1st European Workshop on Internet Early Warning and Network Intelligence

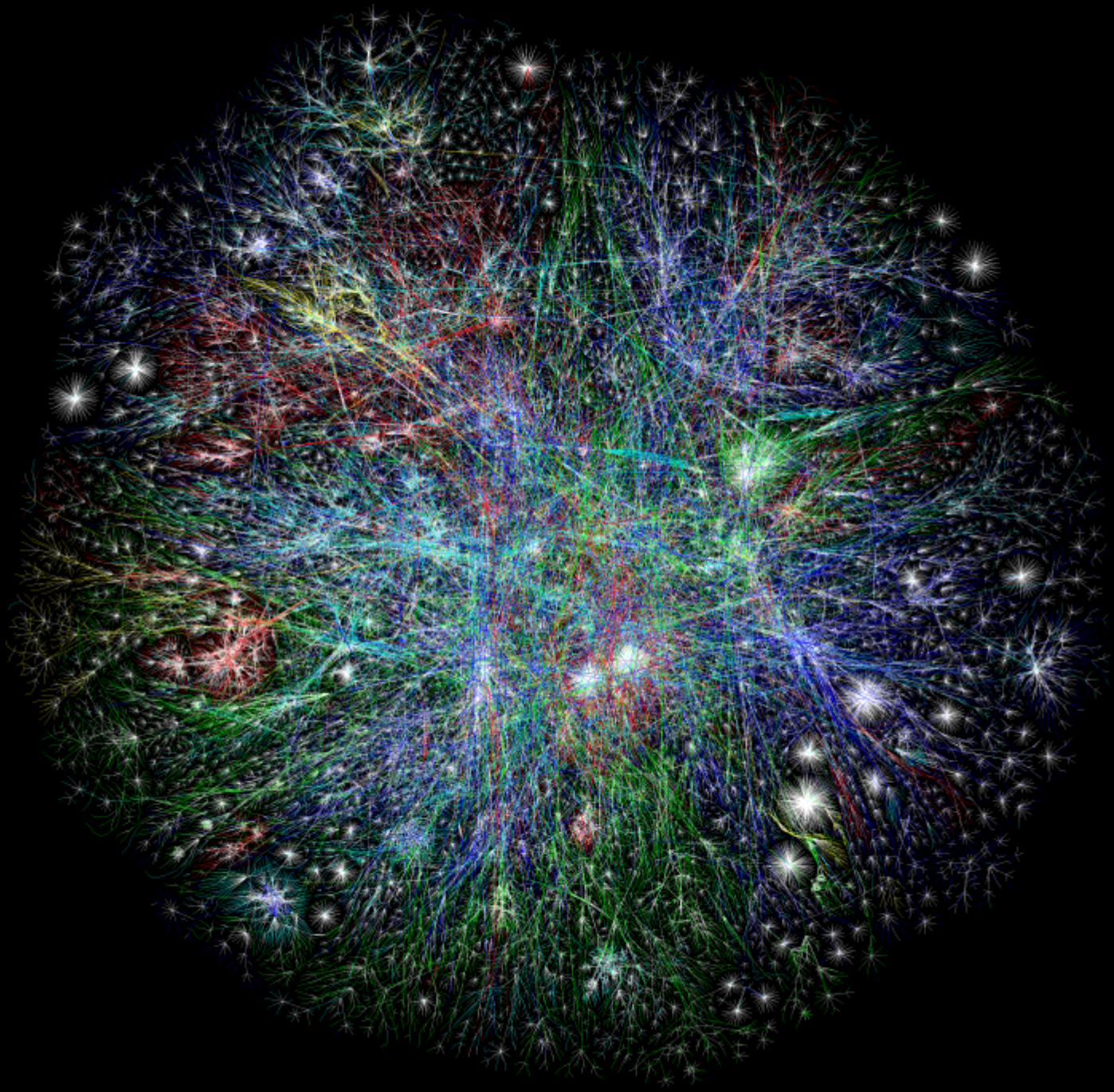
Network Security Visualisation Techniques in Early Warning Systems

Marcus Weseloh

Hamburg, 27.01.2010

Motivation

"One picture is worth ten thousand words."



Source: Opte.org

Words in image:

> 10,000

Words in image:

> 10,000

Words in my head:

3

"That looks pretty!"

Goal:

Find visualisation techniques that provide valuable new insights for analysts working with early warning systems.

Key Questions

- What are the cognitive principles behind effective visualisation?
- Which tasks could benefit from visualisation?
- Which visualisation technique is suitable for which task?

Talk Overview

- The CarmentiS Early Warning System
- Information Visualisation
- Traffic Analysis Tasks
- Review of Visualisation Techniques
- Implementations

The CarmentiS System

CarmentiS

- Project of CERT-Verbund and BSI.
- Based on netflow toolkit by Peter Haag of SWITCH-CERT (nfdump/nfsen)
- Extends architecture to include other event sources like honeypots, IDS and malware sensors.

CarmentiS uses netflow as base for all other types of events

therefore:

Focus on visualisation techniques suitable for traffic analysis!

Information Visualisation

Principles of Visual Perception

Preattentive Processing

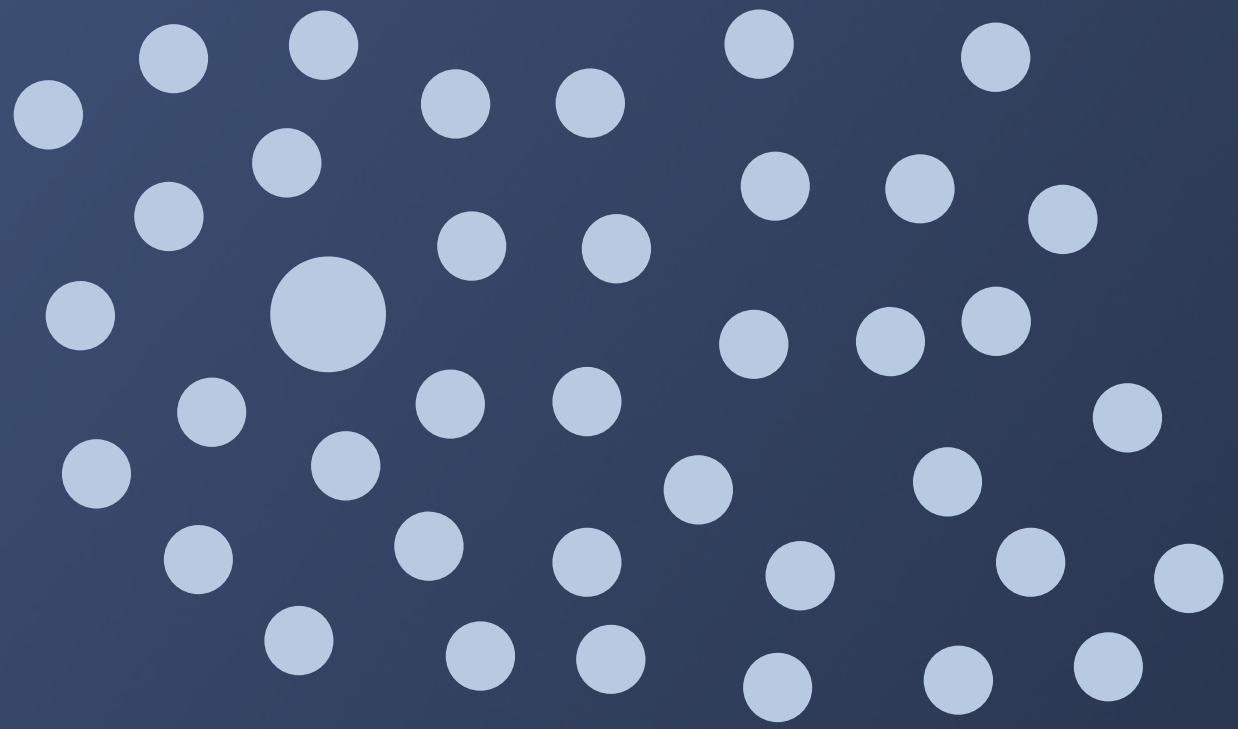
- Processing of visual attributes prior to conscious thought.

- Enables us to encode information in such a way that it “pops out” at the viewer.

Some Examples

Find the “odd one out”!

Size



Orientation

Parallelism

Parallelism

Parallelism

Preattentive Attributes

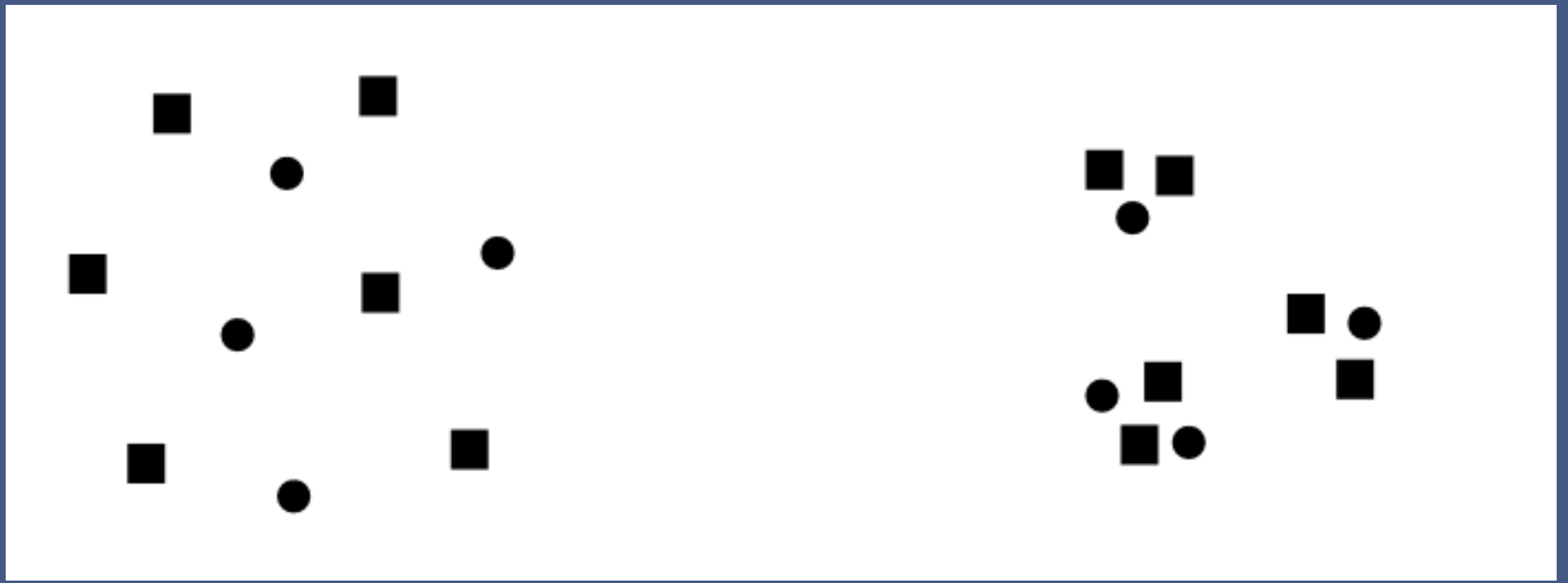
- Size
- Orientation
- Colour
- Shape
- Concavity / Convexity
- Texture

… and more

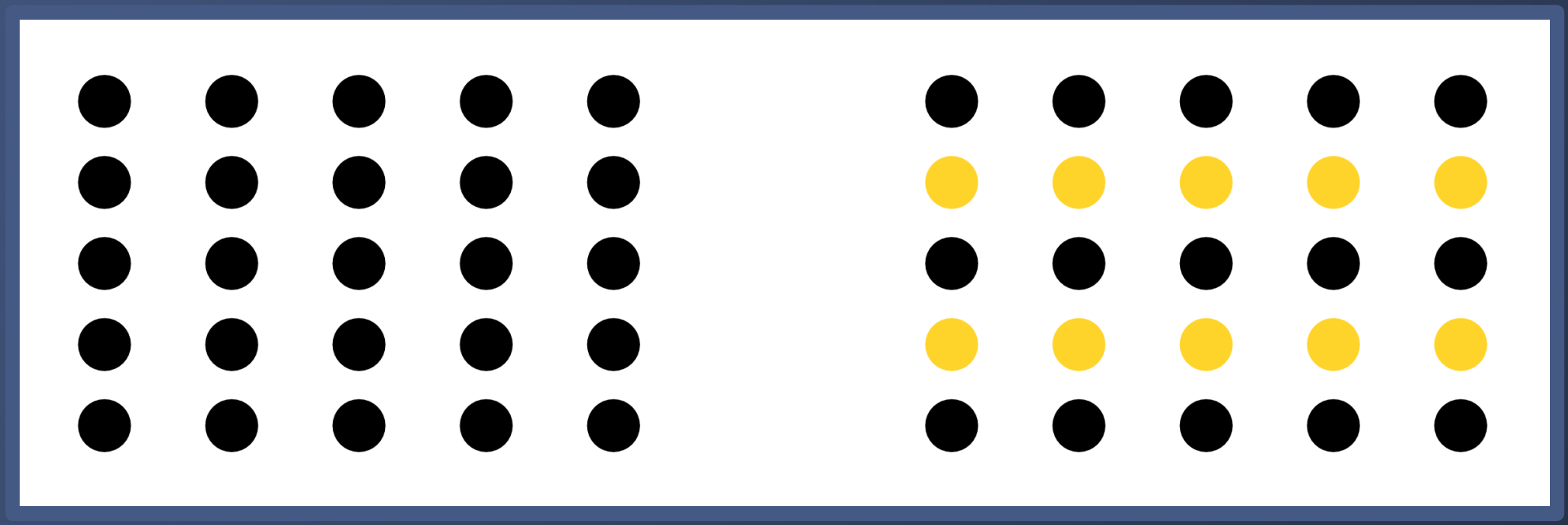
Gestalt Principles

- Kurt Koffka, German Psychologist (1935)
- Formulated as series of laws
- Explains human pattern perception
- Useful to clarify grouping and ease perception of clusters in visualisations

