigation Guide can be consulted at: http://www.google.co.in/url?q=http://www.ncjrs.gov/pdffiles1/nij/219941.pdf&sa=U&ei=PF49TZSBLM6s8AbpionJCg&ved=0CBQQFjAB&usg=AFQjCNEYpv_6HqlGhsXwo5c_F4dFM-0U5w (19 January 2011).
14. Read article *Digital Camera Considerations for Crime Scene Investigations* at: http://www.policecentral.com/wp-digicam.htm (23rd January 2011).
15. A technical note on *Advanced Digital Forensics* can be accessed at: http://drtomoconnor.com/3100/3100lect08a.htm (26 January 2011).

Books

1. Vacca, J.R. (2005) *Computer Forensics: Computer Crime Scene Investigation*, 2nd edn, Charles River Media Inc.
2. Casey, E. (2004) *Digital evidence and computer crime: Forensic Science, Computers and the Internet*, 2nd edn, Academic Press.
3. Cross, M. and Shinder, D.L.J (2008) *Scene of the Cybercrime*Syngress Publishing Inc. and Elsevier Inc.

Video Clips

1. A video clip *Computer Forensics - Keyword Searches - Electronic Discovery* can be viewed at: http://www.youtube.com/watch?v=xLEDjEz3BZI (25 January 2011).
2. See the video clip to understand what happens when you delete a file at: http://www.youtube.com/watch?v=g8tEjW243OI (26 January 2011).
3. A video clip on EnCase Computer Forensics Demo is available at: http://www.youtube.com/watch?v=O4ce74q2zqM (20 January 2011).