CERIAS Tech Report 2003-29

GETTING PHYSICAL WITH THE DIGITAL INVESTIGATION PROCESS

Brian Carrier & Eugene H. Spafford

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907

Getting Physical with the Digital Investigation Process

Brian Carrier Eugene H. Spafford

Center for Education and Research in
Information Assurance and Security – CERIAS
Purdue University

Abstract

In this paper, a process model for digital investigations is defined using the theories and techniques from the physical investigation world. While digital investigations have recently become more common, physical investigations have existed for thousands of years and the experience from them can be applied to the digital world. This paper introduces the notion of a digital crime scene with its own witnesses, evidence, and events that can be investigated using the same model as a physical crime scene. The proposed model integrates the physical crime scene investigation with the digital crime scene investigation to identify a person who is responsible for the digital activity. The proposed model applies to both law enforcement and corporate investigations.

Key Words: Computer Forensics, Incident Response, Crime Scene Investigation

1 INTRODUCTION

Many criminal investigations will include computers at some point in the case. Murder and rape suspects may, through a search warrant, have their email and Internet activities analyzed to find evidence about their motives or hiding locations. Corporations investigate computers when an employee is suspected of unauthorized actions. Fraud investigations collect transaction history evidence from servers. It is therefore important that a process model for the digital investigation exists and that it easily interacts with the physical investigations that have long existed.

This work proposes a process model for digital investigations that meets the following requirements:

- The model must be based on existing theory for physical crime investigations.
- The model must be practical and follow the same steps that an actual investigation would take.
- The model must be general with respect to technology and not be constrained to current products and procedures.
- The model must be specific enough that general technology requirements for each phase can be developed.
- The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

This work examined the physical forensic literature for models that could be applied to digital forensics. Physical forensic analysis typically answers identification or comparison questions, such as "can substance X be identified" or "are substance X and Y the same" [25]. The term "digital forensics" has historically been used to describe a much more involved process where the investigator must trace user activity and cannot provide a simple yes or no answer.

The difference in activities between physical and digital forensics led the authors to the concept of a digital crime scene. Instead of treating the computer as a substance that needed to be identified, it is treated as a secondary crime scene. It should be treated as though the computer is a door that leads the investigators to a new room. When viewed in this way, the same principles that are used to process a room where jewelry was stolen can be used to process a server where credit card numbers were stolen - although the technology required to perform the process will obviously be different. This paper uses the term "digital investigation" instead of the more common "digital forensics"

Other books and papers have used the terms "digital crime scene" and "computer crime scene", but this paper approaches the term in a different manner. Some consider any crime scene with a computer to be a "computer crime scene"[16], but this paper only considers the digital environment created by the hardware and software to be the "digital crime scene". Others use the term "digital crime scene" in a way similar to this paper [18, 28, 29], but they do not apply physical crime scene investigation techniques to it.

The investigation of a computer or other digital device is also more similar to a physical crime scene investigation than a physical forensic analysis because of the amount of potential evidence. A physical crime scene can be processed to identify many pieces of evidence. Blood on a wall is one piece of evidence and it can be analyzed to identify the owner of the blood, the type of object that struck the victim, the location of the victim, the location of the attacker, and the time of attack. Similarly, a fingerprint is one piece of evidence that can be analyzed to show identity information and orientation information about how the person was facing.

A computer itself is, typically, only one piece of physical evidence, but it can be processed to identify thousands of pieces of digital evidence and each piece of digital evidence can be analyzed to identify ownership, location, and timing. The digital evidence can be analyzed to produce similar characteristics as physical evidence. Therefore, the investigation of billions of bytes of digital data is similar to the investigation of a house where an investigator must look at thousands of objects, fibers, and surface areas and use his experience to identify potential evidence that should be sent to a lab for analysis.

The background information on process models and physical crime investigations are given in Section 2. Section 3 describes the proposed model and Section 4 discusses the impact of the model. Lastly, Section 5 illustrates the model with two case studies.

2 PREVIOUS WORK

The process model outlined in this paper is not the first process model for digital investigations. Several others have been proposed in the past and have been used to organize investigation procedures, organize training material, and identify research areas. This section details three models including an incident response model, a law enforcement model, and an abstract model that applies to both fields. This section also describes the documented theory on physical crime scene investigations.

2.1 Incident Response Process Model

In the book Incident Response [22], an "incident response methodology" is given with the following phases:

- **Pre-incident Preparation:** Prepare for an incident with proper training and infrastructure.

- **Detection of the Incident:** Identify a suspected incident.
- **Initial Response:** Verify that the incident has occurred and collect volatile evidence.
- **Response Strategy Formulation:** Determine a response based on the known facts.
- **Duplication:** Create a backup of the system.
- **Investigation:** Investigate the system to identify who, what, and how.
- **Secure Measure Implementation:** Isolate and contain the suspect system before it is rebuilt.
- **Network Monitoring:** Observe the network to monitor attacks and identify additional attacks.
- **Recovery:** Restore the system to its original state with additional security measures added.
- **Reporting:** Document the response steps and remedies taken.
- **Follow-up:** Review the response and adjust accordingly.

This methodology is oriented towards the specific scenario of responding to a critical system that is suspected of being compromised. The granularity of the phases shows the focus on verifying an attack against a live system and restoring the system to its original state. The most time consuming phase of an investigation is the analysis of the system and that is only one of the eleven phases. For the corporate incident response team this is an appropriate focus, but our needs are broader and the analysis phase must be broken into more clear phases.

2.2 Law Enforcement Process Model

The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide [10]. The guide is a first responder's reference to different types of electronic evidence and includes procedures that can be used to safely handle them. The guide is oriented towards those who respond to the physical crime scene, so emphasis is placed on those requirements. Little attention is paid to the analysis of the system. The following phases are given:

- **Preparation:** Prepare equipment and tools to perform needed tasks during an investigation.
- **Collection:** Search for and collect electronic evidence.
    - **Secure and Evaluate the Scene:** Secure the scene to ensure the safety of people and the integrity of evidence. Potential evidence should be identified in this phase.
    - **Document the Scene:** Document the physical attributes of the scene including photos of the computer.
    - **Evidence Collection:** Collect the physical system or make a copy of the data on the system.
- **Examination:** A technical review of the system for evidence.
- **Analysis:** The Investigation team reviews the examination results for their value in the case.
- **Reporting:** Examination notes are created after each case.

This process model is based on the standard physical crime scene investigation process model that has been well documented, and will be described later. As with the incident response model, this model does not give much attention to the examination and analysis process and therefore does not directly meet our design goals.

This model can be confusing because it considers the collection of the physical hard disk to be the collection of electronic evidence. At that point in the investigation, it is unknown to the investigator if the physical hard disk contains relevant electronic evidence or not. The collection of evidence typically occurs after it has been recognized, but in this model it is collected before the digital data has been examined. Therefore, the collection phase more accurately collects the physical evidence and the individual pieces of electronic evidence will be collected when it is examined.

