Paper 1

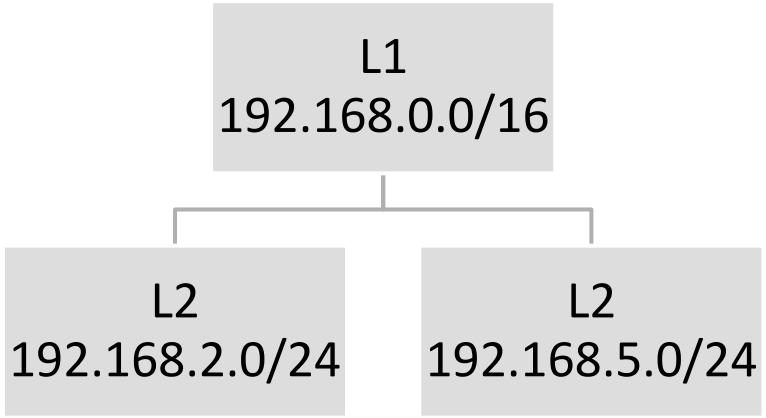
- ***OverFlow: An Overview Visualization for Network Analysis***
  - 2009. Glanfield, Brooks, Taylor, Paterson, Smith, Gates, McHugh

Motivation

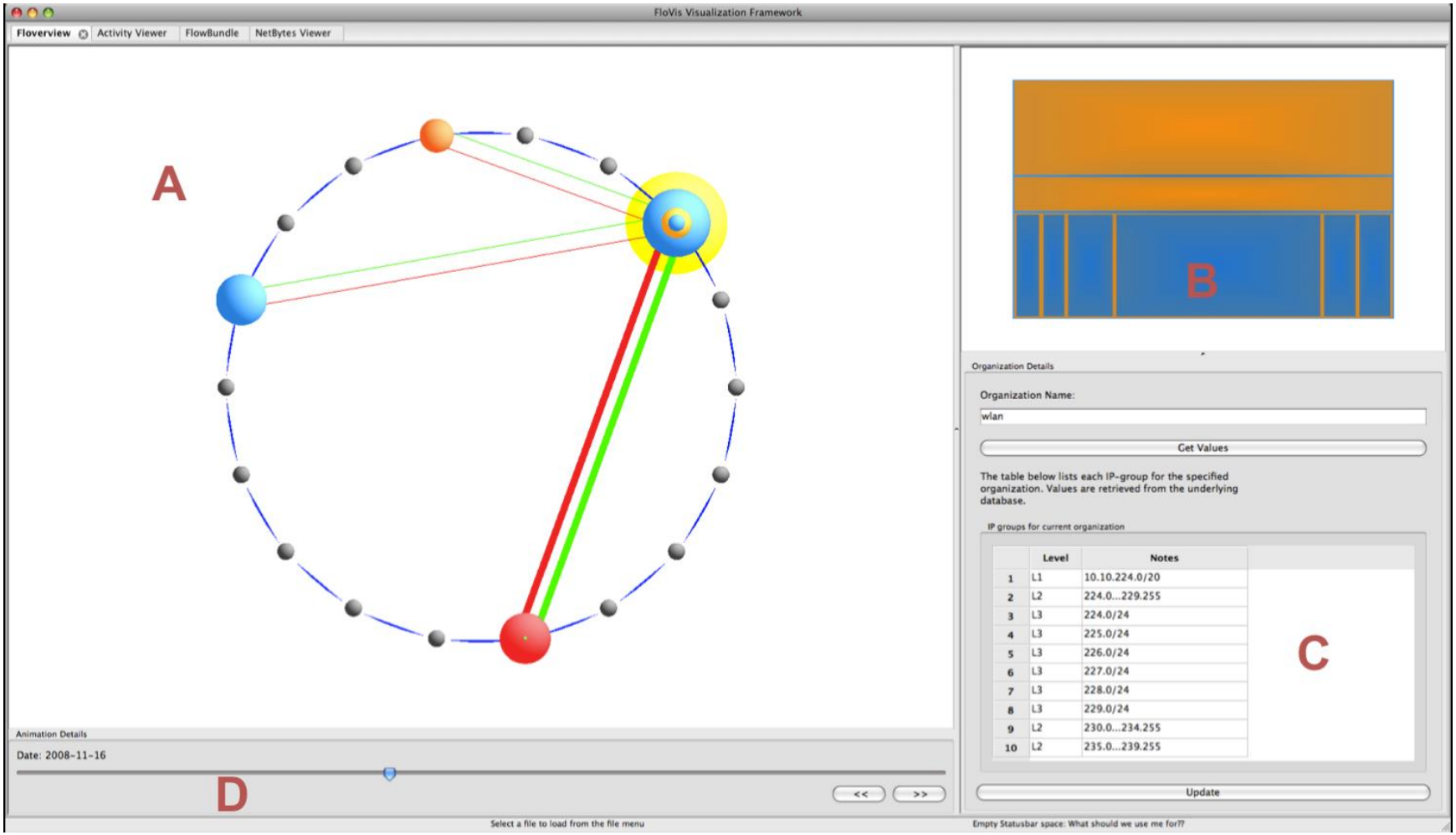
- Große Anzahl an Security Events
- Automatische Analyse limitiert
- Visualisierung als weiterer Ansatz
  - High Level Visualisierung
  - Auswahl der Daten

