An Event-Based Digital Forensic Investigation Framework*

Brian D. Carrier carrier@cerias.purdue.edu
Eugene H. Spafford spaf@cerias.purdue.edu

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

Abstract

In this paper, we present a framework for digital forensics that includes an investigation process model based on physical crime scene procedures. In this model, each digital device is considered a digital crime scene, which is included in the physical crime scene where it is located. The investigation includes the preservation of the system, the search for digital evidence, and the reconstruction of digital events. The focus of the investigation is on the reconstruction of events using evidence so that hypotheses can be developed and tested. This paper also includes definitions and descriptions of the basic and core concepts that the framework uses.

1 Introduction

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [Pal01], the need for a standard framework has been understood, yet there has been little progress on one that is generally accepted. A framework for digital forensics needs to be flexible enough so that it can support future technologies and different types of incidents. Therefore, it needs to be simple and abstract. On the other hand, if it is too simple and abstract then it is difficult to create tool requirements and test procedures for each phase.

For this paper, we have examined the concept of an investigation to determine what is required. The result is an event-based framework that can be used to develop hypotheses and answer questions about an incident or crime. Hypotheses are developed by collecting objects that may have played a role in an event that was related to the incident. Once the objects are collected as evidence, the investigator can develop hypotheses about previous events at the crime scene.

This framework is based on the process model that is used at physical crime scenes, which has been refined from being used for dozens of years and accepted in countless court cases. Using this model we show that investigating a computer is more similar to investigating a physical crime than it is to, for example, conducting a forensic analysis of a blood sample. Our framework includes clear goals for each phase and, in future work, requirements will be developed for each phase.

Section 2 of this paper describes the basic concepts that are used in this framework. Section 3 describes the big picture of the framework and Section 4 focuses on the investigation of a digital crime scene. Section 5 compares this model to other models and Section 6 concludes the paper.

*Presented at DFRWS 2004

2 General Concepts

2.1 Definitions

Before we describe the investigation process, we need to define the basic and fundamental concepts. There are few agreed upon definitions in the area of digital forensic research, so we will clearly state the definitions we are using, even the most basic ones. *Digital data* are data represented in a numerical form. With modern computers, it is common for the data to be internally represented in a binary encoding, but this is not a requirement. A *digital object* is a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process.

In addition to its numerical representation, digital data has a physical representation. For example, the bits in a hard disk are magnetic impulses on platters that can be read with analog sensors. Network wires contain electric signals that represent network packets and keyboard cables contain electric signals that represent which keys were pressed. A computer converts the electric signals to a digital representation. Digital photography and video are a digital representation of the light associated with physical objects. Digital data can be stored on many mediums and each has different properties that determine how long the data will reside. For example, data will reside on a keyboard cable for a fraction of a second, but it may reside on a hard disk for a hard disk for years.

Digital objects have characteristics, or unique features, based on their creator and function. For example, the characteristics of a hard disk sector will be different when it is used to store the contents of an ASCII text document versus a JPEG image. We can use the characteristics to identify the data. The *state* of an object is the value of its characteristics. If a letter were changed in an ASCII text document, then the object corresponding to the file would have a new state. Similarly, the state of a running computer process changes every time data is written to its memory.

A *digital event* is an occurrence that changes the state of one or more digital objects[CS04a]. If the state of an object changes as a result of an event, then it is an *effect* of the event. Some types of objects have the ability to cause events and they are called *causes*. Note that because digital objects are stored in a physical form, then their state can be changed by both physical and digital events. An object is *evidence of an event* if the event changed the object's state. This means that the object can be examined for information about the event that occurred. However, future events could cause an object to no longer have information about past events. Every object is evidence of at least one event, because there had to be an event that created the object.