2.3 An Abstract Process Model

Researchers at the U.S. Air Force identified the common traits that various process models had and incorporated them into an abstract process model [23]. It has the following phases:

- **Identification:** Detect the incident or crime.
- **Preparation:** Prepare the tools, techniques, and obtain approval.
- **Approach Strategy:** Develop a strategy to maximize the collection of evidence and minimize the impact on the victim.
- **Preservation:** Isolate and secure the physical and digital evidence.
- **Collection:** Record the physical crime scene and duplicate digital evidence.
- **Examination:** Search for evidence relating to the suspected crime.
- **Analysis:** Determine significance and draw conclusions based on the evidence found. Repeat examination until a theory has been supported.
- **Presentation:** Summarize and provide an explanation of the final conclusions and theory.
- **Return Evidence:** Return the evidence that was removed from the scene back to the owner.

This process model does well at providing a general framework that can be applied to a range of incidents. In reality, the Preparation Phase should be before the Notification Phase so that the equipment and personnel are ready when the incident is detected. This model uses many of the same phases as the one given at the first Digital Forensic Research Workshop (DFRWS) [21], but adds a description for each phase.

This model, and the previous DOJ model, uses the examination and analysis phases to identify and collect digital evidence. The names of these phases can be confusing because their meaning is only slightly different and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system". The definition of examine is "to study or analyze" and the definition of analyze is "to examine methodically by separating into parts and studying their interrelations" [9]. While we agree that the two phases described in this model are different, the similarity in the names can lead to confusion.

2.4 Physical Crime Scene Investigation

For a historical perspective on investigation theory, the physical crime investigation literature was consulted. The following are the high-level phases of a crime scene investigation [17, 19, 25]:

- **Crime Scene Preservation:** The first responder assists the wounded, searches for and arrests the suspect, and detains any witnesses. The scene should be secured and access restricted to authorized investigators.
- **Crime Scene Survey:** The investigator walks around the crime scene to identify obvious pieces of evidence and pieces of evidence that are transient. Initial observations of who, what, where, when, and how are documented and an initial theory is created.
- **Crime Scene Documentation:** The crime scene is documented using photographs, sketches and video. Evidence should be clearly documented and collected.
- **Crime Scene Search:** Search patterns are used to identify additional evidence that was not found in the survey. The theory developed in the survey is used to look for specific pieces of evidence that are still missing: the murder weapon for example.
- **Crime Scene Reconstruction:** The events that occurred at the crime scene are determined using the crime scene appearance, the locations and positions of the physical evidence, the forensic laboratory analysis results, and the scientific method.

This model allows the crime scene to be thoroughly documented and uses the investigator's experience to find useful pieces of evidence. Not all physical objects can be taken from the crime scene, so the Search Phase must be thorough enough to gather the needed evidence but not overload the laboratory with unrelated objects.

3 AN INTEGRATED DIGITAL INVESTIGATION PROCESS

The proposed process model in this paper uses many of the same phases as those described in Section 2, but approaches the problem from a different point of view. This model uses the theory that a computer is itself a crime scene, called the digital crime scene, and applies crime scene investigation techniques. The laws of nature bind the physical world, while the instructions in hardware and software bind the digital world. A physical crime scene investigation uses the laws of nature to find physical evidence and the digital crime scene investigation uses the code to find digital evidence.

In physical crime scene investigations, a famous theory is the Locard Exchange Principle. It states, "when two objects come into contact, a mutual exchange of matter will take place between them" [17]. For example, hairs and fibers from the criminal are frequently left behind at a physical crime scene. A similar effect can occur in a digital crime scene. Temporary files, memory contents that are saved to disk, and deleted file fragments may exist because of a piece of software that the suspect executed. Data enters and exists the digital crime scene and leaves traces of digital evidence behind. The digital investigator is left at the mercy of the operating system and application developers though because they control what evidence is written to storage locations.

Using the concept that a computer is itself a crime scene, the investigation theory for a physical crime scene was applied to a digital investigation. The resulting process model is described in the following sections and each section includes a brief description of the actions that could be taken. The digital crime scene investigation is integrated with the physical crime scene so that physical evidence can be collected that ties the digital activity to a person. The digital crime scene can be considered a secondary crime scene to the physical crime scene.

In this field, there are many interpretations and meanings of key words. To prevent confusion, we will define the basic terms of the process. There are many definitions for each of the terms and these were chosen because they most accurately reflect our approach to the problem. Future work will include a more thorough discussion and analysis of these basic terms.

- **Physical Evidence:** Physical objects that can establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and its perpetrator [25]. The actual computer, hard disk, PDA, and CD-ROM are examples of physical evidence.
- **Digital Evidence:** Digital data that can establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and its perpetrator [13]. The data in memory, on the hard disk, or in a cell phone are examples of digital evidence.
- **Physical Crime Scene:** The physical environment where physical evidence of a crime or incident exists. The environment where the first criminal act occurred is the primary physical crime scene and subsequent scenes are secondary physical crime scenes. We created this definition based on the one given by Lee [19].
- **Digital Crime Scene:** The virtual environment created by software and hardware where digital evidence of a crime or incident exists. The environment where the first criminal act occurred is the **primary digital crime scene** and subsequent scenes are called **secondary digital crime scenes**.

This process model applies to both corporate and law enforcement investigations. Therefore, the terms "crime scene" and "incident" are used in the general sense. A physical crime scene is meant to include an employee's desk that is being investigated by Human Resources, a data center that contains a server that was broken into, an apartment for a child pornography investigation, or a car where a man was found murdered with his laptop open on the passenger seat. An incident is any series of events that cause a response team or evidence collection team to be deployed. This includes a server intrusion, a search warrant being served on a suspect's house, and a police officer responding to an emergency 911 call.

We assume that the size of a crime scene is initially defined by the natural boundaries around the known evidence. For example, if a crime is committed in a house, then the house and the property around it could be the initial physical crime scene and the size may later be increased or decreased based on the additional evidence that is found. For a computer, the initial digital crime scene is typically the virtual environment created by the local operating system and hardware. Each computer involved in an incident will likely be a separate crime scene.

The terms "examine" and "analyze" are used in this paper to mean that an object is being processed in some way to collect information from it. As noted in the Previous Work Section, some models use these terms as separate actions, but their definitions are very similar and it can lead to confusion. The goal of this paper is to illustrate a process model and therefore we will try to avoid confusion by only using the term "analysis", but you can replace it with examination if you prefer.

The process model has 17 phases organized into five groups, which are listed here and shown in Figure 1.