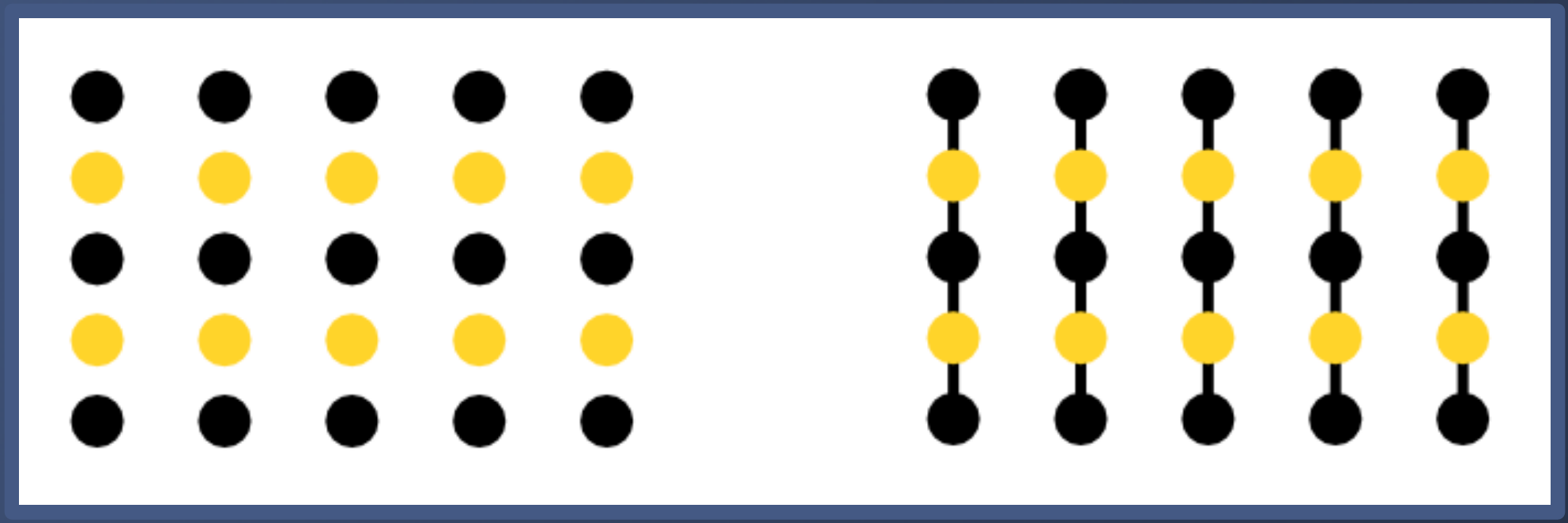
Proximity



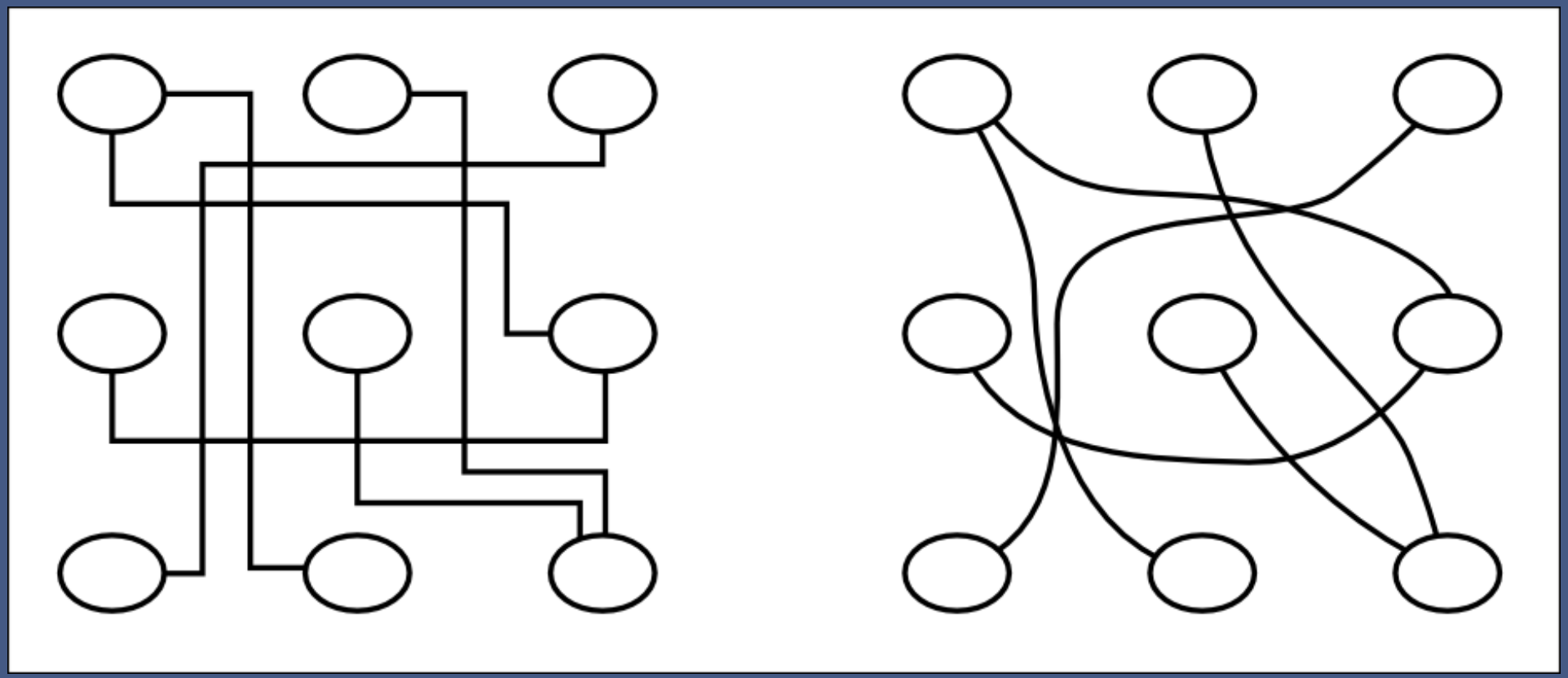
Similarity



Connectedness

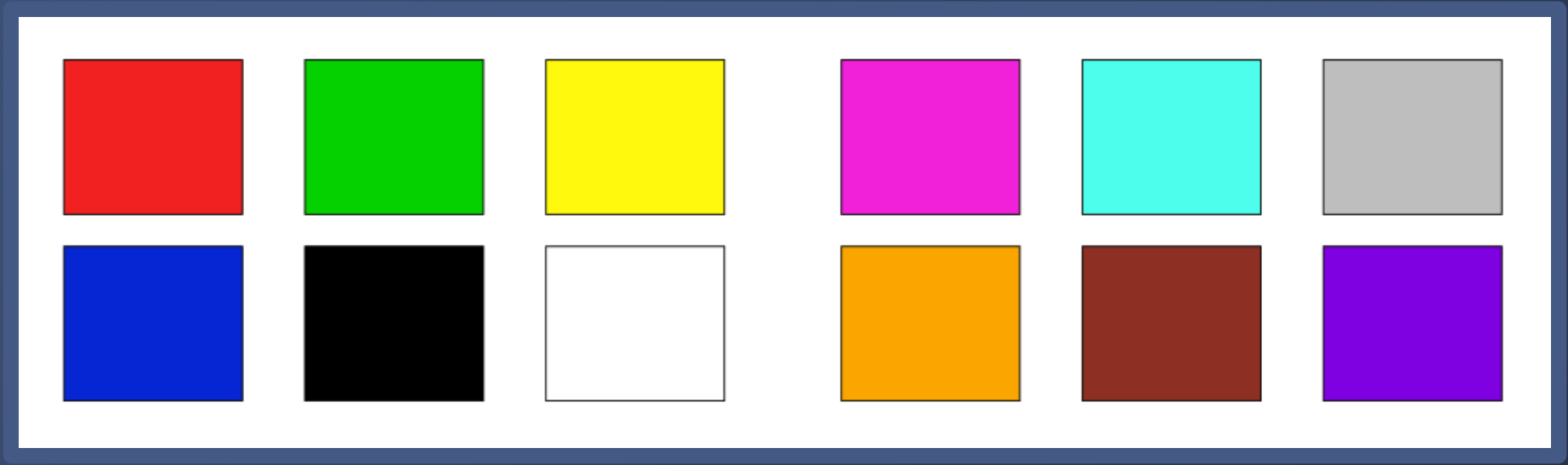


Continuity



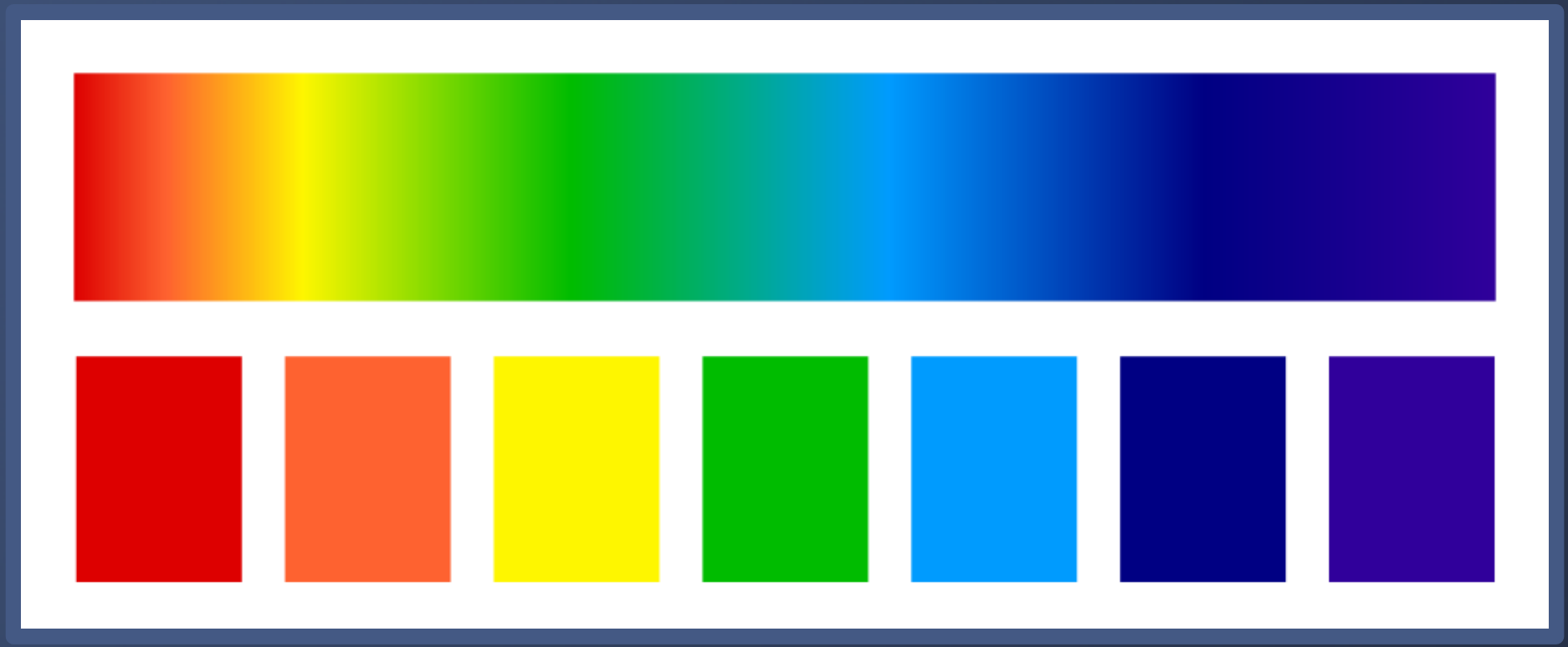
Use of Colour

Colour for Categorical Data

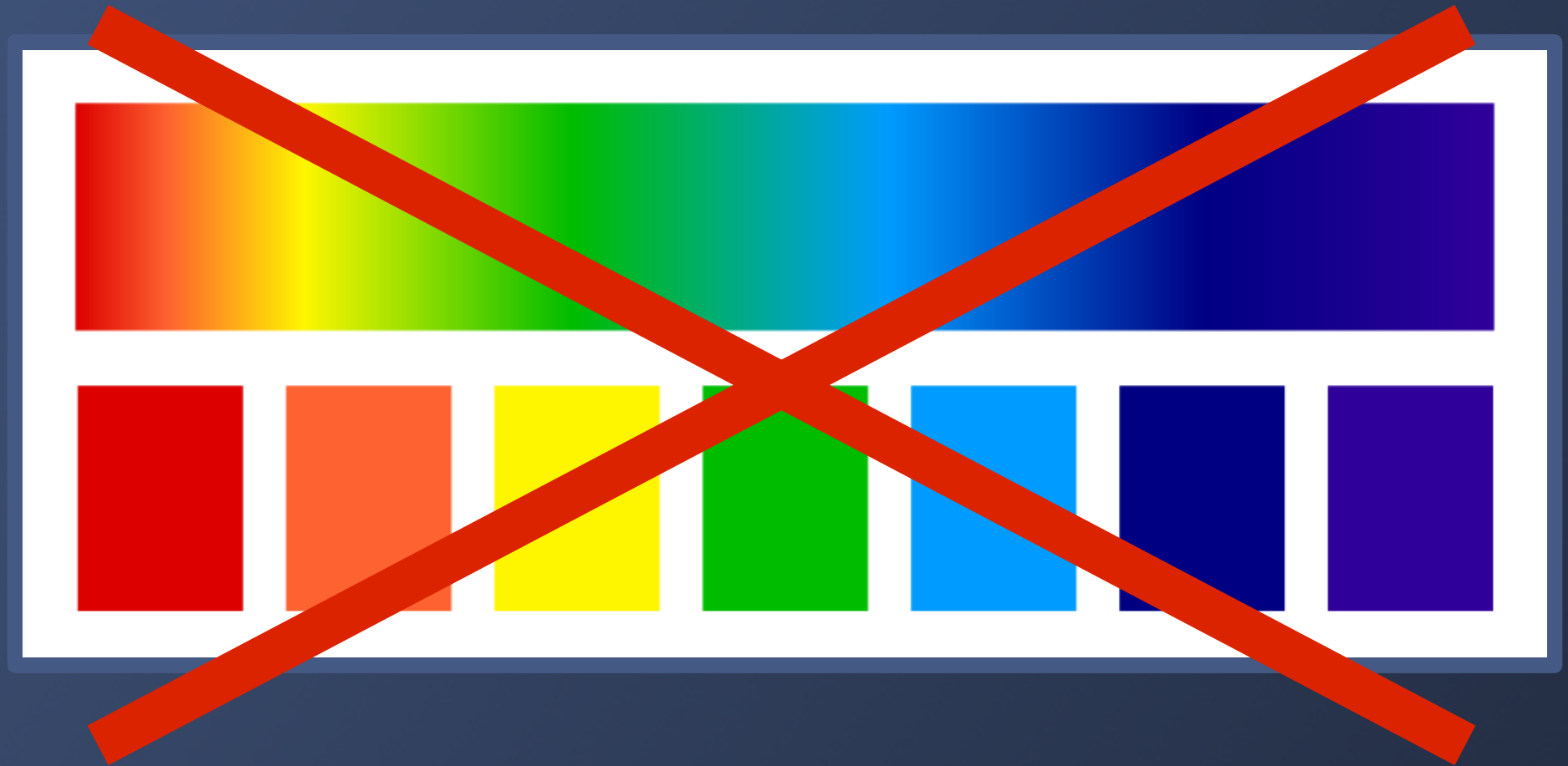


Colour for Continuous Data

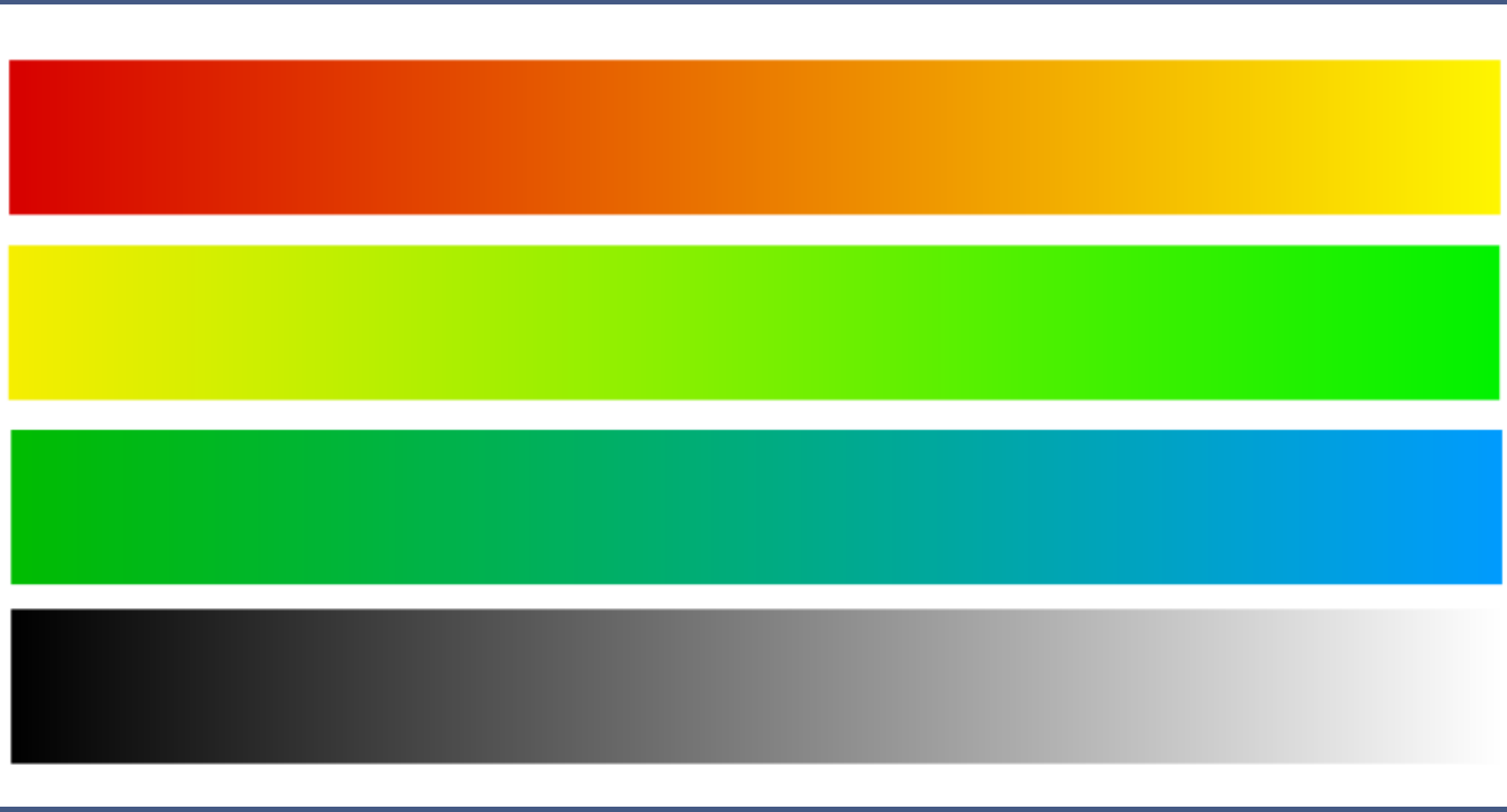
Rainbow Scale?



There is no intrinsic order in the rainbow colour scale!



Colour for Continuous Data



Traffic Analysis Tasks

Information Seeking Mantra:

"Overview first, zoom and filter, details on demand"

Shneiderman (1996)

Four Stages in Traffic Analysis

- Anomaly detection
