



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 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





Anforderungen

NETZ
[G]

- 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

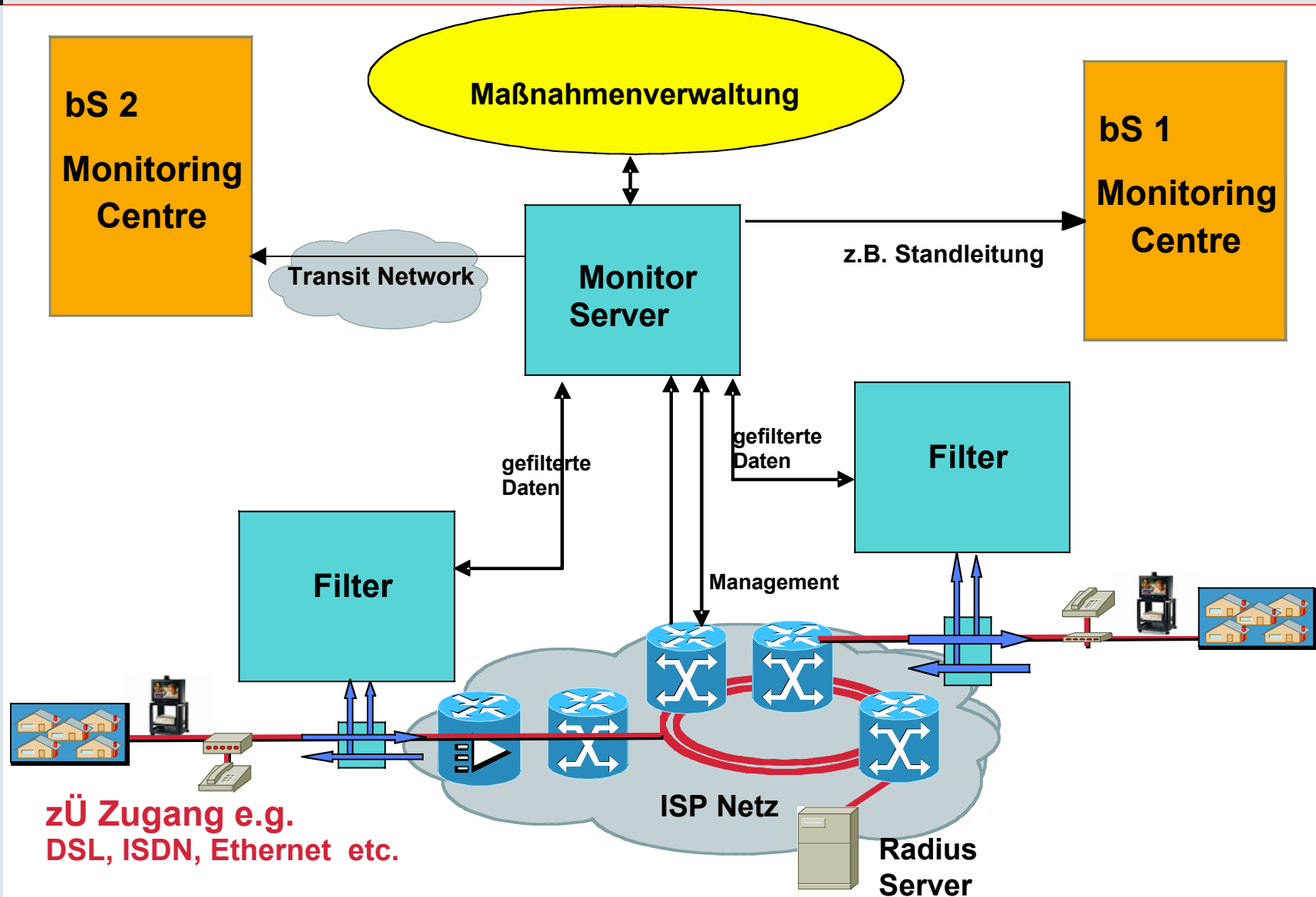


Datenüberwachung braucht Datenschutz!