1. Readiness Phases
2. Deployment Phases
3. Physical Crime Scene Investigation Phases
4. Digital Crime Scene Investigation Phases
5. Review Phase

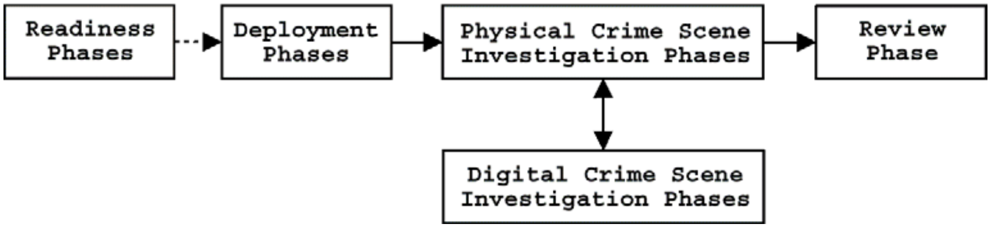
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 1: The five groups of phases in the investigation process.

Each phase will be discussed in the following sections. Note in the figure that the physical crime scene is processed along with the digital crime scene and the results of the digital investigation are fed into the physical crime scene investigation.

3.1 Readiness Phases

The goal of the readiness phases is to ensure that the operations and infrastructure are able to fully support an investigation. Both digital and physical evidence can be lost if it is not maintained and collected properly. This phase is ongoing and is not tied to a specific incident or crime [27].

The **Operations Readiness Phase** provides training and equipment for the personnel that will be involved with the incident and its investigation. This includes training the responders, the lab analysts, and staff that will be receiving the initial reports of the incident. The equipment that responders bring to the crime scene must be functioning properly and up to date. The equipment in the analysis lab should also be maintained and ready when the incident data is delivered.

The **Infrastructure Readiness Phase** ensures that the needed data exists for a full investigation to occur. After all, it is difficult to analyze data if it does not exist. This phase only applies to those who maintain the environment that could be the target of a crime. Physical examples for this phase include deploying video cameras and card readers to record who was in the area at the time of the crime. Digital examples for this phase include sending server logs to a secured log host, synchronizing the internal clocks on servers with NTP [20], creating a baseline of MD5 [24] hashes of critical executables, and maintaining a change management database.

3.2 Deployment Phases

The goal of the deployment phases is to provide a mechanism for the incident to be detected and confirmed. The tasks performed under these phases differ widely between law enforcement and a corporate investigations team.

The **Detection and Notification Phase** is where an incident is detected and the appropriate people are notified. This could come in the form of a 911 call, a network-based Intrusion Detection System (IDS) alert, or an online undercover police officer who is solicited for illegal actions. This phase defines the start of the investigation process.

The **Confirmation and Authorization Phase** will proceed differently depending on the situation. The goal of this phase is to receive authorization to fully investigate the incident and the crime scene. For a law enforcement situation, this typically requires a search warrant or other legal approval that requires sufficient evidence or suspicion.

For corporate incidents, search warrants are not needed as long as the appropriate privacy policies are in place. In a server intrusion situation, this step typically involves the incident response team verifying that a system has been compromised by looking at the live system for evidence such as rootkits and suspicious network activity. During a live analysis to verify the incident, it is important to treat the system as a crime scene and minimize the impact to the system. After the incident has been confirmed, approval from a supervisor is typically needed to take further actions. For servers whose uptime is critical to a company, the approval may need to come from the executive level.

3.3 Physical Crime Scene Investigation Phases

The goal of the physical crime scene investigation phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. One of the goals of a digital investigation is to identify people who are responsible for the incident and therefore physical evidence is required. The phases presented here are the standard physical crime scene investigation phases, but this paper focuses on the topics that are most relevant for digital incidents. For a law enforcement case, a physical crime scene expert will complete most of the tasks outlined here. In a corporate setting, they will be completed by the computer response team or the physical security team. The phases in the physical crime scene investigation phases are shown in Figure 2.

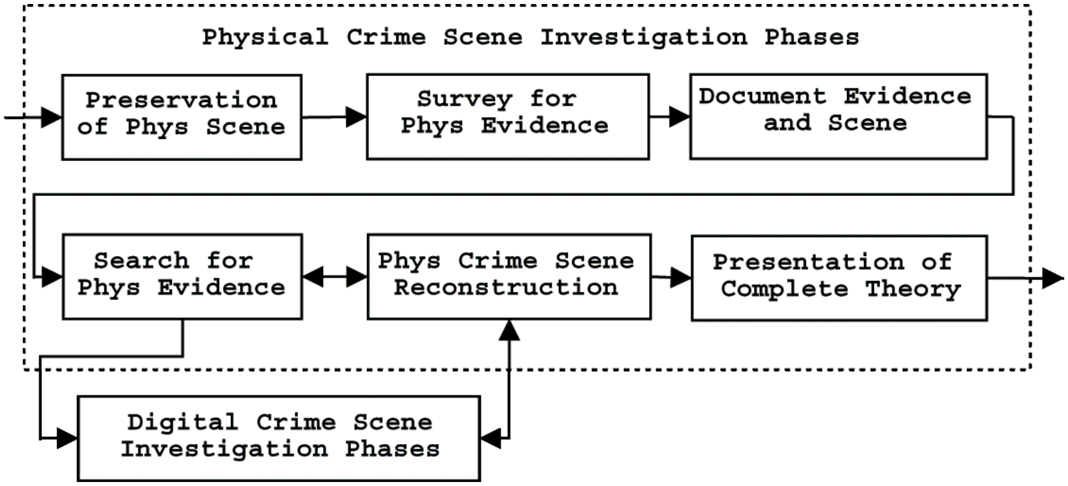
Physical Crime Scene Investigation Phases
Preservation of Phys Scene
Survey for Phys Evidence
Document Evidence and Scene
Search for Phys Evidence
Phys Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation Phases

Figure 2: The six phases in the physical crime scene investigation and the interaction with the digital crime scene investigation.

The **Preservation Phase** of the physical crime scene is typically indifferent to the type of crime. The activities include securing the exits, helping the wounded, detaining the suspects, and identifying witnesses. In a digital incident, the physical crime scene should be secured using the same procedures as a non-digital incident. In a server intrusion investigation, this phase may include identifying who had been in the data center and preventing others from entering because an employee could be responsible for the incident. Note that this phase preserves the crime scene so that evidence can be later identified and collected. It does not preserve specific pieces of evidence.

The **Survey Phase** of the physical crime scene involves a walk through of the scene by the investigator and, typically, the first person who responded to the incident. The goal is to identify the obvious pieces of physical evidence, the fragile pieces of physical evidence, and develop an initial theory about the crime. For example, in a murder investigation this phase would include walking around an apartment and identifying how the attacker gained entry, where the murder took place, and what happened to the victim after the murder. Fragile pieces of evidence should be documented and collected immediately so that they are not damaged.