Some environments have developed policies and laws that forbid certain events from occurring. An *incident* is an event or sequence of events that violate a policy and more specifically, a *crime* is an event or sequence or events that violate a law. In particular, a *digital incident* is one or more digital events that violate a policy. In response to an incident or crime, an investigation may begin. An *investigation* is a process that develops and tests hypotheses to answer questions about events that occurred. Example questions include"what caused the incident to occur", "when did the incident occur", and "where did the incident occur".

To develop and test hypotheses about the events that occurred before, during and after the incident, we need to determine what actually happened. The only proof that an event may have occurred is if evidence of the event exists. If the object whose state was changed by the event still exists, then we can examine it for information about the event and about other objects that were causes or effects of the event. Therefore, we can make our previous evidence definition more specific and state that an object is evidence of an incident if its state was used to cause an event related to the incident or if its state was changed by an event that was related to the incident. Rynearson

observed "Everything is evidence of some event. The key is to identify and then capture evidence relative to the incident in question [Ryn02]."

For this framework, we will use the following definitions of evidence, which are a little more general and do not focus on the cause and effect relationship. *Physical evidence of an incident* is any physical object that contains reliable information that supports or refutes a hypothesis about the incident and *digital evidence of an incident* is any digital data that contain reliable information that supports or refutes a hypothesis about the incident[CS04b]. It is understood that an object has information about the incident because it was a cause or effect in an event related to the incident.

Note that because digital data has a physical form, then physical evidence can contain digital evidence. Using this definition, a hard disk is physical evidence and the sectors and files that contain information about the incident are digital evidence. Note that other guides have not made a clear distinction. The Electronic Crime Scene Investigation Guide [Tec01] describes the recognition and collection of a hard disk or other storage device as the collection of electronic, or digital, evidence. In our framework, the collection of the hard disk is the collection of physical evidence and the collection of a digital object from the hard disk is the collection of digital evidence. Also note that the difference between physical and digital evidence is in their format and has nothing to do with the type of incident. Therefore, we can have digital evidence for a physical incident or crime. For example, a digital video camera will create a digital representation of a physical event and the resulting file will be digital evidence of the event. We can also have physical evidence for a digital crime.

2.2 Digital Forensic Investigation

The preceding section discussed the basic concepts of an investigation and it never used the word forensic. To determine where, if at all, the term forensic can be applied we will first consult its definition. The American Heritage Dictionary defines forensic as an adjective and "relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law [Hou00]." Therefore, to be considered forensic, a process must use science and technology and the results must be able to be used in a court of law.

With digital evidence, technology is always needed to process the digital data and therefore the only difference between a forensic and a non-forensic investigation of digital data is whether or not the evidence can be used in a court of law. A *forensic investigation* is a process that uses science and technology to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred. In particular, a *digital forensic investigation* is a process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. The requirements to enter digital evidence into a court of law are specific to that court and will not be discussed in this paper. As an example though, consider the Daubert guidelines that are used by some U.S. courts to determine the reliability of scientific and technical evidence [SB03]. These guidelines consider if the procedure has been published, if it is generally accepted by the community, if the procedure has been tested, and if the procedure has an error rate.

2.3 Digital Analysis Types

A digital investigation may encounter many formats of digital data and therefore there exist several types of analysis. The different analysis types are based on interpretation, or abstraction, layers, which are generally part of the data's design [Car03]. For example, consider the data on a hard disk, which has been designed with several interpretation layers. The lowest layer may contain

partitions or other containers that are used for volume management. Inside of each partition is data that has been organized into a file system or database. The data in a file system is interpreted to create files that contain data in an application-specific format. Each of these layers has its own analysis techniques and requirements. Examples of common digital analysis types include:

Media Analysis: The analysis of the data from a storage device. This analysis does not consider any partitions or other operating system specific data structures. If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.

Media Management Analysis: The analysis of the management system used to organize media. This typically involves partitions and may include volume management or RAID systems that merge data from multiple storage devices into a single virtual storage device.

File System Analysis: The analysis of the file system data inside of a partition or disk. This typically involves processing the data to extract the contents of a file or to recover the contents of a deleted file.

