Computer Forensic
Evidence Collection and Management

Chapter 7

Managing the Crime/Incident Scene

Chapter Objectives

- Understand the requirements for managing the incident/crime scene.
- Become familiar with the responsibilities of the first responder at an incident site
- Identify those steps necessary to make electronic evidence admissible in court
- Look at the issues relating to electronic and computer crime-scene investigations
- Identify the various players involve I an electronic/computer investigation.
- See how electronic forensics provides support in solving crimes
- Look at the investigative differences between corporate security and those law enforcement.

Introduction

- The initial response to an incident involving computers or electronic evidence can originate from a variety of sources.
- Specific responsibilities include protecting the incident scene, preserving evidence, collecting evidence, and submitting the evidence for further analysis.
- First responders and computer forensic experts have to confirm with many rules and regulations if the evidence they uncover is to be acceptable to the courts.
- The first step tin obtaining computer forensic evidence is getting a search warrant to seize the suspect.
- If it is thought that the evidence is contained in e-mails, this also should be specifically mentioned in the search warrant.
- In all circumstances, data not connected to the crime must mot be touched.

Scope of a problem

- Criminal activities are proliferating in our society with the help of computers and related electronic devices.
- Members of law enforcement must posses current knowledge, resources, and equipment to effectively investigate today's criminal activity.
- Illegal activates and violations of corporate security and computer-use policies are escalating.
- Computers, electronic devices, and digital media are increasingly used in unlawful activities.

The Incident Scene

- The first responders to an incident/crime scene have the responsibility of protecting any all computer and electronic evidence that might be useful in future civil and criminal actions.
- Computer and electronic evidence is more subtle and might no be evident to obvious at the incident scene.
- Investigators must take a broader view of the incident scene to include other possibilities such as computer forensic evidence.
- Much of this potential evidence might be circumstantial, but it could possibly be used to support the primary physical and direct evidence that bee developed.

Scope of a problem (Cont.)

The Initial Response

- A law enforcement agency investigating a crime scene could identify a number of computers and other electronic devices that might contain electronic evidence relevant to the current criminal investigation.
- Valuable evidence can be lost by careless and improper handling by untrained personnel.
- A prompt assessment of the situation must be made, usually with limited information.
- Answers to the following questions will better prepare the first responder in determining the role of the computer or electronic devices in some potential illegal activity.
  - Are any of the hardware or software components stolen?
  - Did the suspect use the system to commit some offense?
  - Is the computer used to store evidence of some offense?
  - Did a computer intruder use the computing device to attack other systems and to store stolen credit card information?
  - Was the device used in violation of a corporate security policy?
- Procedure for initiating the documentation and audit trail are similar for al investigations.
- The investigator receiving the initial complaint must record the incident in some type of log or journal
- Investigators must decide what, if nay, evidence can be collected from the incident scene.
- While the computer forensic expert needs to uncover evidence, care must be exercise to protect the personal information of any innocent third parties.

Crime Scene Investigation

- The purpose of a crime scene investigation is to establish events that occurred and to identify those responsible.
- This is done by carefully documenting the conditions at a crime scene and recognizing all relevant physical evidence.
- A crime scene investigation is a difficult and time-consuming job.
- A investigator must not leap to conclusions as to what happened based upon limited information, but must keep an open mind regarding evidence collected at the scene.

Electronic and Computer Investigations

- Most police investigation begin at the scene of a crime. This is usually not true with computer system investigations.
- The scene is simply defined as the actual site or location in which the incident took place.
- The scene should be secured by establishing a restricted perimeter. The purpose of securing the scene is to restrict access and prevent evidence destruction.
- Once the scene is secured, the restrictions should apply to all nonessential personnel, including law enforcement personnel.
- An investigation may involve a primary scene as well as several secondary scenes at other locations.
- The protocol for critical incident management being taught today identifies a three-layer or three-tier perimeter:
  - The outer perimeter
  - The inner perimeter
  - The core or scene itself.

Physical Evidence at a Crime Scene

- Evidence used to resolve an issue can be categorized as:
  - Testimonial evidence: any witnessed accounts of an incident
  - Physical evidence: any material items that would be present on the crime scene

- These items would be presented in legal proceeding or corporate investigations to prove or disprove the facts of an issue.
  - The investigator might use evidence collected at the incident scene to:
  - Prove that a crime has been committed or a policy violation exists
  - Link a suspect with a scene or a victim
  - Establish any key elements or a crime or incident
  - Establish the identify of a victim or suspect
  - Corroborate verbal witness testimony
  - Exclude those not involved.

