

HESSEN



EINSATZ DER NETZWERKFORENSIK FÜR ERMITTLUNGSBEHÖRDEN

Hessisches Landeskriminalamt

Andreas Frantzen

19.12.2013

Über mich....



- Digital Forensiker, Netzwerk-Forensiker
- Studium an der HS Fulda – Angewandte Informatik – Vertiefungsrichtung : Telekommunikationstechnik
 - Abschluss als: Dipl. Inf. (FH)
- Seit 08.2009 beim Hessischen Landeskriminalamt
 - 08.2009 bis 08.2012 aktiv im Bereich „Cybercrime“
 - 09.2012 bis heute aktiv im Bereich „Netzwerkforensik“
- Fernstudium an der Hochschule Albstadt-Sigmaringen im Studiengang „Digitale Forensik“
 - Dauer: 6 Semester
 - Voraussichtlicher Abschluss als „Master of Science“ 09.2014

Zum Vortrag...

- Dauer: ~40 Minuten
- Drei Abschnitte
 - Was macht die Netzwerkforensik?
 - Themenheranführung, Gerätschaften,...
 - Analyse von Netzwerkdaten mit Wireshark
 - Wireshark, Filtern von Daten, Bitebene, Metaebene,...
 - Analyse von Netzwerkdaten mit Cascade Pilot
 - Grafisches „Eintauchen“ in die Netzwerkdaten
- Abschluss: ~15 Minuten für Fragen

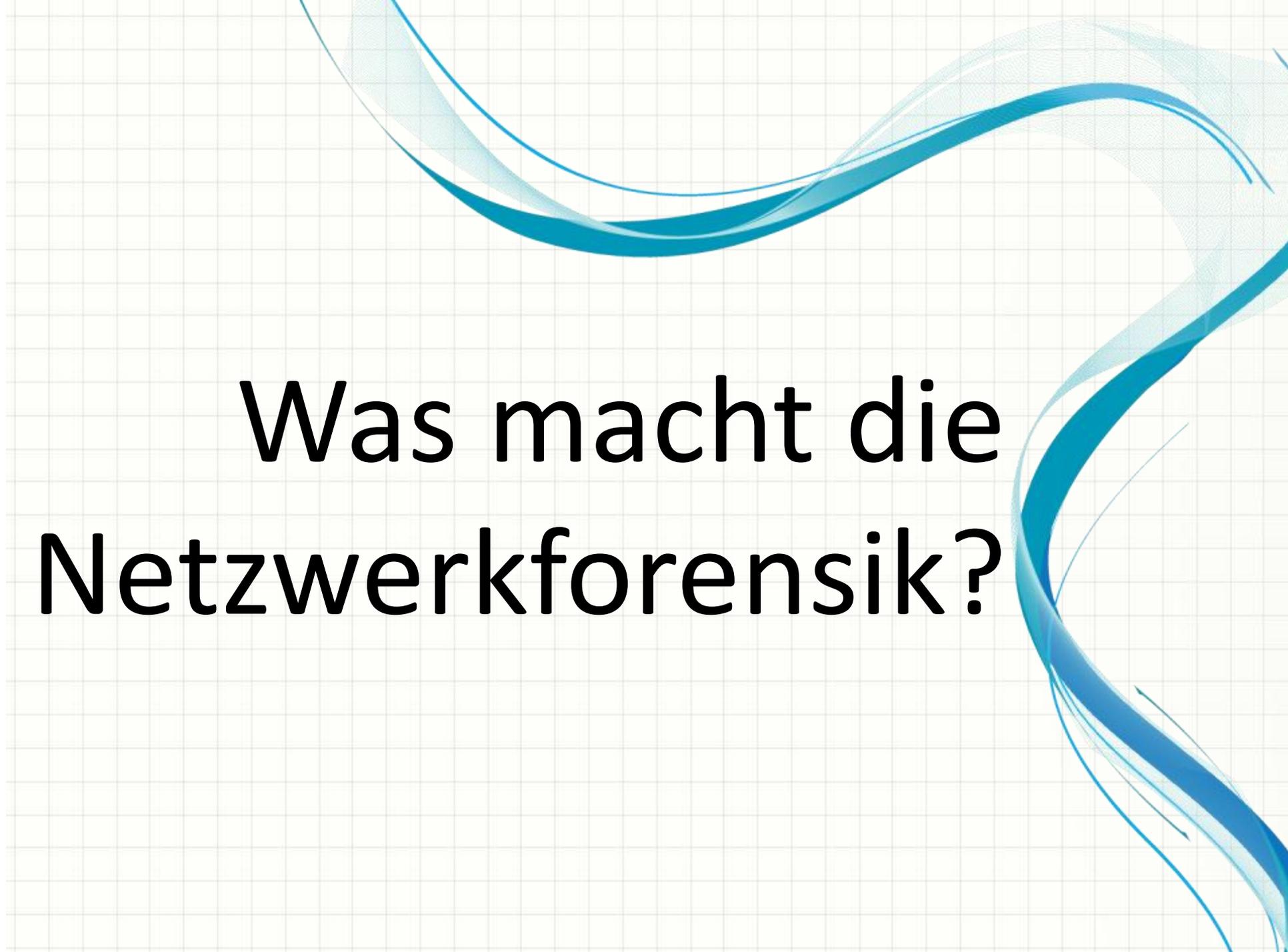


Bekämpfung von Cybercrime im HLKA

- 4 Bereiche für Ermittlungstätigkeiten
 - Cybercrime (IuK-Ermittlung)
 - Internet-Task-Force (inkl. Ansprechstelle: KiPo)
 - Digitale Forensik (forensische IuK)
 - Netzwerk Forensik
- Enge Zusammenarbeit bei Kriminalfällen.
 - Bildung von temporären Ermittlungsgruppen
 - Zusammenarbeit mit der Bekämpfung für organisierte Kriminalität, Wirtschaftskriminalität und anderen Bereichen.

Zum Sachgebiet „Netzwerkforensik“

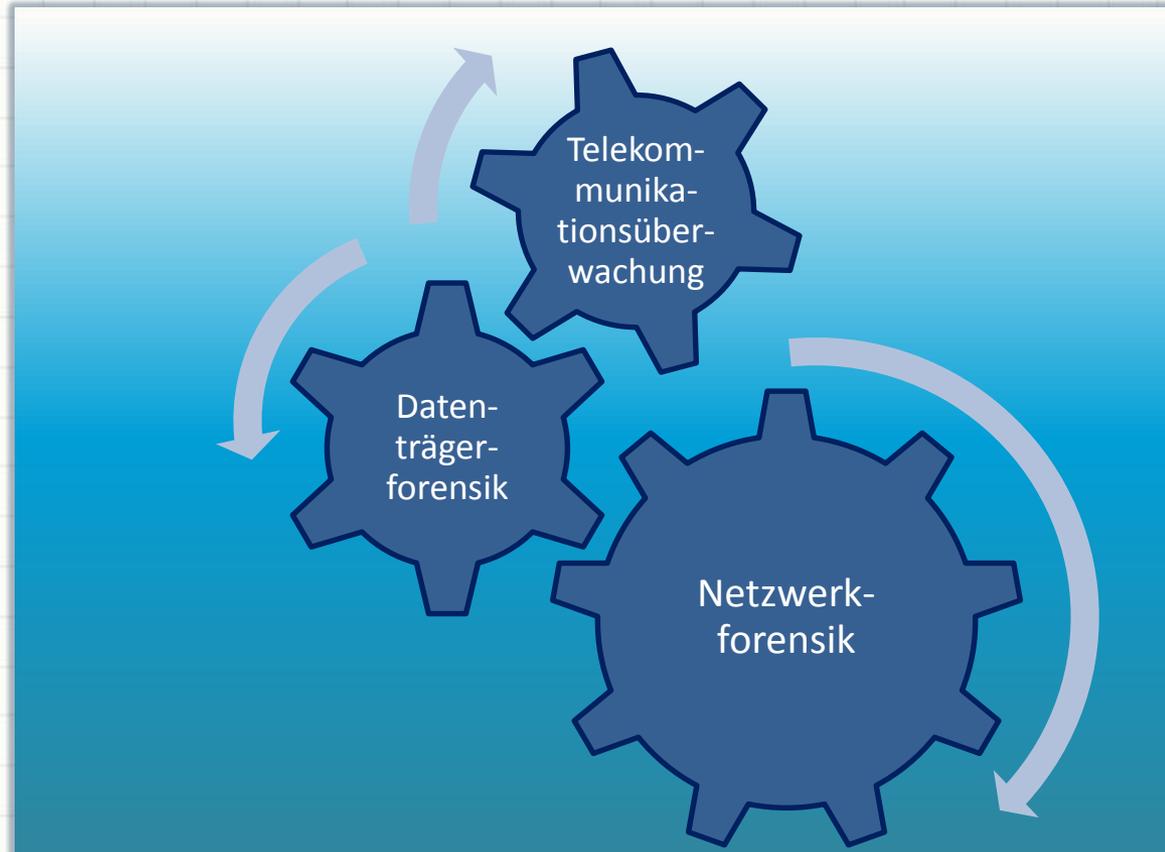
- Neu im HLKA: eingerichtet Anfang 2012
- Aktuell vier Mitarbeiter
 - 1x Chef: Kriminalhauptkommissar
 - 2x Diplom-Informatiker
 - 1x Telekommunikationselektroniker
- Wir sind eine dienstleistende Dienststelle.
 - Nicht selbstständig aktiv.
 - Keine „Internet-Streife“.
 - Zusammenarbeit mit anderen Ermittlungseinheiten

