**The Digital Forensic Investigation Process**

Corbin Osman

American Public University System

ISSC452 - Cybersecurity

Andre Slonopas

11/26/2023

**Introduction**

The practice of forensics greatly aids law enforcement and the criminal justice system in combating criminal activity. Forensic investigators and analysts search for evidence that helps them understand how a crime was committed and who may have been involved. One area within the field of forensics that deals with the collection and analysis of digital evidence is digital forensics. This field, also referred to as computer forensics, involves the search for and analysis of evidence in the digital realm that provides insight into the actions and intents of others. It is a vital field and continues to grow in relevance as more of the world begins to use technology across all walks of life.

The purpose of this paper is to help readers understand the field of digital forensics, know its role in criminology, and teach about the digital forensic investigation process. Readers will come to understand the importance of digital forensics and learn why it is critical to follow established standards and procedures. Following a digital forensic investigation process will help investigators properly collect and carefully examine digital evidence, analyze the data and information offered by the evidence, and report on conclusions made from what the digital evidence supports.

**What are Digital Forensics?**

To best understand what digital forensics is, it is first necessary to know what digital evidence is. Digital evidence, as shared by the National Institute of Justice, is data or information either transmitted or stored that can be relied upon in a court case (National Institute of Justice). Examples of digital evidence that may be found are text or email communications, photos, videos, audio files, internet searches, and more. This information and data can contain evidence that shows how an individual or party was involved in a particular crime, and it can be found by forensic investigators and analysts. When there is suspicion of a crime having been committed, investigators will obtain legal consent to confiscate devices and accounts that may contain digital evidence. In a secure environment, they will then search for potential evidence with the help of tools and forensic practices.

**Importance of Digital Forensics in Investigations**

The field of digital forensics is important in criminology as it helps to locate evidence that can be used to prosecute criminals for their intents and actions. Digital forensics has applications in both the digital and physical worlds. Online and using technology criminals commit crimes such as identity theft, credit fraud, child pornography, and network attacks. These are often performed using technology in some form, whether online or over a network, but crimes involving digital evidence are not exclusive to just online interactions. Criminal activity performed physically such as theft, assault, and homicide can also be solved with the aid of digital forensic evidence. An example of digital forensics being used to solve a crime is the case of Larry J. Thomas vs. the state of Indiana. Larry had been accused of committing a robbery and murder, and through forensic investigation investigators were able to find evidence in one of Larry’s social media accounts tying him to pieces of evidence found at the scene of the crime (Thomas v. Indiana, 2019).

When evidence is presented in a criminal case, the evidence’s integrity must be assured. If evidence has been tampered with or interacted with improperly, the evidence may no longer be considered valid. If it is determined to be inadmissible, the data or information cannot be used as evidence. For this reason, digital evidence that is found must be collected, transmitted, stored, and examined in ways that keep its integrity intact. This helps ensure that when the time comes to present the evidence, its validity and integrity will not be questioned.

**The Digital Forensic Investigation Process**

When searching for and analyzing evidence, it can be beneficial to establish and follow a process that guides investigators and analysts through forensic investigations. Having a process and procedures to follow will help ensure that the evidence collected and analyzed will be handled properly and that time will be saved through quick and planned steps (Thakar et al., 2021). It is up to each investigation agency to determine what type of investigation process they will implement, but four general steps would be helpful to consider. These four steps are collection, examination, analysis, and reporting. Implementing these steps in some form in a forensic investigation process will help ensure that evidence is secure and properly stored.

Let us now explore each of these four steps in depth to better understand their roles and functions in the overall forensic investigation process.

**Collection**

One of the first steps to take when beginning a forensic investigation is to collect evidence that may aid in solving a crime. Within the field of computer forensics, there are certain types of evidence that investigators should search for and collect. The majority of these can be sorted into one of two categories: physical evidence and digital evidence. Physical evidence can be devices such as desktop computers, laptops, mobile devices, and external hard drives. It may also refer to peripherals or other electronic components such as routers, cables, and other media devices like cameras and music players. Digital evidence, as briefly explained earlier, usually refers to evidence in digital form such as texts, emails, videos, photos, and similar media. When exploring a crime scene, investigators should look for these and similar types of evidence to collect.

When collecting evidence that will later be examined, it is crucial that investigators properly handle, transmit, and store evidence so it remains secure. If devices are damaged in transport, the evidence they contain may be harmed. Secure cases should be available to transport devices when moving them from a crime scene to a forensic laboratory. If devices are powered on when collected, it is important to try and maintain their powered-on state as the data and information they contain are often volatile. If the device is turned off, leave it in an off state (Abdalla et al., 2007). Implementing and using a chain of custody form will show who handles evidence at specific times throughout the investigation and what examinations may have been performed. In all instances, investigators should document the evidence they find and collect so they can later show what they have collected from a crime scene.