Type of Evidence

Evidence identified and collected will fall into two general categories:

- **Those involving petty crimes and felonies**
- Evidence may include:
  - Impressions from fingerprints, tool marks footwear, fabrics, tire marks, bite marks
  - Human matter my include blood, semen, body fluids, hair, nail scrapings, and bloodstain patterns
  - Weapon evidence may include gunshot residues, weapons gunpowder patterns, casings, projectiles, fragments, pellets, wadding, and cartridge.
  - Miscellaneous evidence might include arson accelerant, paint, glass, and fibers

- **Those involving computer and electronic crimes concerning corporate policy violations.**
  - Evidence may include:
    - Desktops computers, laptops, printers, copiers, cell phones, personal digital assistants (PDAs), CDs, floppy disks, USB memory sticks, digital cameras, Zip disk hard drives and any other device that has a storage capacity.

Processing the Crime Scene

An organized approach is a sequence of established and accepted duties and protocols. An organized approach ensures the following activates:

- Conducting through and legal search
- Expeditious processing of evidence without compromise
- Complete scene documentation
- Utilization of standard methods and techniques for evidence recovery
- Understanding use and knowledge of resources and equipment
- Ensuring all pertinent evidence is recovered
- Proper handling and packaging of evidence
- Distributing evidence to labs for analysis
- Following safety precautions.

There are three basic and simple states in properly processing the crime scene.

Evidence Recognition and Identification

- The recognition or identification of evidence begins with the initial search of the scene.
- The search can be defined as the organized and legal examination of the crime scene to locate items of evidence to the incident or crime under investigation.
- Factors such as the number of searchers, the size of the area to be searched, type of evidence, etc. are used to determine the method or pattern to be employed in the crime scene search.
- A plan of operation can be developed and initiated fro an initial walk-through of the scene.
- The incident scene must be preserved with minimal contamination and disturbance of physical evidence.

Processing the Crime Scene (Cont.)

Scene Documentation

- In the documentation stage of an organized approach for processing the crime scene all functions have to correspond and be consistent in depicting the crime scene.
- An incident scene sketch will be useful later in the investigation.
- Consideration of hazards or safety conditions may also need to be addressed.

Evidence Collection

- The evidence collection or recovery step in crime scene processing include the methods, techniques, and procedures used in retrieving evidence.
- Teamwork in crime scene investigations is essential.
- The work done at a crime scene is very challenging and time consuming. The investigator's imagination will determine the process of retrieving the evidence and the time frame involved.
- Documenting computer crime scene conditions can include immediately recording transient details.
- In additions, it is important to be able to recognize what should be present at the scene, but is not, and objects that appear to be out of place.
- A crime scene is not merely the immediate area where a suspected concentrated his or her activities, but is also adjacent areas, off-site areas, and vehicles.
- Although there are common items frequently collected as evidence, literally any object can be physical evidence.

Issues and Warnings when Seizing Evidence

- Only evidence relevant to a case can be seized by investigators. Knowing the role of the computer will indicate what should be taken.
- Any suspects present must be prevented from touching the computer devices. A computer that is running at the time of seizure should not be allowed to shut down, as this sequence might delete valuable evidence.
- When a computer and its peripherals are removed from a crime scene, a great deal of care has to be taken while dismantling the equipment to prevent any malicious programs from being activated should the computer power system be booby trapped.
- The entire setup should be photographed or a video taken before starting disassembly; notes should be taken at every stop; and every cable should be labeled starting where it was attached.
- A number of issues are unique to investigating and prosecuting computer and electronics criminal cases. First, the investigation may interfere with the normal conduct of the organization's business.
  - Several additional considerations that must be addressed include:
  - There is a compressed time frame for the investigation
  - Experts might be required and might not be available.
  - Some jurisdictions define electronic evidence differently
  - Locations of the crime are geographically dispersed.

Issues and Warnings when Seizing Evidence (Cont.)