The background features a light gray grid pattern. Overlaid on this are several flowing, wavy lines in shades of blue and cyan. These lines originate from the top left and curve downwards and to the right, eventually exiting the frame on the right side. The lines have a soft, ethereal quality with some transparency and a slight gradient.

**Was macht die
Netzwerkforensik?**

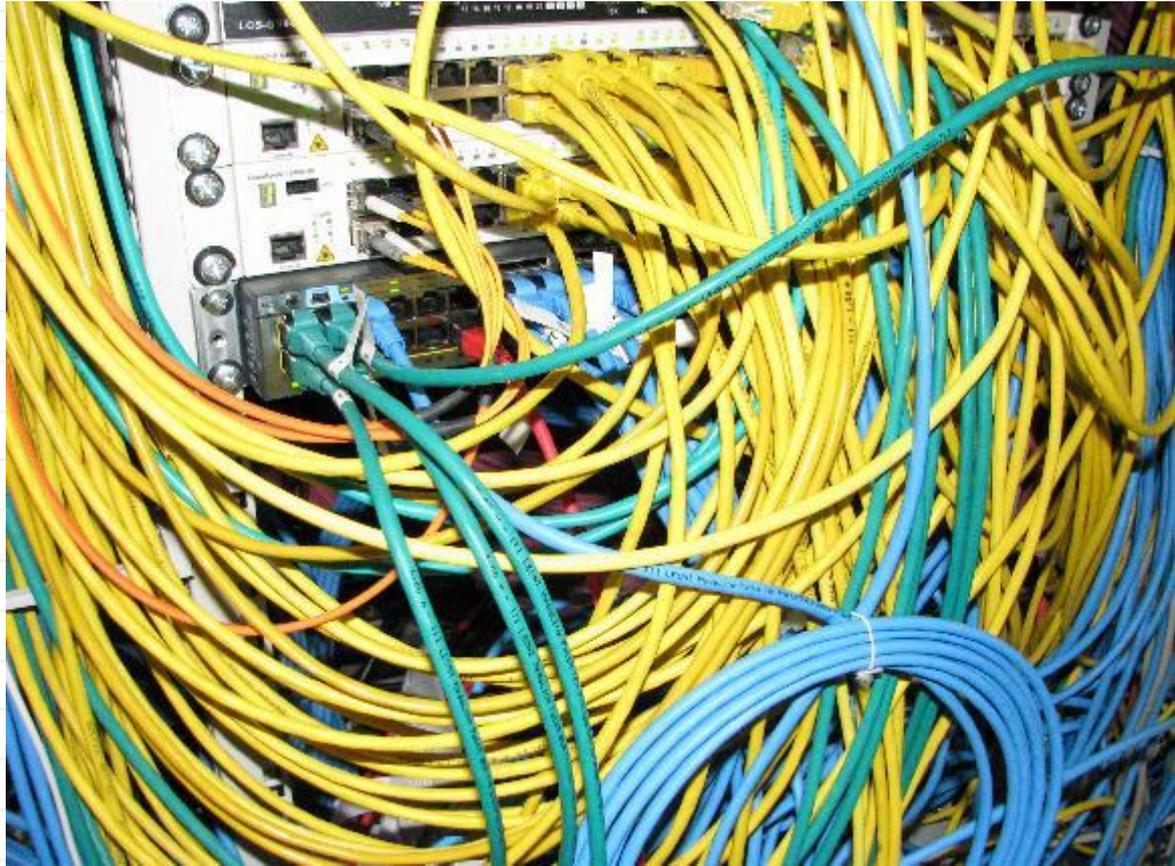
Was macht die Netzwerkforensik?

- Eine Art von erweiterter TKÜ (keine DSL-TKÜ o.ä.)
- Mehrere Schnittpunkte zu anderen Bereichen
- Server-TKÜ
 - Webserver
 - Foren
 - Chats
- Unterstützung
 - Hackingfälle
 - Analyse
 - Datenaufbereitung



Ausleiten von Netzwerkdaten?

- Beispiel: Netzwerkinstallation chaotischer Ordnung
- Rasche Analyse von Installationen für Tapping
- Unterstützung durch lokale Admins.
- Was ist Tapping?
 - Spiegelung der Netzwerkdaten
 - Datenausleitung zum Einsatz-Computer.



Einsatzwerkzeuge: hier ein Tap

- Ein Netzwerk-Tap leitet spurenarm Netzwerkdaten aus
- Beispiel: Eingang A, Ausgang B, Kopie auf C und D
- Taps werden im DVZ direkt am Zielsystem angebracht.
- Oft können die Betreiber die Daten selbst ausleiten.
→ kein Tap



