GTEN

Intelligence *for a better world*

GTEN AG

Volker Mogk-Hohenleitner

Präventionstag 18.05.2004

Ein Weg zu mehr Vertrauen in das Internet

GTEN ist anerkannter Partner für Carrier, Provider und Ermittlungsbehörden im Bereich Netzüberwachung zur Strafverfolgung.

Damit können wir gemeinsam mit unseren Kunden einen Beitrag zur weltweiten Verbrechensbekämpfung im Internet leisten und mithin mehr Vertrauen in dieses Medium generieren!

GTEN®
Intelligence for a better world

GTEN AG - Historie

GTEN verfügt über nahezu 20 Jahre Erfahrung

auf dem Gebiet der Daten- und Protokollanalyse

- 1986 Gründung der DATAKOM GmbH
- 1997 Start der Entwicklung der G10 Technologie
  Viele Gespräche mit RegTP, BMWi, BKA, LKAs und Netzbetreibern
- **2000/2001 Gründung der GTEN AG**
- Heute: ca. 20 feste und ebenso viele freie Mitarbeiter in München und Bremen

Notwendigkeit von Datenüberwachung (I)

- Paradigmenwechsel von Sprache zu Daten als globaler Trend in der Telekommunikation
- Prävention von Schwerkriminalität
  - Terrorakte u.a. über das Internet vorbereitet:

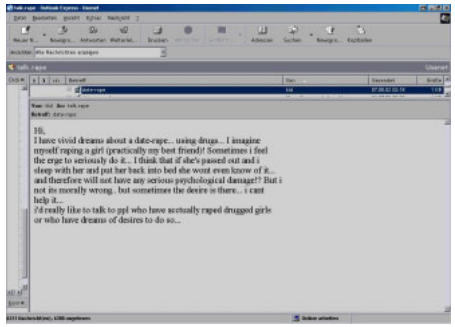
New York, 11.Sept. 2001

Madrid, 11.März 2004

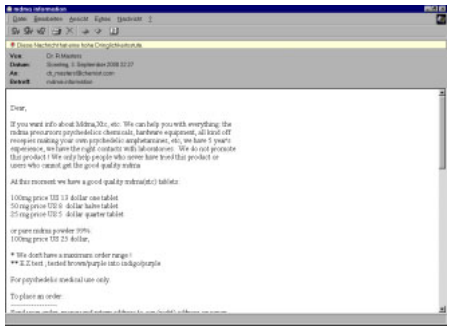
Notwendigkeit von Datenüberwachung (II)

