Survey on Digital Investigation Process Model

Sulbha V. Patil
T.G.P.C.E.T. Mohagaon, Wardha Road, Nagpur.

Revati A. Parate
A.G.P.C.O.E., Mohagaon, Wardha Road, Nagpur

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. This paper provides a useful review of previous work and then maps the digital investigative process to the physical investigative process. Their product is called the Integrated Digital Investigation Process and defines 17 phases organized into 5 groups: Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation and Review Phases. 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 and applies to both law enforcement and corporate investigations [2]. The focus of the investigation is on the reconstruction of events using evidence so that hypothesis can be developed and tested. This paper also includes definitions and description of the basic and core concepts that the framework [3].

Keywords
Digital Forensics, Law enforcement, Evidence, digital Investigation, Incident Response, Crime Scene Investigation.

1. INTRODUCTION
The field of digital forensics is undergoing a rapid metamorphosis; it is changing from skilled craftsmanship into a true forensic science. Derived as a synonym for computer Forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as "the collection of techniques and tools used to find evidence in a computer", digital forensics has been defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [1, 7].

The digital age can be characterized as the application of computer technology as a tool that enhances traditional methodologies as many criminal investigations will include computers at some point in the case [1, 2]. The incorporation of computer systems as a tool into, commercial, educational, governmental, and other facets of modern life has improved the productivity and efficiency of these entities. In the same manner, the introduction of computers as a criminal tool has enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. These "cyber-crimes" are not necessarily new crimes, but rather classic crimes exploiting computing power and accessibility to information. They are a consequence of excessive availability and user proficiency of computer systems in unethical hands. To catch and prosecute criminals involved with digital crime, investigators must employ consistent and well-defined forensic procedures or digital investigation process model that easily interacts with the physical investigations that have long existed [1, 3]. This paper is about digital investigation process model. The process model is used to develop hypothesis and answer questions about an incident or crime. Hypothesis is developed by collecting objects that may have played a role in an event that was related to the incident.

2. GENERAL CONCEPTS

2.1 Digital Data
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. 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 [3]. Network wires contain electric signals that represent network packets and key board 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 [4].

2.2 Digital object
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. 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 [3].

2.3 Digital event
A digital event is an occurrence that changes the state of one or more digital objects. 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. 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 [3].

2.4 Incident
An incident is an event or sequence of events that violate a policy and more specifically, a crime is an event or sequence of events that violate a law. In particular, a digital incident is one or more digital events that violate a policy [3].

2.5 Investigation
An investigation is a process that develops and tests hypotheses to answer questions about events that occurred. In response to an incident or crime, an investigation may begin. Example questions include "what caused the incident to

occur", "when did the incident occur", and "where did the incident occur" [3].

2.6 Physical Evidence of an incident

Physical evidence of an incident is any physical object that contains reliable information that supports or refutes a hypothesis about the incident [3].

2.7 Digital Evidence of an incident

Digital evidence of an incident is any digital data that contain reliable information that supports or refutes a hypothesis about the incident [3].

2.8 Physical Crime Scene

It is the physical environment where physical evidence of a crime or incident exists. The environment where the first criminal act occurred is the primary crime scene and subsequent scenes are secondary physical crime scenes [3].

2.9 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 [3].

2.10 Digital Forensic Investigation

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" [3]. 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 b entered into a court of law, to answer questions about events that occurred [2].

2.11 Digital Analysis Types

A digital investigation may encounter many formats of digital data and therefore there exist several types of analysis. The diff erent analysis types are based on interpretation, or abstraction, layers, which are generally part of the data's design. Following are the examples of common digital analysis types:

2.11.1 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 [3].

2.11.2 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 merged at a from multiple storage devices into a single virtual storage device [3].

2.11.3 FILE SYSTEM ANALYSIS

The analysis of the file system data inside the partition or the disk. This typically involves processing the data to extract the contents of a file or to recover the contents of a deleted file [3].

2.11.4 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 [3].

2.11.5 APPLICATION ANALYSIS

The analysis of the data in side of a file. Files are created by users and applications and the format of the contents are application specific [3].

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

1.1.1.1 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 [3].

1.1.1.2 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 [3].

1.1.1.3 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 [3].

1.1.1.4 Video Analysis

Digital video is used in security cameras and in personal video cameras and webcams. Investigations of on line predators can sometimes involve digital video from webcams. This type of analysis examines the video for the identification of objects in the video and location where it was shot [3].

3. REVIEW OF LITERATURE

Several process model have been proposed in the past and have been used to organize investigation procedures, organize training material, and identify research areas. Various such models includes an incident response model, a law enforcement model, and an abstract model as follows:

3.1 Incident Response Process Model

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.

- **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 [2].

3.2 Law Enforcement Process Model

The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide.

This process model is based on the standard physical crime scene investigation. As with the incident response model, 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.

Following are the various phases of the model:

- **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 [2].

3.3 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 [1].

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), but adds a description for each phase.

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 [1, 2].

3.4 Physical Crime Scene Investigation

For a historical perspective on investigation theory, the physical crime investigation literature was consulted. 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.

Following are the high-level phases of a crime scene investigation:

- **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 [2, 3]

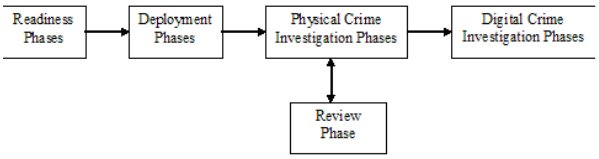
4. METHODOLOGY

4.1 AN INTEGRATED DIGITAL INVESTIGATION PROCESS

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" [2].

