Chapter 2
Digital Evidence

Richard Boddington
Murdoch University, Australia

ABSTRACT

Digital evidence, now more commonly relied upon in legal cases, requires an understanding of the processes used in its identification, preservation, analysis and validation. Business managers relying on digital evidence in the corporate environment need a greater understanding of its true nature and difficulties affecting its usefulness in criminal, civil and disciplinary proceedings. This chapter describes digital evidence collection and analysis, and the implications of common challenges diminishing its admissibility. It looks at determining the evidentiary weight of digital evidence that can be perplexing and confusing because of the complexity of the technical domain. Digital evidence present on computer networks is easily replaced, altered, destroyed or concealed and requires special protection to preserve its evidentiary integrity. Consequently, business managers seeking the truth of a matter can find it a vexing experience, unless provided with a clear appraisal and interpretation of the relevant evidence. Validating evidence, that is often complex and incomplete, requires expert analysis to determine its value in legal cases to provide timely guidance to business managers and their legal advisers. While soundly configured security systems and procedures enhance data protection and recovery, they are often limited in the way they preserve digital evidence. Unprepared personnel can also contaminate evidence unless procedural guidelines and training

DOI: 10.4018/978-1-60566-806-2.ch002

are provided. The chapter looks at the benefits for prudent organisations, who may wish to include cyber forensic strategies as part of their security risk contingency, planning to minimise loss or degradation of digital evidence which, if overlooked, may have adverse legal repercussions.

INTRODUCTION: THE INVESTIGATION DOMAIN

Chapter two introduced the digital evidence domain and this chapter expands on this by providing details of how to handle digital evidence in order to preserve its integrity in court.

Forensic science adopts six stages in the investigation of forensic evidence that recognize, preserve the scene, classify, compare and individualize, and reconstruct the evidence (Crime Scene Investigation, 1994). Cyber forensics is still in its infancy and non-standardized processes are common in some civil and criminal investigation agencies, and standards, if they do exist, vary in different jurisdictions (Baryamureeba & Tushabe, 2006; Carrier & Spafford, 2003; Whitcomb, 2002). Courts expect computer forensic investigators and forensic auditors to have a sound understanding of computer technology for their testimony to have any credibility. This technical expertise is also important in civil actions and disciplinary proceedings, not intended to appear in court cases, to ensure that natural justice takes place (Mohay, 2003).

Several cyber forensic investigation models are in use emphasizing slightly different stages in the investigation process, and there is no universally agreed model used by investigators (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). Figure 1 is a simple model highlighting the processing of digital evidence in the investigative and legal domains. The investigation domain consists of four stages taken by investigators in evidence preservation, location, selection and validation that precede the two stages in the legal domain involving legal practitioners constructing and then presenting legal arguments (Boddington, Hobbs, & Mann, 2008).

Preserving the Evidence

Preserving the evidence is the critical first stage in the investigative domain and may be overlooked by business managers, who fail to appreciate the fragility of digital evidence and take the correct steps to avoid contamination or loss of the evidence. Well-intentioned, but uninformed and improper handling and examination may fail to stabilize the evidence and may actually cause it to be altered, damaged, destroyed or contaminated (Ashcroft, 2001; Carrier, & Spafford, 2003). It is important to minimize overwriting digital evidence at the point of seizure and during the copying