In a digital incident, examples of physical evidence that are identified in the survey include the number and location of computers, what network connections the computers have, PDAs, cell phones, passwords on pieces of paper, and CD-ROMs or other removable media. At the conclusion of this phase, the investigator will have an idea about how to process the physical crime scene and what special skills are needed. If a computer specialist was not on-site at this point, one would be contacted to collect the evidence. A computer that is running and plugged into a network can be considered fragile evidence because its digital evidence could be deleted with commands from a remote system. Therefore, some procedures include unplugging a computer from the network when it is found or deploying a network monitor to view what data is being sent to the system until the full investigation begins.

The **Documentation Phase** of the physical crime scene involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded. For a digital incident, it is important to document and photograph the connections on the computer and document the state of the computer. It could also be important to document the number and size of the hard drives and the amount of memory. In some cases, the hardware MAC address of the network cards should also be recorded so that DHCP logs can used to identify the system activity. Serial numbers and asset tags are useful to record in this phase. To identify what should be recorded, consider that the analysis lab may only get a copy of the hard disk and no original physical hardware. Anything that could be of use to the analysis lab and later reconstruction should be recorded. Note that the Documentation Phase is not the phase where a final incident report is generated.

The **Search and Collection Phase** of the physical crime scene involves an in-depth search and collection of the scene for additional physical evidence. The search can be oriented towards missing pieces of physical evidence, such as a weapon, or be methodical and have strict search patterns. Each type of evidence typically has specific procedures on how it should be collected. For a digital incident, this phase may involve looking for additional media and digital devices at the crime scene. It can also include contacting people to preserve and obtain access logs for the doors of a data center, change logs for server updates, firewall logs, IDS logs, and remote access logs. This is the last phase that typically occurs on the actual crime scene. The physical evidence that was collected from the scene is sent to labs for analysis and the results are used in the next phase, Reconstruction.

The Search and Collection Phase of the physical crime scene is where the digital crime scene investigation begins. The computer system itself will be considered physical evidence and therefore collected. The collection procedures should document how to collect volatile data from a running system and how to power it off. The digital crime scene investigation phases are outlined in detail in the next section.

The **Reconstruction Phase** of the physical crime scene involves organizing the analysis results from the collected physical and digital evidence and using the crime scene photographs to develop a theory for the incident. The scientific method is used with the evidence to test the incident theories. With a digital incident, the results of the digital crime scene investigation are correlated with physical evidence to link a person to the digital events. Examples of this phase would include linking data center access logs to logins, linking on-line chat activity found on the system with the activity with an undercover officer, and linking activity on a compromised server with activity on the suspect's home system and network activity recorded by an ISP. To be most effective, this phase should involve digital crime experts to help link the events from multiple sources of digital evidence. Note that crime scene reconstruction is not the same as crime scene recreation, which makes a physical model of the crime scene.

The **Presentation Phase** of the physical crime scene involves presenting the physical and digital evidence to a court or corporate management. This phase presents the evidence and the theory that was developed from the physical crime scene reconstruction.

3.4 Digital Crime Scene Investigation Phases

The digital crime scene investigation phases begin when the physical digital device is collected as physical evidence from the physical crime scene or when recorded network traffic is analyzed for evidence. These phases approach the computer as a crime scene and search it for evidence. The goal is to identify the electronic events that occurred on the system and present that to the physical crime scene investigation. Someone who has specialized training with analysis tools and techniques typically performs the tasks in these phases. The phases are shown in Figure 3.

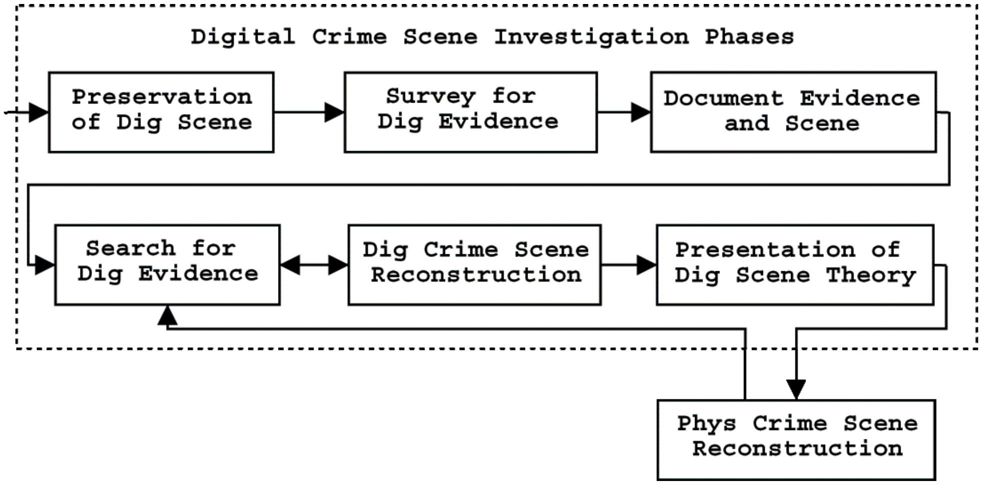
Digital Crime Scene Investigation Phases
Preservation of Dig Scene
Survey for Dig Evidence
Document Evidence and Scene
Search for Dig Evidence
Dig Crime Scene Reconstruction
Presentation of Dig Scene Theory
Phys Crime Scene Reconstruction

Figure 3: The six phases in the digital crime scene investigation. The results are fed back to the physical crime scene investigation.

In this model, each digital device is considered a separate crime scene. The analysis results of each digital device will be sent to the Physical Crime Scene Reconstruction Phase and the linkage between the devices will be identified. This allows the analysis of different types of devices to be done at different locations. Physical crime scenes are organized into primary and secondary scenes, where the primary scene is where the first criminal act occurred [19]. Digital crime scenes can also be organized into primary and secondary scenes. For example, the server that was broken into would be the primary digital crime scene and the log server that was later broken into to modify the logs relating to the intrusion would be a secondary digital crime scene.

The **Preservation Phase** of the digital crime scene involves securing the entrances and exits to the digital scene and preserving the digital evidence that could change. In the physical world, this involves reducing foot traffic and collecting physical evidence that could be lost because of weather. In the digital word, this includes isolating the system from the network, collecting the volatile data that would be lost when the system is turned off, and identifying any suspicious processes that are running on the system. Suspect users that are logged into the system should be noted and possibly investigated. Log files can be considered an eyewitness to the crime and should be secured if there is a threat that they will be lost before the system is copied. Note that other models use "preservation" to refer to preserving digital evidence. In this model, the entire digital environment is being preserved. In fact, no digital evidence has been identified yet when this phase occurs.

