D11 Digital Crime Scene Reconstruction

Brian D. Carrier, MS, and Eugene H. Spafford, PhD, Purdue University - CERIAS, Recitation Building, 656 Oval Drive, West Lafayette, IN 47907*

The goal of this presentation is to show the high-level theory and procedures that have been developed for physical crime scene reconstruction can be applied to digital crime investigations. This allows the field of digital forensics to utilize theories that have been tested and proven in the courts.

This presentation will impact the forensic community and/or humanity by demonstrating the observation that digital forensics is more similar to a crime scene investigation than it is to other forensic areas. The physical computer is just the housing for many pieces of evidence, each of which can be used to reconstruct the events that occurred prior to a crime. This presentation shows how to categorize digital evidence so that it can be used in a digital crime scene reconstruction. This will make solving investigations more efficient and give more credibility to the result of digital investigations.

This paper applies the high-level theory and procedures of physical scene crime investigations to digital crimes. Using the physical crime scene investigation phases, including preservation, survey, documentation, search, and reconstruction, this paper describes how a digital device can be investigated using the same high-level procedures that have been developed over many years in the physical world. Digital devices and computers are now involved with the investigation of many crimes, including the use of a computer to attack a high profile Internet site, distributing child pornography over the Internet, or two criminals communicating via email. In each case, one or more computers must be analyzed to find traces of digital evidence. This process has been called digital or computer forensics and applies to laptops, servers, mainframes, cell phones, and PDAs.

The area of digital forensics is relatively young and is in the process of developing the theories and methodologies that are needed to make it more science than art. Digital evidence has not been seriously challenged in the courts, but it is expected to be in the future. By correlating the phases of digital investigations with those of physical investigations, credibility can be achieved for the digital investigation process.

This paper approaches the computer as a crime scene and applies the theory of physical crime scene investigation. A digital crime scene is the virtual world that is created by an operating system, software, and hardware. Data is constantly entering and exiting the system and traces of system activity are left behind. Temporary files are created when documents are opened and the Internet activity of a user can be traced days later. The classical crime scene investigation phases of securing the scene, surveying the scene for obvious evidence, documenting the scene, searching the scene for additional evidence, and performing a crime scene reconstruction all directly apply to the phases of a computer investigation. This paper provides an overview of how a computer investigation uses the same high-level phases as a physical crime scene investigation, but with different procedures. The process model considers the digital crime scene to be a secondary crime scene to the physical location where the computer is located. This is important because the end goal of any digital investigation is to identify the person responsible.

The primary focus of this paper is on the crime scene reconstruction phase for a digital crime scene, where evidence is classified and the scientific method is used to reconstruct the events that occurred during the incident. This research uses the published literature to show that digital crime scene reconstruction is similar to physical crime scene reconstruction and that digital evidence can be classified in the same categories as physical evidence, although with different criteria. For example, the existence of and contents of a given file can be functional evidence that an application was executed on the system. Similarly, the existence of deleted data that was created when an application was executed can be functional evidence. Many applications and operating systems save a history of user activity and it can be used as relational evidence because it shows what actions the user performed and in what location they were performed. Relational evidence can also be found in the existence of a temporary file that shows that an application was executed in that directory.

The paper will show how digital evidence can be sorted into each of these categories to efficiently solve digital investigations and discusses how much the evidence can be trusted. Digital investigations are becoming more common and generally accepted process models and approaches must be defined. The physical investigation procedures are generally accepted and should be applied to digital investigations whenever possible. This paper shows the first attempt at defining the process and classification definitions for digital crime scene reconstruction.

Digital Forensics, Digital Evidence, Crime Scene Reconstruction

** Presenting Author*