Appendix F

Guidelines for Computer Forensics Laboratory Set-Up and Guidance on Forensic Readiness Activities in Organizations

Introduction

Forensics is explained in Chapters 7 and 8. Forensics science is about the examination of scenes of crime, recovery of evidence, laboratory scrutiny and clarification of findings and presentation of the conclusions reached for intelligence purposes or for use in court. As mentioned in Chapter 7, computer forensics is the application of computer investigation and analysis techniques to determine potential legal evidence.

This is rather large but extremely informative appendix, as the purpose is to focus on the forensics laboratory set-up aspects and to explain what organizations need to do to be "forensically ready." The difference between security policy and forensics policy is also mentioned in this appendix. There are two parts to this appendix:

1. **Part I:** Guidelines for setting up computer forensics lab (including the Standard Operating Procedures – SOPs) and few useful checklists related to forensics laboratory.
2. **Part II:** Guidance on activities to be undertaken to be a forensic-ready organization. There are a number of crucial steps involved and they are explained in this part. Forensics evidence is not easy to handle and organizations need to prepare for it, pre-plan for it and also need to consider the various costs involved.

Material in this appendix serves as an extension of forensics-related chapters mentioned above. The material provided here will also be useful for organizations that have heavy forensics context. Forensics readiness depends on how "Incident Management" is structured in organizations (recall the discussion in Section 9.9, Incident Handling: An Essential Component of Cybersecurity, in Chapter 9). As you go through this appendix, keep in mind the discussion in Section 9.10, Forensics Best Practices for Organizations, in Chapter 9.

Tools and Procedures used in Forensics Laboratories

Appendix I provides the list of software and hardware tools used in computer forensics. The laboratory is equipped with those tools as well as with competent forensics professionals who are trained to use and operate those tools. In Part I of this appendix, guidelines are provided for setting up of computer forensics laboratory. Supplemental checklists are also provided for various aspects that matter for the excellence of computer forensics laboratories. The checklists provided in this appendix serve as SOPs for laboratory.

SOPs are a set of procedures that are expected to be carried out for a given task. When there are dependable methodologies, probability for errors becomes less. If forensic work is carried out in an ad hoc manner, traceability becomes difficult. When staff leaves the laboratory, it can lead to confusion because in absence of SOPs there would be undocumented work. Prevailing laws and statutory compliance may require retention of forensics records. Even if there is a requirement that each case is owned by only one investigator from start to end, SOPs can still be useful for the laboratory. New investigators who may not be familiar with the laboratory's procedures can read the SOPs like a manual and to execute the steps correctly in forensics methods. For example, when a forensics technician is not familiar with duplicator

(Fig. F.1 shows duplication equipment), he/she can refer to the SOP and follow the steps to complete the task. Note, however, that SOPs are not static procedures; they may change over a time as case experience grows richer and as new equipments/tools come in use. Also not all forensics cases are the same; therefore, different procedures may need to be performed.

As computers are vulnerable to be attacked by some criminals, computer forensics is very important. Therefore, computer forensics procedures are also important and that is the focus of this appendix. Some organizations may have the need to be forensically ready and guidance for that is provided in Part II of this appendix.

Guidelines for Setting Up Computer Forensics Laboratory

The general necessities for the proficiency of testing and calibration laboratories are described in ISO/IEC17025. These ISO requirements are applicable to all types of calibration and objective testing and, therefore, need to be interpreted with regard to the type of calibration and testing concerned and the techniques involved. ISO/IEC17025 is an accreditation standard established under an agreement between the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC), which was issued in December 1999 as a standard succeeding to ISO/IEC Guide 25. This accreditation means that the receiver has been accredited as a calibration laboratory accepted internationally, which ensures traceability in conjunction with international standards. Some key terms are important to note in the context of forensics investigation.

Key Terms

There are certain key terms in forensics that the laboratory technicians should be familiar with:

1. **Objective test:** It is a test that is documented and validated and is under control so that it becomes possible to demonstrate that all appropriately trained staff will obtain the same results within defined limits. These defined limits concern expressions of degrees of probability as well as numerical values. Objective tests will be controlled by documentation of the test, validation of the test, training and authorization of staff, maintenance of equipment and where appropriate by calibration of computer forensics equipment, use of appropriate reference materials, provision of guidance for interpretation of the digital evidence, checking of results, testing of staff proficiency and recording of equipment/test performance.
2. **Reference collection:** It is a collection of stable materials, substances, objects or artifacts of known properties or origin that may be used in the determination of the properties or origins of unknown items.
3. **Court statement:** This is a written report of the results and interpretations of forensics tests/examinations submitted to court. Such reports may be in a format prescribed in legislation.
4. **Chain of evidence and chain of custody:** These concepts are explained in Chapter 7 (Box 7.12 and Section 7.8); from that perspective, “control of records” in computer forensics laboratory is very important. Table F.2 presents “evidence control checklist” – it is part of the SOP for a forensics laboratory. You will see this term mentioned in the checklists presented in this appendix.

The forensics science laboratory should have documented procedures to ensure that it maintains a coordinated record relating to each case under investigation. The information included in case records should be documented. Documented case records include an array of information such as records of E-Mail exchanges, voice recordings made through computer equipment, receiving of digital evidence in evidence bag and/or antistatic bags where applicable (see Fig. 8.2 Faraday bags), descriptions of evidence packaging, chain of custody, seals, subpoenas, that is, search warrants, records of observations and test/examination results, reference to procedures used, diagrams, print-outs, digital dumps of hex data, disk images, digital photographs, etc. Generally, the records necessary to support conclusions should be such that in the absence of the analyst/examiner, his/her counterpart should be able to evaluate what had been performed and interpret the data.

In the introductory remarks, we mentioned about the SOPs. In terms of accreditation of digital forensics/computer forensics laboratories, SOPs help to demonstrate that the management at the forensics laboratory, the operations in the laboratory, the forensics professionals and staff engaged in the laboratory, the equipment used in the laboratory, physical location of the laboratory as well as security and safety procedures meet the required standards such as the ISO mentioned in the introduction. The forensics program should be managed by forensically trained staff. The SOP checklist is presented in Table F.1. Evidence control checklist is provided in Table F.2.

Table F.1 Standard operating procedures checklist

Sr. No.	***Question***	***Response***	
1.	Does the laboratory have a written set of Standard Operating Procedure? Comments ____ ____	Yes	No
2.	Do all the laboratory staff understand objectives of the laboratory? Comments ____ ____	Yes	No
3.	Do the Standard Operating Procedures (SOP) address forensic assignments and qualifications of the staff? Comments ____ ____	Yes	No
4.	Do the Standard Operating Procedures address laboratory security? Comments ____ ____	Yes	No
5.	Do the Standard Operating Procedures address evidence handling to maintain its integrity? Comments ____ ____	Yes	No
6.	Do the Standard Operating Procedures address security and safe storage of examination of reports? Comments ____ ____	Yes	No
7.	Do the Standard Operating Procedures address how forensic equipment is maintained, verified, calibrated? Comments ____ ____	Yes	No
8.	Are the procedures accepted in the digital forensics field with regard to preserving, analyzing and reporting (chain of custody/chain of evidence)? Comments ____ ____	Yes	No
9.	Is there a policy for verifying or auditing records on file?	Yes	No

	Comments ____ ____		
10.	Do the Standard Operating Procedures address proficiency examinations and the required time to complete the exams? Comments ____ ____	Yes	No
11.	Do the Standard Operating Procedures address retention of staff records, training records, equipment records (purchase, maintenance, calibration, etc.)? Comments ____ ____	Yes	No
12.	Are staff assignments, duties, responsibilities clearly stated in the Standard Operating Procedures? Comments ____ ____	Yes	No

Date ____Location _____________

SOP Auditor Name ____

Signature of Auditor/Examiner/Inspector ____

Table F.2 Checklist for evidence control

Sr. No.	***Question***	***Response***	
1.	Does the laboratory have a written policy about chain of custody of all evidence submitted to the laboratory? Comments ____ ____	Yes	No
2.	Does the laboratory have a suitable scheme for identification of evidence received in the laboratory? Comments ____ ____	Yes	No
3.	Is the evidence maintained securely and safely? Is there a restricted access to computers and/or equipments on which digital evidence is held? Comments ____ ____	Yes	No
4.	Is the digital evidence maintained in a way to ensure proper control	Yes	No

	and protection from loss, tampering, theft, manipulation? Comments ____ ____		
5.	Does the laboratory have a tracking system to show where the evidence is stored during the investigation process? Does the laboratory have a confidentiality agreement signed with the parties concerned? Comments ____ ____	Yes	No
6.	Have all the staff members been trained in the proper chain-of-custody procedures and is the chain-of-custody information documented? Comments ____ ____	Yes	No
Date ____Location ____________ SOP Auditor Name ____ Signature of Auditor/Examiner/Inspector ____			

Technical Requirements for Computer Forensics Laboratory Staff

A forensics laboratory should have a defined policy for ensuring that all staff members working in the laboratory are competent to perform the work required. The term “competent” implies having the prerequisite knowledge, skills and abilities to perform the job. The laboratory’s policy should also include procedures for retraining and maintenance of skills and expertise. A laboratory should clearly document the understanding about the competencies required for all jobs and records should be maintained to demonstrate that all staff members are competent for the jobs they are asked to carry out. See the checklists presented in Tables F.3, F.4 and F.5.