One of the benefits of the digital world over the physical world is that the environment can be easily replicated. Therefore, it is common in this phase to make a complete forensic image backup of the system so that it can be analyzed in a lab. This is analogous to physical investigators being able to bring an exact copy of a building into the lab for analysis. Copies of the full disk preserve the entire digital crime scene while copies that are simply system backups preserve only the allocated data in the digital crime scene. A critical system can typically be rebuilt after a forensic image has been created so that it can be quickly placed back online. Other cases will require the original hard disk to remain as physical evidence for the duration of the case. When network monitors save network traffic, they are in effect preserving the state of the network.

The **Survey Phase** of the digital crime scene typically occurs in the lab using one of the digital crime scene replica images. It can occur on a live system, similar to what occurs in the physical world, but the lab environment is preferred because it provides a controlled environment and the results can be repeated with another copy of the system. If the Survey Phase is performed on a live system, then a forensic image of the system should still be taken so that any digital evidence can also be collected in a controlled lab environment. This phase is sometimes done in the field to identify if the system should be brought to the lab for a full analysis. Field searches are typically performed by booting the system into a trusted environment so that digital evidence is not modified.

The Survey Phase finds the obvious pieces of digital evidence for the given class of crime. For example, in a child pornography case the investigator would collect all of the graphic images on the system and identify those that could be used as evidence. In a server intrusion, the investigator would look for obvious signs of a rootkit installation, analyze application logs, and look for new configuration files. Other cases may analyze the cache and history of an HTML browser. When analyzing network traffic about an incident, this phase may analyze the traffic for the incident time frame and filter out certain ports and hosts. The Survey Phase will show the investigator the skill level of the suspect and what analysis techniques the investigation will require. The investigator may contact encryption, executable analysis, or data recovery experts at this point.

The **Documentation Phase** of the digital crime scene involves properly documenting the digital evidence when it is found. The exact copy of the system that was acquired during the Preservation Phase has the same role as the sketches and video of a physical crime scene. Each piece of digital evidence that is found during the analysis of the image must be clearly documented. This phase documents individual pieces of evidence and does not create the final incident report. The final report of the digital analysis will be generated in the Presentation Phase.

Digital evidence can exist in many abstraction layers [12] and must be documented accordingly. For example, a file can be documented using its full file name path, the clusters in the file system that it uses, and the sectors on the disk that it uses. Network data can be documented with the source and target addresses at various network layers. As digital evidence can be changed and leave little trace, additional steps should be taken to later verify the integrity. A cryptographic hash value, such as MD5 [24] or SHA-1 [8], should be calculated for the evidence when it is collected so that its integrity can be proven to the courts. Chain of Custody forms should be created in this phase if the evidence could be used in court. In practice, the Documentation Phase is not a specific phase in a digital investigation because the digital evidence is documented as it is found.

The **Search and Collection Phase** of the digital crime scene involves a thorough analysis of the system for digital evidence. This phase uses the results of the Survey Phase to focus on additional analysis types. For example, a keyword search can be performed in this phase after keywords are identified from other evidence. The unallocated file system space can be extracted and processed for deleted files. A low-level timeline of file activity can be analyzed to trace a user's activity. Suspicious executables can be reverse engineered and encrypted files can be analyzed. All of the network packets that were collected by monitoring software can be analyzed. In some cases, it may be appropriate to examine the contents of every cluster (physical search) or every file (logical search). Just as there are different search techniques in a physical crime scene, there are different techniques for a digital crime scene that can be used when appropriate.

The bulk of the investigation time is spent in this phase. In the digital world, evidence is copied from the scene and not removed from the scene. For some types of incidents, it is common to have both technical and non-technical investigators in this phase because of a limited number of trained digital investigators. For example, the technical investigator would extract all pictures from a system and send them to a non-technical investigator who would analyze each picture and identify the ones to be used as evidence. The Survey and Search Phases are similar to the Examination Phase that other models have.

The **Reconstruction Phase** of the digital crime scene involves putting the pieces of the digital puzzle together. The digital evidence is classified and is assessed to determine the amount of trust that can be placed in it [14]. Data that requires advanced analysis techniques, such as executable analysis or decryption, are processed and the results are used in this phase. This phase uses the scientific method to test and reject theories based on the digital evidence. This phase will identify how the digital evidence got there and what its existence means. When digital evidence is still missing, the Search Phase will resume to identify additional evidence. For example, in a server intrusion this phase would correlate the exploitation of a vulnerable service with the installation of a rootkit and the deployment of a network sniffer. The source IP address of network connections could lead to an additional digital crime scene to analyze. This phase is similar to the Analysis Phase that other models have.

The **Presentation Phase** of the digital crime scene involves presenting the digital evidence that was found to the physical crime scene investigation team. Recall that the physical crime scene team uses the results of the digital crime scene investigation in their Reconstruction Phase. Also note that the digital crime scene investigation of a system does not involve data from other digital sources, such as IDS and firewalls. The physical crime scene investigators integrate the results from each of the digital crime scenes. Therefore, this phase documents and presents the findings of a specific digital crime scene to the other investigators. In many cases, the physical and digital investigation teams are the same and the information is shared on an ongoing basis.

3.5 Review Phases

The final phase is the **Review Phase** and it involves reviewing the investigation to identify areas of improvement. For digital incidents, this includes how well each of the physical and digital investigations worked, how well the physical and digital investigations worked together, and whether enough physical and digital evidence existed to solve the case. The result of this phase could be new procedures, new training, or nothing if everything actually went as planned.

4 MODEL DISCUSSION

This model gives an accurate view of the digital investigation process and differentiates between digital evidence collection and digital forensics. Physical forensic sciences typically answer comparison questions such as "Are X and Y similar?" or identification questions such as "Can you identify X?" [25]. The actions that have historically fallen under the category of digital forensics are broader and include event reconstruction. Therefore, digital investigation is a more accurate term from the perspective of the people who are analyzing the system. From the perspective of the physical crime scene investigator who sends the computer to a lab for analysis though, the process will likely always be considered digital forensics.

This model also shows the amount of effort that needs to be dedicated to properly investigate a digital incident. Many law enforcement investigations have only one person analyzing each computer and there is a backlog of systems. This is analogous to sending one officer to a physical crime scene and expecting her to find all of the evidence and recreate the crime. Adequate resources are needed to properly investigate a digital incident.

When current technologies are examined with respect to these phases, it can be seen that the current digital "forensic" analysis tools allow the user to view the digital crime scene and collect digital evidence from it [1, 2, 3, 7, 11]. The tools are used in the Digital Survey and Search Phases to collect evidence. Link analysis [4] and timeline tools help the investigator in the Digital Reconstruction Phase. Therefore, with this model many current digital forensic tools may be more appropriately called digital evidence collection tools. Digital evidence collection tools translate digital data to an abstraction layer that helps the investigator [12]. The tools use engineering techniques to display the data to the investigator and not science.

