SILENTRUNNER MOBILE NETWORK FORENSICS SOFTWARE IS LIKE HAVING A SURVEILLANCE CAMERA ON YOUR SUSPECT'S NETWORK

Operating like a network surveillance camera, SilentRunner Mobile allows you to monitor, capture, analyze and graphically visualize network traffic to see exactly what a suspect is doing during a law enforcement or government digital investigation. Captured network activity can be played back on demand. Furthermore it's easy to deploy to enable quick access to network traffic once surveillance is determined to be necessary.

It is a passive network monitoring solution that visualizes network activity by creating a dynamic picture of communication flows, giving you a clear picture of your suspect's activities. SilentRunner Mobile can play back events from thousands of communications to validate whether criminal or malicious activity has taken place. This dramatically enhances your ability to identify all offenders and exploits, build a case, and locate any stolen information or misused resources.

Product Details:

Network Forensics Software for Real-Time Capture and Visualization

- SilentRunner *Mobile* promiscuously monitors and records network traffic in all seven layers of the Open Systems Interconnection stack.
- Monitors more than 2,500 protocols and services out of the box.
- High-performance collection of network speeds up to 100 Mbps with advanced processing and indexing.
- Advanced visualization tools allow you to create a picture of communication flows to swiftly expose anomalies, illegal connections and security and network problems.
- Using interactive graphical representations illustrating propagation, you can
 efficiently analyze users, hosts, domains, applications, protocols and addresses —
 detecting changes or abnormalities from established network baselines.
- Capture and analyze wireless Ethernet 802.11a and 802.11n.
- Capture and analyze webmail, chat and social media content.
- Receive real-time email alerts.

Content and Pattern Analysis

- Determine the exact behavior of a suspect by viewing their network usage patterns and which content they're accessing.
- Build "integrated maps" of certain assets or users such as after-hours usage spikes, data traffic or malware.
- Independent of keyword or linguistic matching, you can determine how proprietary or inappropriate information proliferated from code servers, HR or financial databases, R&D labs and others.

Network Forensic Analysis and On-demand Incident Playback

- SilentRunner Mobile stores and catalogs network data into a central repository allowing you to play back the exact sequence of events aiding to ensure effective and accurate investigations.
- Directly visualize audit logs and alerts, and correlate actual network traffic to provide a complete picture of activity around the time a suspicious event occurred.
- Load custom filters, for example, an Excel spreadsheet with 2000 IP addresses.
- Play back captured VolP calls in seconds.
- Web reconstruction reporting: keyword searches, file transfers, video files and more, within captured Web traffic.
- Conduct post-event analysis and reconstruct events in their exact sequence to immediately uncover malicious or illegal behavior.
 - SilentRunner Mobile maintains a millisecond clock to record packet timing.
 - Quickly determine communication precedent and data proliferation.

Flexible Architecture

- Leverage distributed monitoring to gain visibility into multiple network segments at once and correlate network data across the enterprise.
- SilentRunner supports both centralized and distributed database architectures to provide quick and efficient data analysis.
- Mobile deployment supports local policy audits and investigations.

Contact

Request Information

Brochures

- <u>SilentRunner Mobile</u>
- SilentRunner FAQs
- VoIP Investigations FAQs
- AD Legal Brief
- SilentRunner Real-World Applications
- MORE >

White Papers

- SilentRunner Privacy White Paper
- LEGAL JOURNAL: The Rules of Evidence and AccessData Technology
- The Importance of Integrating Host and Network Forensics
- MORE >

Product Webinars

- SilentRunner: Integrating Network Forensics into Your Investigative Arsenal
- SilentRunner: VoIP Investigations

Go To Top »

Products

- Forensic Toolkit
- AD Enterprise
- AD eDiscovery
- AD Summation iBlaze
- AD Summation Enterprise
- AD Summation CaseVantage
- CIRT
- SilentRunner Sentinel
- AD Lab
- Mobile Phone Examiner Plus
- Distributed Network Attack
- Password Recovery Toolkit

Support

- AD Downloads
- Previous Releases

- Discussion Forum
- Technical Papers

Resource Library

- Brochures
- White Papers
- Webinars

Training

- AccessData Bootcamp
- AccessData Forensics
- Windows Forensics 7
- FTK 3 Transition Day
- Applied Decryption
- Internet Forensics
- Windows Forensics XP
- Windows Forensics Vista
- Windows Forensics Registry
- Mobile Forensics 101
- Mobile Forensics 202
- Mobile Forensics 303
- MORE

Contact Us

- Americas/Asia Pacific
- Europe/Middle East/Africa
- Summation Software Support
- eDiscovery/Litigation Support Services
- Discovery Cracker Support