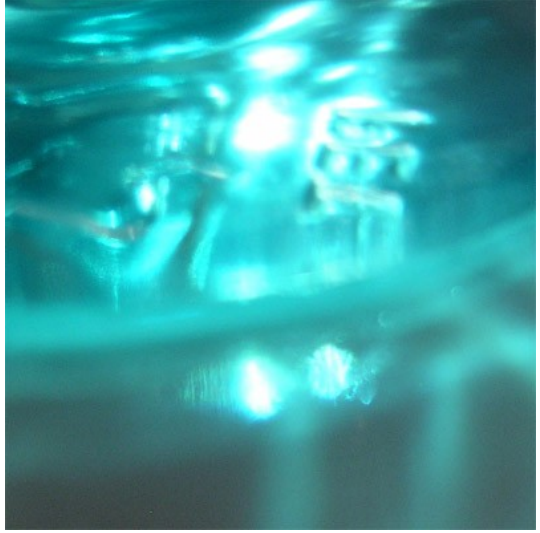
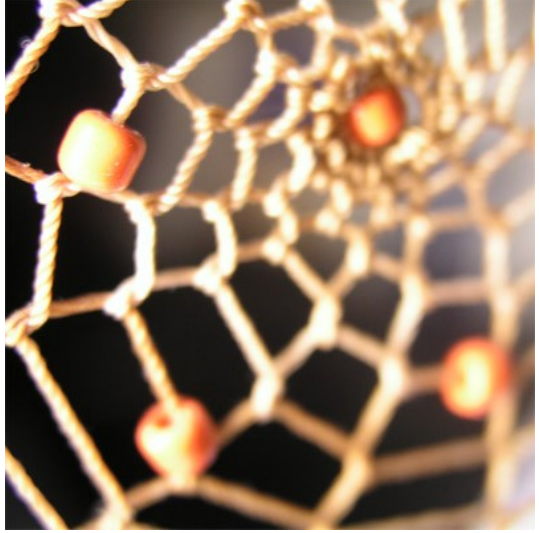




Diplomarbeit: Svenja Wendler

Strukturfindung im Internetverkehr mittels Assoziationsregeln

Svenja Wendler
svenja@wendler-im-netz.de

Institut für Internet-Sicherheit
www.internet-sicherheit.de
Fachhochschule Gelsenkirchen

if(is) internet-sicherheit.

