

Paper 1

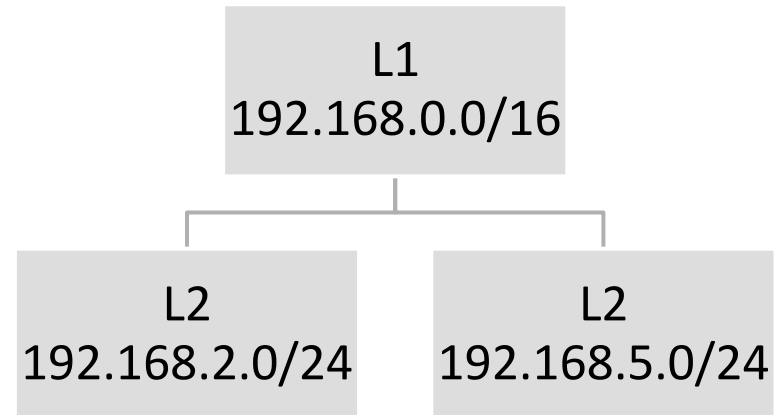
- ***OverFlow: An Overview Visualization for Network Analysis***
 - 2009. Glanfield, Brooks, Taylor, Paterson, Smith, Gates, McHugh

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

The screenshot displays the FloVis Visualization Framework interface, which is divided into several sections:

- Main Visualization Area (A):** A network diagram showing a central blue node with a yellow halo, connected to other nodes (blue, orange, red) and a ring of grey nodes. The diagram is labeled with a red 'A'.
- Bar Chart (B):** A bar chart with orange and blue bars, labeled with a red 'B'.
- Organization Details (C):** A panel containing:
 - Organization Name: wlan
 - Get Values button
 - Text: "The table below lists each IP-group for the specified organization. Values are retrieved from the underlying database."
 - Table of IP groups for current organization (labeled with a red 'C'):
- Animation Details (D):** A panel at the bottom left showing the date 2008-11-16 and a timeline slider, labeled with a red 'D'.

At the bottom of the interface, there are two status bars:

- Left: Select a file to load from the file menu
- Right: Empty Statusbar space: What should we use me for??

| | Level | Notes |
|----|-------|-----------------|
| 1 | L1 | 10.10.224.0/20 |
| 2 | L2 | 224.0...229.255 |
| 3 | L3 | 224.0/24 |
| 4 | L3 | 225.0/24 |
| 5 | L3 | 226.0/24 |
| 6 | L3 | 227.0/24 |
| 7 | L3 | 228.0/24 |
| 8 | L3 | 229.0/24 |
| 9 | L2 | 230.0...234.255 |
| 10 | L2 | 235.0...239.255 |

FloVis Framework

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

Demo

- <http://vimeo.com/29159829>

Paper 2

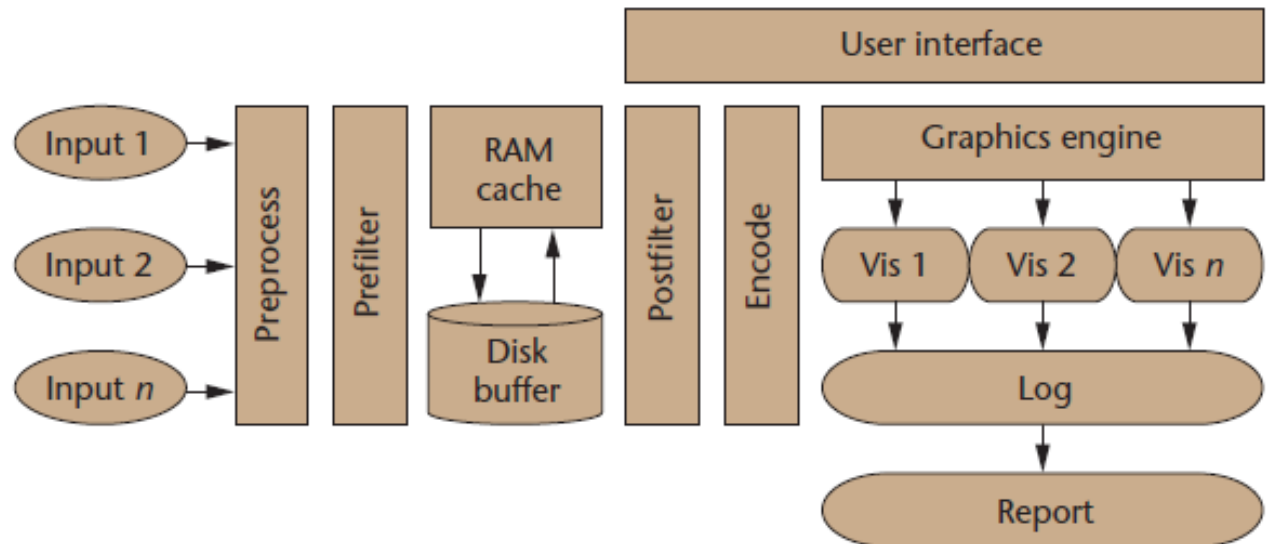
- ***Countering Security Information Overload through Alert and Packet Visualization***
 - 2006. Konti, Abdullah, Grizzard, Stasko, Copeland, Ahamad, Owen, Lee