OverFlow: Data Representation

- Kommunikation zwischen Netzwerkhierarchien
- Flexibel gruppierbar
- Darstellung als Baum
- Metadaten:
  Protokolle, flow-counter, notes, …



OverFlow: Netzwerkhierarchie



FloVis Framework

- OverFlow -> Kontext
- Plugins -> Fokus
- Vorteil: Erforschen der Daten durch simultane, multiple Visualisierungen; erweiterbar

Demo

- http://vimeo.com/29159829

Paper 2

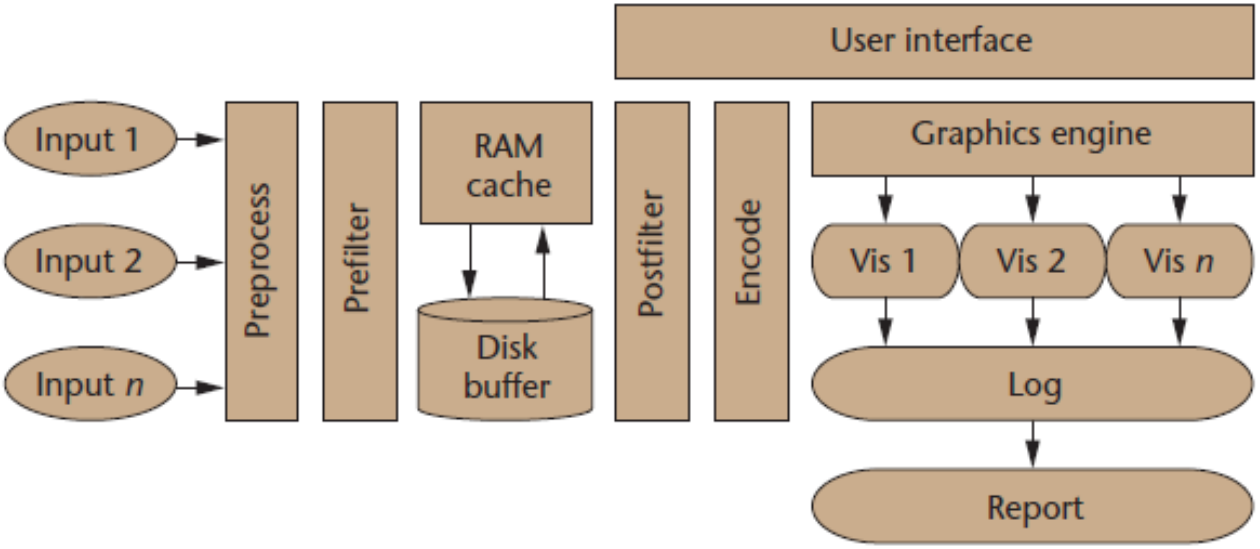
- ***Countering Security Information Overload through Alert and Packet Visualization***
  - 2006. Konti, Abdullah, Grizzard, Stasko, Copeland, Ahamad, Owen, Lee