Inhalte

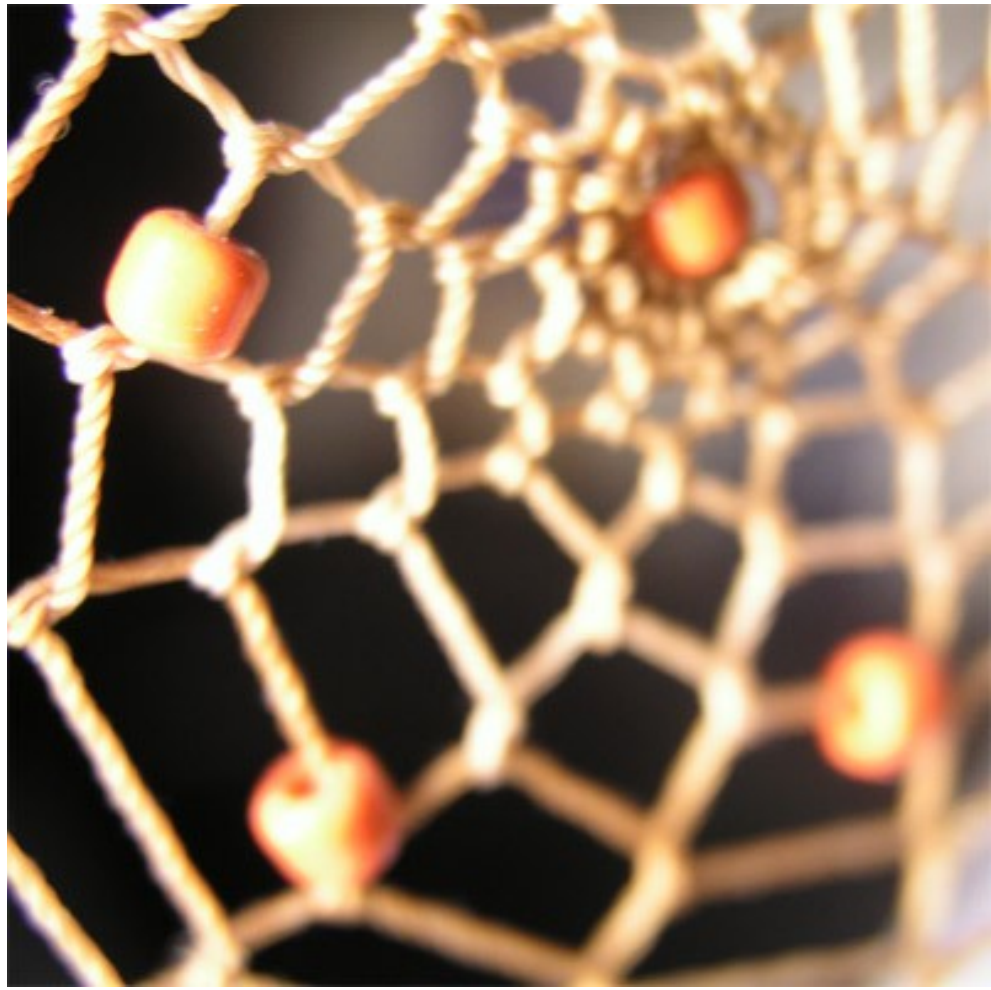
Assoziationsregeln

Internet-Analyse-System

Neues Analysemodul

Beispielanalyse

Ausblick



Assoziationsregeln

4 Bestandteile

- Vorraussetzung
- Folge
- Wahrscheinlichkeit
- Häufigkeit

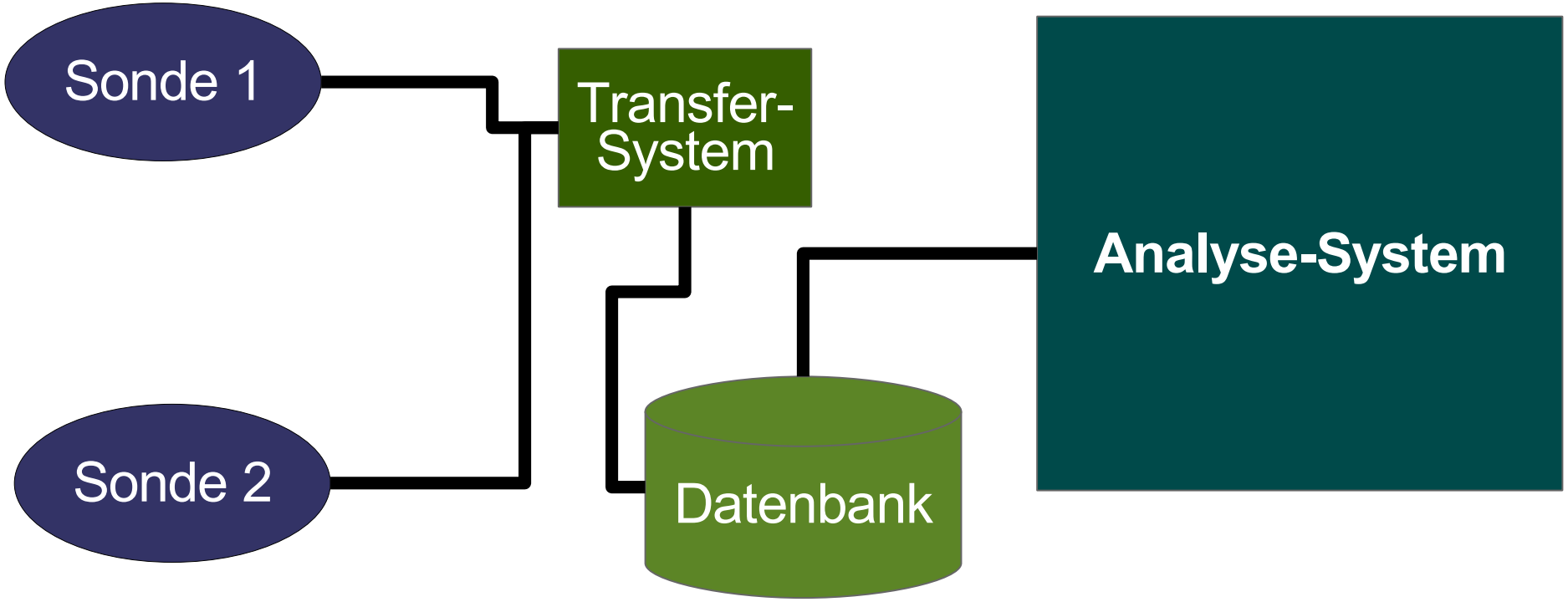
„Wenn Milch gekauft wird, dann werden auch Äpfel gekauft“

In dieser Arbeit:

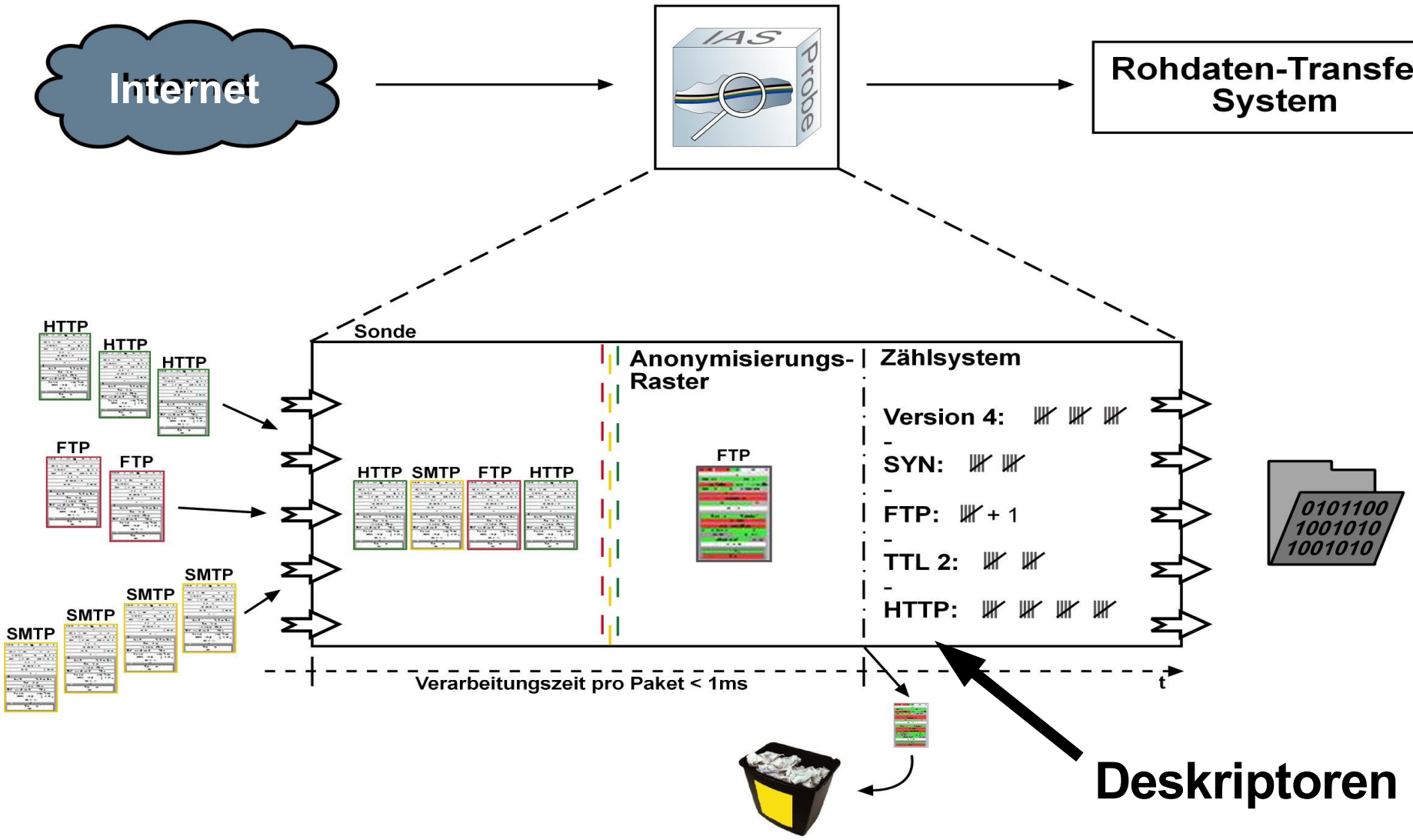
Wenn Internet (HTTP), dann auch E-Mail (SMTP)

Internet Analyse System

1. Sonden – zeichnen Internetverkehr anonymisiert auf
2. Datenbank – speichert die Verkehrsdaten (Kommunikationsparameter)
3. Analyse-System – analysiert die Daten und stellt sie grafisch dar



Datenerfassung in einer Sonde



Strukturen im Internet-Datenverkehr finden

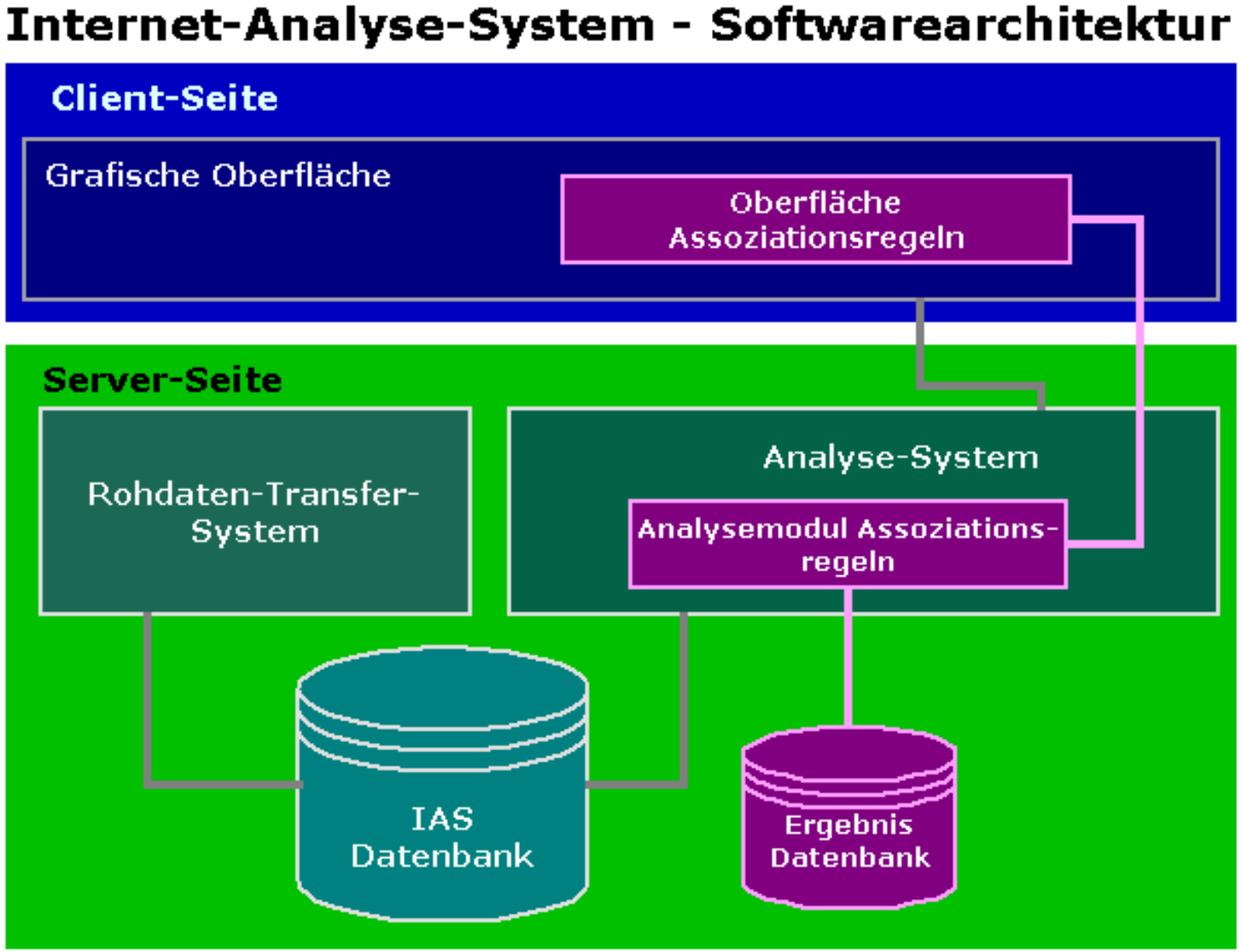
Beziehungen zwischen Protokollen und Diensten unterschiedlicher Art:

- Zusammenhänge auf Grund des Protokollstacks
  - **IP und TCP, UDP oder ICMP**
- Protokollsemantische Zusammenhänge
  - **TCP Verbindungsaufbau - SYN,ACK-Flags**
- Verhaltenstechnische, wirklich neue Zusammenhänge
  - **Wenn jemand E-Mails schreibt surft er auch im Internet**

erweiterbar:

- Normalzustände
- Anomaliezustände

Einbindung des Analyse-Moduls



modular
lose gekoppelt

realisiert mit:
J2EE,
Java Swing
JBOSS-Server

Beispiel E-Mail-Datenverkehr und DNS (1)

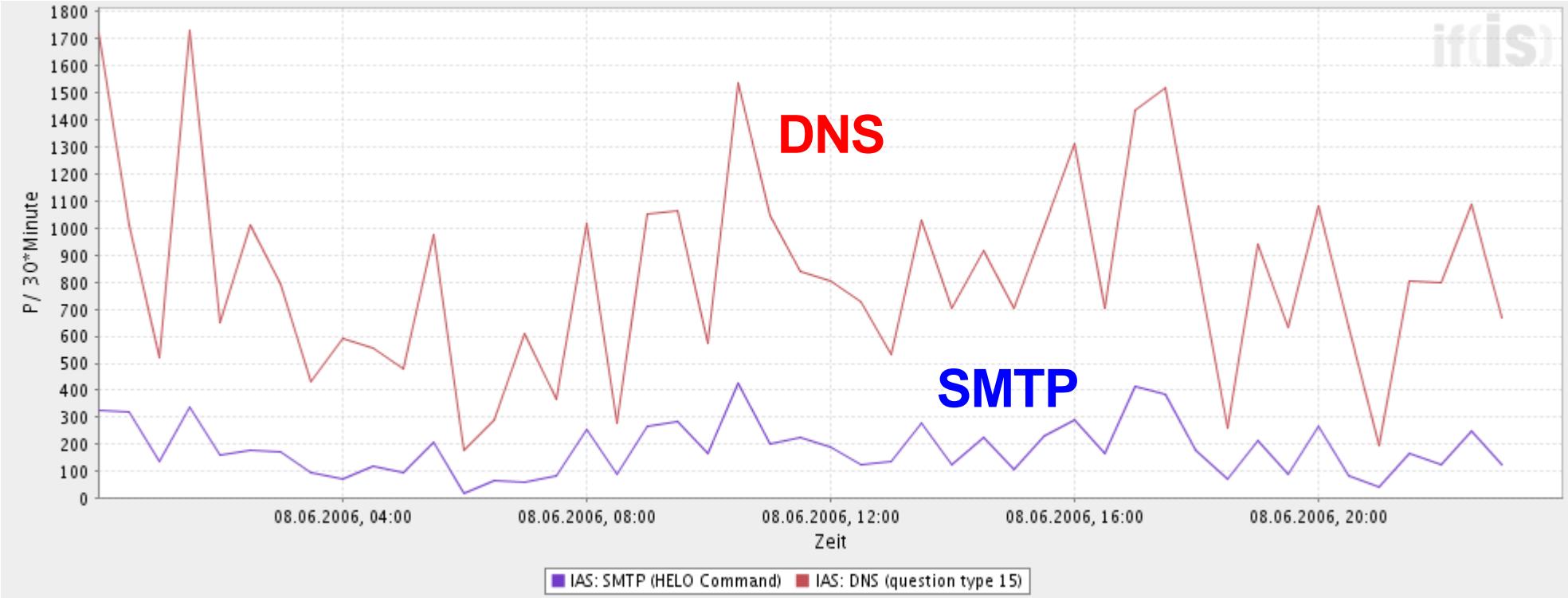
Zusammenhänge der Kategorie 2 „protokollsemantisch“ finden
Beziehung zwischen E-Mail-Session und DNS-Anfrage