Table F.3 Computer forensics Laboratory Manager assessment checklist

Sr. No.	***Question***	***Response***	
1.	Does the Laboratory Manager possess the minimum qualifications required for the role being performed? Comments ____ ____	Yes	No
2.	Does the Laboratory Manager have the experience in staff management? Comments ____ ____	Yes	No
3.	Does the Laboratory Manager have the prerequisite knowledge related to digital forensics/computer forensics?	Yes	No

	Does the Manager also have the experience in conducting forensics examinations of digital evidence? Comments ____ ____		
4.	Is the Laboratory Manager’s responsibility and authority well-defined? Comments ____ ____	Yes	No
5.	Does the Manager possess adequate exposure about interfacing with Legal agencies involved in connection with the evidence, gathers and analyzed? Comments ____ ____	Yes	No
6.	Does the policy address delegation of duties by the Manager? Comments ____ ____	Yes	No
7.	Does the Manager regularly review the staff activities and records in the Laboratory? Comments ____ ____	Yes	No
8.	Does the Laboratory Manger hold meetings to review laboratory policies and procedures on a regular basis? Comments ____ ____	Yes	No
9.	Are the laboratory procedures accepted in the digital forensics field with regard to preserving, analyzing and reporting? Comments ____ ____	Yes	No
10.	Does the laboratory maintain records about last Managers for the statutorily specified period? Comments ____ ____	Yes	No
11.	Does the Laboratory Manager maintain records of previously assigned staff for the statutorily specified period? Comments ____ ____	Yes	No

Date ____Location ___________

SOP Auditor Name ____

Signature of Auditor/Examiner/Inspector ______________________________________

Guidelines for Test Methods, Calibration Methods and Their Validation

There should be full documentation of all methods – this includes procedures for forensics quality control. Reference to materials should be used where appropriate. All technical procedures used by a computer forensics laboratory should be fully validated before using those procedures on casework. When a new (validated) method is introduced, it should first demonstrate the reliability of the procedure in-house with reference to a benchmark for performance characteristics of that procedure. Records of performance verification should be maintained for future reference. There should also be a procedure to identify infrequently performed tests or analyses. All technical procedures used by a computer forensics laboratory must be fully validated before being used on casework.

Guidelines on Equipment Used in Computer Forensics Laboratory

Tools and equipment form a key aspect of computer forensics laboratory. Compilation on software and hardware tools used in computer forensic laboratory is provided in Appendix I. You can see some forensics equipment in Figs. 7.14–7.18 in Chapter 7. As a quick recall, we provide below a summary of some more typical hardware tools used in the laboratory. Figure F.1 depicts those devices/equipments listed. Those are the essential equipments in a computer forensics laboratory.

1. **Computer Forensic Data Server and Forensic Network:** A forensics data server is used to keep forensics images in a centralized, secured and organized manner. This allows forensics investigators to focus fully on case analyses rather than looking for them. The forensics server should have a large data capacity along with the ability to authenticate users as per laboratory security procedures. Also, the server should have the capacity to perform backup of data in case the storage devices fail. There are many vendors who sell such servers (see the list in Appendix I). The forensics network should not be connected to the Internet. This is to avoid any possibility of external access to the evidence. The forensics server is used to store the case files and images acquired.

   It is advisable to have a machine with Internet connection next to the forensics machines so that the investigator can use the Internet for reference, get software updates (and transfer it to a forensics machine to install), look for assistance on forums and check E-Mails. As part of a quality system, forensics laboratories are required to have a program for the maintenance and calibration of the equipment used in the laboratory. The equipment used in a forensics science laboratory is diverse (see Fig. F.1). It was mentioned earlier that at times, there may be a requirement that each forensics case is owned by only investigator from start to end – the Investigation Team Manager not only needs to guide each investigator, but he/she also needs to know what is going on in each case. From this perspective, it helps if the Investigation Manager can remotely access other forensics machines of team members from his/her forensics machine, and can do work on each one from one location. This way, the Manager can easily check up on each, without having to get up and look at each screen. This of course would depend on the team size, number of investigation projects going in parallel and staffing structure in the laboratory as well.

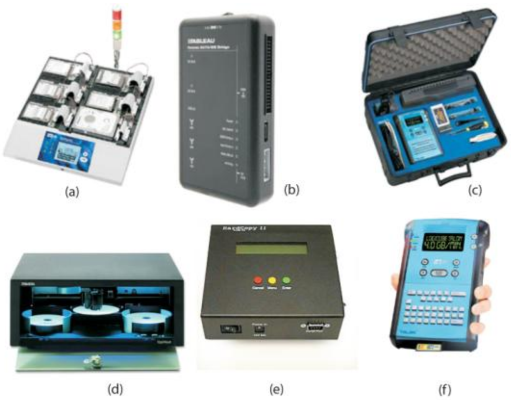

Figure F.1 Tools and equipment in computer forensics laboratory. (a) Wiping equipment, (b) Write protection equipment, (c) Portable forensics kit, (d) Archiving equipment, (e) Duplication equipment, (f) Data capturing device (handy model).
Photo courtesy of Logicube, Inc. All rights reserved. www.logicube.com

2. **Duplicating devices:** Investigators always create forensics duplicates of the original evidence using good imaging tools (you can refer to the list of tools provided in Appendix I). Even then, there are situations wherein they have to step outside the laboratory to perform an acquisition. It would impractical for investigators to carry their laboratory machines with them to the crime scene. Therefore, they usually rely on a mobile solution, for example, a laptop in a briefcase with the forensics software installed. They can also use portable forensics kit (see Fig. F.1).
3. **Data archiving devices:** Image files are usually placed on the forensics servers in the laboratory. Those files occupy tremendous space if they are not removed after their use. Once a forensics case becomes inactive, it needs to be archived. When it is a large case, tapes are used for archival. However, many forensics cases can be small enough to be put on DVDs. Typically, technicians use one of the forensics machines in the laboratory to burn these files to DVD. When performed manually, the task is tedious. First, it has to be ensured that the files all fit in one DVD. If not, the files must be manually split. Thereafter, when each DVD is done, technicians must manually remove one DVD and put the next one in and repeat the process. These activities waste the investigator's time and the machine used to burn the DVDs. Therefore, it is advisable to use an automated machine.
4. **Forensics write blockers:** This is one of the basic pieces of equipment needed in a computer forensics laboratory. A write blocker is used to prevent an operating system (OS) from making any changes to the original or suspect media from erasing or damaging potential evidence. Software write blockers work at the OS level and are specific to the OS. This is the reason why in spite of there being software tools available with built-in software write blockers (refer to Appendix I), various types of physical write blockers are required as well to work with a multitude of devices. USB-based writeblock software is also available. While using this, to make it work properly, you should not start by first connecting the USB to the computer. You should first enable the writeblock and then plug the device. Any devices connected when the writeblock was enabled will not be protected. Always, verify that all software under use is working properly. It is advisable to have a software program that tells you the current status of the writeblock (enabled or disabled). Note that Windows XP SP2 allows users to writeblock USB devices through the registry.
5. **Media wiping equipment:** You need to wipe the media you worked on before you start your case. Wiping of the media is done to ensure that there is no cross-contamination between your cases. When investigators wipe multiple drives, they generally prefer to use a hardware solution that allows multiple drives to be connected at once. However, to verify that a drive has been zeroed out, or to wipe a single drive, they need to select an appropriate tool that helps them to decide whether to do a single pass or a Department of Defense (DoD) wipe. To quickly verify a wiped drive, it is advisable to run the checksum function and see that it adds up to 0. Refer to discussion about DoD Data Sanitization Method in Chapter 7 (Section 7.12.2).

6. **Recording equipment:** Admissibility of forensics evidence in courts is a crucial aspect in forensics. Readers will recall the discussion about this in Chapter 7 (Box 7.4, Sections 7.4, 7.5.1, 7.7.1 and 7.7.2). Computer forensics investigators need an unbiased way of recording events and objects. Remember the admissibility of evidence in court is very important. Investigators must use some form of unbiased method for documentation. One useful way to permanently record an unbiased view of a case is possible through video or audio recording of important aspects of the case. Even recording your thoughts on the case is important. As an investigator, you can use a simple digital recorder that can act as your personal note taker. Investigators generally like to visit the crime scene with a video camera. They must document their methods.
7. **Imaging tools:** It is also important to understand why forensics analysts would never work with the "original" data although it is easier to do analysis directly on original evidence. Evidence would be exposed to the risk of contamination. One of the cardinal rules in computer forensics is never work on the original evidence. This is because evidence is very fragile. Evidence must be handled properly as it can be very easily destroyed. With only one strike on keyboard evidence could be accidentally destroyed or modified. Thus, to summarize, working with the original data is not considered a forensics best practice and therefore imaging tools are required in a computer forensics laboratory.