Motivation

- Security Datenflut
- Durch Überlastung unzuverlässiges Personal
- (Damals) üblich: Analyse von Anzahl, Stufe, Zeitpunkt der Alarme mittels unzureichender Tools, Logfiles & Scripts
- Priorisierung von Alarmen
  - High Level Visualisierung
  - Details on demand

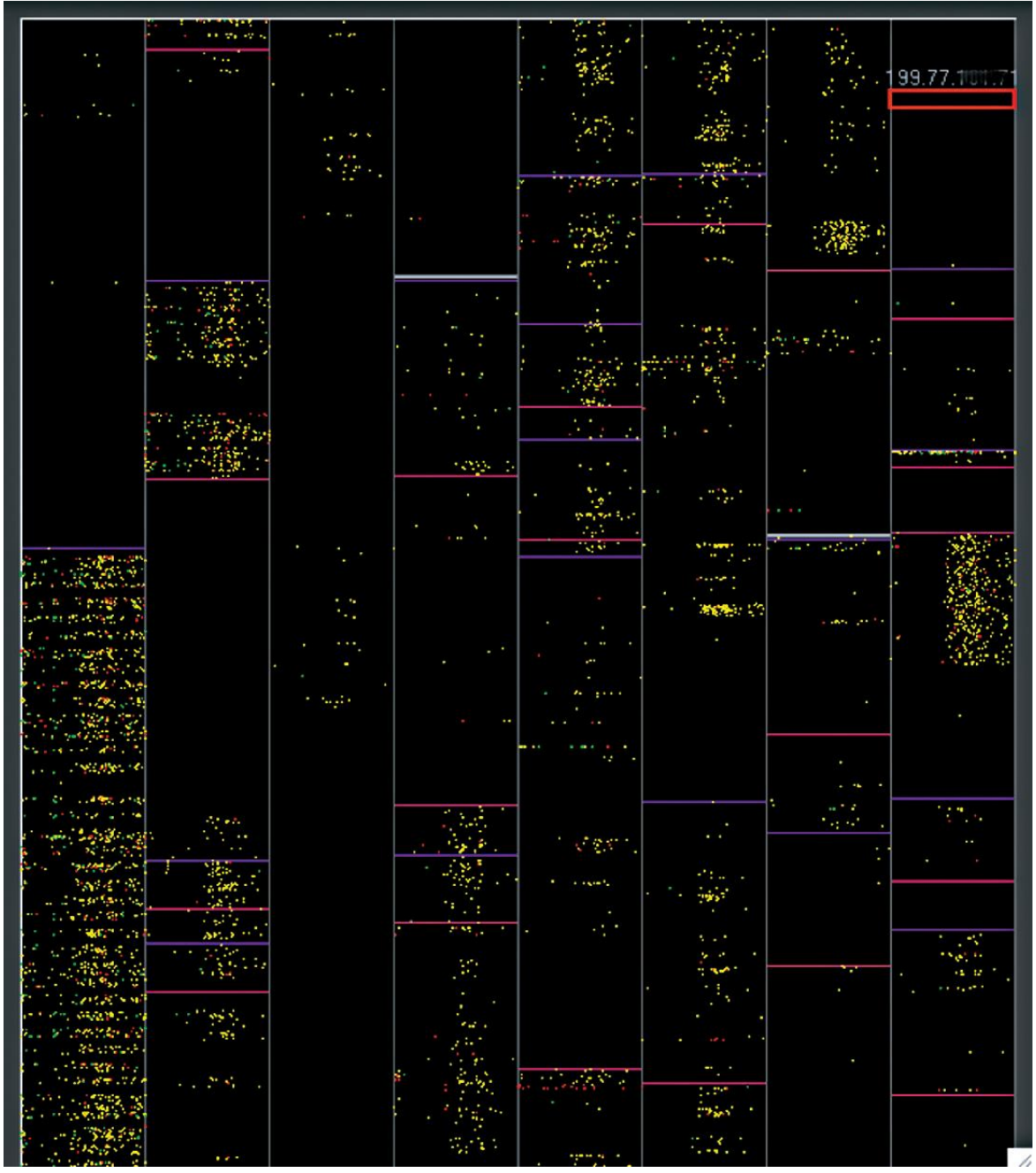
Applikationen

- IDS RainStorm
  - Analyse von Intrusion Alarmen
- Rumint
  - Analyse von Paketen