GTEN
[G] [T] [E] [N]

- 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

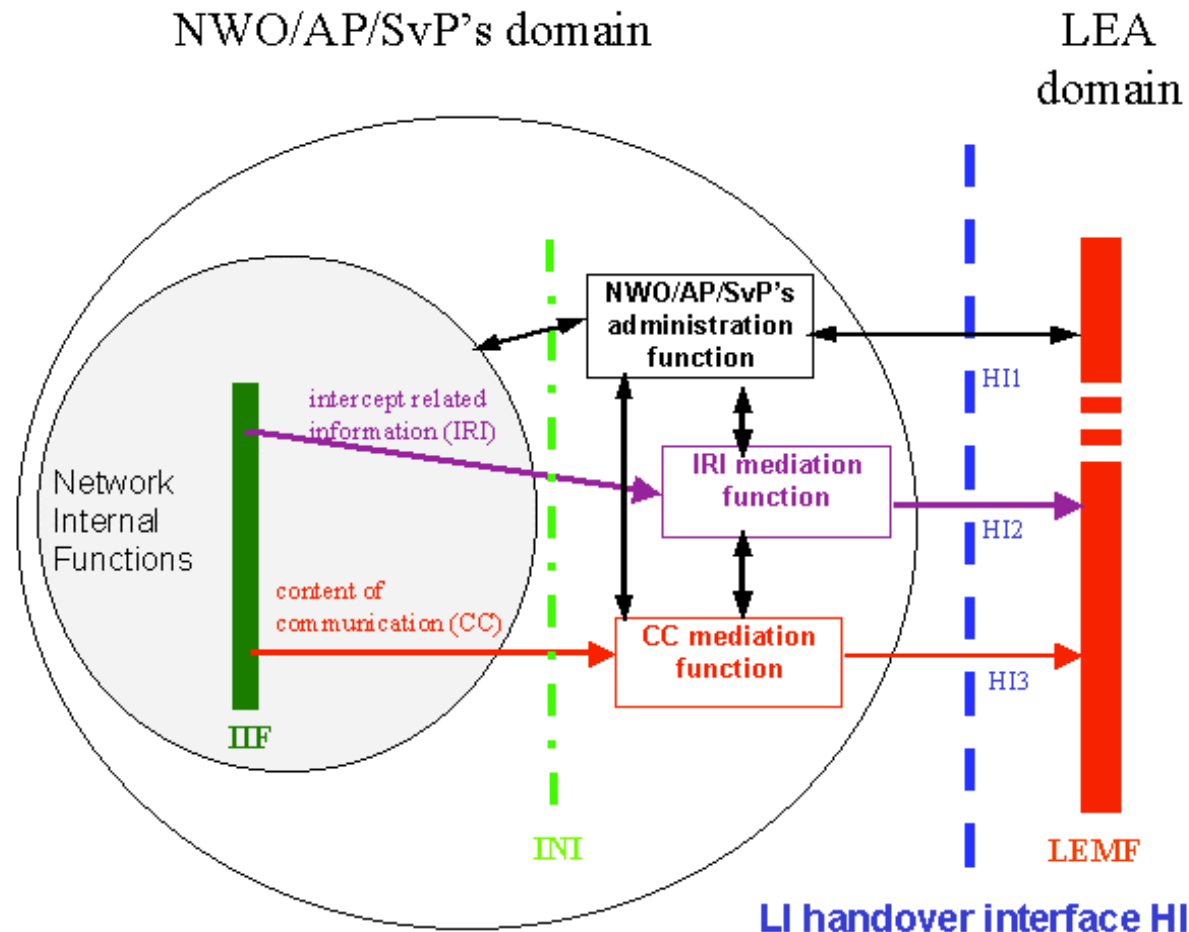
Internetüberwachung



zÜ Zugang e.g.
DSL, ISDN, Ethernet etc.



