



Annual ADFSL Conference on Digital Forensics, Security and Law

2007
Proceedings

Teams Responsibilities for Digital Forensic Process

Salma Abdalla

Information Technology Industry Development Agency (ITIDA), salma@mcit.gov.eg


Sherif Hazem

Faculty of Engineering, Arab Academy for Science and Technology Information Technology, Industry Development Agency (ITIDA), snoureldin@mcit.gov.eg

Sherif Hashem

Faculty of Engineering, Cairo University, Information Technology Industry Development Agency (ITIDA), shashem@mcit.gov.eg

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Abdalla, Salma; Hazem, Sherif; and Hashem, Sherif, "Teams Responsibilities for Digital Forensic Process" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 1.
<https://commons.erau.edu/adfsl/2007/session-8/1>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



Teams Responsibilities for Digital Forensic Process

Salma Abdalla

Information Technology Industry Development Agency (ITIDA)
salma@mcit.gov.eg

Sherif Hazem

Faculty of Engineering, Arab Academy for Science and Technology
Information Technology Industry Development Agency (ITIDA)
Snoureldin@mcit.gov.eg

Sherif Hashem

Faculty of Engineering, Cairo University
Information Technology Industry Development Agency (ITIDA)
SHashem@mcit.gov.eg

ABSTRACT

This paper presents a detailed digital forensics process model and the responsible teams to perform it. The discussed model presents three teams and a forensic leader who coordinate between the three teams; these teams are physical crime scene team, laboratory examination team and courtroom team. These teams are responsible of achieving the digital forensic model by applying five main phases which are preparation phase, physical forensics and investigation phase, digital forensics phase, reporting and presentation phase and closure phase.

Most of the existing models in this field are either theoretical that deals with data processing or based on a legal point of view. Although they gave good information to base on it a guide, but they are not detailed enough to describe fully the investigative process and do not define teams and their responsibilities for investigation in a way that can be used by investigators during investigation.

In this model the responsibilities and procedures of each team is represented given detailed steps for each team, so it can be used as guidance for the forensic investigators during investigation and assist their training.

Keywords: digital forensics, computer forensics, digital investigation, forensic model, reference framework, Forensic teams' responsibilities.

1. INTRODUCTION

Digital forensics can be defined as the process of extracting information and data from digital storage media and guarantee its accuracy and reliability. The challenge is actually finding this data, collecting it, preserving it and presenting it in a manner acceptable in a court of law (Marcella & Greenfield 2006; Palmer 2001). Digital forensic science is a relatively new discipline that has the potential to greatly affect specific types of investigations and prosecutions (Hall & Wilbon 2005; Asian School of Cyber Laws 2006).

To be able to perform digital forensic investigation, the organization providing this service must have the capability means that helps an organization to be prepared to detect and counter cyber crime incidents in a skilled and efficient manner. Such capability is combination of technically skilled people, policies, and techniques to constituting a proactive way for handling cyber crime incidents. There are some important conditions that should be followed by the organization to have these capabilities such as providing proper training for personnel of teams, ensuring that personnel are aware of the types of evidence usually encountered and the proper handling of the evidence, and the lab

should be equipped with the proper up-to-date equipments and forensic tools required for all operating systems and all system files for investigation.

In this paper a comprehensive and complete teams responsibilities model is discussed which propose detailed steps for each team, so it can be used as a reference frame work, support training of investigators and tool development. This model is based on previous models to meet special challenges of electronic evidence nature and make it admissible in courts. These challenges can be achieved by three different teams and a forensic leader who leads and coordinates between the three teams. These teams are physical crime scene team who is responsible of the physical forensics and investigation phase in the crime scene, laboratory examination team who is responsible of the digital forensics phase (the digital crime scene) and courtroom team who is responsible of both the legal and non-technical parts of the investigation which includes reporting and presentation phase and closure phase.

The rest of the paper is divided into 2 sections. Section 2 discusses the teams' detailed responsibilities and procedures steps and Section 3 is model discussion and conclusion.

2. TEAMS RESPONSIBILITIES

2.1 Forensic Leader

A forensic leader is the person in charge who is responsible for coordinating between the three teams and responsible of achieving some other responsibilities such as:

1. Secure the scene.
2. Prepare administrative log, and narrative description.
3. Resolve problems.
4. Make final decisions.

He is also responsible with the help of the three teams to achieve the preparation phase which is the first stage of incident handling procedures, it must be applied before handling any investigation, the purpose of this phase is to make sure that the operation and infrastructure can support the investigation. Preparation phase can be subdivided into pre-preparation, case evaluation, preparation of detailed design for the case, preparation of investigation plan and determination of required resources.

2.1.1 Pre-preparation

1. Detect and identify the incident and make risk assessment of vulnerabilities and threats.
2. Discuss the search with involved personnel before arriving at the scene (Federal Bureau of Investigation 2003).
3. Establish a command headquarters for communication and decision making in major or complicated crime-scene searches (Federal Bureau of Investigation 2003).
4. Make preliminary personnel assignments for the physical crime scene team before arriving at the scene, while the assignments are keeping with the attitude, aptitude, training, and experience of search personnel.
5. Develop legal activities coordination plan (Federal Bureau of Investigation 2003), obtain a search warrant, if necessary, and obtain written and signed permissions from the concerned authorities to proceed.
6. Prepare the paperwork to document the search (Federal Bureau of Investigation 2003).
7. Provide all the needed requirements such as protective clothing, communication, lighting, shelter, transportation, equipment, food, water, medical assistance, etc.