- Identification of anomaly boundaries
- Anomaly analysis
- Detailed flow information

Anomaly Detection

Goal: Spot significant changes in traffic flows that could indicate an anomaly.

Anomaly Boundaries

Goal: Find the boundaries of the anomaly to reduce amount of processed data.

Anomaly Analysis

Goal: Identify the anomaly as a known type or find attributes that could identify a new anomaly in the future.

Flow Details

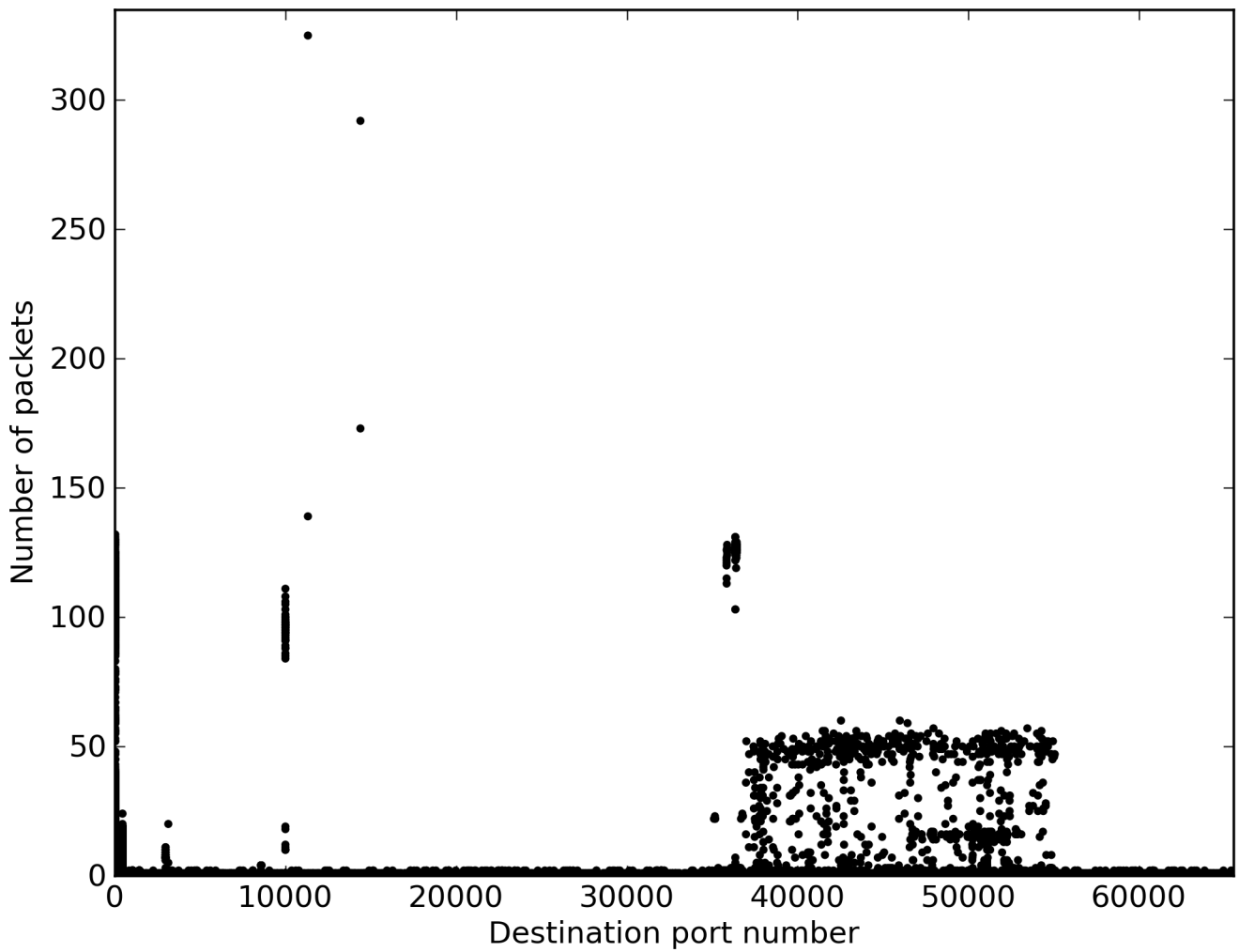
View all information for a single flow record.

Four Stages in Traffic Analysis

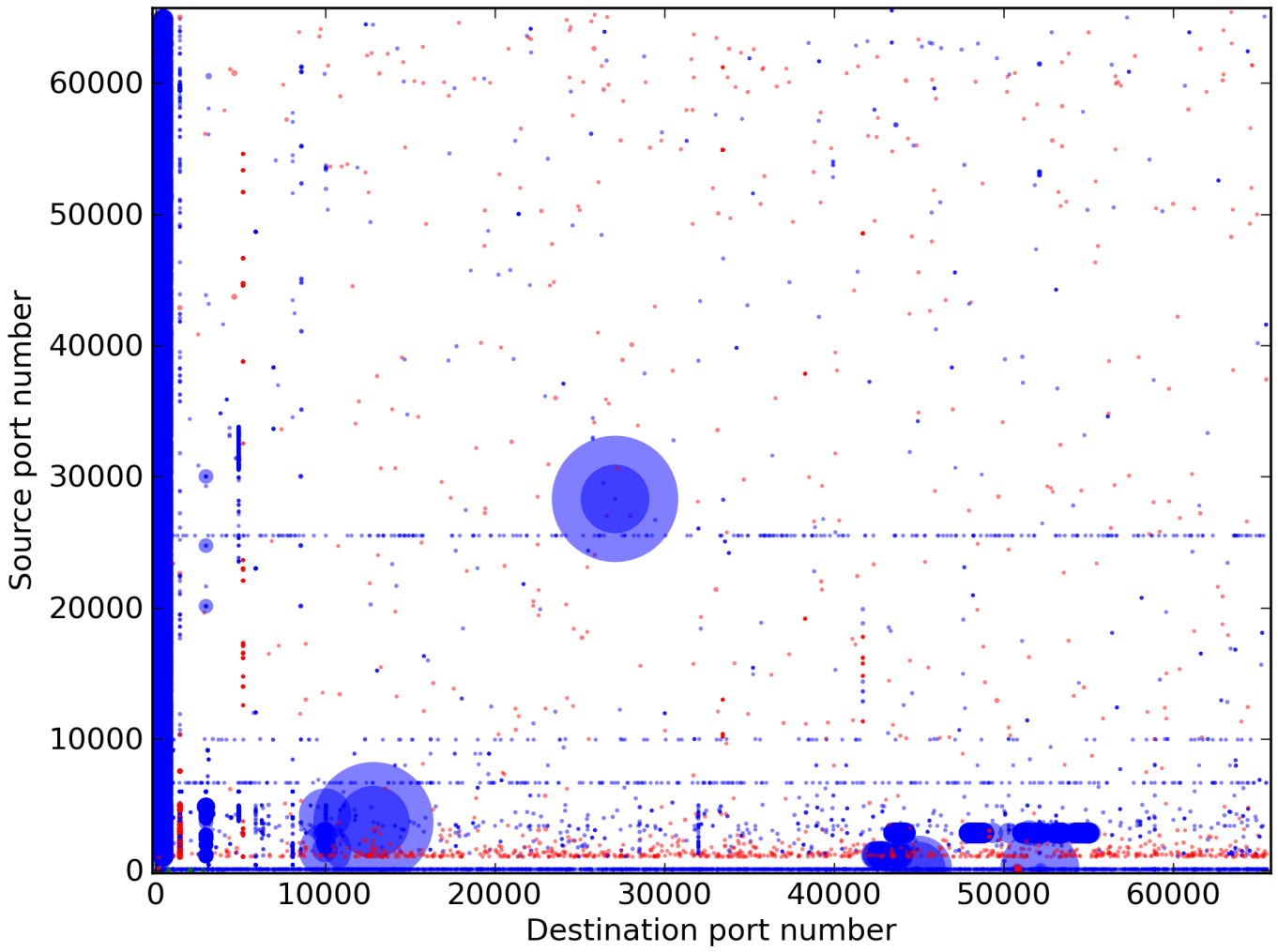
- Anomaly detection
- Identification of anomaly boundaries
- Anomaly analysis
- Detailed flow information