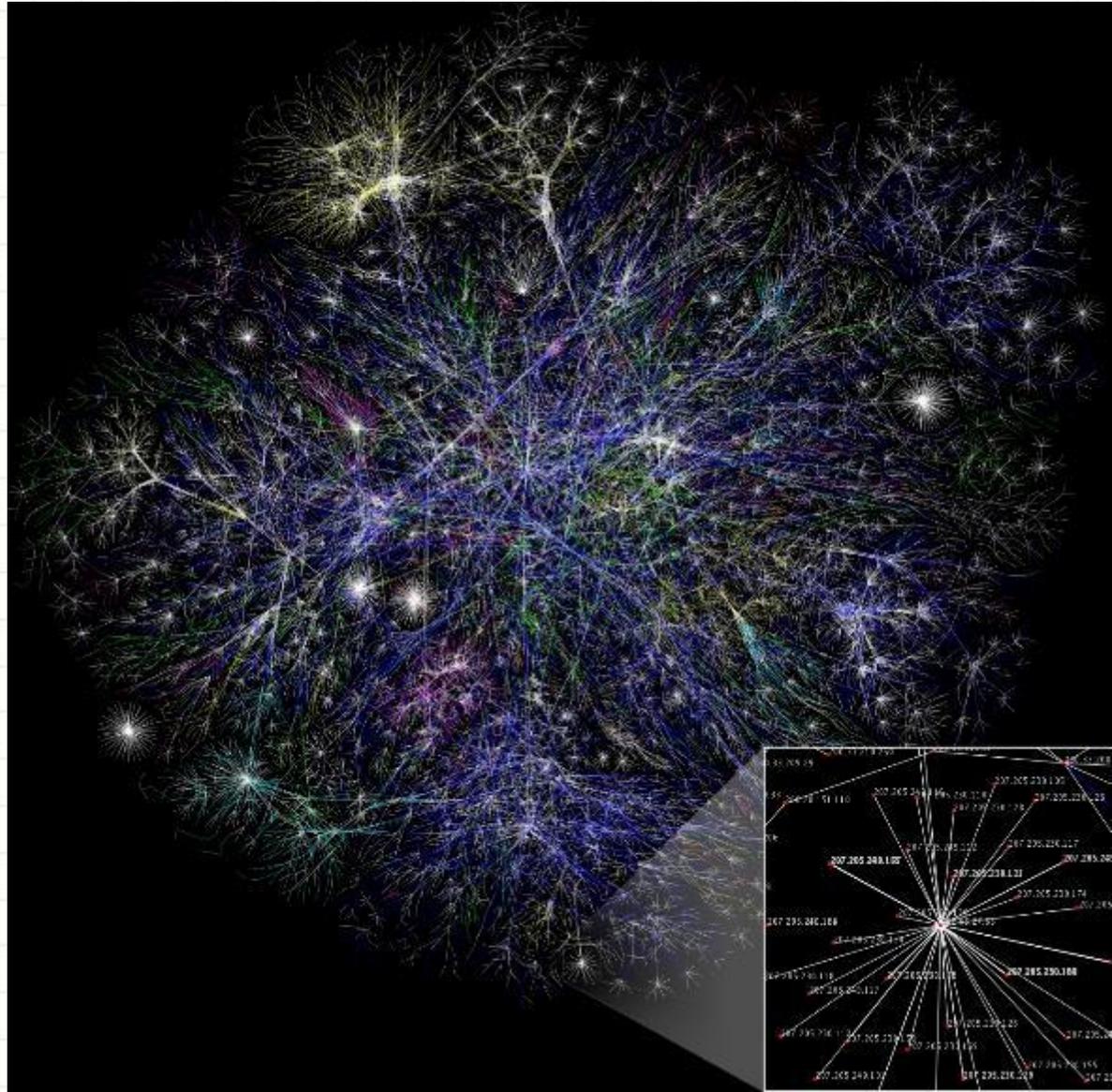
Mobiler Network-Analyser

- Mobiles Analysegerät für Netzwerkdaten
 - Beispiel: Einfache grobe Sichtung der laufenden Netzwerkverbindungen, Test von Kabeln, Bandbreitenmessung.
 - Ist die betroffene IP auf der Leitung zu sehen?
 - Welche Datenfehler sind zu erkennen?
 - Was für Traffic läuft gerade?
 - IPSec, SSL, HTTP, IMAP?



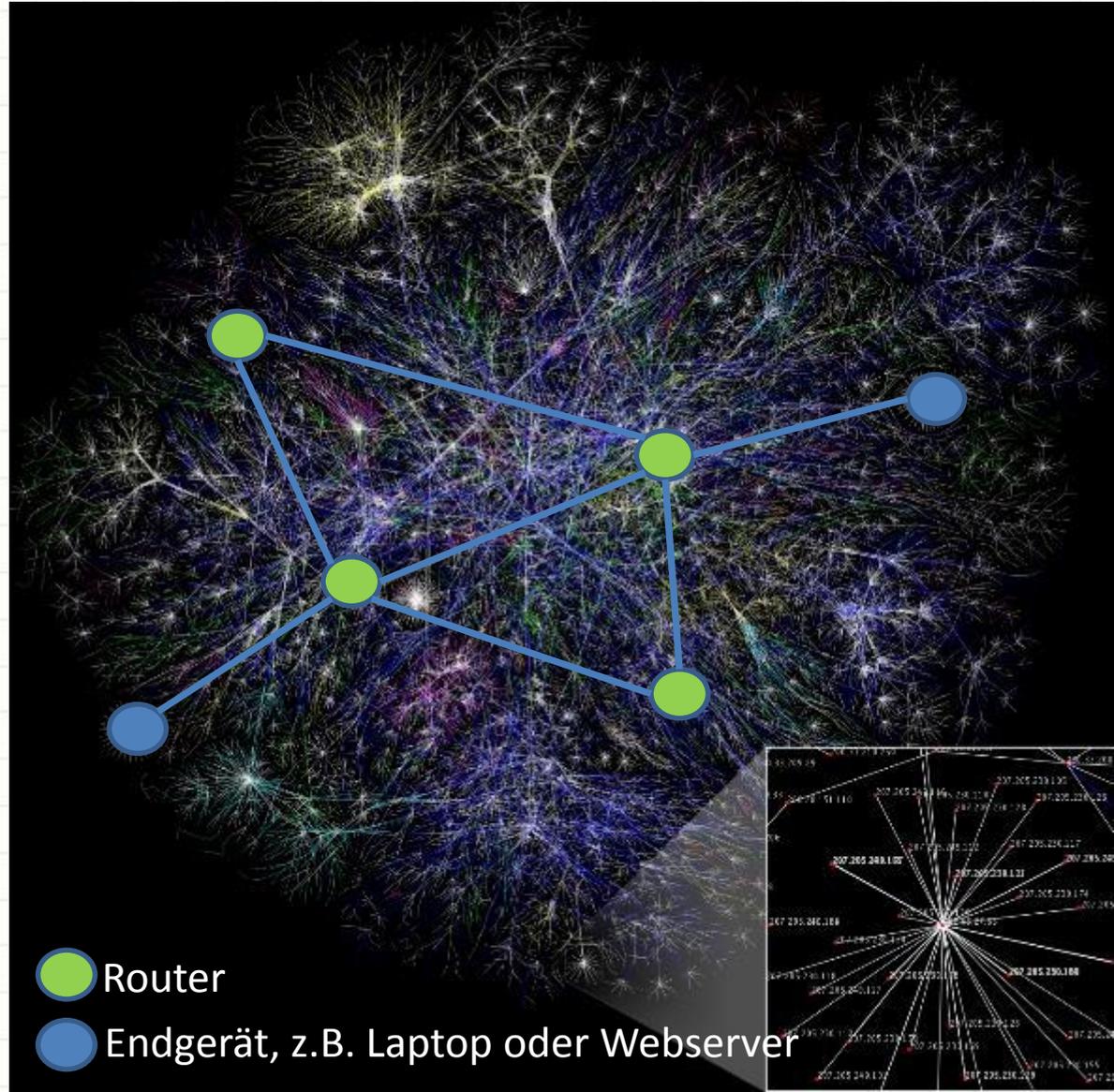
Netzwerkforensik im Internet

- Viele verschiedene Netze unterschiedlicher Art.
- z.B. Glasfaser-, Kupfer-, Funk-, Satelliten-Verbindungen