- Medien zur Vorbereitung von Verbrechen

✓ Internet Chat



✓ e-Mail



✓ Web-based instructions

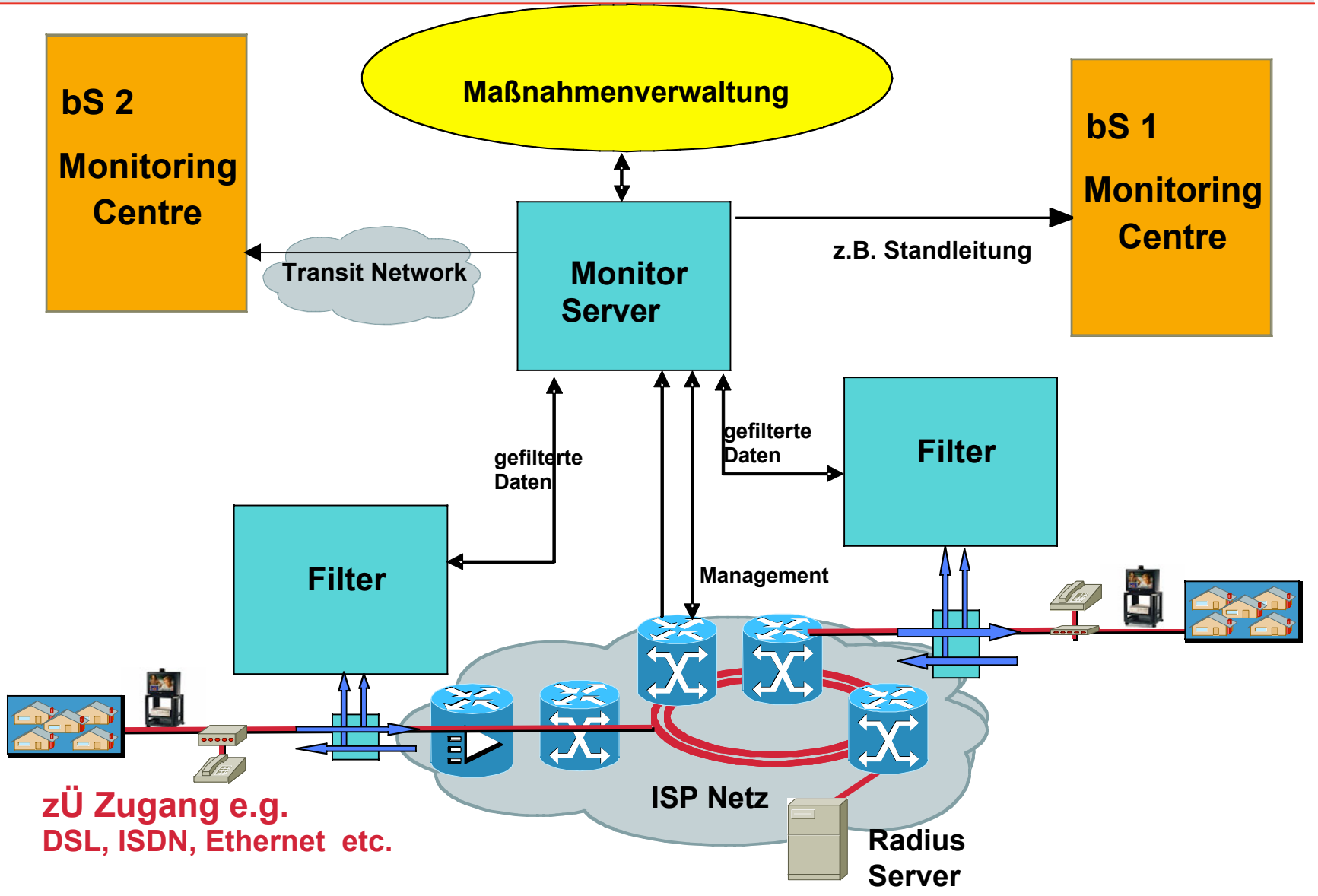
Anforderungen

- Gesetzliche Bestimmungen
  a) Vollständige Ausleitung einer Kopie der Daten des züA
  b) Datenschutz der übrigen Teilnehmer
  c) Gesichertes Transitnetzwerk zur bS
- Technische Herausforderungen
  a) Transparentes, passives Auskoppeln aus unterschiedlichen Netzen
  b) Kein negativer Einfluss auf Zuverlässigkeit, Verfügbarkeit und Performance
  c) Gesicherte Schnittstelle zur bS
- Kommerzielle Kriterien
  a) Kosten Effizienz
  b) Migrationspfad
  c) Investitionsschutz

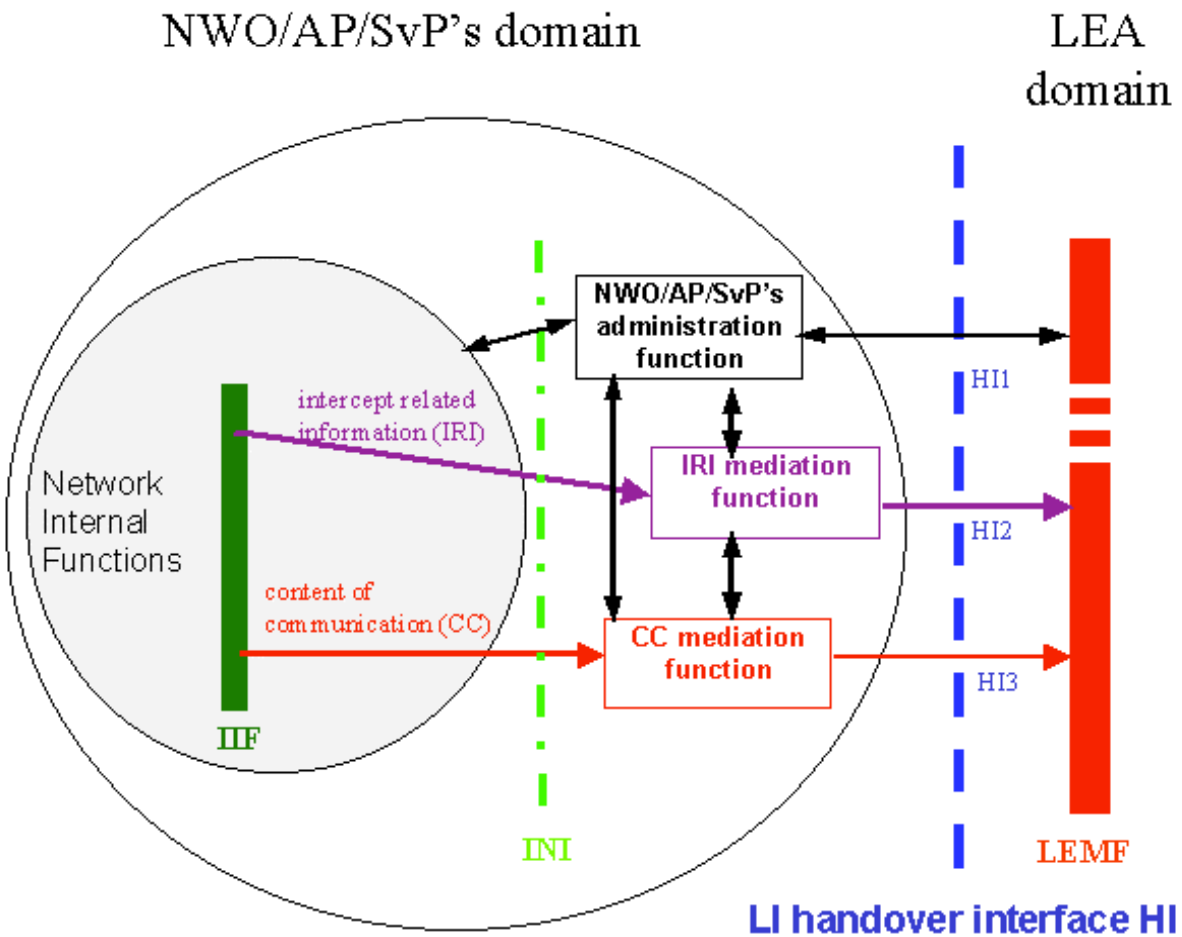
Datenüberwachung braucht Datenschutz!