It has been debated if the evidence gathered from a live computer is reliable. Using this model, collecting evidence from a live computer is no different than collecting physical evidence. The physical crime scene will be modified when the investigator walks around just as the digital crime scene will be modified when the investigator runs digital evidence collection software. The challenge is to minimize the changes, understand the effect of the changes, and minimize the trust that is placed on the operating system of the live system.

This model clearly shows the interaction between the physical and digital realms. Many procedures focus mainly on the digital evidence and include basic physical evidence such as taking pictures of the back of the system. This model includes an equal number of phases for the physical crime scene as the digital crime scene. The motivation for this is because the end goal of any digital investigation is to tie the digital activity back to a human. Therefore, physical evidence will be needed and should be taken into account during the investigation. The digital crime scene can be considered a secondary crime scene to the physical crime scene.

The physical crime scene is well understood for law enforcement investigations. In general, the physical crime scene is less understood for digital investigations led by corporate investigators. For example, many incident response teams do not have formal procedures for analyzing the physical area around a compromised server. In reality though, a disgruntled system administrator who had physical access to the system could have performed the incident. He may have left physical evidence behind that could be lost if it is not searched for when the responders arrived.

The model also shows that the difficulties that digital investigators face are similar to those faced by physical investigators. For example, the Survey and Search Phases of both crime scenes must be able to identify the useful pieces of evidence. The physical crime investigator cannot send every physical object to the lab for analysis. He must use his experience to identify what is normal and what is not. Similarly, a digital investigator cannot send every executable on the system to be reverse engineered. Both types of investigators face the difficulty of finding small pieces of evidence, such as a hair in a carpet or a deleted file in a 100 GB file system.

Lastly, by breaking the analysis process into the Survey Phase and the Search Phase, it is easier to document and teach the process. A common problem for an inexperienced digital investigator is that he does not know how to begin the Examination Phase that other models describe. The physical investigation model of breaking the Examination Phase into two phases makes the process more intuitive. In the author's experience, digital investigations occur by finding the obvious quick hits and then expanding on them.

5 CASE STUDIES

In this section, two case studies will be given. They illustrate example activities that might occur in the phases described in this paper. The case studies contain high-level descriptions of actions, but are not a comprehensive description of the investigation. The first case study is for a corporate server intrusion and the second is for a law enforcement investigation for possession of child pornography. The case studies are fictional, but are common scenarios based on the author's experience.

5.1 Server Intrusion

The first case study involves a medium sized company, ACME Manufacturing. In this example, ACME was notified that one of its systems might have been broken into. This case study follows the process of confirming, responding to, and analyzing the suspected incident.

As previously mentioned, the readiness phases are ongoing and allow an organization to prepare for an incident. For the *Operations Readiness Phase*, ACME developed incident response procedures, purchased incident response kits, hired a forensic consulting company on retainer, and sent one of its system administrators to incident response training. For the *Infrastructure Readiness Phase*, ACME ensured that the appropriate information was being logged on its servers and allocated money in the budget for a central log server. The times on all servers were synchronized with NTP.

In the *Detection and Notification Phase* of this incident, the head system administrator at ACME Manufacturing received a phone call reporting that one of ACME's servers was scanning the Internet for systems that were vulnerable to an SSH vulnerability. The caller provided the ACME system administrator with the IP address of the suspect system, which was the primary public DNS server. The ACME system administrator referred to his incident response procedure manual and the incident was escalated to the administrator who went to incident response training.

The incident response administrator began the *Verification and Authorization Phase* by confirming the incident. He took his incident response kit to the data center where the Solaris DNS server was located. He plugged the laptop into the network, looked at the traffic, and saw the scanning identified by the caller. While his computer was plugged into the network, he performed a port scan of the server and identified a suspect port that was open. He knew that the CIO would require more proof of the incident than simply the network traffic, so he went to the server for additional evidence. Before touching the server, he made a quick survey of the area around the server for physical evidence and found none.

The administrator placed a CD-ROM of trusted tools into the Solaris system and logged in. He executed tools from the CD to collect volatile data such as information about running processes, open network ports, and open file handles. All data was sent to his laptop using network tools, such as netcat [15], so that evidence was not overwritten on the server disk. The output was viewed on the laptop and showed the process that was scanning the Internet and the process that had the suspicious port open. The administrator presented this information to the CIO of the company.

Before the CIO would authorize the primary DNS server to be taken down, he wanted to know if the secondary DNS server was compromised in the same way. The administrator looked at the network traffic from the secondary DNS and performed a port scan of it. It had no suspicious ports open, so the CIO authorized that the primary DNS could be taken down for a short amount of time. A more thorough analysis of the secondary DNS would be performed after the primary DNS was rebuilt.

The incident was now official and the physical crime scene investigation began. It was unlikely that an insider was responsible for this incident, but the administrator requested the records from the data center key card access system as part of the *Physical Preservation Phase*. The *Physical Survey Phase* showed no physical evidence in the data center. The serial number and hardware configuration of the server were documented in the responder notes during the *Physical Documentation Phase*. The *Physical Search and Collection Phase* of the crime scene included the beginning of the digital crime scene investigation. The firewall administrator was also contacted and told to make copies of his existing logs, calculate MD5 hashes of them, and increase the logging levels.

The *Digital Preservation Phase* of the digital crime scene involved saving and making copies of the digital data. Much of the volatile data had already been saved during the Verification Phase, but the memory contents of the scanning tool and the process that had the suspicious port open had not been saved. They were collected using trusted tools from the CD and saved to the laptop over the network. To acquire the disks, the responder booted the Solaris server from a custom CD that had incident response tools on it. The responder calculated the MD5 value of the disk, copied the disk over the network to the laptop using the incident response tools, and verified the hash of the forensic image on the laptop. The digital crime scene had been preserved. The responder made a copy of the forensic image on the laptop and imported it into his analysis software to verify that the image was not corrupt. After the image was tested, another administrator rebuilt the original system so that it could be placed back online with additional monitoring until the attack vector was known.

The forensic image was sent to the consulting company that was on retainer and they continued the investigation. The image was loaded into their analysis software and the *Digital Survey Phase* began. The Survey Phase included the following steps:

- Compare the MD5 hashes of the system binaries with the Solaris fingerprint database [6] to look for altered files
- Look for evidence of a rootkit, such as unexpected files in the '`/dev/`' directory and files and directories with names beginning with '.'
- Compare the patch level of the system with known vulnerabilities to identify possible intrusion methods
- Analyze the startup, shutdown, and application configuration scripts of the system
- Create a timeline of file activity and look for suspicious activity from a high-level, such as archive files being opened and programs being compiled.
- Analyze the logs for suspicious activity and logins

Each time a piece of digital evidence was found; it was *documented* with its file name and physical location on disk. Evidence was documented in ink for the investigation notes and using the analysis tool's built-in reporting. The Survey Phase identified a rootkit, a new version of SSH that was installed, and several new executable files. The logs from the incident were missing.