2.1.2 Case evaluation

1. Initial case assessment: Investigator should perform initial assessment about the case by for example: asking questions related to the rule of computer /network in question and evidence related to the case.
2. Identifying the case requirements : which involves outing details of the case in systematic order such as:
 - a. Situation of the case: a case can be violation of company policies by employee or Child pornography, etc.
 - b. Nature of the case: personal work on employer's computer or on a whole network or unknown criminal, etc.
 - c. Specifics about the case: for example the role of computer or employee in question.
 - d. Type of evidence: Can be hard disk, floppy, CD, etc.
 - e. Operating system used by the suspect if possible.
 - f. Knowing disk format [e.g. FAT32, NTFS, EXT3, etc.].
 - g. The motive of the suspect: try to find motive of the crime and develop a general theory of the crime.

2.1.3 Preparation of detailed design for the case

The general outline to investigate the case, in which detailed steps are prepared taking into account the estimated time, resources and money required to complete each step.

2.1.4 Preparation of investigation plan

1. Develop an onsite plan which must include policies, procedures, personnel assignments, and technical requirements.
2. Plan for what to look for during search.
3. Approach strategy for both evidence collection and preservation.
4. Steps for evidence examination and analysis should be predefined.

2.1.5 Determination of required resources

1. Determine kind of software and hardware for investigation according to suspect operating system.
2. Specify tools that are accepted by courts [tested].
3. Accumulate evidence collection and packaging materials and equipment.

2.2 Physical Crime Scene Team Responsibilities

Physical crime scene team which consists of first responders, investigators, search and seizer coordinators and crime scene technicians is responsible for recognition, collection of physical evidence, preservation, transportation and storage of electronic evidence from the physical crime scene.

Each one of the team must understand the fragile nature of electronic evidence and the principles and procedures associated with its preservation. Actions that have the potential to alter, damage, or destroy original evidence may be closely scrutinized by the courts (Carrier 2006; National Institute of Justice 2001). The proper sequence for handling the team responsibilities is through the physical forensic and

investigation phase .The goal of this phase is to collect, preserve, analyze the physical evidences and reconstruct what happened in the physical crime scene. It can be subdivided into physical preservation, preliminary survey on physical scene, evaluate the physical scene, initial documentation, photographing and narration, search and collection of physical evidence and final survey for physical crime scene.

2.2.1 Physical preservation

1. Take extensive notes all the time and for everything, and consider the safety of all personnel (Federal Bureau of Investigation 2003).
2. Secure the physical crime scene:
 - a. Follow jurisdictional policy for securing the crime scene, by ensuring that all persons are removed from the immediate area from which evidence is to be collected and do not alter the condition of any electronic devices. (National Institute of Justice 2001)
 - b. Take immediate control on the scene by keeping out unauthorized personnel and record who enters and leaves.
3. Determine the extent to which the scene has been protected and get information about who have knowledge about the original condition.
4. Make interviews: (National Institute of Justice 2001)
 - a. Separate and identify all persons (witnesses, subjects, or others) at the scene and record their location at time of entry.
 - b. Consistent with departmental policy and applicable law, obtain from these individuals information such as:
 - i. Owners and/or users of electronic devices found at the scene, as well as passwords, user names, and Internet service provider.
 - ii. Any passwords required to access the system, software, or data. [An individual may have multiple passwords, e.g., BIOS, system login, network or ISP, application files, encryption pass phrase, e-mail, access token, scheduler, or contact list].
 - iii. Purpose of the system.
 - iv. Any unique security schemes or destructive devices.
 - v. Any offsite data storage.
 - vi. Any documentation explaining the hardware or software installed on the system.
5. Place labels over all the drive slots and over the power connectors.

2.2.2 Preliminary survey on physical scene

1. Select a narrative technique [written, audio...] then start taking preliminary photographs (Federal Bureau of Investigation 2003).
2. Delineate the extent of the search area. Usually expand the initial perimeter (Federal Bureau of Investigation 2003).
3. Identify and protect transient physical evidence.
4. Document physical and environmental conditions of the scene and all personnel movements.
5. Detect or suspect unauthorized activity; and report detected or suspected unauthorized activity to the proper authority (Beebe & Clark 2004).

6. Identify telephone lines attached to devices, if a telephone connection is present, attempt to identify the telephone number.
7. Document, disconnect and label each telephone line from the wall not from the device.