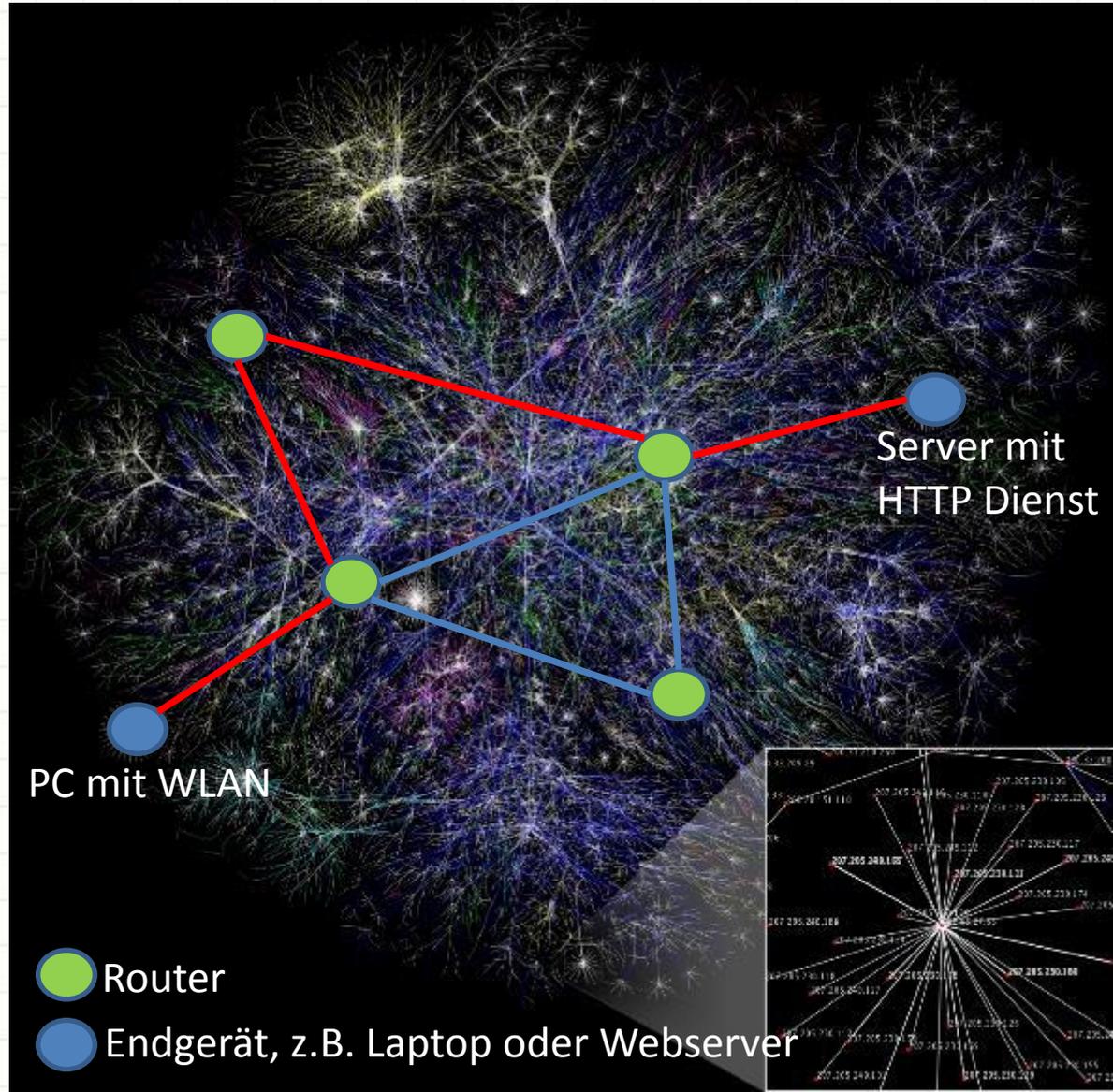
Netzwerkforensik im Internet

- Gespiegelte WAN Daten von Netzwerknoten.
 - Schnell riesige Datenmengen.
- Flowdaten von Routern.



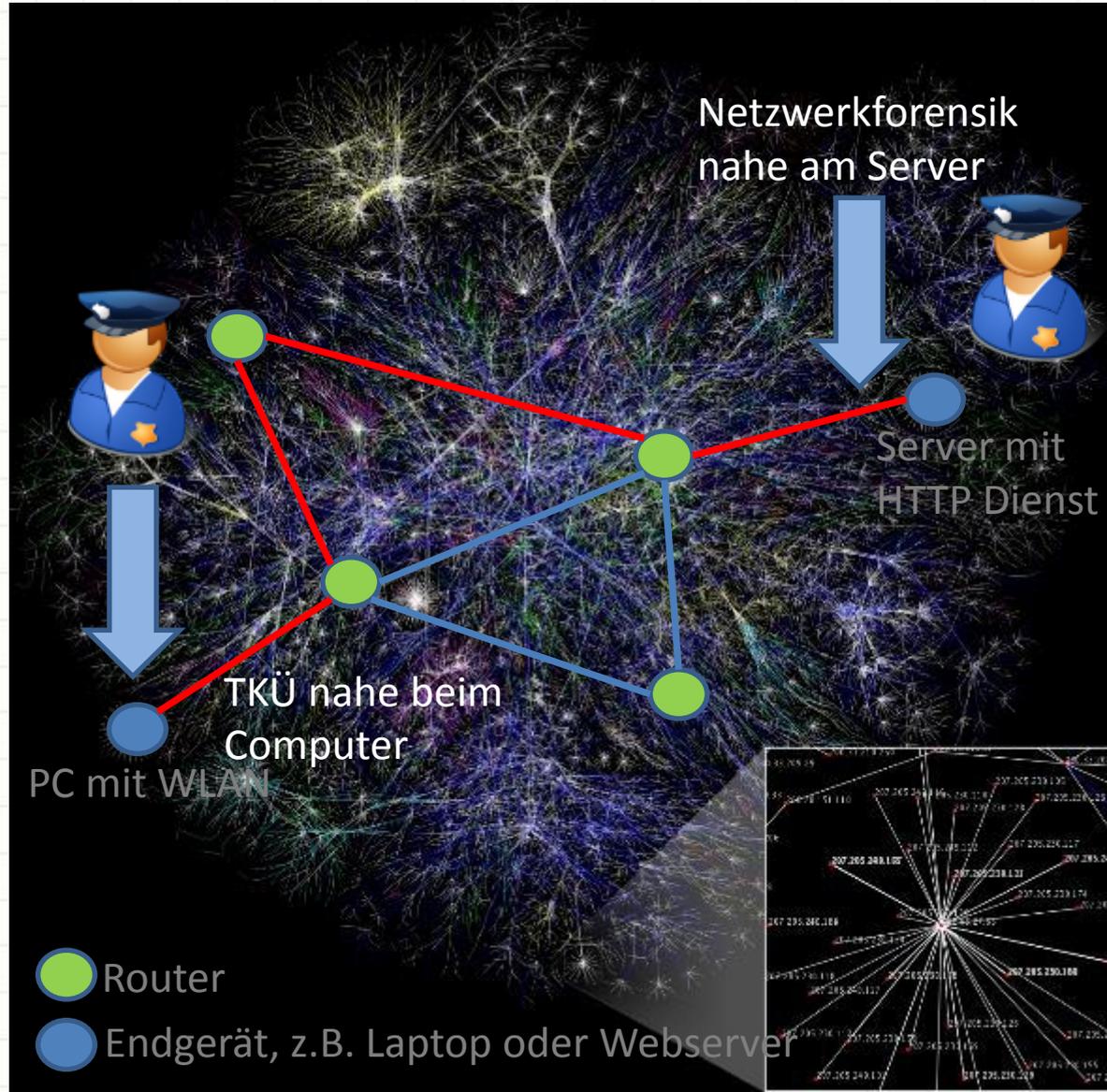
Netzwerkforensik im Internet

- Flowdaten von Routern.
 - Verkehrsdaten ohne Inhalt
 - Größte Mengen ohne Probleme speicherbar.



Netzwerkforensik im Internet

- TKÜ zeichnet möglichst nah an der Person auf.
- NWF zeichnet möglichst nah am Server auf.
 - Server-TKÜ



Mobile Forensik-Computer

- Zum forensischen Spiegeln von Festplatten vor Ort
- Beispiel: Server hat ein RAID 1, Kopie im Betrieb
- Schnelle Kopie von Festplatten
 - Hoher Daten-Durchsatz
 - Bad Blocks?
 - Fehler?
 - Prüfsummen erzeugen.
- Keine Änderung



Speicherabbild mit ColdBootAttack

- Rechner wird kalt neu gestartet, vorhandener RAM kann dann gesichert werden. Nachteil: Auffällig.
- Funktioniert oft. Kein Allheilmittel. Hier nur IA-32.

```
ISOLINUX 3.61 2008-02-03 Copyright (C) 1994-2008 H. Peter Anvin
```

```
-----  
msramdmp - McGrew Security Ram Dumper - v 0.5.1  
http://mcgrewsecurity.com/projects/msramdmp/  
Robert Wesley McGrew: wesley@mcgrewsecurity.com  
-----
```

```
Found msramdmp partition at disk 0x80000000: partition 1  
Partition isn't marked as used. Using it.  
Marked partition as used.
```

```
Writing section from 0x00000000 to 0x0009FFFF  
Writing section from 0x00100000 to 0x3ffff000
```

```
Done! You can turn off the machine and remove your drive.  
boot: _
```

32-Bit
Adressen

Eine detaillierte Vorbereitung für die Ermittler ist notwendig.

Datenträger und Betriebssystem zur Sicherung muss vorher mitgebracht und getestet werden.

Analyse von Speicherabbildern

- Wie war der Zustand des gesicherten Systems?
 - Offene Netzwerkverbindungen?
 - Interne IPs der VPN Verbindung?
 - Historie der Kommandozeile?
 - Cached Hives der Windows-Registry.
- Schadhafte Prozesse im Speicher?
 - Hacking, Rootkit oder Malware-Befall?
- Suche nach kryptografischen Schlüsseln
 - dm-crypt, True-Crypt, Bitlocker, ...
- Suche nach unbekannter Software
 - Binäre Daten eines Prozess extrahieren



Aufbereitung der gesicherten Daten

- Aus forensischen Daten VM Image erzeugen.
 - Für Ermittler leicht zu bedienen.
 - Benutzer können „Klicken“.
 - Alles sieht „normal“ aus, nützlich bei Foren, E-Mails,...
 - Ermittler haben oft keinen detaillierten technischen Hintergrund.
 - → Dokumente, Mails benutzerlesbar extrahieren.
- „E-Mail Überwachung“: Daten indexier- und durchsuchbar auf DVD zuliefern.
 - Ermittler suchen oft Zusammenhänge.
 - E-Mail wird betrachtet wie in einem Mailclient.