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

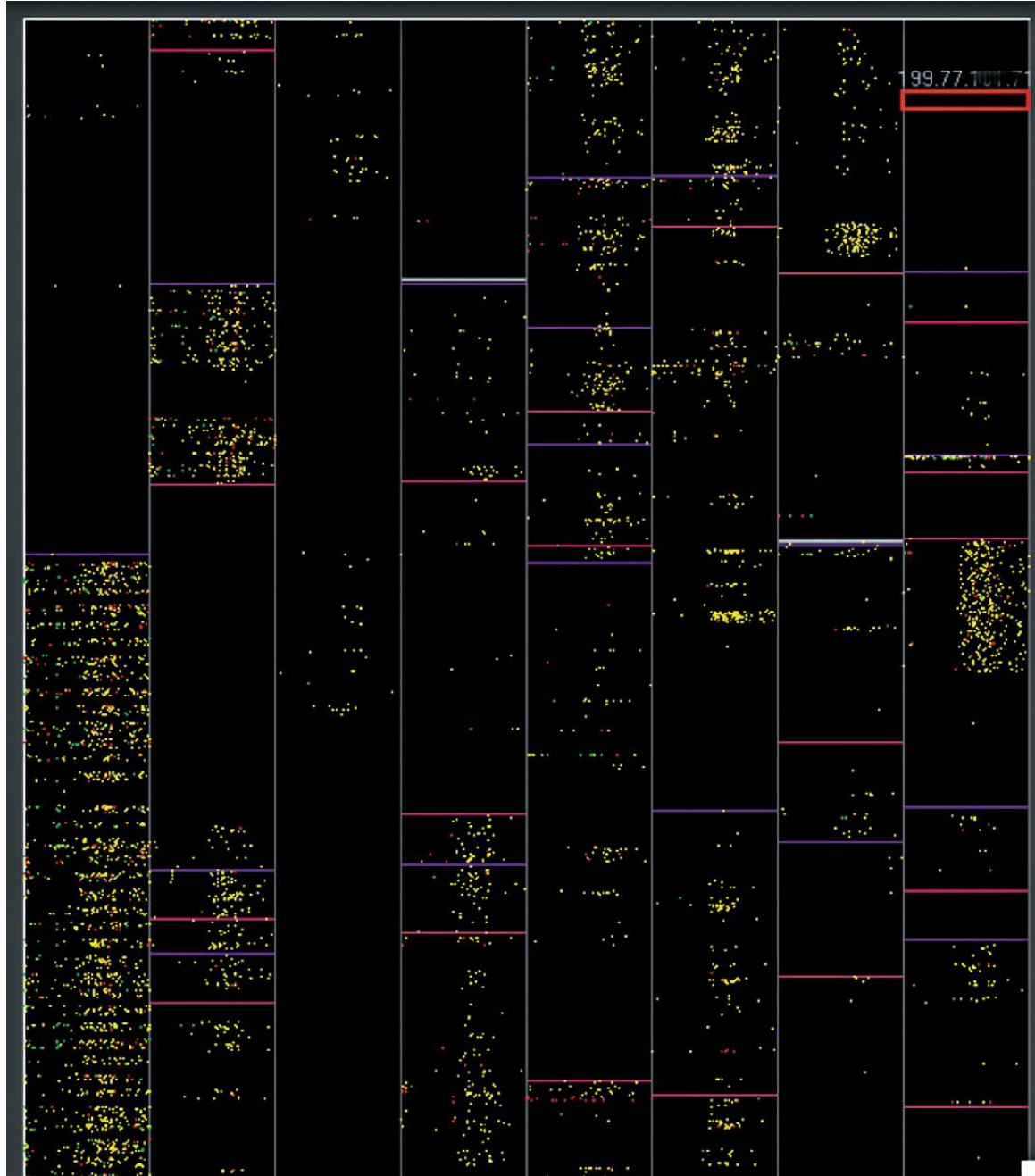
- ▣ IDS RainStorm
 - Analyse von Intrusion Alarmen
- ▣ Rumint
 - Analyse von Paketen