2.2.3 Evaluate the physical scene

1. Validate the incident and assess damage/impact via interviews of technical/business personnel, review of pertinent logs and review of network topology, etc. (Beebe & Clark 2004).
2. Ensure that the collection and packaging materials and equipment are sufficient.
3. Ensure the protection of Non digital evidences such as finger prints.
4. Search the easily accessible areas, progress to out-of-view locations while looking for hidden items.
5. Evaluate whether evidence appears to have been moved or used.
6. Identify the number and type of computers and determine if a network is present.
7. Identify both internal and external storage devices that need to be seized.
8. Determine exactly where each device is physically located and label its location using labels.
9. Identify any application and/or users that are affected by a problem.
10. Determine which devices are on the network and determine which devices connect this network to the Internet and systematically search each part of the network for problems.
11. Determine how the devices are configured (Schweitzer 2003).
12. Make a complete evaluation of the crime scene.
13. Test the design: The decision made or steps taken should be reviewed. By reviewing the investigator can find out whether these steps are correct or need to be adjusted.

2.2.4 Initial documentation, photographing and narration

1. Nothing is insignificant to record if it catches one's attention (Federal Bureau of Investigation 2003).
2. Initial documentation
 - a. Document everything
 - b. Observe and document the physical scene, such as the position of the mouse and the location of components relative to each other [e.g., a mouse on the left side of the computer may indicate a left-handed user] (National Institute of Justice 2001).
 - c. Document the condition and location of the computer system, including power status of the computer (National Institute of Justice 2001).
 - d. Identify and document electronic components that will not be collected.
 - e. Take written notes on what appears on the monitor screen (National Institute of Justice 2001).
 - f. Active programs may require videotaping or more extensive documentation of monitor screen activity (National Institute of Justice 2001).

- g. Use case management system so that the written data are protected and made available to a database of case information. With the case management system create three log files:
 - i. Search and seizer evidence log that include brief descriptions of all computers, devices or media located during the search for evidence. It also should document the date and time of the investigation, the names of all people who are involved with investigative activities (Wright 2001) and timestamp of the whole processes.
 - ii. Lab evidence log that includes: date and time of arrival of the seized evidence at the lab; a brief description of the evidence, the condition of the evidence upon arrival and name and signature of the investigator checking in the evidence (Wright 2001), then it will include details about the examination processes and who perform it.
 - iii. Collection log file which includes details about collection steps in digital forensic phase, and also includes image of the collected data, the check sum or md5 sum of the original and collected data and the investigators details including digital signatures and timestamp.
3. Additional documentation of the system will be performed during the rest of phases. Documentation is an ongoing process through the whole forensic phases. Therefore document each and every step done by the investigator or examiner and document anything that is found.
4. Use photographs and sketches to supplement, not substitute for, the narrative (Federal Bureau of Investigation 2003).
5. Do not collect evidence or touch anything during the narrative.
6. The narrative should include the following: (Federal Bureau of Investigation 2003)
 - a. Case identifier.
 - b. Date, time and location.
 - c. Identity and assignments of personnel.
 - d. Condition and position of evidence.
7. Prepare a photographic log that records all photographs, description and location of evidence and then include it in the search and seizer log file.
8. Photograph all stages of the crime-scene investigation, including discoveries (Federal Bureau of Investigation 2003).
9. Photograph the condition of evidence before and after examination.
10. Complete room should be recorded with 360 degrees of coverage, when possible, and photograph the front of the computer as well as the monitor screen and other components (National Institute of Justice 2001).

2.2.5 Search and collection of physical evidence

According to the case and depending on the initial case evaluation and plan , these steps can change depending on the case nature, taking decision depends on the case and should be taken with utmost care.

These are general steps for searching for physical evidences such as PCs or other equipments that can be used by the suspect:

1. Start the search and seizure evidence log in the case management system to document all devices state.

2. Search from the general to the specific for evidence and be alert for all evidence makes sure to protect the integrity of the evidence.
3. Wear latex or cotton gloves to avoid leaving fingerprints (Federal Bureau of Investigation 2003).
4. Search entrances and exits, and photograph all items before collection and notate the photographic log and mark evidence locations on the sketch (Federal Bureau of Investigation 2003).
5. Complete the search and seizer evidence log with notations for each item of evidence. If possible, have one person serve as evidence custodian (Federal Bureau of Investigation 2003).
6. Two persons should observe evidence in place, during recovery, and being marked for identification. Mark directly on the evidence when necessary, but first attempt to place identifying marks on evidence containers (Federal Bureau of Investigation 2003).
7. To avoid damage to potential evidence, remove any floppy disks that are present, package the disk separately, label the package and do not remove CDs or touch the CD drive (National Institute of Justice 2001).
8. Identify storage devices that need to be seized; these devices can be internal, external, or both.
9. Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following cases applies and follow the steps for that case:
 - a. **Case 1:** Monitor is on and desktop is visible.
 - i. Photograph screen and record information displayed (National Institute of Justice 2001).
 - ii. Records make model and serial numbers (National Institute of Justice 2001).
 - iii. Photograph and diagram the connections of the computer and the corresponding cables (National Institute of Justice 2001).
 - iv. Label all connectors and cable ends [including connections to peripheral devices] to allow for exact reassembly at a later time (National Institute of Justice 2001).
 - v. Isolate the network [Depends on the case as mentioned before].
 - vi. Perform order of volatility and collect the volatile data that would be lost when the system is turned off, and identifying any suspicious processes that are running on the system then follow digital evidence acquisition procedures which will be discussed later in the digital forensic phase.
 - vii. Record in notes all actions taken and any changes that observed in the monitor, computer, printer, or other peripherals that result from the performed actions (National Institute of Justice 2001).
 - viii. Remove the power source cable from the computer not from the wall outlet [Decision of shutting down the computer depend on the case] and then start packaging procedures.
 - b. **Case 2:** Monitor is on and screen is blank [sleep mode] or screen saver [picture] is visible.
 - i. Move the mouse slightly [without pushing buttons]. The screen should change and show work product or request a password (National Institute of Justice 2001).
 - ii. If mouse movement does not cause a change in the screen, don't perform any other keystrokes or mouse operations (National Institute of Justice 2001).
 - iii. Continue with all the steps of case 1.