The background features a light gray grid pattern. Overlaid on this are several flowing, wavy lines in shades of blue. These lines start from the top left, curve downwards and to the right, then loop back and curve downwards and to the left, ending near the bottom right. The lines have a slight gradient and a soft, ethereal quality, with some overlapping and fading into the background.

Analyse von Netzwerkdaten

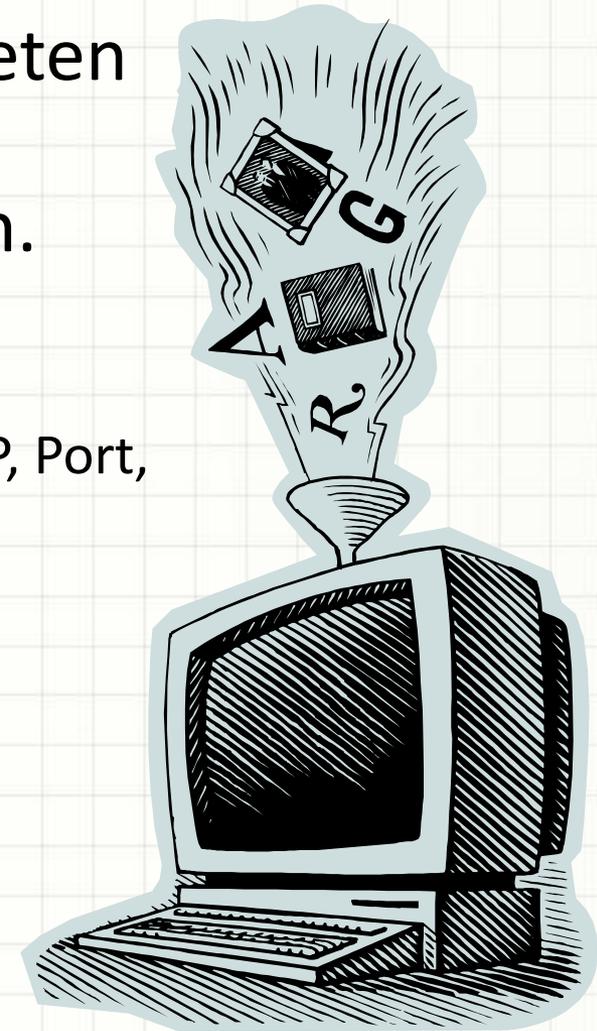
Analyse von Netzwerkdaten

- Es fallen schnell riesige Datenmengen an.
 - Verarbeitungsproblem
 - → begrenzte Kapazität
 - Speicherplatz begrenzt
 - Rechenleistung begrenzt
 - Grenzen von Software
- Lösung: „Intelligente Datenreduktion“
 - Gezieltes Aufzeichnen → Live-Filter
 - Flow-Daten aufzeichnen
 - Speichern der Inhaltsdaten nach Bedarf



Die Nadel im Datenhaufen

- In vielen unwichtigen Datenpaketen müssen die wenigen wichtigen Pakete herausgearbeitet werden.
 - Flowdaten: Keine Inhaltsdaten, sehr lastarm.
 - Verkehrsdaten vorhanden, wie IP, Port, Protokoll, etc.
- Beispiel: Flowdaten
 - Kommunikation betrachten
 - Daten eingrenzen
 - Filter erzeugen
- Aufzeichnung „durchsieben“.



Kurze Analyse eines Webaufrufs

- Datenmitschnitt von einer knappen Minute
- Aufruf der Webseite www.welt.de
- Analyse der Aufrufe durch den Browser.

Beispiel:	Zeit (s)	Pakete	Größe (MB)
	78	4.076	2
1 Stunde	3.600	188.365	94
2 Stunden	7.200	376.729	188
12 Stunden	43.200	2.260.375	1.126
24 Stunden	86.400	4.520.750	2.252
48 Stunden	172.800	9.041.499	4.503
1 Monat	2.592.000	135.622.490	67.545
3 Monate	7.776.000	406.867.471	202.635

Analyse mit Wireshark

- DNS Aufrufe aus Datenstrom filtern.

The screenshot shows the Wireshark interface with the following elements:

- Filter:** A red box highlights the filter expression `dns matches www.welt.de`. A blue arrow points to it with the text "Filter auf Netzdaten."
- Packet List:** A table of captured packets. Row 509 is highlighted in black. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** The selected packet (No. 509) is expanded to show the "Queries" section. A red box highlights the "Name: www.welt.de" field. A blue arrow points to it with the text "Suchwort auf Metaebene".
- Packet Bytes:** The raw bytes of the packet are shown at the bottom. A red box highlights the ASCII representation of the domain name: `.....w ww.welt.de.....`. A blue arrow points to it with the text "Suchwort auf Bitebene".
- Annotations:** A blue box on the right contains the text: "Filter auf die DNS Einträge die www.welt.de beinhalten. DNS ist ähnlich eines Telefonbuchs. Auflösung des Namens zu einer IP Adresse." Below this, two green boxes are labeled "Metaebene" and "Bitebene".

Analyse mit Wireshark

- DNS Aufrufe auf „Facebook“ ausfiltern.

Filter: `dns matches facebook.com`

Filter auf Netzdaten.

Suchwort auf Metaebene

Der Aufruf einer Webseite ruft weiter vielerlei von anderen Seiten auf, bzw. lädt Inhalte von anderen Seiten nach.

Stichwort: „Gefällt mir“, „Werbung“, „Drive-By“, ...

Suchwort auf Bitebene

Metaebene

Bitebene

No.	Time	Source	Destination	Protocol
684	8.665330	192.168.137.57	192.168.137.1	DNS
688	8.670731	192.168.137.57	192.168.137.1	DNS
690	8.678983	192.168.137.57	192.168.137.1	DNS
692	8.680984	192.168.137.57	192.168.137.1	DNS
697	8.693331	192.168.137.57	192.168.137.1	DNS
702	8.707070	192.168.137.1	192.168.137.57	DNS
719	8.716000	192.168.137.1	192.168.137.57	DNS
730	8.721900	192.168.137.1	192.168.137.57	DNS
734	8.728400	192.168.137.1	192.168.137.57	DNS
736	8.729400	192.168.137.1	192.168.137.57	DNS
742	8.730800	192.168.137.1	192.168.137.57	DNS

```
Queries
  www.facebook.com: type A      class IN
  Name: www.facebook.com
  type: A (Host address)
  Class: IN (0x0001)
```

```
0000 00 23 14 93 e3 75 60 45 bd f1 5e 74 08 00 45 00  .#. .u^E ..^T..E.
0010 00 3e 7b 0d 00 00 80 11 00 00 c0 a8 89 39 c0 a8  .>{.....9..
0020 89 01 e7 74 00 35 00 2a 34 af 59 b5 01 00 00 01  t5*4Y
0030 00 00 00 00 00 00 03 77 77 77 08 66 61 63 65 62  .....w ww.Faceb
0040 6f 6f 6b 03 63 6f 6d 00 00 01 00 01  .ook.com. ....
```