- Durchführen von Maßnahmen
  - nur durch sicherheitsüberprüftes Personal
  - nach richterlicher Anordnung
- Ausleitung ist für überwachten Teilnehmer nicht sichtbar
- Filterkriterien
  - stellen sicher, dass nur relevante Daten ausgeleitet werden.
  - Nicht relevante Daten werden nicht gespeichert und verworfen.
  - Schutz des unbescholtenen Teilnehmers wird gewahrt
- Sicherheitsvorschriften
  - Damit die ausgeleiteten Daten nicht in unbefugte Hände gelangen
  - Damit die ausgeleiteten Daten nicht manipuliert werden können

Internetüberwachung



ETSI Handover Interface Konzept



IIF: internal interception function
INI: internal network interface

HI1: administrative information
HI2: intercept related information
HI3: content of communication

GTEN Lösungen im Überblick

Front-End-Lösungen

- Front-End Lösungen bieten um-fassende Möglichkeiten, die Kommu-nikation einzelner Kunden eines Netzbetreibers gesetzeskonform zu überwachen
- Unabhängig vom zugrunde liegenden Protokoll wird eine Kopie der Daten-Kommunikation angefertigt und real-time an die berechtigte Stelle zur weiteren Auswertung übertragen
- Die Lösungen können entweder als permanent installierte Systeme oder alternativ als Service Option von GTEN zum Einsatz kommen

Back-End-Lösungen

- Back-End Lösungen empfangen die auf Front-End Seite ausgeleiteten Daten über einen richterlich angeordneten Zeitraum
- Der emfangene Datenstrom wird rekonstruiert und dem Ermittler als exakte Kopie der genutzten Medien (Internet, Mail, Chat etc.) dargestellt.
- Um die so gewonnen Erkenntnisse gerichtlich verwerten zu können, muss die Integrität der empfangenen Daten gewährleistet sein

Back-End Lösungen – Übersicht

- Monitoring Center
  - Kombiniertes Sprach-, Fax-, Modem- und IP-Daten Monitoring Center
  - POSEIDON zeichnet IP Daten auf und rekonstruiert diese
  - POSEIDON Mobil für Ausleitung, Aufzeichnung und Rekonstruktion von IP-Daten direkt, mobil in jedem Netz

GTEN Back-End Produkte – Übersicht

POSEIDON

Sprache/Fax/Modem/
Daten Monitoring Center

POSEIDON Mobil

GTEN Back-End Produkte (I)

Monitoring Center

[Einsatz]

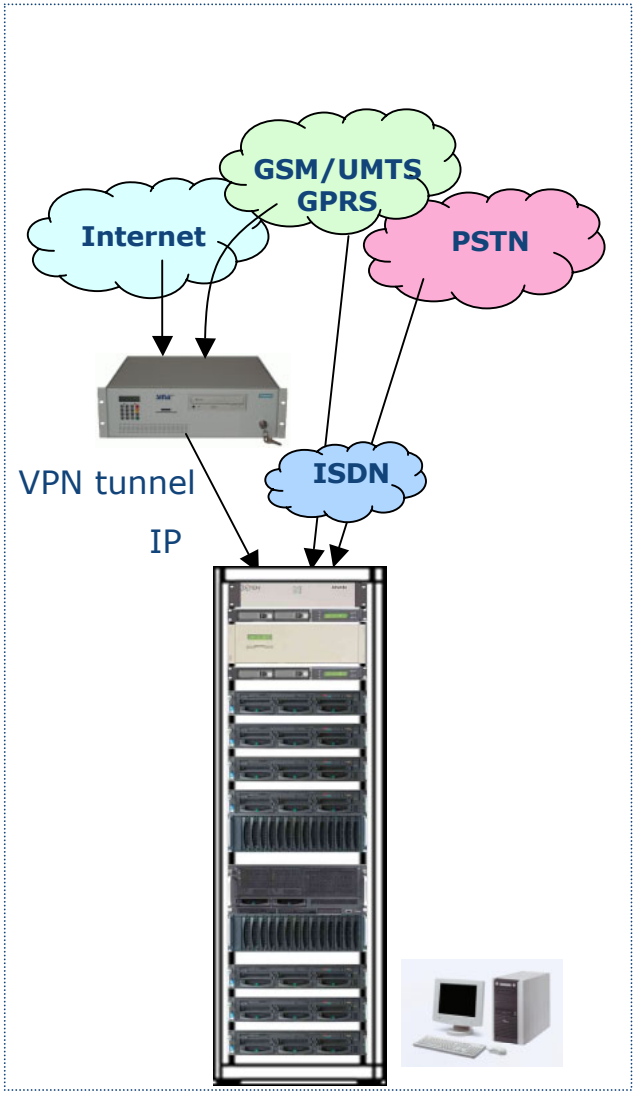
- Aufzeichnung, Decodierung, Archivierung und Evaluation aller Arten von Kommunikationsdaten (Sprache, Fax, Modem, IP)

[Features]

- Interfaces:
  - große Anzahl unterschiedlicher Hersteller (Siemens, Ericsson, Motorola ...)
- Dekodierung / Demodulation
  - IP-Daten: HTML, Chat, eMail, FTP, Telnet, VoIP, AOL, IRC, AIM, NNTP, ...
  - G3-Faxe
  - Breite Palette von Modems

[Option]

- GIS – Geographisches Informationssystem (Ortsdaten von mobilen Nutzern von GSM / UMTS)



GTEN Back-End Produkte (II)

POSEIDON

IP-Daten Aufzeichnung und Rekonstruktion

[Einsatz]

- Aufzeichnung des IP Datenverkehrs
- Rekonstruktion von IP-Daten wie HTML, Email, WebMail, Chat, Telnet, FTP, VoIP, etc.
- Komplettes **I**nternet **M**onitoring **S**ystem für beliebige Transportnetze und Fileserver

[Features]

- sammelt, zeichnet auf und analysiert IP-Daten die über verschiedenen Netzwerke transportiert werden
- Evaluation von IP-Daten via LAN mit MS Internet Explorer auf einem Notebook/PC
- Alarm bzgl. verschiedener Aufzeichnungsereignisse
- Möglichkeit IP-Daten vor oder nach der Aufzeichnung zu filtern
- Statistische Zusammenfassung aller aufgezeichneten IP-Daten
- Passwortschutz und Logfiles bieten ein Maximum an Sicherheit und Datenintegrität

...und das Problem der reisenden Straftäter..