Application Analysis: The analysis of the data inside of a file. Files are created by users and applications and the format of the contents are application specific.

Network Analysis: The analysis of data on a communications network. Network packets can be examined using the OSI model to interpret the raw data into an application-level stream.

Application analysis is a large category of analysis techniques because there are so many application types. Some of the more common ones are listed here:

OS Analysis: An operating system is an application, although it is a special application because it is the first one that is run when a computer starts. This analysis examines the configuration files and output data of the OS to determine what events may have occurred.

Executable Analysis: Executables are digital objects that can cause events to occur and they are frequently examined during intrusion investigations because the investigator needs to determine what events the executable could cause.

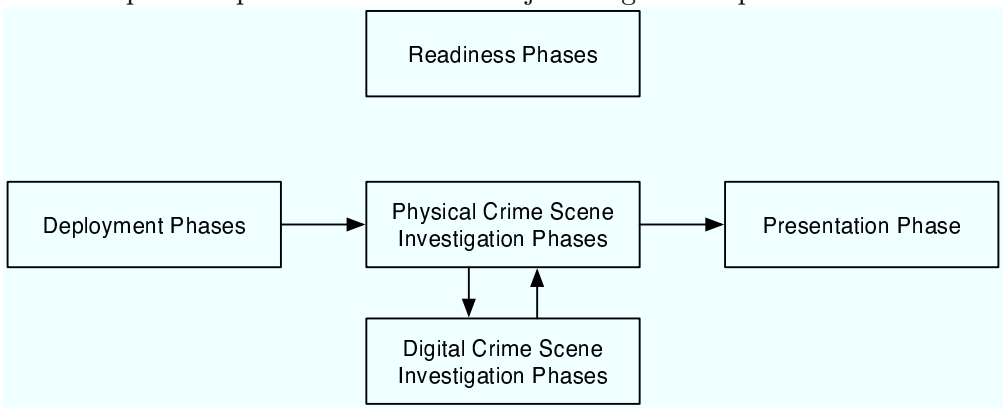
Image Analysis: Digital images are the target of many digital investigations because some are contraband. This type of analysis looks for information about where the picture was taken and who or what is in the picture. Image analysis also includes examining images for evidence of steganography.

Video Analysis: Digital video is used in security cameras and in personal video cameras and web-cams. Investigations of on-line predators can sometimes involve digital video from web-cams. This type of analysis examines the video for the identify of objects in the video and location where it was shot.

3 The Digital Investigation Process Model

We will now describe the process model that we propose. This model is based on the phases that are documented for investigating physical crime scenes [JN03][LPM01][Saf00]. The phases are applied to a digital crime scene, where we consider the digital crime scene investigation to occur as a subset of a physical crime scene investigation. The general concepts of this model have already been published [CS03]. It is organized into five categories of phases, as shown in Figure 1.

Figure 1: Graphical representation of the major categories of phases in the framework.



Readiness Phases: Includes the *operations readiness phase* that trains the appropriate people and tests the tools that will be used to investigate a system. The *infrastructure readiness phase* configures the equipment to help ensure that the needed data exists when an incident occurs. For example, in a corporate or military environment this could include adding network monitoring tools and increasing the logging levels.

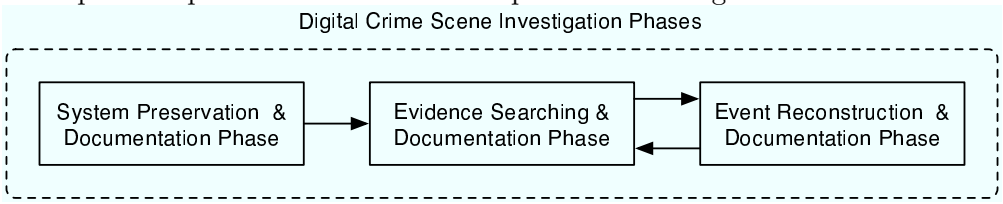
Deployment Phases: Includes the *detection and notification phase* where the incident is detected by the victim or another party and the investigators are alerted. For example, a network intrusion could be detected by an intrusion detection system and a contraband incident could be detected using the logs or communications of the suspect. This category of phases also includes the *confirmation and authorization phase* where the investigators receive authorization to conduct the investigation. In a corporate environment, this could include the incident response team doing a brief analysis of a system to confirm that it has indeed been compromised. If it is a critical system, additional permission may be needed before a full analysis can be conducted. In a law enforcement environment, the officer may need to obtain a search warrant before the investigation can progress.