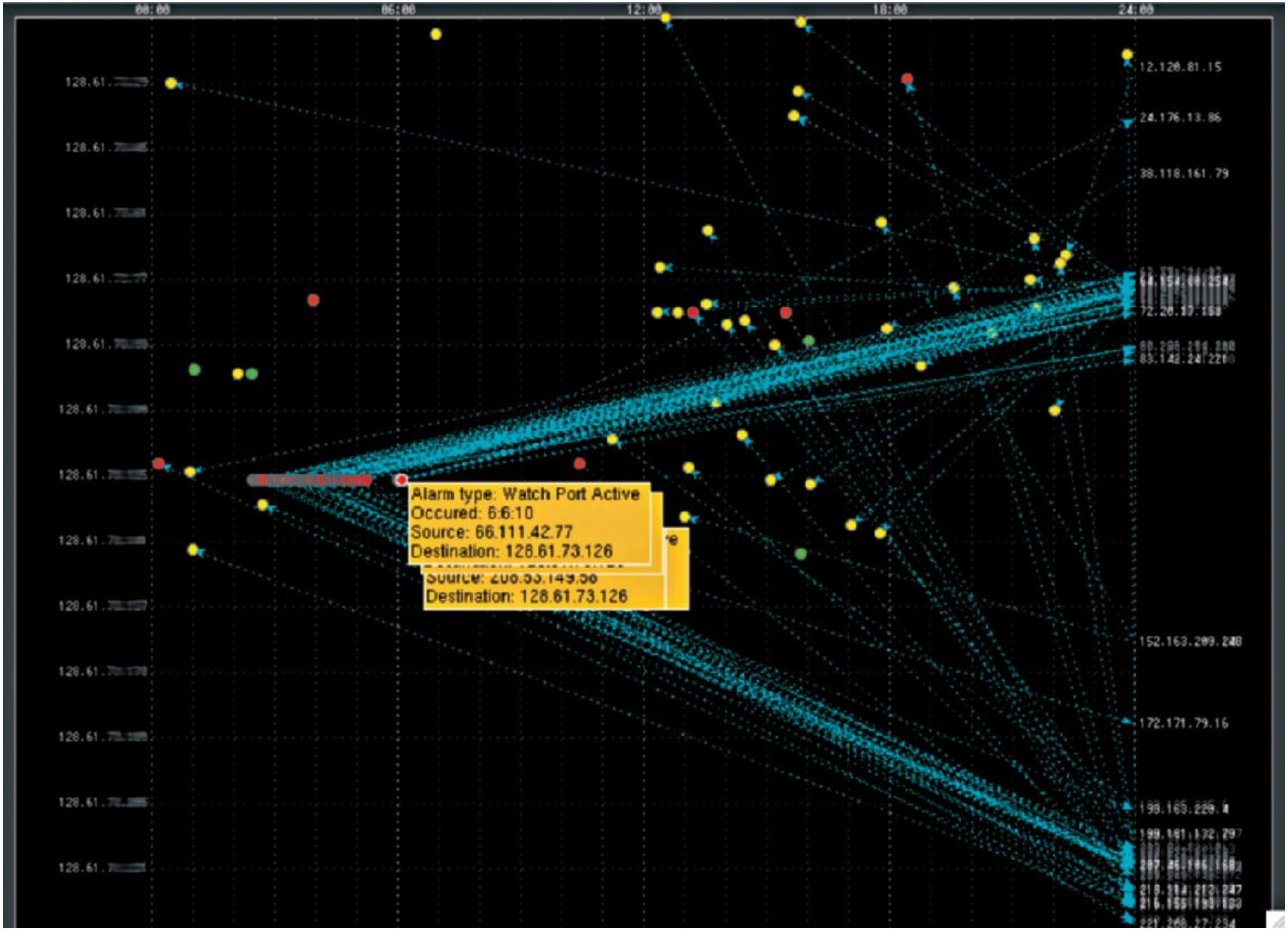


RainStorm

- Ziel: Kritische Events identifizieren
- Main View: Gesamter IP-Bereich
- Zoom View
- Filtering