**Examination**

The next important step after evidence has been collected and safely secured is examination. At this stage, it is still very important that data and physical evidence be properly handled so their integrity remains ensured. To avoid unintentional damage or modification of digital evidence, a strong practice is to work on a copy of the original data. This is often referred to as a forensic image. By examining the data on the forensic image, investigators can perform tests and functions to search for incriminating data and information without risking the integrity of the original data. If something happens to the copy of the data, another copy can be made from the original evidence and analysis can continue.

Within devices seized, there are several ways investigators can search for digital evidence. Using forensic applications such as the Forensic Toolkit and The Sleuth Kit allows investigators to scan devices and directories for files and information that may be used as evidence. Investigators may also run commands from an operating system’s command prompt to learn about and search a device’s file system and its contents (Abdalla et al., 2007). Scanning devices and searching for data that has been deleted may also yield results in the search for evidence. There are many more ways investigators can search devices and accounts for evidence, and the practices used will differ depending on the type of device being examined and the operating system it runs. Throughout the examination step in the forensic investigation process, it is important to keep integrity in mind and ensure that all actions taken and evidence found are recorded for later reference.

**Analysis**

When the examination process is complete, investigators will work to analyze the evidence found and attempt to understand how it relates to the crime that was committed. A few of the questions that they should ask are who created or used the evidence, who had access to the evidence, where was the evidence located, when was the evidence created, received, or shared, and how was the evidence transmitted, if at all. Investigators should not limit their analysis to these questions alone but should strive to perform a thorough analysis of the evidence collected and examined to understand the five W’s as they pertain to the crime.

Throughout the analysis process, it is important that investigators and analysts explore different possibilities for what the evidence suggests. Certain pieces of evidence may have more evidential strength than others, but even smaller pieces of evidence put together can provide sufficient insight into the details of a crime (Horsman & Sunde, 2022). At this stage in the investigation process, it may not be necessary or wise for investigators to arrive at a final opinion and conclusion about the evidence. Still, it is smart to keep relevant details and factors in mind as the investigation continues.

**Reporting**

After the analysis phase of the investigation process is finished, investigators can report on their findings and conclusions. A conclusion should be determined, but it may still help to present different possible conclusions and explain why they were not selected. The audience to which the report is to be presented should be kept in mind, as reports and findings should be shared and explained in a way that anyone can reasonably understand. Considering that evidence may be presented in a court of law that includes a jury, investigators should ensure that the evidence presented can be understood by jury members.

When appropriate, it can also be helpful for investigators to suggest solutions to prevent the crime that had been committed from happening again in the future. This can be especially helpful after an incident such as a data breach or network attack, and recommendations on how to improve security can be shared by investigators and analysts. When reports are created, they should be reviewed to ensure that all findings are accurate and presented in an optimal way. Improper reporting can result in problems with the evidence and its validity and integrity.

**Conclusion**

In summary, digital forensics plays a vital role in the discovery of evidence that helps to combat criminal activity. Forensic investigators and analysts have tools and techniques that aid them in collecting, examining, analyzing, and reporting about the evidence they collect. The integrity and accuracy of data will be assured as an established forensic process is followed, and improvements can be made in the process as newer techniques and practices are developed. In years to come digital forensics will continue to grow as newer methods of evidence recovery and examination are created, and newer technologies will aid in quicker scanning and searching of devices. Law enforcement and private agencies will benefit from training investigators and analysts in the practice of digital forensics, and more crimes will be solved as evidence is found, examined, and reported.

Resources

Abdalla, S., Hazem, S., Hashem, S. (2007). Guideline Model for Digital Forensic Investigation. *Annual ADFSL Conference on Digital Forensics, Security and Law*. 2. https://commons.erau.edu/adfsl/2007/session-7/2

*Digital Evidence and Forensics | National Institute of Justice*. (n.d.). National Institute of Justice. https://nij.ojp.gov/digital-evidence-and-forensics

Horsman, G., & Sunde, N. (2022). Unboxing the Digital Forensic Investigation Process. *Science & Justice*, *62*(2), 171–180. <https://doi.org/10.1016/j.scijus.2022.01.002>

Larry J. Thomas v. State of Indiana. 18A-CR-1714. (2019, March 27). https://law.justia.com/cases/indiana/court-of-appeals/2019/18a-cr-1714.html

Thakar, A., Kumar, K., Patel, B. (2021). Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework. *J. Phys.: Conf. Ser. 1767 012054*. https://iopscience.iop.org/article/10.1088/1742-6596/1767/1/012054