

▶ INFORMATION
TECHNOLOGY
FORENSICS

CONSULTING &
INVESTIGATIONS

INFORMATION
SECURITY

NETWORK FORENSICS

In our highly networked world, electronic evidence is not just the files on workstations and servers. Computer networks create massive amounts of data in the form of log files, audit trails, and system parameters. All this data can become crucial evidence in a variety of matters including, but not limited to, internal fraud, intellectual property theft, wrongful termination, harassment, and commercial litigation. OnlineSecurity's network forensics services provides evidentiary analysis and data collection from computer networks to determine what, when, how, and why events occurred.

Service Description

Network forensics can take many forms based on the extent and availability of log files, audit trails, and other system data. In addition, the requirements of the matter will dictate what service is provided. Some examples:

- ▶ Reviewing access logs to determine if a competitor accessed proprietary information.
- ▶ Reviewing log files from an email server to determine if, in fact, an email was received.
- ▶ Recreating a network environment to recover information and evidence from backup systems.
- ▶ Reconstructing the time series of events on a network to determine exactly when information was used.
- ▶ As required by the specific needs of a matter, OnlineSecurity forensics engineers will craft a custom solution to secure all available evidence from a network in a legal matter.

Delivery Mechanism

- ▶ OnlineSecurity will meet with the client to determine the scope of forensic analysis and evidence collection as dictated by the specific parameters of the matter.
- ▶ OnlineSecurity will also meet, unless restricted by the particular requirements of the matter, with the system administrators of the network to avoid business interruption or network downtime.
- ▶ Forensic analysis and collection can be performed at the client site or at OnlineSecurity's forensic laboratory depending on the requirements of the matter and the nature of the network metadata examined.
- ▶ Throughout the forensic process, OnlineSecurity engineers will follow court accepted forensic protocols, so that in the event the evidence must be presented in court, OnlineSecurity can testify to the authenticity, integrity, and veracity of the evidence.

Deliverables

- ▶ Subject to discovery and disclosure considerations, OnlineSecurity will provide to the client a detailed forensics report encompassing network architecture, forensic parameters, and observations.

Pricing

- ▶ Quotes for network forensics are based on the specific considerations of the engagement, i.e. location, number of systems, system architecture, depth of analysis, etc. and will be priced by time and material required.

L

Los Angeles

5870 W. Jefferson Blvd., Suite A
Los Angeles, CA 90016
voice: 310.815.8855
fax: 310.815.8808

New York

Boston

Seattle