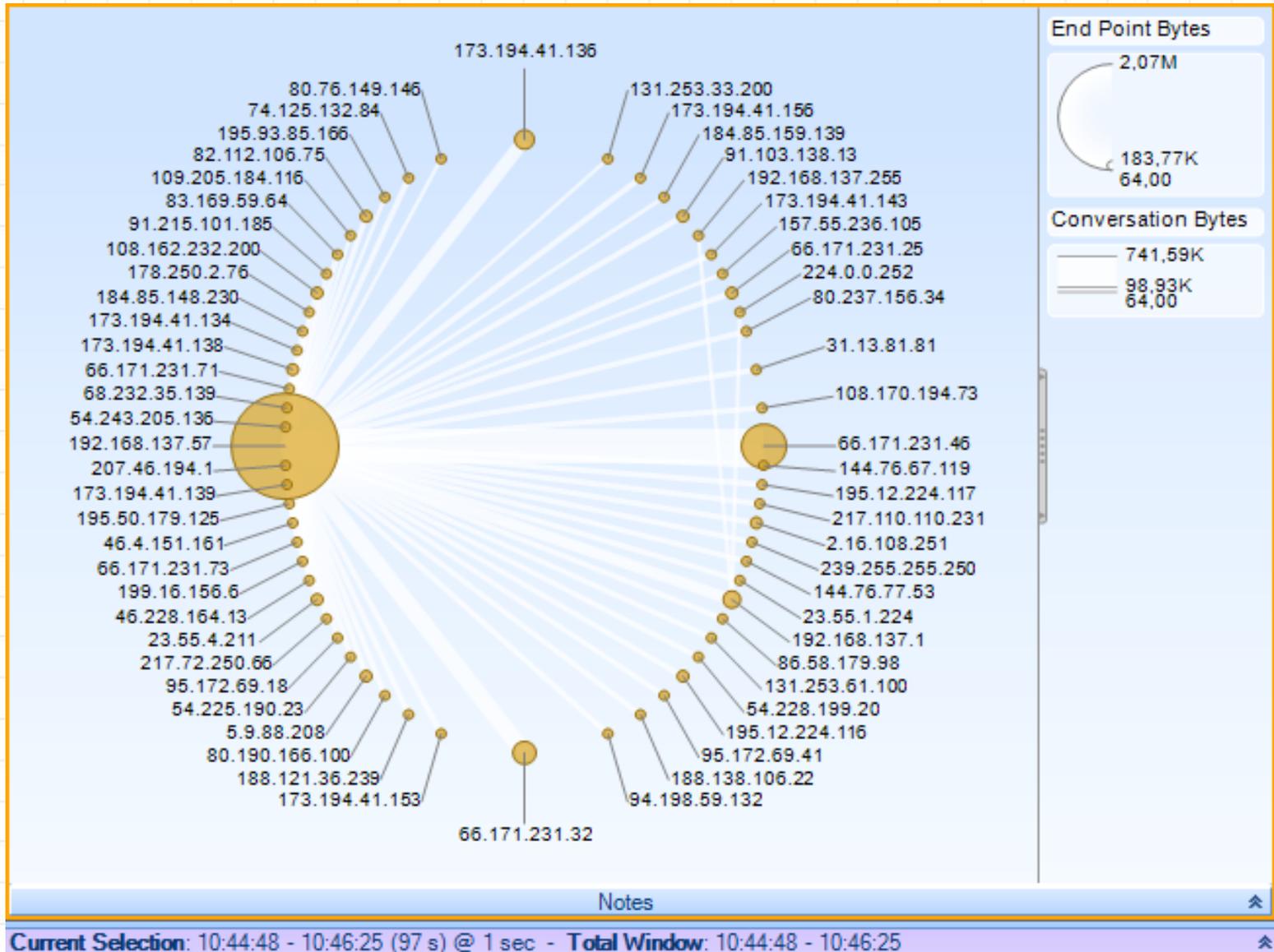


Analyse von Netzwerkdaten mit Cascade Pilot

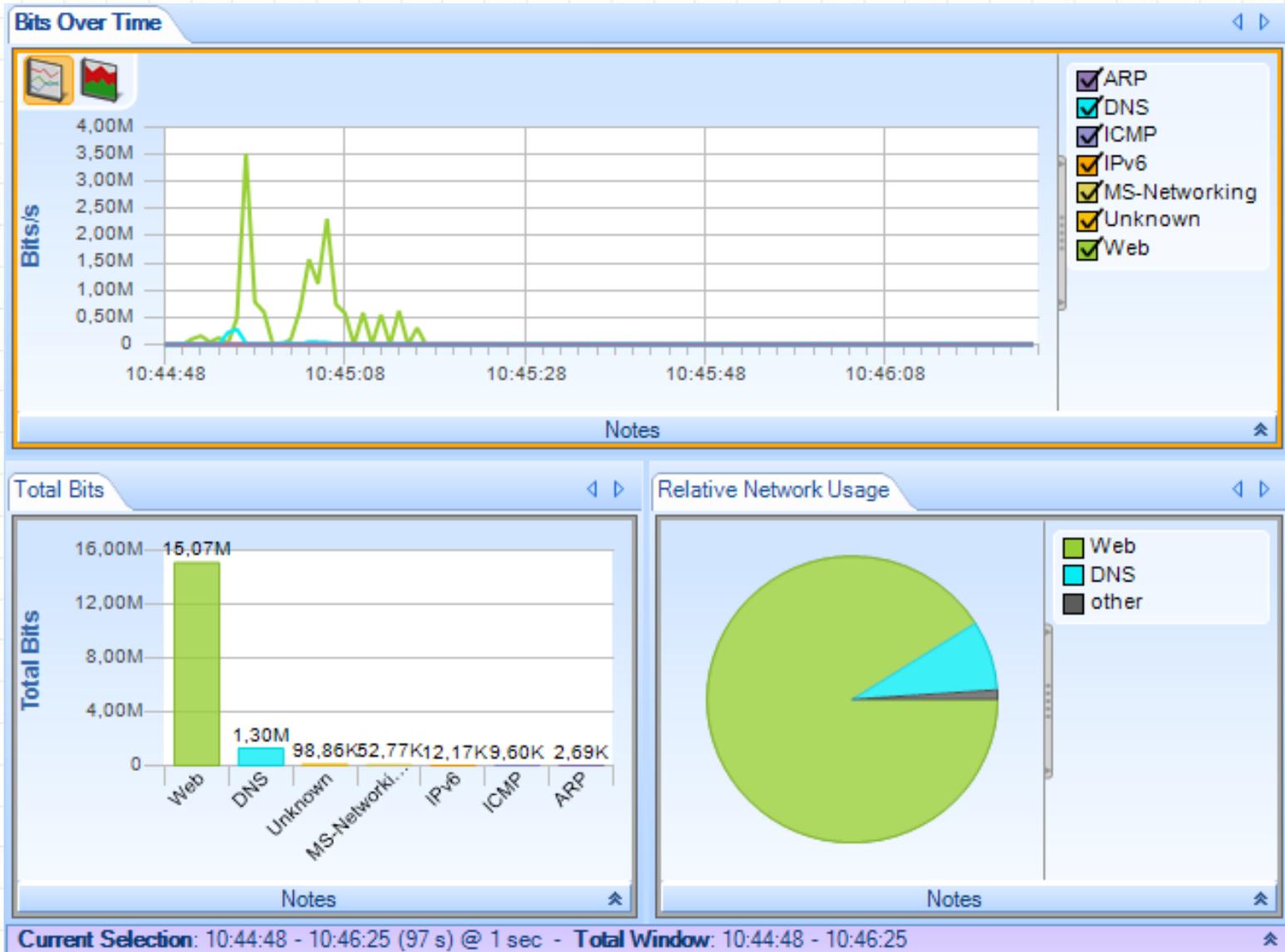
Nutzung automatischer Tools

- Die Analyse über eine grafische Metaebene von gespeichertem Netzwerkverkehr erleichtert die Auswertung.
 - Drop-Down-To-Funktion
 - Automatisches Eingrenzen von Daten (Filter)
 - Hervorheben von Verbindungen
 - Auffälligkeiten sind so z.T. leichter zu erfassen.
- Ergebnisse können Ermittlern leicht aufbereitet werden.