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

GTEN
[G]

Front-End-Lösungen

- Front-End Lösungen bieten umfassende Möglichkeiten, die Kommunikation einzelner Kunden eines Netzbetreibers gesetzeskonform zu überwachen
- Unabhängig vom zugrunde liegenden Protokoll wird eine Kopie der Daten-Kommunikation angefertigt und real-time an die berechnete 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 empfangene 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

GTEN
[G] [T] [E] [N]

- 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

GTEN



POSEIDON



Sprache/Fax/Modem/
Daten Monitoring Center



POSEIDON Mobil



GTEN Back-End Produkte (I)

Monitoring Center

[Einsatz]

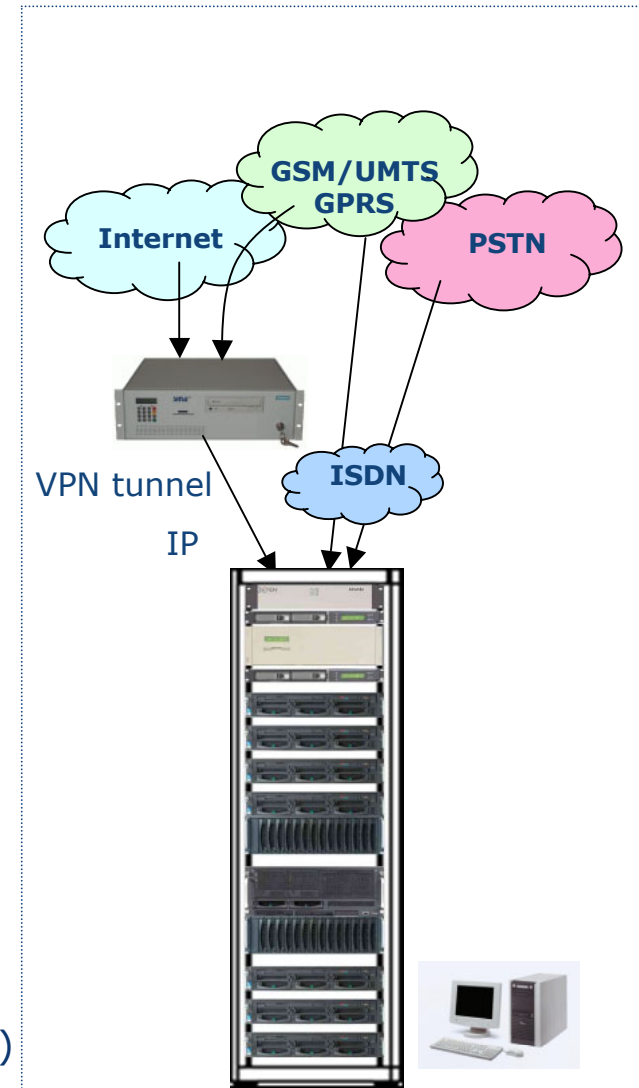
- Aufzeichnung, Decodierung, Archivierung und Evaluation aller Arten von Kommunikationsdaten (Sprache, Fax, Modem, IP)

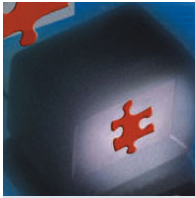
[Features]

- 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)

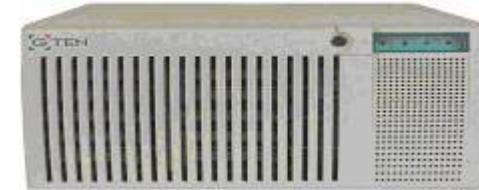




GTEN Back-End Produkte (II)

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)

GTEN

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse <http://10.28.1.142/servlet/TCPReconPageSessRecon?recorder=PO51-001.GTEN.COM&iface=sf3&begin=1079440005.976016&end=1079440009.6> Wechseln zu Links

Prev Emails Next View: App View Show Header

Client IP: 213.217.105.66 Server IP: 64.156.215.6 Session ID: 34 Filter: port smtp or port pop3 or port imap

Email Reconstruction

Save as eml

From:	"Peter Weinlich" <Peter.Weinlich@gten.com>
To:	<peter44hb@yahoo.de>
Date:	Tue, 16 Mar 2004 13:23:49 +0100
Subject:	The file you are waiting for
Attachments:	VOLVO V70.pdf 0

Dear Peter,

attached please find the file you asked for.