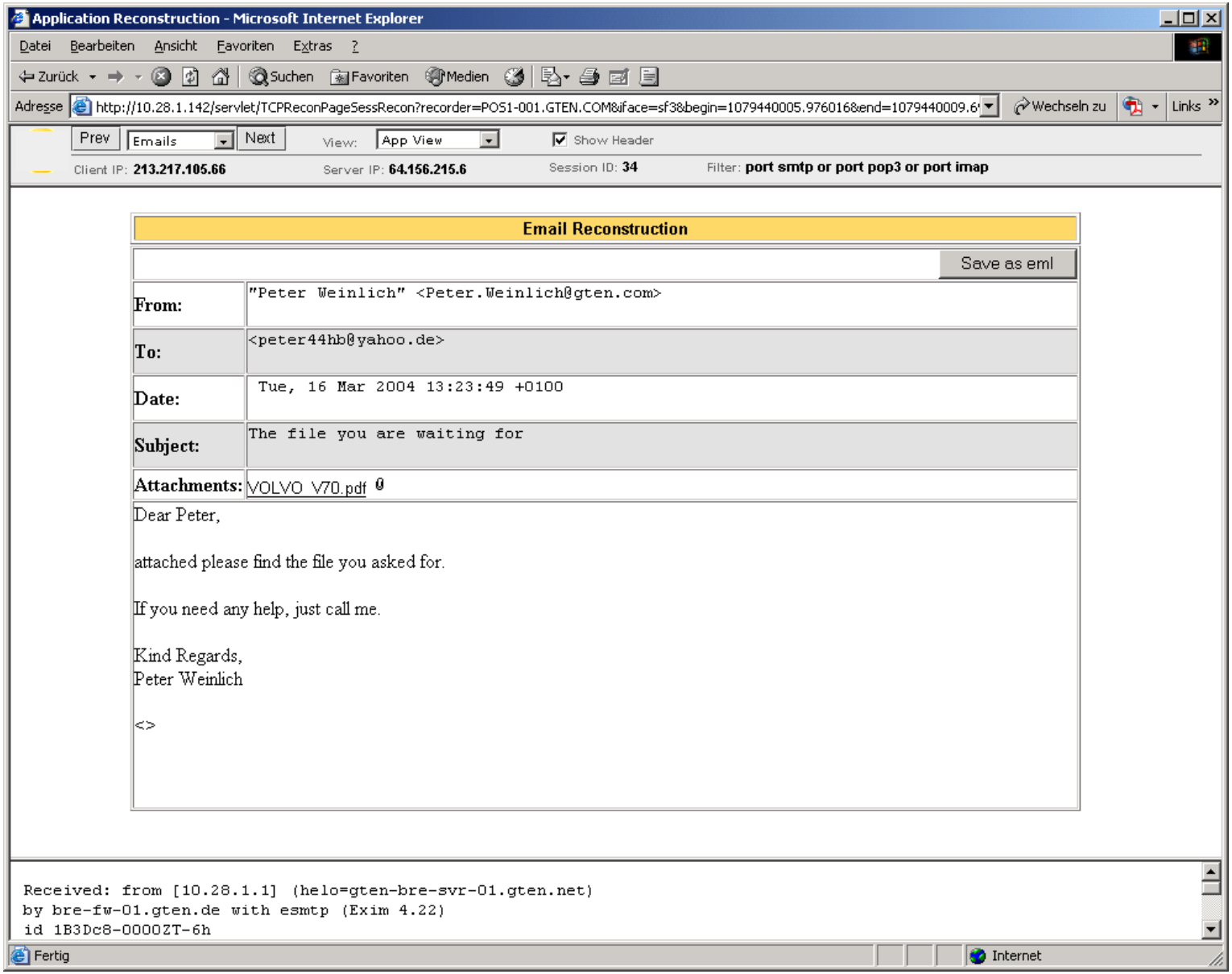
POSEIDON Mobil

IP-Daten Aufzeichnung und Rekonstruktion für mobile Anwendung

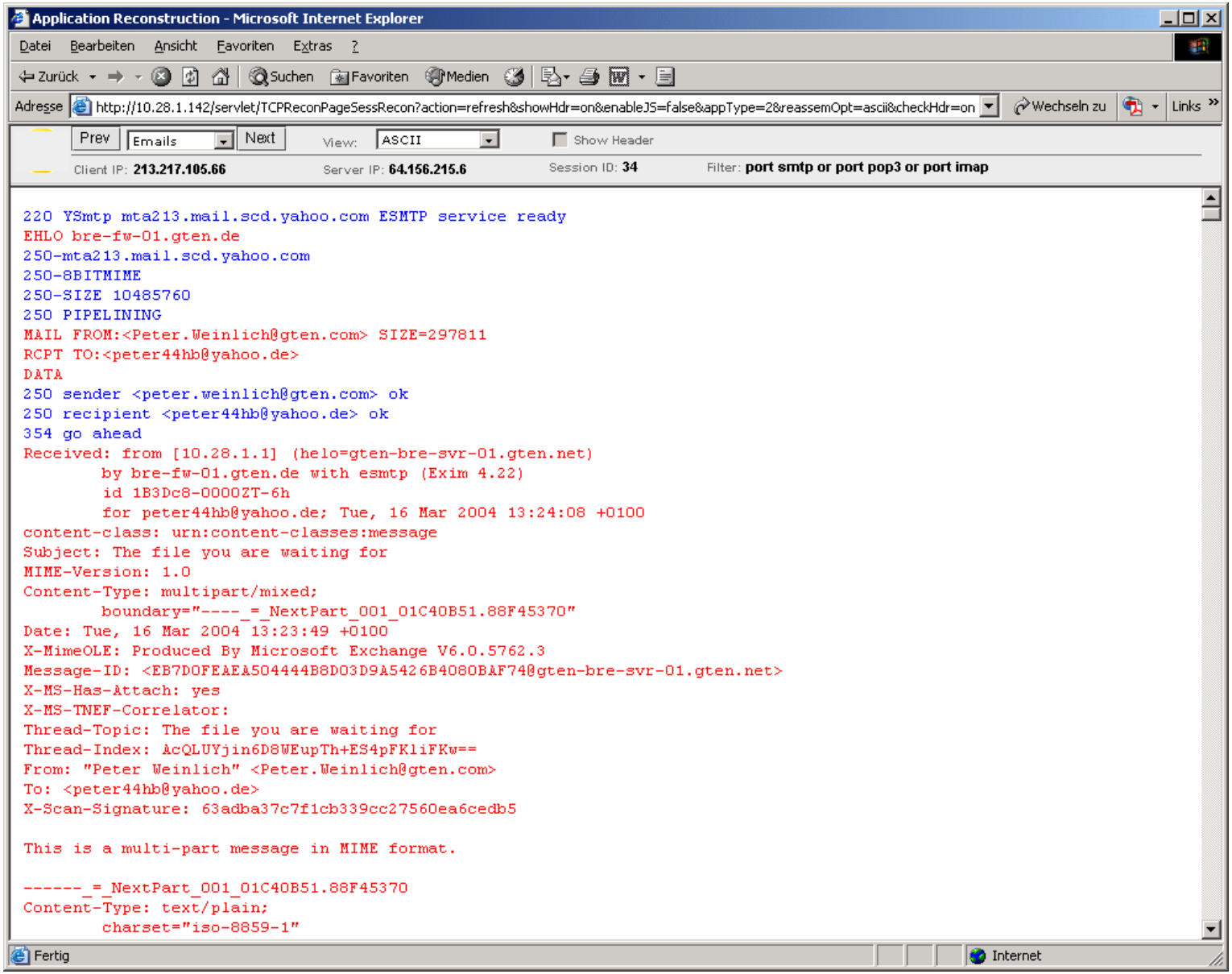
[Einsatz]

- direkte Aufzeichnung des IP Datenverkehrs vor Ort
- Aufzeichnung von IP Datenverkehr in unterschiedlichen Netzen wie:
  - Ethernet (Fast und Gigabit Ethernet)
  - ATM
  - POS
  - E1/T1, E3/T3
- Rekonstruktion von IP-Daten wie HTML, Email, WebMail, Chat, Telnet, FTP, VoIP, etc.

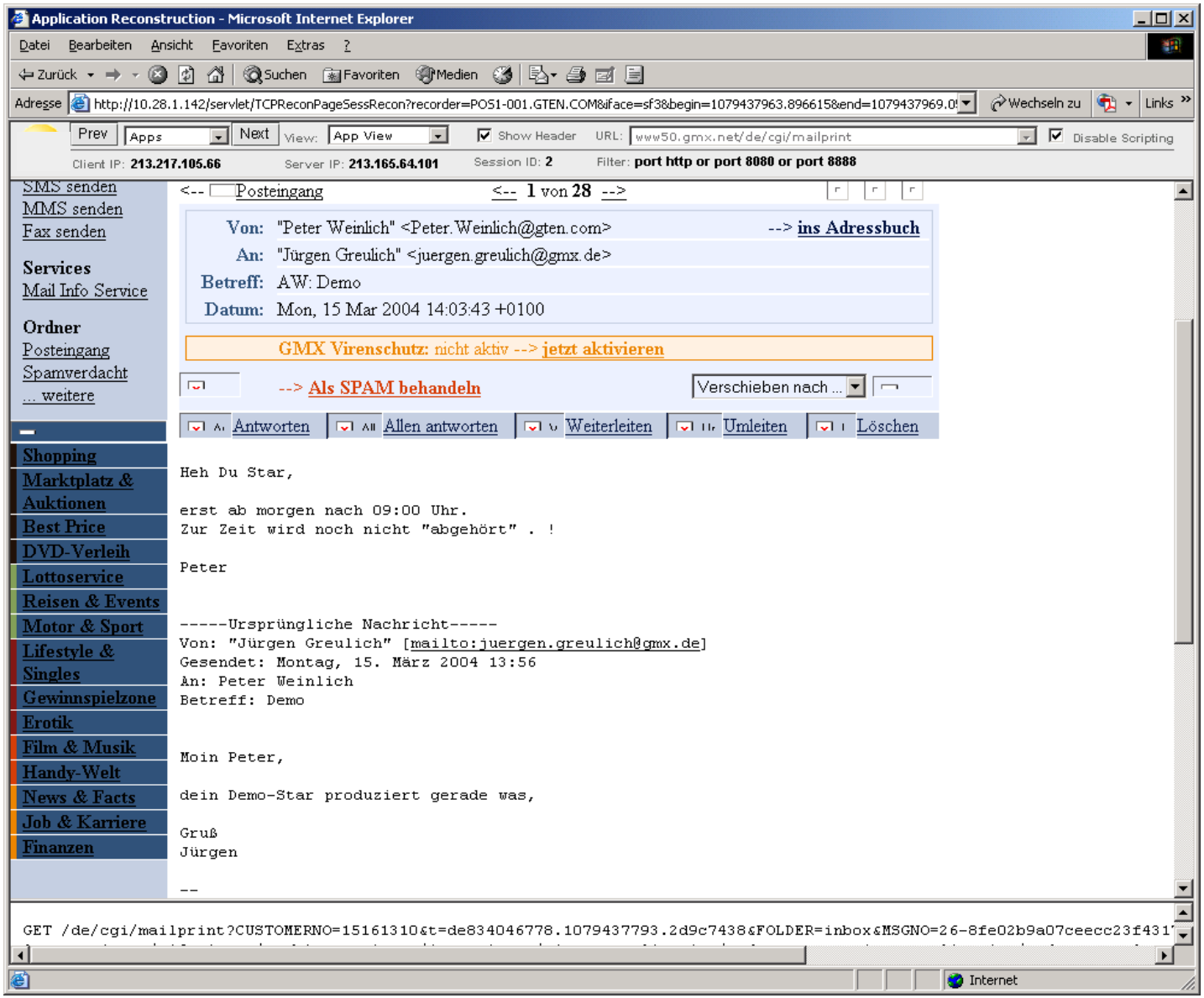
Rekonstruierte eMail (Applikation)