Review of Visualisation Techniques

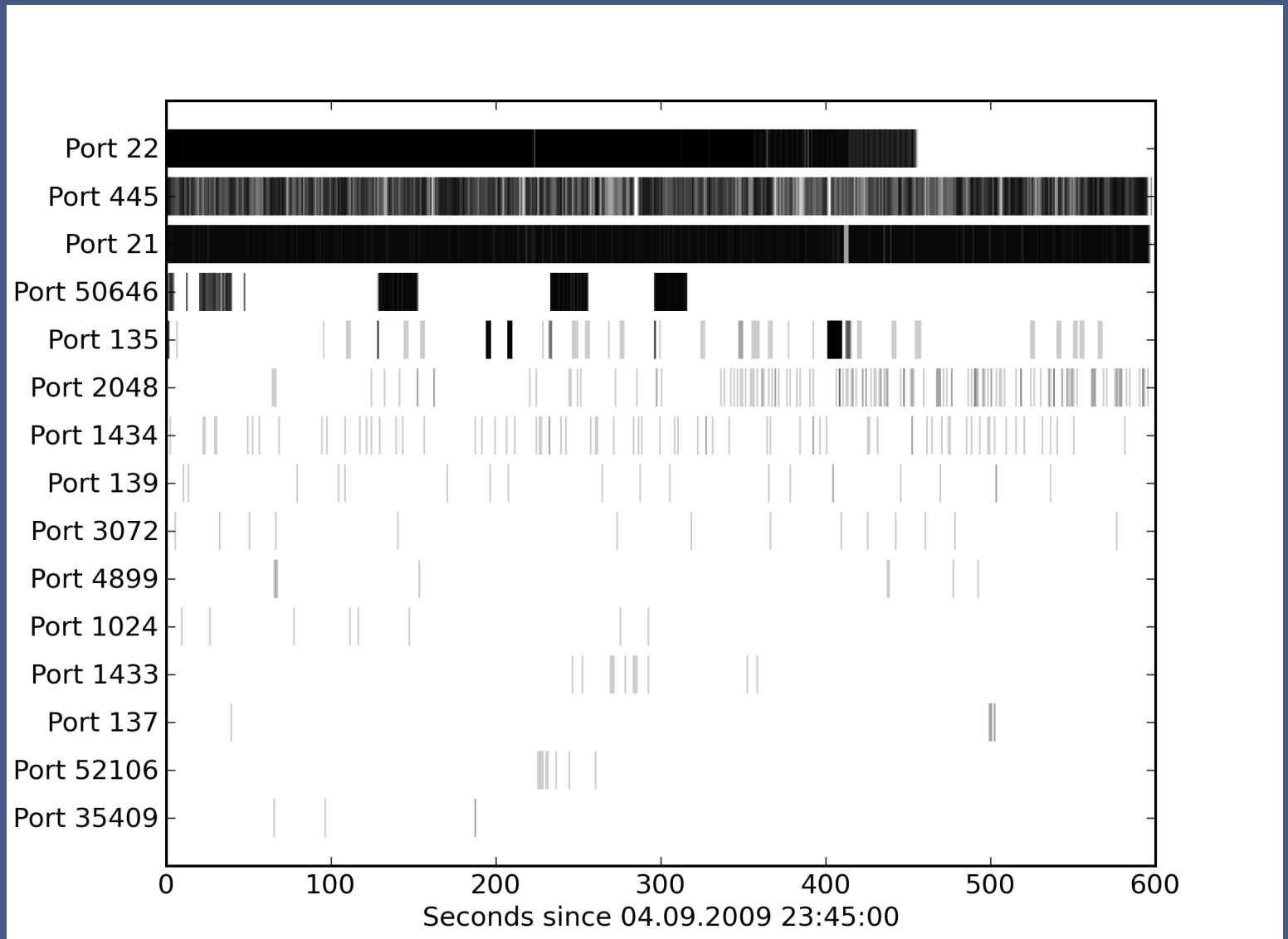
Scatter Plots



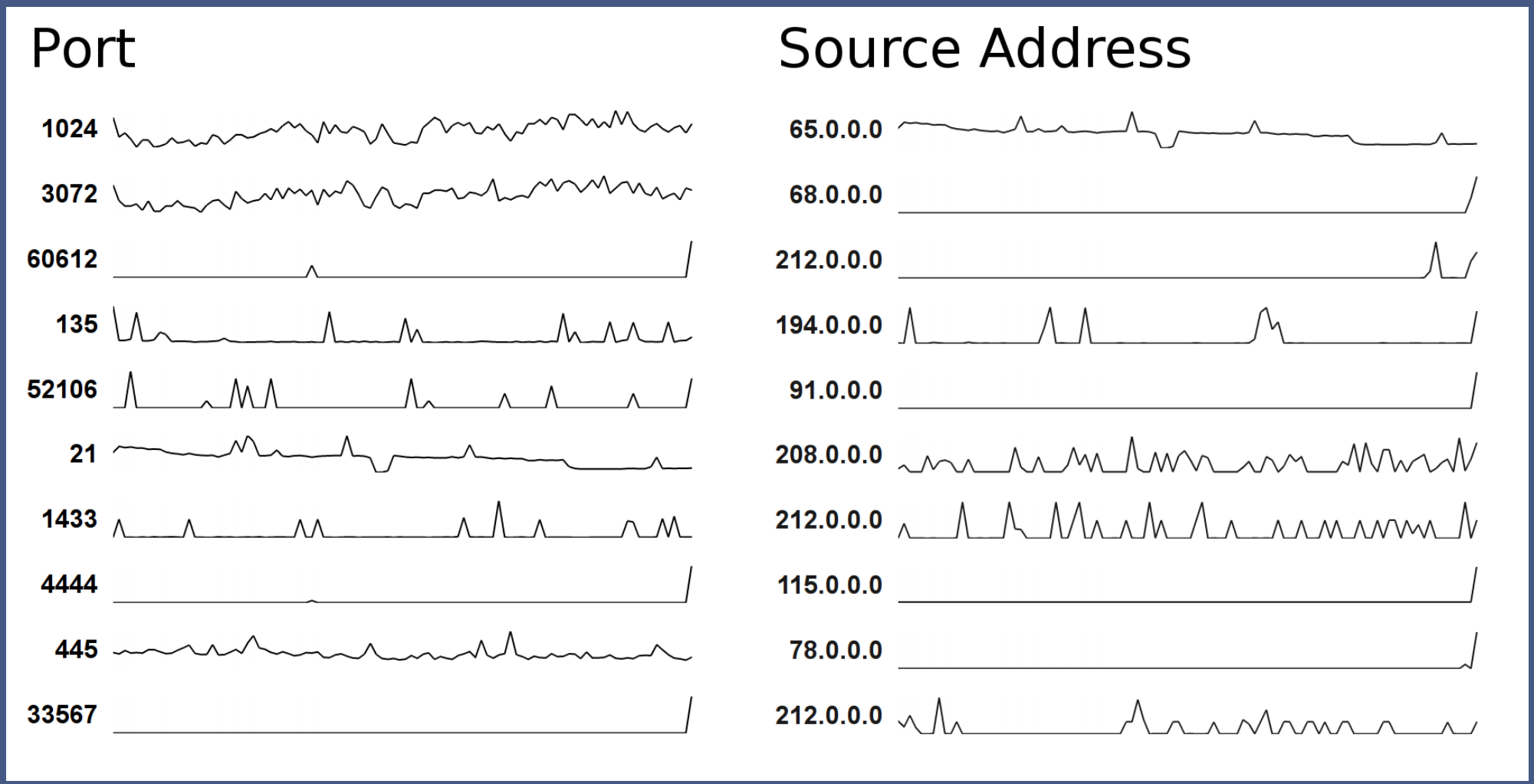
Enhanced Scatter Plots



Time Table


Port 22
Port 445
Port 21
Port 50646
Port 135
Port 2048
Port 1434
Port 139
Port 3072
Port 4899
Port 1024
Port 1433
Port 137
Port 52106
Port 35409
0
100
200
300
400
500
600
Seconds since 04.09.2009 23:45:00

Sparklines


Port
1024
3072
60612
135
52106
21
1433
4444
445
33567
Source Address
65.0.0.0
68.0.0.0
212.0.0.0
194.0.0.0
91.0.0.0
208.0.0.0
212.0.0.0
115.0.0.0
78.0.0.0
212.0.0.0

Implementations

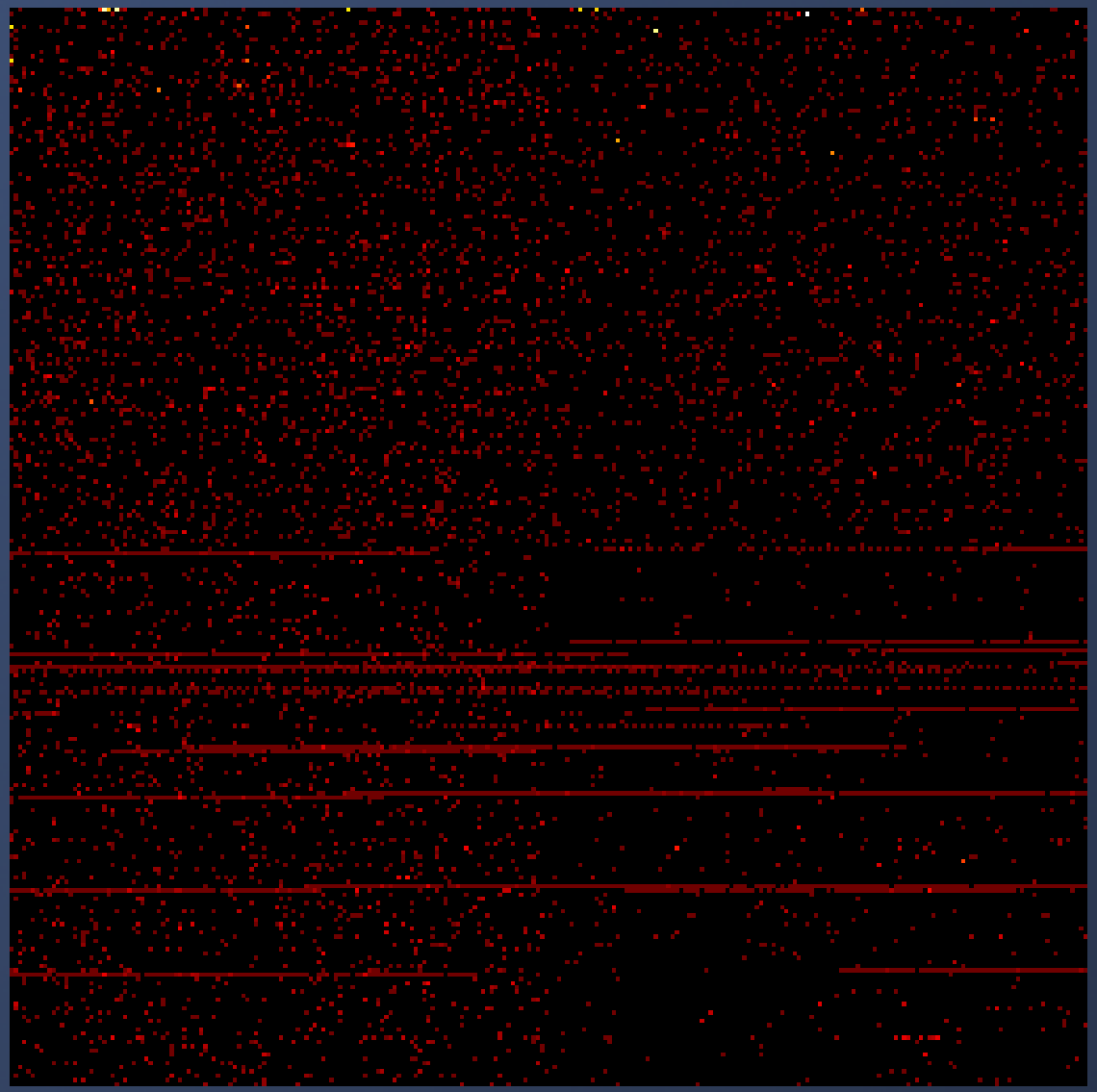
Web-based Visualisations

- Implemented using plug-in interface
- PortMap – specialised scatter plot
- LinkGraph – directed graphs
- HeatMap – … an Ipv4 heat map

PortMap

- Specialised scatter plot
- Displays whole TCP & UDP port range (0 – 65,535)
- X-Axis: port number % 256
- Y-Axis: port number / 256
- Colour encodes number of flows / bytes / packets

PortMap



PortMap - profile live

Query Type

- **Precalculated**
  Shows precalculated values, suitable for overview and animation.
- **Custom (coming soon...)**
  Allows custom filters and source selection. Queries might take a long time.

