Trisul Network Metering and Forensics

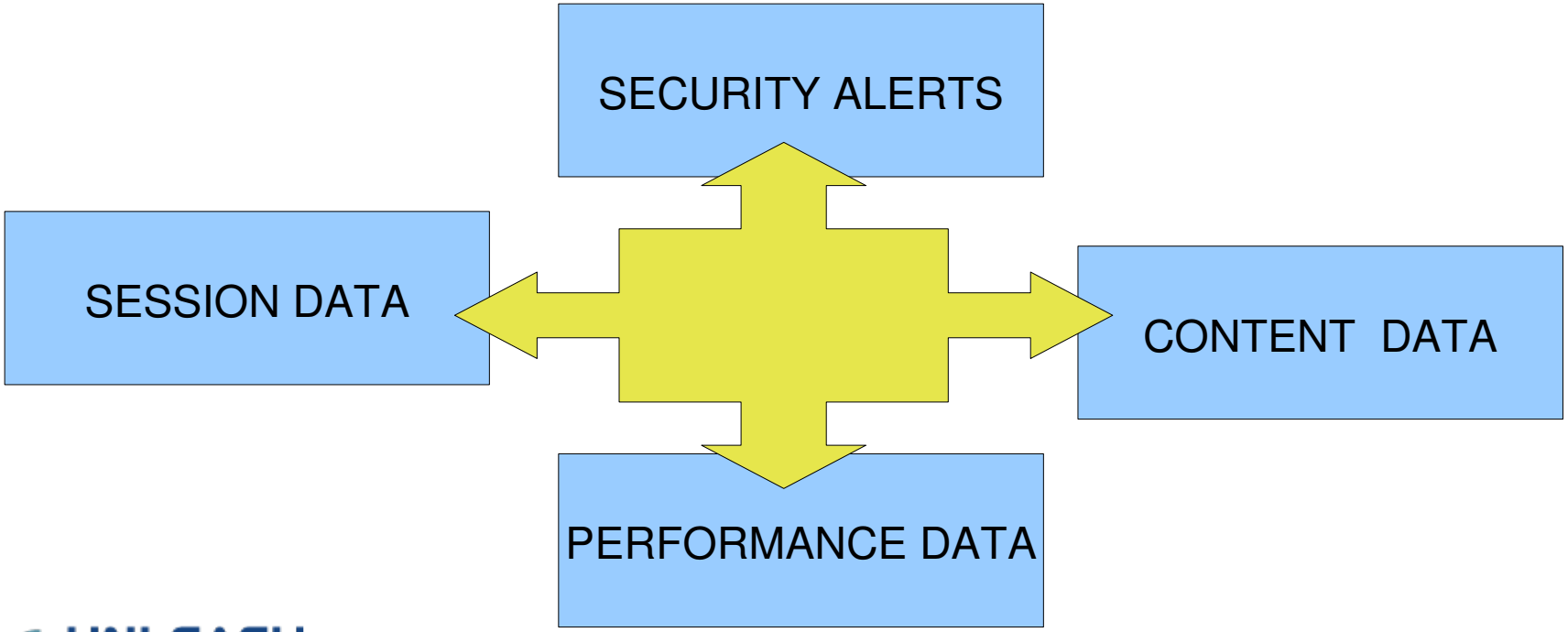
Really know your network

UNLEASH networks

Trisul Network Metering and Forensics

What is Trisul

- A new Network Security Monitoring platform
- Gives you unprecedented visibility into your network activity
- Real time and Retro analysis features
- Pulls together four vital aspects of todays networks



Trisul Network Metering and Forensics

Trisul capabilities

- 24x7 Linux based
- Runs on commodity hardware
- Supports Packet capture, Netflow, or PCAP import
- Tracks detailed L2 and L3 usage statistics
- Isolate and drilldown specific targets
- Stores raw packets for deep inspection (forensics)
- Stores flow details
- Integrated with Snort IDS to correlates threats
- Support for various top-N

How it differs from SNMP and Netflow based tools ?

- Can track Layer 2 events and anomalies
- Gives you exact packets that can later be investigated by Unsniff or Wireshark
- Jump from statistics to flows to security alerts – finally to raw content
- Much more granular than Netflow, no load on router if using a tap
- Trisul can also accept Netflow records (so it is a superset of Netflow based tools)

Trisul Network Metering and Forensics

Applications

- 24X7 perimeter monitoring
- Pin point network utilization tracking
- Data Leak Prevention
- Aid incident investigation
- Retro analysis help desk
- Track down L2 issues now and in the past
- Policy violations
- Statutory monitoring as part of SLA
- Part of corporate security posture
- Daily security and health reporting via PDF reports
- more..