IP Selector / Zoom
Zeilenweise
Pro Pixel 20 IPs
24 h

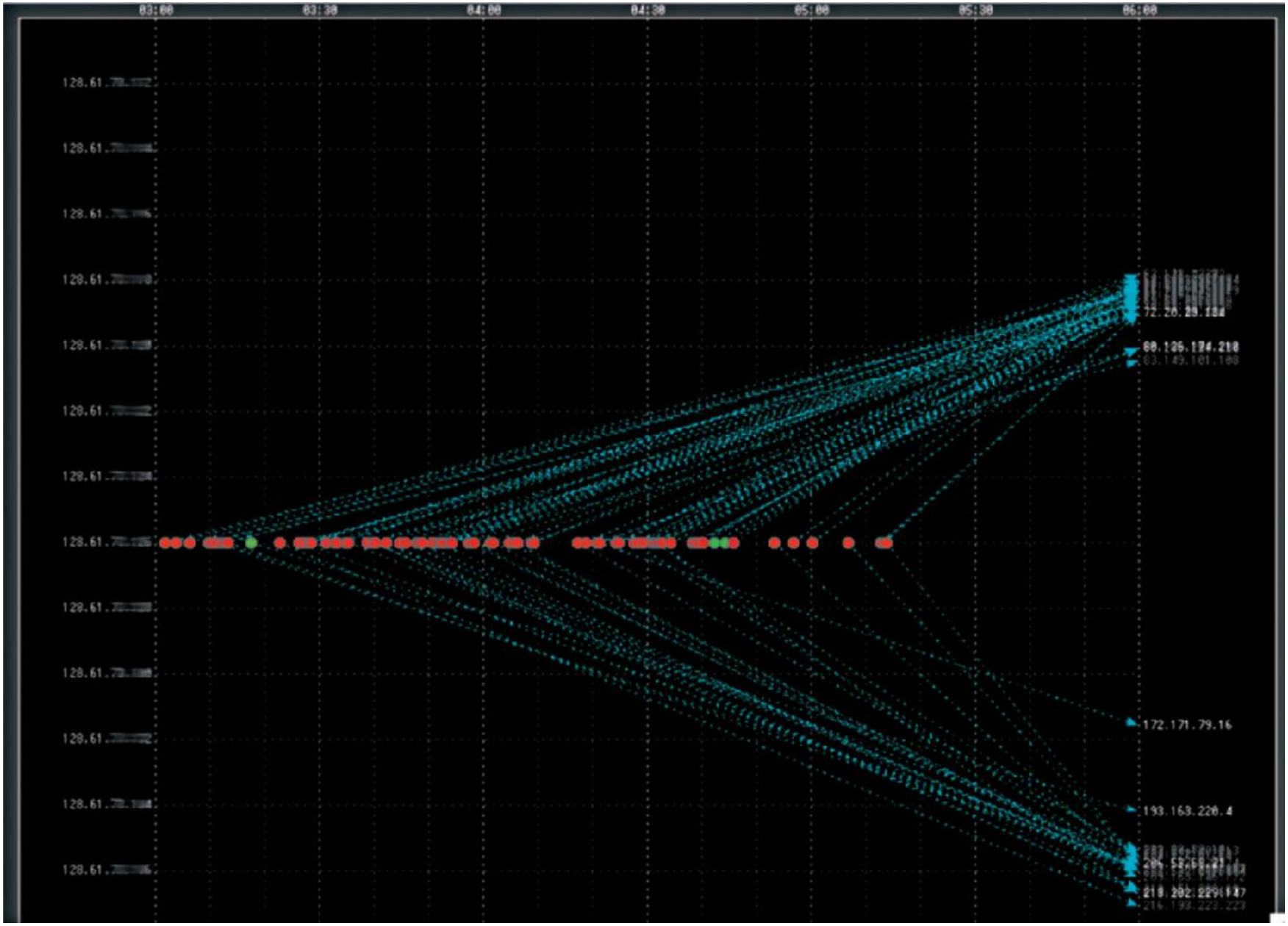
24 h



Destination