Physical Crime Scene Investigation Phases: After authorization for the investigation has been granted, the physical investigation begins and the physical objects at the crime scene where a digital device exists are examined. It is in this set of phases where physical evidence will be collected that could link a person to the suspect computer activity. This set of phases includes the search for physical evidence and the reconstruction of physical events. When a physical object is found that may have digital evidence in it, a digital investigation begins. This phase will receive and correlate the analysis results from one or more digital crime scene investigations.

Digital Crime Scene Investigation Phases: Includes the phases that examine the digital data for evidence. This set of phases is actually a subset of the physical crime scene investigation phases and the conclusions that are made from the digital investigation will be used in the physical investigation. An investigation occurs for each self-contained digital device. We will examine this phase in more detail in this paper. In general, this process involves the preservation of the system, the search for digital evidence, and the reconstruction of digital events.

Presentation Phase: After theories have been developed and tested about the events related to

Figure 2: Graphical representation of the three phases in the digital crime scene investigation.



the incident, the results must be presented to either a corporate audience or a court of law. This phase deals with that process.

While each of these five categories of phases is important, this paper will focus on the digital crime scene investigation. The readiness and deployment phases are largely operational and do not involve technical analysis techniques. Although, the infrastructure readiness phase should take existing analysis techniques and challenges into account when determining what data should be recorded and saved. The deployment phases may have legal requirements, such as search warrants, but these procedures are not unique to digital investigations. The physical crime scene investigation phases are the same as those that currently exist in references on the topic and have been examined in detail. The challenges of the presentation phase include describing complex ideas in a simple fashion to a non-technical audience. This is not directly a technical research topic, but any research should take the presentation requirement into account when designing a tool or procedure and provide guidelines for effective descriptions of the technology.

4 The Digital Crime Scene Investigation Phases

This section will outline the phases in the digital crime scene investigation. This approach has three major phases and two of the phases have sub-phases that will be described in their respective section. Figure 2 shows the flow from crime scene preservation to evidence searching to event reconstruction. Each of the phases will now be described in more detail.

4.1 Digital Crime Scene Preservation and Documentation

The first phase of a digital investigation preserves the crime scene. We define the digital crime scene as the virtual environment created by the hardware and software where digital evidence about a crime or incident exists. The boundaries are made where it is natural for the environment and incident. Recall that an investigation is looking for objects whose state is an effect of an event that was related to the incident. Therefore, we want to preserve the state of as many digital objects as possible by reducing the number of additional events that may occur. Any event could modify the state of a piece of evidence and destroy the relevant information. The goal of this phase is to take steps to preserve the crime scene state. We also need to document the state of the digital crime scene so that we can later refer to its original state if anything is modified and so that we can show that a certain piece of evidence existed at the crime scene.

At a physical crime scene, this phase occurs when a first responder arrives at the scene and assists the wounded, detains suspects, and limits the amount of unofficial traffic in the area. After the area is secured, then only authorized investigators are allowed to enter. The crime scene is documented through video, photography, and sketches [LPM01].

At a digital crime scene, the actions in this phase, more than in the other investigative phases, are dependent on the goals and details of the incident. At one extreme is imaging and the system is

powered off and mirror copies of the hard disks are made. Copies of the memory may also be made using software [Ven03] or, in the future, hardware [CG04]. This type of preservation can create an exact copy of the system so that it can be recreated in a lab. This is analogous to making a copy of a building and taking it to the police station for analysis. When imaging occurs, the investigator has full documentation of the crime scene and as long as the integrity of the image is maintained then no additional steps are needed. In practice, many make a backup copy of the image as a safeguard.