Time

t_{start}: 201001250000 **Resolution:** 1 Day Update

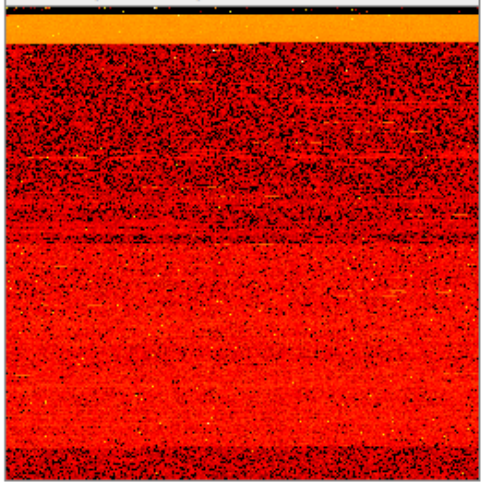
You can use your mouse wheel over a PortMap image to change the current timeframe.

prev next Zoom: 256 x 256 Add Portmap

TCP Src Flows

Protocol: TCP
Show: Src Flows
Topcut: 0
Update

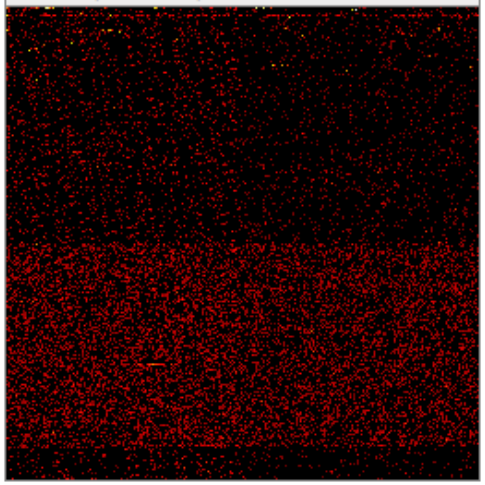
clear | counts | to details tab



TCP Dst Flows

Protocol: TCP
Show: Dst Flows
Topcut: 0
Update

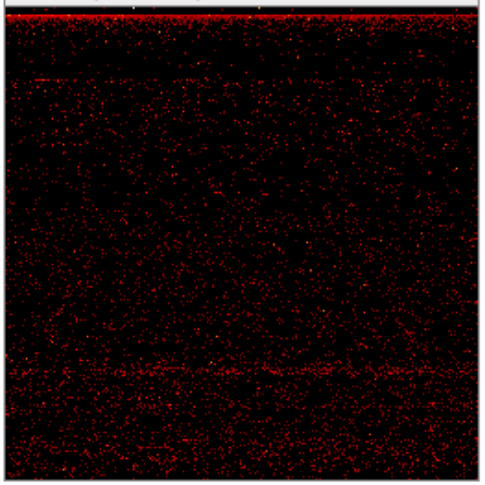
clear | counts | to details tab



UDP Src Flows

Protocol: UDP
Show: Src Flows
Topcut: 0
Update

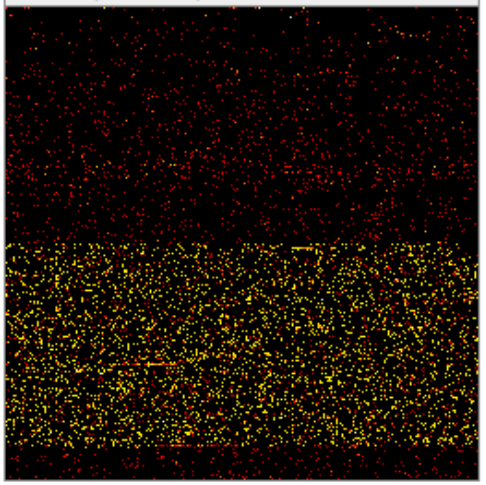
clear | counts | to details tab



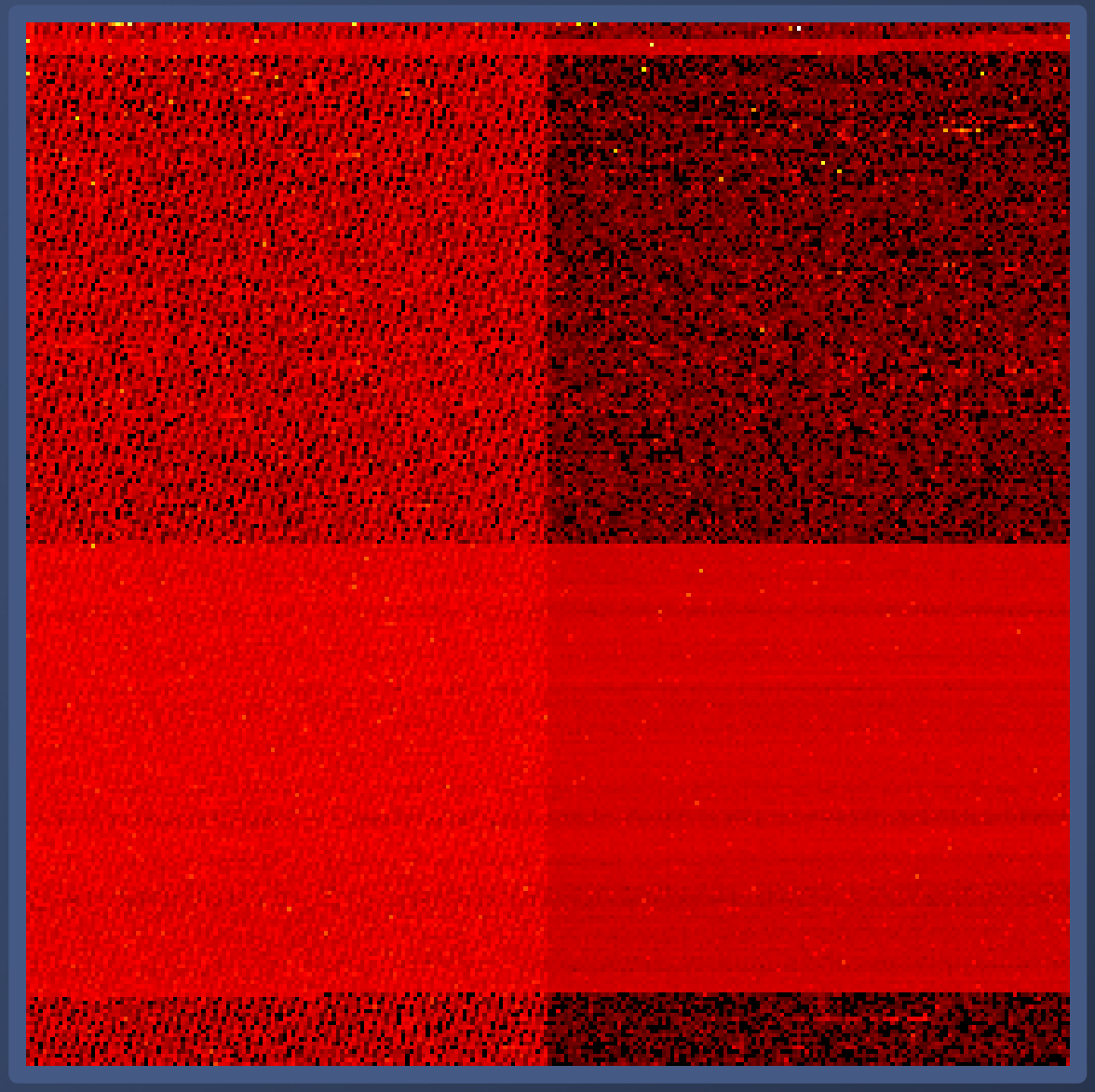
UDP Dst Flows

Protocol: UDP
Show: Dst Flows
Topcut: 0
Update

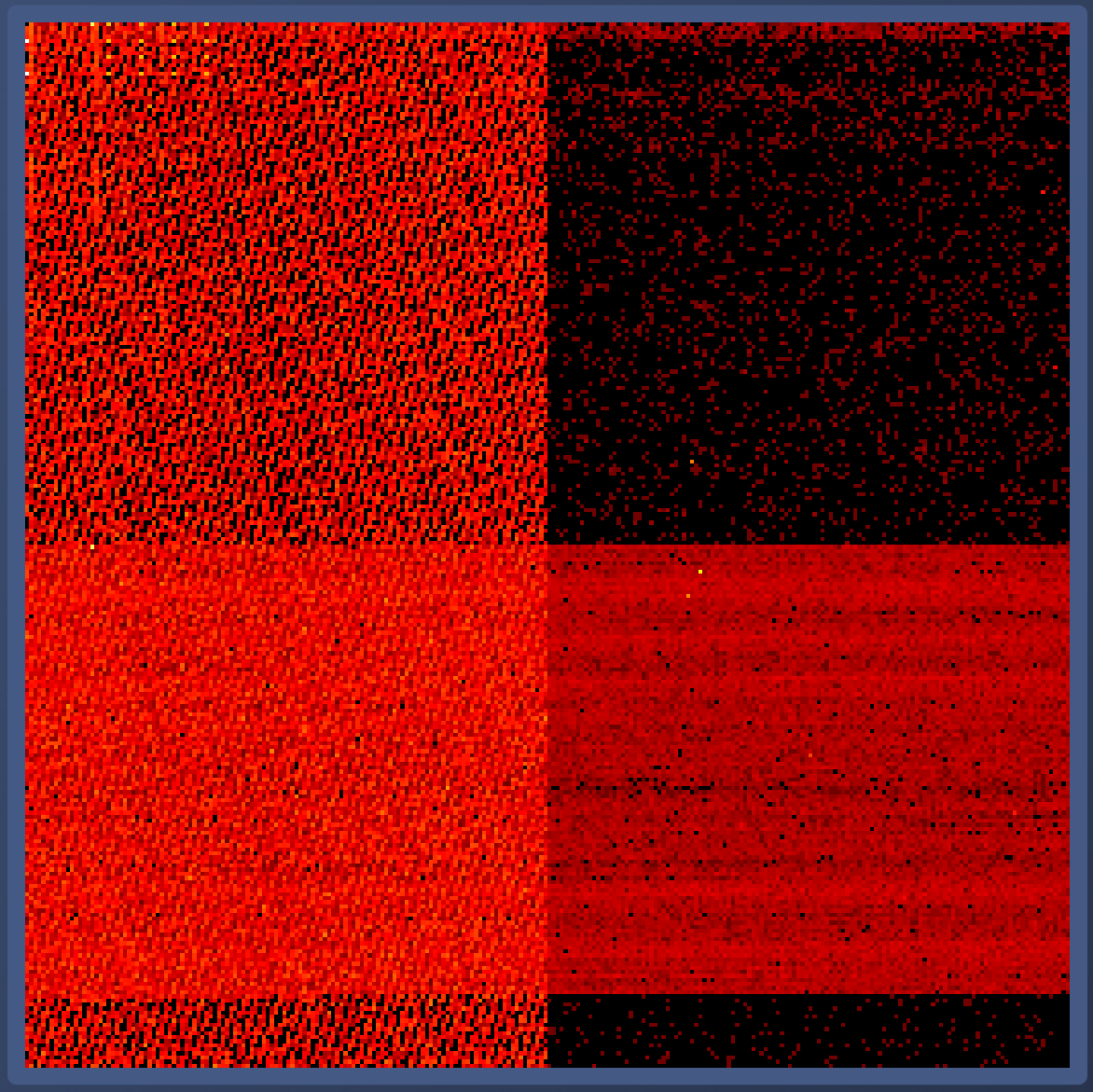
clear | counts | to details tab



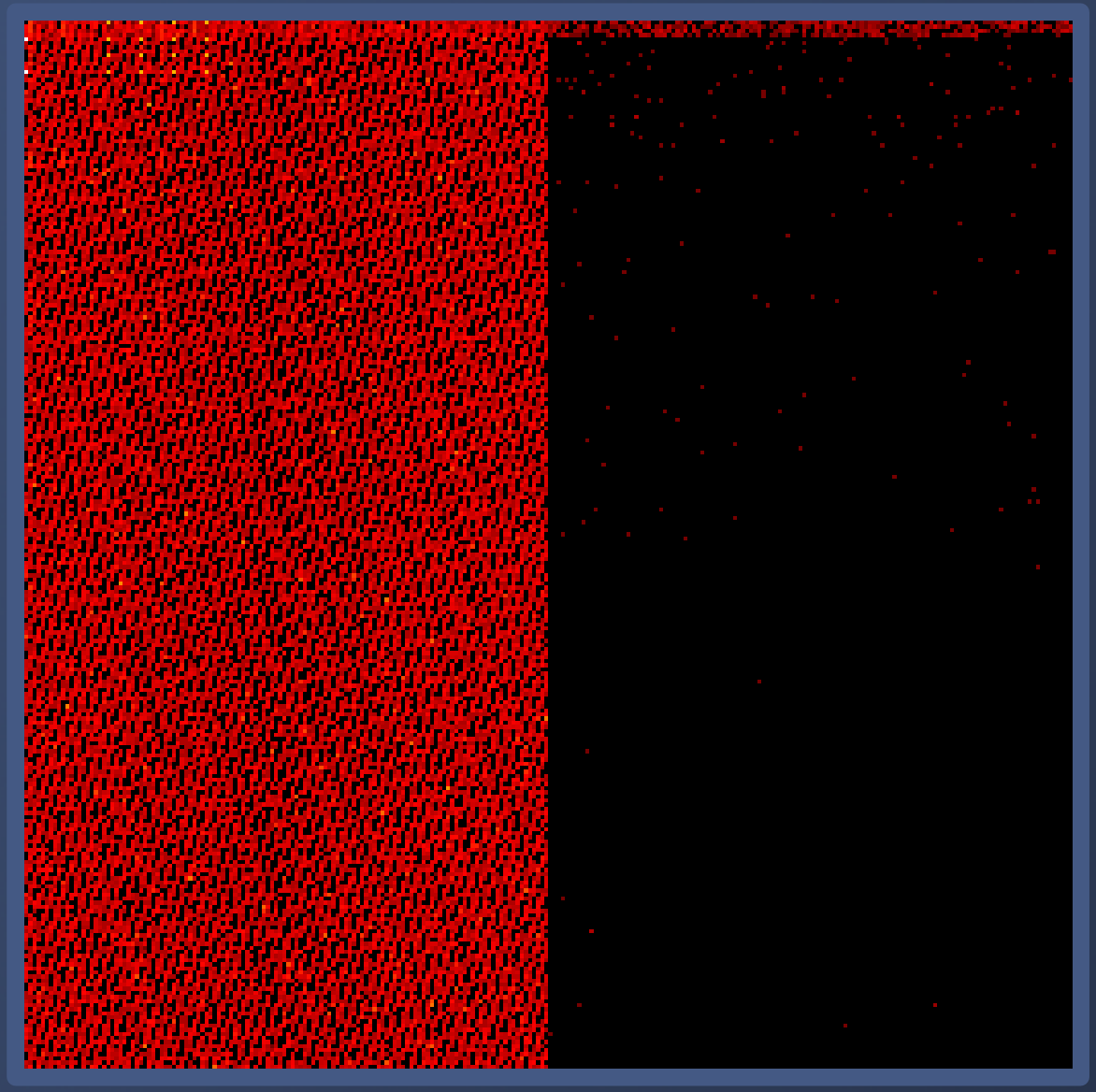
TCP dst flows, 48h



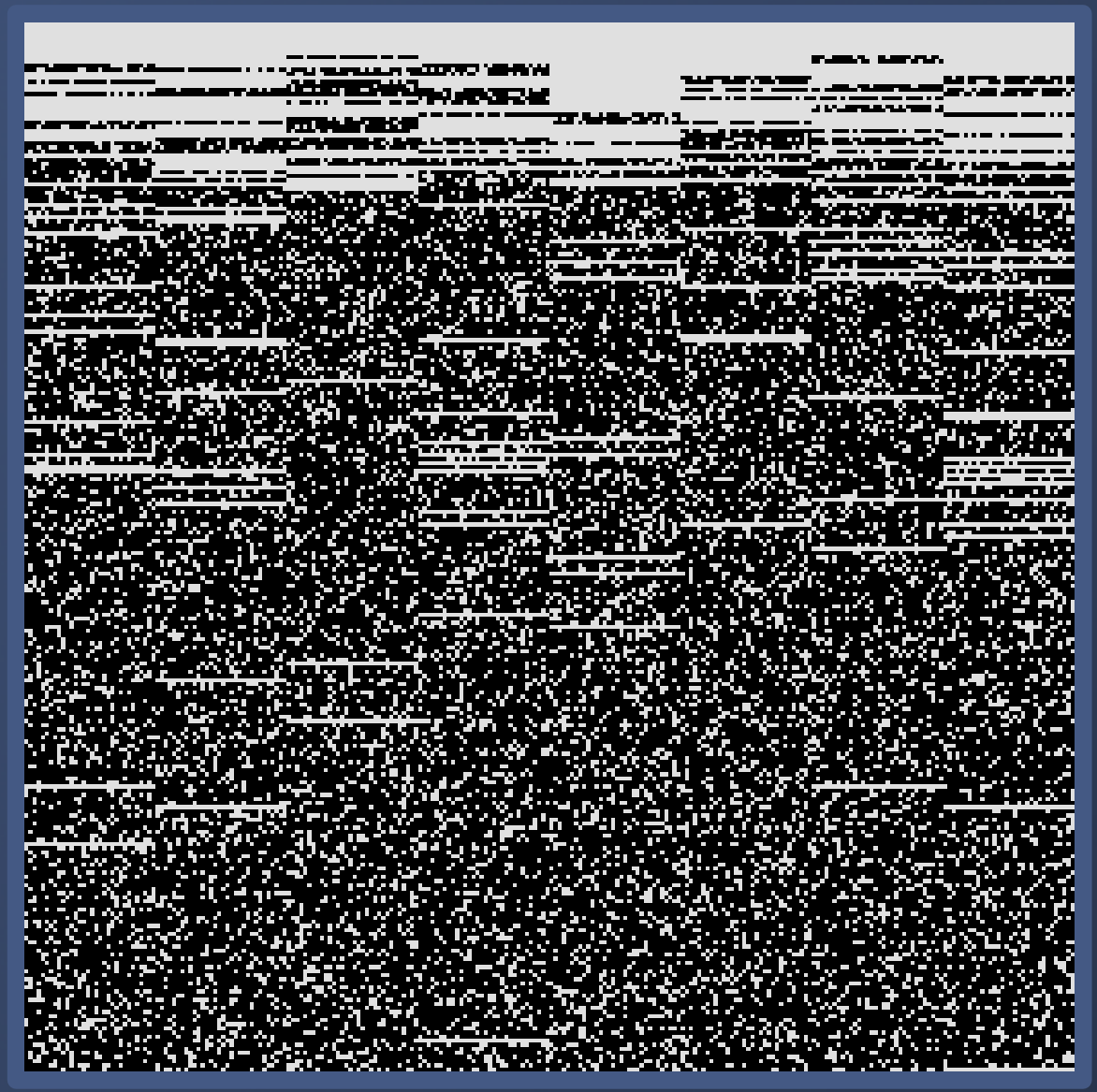
