

TRACK: IT Advanced
SESSION #: ITA7
DATE: Tuesday February 5, 2008
TIME: 1:00-2:00PM
SESSION TITLE: “Log Forensics Uncovered”
SPEAKER(S): Anton A. Chuvakin, Phj.D , Chief Logging Evangelist
ORGANIZATION: LogLogic

ABSTRACT: As high profile data breaches like the recent one with TJ Maxx grab headlines and as corporate regulations like PCI and Sarbanes-Oxley continue to emphasize preserving and securing data and assurance of IT controls, organizations are increasingly looking for ways to collect and manage immutable IT data. Unfortunately, this task can be difficult and time consuming. However, logs often can provide most of the answers needed for the investigators without diving deeply into a time-consuming disk image forensics. In this presentation, Dr. Chuvakin will cover the use of various systems and network logs and audit trails in forensic processes, beginning with the an important issue of defining “log forensics.” He will then describe a methodology for log collection and analysis – with forensic use in mind - as well as practical examples. In addition, he will touch on the rarely-covered but critical item of preserving log evidence integrity and possible challenges to such integrity.

Attendees will learn:

- Logs: What and Where From?
- Log Analysis: Why and How
- Defining Log Forensics
- Specifics of Log Analysis for Forensic Use
- Challenges to Data Integrity and Response

SPEAKER BIO(S): Anton A. Chuvakin, Ph.D is Chief Logging Evangelist at LogLogic, a log management and intelligence company. His role is to define and execute a product vision, strategy and roadmap in addition to conducting research and supporting key customers with their implementation requirements. His areas of interest are intrusion detection, log analysis and log data mining, computer forensics, honeynets/honeypots, Unix security and “Social engineering.” A frequent speaker and author of numerous publications, Dr. Chuvakin has been a co-author, contributor and editor of books in on topics in his field. He holds multiple certifications related to computer forensics and information security and received his Ph.D. in Physics from SUNY at Stony Brook.