RainStorm

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

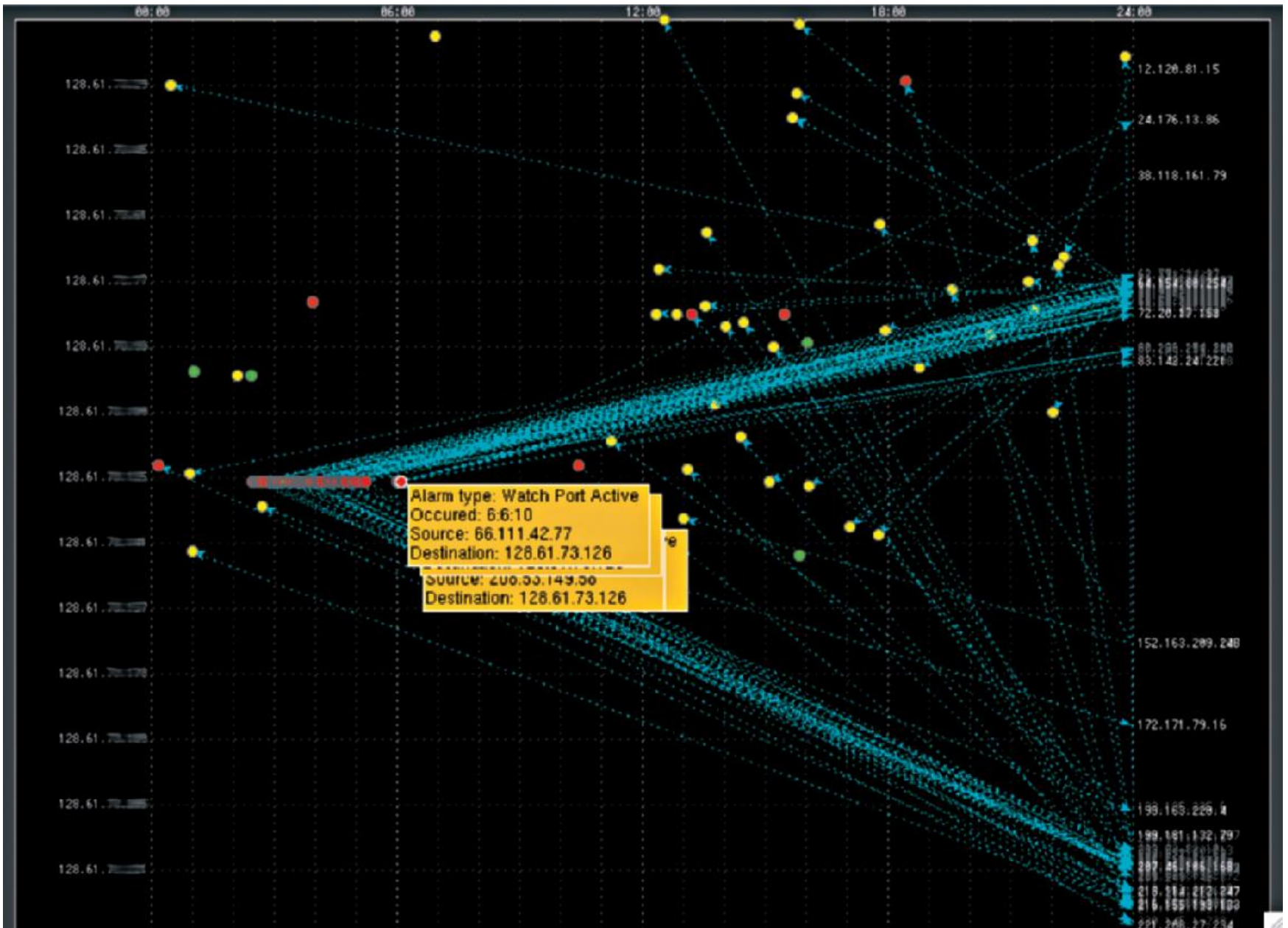
Zeilenweise