Computer and electronics chain-of-custody checklist

Computer and Electronics Chain of Custody Checklist

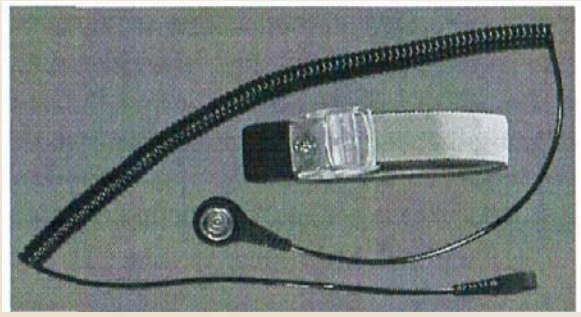
☐	Created unique case and evidence number
☐	Documented some asset tag or serial number that uniquely identifies the evidence
☐	Document make and model of system the data was taken from
☐	Documented BIOS time
☐	Documented location the evidence was found in (inside case, inside drawer of desk, inside briefcase)
☐	Documented physical description of evidence
☐	Annotated notes for any accesses to the evidence before you arrived
☐	Annotated notes for any step that occurs outside of your normal process
☐	Filled in history annotating when you received the drive and from whom
☐	Updated chain of custody for each action taken with the original evidence

Computer and electronics evidence receipt checklist

Computer and Electronics Evidence Receipt Checklist

☐	Took evidence with authorization
☐	Created unique case and evidence number
☐	Documented some asset tag or serial number that uniquely identifies the evidence
☐	Received signature from owner or manager
☐	Noted date and time of seizure
☐	Completed receipt for all evidence taken
☐	Provided copies to owner or manager

Static-ground devices



Steps for a Crime/Incident Scene Search

- Education and preparation are major components of a successful crim scene search for electronic evidence.
- Some of the steps involved also apply to crime scene searches for crimes involving misdemeanors and felonies; however the orientation device might be a tool what was used in committing a crime, which means that normal-evidence-gathering techniques for forensics processing should be followed.
- The basics steps are:

Secure and Protect Scene

- It is essential to secure and protect the area comprising the computer system in questions.
- It is also essential that the organization's computer personnel be excluded from the area.
- Document anyone who has access to the site or anyone who might have a reason to be involved with the computer site.

Steps for a Crime/Incident Scene Search (Cont.)

Initiate Preliminary Survey

- Computer and electronic evidence usually takes on the same form: computers, peripherals, cell phones, PDAs, various storage media, digital cameras, tec.
- A cautions walk-through is a good first step to get a feel for the complexity of the sites.
- Due to the networking capabilities of computer system, even remote sites or vehicles might become involved in the investigation.
- Specific activities that might be included in this phase of the investigation include:
  - Determine all the locations that might need to be searched.
  - Look for any specifics that must be addressed relating to hardware and software
  - Identify possible personnel and equipment needs for the investigation.
  - Determine which devices can be physically removed from the site
  - Identify all individuals who had access to the computer or electronic resources.

Evaluate Physical Evidence Possibilities

- This step is continuation for the preliminary survey and may not be perceived as a separate step.
- After the site is thoroughly photographed, a more detailed search can begin.
- Any network capability and connections to the computer site must be identified.
- Prioritize the evidence collection process to prevent loss, destruction, or modification.

Steps for a Crime/Incident Scene Search (Cont.)

Prepare Narrative Description

- A journal or narrative must be prepared concerning the investigation and the crime scene search.
- Describe the site in broad terms and then get very specific with details.
- The narrative effort should not degenerate into a sporadic and unorganized attempt to reover physical evidence.

Take Photographs of Scene

- Developing a photographic profile of the crime scene is a requirement for compute forensic investigations. Any video screens being displayed would be photographed.
- Specifics for identifying and capturing photographic evidence are as follows:
  - Capture overall, medium, and close-up views of various items of computer and electronic evidence
  - Use a scale device such as ruler for size determination
  - Take a photograph of the item with and without the scale device
  - Photograph the item in place before its collection and packaging
  - Photograph any item or place that might corroborate the statements of a suspect or witness
  - Take crime area photographs from eye level
  - More is better-film is cheap; consider digital
  - Prior to lifting latent fingerprints, photograph should be a 1:1 ration

Steps for a Crime/Incident Scene Search (Cont.)

Photographs

- Photographs should be taken as soon as possible to depict the scene as it is observed before anything is handled, moved, or imitated into the scene.
- There are three positions or views that the crime scene investigator need to achieve with the photographs:
  - Overall scene photographs showing most possible view of the scene
  - Mid-range photographs showing the relationships of times
  - A close-up of the items of evidence.
- Software products and other electronic devices often have a radio frequency identifier sensor attached.
- A photographic log must be maintained for all evidence photographed.

Computer and Electronic Photographic Log

Investigator-	Agency -	Case # -
Camera brand-	Camera lens -	
Film type/brand-	Film speed-	Film/digital -

Photo #	Date/Time	Photo Description/Location

Steps for a Crime/Incident Scene Search (Cont.)

