IDEA GROUP PUBLISHING
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

ITB13039

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos© 2006, Idea Group Inc.

Chapter VI

Log Correlation: Tools and Techniques

Dario Valentino Forte, CFE, CISM, Italy

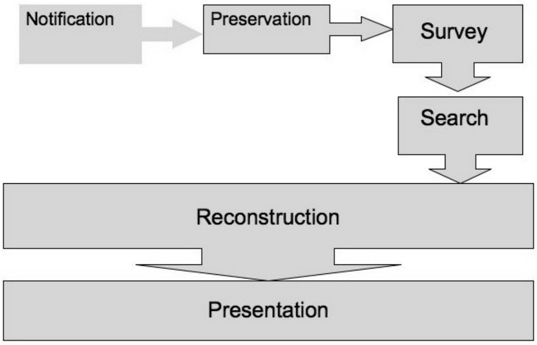
Abstract

Log file correlation comprises two components: Intrusion Detection and Network Forensics. The skillful and mutualistic combination of these distinct disciplines is one of the best guarantees against Points of Failure. This chapter is organized as a tutorial for practitioners, providing an overview of log analysis and correlation, with special emphasis on the tools and techniques for handling them in a forensically compliant manner.

Digital Forensics: Background

The increasingly widespread use of distributed systems requires the development of more complex and varied digital forensic investigative procedures of both the target (the attacked machine) and the analysis platform (forensic workstation). Our discussion here of log analysis and related issues will focus on UNIX-based platforms and the various UNIX "dialects" such as Solaris, AIX, xBSD and, of course, LINUX.

Figure 1. The investigative process



A Digital Forensics Primer

Forensic operations are essentially platform independent, although the same cannot be said for all file systems and log files. In order to adhere to the rules of due diligence contained in the IACIS (International Association of Computer Investigative Specialists, www.cops.org) code of ethics, we must have a clear idea of the general characteristics of file systems and their corresponding log files.

First, let us understand what is meant by "investigative process" in a digital forensics context. This process comprises a sequence of activities that the forensic examiner should carry out to ensure compliance with juridical requirements now common to all countries.

The investigative process may be broken down into six steps (Spafford & Carrier, 2003) as illustrated in Figure 1.

- **Notification:** When an attack is detected by an automatic device, internal personnel, or via external input (for example by a system administrator in another company, or by another business unit in the same company) a first report is generated. The next action usually entails setting up and deploying a response team, whose first task is to confirm that an attack has indeed occurred.
- **Preservation:** This critical incident response step represents the first digital forensic action. The main objective here is to ensure that no alterations are made to the scene of the crime so as not to preclude any future investigative or analytical measures. The "digital crime scene" is usually duplicated via the creation of an image disk so that detailed analyses may subsequently be performed in a properly equipped laboratory.
- **Survey:** This is the first evidence collection step. The scene of the crime is examined for any obvious digital evidence and hypotheses are developed to orient further investigation.