Pro Pixel 20 IPs



IP Selector / Zoom

24 h

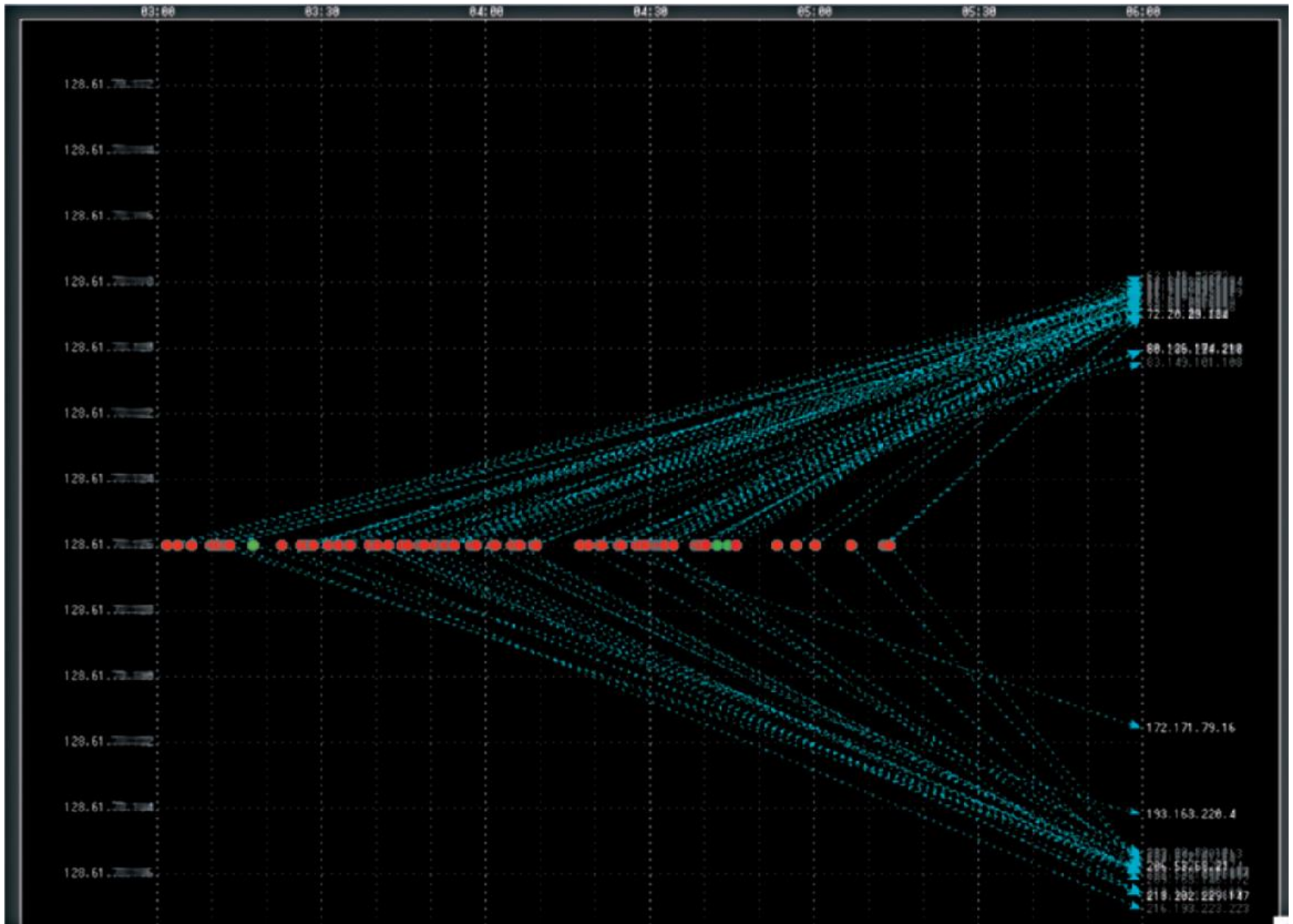
24 h



Destination