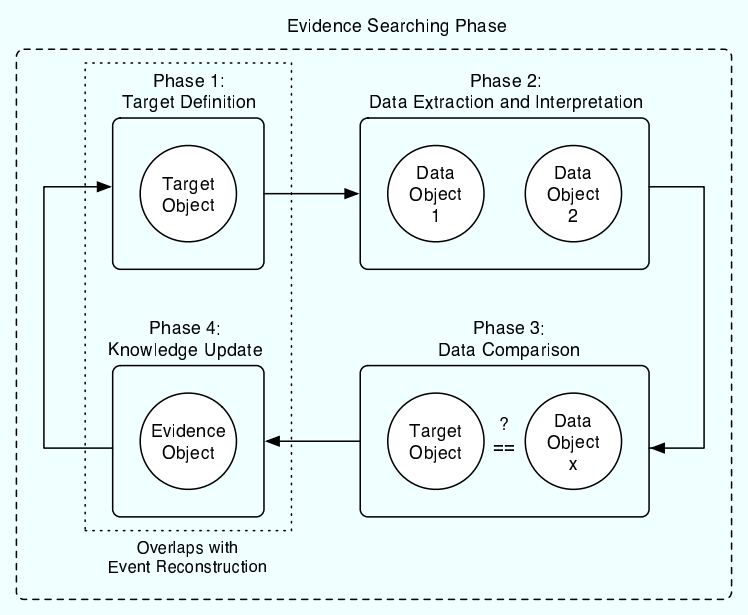
On the other extreme is not taking any steps to preserving the crime scene. This could be the scenario on a critical server where it cannot be turned off and no processes can be killed. For this scenario, the crime scene could be documented by running data collection tools from a CD and writing the tool output to a floppy disk or over the network. Somewhere in between these two extremes is the process of containment, which frequently occurs when responding to a system intrusion. Suspect processes and non-critical processes are killed so that they cannot overwrite evidence. Network filtering is applied or the network cable is plugged into an empty hub so that malicious sessions cannot occur. Copies of critical log files are copied from the system so that they are not lost. An image of the system could be made while it is still running. The goal is to keep the system running, but minimize the amount of data that is changed. This is similar to reducing the number of unauthorized people that can enter a physical crime scene. Investigators will need to walk around the crime scene to search for evidence and to document the scene, but the number is kept to a minimum and the ones that are authorized have training and it is known what they should do.

From a non-forensic investigation point of view, this phase is not required. An investigation could occur on a live system and accurate conclusions could be made. This phase is frequently performed because it improves the probability of finding reliable and relevant evidence, but the same evidence may still exist even if preservation steps are not taken. From a forensic investigation point of view, then this phase may be required. Some courts may require that the suspect be able to analyze an image of the system and therefore an image of some sort is required. General technology-based requirements can be developed for this phase, but it will be up to the courts to determine what preservation steps are required for any digital evidence to be entered into a court of law.

We have become used to the concept that an image of the disk exists, but this concept may need to be reconsidered as disk sizes get larger and it becomes infeasible to make copies of every disk. While it is useful and beneficial to be able to give the suspect a copy of the disk image, this may not be a sufficient reason why images are made. Consider a physical crime scene. Law enforcement investigators search the scene for evidence and present the evidence to the defense, but the defense does not have full access to the original crime scene to do their own investigation. Fingerprints are lifted from walls at a crime scene, but the wall is not seized as evidence. The new challenges of real-time digital forensics and uptime requirements of servers may show that evidence can be entered into court even when a complete image is not made. Unfortunately, not having a complete image may allow false conclusions to be made because the contradicting evidence does not exist.