- c. **Case 3:** Monitor is off.
 - i. Document that the monitor is off, then turn the monitor on, then determine if the monitor status is as described in either case 1 or 2 above and follow those steps.
 - ii. If the computer itself is off then start packaging procedures.

10. Packaging procedure:

- a. Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packaging (National Institute of Justice 2001).
- b. Pack magnetic media in antistatic packaging [paper or antistatic plastic bags] (National Institute of Justice 2001).
- c. Avoid using materials that can produce static electricity, such as plastic bags (National Institute of Justice 2001).
- d. Avoid folding, bending, or scratching computer media.
- e. Ensure that all containers used to hold evidence are properly labeled (National Institute of Justice 2001).
- f. Label each package with a unique label (Association of Chief Police Officers), which must include some details as name of the person and organization that packed the material , the content of package , the place where it is going to be packed and from where it was taken, and the time and date of packing.

11. Transportation procedure:

- a. Keep electronic evidence away from magnetic sources.
- b. Don't store electronic evidence in vehicles for long periods of time as different temperature and weather conditions can damage evidence.
- c. Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations (National Institute of Justice 2001).
- d. Maintain the chain of custody on transported evidence.

12. Storage procedure: Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants (National Institute of Justice 2001).

13. Seal all evidence packages at the crime scene.

14. Constantly check paperwork, packaging, and other information for errors.

2.2.6 Final survey and reconstruction for physical crime scene

- 1. Discuss the search with all personnel, then ensure all documentation is correct and complete (Federal Bureau of Investigation 2003).
- 2. Photograph the scene showing the final condition (Federal Bureau of Investigation 2003).
- 3. Ensure all evidence is secured, ensure all equipment is retrieved and ensure hiding places or difficult access areas have been overlooked (Federal Bureau of Investigation 2003).
- 4. Analyze any Non digital evidence that can help in the case [as finger prints, paper, etc.].

5. Reconstruct the events that occurred at the crime scene by using the crime scene appearance, the locations and positions of the physical evidence, the forensic laboratory analysis results, and the scientific method.

2.3 Laboratory Examination Team Responsibilities

Laboratory examiners are responsible for the digital crime scene or secondary scene. The laboratory examiners team should include digital evidence recovery experts, cyber forensic analysts and intelligence gathering specialists. Each case is unique and the judgment of the examiner should be given deference in the implementation of the procedures suggested. Investigation in the digital scene should be followed according to the digital forensic phase. This phase works in parallel or after the physical forensic and investigation phase according to the case nature. The goal of this phase is to identify and collect the electronic events that occurred on the system and analyze it, so that it can be used with the results of the previous phase to reconstruct events. It includes sub phases which are survey the digital scene, evaluation and assessment, acquisition of digital evidences, digital evidence examination, reconstruction of extracted data and conclusion.

2.3.1 Evaluation and assessment

1. Determine the evidence that was seized.
2. Determine additional information regarding the case as aliases, e-mail accounts, e-mail addresses, Internet Service Provider [ISP] used, names, network configuration and users, system logs, passwords, user names.
3. Assess the skill levels of the computer users involved knowing that skilled users can use complex ways to cover their crime.
4. Prioritize the order in which evidence is to be examined (Federal Bureau of Investigation 2003).
5. Determine if additional personnel or equipment will be needed.
6. Identify and evaluate storage locations in which the evidences were stored.
7. Identify proprietary software and the operating system in question.
8. Ascertain the condition of the evidence as a result of packaging, transport, or storage (National Institute of Justice 2004).
9. Assess the need to provide continuous electric power to battery-operated devices (National Institute of Justice 2004).
10. Verify operation of the examiner's computer to include hardware and software (National Institute of Justice 2004).

2.3.4 Acquisition of digital evidences

Collecting of data can be done on a life system or on a shutdown system

1. Life System Case :

- a. Prepare an order of volatility in which the order of collection should be from most volatile to the least. Order of volatility can be:
 - i. Registry, cache.
 - ii. Routing table, ARP cache, process table and kernel statistics.
 - iii. Memory.
 - iv. Temporarily internet file.
 - v. Disk.