   Imaging a disk means creating physical sector copy of a disk and compressing this image in the form of a file. This image file can then be stored on different media for archiving or later restitution. During an imaging process an image of the entire disk gets copied. This is done despite of any software on the disk. An important point is that the complete content of the disk is copied including the location of the data. Sector-by-sector copy is obtained through disk imaging, typically for forensics purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not have to be the same geometry as the original if arrangements are made to replicate the geometry if it becomes obligatory to boot into the acquired image. Disk imaging is also one of the methods for backup with the exception that backup only copies the active file. Imaging is very important from evidential perspective. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data typically gets stored in Windows swap file, unallocated space and file slack.
8. **Image mounting tools:** Sometimes forensics professionals want to mount images to preview the drive. There are many tools capable with this functionality. However, sometimes it is easier to see an image mounted in an interface that they are accustomed to. For example, when working on Windows platform, you can use software tool that allows you mount images captured from other tools (e.g., dd, EnCase) as Windows drives. From there, you can preview the drive as if it were part of our local computer. Sometimes, you may receive UNIX drives to investigate. In such situations, you would need to boot a system using Linux that runs from CD (e.g., Knoppix) to create a Samba server. Next you can image the drive through the network. Software programs are available (e.g., "Mount Everything") to let you mount the UNIX drive as a Windows partition. It is seen as a new drive on Windows Explorer and that makes it much easier to image.
9. **Accessories:** Recall Fig. 7.15 of Chapter 7. What is shown in that figure is simply one of the accessories used, that is, connectors. In addition to connectors, forensics analysts also need a variety of other accessories to handle different types of media that is expected to arrive at our laboratory. First of all, they need standard cables such as IDE cables, power cables, SATA (Serial Advanced Technology Attachment) cables. SATA cable connects a motherboard to a SATA hard drive, USB A to B, USB A to mini-B and CAT5e cable. These accessories do not cost much, that is, they are not very expensive. Figure F.2 shows the accessories mentioned here.

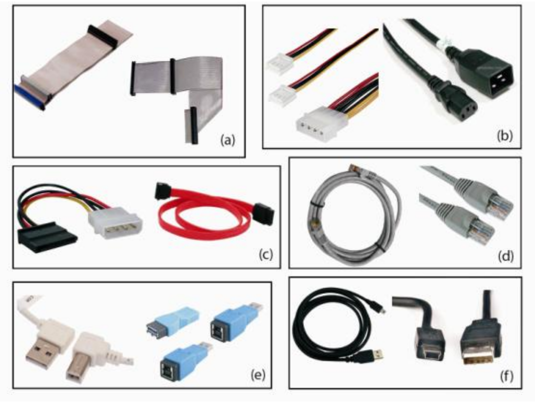

Figure F.2 Accessories – cables and connectors. (a) IDE cable connectors, (b) Power cables, (c) SATA cables, (d) CAT5 cables, (e) USB connectors, (f) USA A to mini-B connectors.

The forensics laboratory also needs some adapters. A USB-to-SATA/IDE 2.5/IDE 3.5 adapter is used for connecting SATA drives, laptop drives and IDE drives to standard USB ports. A SATA-to-IDE cable is used for connecting SATA drives to IDE write blockers. This is a less expensive choice as compared to buying a separate SATA and IDE write blockers. These additional accessories required in computer forensics laboratory are depicted in Fig. F.3.

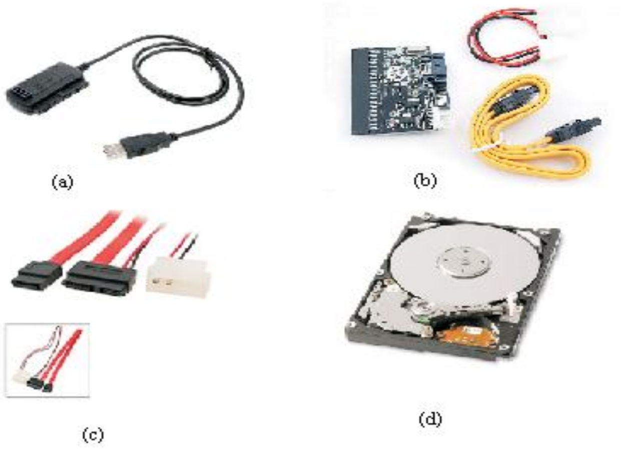

Figure F.3 Additional accessories used in computer forensics laboratory. (a) USB-to-SATA/IDE IDE adapter, (b) IDE to SATA cable, (c) SATA to IDE cable, (d) laptop drive.

Besides the accessories mentioned previously (see Fig. F.3), some more accessories that need to be bought are extra hard drives and external hard drive enclosures (see Fig. F.4). Using these enclosures, disk space can be easily added to forensics machines in the laboratory and disks can be easily moved to other machines. You can also buy USB flash drives for fast file transfers among the forensics machines.

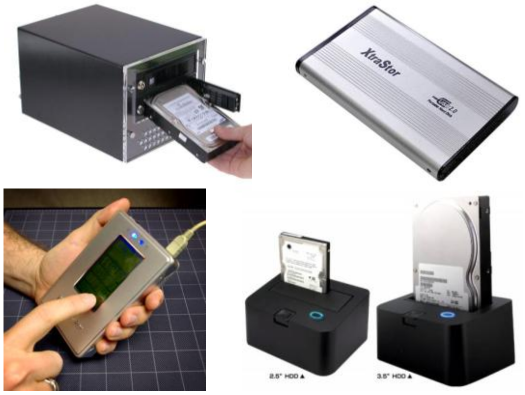

Figure F.4 External hard drive enclosures.

Forensics analysts and forensics laboratory technicians, in their day-to-day work handle floppies, CDs/DVDs, IDE hard drives, SATA hard drives and USB devices because those are the more common types of media they receive. However, at times they may also receive other types of media such as SCSI drives, tape drives and other media for which they may not have any solution. Several options are available in such time. They can buy equipment to handle these types of media or the work can be outsourced to a company that has expertise in data conversion. Of course, before deciding for outsourcing, the laboratory must assess their forensics competence. Such a decision would depend on the budget sanctioned to the laboratory and the inhouse capabilities of the laboratory technicians.

It was mentioned before that as part of a quality system, forensics laboratories are required to have a program for the maintenance and calibration of the equipment used in the laboratory. From that perspective, the competence, skills and capability of the staff working in the laboratory is very important. There are number of computer forensics certifications available in the market.

Readers can refer to Chapter 12 (in CD) where information is provided computer forensics related certifications: (a) Vendor-neutral certifications and (b) vendor-specific certifications.

1. Vendor-neutral forensics certifications:
   - CCE: Certified Computer Examiner.
   - CCFE: Certified Computer Forensics Examiner.
   - CDFE: Certified Digital Forensics Examiner.
   - CEDS: Certified eDiscovery Specialist.
   - CHFI: Computer Hacking Forensic Investigator.
   - CSFA: Cybersecurity Forensic Analyst.
   - GCFA: GIAC Certified Forensic Analyst.
   - GCFE: GIAC Certified Forensics Examiner.
   - CFCE: IACIS Certified Forensic Computer Examiner.
2. Vendor-specific forensics certifications:
   - ACE: AccessData Certified Examiner.
   - CFIP: Certified Forensics Investigation Practitioner.
   - CMFS: Certified Mac Forensics Specialist.
   - CMI: Certified Malware Investigator.
   - EnCE: EnCase Certified Examiner.
   - EnCEP: EnCase Certified eDiscovery Practitioner.

Tables F.4 and F.5 are part of SOPs for a computer forensics laboratory.

Table F.4 Digital forensics examiner checklist

Sr. No.	***Question***	***Response***	
1.	Does each forensics examiner engaged in the laboratory have the prerequisite forensics education/professional/technical certifications to enable him/her carry out his/her day-to-day duties in the forensics laboratory? Comments ____ ____	Yes	No
2.	Has each examiner been taken through successful completion of minimum 84 hours of digital forensics training? Comments ____ ____ Is it an accredited or standard training in computer forensics imparted by a recognized institute/agency? Is it an industry recognized certification in digital forensics/computer forensics? Comments ____ ____	Yes	No
3.	Is the training received from an instructor approved by the authority in the domain of computer forensics? Comments ____ ____	Yes	No
4.	Are training syllabi or certification of completion maintained? Is the attendance record available for each of the training completed? Comments ____ ____	Yes	No
5.	Has the examiner successfully completed, or at a minimum, an annual or semi-annual proficiency exam? Comments ____ ____	Yes	No
6.	Has the examiner undergone refresher training/follow-up training to keep up with the developments in forensics technology and new tools/equipments available in the market? Comments ____ ____	Yes	No
7.	Is each examiner knowledgeable in handling forensics examination equipments, tools (software as well as hardware) and the procedures used in conducting forensics examinations? Comments ____	Yes	No

____

Date ____Location __________

SOP Auditor Name ____

Signature of Auditor/Examiner/Inspector __________________________________

During the list of equipments mentioned, it is seen that technicians or laboratory assistants play an important role as team member of the forensics analyst or investigation lead or Laboratory Manager. Make a note of the checklist in Table F.5.

Table F.5 Technician/laboratory assistant checklist

Sr. No.	***Question***	***Response***	
1.	Does each technician/laboratory assistant meet the requirements of their job classifications as stated in the SOP? Comments ________________________________ ________________________________	Yes	No
2.	Is there a computer forensics competency test available for technician/laboratory assistant commensurate with the tasks assigned to them? Comments ________________________________ ________________________________	Yes	No
3.	Did all technicians/laboratory assistants successfully complete the competency test? Are the records maintained? Comments ________________________________ ________________________________	Yes	No
4.	Are technicians or laboratory assistants required to complete an annual or semi-annual competency test? Comments ________________________________ ________________________________	Yes	No
5.	Are records maintained about current and last technicians/laboratory assistants in the laboratory for review of the minimum statutory period specified? Comments ________________________________ ________________________________	Yes	No

Date ____Location __________

SOP Auditor Name ____

Signature of Auditor/Examiner/Inspector __________________________________

Physical security and safe-keeping of digital evidence in computer forensics laboratory is extremely important. Proper design of the laboratory facilitates the forensics analysis activities performed in the laboratory. Security alarms and CCTV are important part of laboratory facilities. The checklist presented in Table F.6 is from that standpoint.