As a final note, this phase is about the preservation of the crime scene and all objects in it. It is not about the preservation of evidence because we have not yet recognized any evidence. The term preservation is commonly used for both types of data and it should be made clear what we are referring to in this phase. The preservation of a digital crime scene is important and typically the documentation data associated with this phase is also preserved. The MD5 or SHA-1 hash is typically calculated for the images and other data that are copied from the system so that any changes can be later detected.

Figure 3: Graphical representation of the four phases that occur in the digital evidence searching phase.



4.2 Digital Evidence Searching and Documentation

After steps have been taken to preserve the state of the digital objects at the digital crime scene, the crime scene is searched for evidence. The goal of this phase is to recognize the digital objects that may contain information about the incident. Searching is a four phase process [CS04b], as shown in Figure 3. The first phase is to define a target that will be used to locate the evidence. For example, if you are looking for a file named `foo.txt`, then the target would have a name of `foo.txt`. If you are looking for a file with "bar" in the content, then the target would have "bar" in the content. The second phase is to extract data from the crime scene in some search pattern and the third phase is to compare the extracted data with the target. After new evidence is found, the fourth phase updates the general knowledge about the investigation so that more targets can be defined.

The target definition process is the most challenging of the search phase and targets are defined from either experience or existing evidence. Experience from similar cases will help an investigator to determine what types of evidence should exist and targets can be defined for them. For example, at a physical crime scene where a murder occurred, and investigator's experience may lead her to expect evidence to include any objects with blood on them and any entry or exit points to the crime scene with signs of forced intrusion. In her head, the investigator defines a target object for each of these expected types of evidence. At a digital crime scene, examples include locations where evidence could be hidden and file names that evidence often have.

Targets are also defined based on evidence that has already been found. For example, if evidence is found in a file, then a search may be conducted to find every file in the same directory. If a keyword is found inside of a file, then related searches may be conducted to find similar files.

Searches are conducted in a, typically, ordered pattern. Physical crime scene search patterns typically reflect geometric shapes and occur in lines or circles [LPM01]. At a digital crime scene, we will conduct our searches using the interpretation, or abstraction, layers [Car03]. Common examples include looking at each file, looking at each sector, or looking at each network packet.

Searches that are conducted at different abstraction layers will provide different amounts of data that can be used to recognize the evidence.

If a common class characteristic is used to define the target, then many results may be found and data reduction techniques are needed to determine which are actually evidence. For example, if a search for all files with a ".jpg" extension is performed, then thousands of files may be identified, but only a few may be contraband or evidence of an incident.

In current investigations, the target object is defined in the investigator's memory and he browses the file system and network packets looking for an object that meets the signature. The comparison is done using visualization techniques. For example, looking for a file that has a certain name or looking for a file that was modified at a give time. Keyword searches are more automated and are frequently done to find files and sectors that have specific value in their content. Hash databases are also used in an automated fashion and can be used to search for files whose content has a specific value.

After an object has been identified as evidence, then it must be documented and preserved. The requirements for documentation and preservation will depend on the legal requirements for the court. Even investigations that are conducted without a legal expectation will need basic documentation so that the evidence can be used in the next phase of the investigation. Digital evidence is typically preserved by calculating the MD5 or SHA-1 hash of it and making copies of it.