The *Digital Search and Collection Phase* included searching for more detail about the incident. The unknown executables were analyzed to identify their function, and keyword searches were performed on phrases from the rootkit. The file activity timeline was used to identify other files associated with the rootkit installation times.

The *Digital Reconstruction Phase* analyzed the evidence found thus far and the results from the executable analysis. The evidence showed that the attacker likely gained access via a vulnerable version of the SSH server. Once the system had been compromised, the attacker replaced the vulnerable version of SSH with a version with a back door password and installed a rootkit to hide data from the users. The suspicious open port was for a server that used a custom protocol that gave the attacker remote control of the system. Evidence also showed the previous host that the attacker logged in from, although it was unlikely to be his actual home system. No evidence could be found that suggested that the attacker had access to sensitive company information. The *Digital Presentation Phase* of the investigation resulted in a final report of the analysis by the consulting company.

The report was given to ACME and it was used with the logs for the corporate firewall and the data center key cards in the *Physical Reconstruction Phase*. The scenario of an insider with physical access to the server was ruled out using the key card logs, the times of the incident, and the presence of the remote IP addresses. Using the firewall logs, it could be seen that the attacker tried to gain access to the corporate network using the compromised system, but was blocked.

In the *Physical Presentation Phase* of the investigation, a final ACME report was generated. It documented the digital investigation findings and the firewall and key card logs. When presented to management, it was decided to patch all systems, ignore this incident, and remain on high alert for a few more days. The administrators of the hosts where the attacker came from were notified of the incident so that they could clean their systems. If those systems were investigated, they would be considered secondary digital crime scenes in this model, and possibly in other jurisdictions.

The final phase, the *Review Phase*, discussed how the incident could have been better handled. One outcome was to install the central log server sooner than planned.

5.2 Contraband

The second case study involves the investigation of home computers for contraband. In this example, law enforcement officials were analyzing a web server that contained pornographic images of minors. The server had logs that recorded which users downloaded the pictures and all users were required to pay a monthly free for access to the contraband files. The police collected the financial records. This example is of an investigation into one of the users who downloaded files from the server.

In the *Operations Readiness Phase*, law enforcement trained its physical crime scene investigators on how to handle computers and digital evidence. It also trained the digital crime scene investigators and forensic lab specialists. Equipment was maintained and up to date.

The *Detection and Notification Phase* of this incident occurred when the investigators processed the logs from the server. The logs showed the user names and IP addresses of the users that downloaded the illegal images. An investigator was assigned to each of the users to investigate the secondary digital crime scenes.

The *Confirmation and Authorization Phase* required the investigator to link the log entries to a computer and to a person. The investigators were able to identify credit card numbers for some of the website user accounts, but some accounts used other forms of payment. The use of stolen credit cards for this purpose is common, so additional evidence was needed to obtain a search warrant. The server logs had IP addresses for each download so the investigators were able to identify who owned each address, all of which were from dial-up Internet Service Providers (ISP).

Subpoenas were obtained to identify the user and billing information from the ISPs for the dial-up accounts that had the IP addresses at each download time. For website accounts where a credit card was used, the information was compared with the data that the ISP had. Many of the service providers also had Caller-Id information for the dial-up accounts and that was used to confirm the website user's identity. Search warrants were obtained for the homes and computers of the users with the most evidence against them.

This case study is for John Doe, who was one of the users identified by his ISP. Police raided Mr. Doe's house and began a physical crime scene investigation. In the *Physical Preservation Phase*, the police separated John Doe from his computer and prevented pieces of paper around the computer from being removed. The *Physical Survey Phase* of the home identified three computers and an internal network connected to a cable modem. Several cases were full of CD-ROMs, and post-it notes existed with logins, passwords, and web site addresses. The web site in question was on one of the lists. The responder turned the cable modem off.

The *Physical Documentation Phase* took photographs of each computer, the network switch, and the desk where the post-its were found. Hardware information of each computer was also documented. All of the computers were already powered off when the police arrived. The *Physical Search and Collection Phase* involved searching for additional physical evidence such as a digital camera and other storage devices. The digital evidence specialist also began to investigate each computer. The keyboard and mouse from each computer were analyzed for fingerprints.

The digital crime scene investigation began while the physical evidence was being collected. In the *Digital Preservation Phase*, the hard disk of each of the three computers was removed and placed in a portable Linux system. The MD5 value of each disk was calculated, forensic images were created, and the image was verified with the original disk using the MD5 value. Both the forensic images and computers were packaged and taken from the scene. The computers were sent to the evidence locker and the images were sent to the analysis lab.

The *Digital Survey Phase* of each computer was conducted independently of each other in the lab. The final results would be combined in the Physical Reconstruction Phase. Copies of the forensic images were imported into the analysis software and the file system was analyzed. The primary purpose of the investigation was to find contraband graphic pictures, so the analysis tool searched the disks for all files that had a JPEG, GIF, or PNG structure. While the tool was looking at the structure of each file, it was also looking up the MD5 value in a hash database [5]. The tool identified many known child pornography pictures and made thumbnails of the other pictures on the system for the investigators to review manually. The resulting collection of pictures was quickly reviewed and when suspects were found, the directory locations were documented so that they could be analyzed in more detail in the Search Phase.

The Survey Phase also analyzed the history and cache of the HTML browsers and logs for chat programs. To conclude the Survey Phase and identify what other special skills would be needed, a search was performed of the system for encrypted files. All digital evidence was *documented* in the case notes with the file name, physical disk location, and MD5 hash. The built-in reporting system in the analysis software was also utilized and Chain of Custody forms were started.

The *Digital Search and Collection Phase* included a more in-depth search for pictures. The pictures that were extracted in the Survey Phase were analyzed in more detail because previously they were simply skimmed. The directories containing suspect files were identified and all files in them were analyzed and documented. All ZIP and archive files were opened and searched for pictures. Timelines of file activity were also used to identify other system activity that occurred when the pictures were created and accessed.

The sites in the computer's history and cache files were analyzed and the times recorded. The user accounts and login times on the system were also recorded to correlate a specific person with the Internet activity. The passwords for the system were analyzed to identify if the accounts all had passwords that were easy to guess. This could help show if multiple users had access to the system and if each had passwords that were difficult to guess. The applications that were installed on the system were analyzed to find graphic viewers, network tools, evidence wipers, and network services (such as peer-to-peer software). The system was also analyzed for evidence of compromise [26] and remote control software.

The *Digital Crime Scene Reconstruction Phase* analyzed the created, last written, and last access times on each of the suspect files and compared them with the times on the Internet cache files and history entries. Information from graphic viewing applications was also correlated with system activity. Finally, the known user login times were compared with the created, written, and access times of the files and Internet history. The system contained no evidence of compromise, network shares, or remote control software so a potential defense that the system was broken into and the pictures placed there had no supporting evidence.