Source

24 h

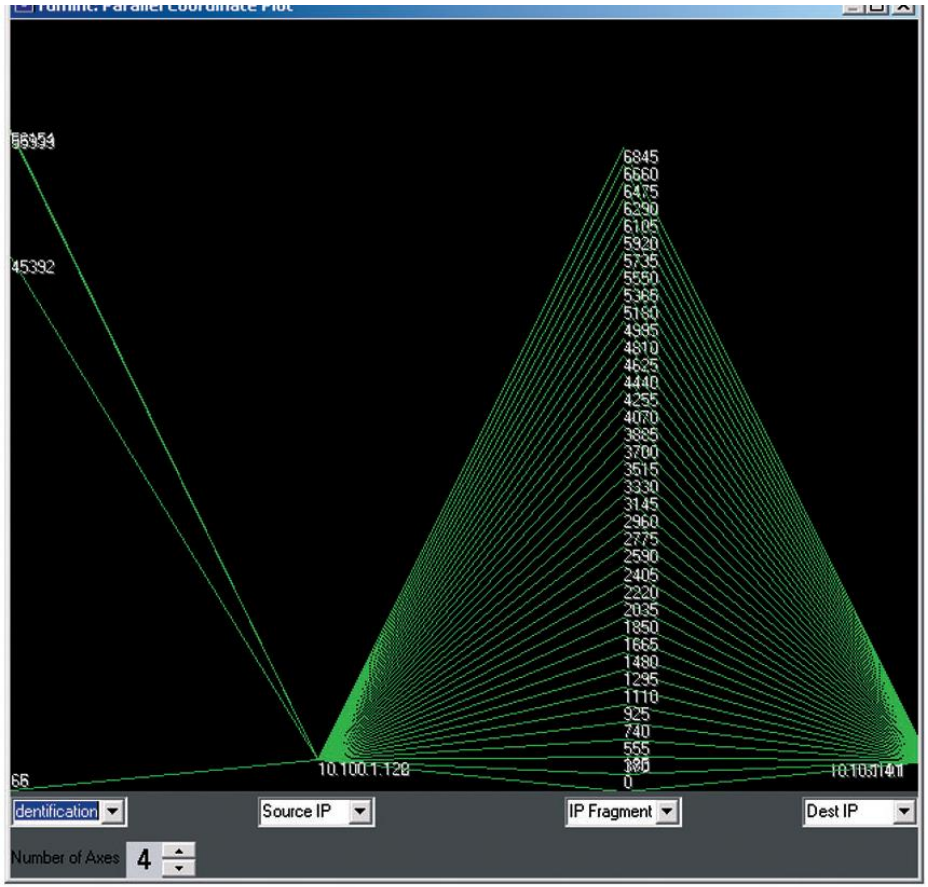


Destination

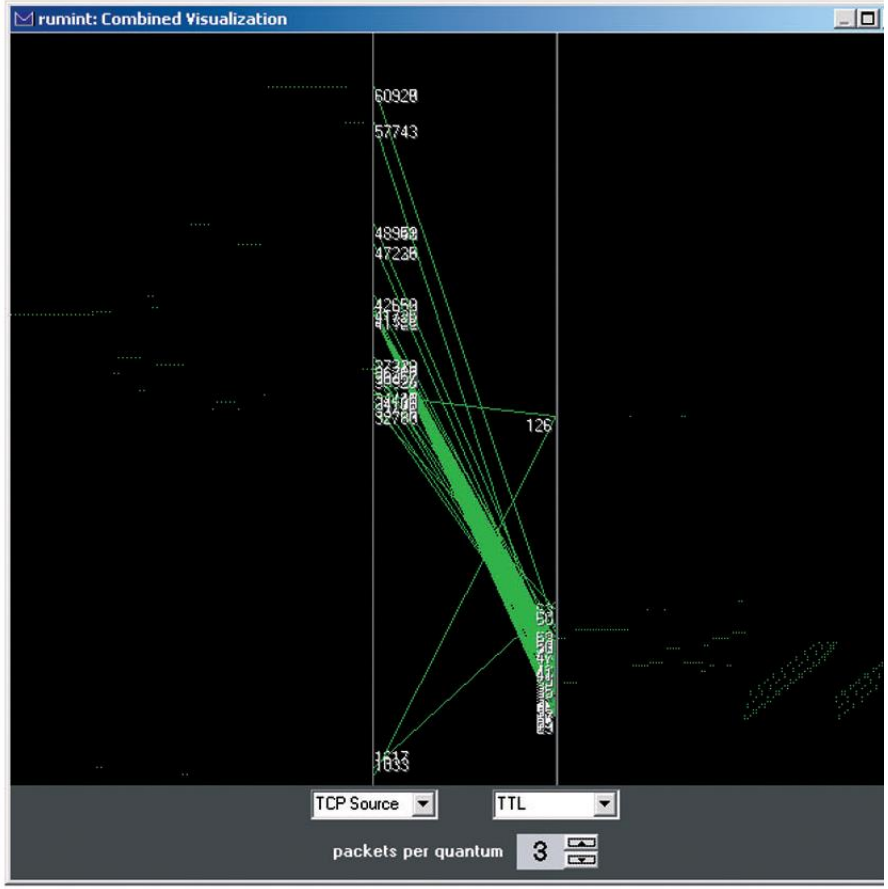
Source

Rumint

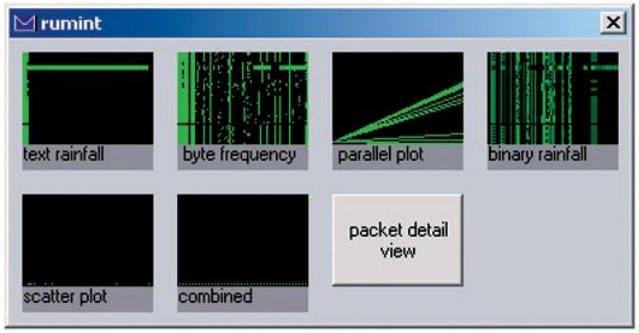
- Ziel: Analyse von Paketen
- Rekorder
- 7 Visualisierungen