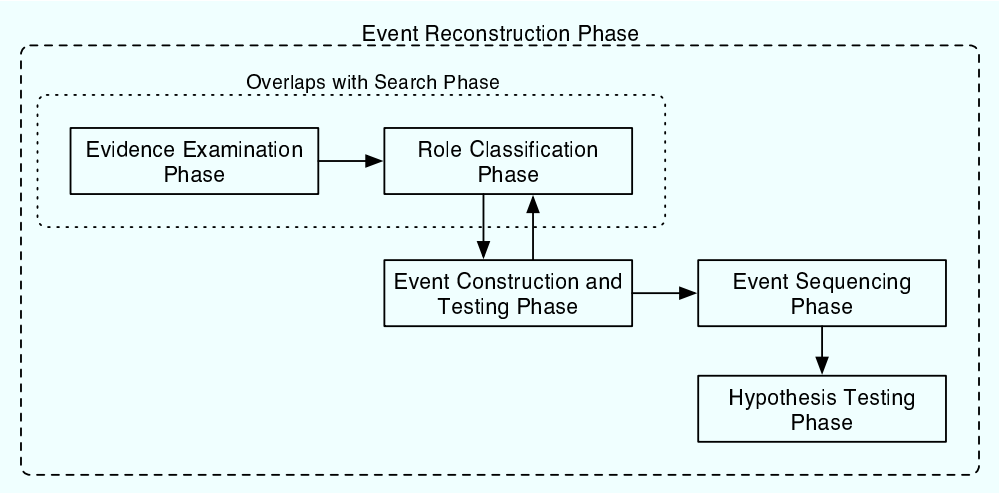
4.3 Digital Event Reconstruction and Documentation

Having an object that has characteristics that reflect possible evidence does not help to answer questions about the incident. To answer questions about the incident, we need to convert the state of the objects into the events that caused the state. For example, if a suspect file is found in the cache of a web browser then we need to develop hypotheses for how it got there. Was it copied there from the command line? Was it placed there by the web browser when the user viewed a web site? Is the directory used by other web browsers? Is the computer used by other people? To make conclusions about the suspect file, we need to develop and test hypotheses about the events that it was an effect of and, when applicable, to determine what events it could have been a cause of. The goal of this phase is to examine each piece of evidence and determine what events it was involved in so that we can determine which events occurred at the crime scene.

Digital event reconstruction is a five phase process [CS04a], as shown in Figure 4. In the *evidence examination phase*, each of the digital evidence objects are examined and identified using their class characteristics and individualized using their individual characteristics. In many cases, the evidence was examined when it was recognized during the search process, but this phase conducts any additional analysis that was not conducted. The second phase, *role classification*, examines the characteristics of each object and creates hypotheses about what roles the object could have played. For example, an investigator could examine an executable file and conclude that it could be the cause of an event to create a specific file or the cause of an event to open a network connection. Other files may have evidence that they were the effect of an object, even if the exact cause of the event is unknown. This process was likely conducted on a smaller scale during the search phase.

After all of the objects have been examined and their possible roles defined, the third phase, *event construction and testing* groups the roles together to form events. Cause and effect roles are grouped together and if other objects must exist for the event to occur then they are searched for. The search may involve the objects that have been collected or it may involve a new search of the crime scene, if it is still available. After possible events have been constructed there may be objects that should exist, but could not be found. Hypotheses about the location of these objects

Figure 4: Graphical representation of the five phases that occur during the event reconstruction phase.



should be created and justified. Once the objects have been identified, the event is tested. This will determine if the event could have occurred as expected and if the needed evidence exists to show that the event occurred.

After the discrete events have been created and tested, the fourth phase, *event sequencing*, orders the events based on their occurrence. Some objects contain temporal information that can be used to sequence two events and other objects contain functional information that can be used to determine if an event needed to occur before another. For example, data must be downloaded to a web browser before the data can be saved to disk. Events are sequenced to form event chains.

The final phase is the *hypothesis testing* phase where the hypotheses about the entire incident are tested using what is known about the events that occurred. The hypothesis must not contradict the events for which evidence exists to support. If a hypothesis relies on events for which not all objects could be found, then confidence in it must be less than the confidence in an event for which all cause and effect objects could be found. Stephenson's Petri net model [Ste03] is an example of a tool that can be used to test an incident hypothesis.

Digital event reconstruction has not been a focus of digital forensics, but it is becoming more important. Consider the recent cases in the UK where suspects have used the trojan defense, which is a defense that claims that the computer contains evidence because it was placed there by a trojan horse and not by the suspect [Geo04]. It may soon not be enough to identify the existence of a file, rather the source and events that created the file must also be determined.

