Chapter 23
A Study of Forensic Imaging to Evaluate "Unsanitized" Destination Storage Media

Gregory H. Carlton
California State Polytechnic University, Pomona, USA

Gary C. Kessler
Embry-Riddle Aeronautical University, Daytona Beach, USA

ABSTRACT

Best practices in digital forensics include a procedure to sanitize media on which forensic images will be stored, thus eliminating potential challenges that contamination of the evidence may occur due to data that exist on the media prior to storing forensic images. This article describes a research project to empirically evaluate the extent to which wiping destination storage media affects evidence. The authors specifically address whether the contents of forensic images differ in any way when written to a freshly wiped and formatted medium when compared to the images being written to a similar medium that had been populated with data and not wiped. They performed these experiments on different types of storage devices.

INTRODUCTION

"The first phase of the computer forensics process – after identifying digital devices that might have a nexus to an investigation – is data acquisition" (Kessler & Carlton, 2014). Within this data acquisition phase, forensic examiners are tasked with creating an exact duplicate of the desired media, typically by obtaining a bit-stream image of the original data (Carlton, 2007). It is essential that this first phase of the computer forensics process be performed correctly, as failure to adhere to the established methodology could result in the evidence not being admissible in court (Casey, 2011).

DOI: 10.4018/978-1-7998-3025-2.ch023

Currently, the established best practice for forensic data acquisition of media includes sanitizing the target media (i.e., the media that will contain the forensic bit-stream image files [BSIFs] of the source data). This sanitization task consists of wiping and freshly formatting the target media prior to writing the BSIF onto it. This task is performed, presumably, to prevent contamination of evidence when writing forensic images onto media that contain "old" information (Kent, Chevalier, Grance, & Dang, 2006; Nolan, O'Sullivan, Branson, & Waits, 2005; SWGDE, 2012).

We were concerned that because of the "best practice" status of this sanitization task, challenges could be mounted to the validity of evidence contained within BSIFs stored on non-wiped media. Such challenges have the potential to exclude digital evidence from being admitted solely due to the fact that the scientific process of forensic data acquisition was not met rather than any direct proof that the BSIFs were actually tainted. We posit that these challenges result from a deviation of ritual rather than a basis in fact demonstrated by the science of the forensic data acquisition process. To evaluate our concerns and measure our hypothesis, we established a series of experiments that are described in the following section.

We contend that the results of these reproducible and repeatable experiments conducted in a controlled environment utilizing scientific methodology and subjected to peer-review will establish a basis from which the courts can address this matter with confidence.

TESTING FRAMEWORK

Our test framework is presented below in four sections, identified as: hypothesis, test framework, test design, and source data.

Hypotheses

Our null hypothesis is "wiping a storage medium has no affect on the content of a BSIF that is written to that medium." Thus, we are testing the claim that the sanitization task is unnecessary by a series of experiments to measure the effect that sanitizing (i.e., wiping) target media has on forensically acquired bit-stream images. This hypothesis is based upon the realities of current practice, in particular, the format of modern BSIFs and the large number of instances where the BSIF is written directly to a network storage device that is clearly not "sanitized" prior to such storage.

Test Framework

There are many variables in the digital forensics data acquisition process, including the operating system (OS) and file system of the source device, the OS of the acquisition device, the imaging tool employed (which might be hardware or software), the type of destination media, and the type of BSIF. To test our hypothesis, we concluded that the only relevant variable was the BSIF type.

There are a large number of BSIF formats (Forensics Wiki, 2012), including:

- AccessData format (AD1)
- Advanced File Format (AFF and AFF4)
- dd raw image
- Encase image (E01, Ex01, L01, and Lx01)