IDEA GROUP PUBLISHING **ITB13037**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter IV

Digital Forensics Tools: The Next Generation

Golden G. Richard III, University of New Orleans, USA

Vassil Roussev, University of New Orleans, USA

Abstract

Digital forensics investigators have access to a wide variety of tools, both commercial and open source, which assist in the preservation and analysis of digital evidence. Unfortunately, most current digital forensics tools fall short in several ways. First, they are unable to cope with the ever-increasing storage capacity of target devices. As capacities grow into hundreds of gigabytes or terabytes, the traditional approach of utilizing a single workstation to perform a digital forensics investigation against a single evidence source, such as a hard drive, will become completely intractable. Further, huge targets will require more sophisticated analysis techniques, such as automated categorization of images. We believe that the next generation of digital forensics tools will employ high-performance computing, more sophisticated evidence discovery and analysis techniques, and better collaborative functions to allow digital forensics investigators to perform investigations much more efficiently than they do today. This chapter examines the next generation of digital forensics tools.

Introduction

A wide variety of digital forensics tools, both commercial and open source, are currently available to digital forensics investigators. These tools, to varying degrees, provide levels of abstraction that allow investigators to safely make copies of digital evidence and perform routine investigations, without becoming overwhelmed by low-level details, such as physical disk organization or the specific structure of complicated file types, like the Windows registry. Many existing tools provide an intuitive user interface that turns an investigation into something resembling a structured process, rather than an arcane craft.

Unfortunately, the current generation of digital forensics tools falls short in several ways. First, massive increases in storage capacity for target devices are on the horizon. The traditional approach of utilizing a single workstation to perform a digital forensics investigation against a single evidence source (e.g., a hard drive) will become completely inadequate as storage capacities of hundreds of gigabytes or terabytes are seen more often in the lab. Furthermore, even if traditional investigative steps such as keyword searches or image thumbnail generation can be sped up to meet the challenge of huge data sets, much more sophisticated investigative techniques will still be needed. For example, while manually poring over a set of thousands (or even tens of thousands) of thumbnails to discover target images may be possible, what will an investigator do when faced with hundreds of thousands of images? Or millions?

The next generation of digital forensics tools will employ high performance computing, more sophisticated data analysis techniques, and better collaborative functions to allow digital forensics investigators to perform examinations much more efficiently and to meet the challenges of massive data sets. In this chapter, we examine some of the technical issues in next-generation tools and discuss ongoing research that seeks to address them.

Challenges

To see the challenges faced by the next generation of digital forensics tools, we examine the looming problems of scale that will soon overwhelm current-generation tools. The primary challenges are fueled by fundamental trends in computing and communication technologies that will persist for the foreseeable future. Storage capacity and bandwidth available to consumers are growing extremely rapidly, while unit prices are dropping dramatically. Along with the consumer's desire to have everything online, where music collections, movies, and photographs will increasingly be stored solely in digital form, these trends mean that even consumer-grade computers will have huge amounts of storage. From a forensics perspective, this translates into rapid growth in the number and size of potential investigative targets. To be ready, forensic professionals need to scale up both their machine and human resources accordingly.

Currently, most digital forensic applications are developed for a high-end, single or dual-CPU workstation that performs queries against a set of target media. In many cases, this