UNLEASH networks

Trisul Network Metering and Forensics

Security Features

Due to the sensitive nature of the product it has been designed with security in mind

- Forensics Module is optional
- Multiple layers of security
- All communication over TLS (DHE is the default key exchange)
- ACL only allows certain subnets to access the system
- Three levels of access (Admin, Operator, Forensics)
- Each user requires current certificate from network administrator
- If forensics enabled, content further encrypted by AES-128
- Can filter privileged subnets/hosts from being monitored

Trisul Network Metering and Forensics

Products in the Trisul family

Trisul Network Metering and Forensics

Core 24x7 platform

Unsniff Network Analyzer 2.0

Portable network analysis platform. Windows based multi layer visualizer for Trisul

Web Trisul

Web based interface to Trisul. Available in Beta today and GA in Dec 09.

Trisul Network Metering and Forensics

Who we are

- Unleash Networks
- Technology partner of Elina Networks
- Deep knowledge of Mobile and IP Core technologies
- Make cutting edge products for network analysis
- Deep packet inspection, security, and forensics a key strength
- Awarded Nasscom Top 100 Innovators of 2007

Flexible Plans

- Deployment of 24x7 monitoring platform Trisul
- IP / GPRS Packet Core Network Auditing
- Month-to-month rental based deployment also available
- IP Security monitoring and auditing also available
- Other time limited services

UNLEASH networks

Trisul Network Metering and Forensics

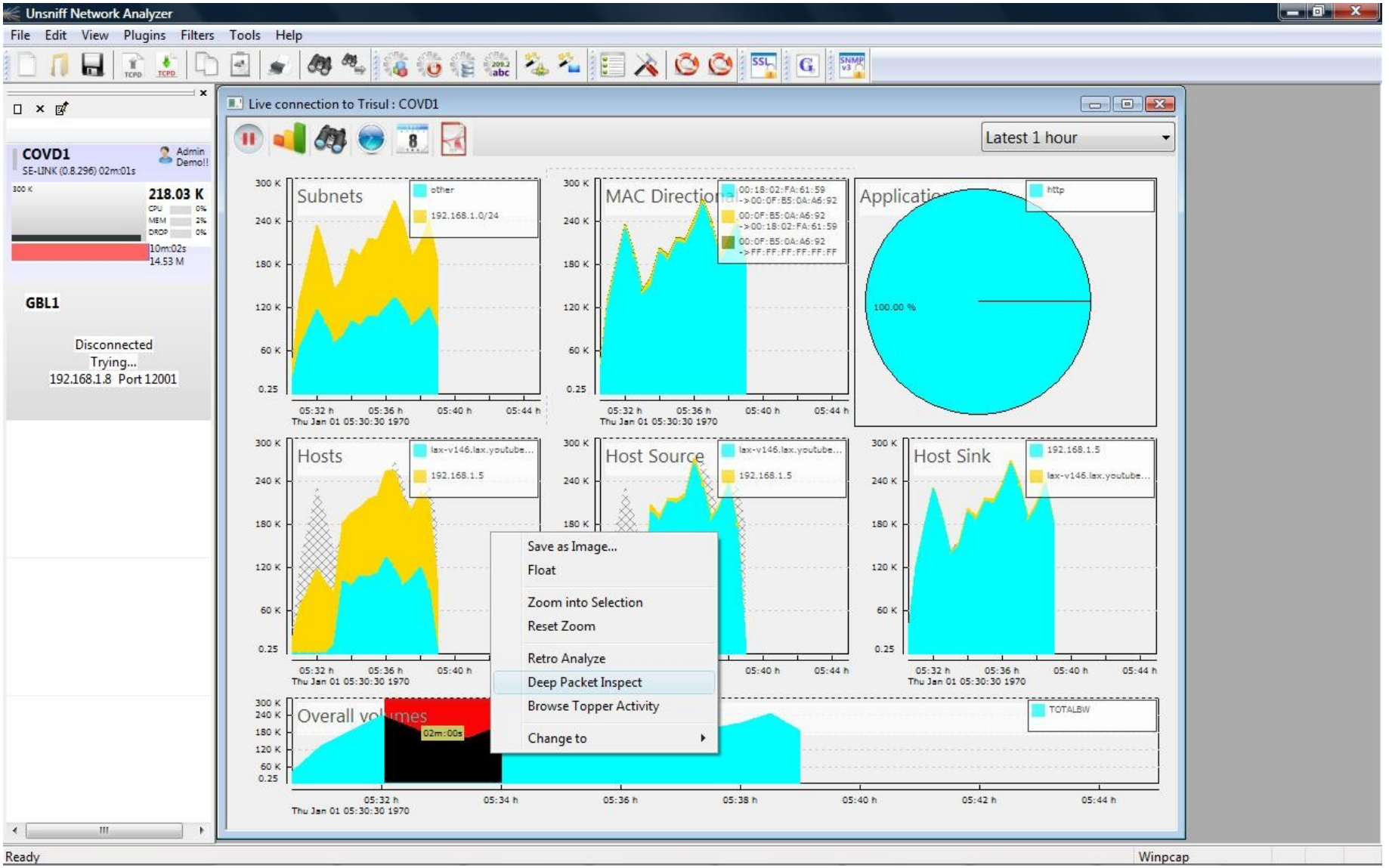
You can download time limited versions of some of our software