E-Mails werden im Internet mittels DNS geroutet (MX-Record)

Geeignete Attribute (Deskriptoren):
- SMTP HELO Command (tritt nur einmal pro E-Mail-Session auf)
- DNS Question Type MX

Ort: **Sonde an der FH nur Ausgangsverkehr**
Zeitraum: **8.6.2006**

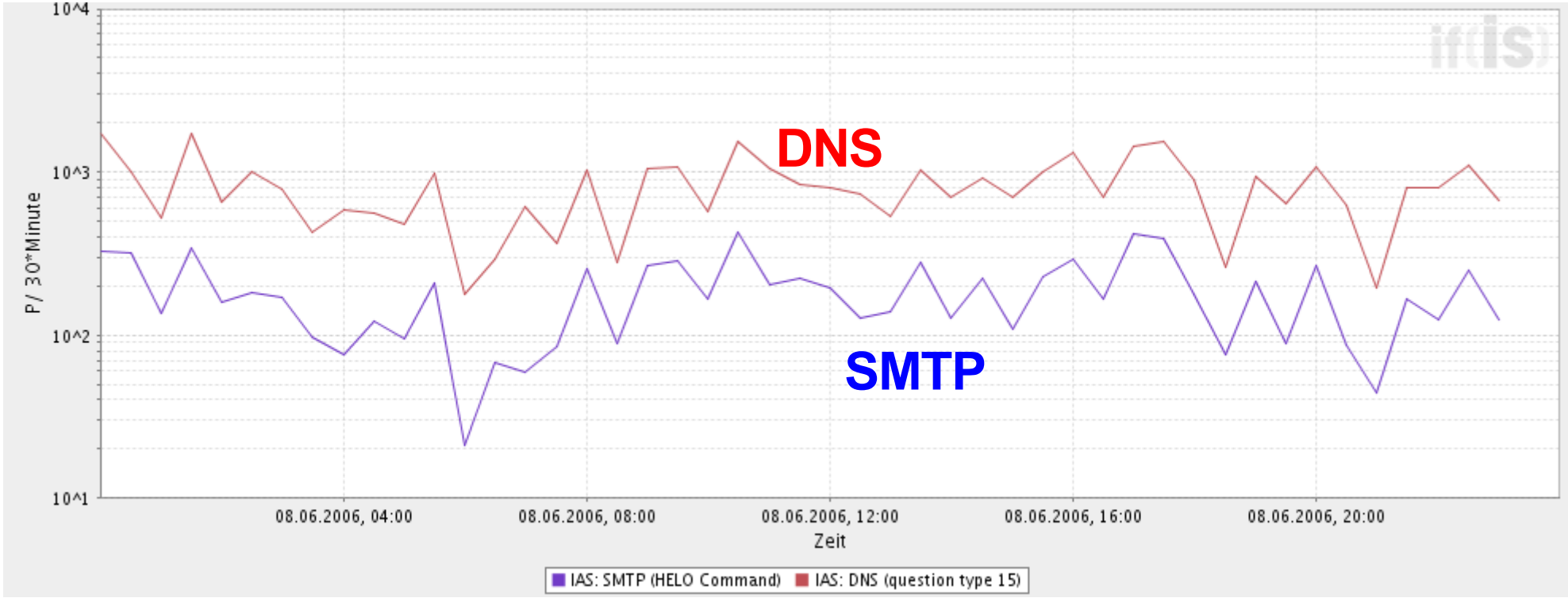
Beispiel E-Mail-Datenverkehr und DNS (2)



