Chapter 11
Testing Digital Forensic Software Tools Used in Expert Testimony

Lynn M. Batten
Deakin University, Australia

Lei Pan
Deakin University, Australia

ABSTRACT

An expert's integrity is vital for the success of a legal case in a court of law; and witness experts are very likely to be challenged by many detailed technical questions. To deal with those challenges appropriately, experts need to acquire in-depth knowledge and experience of the tools they work with. This chapter proposes an experimental framework that helps digital forensic experts to compare sets of digital forensic tools of similar functionality based on specific outcomes. The results can be used by an expert witness to justify the choice of tools and experimental settings, calculate the testing cost in advance, and be assured of obtaining results of good quality. Two case studies are provided to demonstrate the use of our framework.

INTRODUCTION

From a legal perspective, digital forensics is one of the most potent deterrents to digital crime. While more than a dozen definitions of digital forensics have been proposed in the last ten years, the one common element in all of them is the preparation of evidence for presentation in a court of law. In the courtroom, the expert forensic witness gives personal opinions about what has been found or observed during a digital investigation. Such opinions are formed on the basis of professional experience and deductive reasoning.

A digital forensic expert must be familiar with many forensic tools, but no expert can know or use all of the forensic tools available. Questions related to digital forensic software tools used in an investigation are often asked in the courtroom. Such questions may be phrased as: "have you personally used tool A?";

DOI: 10.4018/978-1-60566-836-9.ch011

"did you use tool B because it is faster than tool A?"; "among tools A, B and C, which tool performs best in assisting this case?"; and so on. Endicott-Popovsky et al. (2007) stated that the judge, as well as lawyers on opposing sides, may be very interested in the answers to these questions in order to find possible flaws or errors in the reasoning. Moreover, the defending client may also wonder whether the expert has taken the most appropriate and cost-effective approach. Therefore, the witness must prove his or her integrity by having and applying accurate knowledge of digital forensic software tools.

Where can the forensic expert obtain information about the effectiveness of the tools he chooses to use? Current testing work is led by a few official organizations (CFTT group from NIST, 2001, 2004, 2005) often government supported, with many results unavailable to the general public, or only published for tools which have become commonly used. Mohay (2005) has argued that the increasing time gap between the release of testing results of available tools and of testing results of new tools is a major reason why newly developed tools are rarely accepted into general digital forensic practice. This chapter enables a forensic tool investigator to overcome these problems and comparatively test a set of tools appropriate to his investigation in a simple, reliable and defensible way.

We will consider "software testing" to be any activity aimed at evaluating an attribute or capability of a program or system and determining that it meets its stated or required results. Because the quality of software tools covers many aspects, testing paradigms vary on the basis of the tester's intention; thus a test may be aimed at performance, correctness, reliability, security and so on. Pan (2007) showed that testing for performance can be adapted to testing for other outcomes as long as a suitable metric for the outcome can be determined and the output can be appropriately interpreted as observations.

By way of demonstration, we focus only on performance and correctness in this chapter. Our problem can be phrased as: how can an expert witness without any specialized equipment quickly and correctly acquire knowledge of a given set of digital forensic tools?

We propose an effective and efficient software testing framework which:

- regulates what digital forensic tools should be compared in one experiment;
- identify the testing boundaries;
- determines a testing design prior to the experiment so that the tester can balance the test effort against the accuracy of the test results;
- conducts an experiment according to the testing design;
- obtains observations of good quality;
- interprets the test results (without necessitating complicated statistical knowledge).

The key contributions of this work are twofold: (a) the development of a simple but robust software testing framework for forensic expert witnesses and (b) theoretical and practical contributions from the findings of two case studies.

In the next sections, we present our testing framework for digital forensic tools along with the two case studies in testing password cracking tools and file carving tools.

A SOFTWARE TESTING FRAMEWORK FOR DIGITAL FORENSIC TOOLS

This section presents a forensic software testing framework. The framework is designed to be effective, efficient and more importantly robust against errors, and it consists of three components – selecting a