Table F.6 Laboratory facilities checklist

Sr. No.	*Question*	*Response*	
1.	Does the laboratory have adequate workplace and functionally designed workstations for each staff to work on their forensics examination tasks? Comments ____ ____	Yes	No
2.	Does the laboratory have adequate ventilation, heating and cooling for personnel working in the laboratory? Comments ____ ____	Yes	No
3.	Does the laboratory have controlled access to computers and equipments on which digital evidence resides? Comments ____ ____	Yes	No
4.	Is the physical access to the laboratory controlled and is it limited to authorized personnel only? Comments ____ ____	Yes	No
5.	Does the laboratory administration maintain a distribution log of personnel assigned with keys, locks, lock codes, passwords, etc.? Comments ____ ____	Yes	No
6.	Do all access points in and out of the laboratory have adequate controls? Comments ____ ____	Yes	No
7.	Does the laboratory have a segregated area for holding meetings/discussion with people connected with the cases in progress – lawyers, police officers and other individuals? Comments ____ ____	Yes	No
8.	Does the laboratory have a monitored alarm system or security	Yes	No

	officer on duty during laboratory hours? Comments ____ ____		
9.	Does the laboratory have adequate power supply and wiring for proper functioning of forensics equipments used? Comments ____ ____	Yes	No
10.	Is there a plan in place to address backup power such as backup generator or backup power supplies for forensics examination equipments used in the laboratory? Comments ____ ____	Yes	No
11.	Is there a log of visitors maintained? Comments ____ ____	Yes	No
12.	Does the computer forensic laboratory have systems for smoke detection, fire detection and fire suppression? Comments ____ ____	Yes	No
13.	Is there an adequate number of fire extinguishers placed in suitable areas of the laboratory? Are the fire extinguishers suitable for all fire types? Are those fire extinguishers regularly serviced? Comments ____ ____	Yes	No
14.	Does the laboratory have a technical library containing current reference material on computer forensics, digital evidence examination, etc. (books, journals, white papers)? Comments ____ ____	Yes	No
		Yes	No
Date ____Location _____________ SOP Auditor Name ____			

Signature of Auditor/Examiner/Inspector ____

Additional comments ____

There are also requirements such as a quality manual, etc. for the computer forensics laboratory; however that is not discussed here.

Reporting Computer Forensics Results

It is acknowledged that forensics science laboratories may not be able to contain all of the items in “Court Statements” that are specified in subclause 5.10 of ISO/IEC17025 exactly as per prescribed format of these documents for legislative purpose. Forensics science laboratories may therefore choose to take up one or more of the following ways to meet these requirements:

1. The presentation of a test report that contains all the information mandated by ISO/IEC17025.
2. Providing of an annexure to the Court Statement containing additional information required by ISO/IEC17025.
3. Making sure that the case evidence relating to a particular analysis contains all the relevant information required by ISO/IEC17025.

Part II: Guidance on Activities to be a Forensics-Ready Organization

Having understood the equipments required in SOPs for computer forensics laboratory, let us now understand the activities required in organizations that wish to be forensically ready. The discussion here is to be treated as supplementary information for Chapters 7 and 9 (Section 9.10.3).

In Section 9.10 in Chapter 9, there was a brief discussion on forensics best practices for organizations. In this part of the appendix, we identify a few steps that are essential for getting an organization forensic ready. The key steps are as follows:

1. Defining your business scenarios that necessitate digital evidence.
2. Identifying the available sources and types of potential evidence.
3. Determining the requirement for collecting the evidence.
4. Establishing a capability to securely gather the legally admissible evidence.
5. Putting in place a policy for secure storage and handling of potential evidence.
6. Ensuring that monitoring and auditing is targeted toward detection and deterrence of major incidents.
7. Specifying situations that may call for escalation for formal investigation (possibly with use of digital evidence) may be required.
8. Training your staff about their role in the digital evidence process and the legal sensitivities of evidence.
9. Presenting an evidence-based case to describe cybersecurity incident and its impact.
10. Ensuring legal review to facilitate action on cybersecurity incidents.

The steps listed above are described below. Keep in touch with the chapters and appendices that are mentioned below because they are relevant to the explanations provided below on each of the steps mentioned above.

Step 1: Defining Your Business Scenarios that Necessitate Digital Evidence

This is the first and foremost step to get the organization ready for forensics. You need to define the basis for having the evidence collection competence. With regard to this, it is best to take a risk-based approach. Risks and potential impact on the business from a variety of types of crimes and disputes should be identified. Next, consider the threats to the business and the vulnerable paths. Thus, this is a risk assessment exercise that is tied to most models such as the ISO 27001 and many others. Risk assessment should be performed at the business level. The objective is to recognize the business scenarios where digital evidence may be required and may provide an advantage to the organization in terms of several aspects as explained below.

1. **Reducing the impact of computer-related crime:** A wide range of computer-related crimes presents threats and risks to organizations. Such risks should be looked into with regard to business risks and with regard to prevailing scenario of cybercrime patterns. Further analysis would also be possible with various classes of threats to information systems (refer to the specific chapter in mentioned in Ref. #1, Books, Further Reading).

   A threat assessment is a perpetual exercise that organizations must carry out for an assessment of the potential for a crime to be committed. Crime by insiders also needs to be vigilantly assessed (refer to Fig. 9.2 as well as the discussion in Section 9.1.1 of Chapter 9). Also refer to Ref. #2, Books, Further Reading. Specific questions that should be asked would typically be:
   - Where are people trusted?
   - Are they mobile workers? Do they work remotely?
   - Can all the people be trusted to safeguard organization's information asset?
   - Where are critical points of failure? A vulnerability assessment is also required, not in terms of IT vulnerabilities, but process vulnerabilities and the attractiveness of targets to criminals. Refer to Appendix E and also see Ref. #4, Books, Further Reading.
2. **Effective handling of court orders to release data:** Types of forensics evidences that may be required by a court vary depending on organization's nature of business. E-Mails are one of the common forms of evidence to all organizations. Forensics aspects of E-Mails are explained in Section 7.6, Boxes 7.6 and 7.7 in Chapter 7. It is also worth assessing the likelihood of such evidence being required. Questions to consider:
   - Are we in a business sector that is particularly prone to litigations (e.g., healthcare segment which has the protected health information (PHI) that can be stolen, financial/banking area where the information is targeted by cybercriminals)?
   - Are there any particularly sensitive or controversial activities that might lead to a court case?
3. **Being compliant with regulatory or legal constraints:** This requirement can be business-specific, particularly in the US where there is a sectoral approach of many regulations. For example, the Basel2 regulations for banks, Graham-Leach-Bliley Act (GLBA) for the financial sector and Health Insurance Portability and Accountability (HIPPA) for the healthcare sectors. You can see under Ref. #5, Books, Further Reading to understand the legal frameworks that impact information systems security. With the introduction of laws governing issues, such as electronic document retention (including E-Mails), compliance is becoming ever more important. As another example, consider the need to provide evidence of controls and company communications that show due care in circumstances that have the potential for negligence claims [consider certain requirements under the Sarbanes Oxley (SOX) Act].

   Most jurisdictions have a key legal requirement that potential evidence must not be destroyed. Recall the "chain-of-custody" principal explained in Chapter 7 (Section 7.8, Figs. 7.10 and 7.11, Boxes 7.4 and 7.12). The duty to preserve evidence may arise when litigation is filed or can be reasonably anticipated. Spoliation may be a criminal offense, therfore, an ability to implement a particular evidence preservation process at short notice (which may not be required at other times) could be valuable.
4. **Producing evidence to support company disciplinary issues:** Normally, this may be showing breaking of the organization's Internet acceptable use policy (refer to Appendix C and Section 9.8 in Chapter 9).There are also many other issues where an organization could use digital evidence, such as door swipe logs and phone logs, CCTV clips, etc. to support a case in a disciplinary course of action.
5. **Supporting contractual and commercial agreements:** Detailed documentary support showing resolution becomes necessary when there are commercial and contractual disputes with customers, suppliers and partners or other similar entities that a business may engage with. In modern times, many interactions with these entities are purely electronic. Therefore, preserving the terms and conditions, and dates of agreements can be very useful in avoiding losses and also for successfully leveraging adjudication procedures and other dispute resolution.

6. **Proving the impact of a crime or dispute:** Refer to the discussion in Section 9.9 in Chapter 9. In some incidents, it may become essential to demonstrate the extent of damage that has been caused by an incident or criminal act. This may require evidence gathering in its own right, for example, logs to show downtime, records of staff overtime, costs of new equipment and business lost. It was mentioned in Section 9.9.7 in Chapter 9 that a log retention policy is important because older log entries may show previous instances of similar or related activity.

To conclude, step 1 provides an indication of the likely benefits of being able to use digital evidence in assessing the possible scenarios mentioned above. If the identified risks and the potential benefits of forensics readiness suggest a good return on investment is feasible, then an organization needs to consider what evidence to gather for the risk scenarios. We now turn to explain step 2.