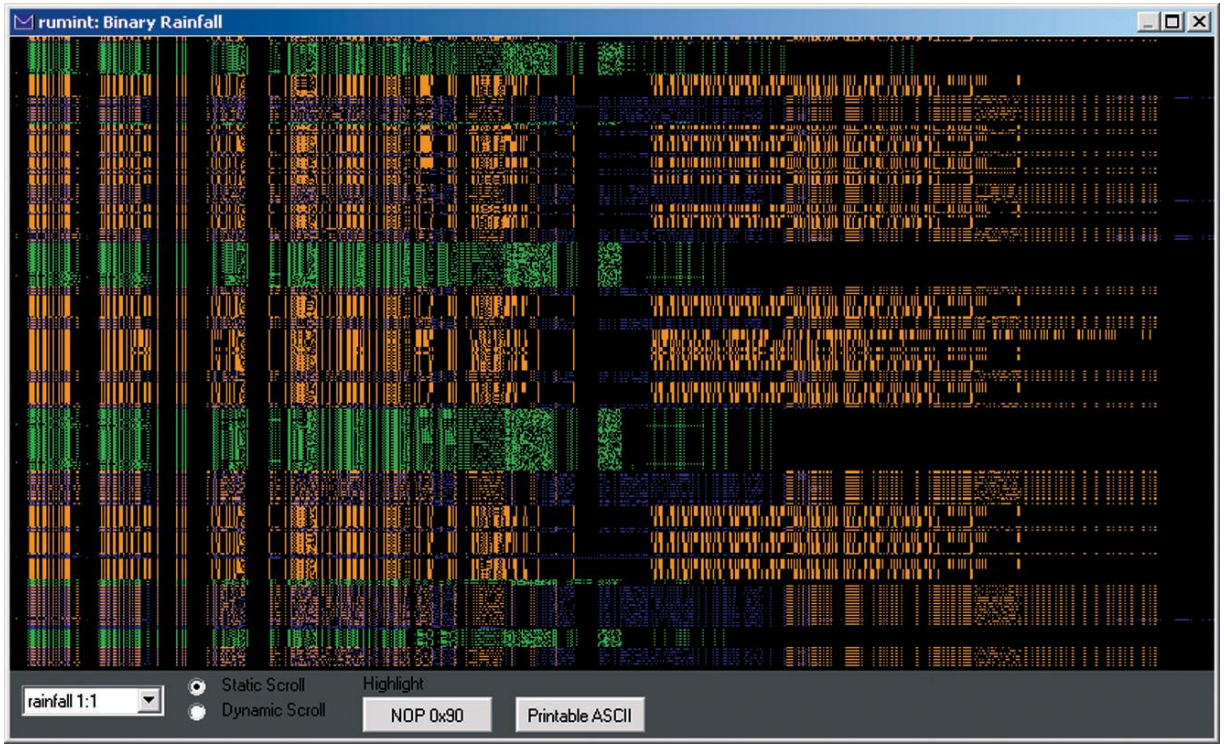
Scaled header value fields



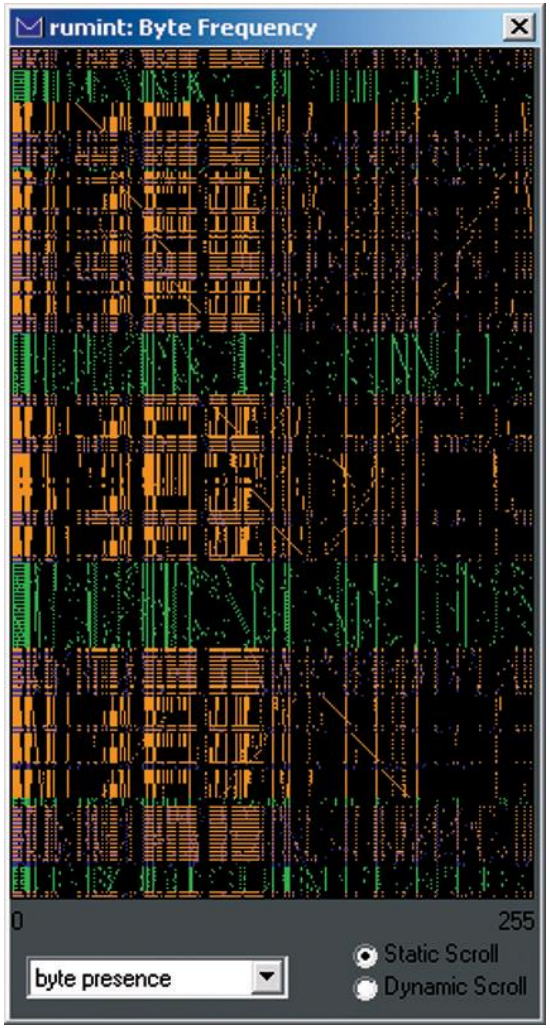
2 Attributes, animated



Thumbnail Preview



Zeilenweise
Rainfall



Byte Frequency

Diskussion