- vi. Remote logging and monitoring data that is relevant to system in question.
 - vii. Physical configuration, network topology.
 - viii. Archival media.....
- b. Prevent outside interference and prevent execution of programs on a crime scene computer.
 - c. Start collection log file and create in it sub-directory to hold the evidence image.
 - d. Document the details of the investigation in the log file including investigator details, case background details, investigation dates and investigators digital signatures.
 - e. Document details of the disk media including investigator name and organization, case number, media evidence number, date and time imaging was done, name, model and serial number of computer, IP and system host name, make model, and serial number of hard disk [HD], internal storage devices and hardware configuration and scope of investigation.
 - f. Capture an accurate image of the system as soon as possible with minimum tampering or change in the system.
 - g. Command line tools are preferred than GUI interface tools, and use safe and tested tools.
 - h. Collect volatile data present on registry as:
 - i. System time and date and running processes.
 - ii. Currently open sockets, application listening on open sockets, current users logged on and system currently or recently connected.
 - i. Use cash monitoring tools to view real time state cash and document it then dump memory information using tools running from CD and save the result on floppy or another CD.
 - j. Use network monitors, system monitors, surveillance cameras for activity monitoring.
 - k. Obtain network-based evidence from sources such as intrusion detection systems, routers, firewalls, log servers, etc., make sure that time is synchronized between of all logs and systems.
 - l. Before imaging use write protectors or write blocker tools to insure the integrity of information gathered from disk.
 - m. In this case the subject computer will be used to acquire digital evidence, attach the examiner's evidence storage device as hard drive and tape drive.
 - i. Ensure that the examiner's storage device is forensically clean when acquiring the evidence (National Institute of Justice 2004).
 - ii. Investigate the geometry of any storage devices to ensure that all space is accounted for, including Host protected area [HPA] data and device configuration overlay option [DCO] (National Institute of Justice 2004).
 - iii. The examiner should calculate a mathematical value for the subject evidence before acquiring the evidence as performing an independent cyclic redundancy check [CRC] or hashing.

- n. Acquire data of the disk by making bit stream copy of the original storage medium, which is an exact duplicate of the original disk and this is also done for all evidence storage medium as floppy disks, which is done by using one of these methods:
 - i. Creating a bit stream disk to image file: which is the most common type, as it provide the investigators the ability to make many copies of the digital evidence acquired, and also this image can be used with a lot of applications and other tools to continue the forensic stages.
 - ii. Making bit stream disk to disk copy: Used if the investigator is unable to create bit stream disk to image file.
- o. Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools, such as: (National Institute of Justice 2004)
 - i. Stand-alone duplication software.
 - ii. Forensic analysis software suite.
 - iii. Dedicated hardware devices.
- p. Verify the integrity of the information gathered by making hash values and checksums for both the image and the original data and comparing them.
- q. Change the read-write permission of the image to read only.
- r. Retrieve configuration information from the suspect's system through controlled boots (National Institute of Justice 2004).
- s. Perform a controlled boot to capture CMOS/BIOS information and test functionality (National Institute of Justice 2004).
 - i. Boot sequence [this may mean changing the BIOS to ensure the system boots from the floppy or CD-ROM drive].
 - ii. Time and date and then document it.
 - iii. Power on passwords.
- t. Disconnect storage devices and perform a second controlled boot to test the computer's functionality and the forensic boot disk (National Institute of Justice 2004).
 - i. Ensure the power and data cables are properly connected to the floppy/CD-ROM drive.
 - ii. Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.
- u. Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS (National Institute of Justice 2001).
 - i. Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.
 - ii. Drive configuration information includes logical block addressing [LBA]; large disk; cylinders, heads, and sectors [CHS]; or auto-detect.
- v. Collect evidences from removable media sources such as backup tapes, floppy disks, CD-ROM, etc.
- w. Power system down by removing the power cable and then remove and acquire storage device of the suspect, if possible.

- x. Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system: (National Institute of Justice 2001)
 - i. RAID, removing the disks and acquiring the individually may not yield usable results.
 - ii. Laptop systems, the system drive may be difficult to access or may be unusable when detached from the original system.
 - iii. Hardware dependency [legacy equipment], older drives may not be readable in newer systems.
 - iv. Equipment availability, the examiner does not have access to necessary equipment.
 - v. Network storage. It may be necessary to use the network equipment to acquire the data.
- y. Prepare chain of custody in which gathering process must be documented which should include timestamp, digital signatures and signed statements.
- z. Duplicate the evidence disk drive, perform at least two copies.

2. Computer already shutdown:

Never turn on or operate suspects computer during investigation if it is off leave it off

- a. Determine disk structure, model and size (National Institute of Justice 2001).
- b. Before imaging use write protectors or write blockers tools to insure the integrity of information gathered from disk.
- c. Remove and acquire storage device of the suspect using the examiner's system, then configure it on the examiner's system to be recognized.
- d. Exceptional circumstances that may result in a decision not to remove the storage devices from the subject system are mentioned above in section x in the live system case.
- e. Avoid tools that use a GUI interface, command line tools are preferred and use safe and tested tools.
- f. Then follow steps from n-q in the live system case.
- g. Prepare chain of custody in which gathering process must be documented which should include timestamp, digital signatures and signed statements.
- h. Duplicate the evidence disk drive.