Grafik aus dem Internet-Analyse-System

Anzahl der DNS und SMTP Pakete über die Zeit am 8. Juni 2006

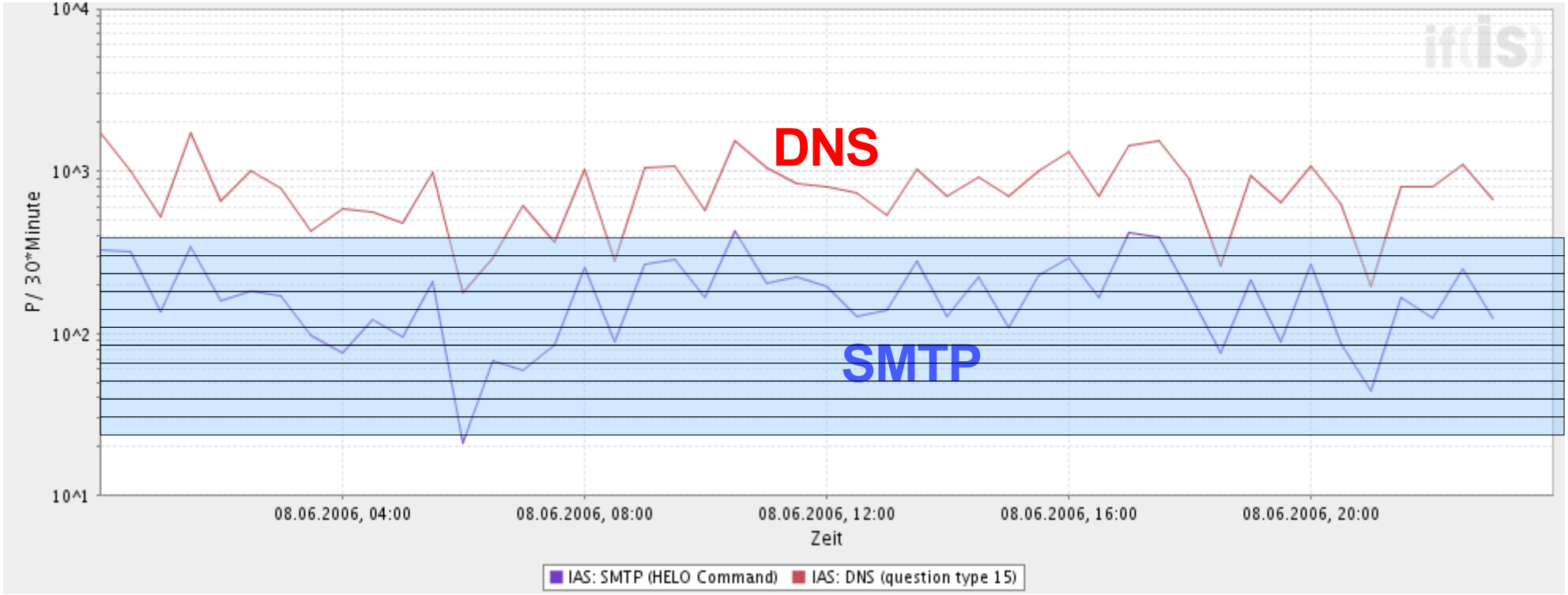
Beispiel E-Mail-Datenverkehr und DNS (3)



Anzahl der DNS und SMTP Pakete über die Zeit

(logarithmische Skalierung)

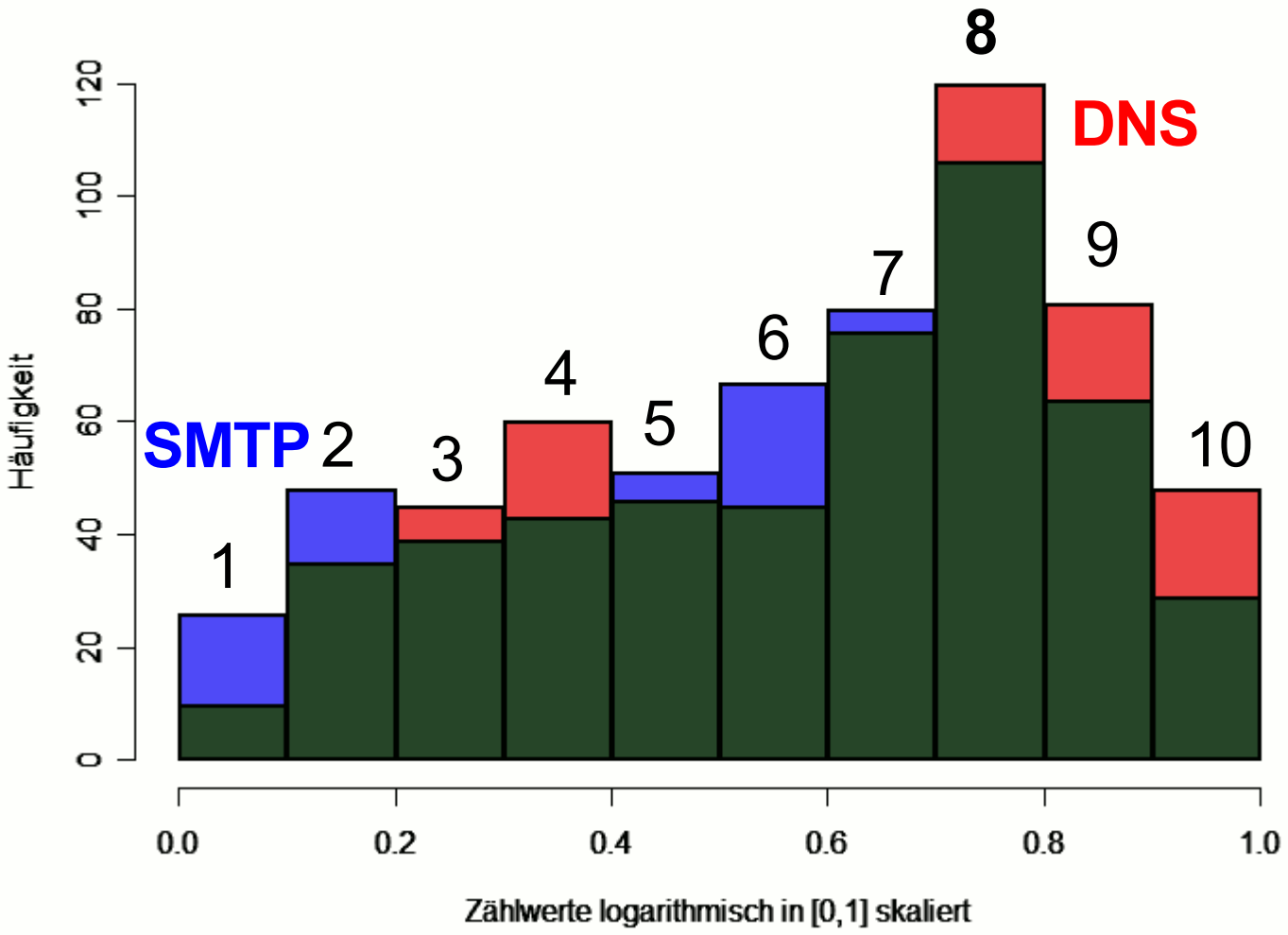
Beispiel E-Mail-Datenverkehr und DNS (4)



