# Chapter 8
# Privacy Concerns with Digital Forensics

**Neil C. Rowe**
*US Naval Postgraduate School, USA*

## ABSTRACT

*Digital forensics is a rapidly growing technology for examining the contents of computers and digital devices. It raises many challenges to conventional notions of privacy because it involves a considerably more detailed search of digital data than is possible with other techniques, and it can be done surreptitiously. However, there are analogies to homes and the rights of individuals to be free from unwarranted searches and seizures in their private spaces. Even though commercial software and data comprises most of digital space, there are clearly enclaves of data that deserves to be kept private. We discuss the techniques of digital forensics and investigative targets. We identify key challenges to privacy, and outline both the legal protections and the technical protections available. Unfortunately, privacy laws are ineffective in most countries, and users need to take their own measures to protect themselves.*

## INTRODUCTION

Digital forensics analyzes the files and memory of computers and digital devices (Jones, Bejtlich, & Rose, 2006). It is primarily focused on the secondary storage such as magnetic disks and flash drives (containing information that remains after power is turned off), but can also examine more volatile information such as main memory and network data. Its main uses are to obtain evidence in legal proceedings both criminal (Greengard, 2012) and civil (Matthews, 2010), intelligence gathering about businesses or governments, and "malware" analysis when malicious viruses, worms, or other kinds of Trojan horses have infected a machine or device. Common uses in legal cases are for establishing whereabouts of suspects, disproving alibis, documenting criminal conspiracies, finding child pornography, proving financial fraud, and proving piracy of copyrighted material. Digital forensics can be done under court or administrative order, or when computers and devices are brought in for repair, maintenance, or discard, or by malicious software that gains a foothold on a computer.

DOI: 10.4018/978-1-4666-9905-2.ch008

In this chapter we are concerned with the privacy of information about an individual from government, business, or other organizations. Digital forensics raises such privacy concerns because it is the ultimate invasion of digital space. It can retrieve any digital artifacts left behind on a computer or device, not just those provided by the "official channels" of the operating system or software on that computer or device. It can investigate deleted data and fragments of data since it bypasses the usual access controls on computers. This means that data that users thought was hidden or long gone could be found in a forensic investigation, much more so than with Web postings and email. Forensic investigators or the people they work for could sell discovered personal data to businesses for personal gain; they could get information needed for bullying or stalking; or they could seek embarrassing information and either report it to cause damage to adversaries or use it for blackmail. Furthermore, digital forensics can find private information more quickly than navigating the technical and legal obstacles to access Web and email servers where data is typically more scattered, so digital forensics is a an effective tool to hurt someone quickly.

Even when digital forensics is conducted by responsible people, data collected could easily be misjudged. That is because there is so much of it, interpreting it is highly technical, and context is often missing unlike with, say, police searches of houses. This means that evidence is more likely to be judged suspicious by digital forensics than by conventional investigation, leading to unfair legal consequences. Furthermore, the centralization of all data in computers and digital devices makes it difficult to confine a forensic investigation to a limited set of artifacts. Hence it is difficult to follow search-authorization instructions including search warrants as to whom and what is the subject of search. In addition, it is difficult to see what is being searched in digital forensics unlike with a search of a house, so privacy may be violated without the victim being aware of it.

Clearly we need more legal protections, since current laws are not keeping up with the technology (National Research Council, 2007). The U.S., for instance, has a competing set of privacy laws whose applicability is often unclear (Rodriguez, 2014). It will help to enumerate some privacy principles for cyberspace to which most people can agree and which can serve as a basis for laws (Bernal, 2014). But in the meantime, there are technical measures that individuals can take to effectively protect their privacy such as encryption, obfuscation, and systematic erasure.

In this chapter, we will first explain the techniques of digital forensics and its targets. Then we will enumerate the key privacy issues, the legal solutions to these, and the technical solutions. We conclude with a discussion of future directions.

## THE TECHNIQUES OF DIGITAL FORENSICS

Digital forensics is a technical discipline whose main stages are media acquisition, media searching, and aggregation of results.

### Media Acquisition

Raw material for digital forensics is called "media" in the specialized sense of storage media. It may be obtained by seizing it in searches or raids, by retrieving it over the Internet when protocols allow, or by observing network traffic from a neutral site. An increasing portion of the world's activity takes place in cyberspace, so digital forensics has a good deal of potential raw material.