TCP dst flows, 48h, Src Port 80, Syn Ack Flags



TCP dst flows, 48h, Src Port 80, Syn Ack Flags, 48 Bytes

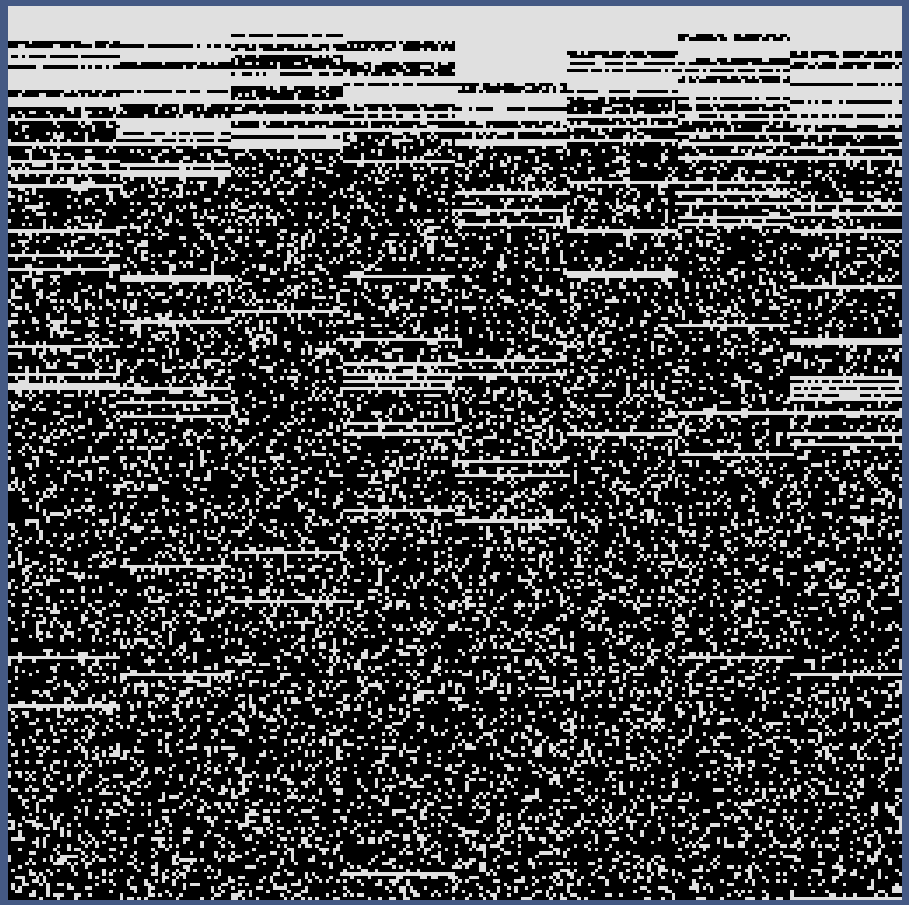


Conficker.C Pattern

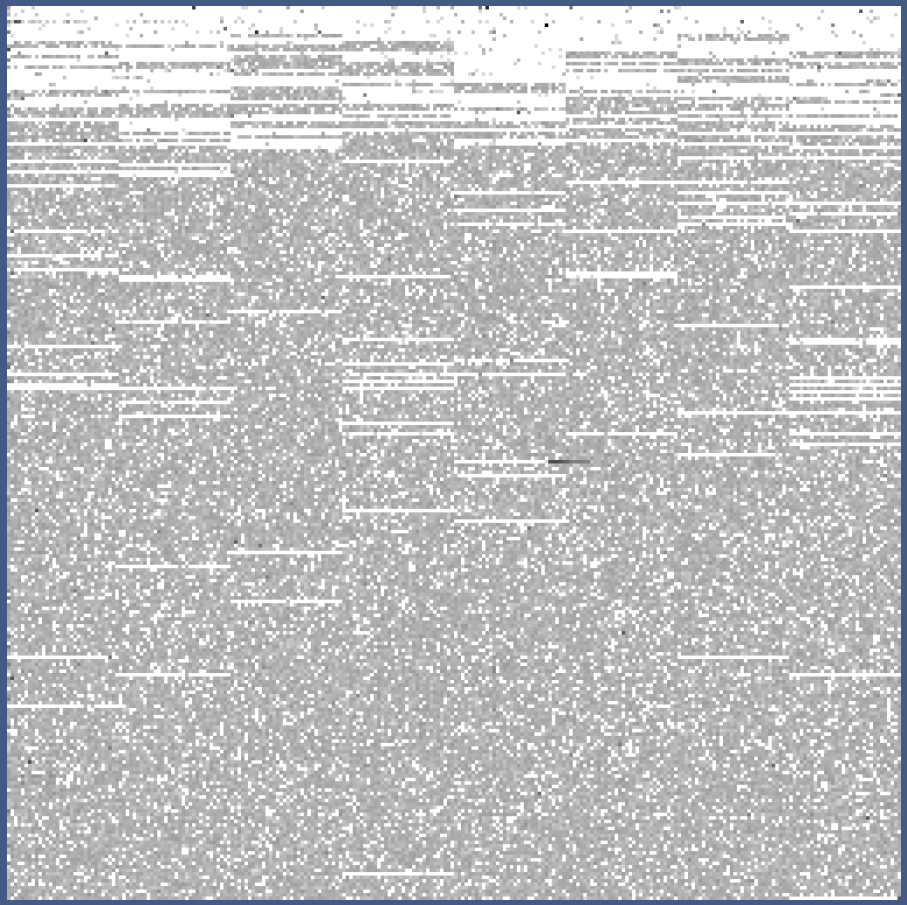


Source: www.bamsoftware.com/wiki/Nmap/PortSetGraphics

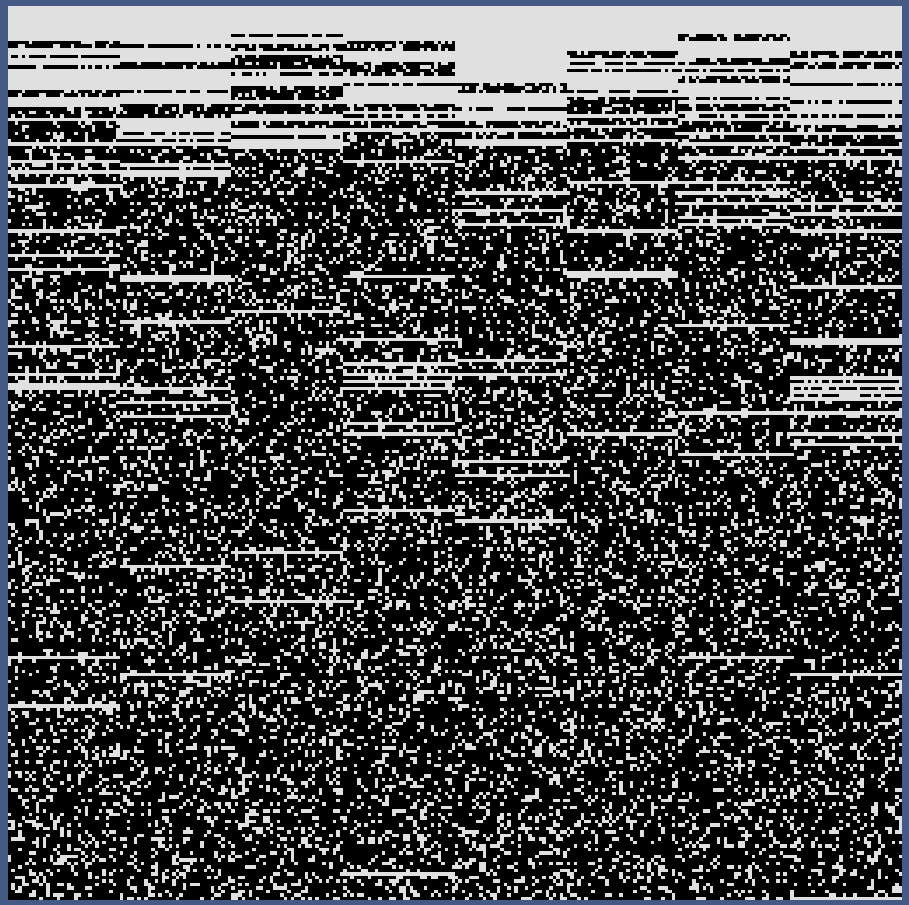
One million generated port numbers, Fifield



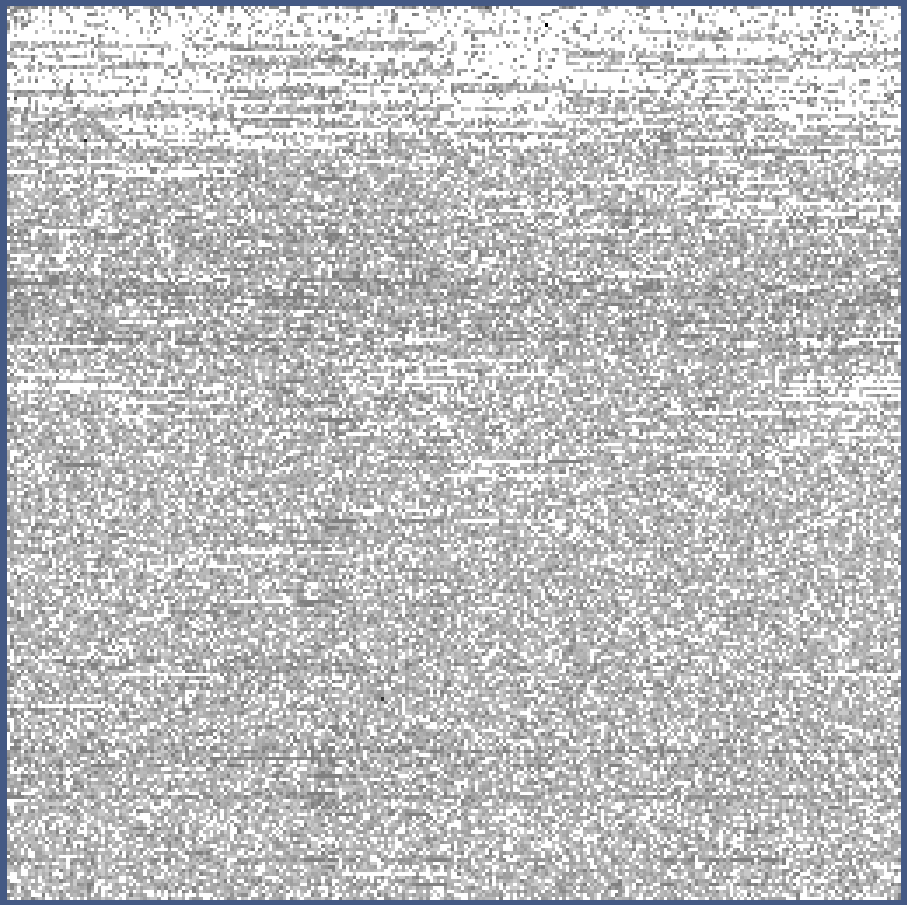
24h darknet UDP dst flows, 17. June 2009



One million generated port numbers, Fifield



48h darknet UDP dst flows, 24.-25. January 2010



TAViS – Traffic Analysis Visualisation System

TAViS Architecture

- Client – Server architecture
- Web-Service provides access to CarmentiS database
- Possibility to aggregate and compress data in Web-Service
- Java client accesses Web-Service
- Modular architecture for easy development of new visualisations

File Edit

First Perspective

Toggle DataSelection | Update | Abort | Save | Load | Add Visualization...