If you need any help, just call me.

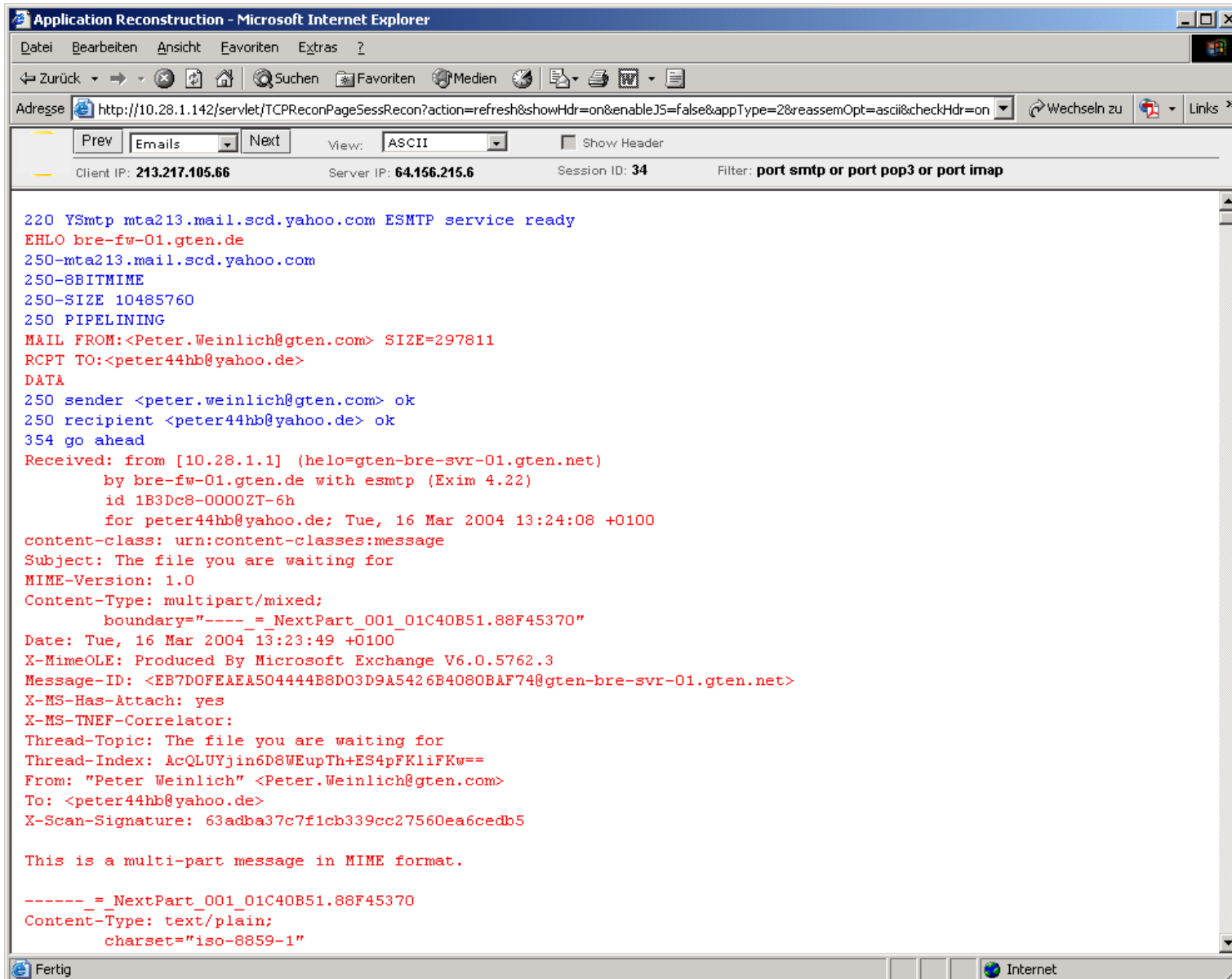
Kind Regards,
Peter Weinlich

<>

Received: from [10.28.1.1] (helo=gten-bre-svr-01.gten.net)
by bre-fw-01.gten.de with esmtp (Exim 4.22)
id 1B3Dc8-0000ZT-6h