Erstellen eines Histogramms, um einen Überblick über die Häufigkeitsverteilung zu bekommen

Beispiel E-Mail-Datenverkehr und DNS (5)

Histogramm mit 10 Mengenklassen

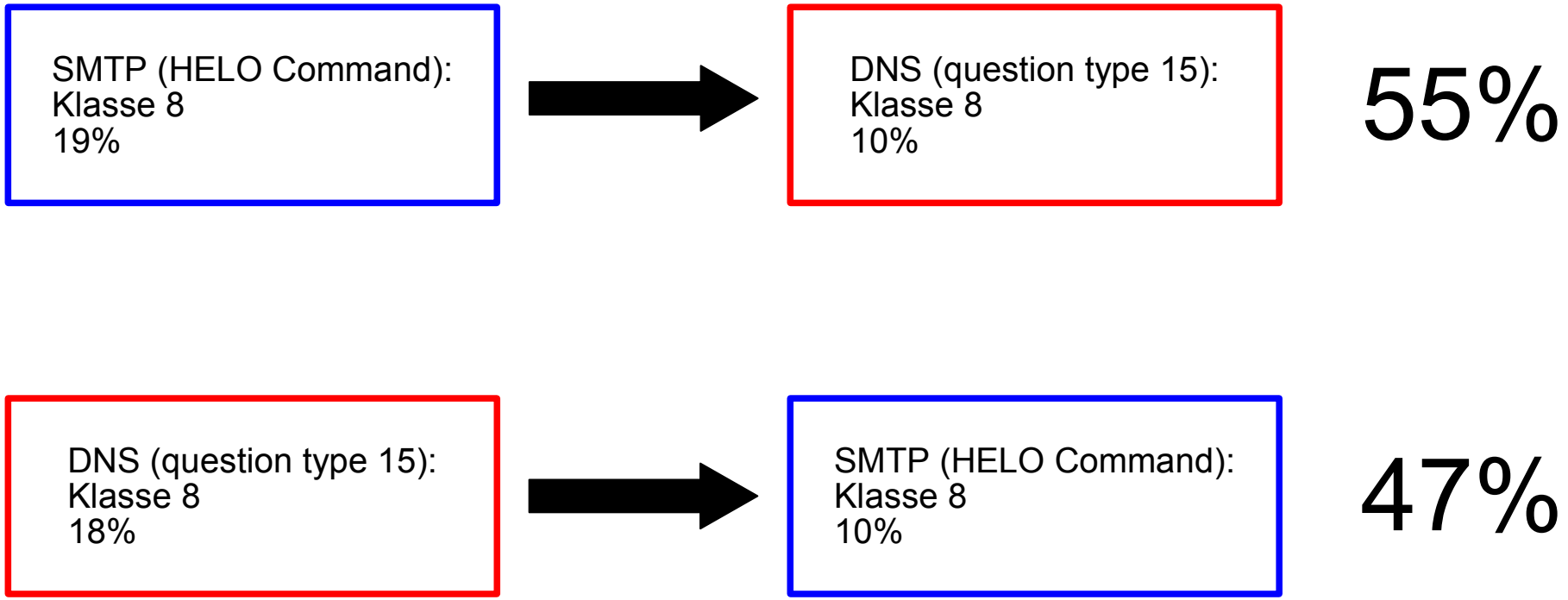


Beide Histogramme haben eine große Schnitt-menge

Beide haben ein Maximum bei Klasse 8

Beispiel E-Mail-Datenverkehr und DNS (6)

Gefundene Regeln

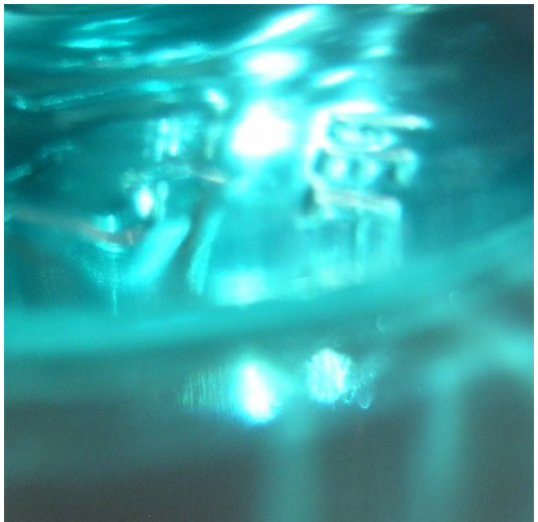


Ausblick

Unbekannte Zusammenhänge zwischen Diensten finden.

Zeitliche Dimension mit in die Analyse aufnehmen.