Update Progress

Request	Status	Results

Source

Profile: live

Channels:

presense_ids
nepenthes_mw
presense_mon
darknet_mon
nepenthes_stat
network_mon

Time

Start: Jan 25, 2010 00:00

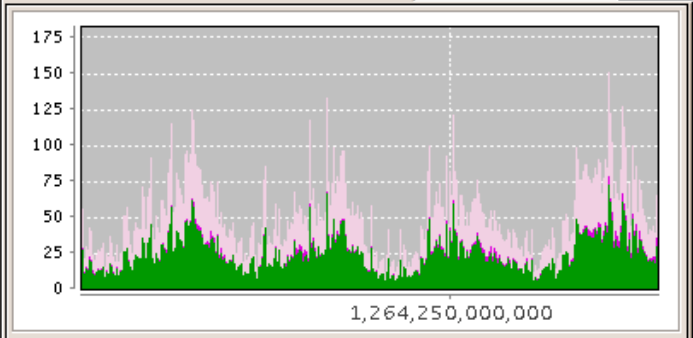
End: Jan 25, 2010 02:00

Misc

Limit to: 1000

Filter:

Profile Overview (flows)



Visualization | Configuration

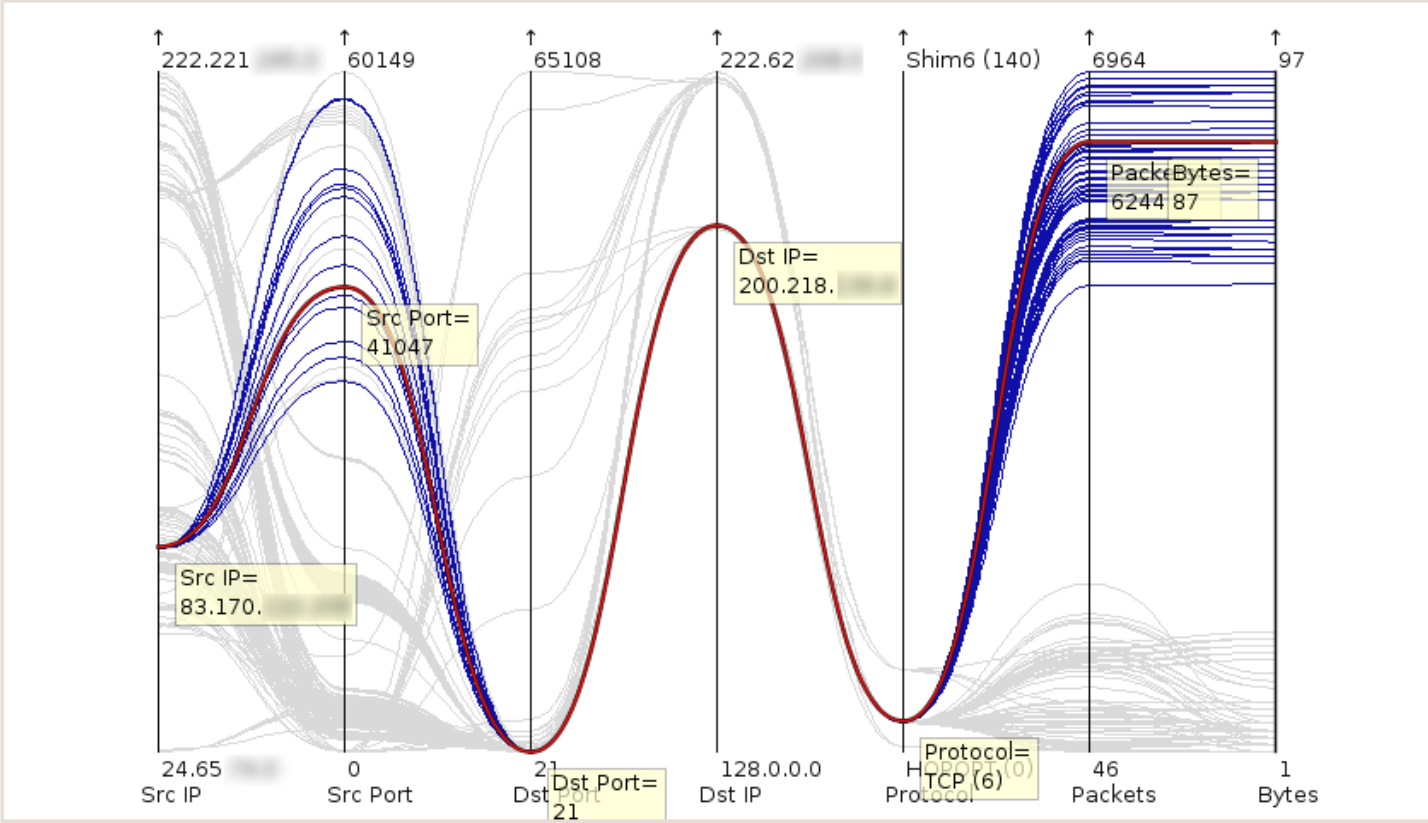
Event Table

Start	End	Proto...	Sourc...	Sourc...	Desti...	Desti...
Sun Ja...	Sun Ja...	UDP (...	195.2...	69	200.2...	45846
Sun Ja...	Sun Ja...	TCP (6)	186.1...	55583	222.6...	22
Sun Ja...	Sun Ja...	TCP (6)	190.1...	13680	222.6...	22
Sun Ja...	Sun Ja...	UDP (...	195.2...	69	200.2...	45846
Sun Ja...	Sun Ja...	TCP (6)	190.1...	13655	222.6...	22
Sun Ja...	Sun Ja...	TCP (6)	190.1...	13342	222.6...	22
Sun Ja...	Sun Ja...	UDP (...	195.2...	69	200.2...	45846
Sun Ja...	Sun Ja...	TCP (6)	91.11...	3193	222.6...	22
Sun Ja...	Sun Ja...	UDP (...	195.2...	69	200.2...	45846