Step 2: Identifying the Available Sources and Types of Potential Evidence

This is the second step in embarking upon forensics readiness. It is important for an organization to understand the sources of potential evidence present on, or could be generated by, their systems. Organizations need to determine the potential evidence data. We know that there are many sources from where computer logs can be available. We had touched upon this when incident response management system was described in Section 9.9.4 in Chapter 9. The purpose of this step is to decide the scope of evidence that may be obtainable from across the variety of systems and applications in use. Some basic questions that can be asked about possible sources of evidence are as follows:

1. Where is data generated?
2. What is the format in which data resides?
3. For how long is it stored?
4. How is it currently controlled, secured and managed?
5. Who has the access to the data?
6. Is the access to data controlled on business need basis?
7. How much data is produced?
8. Is the data archived? If so, where and for how long?
9. How much is reviewed?
10. Are there additional sources of evidence that could be enabled?
11. Who is the custodian/owner of the data? Who is responsible for this data?
12. How could it be made available to an investigation?
13. To what business processes does it relate?
14. Does it contain personal information?

As mentioned in step 1, E-Mail is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving, auditing and retrieval. It should be noted that the E-Mails are not the only means of communication used over the Internet. There is also instant messaging, web-based E-Mail systems and they bypasses corporate E-Mail servers. There are also chat rooms and newsgroups (crimes emanating from Usenet newsgroup explained in Section 1.5.9 in Chapter 1). Security threats in cyberspace are possible even through communication media such as “voice over the Internet.” Each of these communication avenues may need preserving and archiving. A worst case scenario has some of this traffic encrypted.

Under such scenarios, from forensics readiness perspective, the range of possible evidence sources includes:

1. Equipment such as routers, firewalls, servers, clients, portables and embedded devices. Application software such as accounting packages for evidence of fraud and ERP packages for employee records and activities (e.g., in case of identity theft), system and management files.
2. Monitoring software such as Intrusion Detection Software, packet sniffers, keyboard loggers and content checker.
3. General logs, such as access logs, printer logs, web traffic, internal network logs, Internet traffic, database transactions and commercial transactions.

4. Other possible sources of forensics evidence such as CCTV, door access records, phone logs, PABX data, telecom records and network records, call centre logs or monitored phone calls and recorded messages.
5. Backups and archives, for example, laptops and desktops.

Although giving consideration to forensics evidence, it is worth noting that the collection of evidence falls in two categories: (a) One is the *Background* evidence (data gathered and stored for normal business reasons) and the other is the *Foreground* evidence (data specifically gathered to detect crime or to identify criminals). The gathering of foreground evidence is typically referred to as "monitoring," because it normally involves analyzing people's action through the real-time monitoring (e.g., IT or surveillance when permitted legally and feasible practically).

Note also that there are "privacy" implications in collecting forensics evidences because "monitoring" is in general regulated by laws such as those concerning privacy and human rights. Although monitoring may be necessary to fight crime, it is advisable to consult expert legal advice and be aware of the prevailing laws in the jurisdiction to ensure "monitoring" is done legally. The importance of background evidence is sometimes comes from the fact that it has been collected consistent with standard documented business procedures.

It is worth noting this caveat **–** even as the aggregation of evidence from a variety of sources will help the ease of use for evidence during a forensics investigation; it may also become a possible vulnerability! Therefore, the security of this data will be very critical and should be subject to rigid technical and personnel security. As data correlation and event validation are advantageous, this systematic assessment of sources should allow any useful cross-correlations to be identified. Whether or not multiple sources to be actually collected will depend on the evidence requirement explained in step 3 that follows.

Step 3: Determining the Requirement for Collection of Evidence

This is the step toward understanding evidence collection requirement. The principle in this step is to generate an evidence requirement statement, whereby those in charge of managing the business risk can keep in contact with those who run and monitor information systems through an agreed requirement for evidence. Therefore, in this third step, the focus is on deciding which of the possible evidence sources identified in step 2 can help cope with the crimes and disputes identified (refer to step 1) and whether additional ways to collect evidence are necessary.

One of the major benefits of this step is joining IT with the needs of corporate security. Customarily, IT audit logs have been configured by systems administrators separate from the corporate policy. Even if such a policy exists, there is often a major gap between organizational security objectives and the "bottom-up" approach adopted for implementing the audit procedures.

The evidence collection requirement is determined by the typical "cost vs. benefit analysis" approach that is traditionally taken when it comes to money spend. Organizations like to understand how much the required evidence will cost to collect and what benefit it provides (refer to previous paragraph). Like in the previous steps, in this step also, there are a number of critical questions with regard to cost-effectiveness:

1. Can we gather the evidence without undue interference with business processes?
2. Can a forensics investigation be carried out on at a cost that is commensurate with the impact of the security incident?
3. How can we minimize the interruption that may be caused by the investigation to the business?
4. Is the evidence likely to have an impact on the likely success of any formal action?
5. Can the evidence be gathered lawfully without infringing employee rights to privacy?

There are many cost elements involved in the evidence gathering process and they need to be taken into consideration when deciding how much potential evidence can be collected. Those cost elements are summarized as follows:

1. Cost of monitoring (including tools and staff-time).
2. Cost of secure storage – careful handling of forensics evidence is very important – remember the "chain of evidence" and "chain-of-custody" concepts explained in Chapter 7 (Section 7.8, Figs. 7.10 and 7.11, Boxes 7.4 and 7.12).
3. Cost of organizing potential evidence by classifying, indexing and preparation.

4. Cost and implications of retrieval if evidence is demanded by a court.
5. Cost of investigations especially if external incident response team or forensics examination resources that will be used.

It becomes possible for an organization to reduce the costs of any investigations by considering these issues beforehand and by selecting appropriate storage options, auditing tools, investigation tools and appropriate procedures.

In addition to the actual data, there are many other factors that influence the utility, reliability and availability of potential evidence. Those factors are summarized in Table F.7.

Table F.7 Factors to consider in forensics evidence gathering requirements

Factor to Consider in Forensic Evidence Gathering	***Explanation***
Metadata and time stamps (metadata is "data about data" and time stamps are tricky matters).	• Raw data is not easy to use as evidence; especially when out of context. • The date and time of the creation and modification of a file can be critical in terms of providing evidence of an action and allowing it to be correlated with other forms of evidence such as witness statements. Importance of time stamps is explained in Chapter 7 (Sections 7.6, 7.7.2 and Box 7.8). Preparing for the evidence and identifying the evidence is explained in Sections 7.10, 7.17 7.18, 7.19. • Time stamps can be tricky because they can be over-written and the clocks on PCs are often inaccurate. Cryptographic time-stamping services are available along with network time synchronization products – those services can be used to assuage this problem. Consideration can also be given to data through the use of digital signatures to authenticate the creator (or sender) or recipient of a file. The use of hashes can similarly demonstrate the integrity of a file's contents.
Corroboration and redundancy – This is a very crucial consideration in forensics evidence analysis because "integrity" of forensics evidence is important.	• "Logs" were mentioned in this part of the appendix – they are important because they may each contain indications of the same event or activity. • "Duplication" may provide a form of corroboration if, for example, similar activity or independent confirmation of the involvement of a suspect is detected through independent monitoring. • Duplication also serves as an element of redundancy in situation wherein any evidence become corrupted, contaminated or in some way inadmissible. • Recall the discussion in Chapter 7 about "admissibility" of digital evidence (Box 7.4, Sections 7.7, 7.8, 7.10, 7.14, 7.15.1, 7.16.2, 7.19). • Also refer to Chapter 6 (Box 6.12 and Section

	6.4.1). • There may also be instances where evidence collected over a period of time may reduce the need to perform a full-scale forensics analysis of a suspect's hard disk. For example, in the case of an employee, the evidence may be adequate for giving them the confidence to resign, if the employee knows that the organization has seized his/her PC, which can provide corroboration of the evidence gathered through other means. One such situation is illustrated in Section 11.6.1 in Chapter 11 (in CD).
Cause and effect relationships	• In Chapter 7 (Box 7.2), we mentioned about preserving "forensics integrity of data." In Box 7.3 of Chapter 7, we also mentioned about "integrity of the evidence" for litigation purposes. It was also emphasized in Table 7.5 and Section 7.7.3. These are important concepts – evidence should not only point out what happened, but must also point out how, when and by whom. • A variety of pieces of evidence may need to be linked to provide the causal link between the perpetrator and the damaging activity. A forensics chain-of-evidence model can cover access control logs, source OS event logs, network application logs, network traffic logs and the target's OS log. • Relating events in the various logs enable a complete trace of how the incident took place and of the identity or location of the source. • As per the Indian IT Act and its amendments – ITA 2008, "Unauthorized access and Hacking" is a punishable offense (see Tables 1.1, 1.7, Section 1.8.1, Box 1.7). However, there can be cases of "not guilty" verdicts based on concerns that Trojan Horses (discussed in Chapters 2 and 4) may have been responsible and not the alleged person behind! Therefore, gathering suitable evidence might help to show whether or not this was actually the case. This is particularly important in view of "insider threats" discussed in Chapter 9.
Time duration for storage of data and reading time.	• This too is important from evidence integrity perspective. Electronically Stored Information (ESI) ages and tends to deteriorate with the passage of time. • In many investigative situations, the length of time data needs for which ESI to be preserved has to be compliant with the requirements of regulators or law. Certain types of data need to be stored for differing periods of time, depending on regulatory requirements. • This aspect of evidence data storage duration