Fertig Internet

Rekonstruierte e-Mail (ASCII)



The screenshot shows a Microsoft Internet Explorer window titled "Application Reconstruction - Microsoft Internet Explorer". The address bar contains the URL: `http://10.28.1.142/servlet/TCPRconPageSessRecon?action=refresh&showHdr=on&enableJS=false&appType=2&reassemOpt=ascii&checkHdr=on`. The browser interface includes a menu bar (Datei, Bearbeiten, Ansicht, Favoriten, Extras, ?), a toolbar with navigation and search icons, and a status bar at the bottom showing "Fertig" and "Internet".

The main content area displays the reconstructed email in ASCII format. The text is as follows:

```
220 YSmtpl mta213.mail.scd.yahoo.com ESMTPL service ready
EHLO bre-fw-01.gten.de
250-mta213.mail.scd.yahoo.com
250-8BITMIME
250-SIZE 10485760
250 PIPELINING
MAIL FROM:<Peter.Weinlich@gten.com> SIZE=297811
RCPT TO:<peter44hb@yahoo.de>
DATA
250 sender <peter.weinlich@gten.com> ok
250 recipient <peter44hb@yahoo.de> ok
354 go ahead
Received: from [10.28.1.1] (helo=gten-bre-svr-01.gten.net)
      by bre-fw-01.gten.de with esmtpl (Exim 4.22)
      id 1B3Dc8-00002T-6h
      for peter44hb@yahoo.de; Tue, 16 Mar 2004 13:24:08 +0100
content-class: urn:content-classes:message
Subject: The file you are waiting for
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="-----=_NextPart_001_01C40B51.88F45370"
Date: Tue, 16 Mar 2004 13:23:49 +0100
X-MimeOLE: Produced By Microsoft Exchange V6.0.5762.3
Message-ID: <EB7D0FEAEA504444B8D03D9A5426B4080BAF74@gten-bre-svr-01.gten.net>
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: The file you are waiting for
Thread-Index: AcQLUYjin6D8WEupTh+ES4pFKliFKw==
From: "Peter Weinlich" <Peter.Weinlich@gten.com>
To: <peter44hb@yahoo.de>
X-Scan-Signature: 63adba37c7f1cb339cc27560ea6cedb5

This is a multi-part message in MIME format.

-----=_NextPart_001_01C40B51.88F45370
Content-Type: text/plain;
      charset="iso-8859-1"
```

WEB-Mail



GTEN

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse <http://10.28.1.142/servlet/TCPRconPageSessRecon?recorder=POS1-001.GTEN.COM&face=sf3&begin=1079437963.896615&end=1079437969.0!> Wechseln zu Links

Prev Apps Next View: App View Show Header URL: www50.gmx.net/de/cgi/mailprint Disable Scripting

Client IP: 213.217.105.66 Server IP: 213.165.64.101 Session ID: 2 Filter: port http or port 8080 or port 8888

SMS senden
MMS senden
Fax senden

Services
Mail Info Service

Ordner
Posteingang
Spamverdacht
... weitere

Shopping
Marktplatz & Auktionen
Best Price
DVD-Verleih
Lottoservice
Reisen & Events
Motor & Sport
Lifestyle & Singles
Gewinnspielzone
Erotik
Film & Musik
Handy-Welt
News & Facts
Job & Karriere
Finanzen

Posteingang <-- 1 von 28 -->

Von: "Peter Weinlich" <Peter.Weinlich@gten.com> --> [ins Adressbuch](#)
An: "Jürgen Greulich" <juergen.greulich@gmx.de>
Betreff: AW: Demo
Datum: Mon, 15 Mar 2004 14:03:43 +0100

GMX Virenschutz: nicht aktiv --> [jetzt aktivieren](#)

--> [Als SPAM behandeln](#) Verschieben nach ...

A. Antworten AII Allen antworten v Weiterleiten U Umleiten L Löschen

Heh Du Star,
erst ab morgen nach 09:00 Uhr.
Zur Zeit wird noch nicht "abgehört" . !