Source

24 h

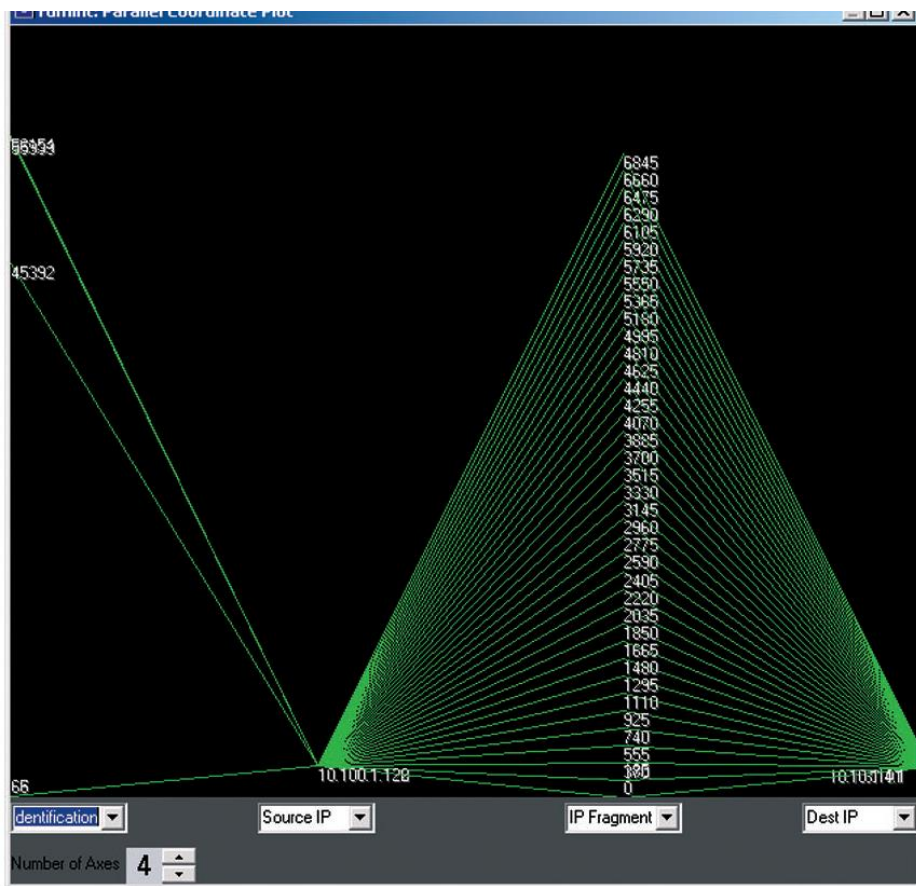


Destination

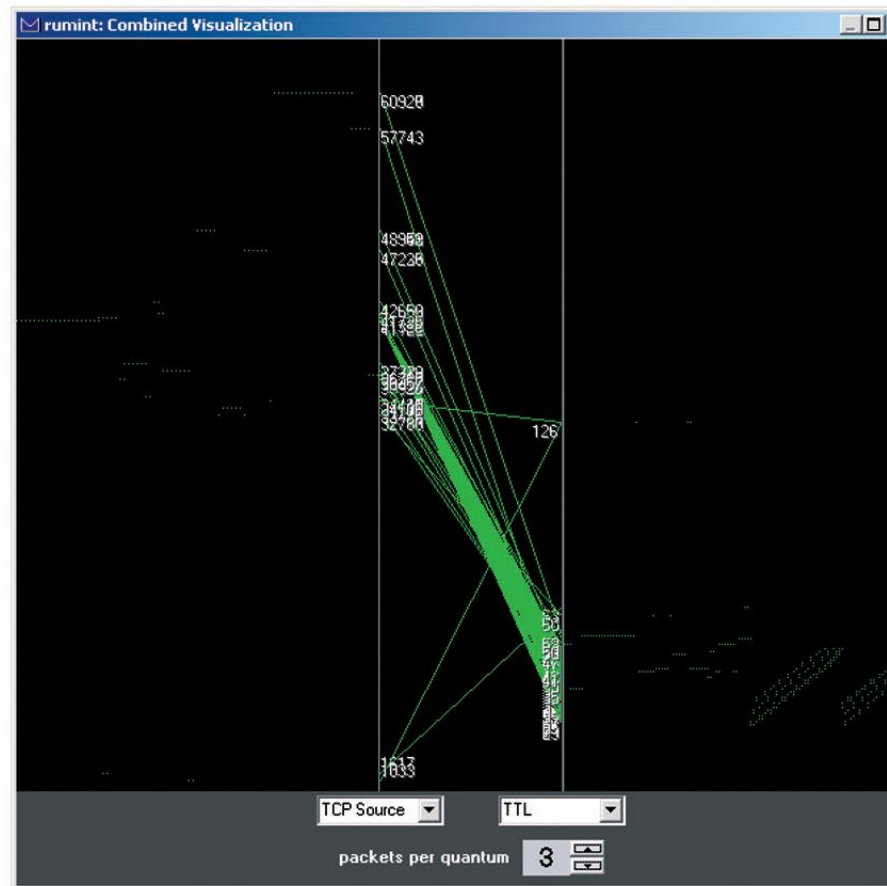
Source

Rumint

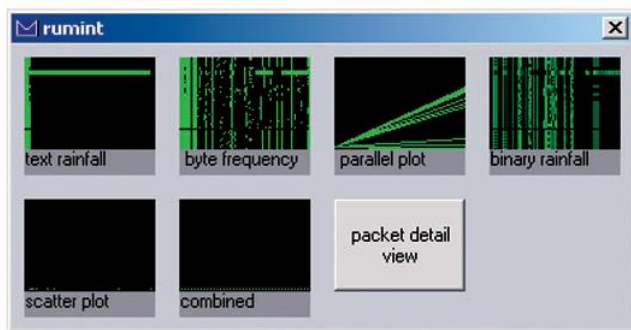
- Ziel: Analyse von Paketen
- Rekorder
- 7 Visualisierungen