	should be specified in a data retention policy. It was explained in Chapter 7 that there is a difference between security policy and forensics policy of an organization (refer to Box 7.2). • Choosing how long to store data which may be of potential evidentiary value is a separate issue related to the cost and benefit evaluation. A recommendation to store E-Mails and firewall logs for a number of years is not unusual when an organization wants to track the progression of a possible large-scale fraud or to prove an employee's continued violation of corporate acceptable use policy. • One particular issue is that of recycling backup tapes. Much information is being lost each time a tape is re-used. The length of this cycle should be reviewed, keeping in mind the potential investigative and evidential value of any data being lost. • Here is another dimension to it – suppose there are 3,000 tapes and they each require approximately 3 hours reading time end to end. So, the time required to read the 3,000 tapes would be approximately 1 year! (375 days). This does not take into account the time required to actually analyze and organize the data itself. This support the point mentioned in Chapter 7 – cybercriminals do exploit the reality that forensics investigations are costly and they take time. • Recall the discussion in Section 9.9 in Chapter 9 about Incident Handling – if there is an incident, it may be wise to defer re-use of backup tapes to avoid loss of useful information or to show a court that there is no attempt to hide evidence.
Size of evidence	• Size of digital evidence brings up many complications. Small case investigation is a different experience than a large case investigation (refer to Ref. #7, Books, Further Reading). • Among many issues, "size of evidence" brings up the consideration about cost implications involved in gathering large-scale sources of evidence. • There is the issue of how to sort through them, how to search them and how to compress them. • Forensics experts recommend using of data indexing and information fusion – for example, products that allow multiple sources to be correlated (refer to Appendix I). • The organization needs to consider data mining issues and how to summaries and

	categories potential evidence. Refer to Section 7.17.2 in Chapter 7.
Hardware used in computer forensics investigations	• Appendix I provide the list of software and hardware tools used in computer forensics. • Some hardware that may hold potential evidence is not or cannot be routinely monitored, for example, PDAs and mobile phones (refer to Chapter 8). Forensics hardware required in hand-held devices is said to be not as advanced as that for computer forensics. • In modern times, employee turn-over is one of the major issues faced by organizations. There is a picky issue when someone leaves the organization: Should the past employee's hard disk, laptop, mobile phone and PDA be preserved in any way in case a need for investigation arises? Given the scale of "insider threats" (described in Chapter 9) this is not uncommon.

Step 4: Establishing the Capability for Secure Gathering of Legally Admissible Evidence

By this time, the organization knows the total evidence available and has decided the type of evidence be collected commensurate with the planned budget for addressing the risks faced. Having understood the evidence requirement, the next step is to make sure that the required evidence is collected from the relevant sources and that it is preserved as a bona fide record. Following two preliminary checks need to be made:

1. Can the evidence be gathered without interfering with business processes?
2. Can the evidence be gathered legally? For this, a legal advice is essential to ensure that the evidence requirement can be met in the manner planned. For example, does it involve monitoring personal E-Mails? "Privacy" issues need to be borne in mind. Recall the discussion in Section 7.16.2 in Chapter 7.

Given the legal compliance requirements in computer forensics, organizations should be careful about personal data usage, or "fishing trips" on employee activities? Fishing trips means ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication. In some countries, some or all of these activities may be unlawful. Relevant laws, in the areas of data protection, privacy and human rights will certainly restrict what can actually be collected as forensics evidence. Countries such as the UK have legal requirements whereby monitoring should be targeted at specific problems, it needs to only be gathered for definite purposes, and employees/staff members need to be told about the monitoring activity taking place when it is done in normal circumstances.

Computer system logs can be faked and evidence can be manipulated or planted to lay the blame on others. Therefore, appropriate security measures are required – this is where organization's Security Policy and Forensics Policy comes into picture (refer to Box 7.2). Local logs are too vulnerable and therefore remote logging should be used. Combining these two logs together helps exposing the attempts to hide or change evidence. There can be inconsistency between them if one of them decreases in size. There are tools available to check file integrity (see Ref. # 22, Additional Useful Web References, Further Reading).

With remote logging, organizations can establish a centralized repository. The repository can be used in broad investigations to look for correlations across multiple independent datasets. Secure logging tools are under development, for example, based on IETF RFC 3195 known as syslog-reliable. It supports encrypted and authenticated event message delivery. Organizations should, ideally, publish guidelines for system management staff for evidence collection and storage.

Physical security of data is always important and it is especially so for backup files or on central log servers, from data protection point of view, and also for secure evidence storage. Physical security is important for preventive measures as well. For securing rooms and swipe card access, it is prudent to have records of who has access to the general location and who has access to the actual machines containing evidence. Any evidence or paperwork associated with a specific investigation should be based on extra security – for example, storing in a secure place such as specially designed data storage devices for computer forensics evidence. Additional security of logs can also be achieved through the use of WORM storage (Write Once Read Multiple). Such aspects are explained in Chapter 7.

Step 5: Establishing a Policy for Secure Storage and Handling of Potential Evidence

This step has the objective of securing the evidence from a long-term perspective after it has been collected. The objective of this step is also to facilitate retrieval of the evidence when required. The activities for this step are concerned with the long-term or offline storage of information that might be required for evidence at a later date.

Organizations need to consider measures such as exercising rigid control over administrator access to systems that store potential evidence, encrypting evidence files and any transfers using strong integrity checking and periodic audits. Physical security measures should also be considered, such as access control using card swipes (and accesses should be logged), safes and multiple copies in different storage locations. In other words, the purpose of this step is to establish strong access control mechanism for safeguarding of computer forensics evidence once gathered. These aspects are touched upon in Sections 9.2.1 and 9.5.2 in Chapter 9.

A policy for protected storage and handling of potential evidence encompasses security measures for making sure that the data is genuine and also the authenticity of procedures to show that integrity of the evidence is preserved whenever it is used, moved or combined with new evidence – remember the "chain-of–custody" concept explained in Section 7.8 in Chapter 7. At all times the evidence must be maintained in a tamper-proof (or tamper-evident state). This makes it necessary to the use of evidence bags in the physical world (see Fig. 8.21 in Chapter 8). Access to the evidence storage area should be controlled and anyone requiring an evidence bag must sign it in and sign it back with the contents unchanged. To denote this practice, UK uses the term continuity of evidence and US uses the term "chain of custody." The chain of custody also includes records of who held, and who had access to, and also the evidence – for example, from swipe control door logs.

The code of practice for the legal admissibility and influence of information stored electronically provided a major contribution to the lawful collection of evidence. This code of practice originates from a need felt for collecting evidence in the paperless office. The key question is about Electronically Stored Information (ESI) – if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? There is a need to broaden the scope to all information management systems, such as those where information is transmitted over networks so that messages from Electronic Data Interchange (EDI) and E-Mail systems can be stored under the code of practice. The code of practice for ensuring legal admissibility of the ESI is based on five principles of good practice for information management:

1. Recognizing and understanding all types of information.
2. Understanding the legal issues and execute "duty of care" responsibilities.
3. Identifying and specifying business processes and procedures.
4. Spotting enabling technologies to support business processes and procedures.
5. Monitoring and auditing business processes and procedures.

These principles are reflected in the code in sections comprising of Information Management Policy; duty of care, procedures and processes, enabling technologies and audit trails. It is to be noted however that observance to the code of practice does not promise admissibility of evidence in the court of law and it does not appear to have been tested in court. However, the code only serves as an attempt to define best practice. The result of implementing this step is to have a secure evidence policy established. Such a policy is supposed to document the security measures, the legal advice and the procedural measures used to ensure the forensics evidence requirement is met. The likely admissibility and weight of any evidence gathered rests upon this policy document.

Step 6: Monitoring and Auditing to Detect and Deter Major Cybersecurity Incidents

Besides gathering evidence for using it in the court later, evidence sources should also be monitored to detect threatened incidents in a timely manner. This is similar to Intrusion Detection System (IDS – see Ref. #3, Books, Further Reading). IDS have a larger scope beyond network attack to address a wide range of threat vectors that may impact the organization. Having ensured collection of the evidence, this step meant for ensuring that it can be used in the process of detection. By monitoring sources of evidence triggers an organization to detect that something suspicious may be happening.

The critical question in this step is when should an organization be suspicious? IDS are commonly used to detect suspicious network events and penetration attempts and to alert system managers to the threat. Network staff will know what they are looking for and will set the IDS rules to trigger when certain activities happen. IDS provide real-time monitoring of a certain set of incidents, which are often linked to a real-time response from the company, such as a pager message. Another device is "Honeypots" – it provides a prompt for a spurious event and calls for a first round of investigation. Event correlation can be used to meet the high-level audit requirement explained in step 3.

Normally, "auditing" is used to refer to the review of records post-facto, that is, after they have been generated. Security auditing tools can be deployed to analyze a range of data which can be reviewed on a quasi-real-time basis or in an annual security audit (see Ref. #4, Books, Further Reading). The occurrence of such auditing needs to be related to the business risk discussed, that is, Information Security Risk Analysis (see Ref. #2, Books, Further Reading). During monitoring and auditing, the types of activities recognized as suspicious will differ depending on business needs. For example, a forensics accountant may look for specific patterns in financial data to trigger suspicion of fraud or theft. Content checking may be used, for example, to identify Intellectual Property leakage or data theft – recall the discussion in Section 10.2 in Chapter 10 (in CD). A doubtful event might be numerous E-Mails on a sensitive subject from a person who is not actually involved in the subject.