IP Konversationen im Überblick



Timeline, Übertragungen in MBit



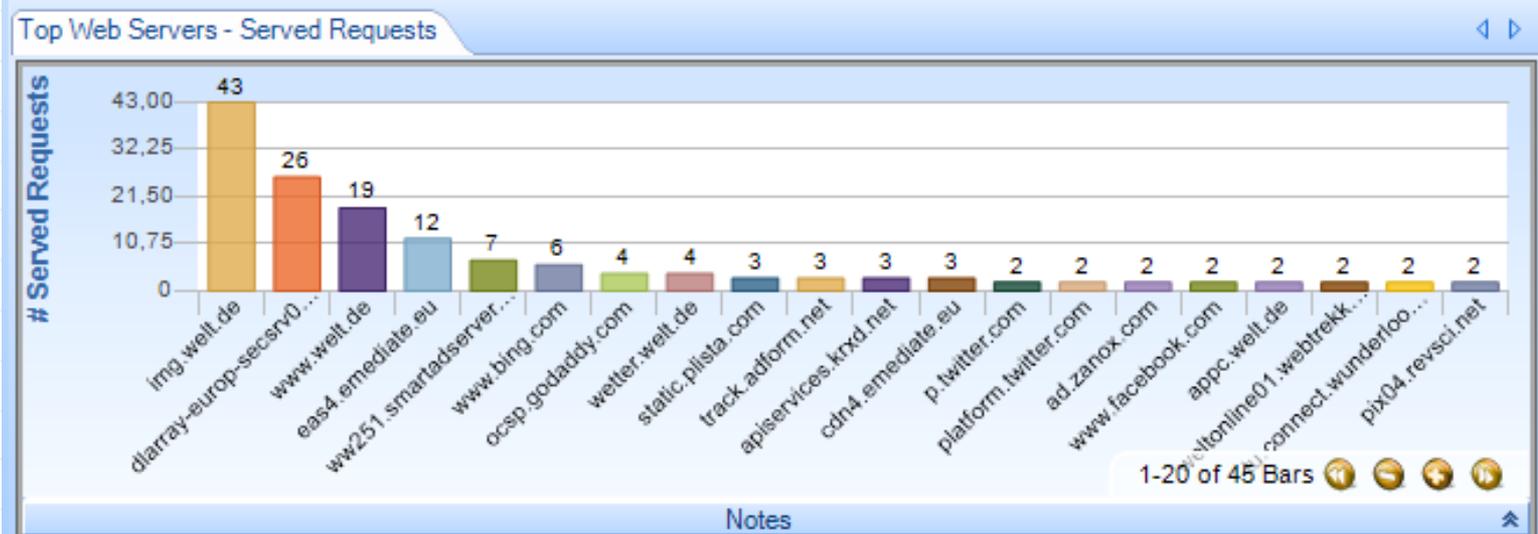
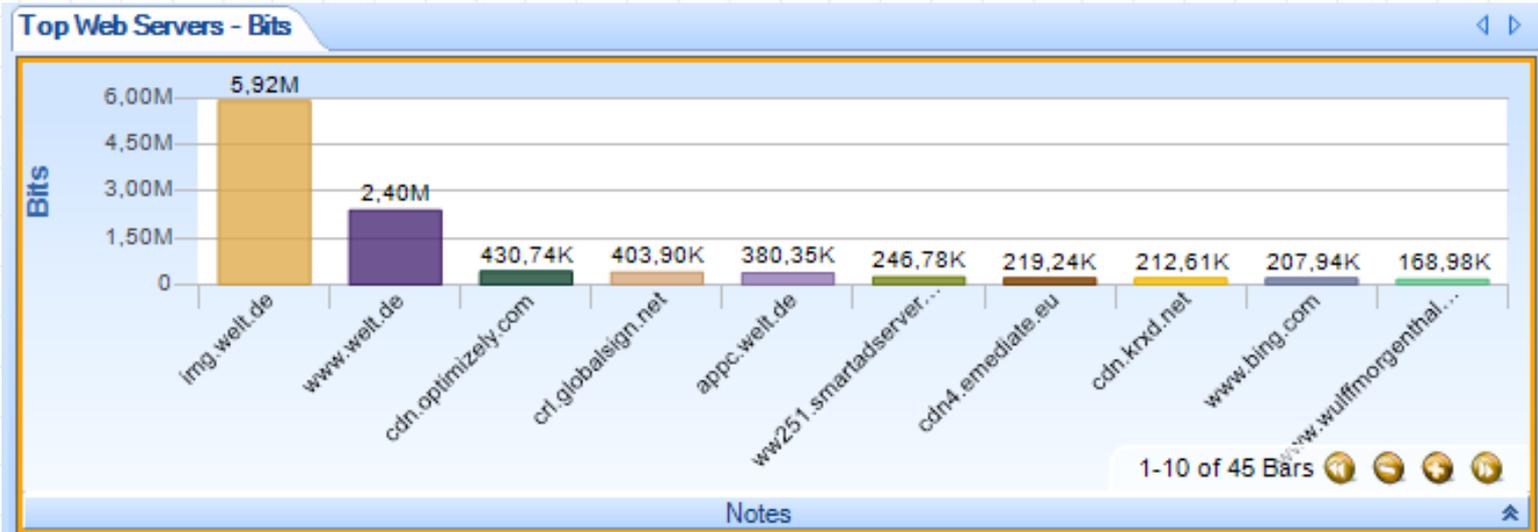
Laufende Netzwerkprotokolle?



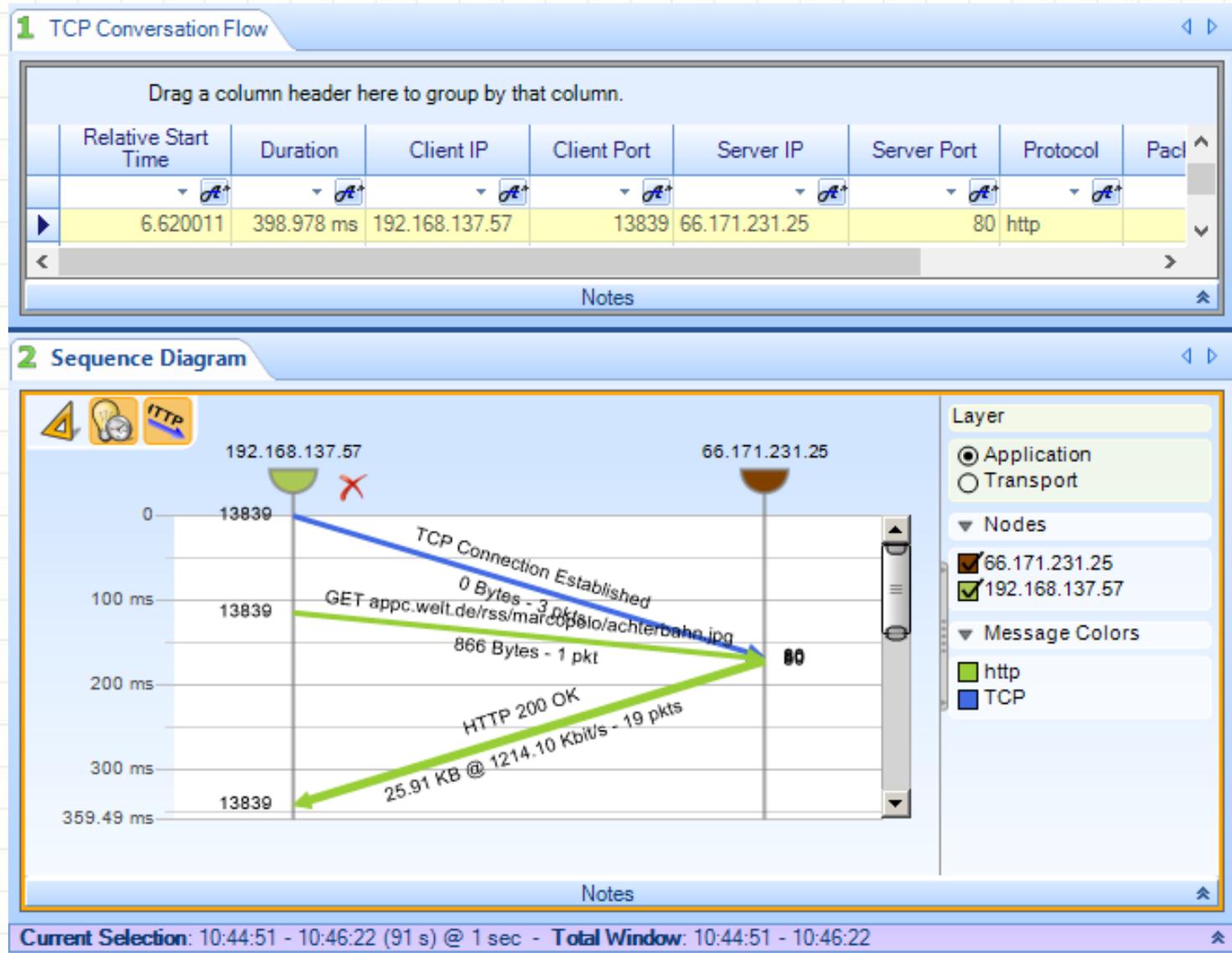
Intensivster TCP und UDP Traffic



Rangliste der Web-Server Aufrufe?