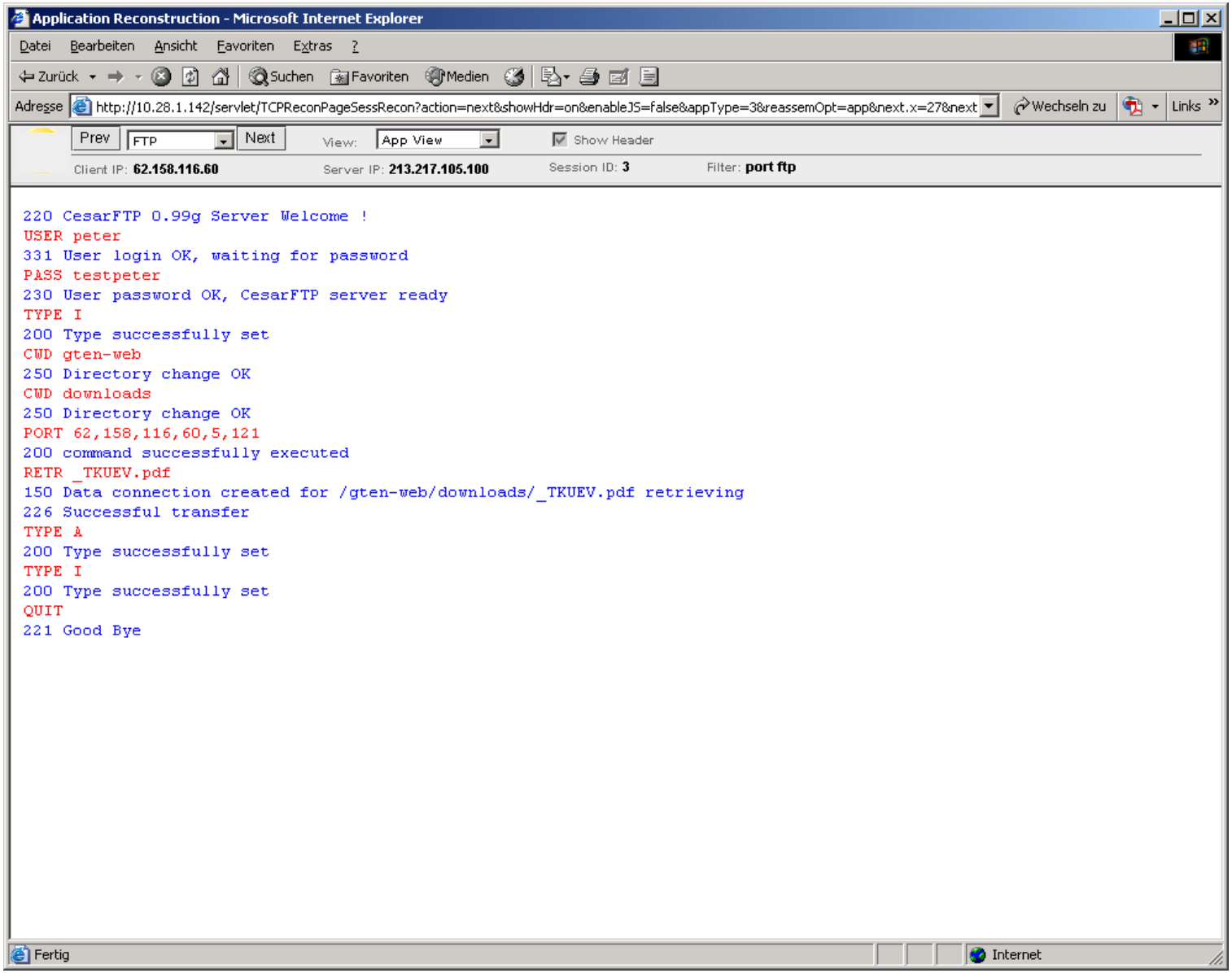
Rekonstruierte e-Mail (ASCII)