A suspicious event needs to be related to business risk for facilitating understanding; it should not be stated in technical terms. Thus, the responsibility lies with managers to explain to those monitoring the data what they want to prevent and the sort of behavior for which IDS and Honeypots might be used to detect. This should be captured in a "suspicion" policy that helps the staff (who monitors and audits staff) to understand the kind of triggers to provoke suspicion and to whom to report the suspicion, and the level of monitoring required, and whether any additional security measures should be taken as a precaution. What exactly is audited and what counts as suspicious will be different with time. The suspicion policy needs to be updated as new incidents are noted, new business processes are established, and when new business relationships need to be protected. The policy should also seek guidance from corporate intelligence of the growing threat and the working style of the organization should take this into consideration.

Step 7: Deciding the Circumstances for Full Formal Investigation

Some distrustful events can be system generated, such as by the rule-base of an IDS or the keywords of a content checker, and some will be triggered by human alertness. Each distrustful event, found in Step 6, needs to be reviewed. An event will require escalation if it is serious enough, or it will require enhanced monitoring or other preventive measures, or it is a false positive. The purpose of this step is to make a decision about reacting to the "suspicious" event. The judgment about whether to bring the situation to the notice of higher management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be addressed in an escalation policy that makes it clear when a "suspicious," that is, distrustful event becomes a definite incident. At this point an investigation should commence and policy should indicate who the points of contact are (available on a 24 × 7 basis) and who else needs to be involved – recall Fig. 9.12 in Chapter 9.

The network and IT security managers and the non-IT managers need to understand each other's position (refer to Steps 3 and 6). Ask questions to understand the level of certainty or level of risk that is suitable for an escalation and strength of case as the basis to proceed. At this stage, a business impact assessment should begin and it should be based on the presence of any of the following factors:

1. Evidence of a cognizable crime.
2. Evidence of internal fraud, theft and other loss.

3. Estimate of possible reparation.
4. Potential for mortification, reputation loss, loss of goodwill, damage to company image, etc.
5. Any instantaneous impact on customers, partners or profitability.
6. Enactment or requirement for damage recovery plans.
7. The incident is reportable under a compliance regime.

Refer to Fig. 7.21 to know more about network hacking steps in Chapter 7; some threshold on the potential for damage could be used as an indicator of whether to escalate matters. Any information about the skill level or intent of any miscreant or indication of the target or vulnerability under threat is also required. In information security terms we might be looking for signs of the following while considering “escalation,” that is, bringing to the notice of higher level, the issues and risks noted:

1. **Reconnaissance:** If a high level of skill or knowledge of sensitive resources is used, then consider escalating (refer to Chapter 2 about “reconnaissance” activity, that is, information gathering).
2. **Compromise:** “Attack vector” is explained in Section 2.6 in Chapter 2; if an attack indicates familiarity about the organization (which is typically gathered through “social engineering” mentioned in Chapter 9), sensitive resources or seems focused on a specific purpose then consider escalating. If unable to prevent in future (e.g., patch the vulnerability) then also it should be escalated.
3. **Exploitation:** Escalate unless trivial or closed-down.

Before proceeding with escalation or calling out the Computer Security Incident Response Team (CSIRT), a couple of key questions should be answered to assess the impact on the organization – Can an investigation be supported at a cost commensurate to the size of the incident? How can any investigation minimize disruption to the business?

In the initial part of an investigation, the likely impact of the security incident may not be clear and the organization may also not be able to estimate the level of effort required for the investigation. When it comes to an actual forensics examination, organizations need ready access to the necessary skill sets within a CSIRT. With regard to this, note that Appendix H provides guidance on structuring the Incidence Response Handling Team. Building an incident response team may involve acquiring the skills from an external agency. In such an event, those skills will need evaluation. Also it should be studied as to the standards followed by the skill supplying agency, along with their professionalism and security. However, all this should be done prior to an incident occurrence or else there is the risk that the most “suitable” company, and not necessarily the most effective, may end up getting the contract for skill supply.

The escalation procedure drawn up under step 7 should involve an Investigation Manager, who can decide on whether to call out the CSIRT and make business-critical decisions such as whether law enforcement should step in. The Investigation Manager is also needed when it becomes obligatory to shutdown operational systems and to determine whether an emergency cut-off or a managed disconnect becomes fitting for an online system.

Confidentiality is critical for incident response team’s operations. First, at all times, those involved should operate with a “need-to-know” policy. They should be particularly be aware whether any staff, such as “whistle blowers,” that is, those who call out early warning/early trouble syndrome and investigators, needs to be kept safe from possible vengeance by keeping their names and their involvement confidential.

Step 8: Train the Staff in Digital Evidence Process and Legal Sensitivities of Evidence

This step is aimed at ensuring that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. Refer to Section 9.9 in Chapter 9 to understand that a large number of staff may become involved in a computer security incident. With regard to this, note also that Appendix H provides guidance on structuring the Incidence Response Handling Team.

Another good action is to ensure that staff is capable to perform any roles related to the handling and preserving of evidence. When staff becomes involved in an incident, some general good advice includes:

1. Keeping written (paper-based) notes which are dated, timed and signed.
2. Reporting as necessary and only to those staff with a need-to-know.
3. Not using compromised systems and applications, not using unlicensed tools and software utilities.
4. Knowing that forensics evidence should not be tampered with.

5. Understanding the laws and regulatory principles relating to computer forensics evidence.

Refer to Section 9.9.1 and Fig. 9.12 as you can see there, a wide range of staff is involved with, impacted by or responsible for evidence and investigations. The following teams will require more specialized awareness training about cybersecurity incident:

1. The investigating team.
2. Corporate HR department.
3. Corporate Personnel Relations department (to manage any public information about the incident).
4. Owners of business processes or data.
5. Line management, Profit Center Managers.
6. Corporate security.
7. System administrators.
8. IT management.
9. Legal adviser.
10. Senior Management (potentially up to board level).

After the escalation of a security incident a composite team built from the above-mentioned entities is likely to be formed. These staff may not know each other well or have a great deal of interaction on a day-to-day basis, but fast and effective teamwork is essential. Team building exercise plays a great role when diverse teams come together to form a single team. This is so because each team will differ in their priorities and potentially different interpretations of company policy. Often there will be no clear lines of authority and extensive negotiation will determine the course of action. This will affect middle managers on a common basis and they will require support and training to appreciate the decision points, to make the right decisions and to avoid tainting evidence or "coloring" a case. Role-play training is ideally suited to this scenario. A key role for the organization when a CSIRT is called in is the "liaison manager" or "incident handler." A CSIRT, whether internal or external, needs a single point of contact to manage communications with the organization and to ensure that any requirements for facilities or resources to expedite the investigation are met. With regard to this, note also that Appendix H provides guidance on structuring the Incidence Response Handling Team.

Again refer to Section 9.9.1 and Fig. 9.12 – in view of the scenario depicted in the figure, training will do good for creating an understanding of the relationships and necessary communications with external organizations that may become involved such as those mentioned below – note, however, that it is only a generic list based on collective understanding of incident management systems; they may vary from country to country:

1. Police and other law enforcement agencies involved with the incident.
2. Overseas prosecution authority or court.
3. Trade Union/Staff Association representatives.
4. Internal or external auditors.
5. Regulatory authorities.
6. Customers, suppliers, contractors and other partner organizations.
7. Facilities management organizations (e.g., companies to whom IT or building security has been outsourced).
8. The media.

Step 9: Present an Evidence-Based Case Describing the Incident and Its Impact

The purpose of this step is to create a policy describing how an evidence-based case should be assembled. In any forensics investigation, the aim is not merely to find a criminal or to revamp any damage. An investigation is supposed to provide answers to questions and demonstrate the credibility of those answers. The questions are based on "who, what, why, when, where and how." Credibility comes in on the strength of forensic evidence and the logical arguments that can be put forth about the integrity of the evidence.

A case file may be required for a variety of reasons: To provide a foundation for interacting with legal advisers and law enforcement agencies, to support a report to a regulatory body, to put up an insurance claim, to justify disciplinary action, to provide feedback on avoiding recurrence of similar incidence in future, to be able to furnish a record in case of a similar event in the future (so that documentation works as support even when the concerned staff has left the organization) and to provide further evidence if required in the future.

When you visit Appendix D, Part III (D.III.1 and D.III.2), you will realize that an incident case file typically has components such as incident description – how it happened, how it was detected, the hypothesis, the root cause of the incident caused, whether the perpetrator was identified, where the perpetrator is located, the evidence indicating the location if an appropriate digital record is not included, paper files, details of interviews, signed witness statements, physical evidence, etc. The argument to support that the evidence "proves" the hypothesis and the impact showing the damage or potential damage to the organization should be inclusive of any evidence to support the evaluation of the damage.

The case file maintained about a cybersecurity incidence should be stored securely and subject to access control (see steps 3 and 5) commensurate with "chain-of–custody" concept. During the case writing-up process a couple of more issues can come up: (a) the investigation may have found evidence that does not make the perpetrator "culpable" (indicative of a person's guilt) and (b) it may also have found some "exculpatory evidence" (indication of innocence). A case is rarely "black and white."

An unambiguous policy in an organization is required for handling such "exculpatory evidence." Sometimes, such evidence could be the subject of a court disclosure order. Ideally speaking, destroying or hiding the evidence is neither advisable nor should be possible and such an act may well be against the law. However, in reality, it may be required if the conclusion of the investigation turns out to be wrong.