Prepare Diagram/Sketch of Scene

- A diagram or sketch establishes a permanent record of items, conditions, and distance/size relationships. They also supplement the photograph record.
- Sketch a re sued along with the reports and photographs to document the scene.
- A general progression of developing a sketch includes the following steps:
  - Layout the general perimeter of the computer or evidence site
  - Fill in fixed objects such as computer desks, computer systems and peripherals
  - Record the position or location of any evidence
  - Record any relevant measurements or distances
  - Provide a key or legend and some orientation
- Items of information that should appear on the sketch include the following
  - Specific locations
  - Date and time
  - Case identifier
  - Sketch preparer
  - Sketch scale
  - Compass orientation
  - Evidence depictions
  - Measurements
  - Key or legend
- A sketch is simply drawn to show items and the position and relationship of items.

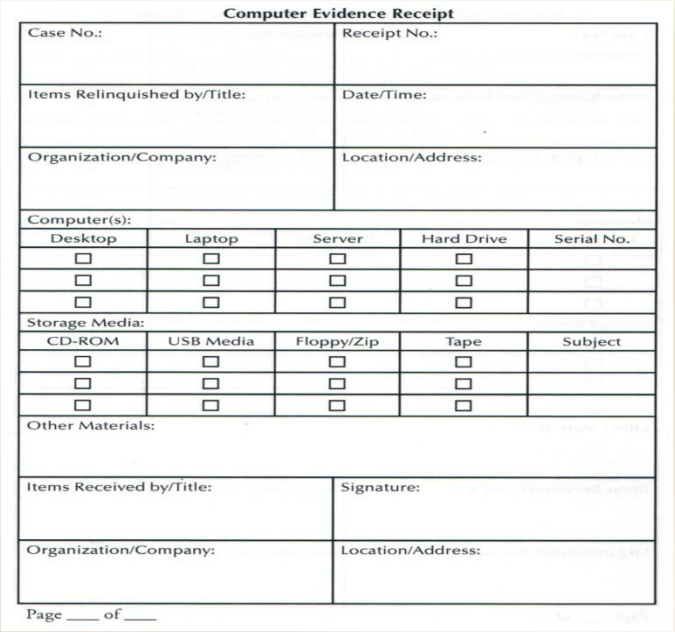
Steps for a Crime/Incident Scene Search (Cont.)

Conduct Final Survey

- After the investigative team has completed all tasks relating to the search, record, and collect phases at the crime scene, a critical review should be conducted to ensure that nothing has been missed.
- A short list will provide assistance to the investigative team:
  - Double-click documentation to detect inadvertent errors
  - Check to ensure all evidence is accounted for before leaving the crime scene
  - Ensure all forensic hardware and software used in the search is gathered
  - Ensure possible hiding places of difficult access areas have not been overlooked.

Release Incident/Crime Scene

- The last step in the evidence investigation phase is to release the incident scene back to the owners.
- The investigation team should provide an inventory of the items seized to the owner/manager of the incident
- A receipt for electronic evidence must be completed for any device seized.



Computer Evidence Receipt

Case No.:	Receipt No.:
Items Relinquished by/Title:	Date/Time:
Organization/Company:	Location/Address:

Computer(s):

Desktop	Laptop	Server	Hard Drive	Serial No.
☐	☐	☐	☐	
☐	☐	☐	☐	
☐	☐	☐	☐	

Storage Media:

CD-ROM	USB Media	Floppy/Zip	Tape	Subject
☐	☐	☐	☐	
☐	☐	☐	☐	
☐	☐	☐	☐	

Other Materials:	
Items Received by/Title:	Signature:
Organization/Company:	Location/Address:

Page ___ of ___

Documentation Procedures

- Reports and other documentation pertaining to an incident must be compile into a case file by the lead investigator or team leaders
- This documentation allows for independent review of work conducted.
- Law enforcement departments and corporate security organizations use a variety of preprinted documents or forms that are designed to record certain aspects of various incident investigations
- Log forms and chain-of-custody forms can be developed that are specific to these electronic and computer investigations.
- There are normally six important categories of documentation that are considered applicable to any search.
  - Journal or narrative description
  - Diagram/sketch
  - Chain-of-custody
  - Photographic log
  - Evidence recovery and receipt
  - Latent print-lift log
- The primary focus in the incident might be oriented toward a computer or electronic investigation and might not include any aspects of a misdemeanor or felony crime; however, a simple corporate computer policy violation might lead to something more significant.

