Chapter 6
Legal and Ethical Challenges in Digital Forensics Investigations

Ngozi Tracy Aleke
https://orcid.org/0009-0005-2328-5680
Illinois Institute of Technology, USA

Mohamed Trigui
https://orcid.org/0009-0007-7442-0656
Illinois Institute of Technology, USA

ABSTRACT

Digital forensics has become an essential part of modern investigative work. The main goal of this field is to analyze electronic evidence while ensuring its integrity and reliability. Digital forensics is used in a variety of cases, from identity theft to homicide and corporate disputes, often through electronic discovery, or eDiscovery. However, digital forensics faces many legal and ethical challenges. This chapter aims to answer questions about evidence admissibility, jurisdiction conflicts, privacy concerns, and compliance with search and seizure laws that create legal difficulties. Ethical concerns, such as protecting the integrity of evidence, respecting privacy, and avoiding digital bias, will be addressed. As reliance on data-driven algorithms grows, transparency and ethical oversight are needed to prevent unfair outcomes. Balancing the goals of law enforcement with the protection of basic human rights is critical to maintaining fairness, credibility, and trust in digital forensic investigations in today's rapidly advancing technological world.

DOI: 10.4018/979-8-3373-0857-9.ch006

INTRODUCTION

As technology advances, it has also brought about disputes and disagreements that require court interventions. Digital forensics refers to the processes and procedures involved in the collection and analysis of digital evidence to maintain its integrity, credibility, and admissibility in court or during a legal investigation. The aim of digital forensics is to support cases, either civil or criminal, by uncovering electronically stored relevant information. Ken Zatyko, in *Forensic Magazine*, defines digital forensics as "the application of computer science and investigative procedure for a purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validation tools, repeatability, reporting and possible expert presentation" (Zatyko, 2007). Contrary to popular belief, digital forensics transcends investigations carried out on a laptop or desktop computer. Digital forensics encompasses mobile devices, network and cloud systems, and the analysis of both digital and analog copies of images, videos, and audio files (Sammons, 2014).

During investigations that relate to digital forensics, evidence is carefully retrieved, assessed, preserved, and documented to support the investigation at hand. When the use of digital forensics is discussed, the majority of individuals tend to associate it with criminal matters relating to child pornography and identity theft only. However, the use of digital forensics also spans homicide investigations, sexual assaults, robbery, stalking, harassment, and rape, to mention just a few. Apart from criminal investigations, digital forensics is also used in civil litigation cases through a process known as electronic discovery or eDiscovery. According to TechTarget, eDiscovery refers to "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case" (TechTarget, 2005). Digital forensics is also utilized by intelligence agencies, as the proliferation of digital technologies has led to a wave of terrorist and threat actors moving their activities online. Many of these threat actors communicate online using coded methods such as cryptography and steganography tools to encrypt and decrypt information relating to their operations. For example, the US Army, through a process known as Document and Media Exploitation (DOMEX), exploits intelligence collected from digital devices recovered from the battlefield in Iraq and Afghanistan during the war in these countries in the early 2000s.