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 [2]. 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 [1,2].

The process model has 17 phases organized into five groups as listed below

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

4.1.1 READINESS PHASE

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.

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 [2, 3].

The **Infrastructure Readiness Phase** ensures that the needed data exists for a full investigation to occur. This phase only applies to those who maintain the environment that could be the target of a crime [2, 3]. 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 [2], creating a baseline of MD5 [2] hashes of critical executables, and maintaining a change management database

4.1.2 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 an online undercover police officer who is solicited for illegal actions. This phase defines the start of the investigation process [2, 3].

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 [2, 3].

4.1.3 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 [2,3].

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 [2, 3]. 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 walkthrough 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 [2].

In digital incident, examples of physical evidence 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 [5].

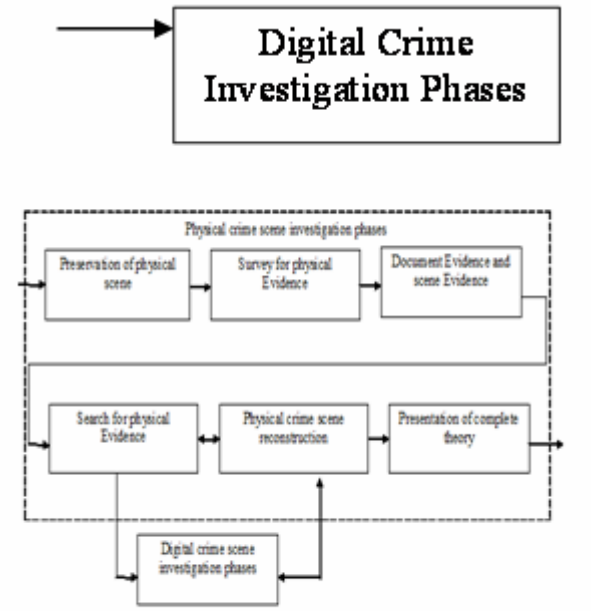


Figure 2: The six phases in the physical crime scene investigation and the interaction with the digital crime scene investigation

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 [2]. 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. 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. For a digital incident, this phase may involve looking for additional media and digital devices at the crime scene [2, 3]. 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 **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.

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

4.1.4 DIGITAL CRIME SCENE INVESTIGATION PHASE

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.

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 [2].

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 [2]. One difference of this model with respect to other models is that other models use "preservation" to refer to preserving digital evidence [3]. In this model, the entire digital environment is being preserved. 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 [5].

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 [2].

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. 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 **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.

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 [2]. 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. For some types of incidents, it is common to have both technical and non-technical investigators in this phase, 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.

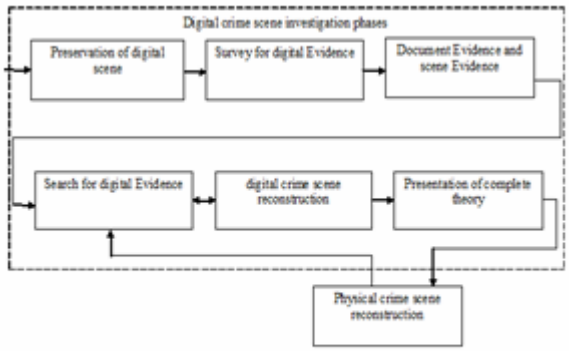


Figure 3. The six phases in the digital crime scene investigation. The results are feedback to physical crime scene investigation.

The **Reconstruction Phase** of the digital crime scene involves putting the pieces of the digital puzzle together [2]. 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 identifying additional evidence. 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. The physical crime scene team uses the results of the digital crime scene investigation in their Reconstruction Phase. 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 [2, 3]. In many cases, the physical and digital investigation teams are the same and the information is shared on an ongoing basis.

4.1.5 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 [2]. The result of this phase could be new procedures, new training, or nothing if everything actually went as planned.

5. 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. 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.

6. REFERENCES

[1] Mark Reith; Clint Carr; Gregg Gunsch, "An Examinattion of Digital Forensic Models," International Journal of Digital Evidence, vol. 1, issue 3, Fall 2002.

[2] Brian Carrier; Eugene H. Spafford, "An Getting physical with digital evidence process," International Journal of Digital Evidence, vol. 2, issue 2, Fall 2003.

[3] Brian Carrier; Eugene H. Spafford, "An Event- Based Digital forensic Investigation Framework."

[4] Ryan Leigland and Axel W. Krings, "A Formalisation of Digital Forensics," International Journal of Digital Evidence, vol. 3, issue 2, Fall 2004

[5] Golden G. Richard; Vassil Roussev; Lodovico Marziale, "Forensic Discovery auditing of digital evidence containers," Elsevier Ltd., 2007.

[6] Brian Carrier; "Open Source Digital Forensic Tools," 2003, www.atstake.com/research/reports/acrobat/atstake_opensource_fornsics.pdf.

[7] Brian Carrier; "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," International Journal of Digital Evidence, vol. 1, issue 4, 2003.

[8] Mark M. Pollitt; "An Ad Hoc Review of Digital Forensic Models," Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)

[9] http://www.digitalevidencepro.com/Resources/Approach.pdf