



QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Computer Forensics Overview

If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing and presenting evidence to the courts. (The word forensics means “to bring to the court.”) Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.

Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal “scientific” discipline. We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks and wireless communications and storage devices in a way that is admissible as evidence in a court of law.

This paper will discuss the need for computer forensics to be practiced in an effective and legal way, outline basic technical issues, and point to references for further reading. It promotes the idea that the competent practice of computer forensics and awareness of applicable laws is essential for today’s networked organizations.

Included in this ZIP file are:

- Intro Page.pdf
- Terms and Conditions.pdf
- Computer Forensics Overview.pdf