After the events have been tested and sequenced, then they must be properly documented so that the final hypothesis and testing can properly represent them. Event chains can be documented by describing the cause and effect objects and what hypotheses were needed to describe why some objects were missing. The final theory is used by the physical crime scene investigation, which will integrate the results from multiple locations and come to a final conclusion.

5 Comparison to Existing Models

This process model reflects the process that has been used and tested by physical crime scene investigators. When the area of "digital forensics" is compared to other forensic sciences, then there are not many similarities. Typical forensic science areas answer comparison questions [Saf00]. An

unknown object is compared to a standard reference and the scientist determines if they are the same. An object is identified by comparing it to several references. The process that occurs in "digital forensics" on the other hand, involves searching for evidence, identifying it, and reconstructing events. The identification and comparison process is only one part of the big picture and therefore leveraging the physical crime scene investigation procedures instead of forensic procedures seems more logical.

The model proposed by DFRWS [Pal01] and later by Reith et. al. [RCG02] contains many of the same ideas as this model, but in different categories. As mentioned in the DFRWS roadmap, it is not clear how the preservation phase and collection phase are different. It is also not clear how the analysis and examination phases are different and where event reconstruction occurs. We propose that the model presented here is more intuitive and more flexible for developing requirements for each phase.

6 Conclusion

In this paper, we have presented a simple framework for the digital investigation process that is based on the causes and effects of events. The phases have been organized into the basic requirements of an investigation: namely that we need to search for evidence that shows the causes and effects of an event and we need to develop hypotheses about the events that occurred at the crime scene. Each phase has a clear goal and requirements and procedures can be developed accordingly. We have also clearly outlined the definitions and concepts that were used in this framework. Choosing a process model is a subjective process and there will likely never be an agreement on a single model. Each must be evaluated with respect to how it can scale for future technologies and how it can handle different types of investigations.

References

[Car03] Brian Carrier. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence*, Winter 2003.

[CG04] Brian D. Carrier and Joe Grand. A Hardware-Based Memory Aquisition Procedure for Digital Investigations. *Journal of Digital Investigations*, 1, 2004.

[CS03] Brian Carrier and Eugene H. Spafford. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, Fall 2003.

[CS04a] Brian D. Carrier and Eugene H. Spafford. Defining Event Reconstruction of a Digital Crime Scene. *Journal of Forensic Sciences*, 2004. To appear.

[CS04b] Brian D. Carrier and Eugene H. Spafford. Defining Searches of Digital Crime Scenes. *Under review*, 2004.

[Geo04] Esther George. UK Computer Misuse Act - The Trojan Virus Defence. *Journal of Digital Investigations*, 2, 2004.

[Hou00] Houghton Mifflin Company. *The American Heritage Dictionary*, 4 edition, 2000.

[JN03] Stuart James and Jon Nordby, editors. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, 2003.

[LPM01] Henry Lee, Timothy Palmbach, and Marilyn Miller. *Henry Lee's Crime Scene Handbook*. Academic Press, 2001.

[Pal01] 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).

[RCG02] Mark Reith, Clint Carr, and Gregg Gunsch. An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, Fall 2002.

[Ryn02] Joseph Rynearson. *Evidence and Crime Scene Reconstruction*. National Crime Investigation and Training, 6 edition, 2002.

[Saf00] Richard Saferstein. *Criminalistics: An Introduction to Forensic Science*. Pearson, 7 edition, 2000.

[SB03] Fred Smith and Rebecca Bace. *A Guide to Forensic Testimony*. Addison Wesley, 2003.

[Ste03] Peter Stephenson. Modeling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence*, Fall 2003.

[Tec01] Technical Working Group for Electronic Crime Scene Investigation. *Electronic Crime Scene Investigation: A Guide for First Responders*, July 2001.

[Ven03] Wietse Venema. *memdump*, 2003. Available at: http://www.porcupine.org/.