Visualization | Configuration

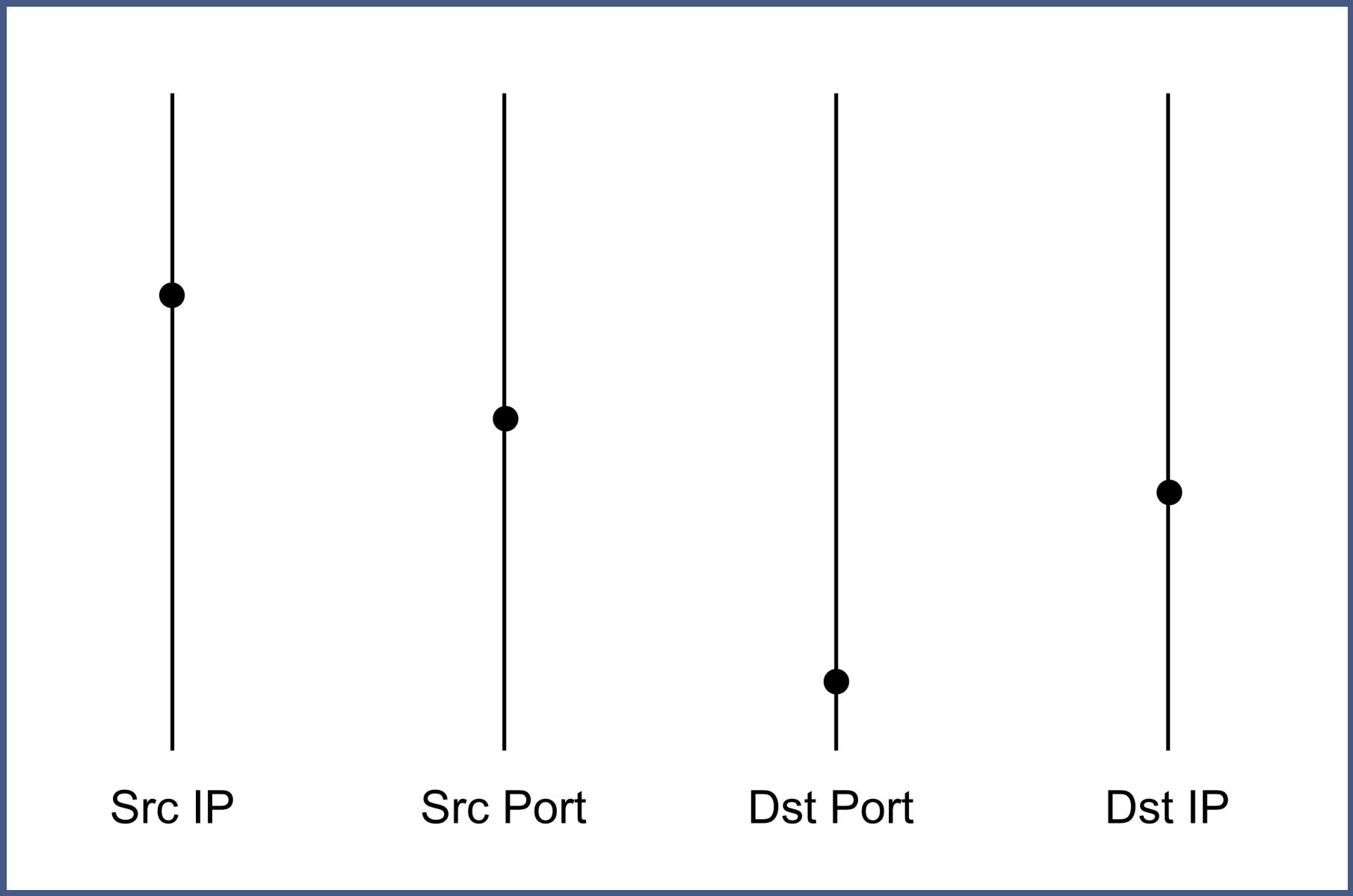
Parallel Coordinates

Reset Scaling | Hover Selection

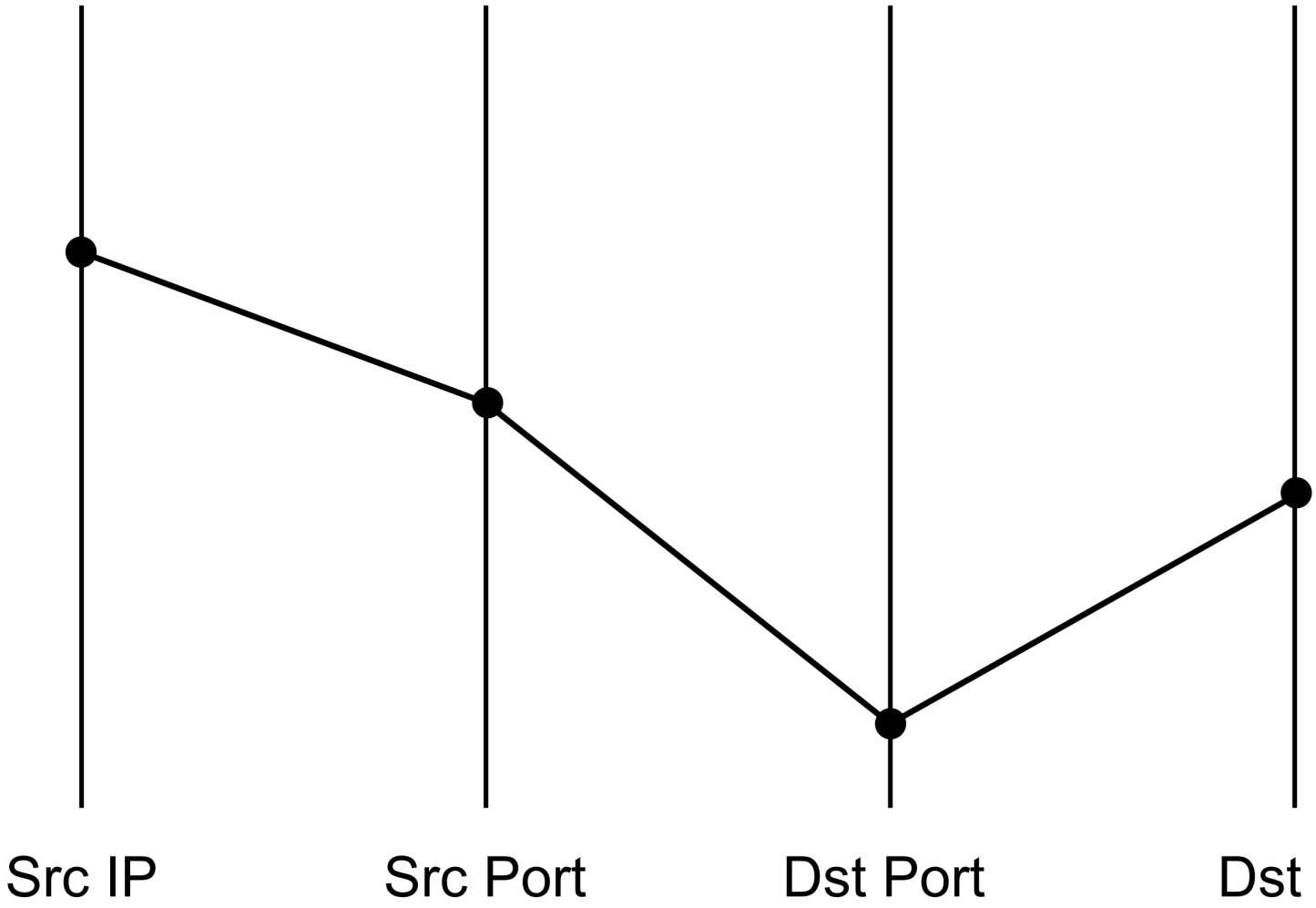


Visualization | Configuration

Parallel Coordinate Plot



Parallel Coordinate Plot



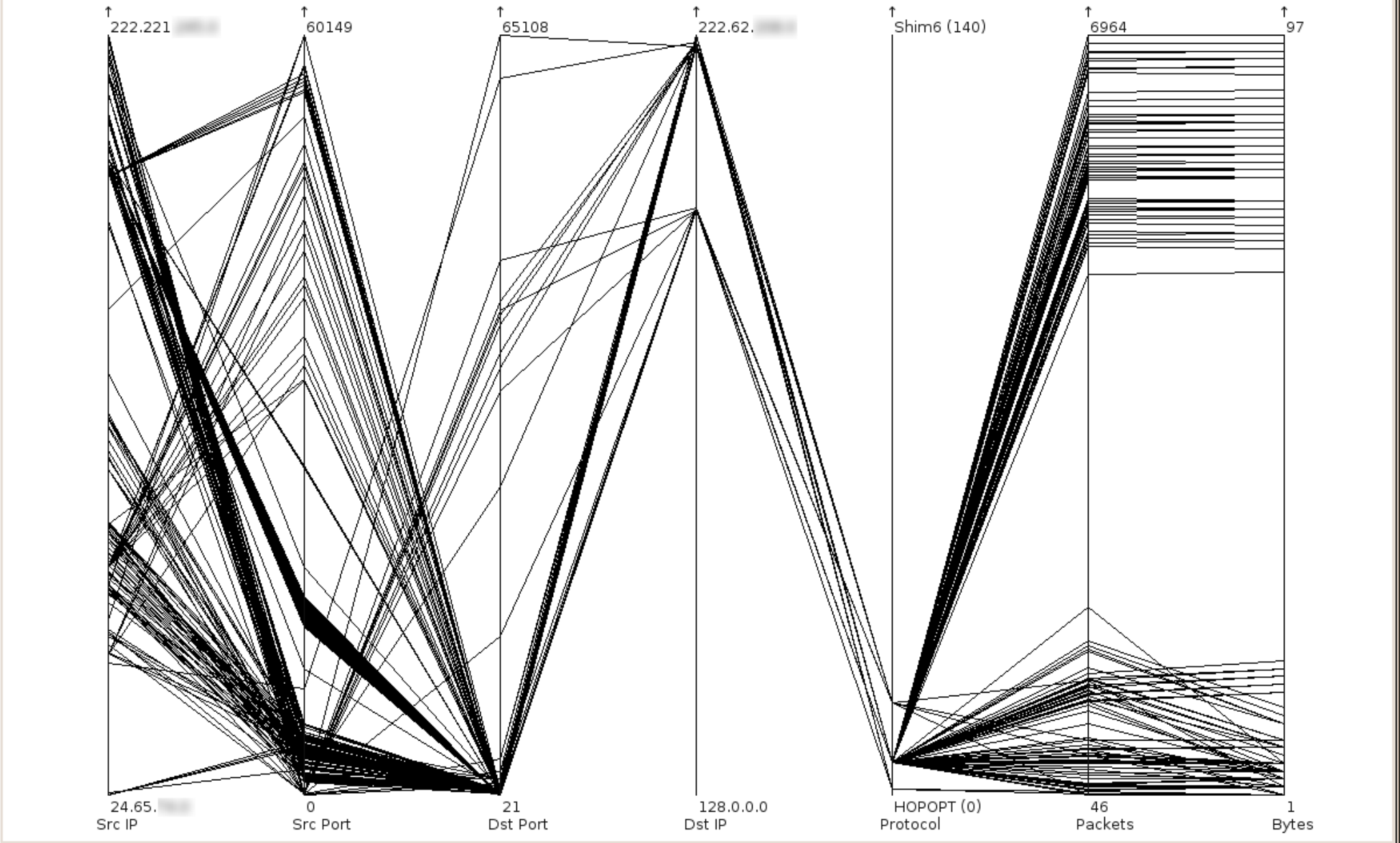
File Edit

First Perspective

Toggle DataSelection | Update | Abort | Save | Load | Add Visualization...

Parallel Coordinates

Reset Scaling | Hover Selection



Visualization | Configuration

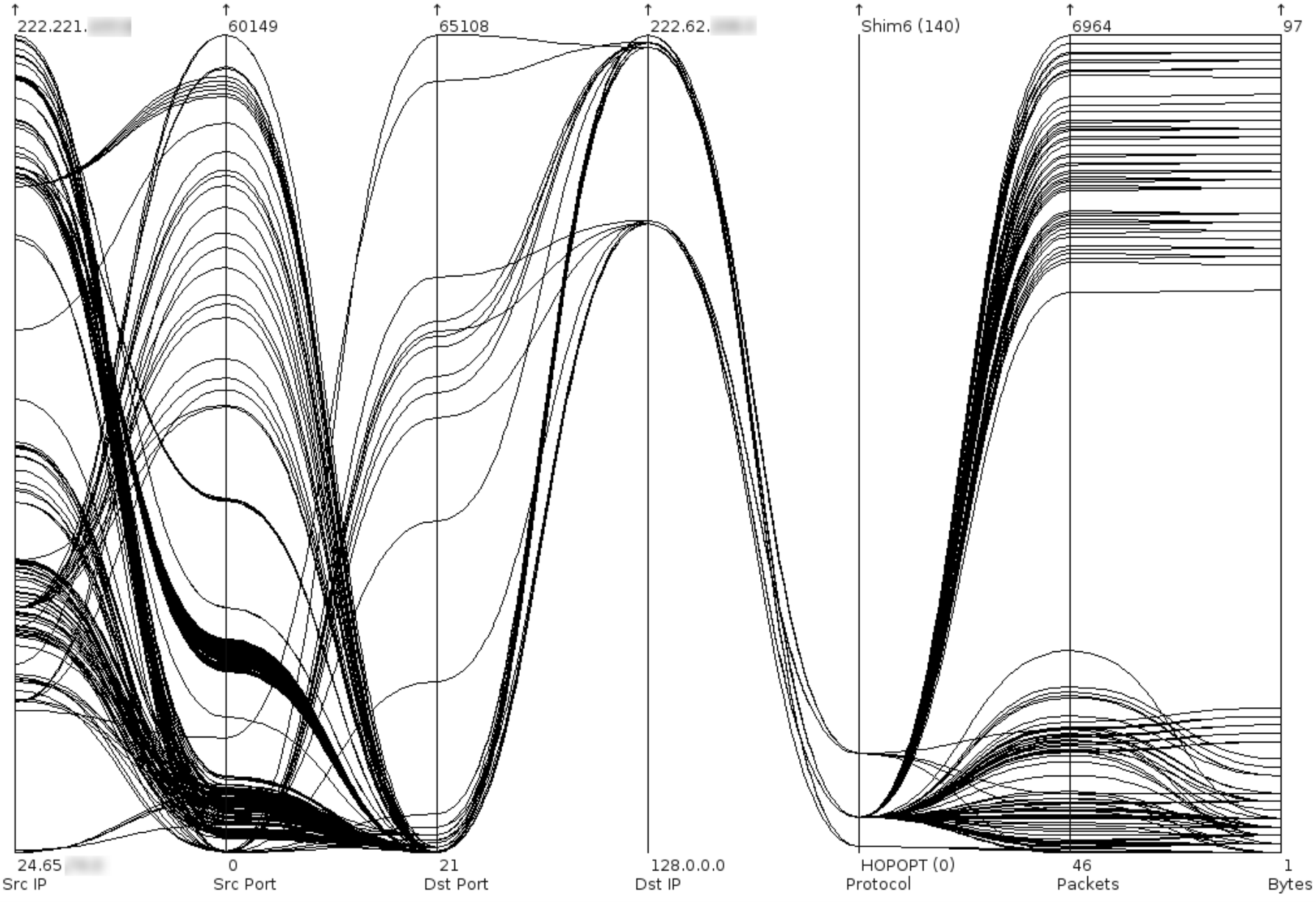
File Edit

First Perspective

Toggle DataSelection | Update | Abort | Save | Load | Add Visualization...

Parallel Coordinates

Reset Scaling | Hover Selection



Visualization | Configuration

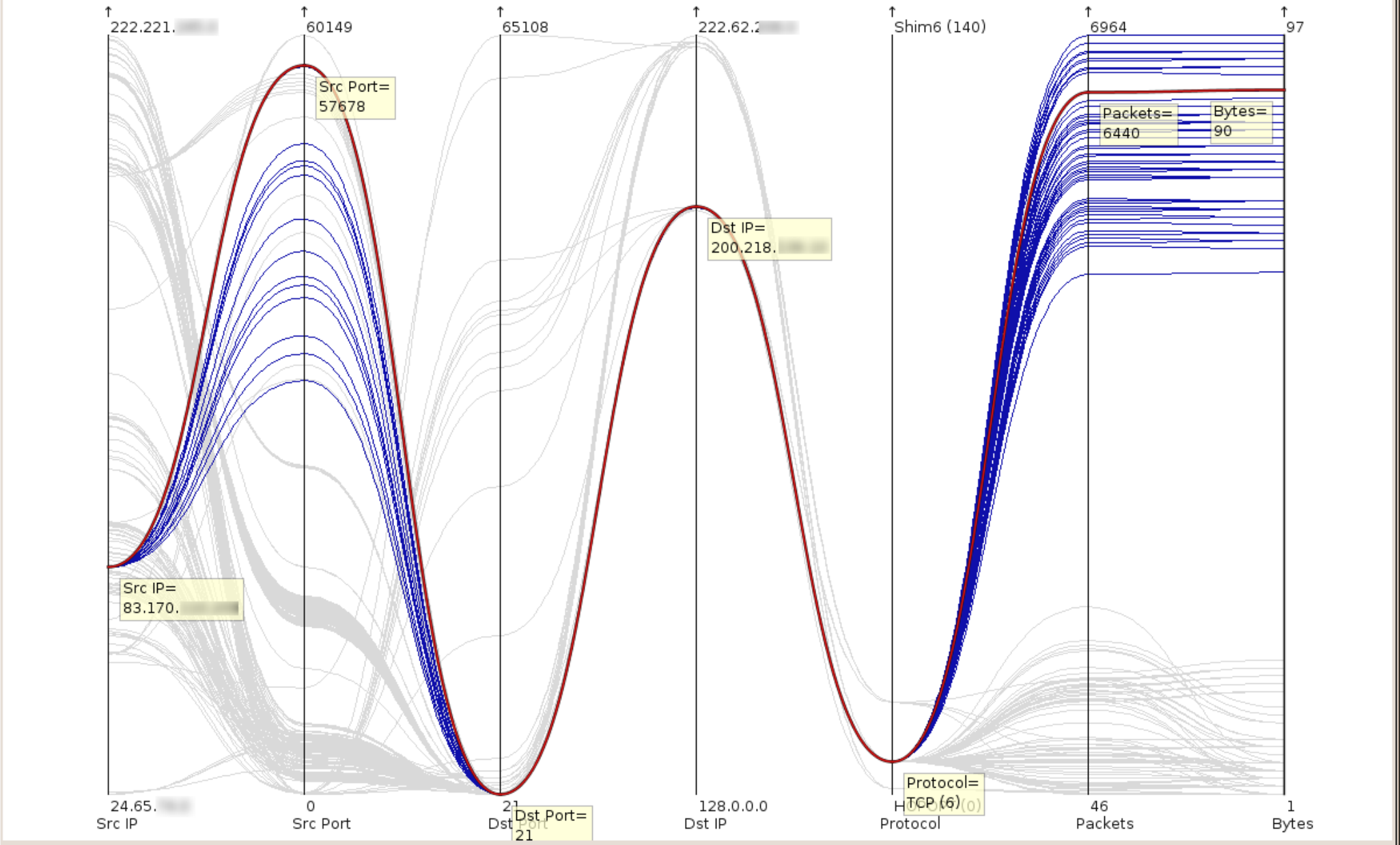
File Edit

First Perspective

Toggle DataSelection | Update | Abort | Save | Load | Add Visualization...

Parallel Coordinates

Reset Scaling | Hover Selection



Visualization | Configuration

Evaluation

- First feedback from analysts very positive.
- More evaluation necessary!
- Traffic analysis tasks heavily influenced by current user interface, compare with other early warning systems.

Summary

- Identified traffic analysis tasks
- Reviewed suitable visualisation techniques
- Implemented three web-based visualisations as CarmentiS plug-ins
- Implemented TAViS and a parallel coordinate display.

Thank you for your attention!

E-Mail: weseloh@dfn-cert.de