



NETWORK FORENSICS

LIMA DPI MONITOR

new needs need new solutions

LIMA DPI Monitor

LIMA DPI is a passive probe system for lawful interception and network monitoring. It uses deep packet inspection (DPI) technology to classify network flows according to their application protocol. Based on user-definable rules, content and signaling data of these flows can be recorded and forwarded to external devices such as mediation systems for further processing. These rules comprise target information including IP addresses, user names, protocol-specific filtering criteria, and arbitrary content keywords. This combination of DPI and flexible target rules delivers high quality interception avoiding the capturing of a large volume of unnecessary network traffic.

Highlights



- Wire speed lawful interception and network surveillance up to 10 Gbit/s and beyond
- Full layer-7 traffic classification with support for encrypted protocols
- Flow-based interception with TCP reassembly and application specific decoding
- Powerful protocol and keyword-based interception rules
- Stream buffer for complete session interception
- Intelligent data reduction at interception point
- Seamless integration in any LI infrastructures such as ETSI, CALEA or customer specific implementations
- Protocol-specific CDR/IPDR generation
- Supports over 140 protocols



High quality search and interception data

LIMA DPI's protocol awareness enables the deployment of powerful application-specific interception rules such as the dedicated search for e-mail addresses, instant messenger user names or SIP phone numbers within relevant flows. It also provides general keyword trigger criteria taking into account the various application-specific encoding schemes such as MIME Base64 encoding for e-mails or gzip compression for Web content. All keyword-based interception trigger criteria are evaluated on fully reassembled TCP streams. The reliable protocol classification of LIMA DPI ensures that all intercepted network sessions only contain packets belonging to them. It provides clean interception data to subsequent mediation and reconstruction systems, improving their accuracy and performance.

Full Session Buffering

Many interception trigger criteria produce a match late in a network session when previous packets have already passed. For many LI applications it is key that complete sessions starting with the very first data packet are intercepted, even if, for instance, a keyword match only happens in the second attachment of an e-mail message. LIMA DPI includes a full stream buffer that stores all sessions that are being monitored and have not yet produced a search hit. The maximum buffering period depends on the number of concurrently monitored sessions, the hit-miss ratio, and the stream buffer capacity in each DPI probe.

Network Statistics – Added Value for ISPs

LIMA DPI probes record detailed traffic statistics that provide operators with in-depth network visibility. Current and historical bit and packet rates for all protocols are available directly on the DPI system in graphical and tabular form. Detailed application statistics can be generated and exported to external database or analysis systems. The application metadata generated by the DPI engine is used to create rich IP detail records (IPDR) that include all information available about a recorded network session.

LIMA DPI benefits

- Intelligent interception and targetting
- Real-time detection up to multiple 10 Gbit/s links and beyond
- Extensive protocol support, updated with regular maintenance releases
- Based on Commercial Of The Shelf hardware