2.3.3 Survey the digital scene

Survey phase is performed on a live system or on the snap shot image. It can occur on a live system, similar to what occurs in the physical world. Mostly it occurs in a lab using one of the digital crime scene replica images as it is preferred because it provides a controlled environment and the results can be repeated with another copy of the system

It examines the obvious locations for evidence and develops strategy for how to search the system for additional evidence, it also provides details and description about data as to be used in extraction activities and it shows the skill level of the suspect.

2.3.4 Digital evidence examination

The purpose of the examination process is to locate, extract and analyze digital evidence to reconstruct the crime scene. Extraction refers to the recovery of data from its media. Analysis refers to the interpretation of the recovered data and putting it in a logical and useful format (National Institute of

Justice 2004).

Examination of the evidence will involve the use of a potentially large number of techniques to find and interpret significant data, while doing so it must preserve the integrity of evidence and chain of custody to present it in court. General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose (National Institute of Justice 2004).

When conducting evidence examination, consider using the following steps:

1. **Preparation:** Prepare working directories on separate media to which evidentiary files and data can be extracted and recovered (National Institute of Justice 2004) and start the lab evidence log from the case management system to record details of examination and the state of evidence at arrival.
2. **Locating evidence:** Making a checklist can help in the examination process, and can be used it to double-check that everything is there.

This step depends on the case and the type of operating system used. There are some areas and files in each operating system that are recommended for evidence gathering, but also this depends on the case. The common areas are:

a. Windows operating system:

1. Files and file system: Using command lines tools can help investigator to ascertain and examine the time, date of installation of the operating system, service packs, patches and subdirectories like drivers that automatically update themselves.
2. Hidden files: such as NTFS alternate data streams that can be detected by the help of tools searching on registry, locate data in hidden or masked file extensions.
3. Detect unusual or hidden files by modifying Windows to display certain hidden file types.
 - a. Compressed files, misnamed files, encrypted files and password-protected files.
 - b. File attributes
 - c. Security ID : Microsoft Security ID are found on registry in profile list that holds profile list key for each user on computer
4. Slack space: The space existing at the end of the file of the last cluster that contains data from computer
5. Windows registry: windows registry is a database where all the information about a computer is stored. The registry is used to store :
 - a. Operating system configuration, application configuration information and hardware configuration information.
 - b. User security information and Current user information.
6. Locate evidence from the Windows print spooler and enhanced metafiles [EMF] files. Even if a user never saved a word-processing document, temporary versions of word-processing documents sometimes remain on the hard drive.

b. Linux/ Unix operating system:

1. Mount the restored imaged working copy and start analyzing the contents.

2. Use the ls command to view the contents of the disk. [ls -aR to list all files including hidden files and list the directories recursively].
3. Make a list of all files along with access times, and search for likely evidence using grep command.
4. List unknown file extensions and changed file appearance.
5. Search in such areas:
 - a. Syslog: This is the heart of Linux logging.
 - b. File access time.
 - c. Detect unusual or hidden files, compressed files, Misnamed files, Encrypted files and Password-protected files.

c. For both operating systems :

Search in such areas:

1. Temporarily internet files, cookies and batch files [*.bat].
2. Memory, it also identifies network logon names, passwords and other sensitive information.
3. Swap files: is space on a hard disk reserved for the operating system to do what's called paging and which is called Virtual memory [The swap file is called win386.swp in windows and in windows NT/2000/XP, it is called pagefile.sys.].
4. Unallocated clusters, unused partitions, hidden partitions, HPA and DCO.
5. Destroyed or deleted Partitions, files and data [The index application in windows locates data that has been destroyed].
6. Locate and retrieve e-mail evidence. E-mail messages can be found in a number of different places, such as the sender's e-mail inbox/outbox a network server's mailbox, or backup media.
7. Scan for backdoors and network sniffers.
8. Locate root kits or viruses.

3. Extracting evidence: There are two different types of extraction, physical and logical.

a. Physical extraction:

During this stage the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive. This may include the following methods: keyword searching [make a list of keyword search], file carving, extraction of the partition table and unused space on the physical drive (National Institute of Justice 2004),and examining the partition structure which may identify the file systems present and determine if the entire physical size of the hard drive is accounted for.

b. Logical extraction:

During this stage the extraction of the data from the drive is based on the file system(s) present on the drive and may include data from areas as active files, deleted files, file slack, and unallocated file space (National Institute of Justice 2004), steps may include:

1. Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location (National Institute of Justice 2004).
 2. Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values (National Institute of Justice 2004).
 3. Extraction of files pertinent to the examination. Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive (National Institute of Justice 2004).
 4. Recovery of deleted files and partitions and extract information from startup and configuration files.
 5. Extraction of password-protected, encrypted, and compressed data as well as file slack and unallocated space.
 6. Determine data relevance, keep in mind, however, that it needs to be fast; don't waste time collecting information that will be of no use to the case (Schweitzer 2003).
 7. Extract IDS, Router, Firewall, application and authentication log files.
 8. Extraction of e-mails and deleted e-mails from .pst [personal e-mail files] and .ost [offline e-mail files] files or from history, cookies and temporarily internet files.
- 4. Reconstruction of extracted data:** Once the evidence is gathered and extracted, it can be used to reconstruct the crime to produce a clear picture of the crime and identify the missing links in the picture.