Forensics experts are required as explained in Chapter 7 – this is because, digital evidence can be difficult for a common man to read and understand. Therefore, the case file should show how to present the evidence – this may even involved use of visualization tools and timeline analysis of the incident or of events leading up to it. The evidence may have to convince general public representation on a jury. As a final point, it is to be noted that if any mistakes or errors occur during a forensics investigation, they should not be hushed up. At times, errors in the forensics process may seem to do indicate weakness of the evidence; however, as long as what actually happened is truthfully recorded, it may still be useful.

Step 10: Ensuring Legal Review to Take Possible Action in Response to the Incident

A legal review of the incident case can become necessary due to some peculiar points noted during collating of the cybercrime case file and there may even be a need to seek legal advice on any follow-up actions. Legal advisers should be able to provide advice on the merit of the case and should be able to propose whether additional measures should be taken. For example, in case of weak evidence, does it become necessary to catch an internal suspect redhanded by monitoring their activity and seizing their PC or laptop? Any sequence of formal action will need to be supported, will need to be cost-effective and should be assessed as likely to end in favor of the organization. Although the definite decision about proceeding will clearly be taken after the incident, extensive legal preparation is required in case of readiness. Legal advisors should therefore be competent based on their skills and experience in appropriately applying the prevailing cyberlaws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case presented in step 9. Legal advice should also identify that the legal issues are likely to span across legal jurisdictions because cyberlaws vary from country to country.

Legal advisers will typically be able to provide advice on the following matters:

1. How to deal with any liabilities that may arise from the incident.
2. Finding and prosecuting/punishing (internal vs. external culprits).
3. Legal and regulatory constraints based on which a course of action can be taken.
4. Protection of reputation (brand image, good will, etc.) and Intellectual property issues (refer to Section 10.2 in Chapter 10).
5. Situations where advice to partners, customers and investors become necessary.
6. Dealing with employees especially when "privacy" challenges are involved (refer to Section 7.16.2 in Chapter 7).
7. Settling commercial disputes.
8. Any additional provisions required.

Often many organizations are not clear about circumstances under which law enforcement agencies need to be contacted. At the same time, there is a need to be in contact with them on a proactive basis (as part of organization's forensics readiness) to understand forensics policies and priorities and also to be able to work together effectively. Organizations' willingness to prosecute may depend on:

1. Severity of crime or scale of impact on the organization.
2. Amount of any financial loss (recall the discussion in Section 9.2.1 in Chapter 9).
3. Whether the impacted party, that is, the victim is potentially part of organized crime, or may look for further opportunities, or has demonstrated serious intent or a motive and method toward committing the crime.
4. Manpower constraints and operational priorities.

Not all investigated cases end up getting prosecuted. With regard to this, Fig. 9.18 in Chapter 9 is worth noting. We end this part of the appendix with a few concluding remarks that are valuable to make a note of.

"Forensics readiness" of an organization is its ability to use digital evidence when required. Further, the aim of readiness involves organization's ability to maximize opportunities for gathering and using digital evidence and at the same time minimizing the costs of related investigations. This combination would help beat cybercriminals who exploit the fact the forensics investigations are costly and heavy on time involved. The ten steps described in this appendix will help to provide a business context to digital evidence. These steps will help organizations to adopt practical approach to the policies and practices required for achieving a forensics readiness capability.

Forensics readiness complements enhance many existing information security activities in an organization. "Forensics readiness" of an organization should be treated as part of an information security risk assessment to determine the possible disputes and crimes that may bring up the need for electronic evidence. It is closely related to incident response and business continuity to ensure that evidence found in an investigation is preserved and the continuity of evidence is maintained. Forensics readiness is a part of security monitoring to detect or to deter disputes that have a potentially damaging impact on business. Forensics readiness also needs to be incorporated into security training, particularly for middle managers who have to deal with an incident in a multidisciplinary team.

Further Reading

Additional Useful Web References

1. To know more about ISO/IEC17025 in Laboratories, visit:
   http://www.labcompliance.com/tutorial/iso17025/default.aspx (27 December 2010).
   http://www.starlims.com/17025.htm?_kk=ISO%2017025&_kt=3a6344e3-3a48-40ac-84f4-e1c8fde76b44&gclid=CKbHxsDum6YCFQH1bwodejVhSg (2 January 2011).
   http://en.wikipedia.org/wiki/ISO/IEC_17025 (28 December 2010).
2. Visit *Building a Computer Lab* at: http://computerforensicslab.blogspot.com/ (23 December 2010).
3. To know how forensics lab techniques work, visit:
   http://science.howstuffworks.com/forensic-lab-technique.htm/printable (18 December 2010).
4. Visit *Introduction to Computer Forensics Tutorials* at:
   http://www.vtc.com/products/Introduction-To-Computer-Forensics-tutorials.htm
   (1 January 2011).
5. Read *Computer Forensic Standard Operating Procedures* at:
   http://www.ehow.com/list_6809822_computer-forensic-standard-operating-procedures.html (28 December 2010).
6. You can view a *Flow Chart for Digital Forensic Analysis* at:
   http://www.cybercrime.gov/forensics_chart.pdf (23 December 2010).
7. Position description for a Computer Forensic Examiner can be seenat:
   http://www.forensicsconsulting.com/pdfs/Forensic%20Examiner%20Job%20Description.pdf (23 December 2010).
8. *Computer Forensic SOP* pdf download link can be accessed at:)
   http://www.pdfebook4u.com/computer-forensics-sop.html (28 December 2010).
9. Read *The Importance of Computer Forensics in eDiscovery* at:
   http://www.dts.ca.gov/pdf/news_events/sec_awareness/Guidance_Software_eDiscovery_Forensics.pdf (25 December 2010).
10. Computer Forensics Processing Checklist can be obtained from
    http://www.crime-research.org/library/Computer%20Forensics%20Processing%20Checklist.pdf
    (30 December 2010).

11. Visit the *Computer Forensics Store* at http://www.forensicstore.com/ (31 December 2010).
12. You can find commercial information about DVD Duplicators and Printers at: http://www.primera.com/ (1 January 2011).
13. The *M2CFG Writeblock Utility* can be used to write-protect all USB devices. This application requires Windows XP with Service Pack 2 or 3 to operate. For a Free Download, you can visit: . http://www.m2cfg.com/downloads.htm (31 December 2010).
14. To know about *Windows Server 2003 Resource Kit Tools*, visit: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en (1 January 2011).
15. For *WinHex*: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor, visit: http://www.x-ways.net/winhex/ (2 January 2011).
16. Information on *Fingerprint Scanners* is available at: http://catalogs.indiamart.com/products/fingerprint-scanners.html (29 December 2010).
17. For KNOPPIX, you may find the resources at:
    KNOWING KNOPPIX The Beginner's Guide to the Linux that runs from CD by Phil Jones available at: http://db.ilug-bom.org.in/Documentation/knowing-knoppix_2004-12-30.pdf (1 January 2011).
    Short presentation on Knoppix is available at: http://foss.in/slides/lb2003/karthik-knoppix.ppt (1 January 2011).
18. *SATA Cables* related resources are as follows:
    To know about these cables, visit: http://en.wikipedia.org/wiki/Serial_ATA (29 December 2010).
    Video clips on SATA can be sourced at:
    http://www.google.co.in/search?q=what+is+SATA+cable&hl=en&prmd=ivns&source=univ&tbs=vid:1&tbo=u&ei=NEIfTduuNZGKvgPVpcz9DQ&sa=X&oi=video_result_group&ct=title&resnum=4&ved=0CBwQqwQwAw (1 January 2011).
19. SATA Cable Manufacturers details can be viewed at: http://www.tradeindia.com/manufacturers/indianmanufacturers/sata-cable.html (31 December 2010).
20. For additional information about importance of time stamp in computer forensics evidence analysis, visit:
    http://www.ehow.com/about_5549778_computer-forensics-analysis.html (14 December 2011).
    http://www.lawgazette.com.sg/2003-3/Mac03-col4.htm (14 December 2011).
    Read article *Digital Forensics: How to configure Windows Investigative Workstations* at: http://blogs.sans.org/computer-forensics?s=FAT&searchsubmit=Find (14 December 2011).
21. Read article *Computer Forensics: Bringing the Evidence to Court* at: http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf (14 January 2011).
22. In network forensics, the tool called Tripwire is used to look for file system tampering – see the presentation available at: http://www.iitg.ac.in/cse/ISEA/isea_PPT/ISEA_02_09/NWForensics-IIT%20Guwahati-21Feb2009OVS.pdf (15 January 2010). It is used to find hacker footprint because basically, it is a file and directory integrity checker tool.

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Framework and Best Practices*, Wiley India, New Delhi. Refer to Chapter 2 (Threats to Information Systems).
2. Ibid, Chapter 6 (Information Security Risk Analysis).
3. Ibid, Chapter 14 (Intrusion Detection for Securing the Network).
4. Ibid, Chapter 35 (Auditing for Security), Section 35.9 (Technology-based Audits – Vulnerability Scanning and Penetration Testing).
5. Ibid, Chapter 27 (Laws and Legal Frameworks for Information Security).
6. Sheetz, M. (2007) *Computer Forensics: An Essential Guide for Lawyers, Accountants and Managers*, John Wiley & Sons, NJ, USA.

7. Volonino, L. and Redpath, I. (2010) *e-Discovery for Dummies*, Wiley Publishing Inc. Refer to Chapter 16 (e-Discovery for Large-Scale and complex Litigation) and Chapter 17 (e-Discovery for Small Cases).