http://www.unleashnetworks.com

THANK YOU

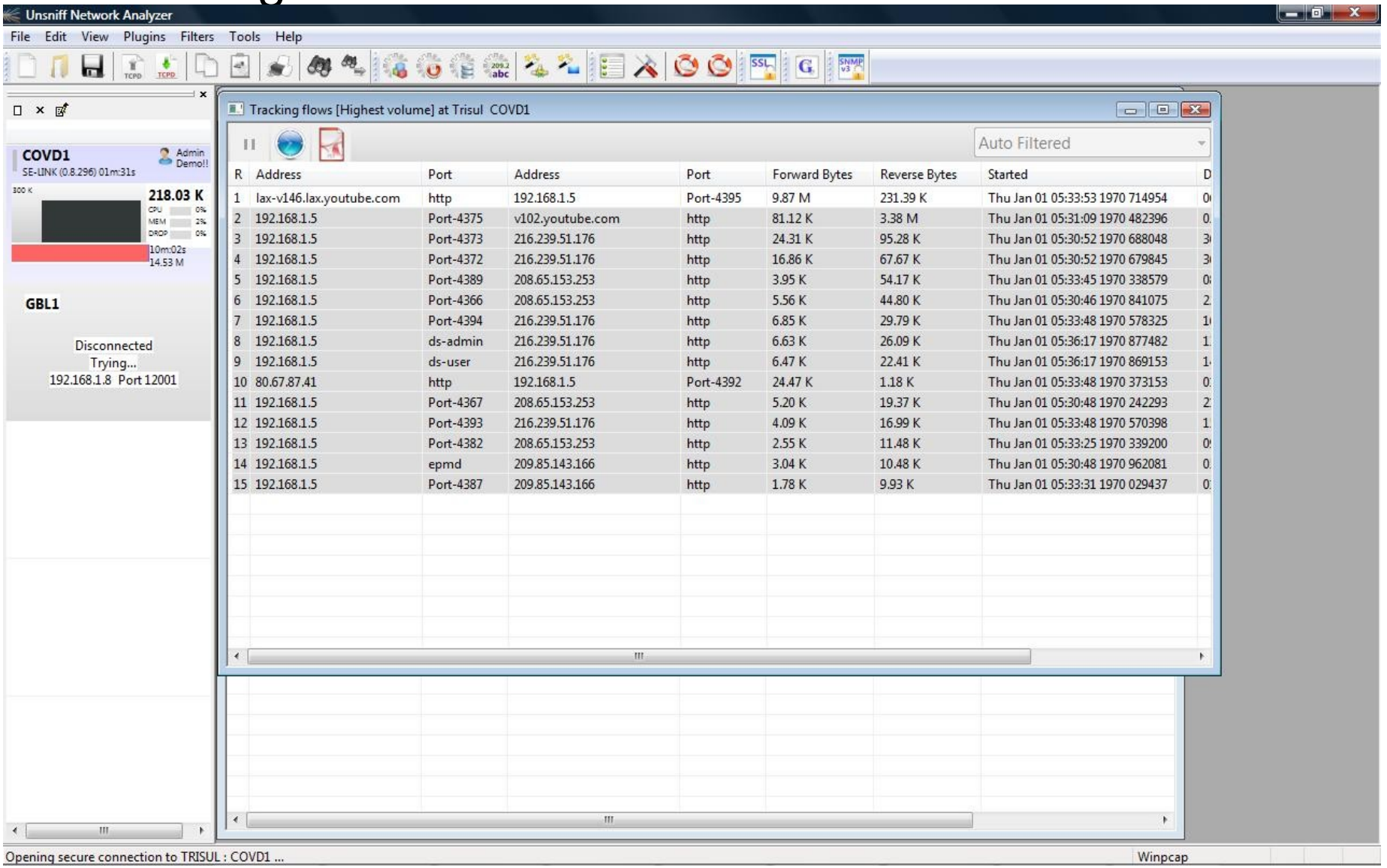
UNLEASH networks

Trisul Network Metering and Forensics
Live view and drilldown



UNLEASH networks

Trisul Network Metering and Forensics
Flow monitoring



UNLEASH networks