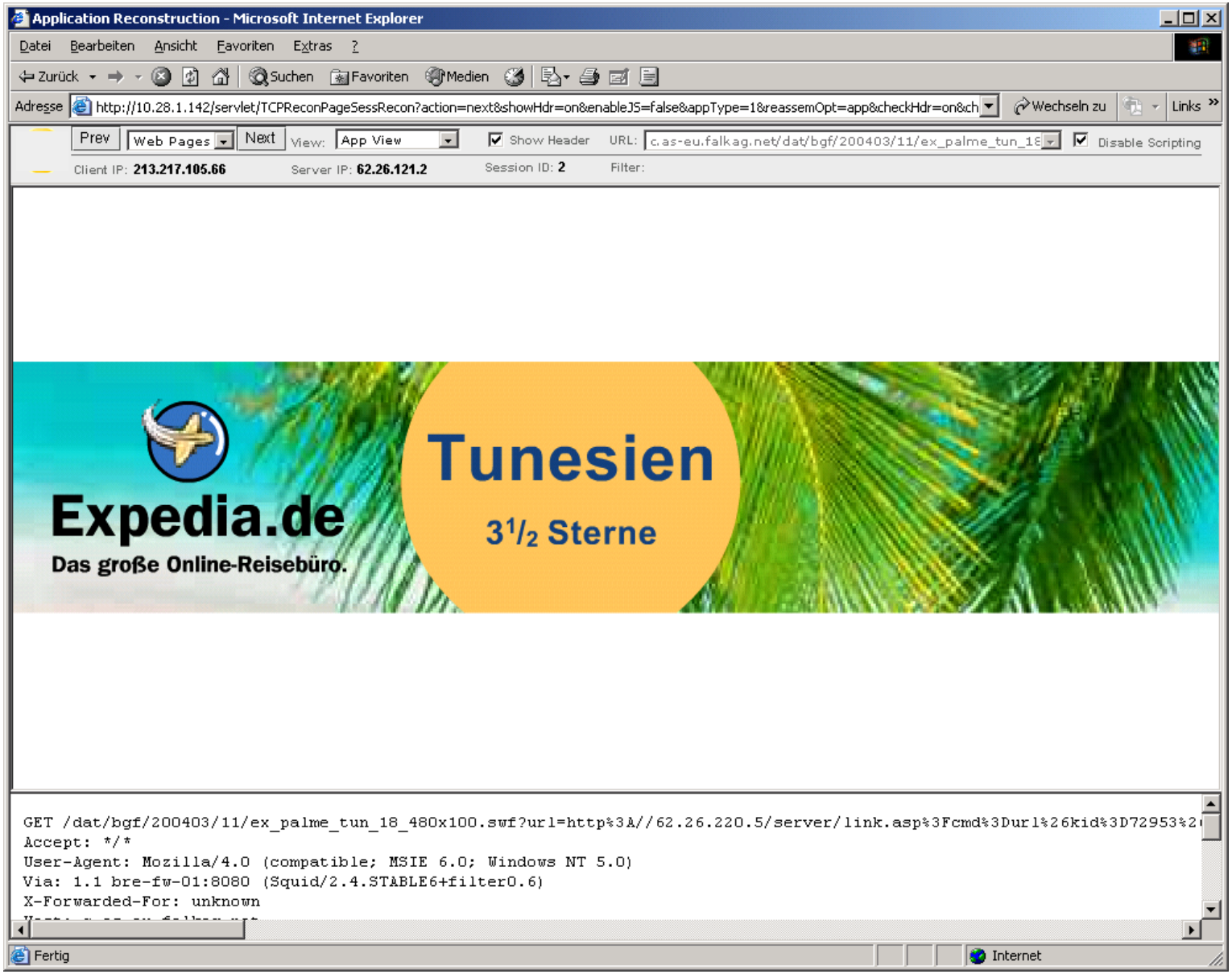
WEB-Mail



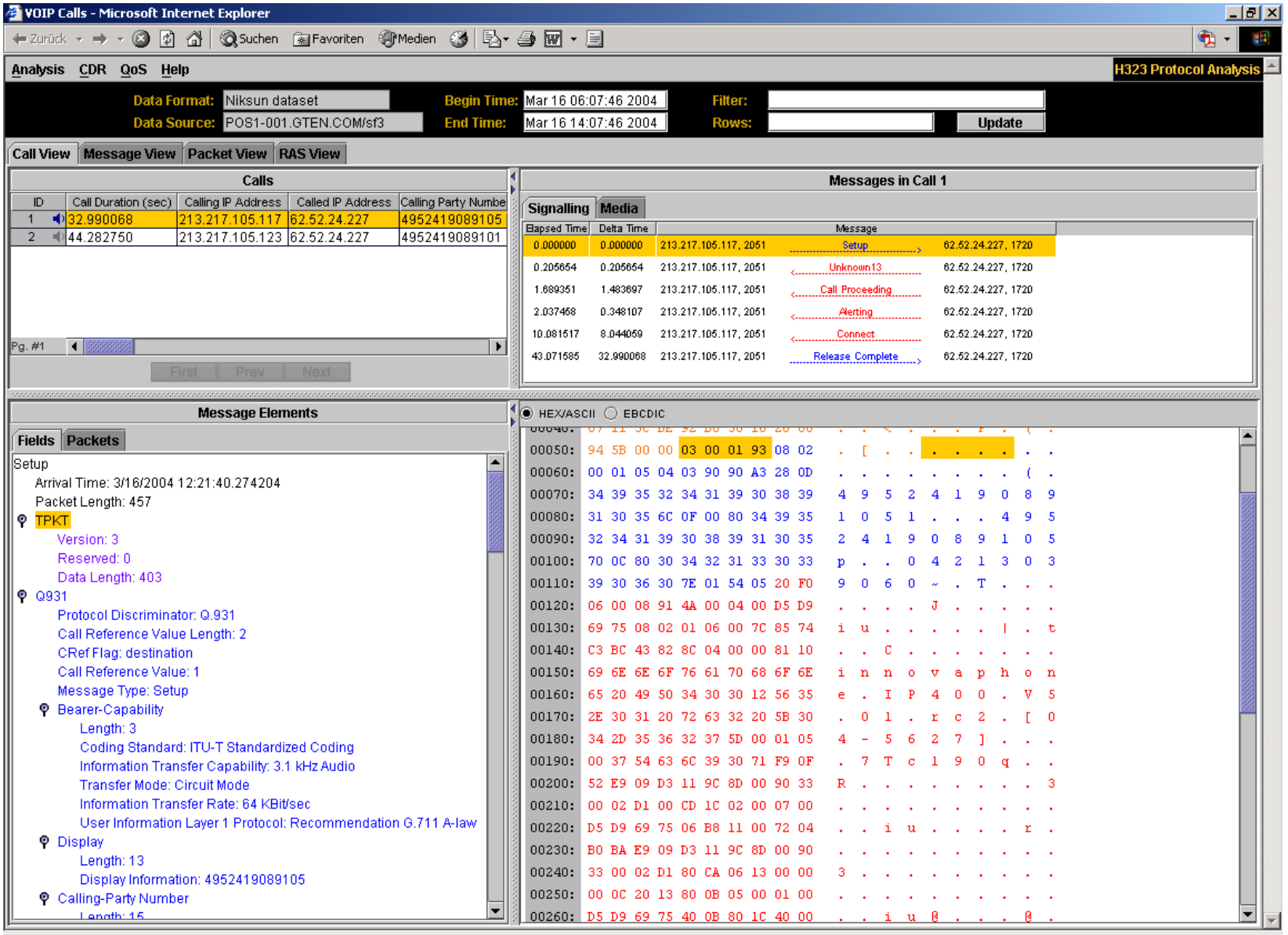
FTP session – User action



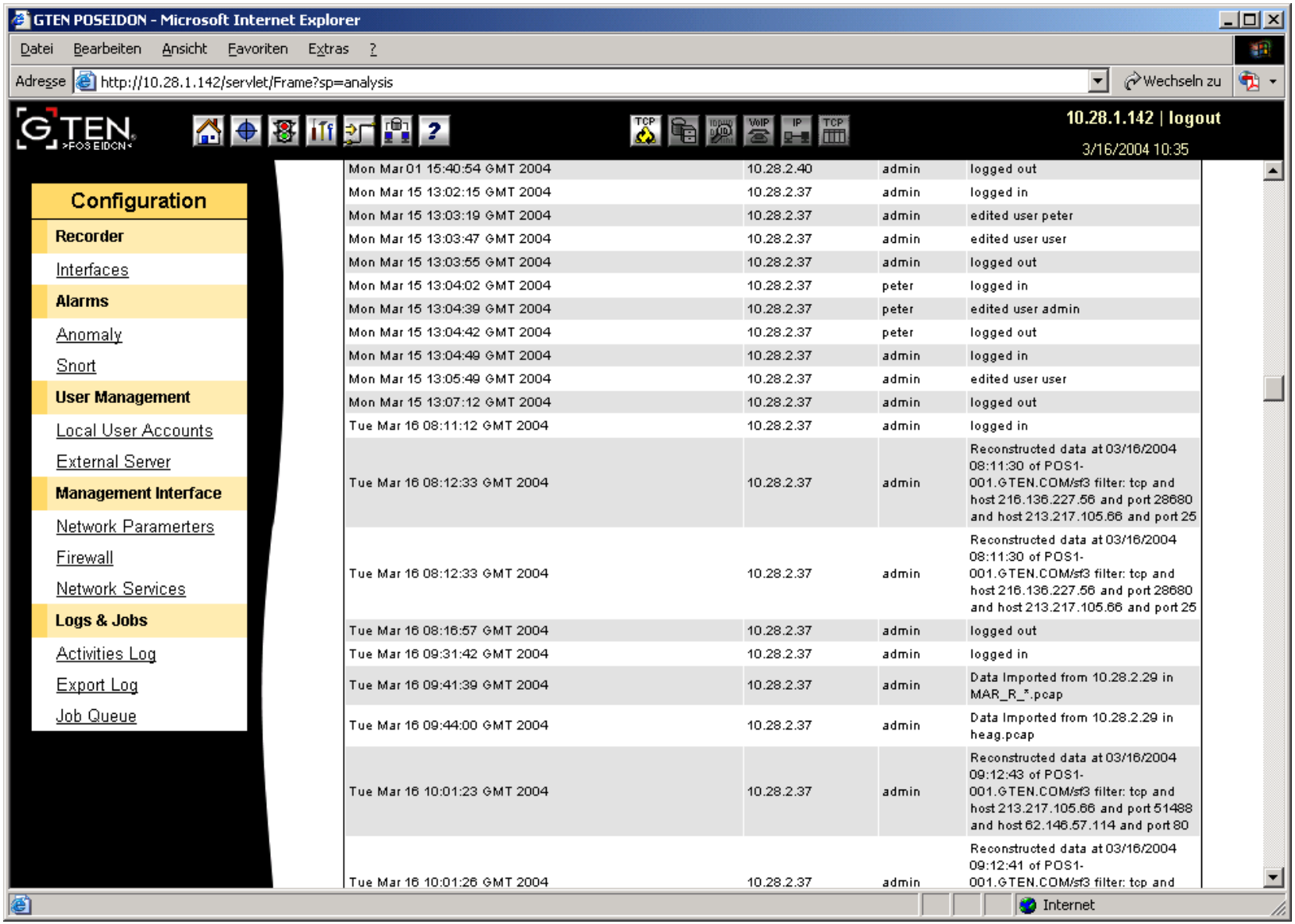
Rekonstruierte WEB-Seite



Voice over IP (Session list)



Access Log



GTEN Erfolgskonzept (1)

- Erstes, durch (BMWi/RegTP) zertifiziertes Rahmenkonzept
- LI-Lösung
  - Modular und skalierbar
  - unabhängig vom jeweiligen Netzwerkhersteller
- GTEN Lösung verfügbar als
  - Poolvertrag mit Service Konzept
  - Fest installiertes System

GTEN Erfolgskonzept (2)

- GTEN Lösung unterstützt alle gängigen Protokolle
  - X.25, ISDN, IP, ATM, etc
  - patentierte Technologie
- Bedeutende Netzbetreiber vertrauen bereits dem GTEN Service-Konzept
- GTEN Lösungen haben keine Auswirkungen auf die Netzwerk Performance