The *Digital Presentation Phase* created a report about the system. The report included details of all pictures and a timeline of user, Internet, and relevant application activity. The findings were presented to the investigators involved in the *Physical Reconstruction Phase*. In this case, the investigators in the Reconstruction Phase included the analysts from all three computers and other detectives. The suspect's actions were linked using the reports from the three computers, the logs from the original web server, the access logs from the Internet Service Provider (ISP), and the physical evidence from the crime scene. Enough evidence was found to prosecute the suspect. The other Internet servers that were identified in the suspect's history file were investigated next.

The *Physical Presentation Phase* created a final report of all activity of the user. This included the activity across all three computers and gave supporting evidence from ISP logs and the logins and passwords that were found on paper at the crime scene. This was presented to the District Attorney who prosecuted the case.

The *Review Phase* included a review of the investigation and identified some new analysis techniques that were utilized. The techniques were added to the official analysis procedures. During the analysis, new suspect files were identified and they were added to the hash database so that they could be quickly found in future investigations.

6 CONCLUSION

This paper has outlined a process model for digital investigations that is based on the crime scene theory for physical investigations. Thousands of physical investigations have occurred and the investigation process has been refined with time. Therefore, it is useful to link a more recent type of investigation to the more established type.

This model considers the computer to be a separate crime scene and more than simply an object of physical evidence. The computer is treated more like the body at a murder scene then it is the gun. The gun will be sent for lab tests to identify if it was fired and who held it. The body is tested for chemicals in the blood stream, evidence of other abuses are searched for, and the organs are analyzed to identify how the person died, including identifying if the gun shot is what actually killed the person. A body contains additional pieces of evidence, such as chemicals, that can be analyzed. Computers are analyzed in a manner similar to a body to identify additional pieces of evidence and the sequence of events that occurred inside of it.

This model allows technical requirements for each phase to be developed and for the interaction between physical and digital investigations to be identified. It is abstract enough that it can be applied to both law enforcement and corporate scenarios. As digital evidence is challenged more in court, using procedures and models from the physical investigation world will add credibility to the analysis results from the digital world.

7 ACKNOWLEDGMENTS

Marc Rogers (CERIAS) and Eoghan Casey provided helpful feedback and comments on this paper.

REFERENCES

[1] Access Data: Forensic Toolkit. Available at: http://www.accessdata.com.

[2] ASR Data Acquisition and Analysis: SMART. Available at: http://www.asrdata.com.

[3] Guidance Software: EnCase Forensic Edition. Available at: www.encase.com.

[4] i2 Ltd: Analyst's Notebook. Available at: http://www.i2.co.uk.

[5] NDIC: HashKeeper. Available at: http://www.hashkeeper.org.

[6] Sun Microsystems: Solaris Fingerprint Database. Available at: http://sunsolve.sun.com/pubcgi/fileFingerprints.pl.

[7] Technology Pathways: ProDiscover DFT. Available at: http://wwww.techpathways.com.

[8] Secure Hash Standard. National Institute of Standards and Technology, FIPS PUB 180, May 1993.

[9] *The American Heritage Dictionary of the English Language*. Houghton Mifflin, 4 edition, 2000.

[10] Electronic Crime Scene Investigation: A Guide for First Responders. Available at: http://www.ncjrs.org, July 2001.

[11] Brian Carrier. The Sleuth Kit. Available at: http://www.sleuthkit.org.

[12] Brian Carrier. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence*, Winter 2003.

[13] Eoghan Casey. *Digital Evidence and Computer Crime*. Academic Press, 2000.

[14] Eoghan Casey. Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, Summer 2002.

[15] hobbit. netcat. Available at: http://www.atstake.com/research/tools.

[16] ICAPO. Computer Usage For Child Abuse Investigators. http://www.vrhome.com/icapo/pedo/webax/index.htm.

[17] Stuart James and Jon Nordby, editors. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2003.

[18] Warren Kruse and Jay Heiser. *Computer Forensics: Incident Response Essentials*. Addison Wesley, 2001.

[19] Henry Lee, Timothy Palmbach, and Marilyn Miller. *Henry Lee's Crime Scene Handbook*. Academic Press, 2001.

[20] David Mills. Network Time Protocol (Version 3). Network Working Group RFC 1305, March 1992.

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

[22] Chris Prosise and Kevin Mandia. *Incident Response: Investigating Computer Crime*. McGrawHill Osborne Media, 2001.

[23] Mark Reith, Clint Carr, and Gregg Gunsch. An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, Fall 2002.

[24] Ron Rivest. The MD5 Message-Digest Algorithm. Network Working Group RFC 1321, April 1992.

[25] Richard Saferstein. *Criminalistics: An Introduction to Forensic Science*. Pearson, 7 edition, 2000.

[26] John Schwartz. Acquitted Man Says Virus Put Pornography on Computer. *New York Times*, Aug 11, 2003.

[27] John Tan. Forensic Readiness. Technical report, @stake, 2001. [28] Brent Turvey. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*. Academic Press, 2 edition, 2002.

[29] John Vacca and Michael Erbschloe. *Computer Forensics: Computer Crime Scene Investigation*. Charles River Media, 2002.

© International Journal of Digital Evidence

ABOUT THE AUTHORS

Brian Carrier (carrier@cerias.purdue.edu) is a Research Assistant at the Center for Education and Research in Information Assurance (CERIAS) at Purdue University, where he is working on his PhD in Computer Science. Previously, Brian was a Research Scientist at @stake, where he led the digital forensic lab and incident response team. Brian has authored several open source digital investigation tools, including The Sleuth Kit and the Autopsy Forensic Browser; has taught at the SANS forensic track, Forum of Incident Response and Security Teams (FIRST), @stake Academy, and SEARCH; has presented at many of the national digital forensic conferences; is a member of the Honeynet Project; and assisted the European Commission's CTOSE project on electronic evidence. Additional papers and tools can be found at: http://www.cerias.purdue.edu/homes/carrier/forensics

Eugene H. Spafford (spaf@cerias.purdue.edu) is a professor of Computer Sciences at Purdue University, and Executive Director of the Center for Education and Research in Information Assurance and Security. In over 25 years of research in computer science, Dr. Spafford has been responsible for a number of firsts in both information security and in cyber forensics. Among other honors, he is a recipient of the National Computer Systems Security Award, and is a Fellow of the ACM, the AAAS and the IEEE. He is currently a member of the National Advisory Board of the FBI's Regional Computer Forensic Laboratory Program, and is on the President's Information Technology Advisory Committee (PITAC). Additional information can be found at: http://www.cerias.purdue.edu/homes/spaf.