Administrative Audit Worksheet

- The administrative audit worksheet provides for documentation of major events, times, and movements relating to the search efforts.
- It also includes documentation of initial and continuing management and administrative steps taken to ensure that an organized search was accomplished.
- The major benefit from conducting this audit is to ensure all the bases are covered and there are no holes in the investigation.
- Components includes the following:
  - Narrative Description: it describes the general appearance of the incident
  - Photographic log: it provides specific documentation of the process of scene photography that records the overall, medium and close-up views of the incident scene
  - Diagram/Sketch: it provides documentation of physical evidence locations.
  - Evidence Recovery log: it includes documentation of the recognition, collection marking, and packing physical evidence for administrative and chain-of-custody purpose
  - Latent Print-lift log: it provides documentation of the recognition, collection, marking, and packaging of the lifts make for latent prints discovered at the scene.

Personnel Duties and Responsibilities

- The number and qualifications or personnel responding to an incident will depend on the size of the security organization or investigative department.
- Often a single individual might perform al the functions
- Large departments might field a team that includes the following personnel:

Team Leader

- The team leaders assumes control of the incident scene and ensures the safety of the personnel and security of the scene.
- In compute and electronic investigations personnel must use appropriate protective equipment and follow standard recommendations to protect them and the evidence from any electrical hazard.
- Additional responsibilities include:
  - Conduct initial walk-through for purpose of making preliminary survey.
  - Determine search patterns, and make appropriate assignments for team members
  - Designate command-post location and ensure exchange of information
  - Coordinate with other law enforcement agencies or corporate security organizations
  - Ensure that sufficient supplies and equipment are available for personnel
  - Control access to the scene and designate an individual to log everyone into the scene
  - Continuously reevaluate efficiency of search during the entire course of operations
  - Release the scene after a final survey and inventory
  - Access forensic needs and call forensic specialist to the scene

Personnel Duties and Responsibilities (Cont.)

- The computer forensic Investigation checklist is a valuable tool to ensure no steps in the investigation are missed.

Computer Forensic Investigation Checklist

Case No.			Case Name		
Task	Date	Signature	Task	Date	Signature
Case assigned			Preliminary report		
Secure and protect scene			Hard disks imaged (2)		
Initiate preliminary survey			Disks carved and pattern match		
Evaluate physical evidence options					
Photograph scene			Cell phone evidence retrieved		
Prepare diagram and sketch			Electronic media searched		
Prepare narrative description					
Record and collect physical evidence			Final walk-through		
Retrieve hard drives			Release crime scene		
Retrieve media					
Take inventory of evidence					
Packed evidence					
Transported evidence					
Evidence to forensic lab					

Personnel Duties and Responsibilities (Cont.)

Photographer and Photographic Log Recorder

- The photographer's primary responsibility is to record evidence and to prepare a photographic log.
- Major evidence items must be photographed before they are moved.
- The photographers must also coordinate these activities with those who are developing the evidence log and scene sketch.

Sketch Developer

- The primary function of the sketch developer is to diagram the immediate area of the incident scene and orient the diagram with the sketch.
- This team member identifies major items of evidence on the sketch and designates and labels areas to be searched.

Evidence Recorder/Custodian

- The evidence collector, recorder, and custodian are responsible for the evidence integrity and chain-of-custody.
- A primary function is to maintain the evidence log. This includes describing evidence and its location on appropriate bags, containers, or envelopes.
- This person must sign and date evidence containers and maintain the chain-of-custody.

Personnel Duties and Responsibilities (Cont.)

Forensic Scientist or Evidence Recovery Technician

- The forensic scientist or evidence recovery technician is accepted as a forensic specialist. This specialty function provides a professional organized step-by-step approach to the processing of a crime scene.
- They must be well versed in all areas of recognition, documentation, and recovery of physical evidence that may be deposited at the scene.

Specialist and Consultant

- It is sometimes necessary to bring in computer forensic science expertise from an outside agency or organization.
- In high-technology crime cases, both the prosecution and the defense will probably employ a computer scientist.
- There are several important issues that should be considered when contracting for computer forensic specialists:
  - Look at the competence and reliability of the specialist
  - Ensue the specialist will work at a crime scene within law enforcement guidelines
  - Identify the role of the specialist in presenting expert testimony in court
  - Determine the cost in advance when contracting forensic consultants.
- Specialist should be identified before they are needed in an actual case.