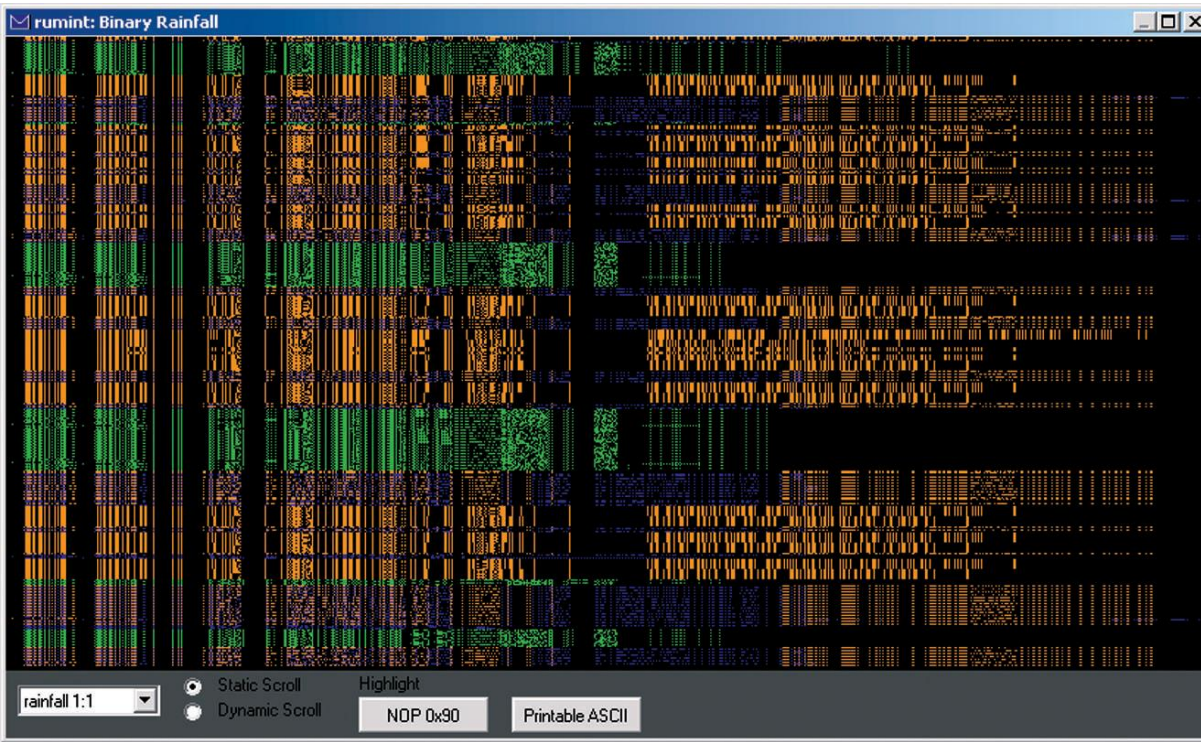
Scaled header value fields



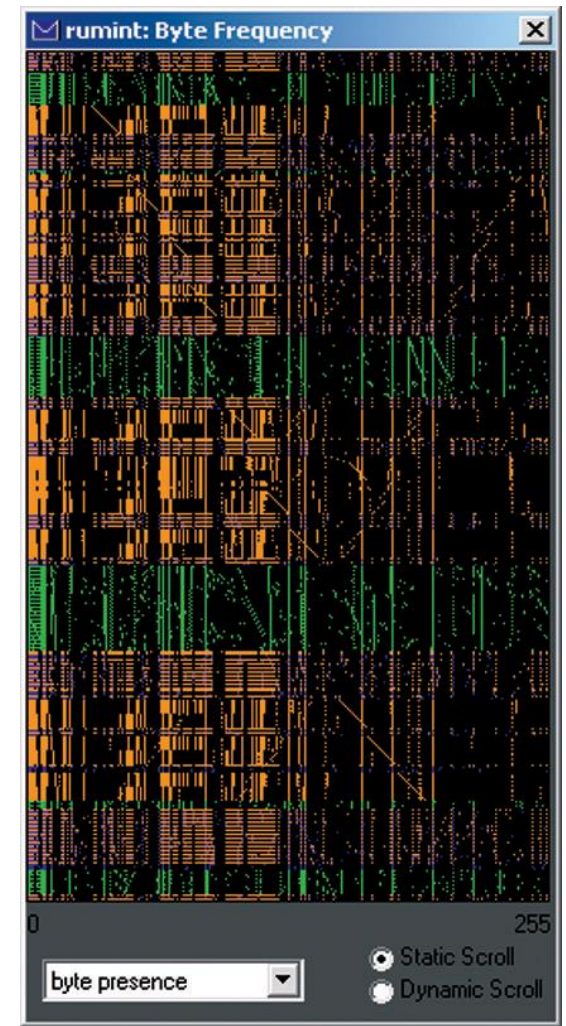
2 Attributes, animated



Thumbnail Preview



Zeilenweise
Rainfall



Byte Frequency

Diskussion