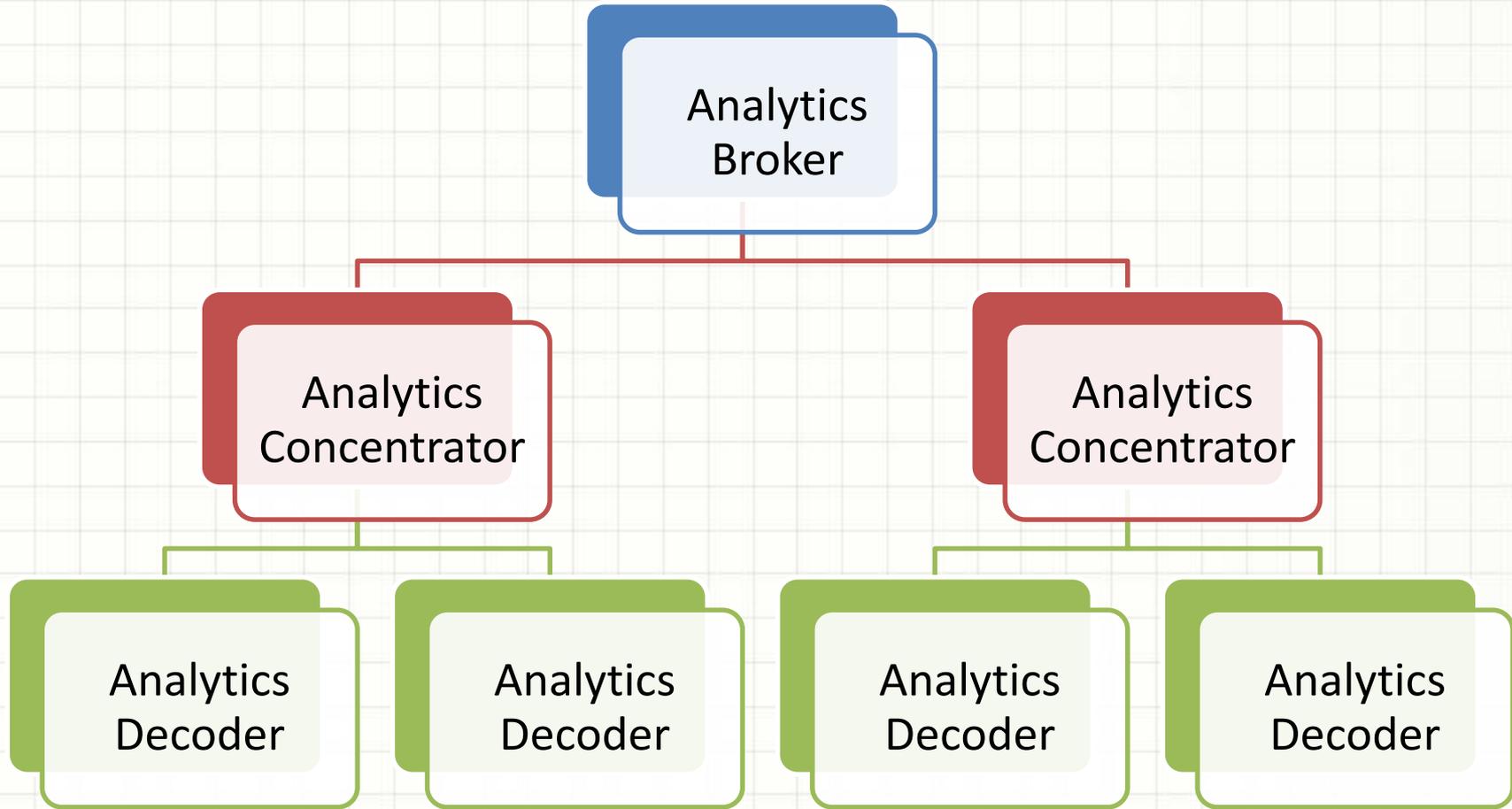
Sequenzdiagramme erzeugen



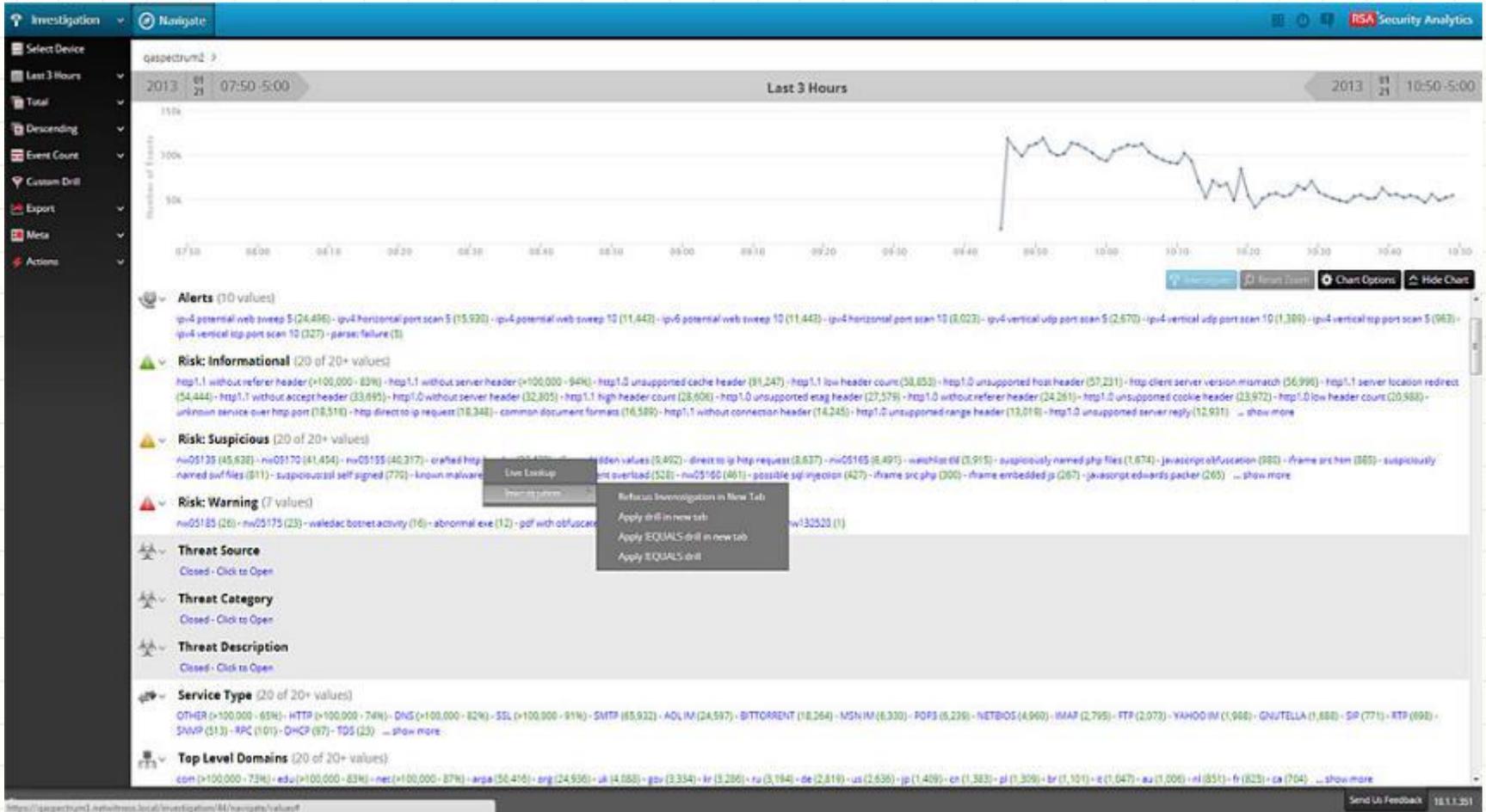
Nutzen von Analyse Appliance

- RSA Security Analytics Server
 - Komplettsystem zur Trafficanalyse
 - Sehr leistungsfähig (auch große Datenmengen)
 - Teuer: >120000 €
- Mehr-Tier Architektur
 - Metadaten werden in Datenbanken gehalten
 - Ermöglicht schnelleres Suchen,
 - Mehrere Rechner mit jeweiligen Datenbanken
 - Concentrator „sammeln“ Daten von den Maschinen ein.

Struktur der Analyse Appliance



Bedienung über Browserinterface



Fazit

- Netzwerkforensik macht keine klassische TKÜ.
- Viele Schnittpunkte mit anderen Bereichen.
- Telekommunikationsüberwachung
 - TKÜ → TKÜ-Anlage
- Netzwerkforensik (Server-TKÜ)
 - STKÜ → Analyse-Computer vor Ort im DVZ.
 - individuelle Hardware,
 - spezielle Software, Netzwerktaps,
 - selbstgebaute Linux-Rechner mit Open-Source Software.

HESSEN



Vielen Dank.

andreas.frantzen@outlook.com