Peter

-----Ursprüngliche Nachricht-----
Von: "Jürgen Greulich" [<mailto:juergen.greulich@gmx.de>]
Gesendet: Montag, 15. März 2004 13:56
An: Peter Weinlich
Betreff: Demo

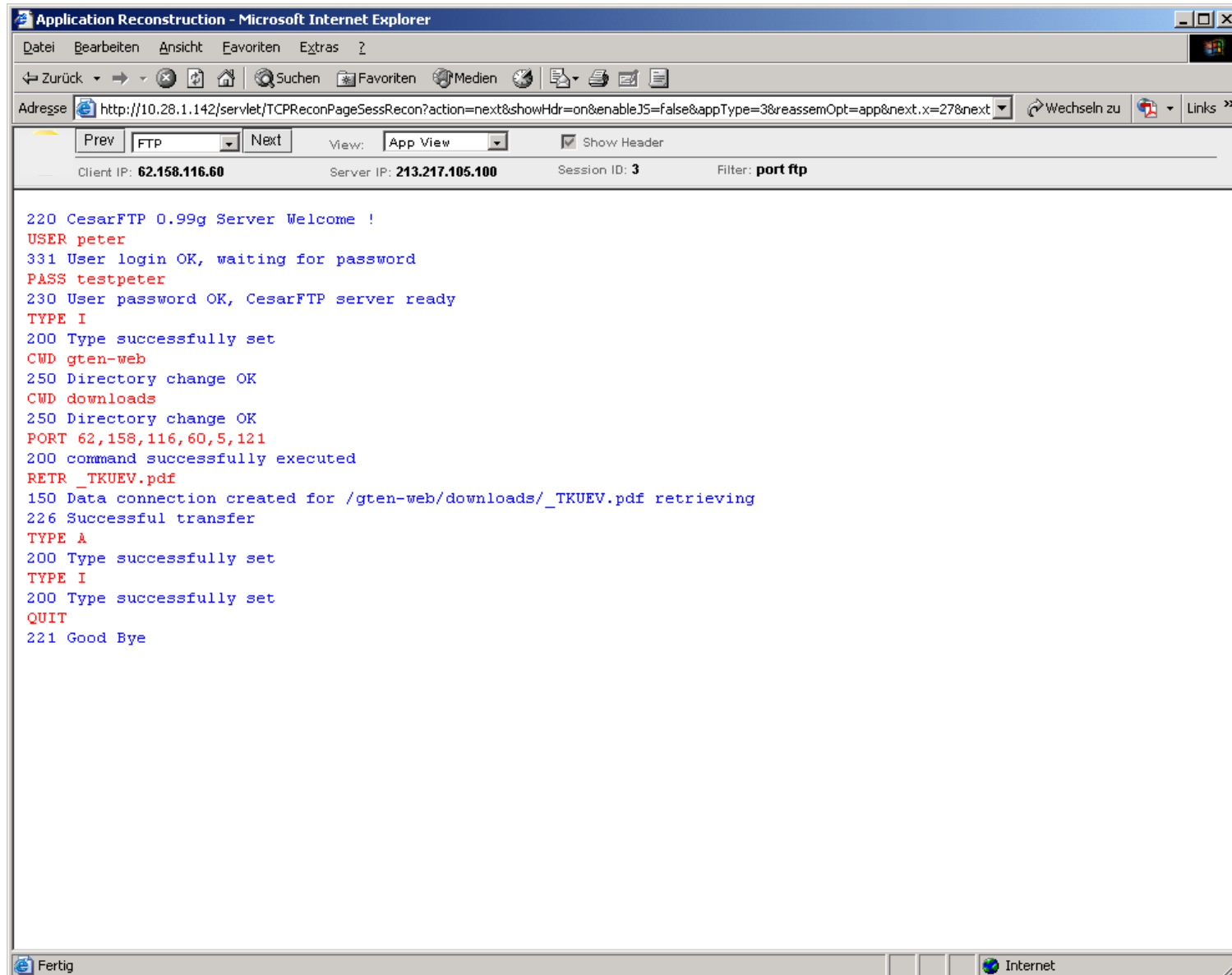
Moin Peter,
dein Demo-Star produziert gerade was,
Gruß
Jürgen