There are three fundamentals of reconstruction for investigating crimes, which are: temporal analysis, relational analysis and functional analysis.

Temporal analysis tries to discover some factors such as what happened and who are involved, while relational analysis facilitate the reconstruction by correlating the actions of suspected victim, at the same time functional analysis discovers how the activities or actions actually happened and discovers the responsible factors. There are many analysis techniques used to present significance of evidences, it's not a must to use all these techniques in all the cases, but it depends on the case nature, some of these techniques are:

- a. Timeframe analysis:** Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred. Two methods that can be used are: (National Institute of Justice 2004).
 1. Reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation.
 2. Reviewing system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs, etc.
- b. Data hiding analysis:** Digital systems can easily hide data. Using data hiding analysis can be useful in recovering some important information which may indicate knowledge or ownership... Methods that can be used include:
 1. Correlating the file headers to the corresponding file extensions to identify any mismatches and analyze the file signatures to detect hidden data.

2. Analyze all password-protected, encrypted, and compressed files, knowing that the password itself may be as relevant as the contents of the file.
 3. Gaining access to a HPA, the presence of user-created data in an HPA may indicate an attempt to conceal data. (National Institute of Justice 2004)
- c. Application and file analysis:** Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user. Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes (National Institute of Justice 2004). Some examples include: Reviewing file names for relevance and patterns.
1. Examining file content which may contain evidence or indicates possession to a specific user.
 2. Correlating the files to the installed applications (National Institute of Justice 2004).
 3. Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments (National Institute of Justice 2004).
 4. Examining the users' default storage location(s) for applications and the file structure of the drive to determine if files have been stored in their default or an alternate location(s) (National Institute of Justice 2004).
 5. Examining user-configuration settings. Analyzing file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it (National Institute of Justice 2004).
- d. Log Files analysis:**
1. Analyze network traffic and analyze each network packet.
 2. Analyze IDS logs and monitor security events.
 3. Perform Protocol analysis and content searching /matching for each packet.
 4. Investigate and analyze Router Logs:
 - a. Syslog logging
 - b. Buffer Logging
 - c. Console logging
 - d. Terminal logging
 - e. SNMP logging
 - f. Access Control List [ACL] logging
 5. Investigate and analyze firewall and switch logs.
 6. Investigate and analyze Application server logs.
 - a. Errors generated and its time
 - b. E-mail server logs
 - c. Logins , executed commands
 - d. Database logs
 - e. Authentication Logs

- f. Operating system log files
7. Correlate log files to get the whole picture in case of network attacks.
- e. Analysis of e-mail messages:**
 1. View e-mail header: which contain information email origin, and how it reached and who send it [The header can be faked except the "received" portion-referencing.].
 2. Trace email regarding Internet domain using source IP address in header.
 3. Verify the validation of e-mail path by checking in router [check ID of message] and firewall logs and analyze logs from e-mail server.
 4. Contact the e-mail provider in the case of web based e-mail [source] to reveal suspects information.
- f. Network analysis:**
 1. Analyze any abnormal system processes, port files and services using commands already on the system or third-party tools.
 2. Analyze startup files to analyze any unauthorized system modification and Check for unusual ports listening for connections from other hosts.
 3. Inspect network configurations for unauthorized entries.
 4. Identify initiating IP address, source port, service, date and time.
 5. Identify unauthorized network trusts.
- 5. Conclusion:** Results obtained from any one of these steps may not be sufficient to draw a conclusion (National Institute of Justice 2004).When viewed as a whole; however, associations between individual results may provide a more complete picture. As a final step in the examination Phase, consider the results from both physical and digital forensics phases, and organize the analyses results from collected physical and digital evidences to link a person to the digital events.

2.4 Courtroom Team Responsibilities

The courtroom team is responsible of reporting and presenting the case, experienced expert witness testimony provided in courts, ensure the chain of custody during all the previous phases and also responsible for the closure phase. This team should consist of both technical professionals and prosecutor who is a member of the legal profession who is responsible for presenting the case against the suspect in court of law. This team should have basic knowledge of forensic computer concepts together with familiarity with legal issues pertaining to seizure and search of computer systems and digital evidence.

2.4.1 Reporting and Presentation Phase

Reporting is a vital importance in digital forensic case. This Phase though is based entirely on policy and law of each country, which are different for each setting. It presents the conclusions and corresponding evidence from the investigation.

Writing a good and comprehensive report increase the chance of convincing the judge and winning the case. Report does not only including communicating facts, but it also presents the expert opinion. The presentation(s) are intended to provide both detailed confirmatory and event reconstruction information (Beebe & Clark 2004). This report should:

- Document whether or not the allegations were substantiated.

- It must be organized in a way, so that anyone who reads it can understand it without reference to any other material, so while writing the report must include any related documents such as log files and pictures.
- Present evidence as testimony. Also fees paid for expert's service and list of all list of civil and criminal cases in which the expert has testified for the preceding four or five years must be included.