Analysemodul in das Internet-Analyse-System integrieren.



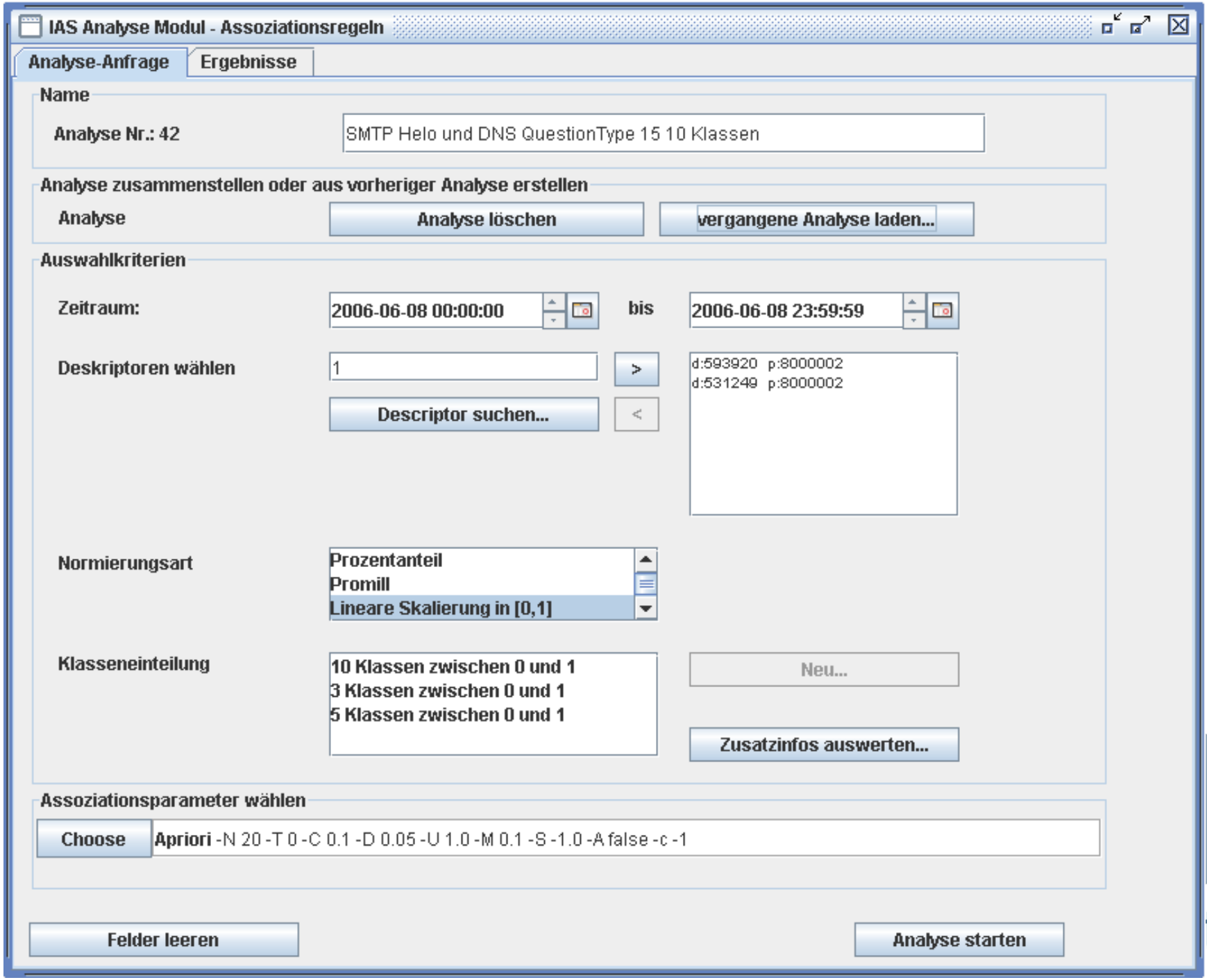
Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Svenja Wendler
svenja@wendler-im-netz.de

Institut für Internet-Sicherheit
www.internet-sicherheit.de
Fachhochschule Gelsenkirchen

if(is) internet-sicherheit.


IAS Analyse Modul - Assoziationsregeln
Analyse-Anfrage
Ergebnisse
Name
Analyse Nr.: 42
SMTP Helo und DNS QuestionType 15 10 Klassen
Analyse zusammenstellen oder aus vorheriger Analyse erstellen
Analyse
Analyse löschen
vergangene Analyse laden...
Auswahlkriterien
Zeitraum:
2006-06-08 00:00:00
bis
2006-06-08 23:59:59
Deskriptoren wählen
1
>
<
Descriptor suchen...
d:593920 p:8000002
d:531249 p:8000002
Normierungsart
Prozentanteil
Promill
Lineare Skalierung in [0,1]
Klasseneinteilung
10 Klassen zwischen 0 und 1
3 Klassen zwischen 0 und 1
5 Klassen zwischen 0 und 1
Neu...
Zusatzinfos auswerten...
Assoziationsparameter wählen
Choose
Apriori -N 20 -T 0 -C 0.1 -D 0.05 -U 1.0 -M 0.1 -S -1.0 -A false -c -1
Felder leeren
Analyse starten