--

GET /de/cgi/mailprint?CUSTOMERNO=15161310&t=de834046778.1079437793.2d9c7438&FOLDER=inbox&MSGNO=26-8fe02b9a07ceecc23f431'

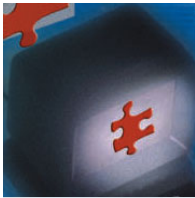
Internet

FTP session – User action



```
Application Reconstruction - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://10.28.1.142/servlet/TCPRconPageSessRecon?action=next&showHdr=on&enableJS=false&appType=3&reassemOpt=app&next.x=27&next
Prev FTP Next View: App View Show Header
Client IP: 62.158.116.60 Server IP: 213.217.105.100 Session ID: 3 Filter: port ftp

220 CesarFTP 0.99g Server Welcome !
USER peter
331 User login OK, waiting for password
PASS testpeter
230 User password OK, CesarFTP server ready
TYPE I
200 Type successfully set
CWD gten-web
250 Directory change OK
CWD downloads
250 Directory change OK
PORT 62,158,116,60,5,121
200 command successfully executed
RETR _TKUEV.pdf
150 Data connection created for /gten-web/downloads/_TKUEV.pdf retrieving
226 Successful transfer
TYPE A
200 Type successfully set
TYPE I
200 Type successfully set
QUIT
221 Good Bye
```



Rekonstruierte WEB-Seite

GTEN
[G]

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse <http://10.28.1.142/servlet/TCPReconPageSessRecon?action=next&showHdr=on&enableJS=false&appType=1&reassemOpt=app&checkHdr=on&ch> Wechseln zu Links

Prev Web Pages Next View: App View Show Header URL: c.as-eu.falkag.net/dat/bgf/200403/11/ex_palme_tun_18 Disable Scripting

Client IP: 213.217.105.66 Server IP: 62.26.121.2 Session ID: 2 Filter:

GET /dat/bgf/200403/11/ex_palme_tun_18_480x100.swf?url=http%3A//62.26.220.5/server/link.asp%3Fcmd%3Durl%26kid%3D72953%2
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Via: 1.1 bre-fw-01:8080 (Squid/2.4.STABLE6+filter0.6)
X-Forwarded-For: unknown

Fertig Internet

Voice over IP (Session list)



GTEN

VOIP Calls - Microsoft Internet Explorer

Analysis CDR QoS Help H323 Protocol Analysis

Data Format: Nixsun dataset Begin Time: Mar 16 06:07:46 2004 Filter:
 Data Source: POS1-001.GTEN.COM/sf3 End Time: Mar 16 14:07:46 2004 Rows: Update

Call View Message View Packet View RAS View

Calls				
ID	Call Duration (sec)	Calling IP Address	Called IP Address	Calling Party Number
1	32.990068	213.217.105.117	62.52.24.227	4952419089105
2	44.282750	213.217.105.123	62.52.24.227	4952419089101

Messages in Call 1				
Signalling		Media		
Bapsed Time	Delta Time	Message		
0.000000	0.000000	213.217.105.117, 2051	Setup	62.52.24.227, 1720
0.205654	0.205654	213.217.105.117, 2051	Unknown13	62.52.24.227, 1720
1.889351	1.483697	213.217.105.117, 2051	Call Proceeding	62.52.24.227, 1720
2.037468	0.348107	213.217.105.117, 2051	Alerting	62.52.24.227, 1720
10.081517	8.044059	213.217.105.117, 2051	Connect	62.52.24.227, 1720
43.071585	32.990068	213.217.105.117, 2051	Release Complete	62.52.24.227, 1720

Message Elements

Fields Packets

Setup
 Arrival Time: 3/16/2004 12:21:40.274204
 Packet Length: 457

TPKT
 Version: 3
 Reserved: 0
 Data Length: 403

Q931
 Protocol Discriminator: Q.931
 Call Reference Value Length: 2
 CRef Flag: destination
 Call Reference Value: 1
 Message Type: Setup