It is preferred to be in PDF format and it should be communicable. No assumptions should be made while writing the report. If something important is discovered include it in the report. Writing should be brief, grammar and spelling must be checked and repetition of word and difficult and slang words should not be used. A good report should have the following features:

- Identity of the reporting agency, case identifier or submission number, investigators and examiners of the case and their signatures, identity of the submitter, date of receipt and report, description of collection and examination procedures, descriptive list of items submitted for examination, including serial number, make and model, providing uncertain and error analysis and conclusions explanation.
- Should include all log files generated by forensic tools to keep trace of all the steps taken.
- Summary and details of findings.

Details of finding should describe in detail the results of the examinations and may include:

- Specific files related to the request and other files, including deleted files that support the findings (National Institute of Justice 2004).
 - String searches, keyword searches, and text string searches (National Institute of Justice 2004).
 - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity (National Institute of Justice 2004).
 - Graphic image analysis (National Institute of Justice 2004).
 - Ownership indicators.
 - Data analysis.
 - Techniques used to hide or mask data, such as encryption, Steganography, hidden attributes, hidden partitions, and file name anomalies (National Institute of Justice 2004).
- List supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation (National Institute of Justice 2004).

2.4.2 Closure Phase

The closure phase involves reviewing the whole case in which it reviews the investigation to identify areas of improvement. It also examines how well each of the physical and digital investigations worked together, and whether the evidences collected were enough to solve the case. The purpose of this phase is to:

- Review the entire process and investigation procedures.
- Collect and preserve all information related to the incident.
- Return the physical and digital properties to their owner.
- Determine what criminal activities must be removed.
- Eradicate system information and apply counter measures to prevent such crimes from

happening again on the system.

The Closure documentation should be performed which include the time and date of release, to whom and by whom released.

3. MODEL DISCUSSION AND CONCLUSION

Knowing the fact that technology is becoming more intertwined in the daily life of the individual will lead to an increase in court cases where digital evidence is a vital component. This requires increase in expertise in the digital forensic investigation area and also requires standardizing the forensic steps taken by investigators. Guidance for these experts to perform the investigation without alerting the integrity of evidences is a must. Therefore this model is presented which is based on both theoretical and practical experiences. It has unique benefits over other models as it gives a deep level of detailed steps for each phase and defined the required teams to perform these phases, presenting detailed responsibilities for each team. It is practical and involves steps that actually investigators do during investigation, general with respect to technology so that it won't be limited to present technologies at the same time it is specific enough so that each of member of each team knows his role.

The proposed model also covers the most popular operating systems windows, UNIX and Linux, and it is technology neutral so it can be used in different platforms and on different cases.

It also presents the needed people or experts in each team to perform each phase of digital investigation which can help organizations in building their labs. This model allows technical requirements for each phase to be developed and identifies interaction between physical and digital investigations. It is abstract enough that it can be applied to both law enforcement and corporate scenarios.

This model also included physical forensics which is already recognized. This will increase the court acceptance of the cases and add credibility to the analysis results from the digital world.

4. REFERENCES

- Marcella J. Albert and Greenfield S. Robert (2006), 'Cyber Forensics', www.cyber-forensic-analysis.com.
- Asian School of Cyber Laws (2006), 'Asian School of Cyber Laws' www.asianlaws.org, 12/2006.
- Association of Chief Police Officers (2005), 'Good Practice Guide for Computer based Electronic Evidence', available at: www.nhtcu.org.
- Beebe, N. & Clark, J. (2004), "A hierarchical, objectives-based framework for the digital investigations process", Paper presented at the DFRWS, June 2004, Baltimore, MD.
- Carrier Brian (2002), 'Open Source Digital Forensics Tools, The Legal Argument', Stake Research Report, www.atstake.com.
- Carrier Brain (2006), 'A Hypotheses-based Approach to digital Forensic investigations', A thesis Submitted to the Faculty of Purdue University , In Partial fulfillment of the requirements for the degree of Doctor Philosophy.
- Federal Bureau of Investigation, Revised 2003, Handbook of Forensic Services , www.fbi.gov,An FBI Laboratory Publication Federal Bureau of Investigation Quantico, Virginia.
- Hall A. Gregory, Wilbon P. Davis (2005), "Toward Defining the intersection of Forensics and Information technology", International Journal of Digital Evidence, Volume 4 (Issue 1).
- National Institute of Justice (2001), 'Electronic Crime Scene Investigator, A Guide for First Responders', <http://www.ncjrs.org/pdffiles1/nij/187736.pdf>.
- National Institute of Justice (2004), 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement', <http://www.ojp.usdoj.gov/nij> .

Palmer Gary (2001), 'A Road Map for Digital Forensic Research', Technical Report DTR-T001-01, DFRWS, Report From the First Digital Forensic Research Workshop (DFRWS).

Schweitzer Douglas (2003), Incident Response Computer Forensics Toolkit, Wiley Publishing, Inc, Indianapolis, Indiana, Chapter 7.

Wright E. Timothy (2001), 'Field Guide' found on www.securityfocus.com/static/submissions.html.