Bearer-Capability
 Length: 3
 Coding Standard: ITU-T Standardized Coding
 Information Transfer Capability: 3.1 kHz Audio
 Transfer Mode: Circuit Mode
 Information Transfer Rate: 64 KBit/sec
 User Information Layer 1 Protocol: Recommendation G.711 A-law

Display
 Length: 13
 Display Information: 4952419089105

Calling-Party Number
 Length: 15

HEX ASCII EBCDIC

```

00050: 94 5B 00 00 03 00 01 93 08 02 . [ . . . . . ]
00060: 00 01 05 04 03 90 90 A3 28 0D . . . . . ( .
00070: 34 39 35 32 34 31 39 30 38 39 4 9 5 2 4 1 9 0 8 9
00080: 31 30 35 6C 0F 00 80 34 39 35 1 0 5 1 . . . 4 9 5
00090: 32 34 31 39 30 38 39 31 30 35 2 4 1 9 0 8 9 1 0 5
00100: 70 0C 80 30 34 32 31 33 30 33 p . . 0 4 2 1 3 0 3
00110: 39 30 36 30 7E 01 54 05 20 F0 9 0 6 0 ~ . T . . .
00120: 06 00 08 91 4A 00 04 00 D5 D9 . . . . J . . . .
00130: 69 75 08 02 01 06 00 7C 85 74 i u . . . . | . t
00140: C3 BC 43 82 8C 04 00 00 81 10 . . C . . . . .
00150: 69 6E 6E 6F 76 61 70 68 6F 6E i n n o v a p h o n
00160: 65 20 49 50 34 30 30 12 56 35 e . I P 4 0 0 . V 5
00170: 2E 30 31 20 72 63 32 20 5B 30 . 0 1 . r e 2 . [ 0
00180: 34 2D 35 36 32 37 5D 00 01 05 4 - 5 6 2 7 ] . . .
00190: 00 37 54 63 6C 39 30 71 F9 0F . 7 T c l 9 0 q . .
00200: 52 E9 09 D3 11 9C 8D 00 90 33 R . . . . . 3
00210: 00 02 D1 00 CD 1C 02 00 07 00 . . . . .
00220: D5 D9 69 75 06 B8 11 00 72 04 . . i u . . . . r .
00230: B0 BA E9 09 D3 11 9C 8D 00 90 . . . . .
00240: 33 00 02 D1 80 CA 06 13 00 00 3 . . . . .
00250: 00 0C 20 13 80 0B 05 00 01 00 . . . . .
00260: D5 D9 69 75 40 0B 80 1C 40 00 . . i u 0 . . . 0 .
    
```

Access Log

GTEN POSEIDON - Microsoft Internet Explorer

Adresse <http://10.28.1.142/servlet/Frame?sp=analysis> Wechseln zu

10.28.1.142 | logout
3/16/2004 10:35

Configuration	Mon Mar 01 15:40:54 GMT 2004	10.28.2.40	admin	logged out	
Recorder	Mon Mar 15 13:02:15 GMT 2004	10.28.2.37	admin	logged in	
Interfaces	Mon Mar 15 13:03:19 GMT 2004	10.28.2.37	admin	edited user peter	
Alarms	Mon Mar 15 13:03:47 GMT 2004	10.28.2.37	admin	edited user user	
Anomaly	Mon Mar 15 13:03:55 GMT 2004	10.28.2.37	admin	logged out	
Snort	Mon Mar 15 13:04:02 GMT 2004	10.28.2.37	peter	logged in	
User Management	Mon Mar 15 13:04:39 GMT 2004	10.28.2.37	peter	edited user admin	
Local User Accounts	Mon Mar 15 13:04:42 GMT 2004	10.28.2.37	peter	logged out	
External Server	Mon Mar 15 13:04:49 GMT 2004	10.28.2.37	peter	logged in	
Management Interface	Mon Mar 15 13:05:49 GMT 2004	10.28.2.37	admin	edited user user	
Network Paramerters	Mon Mar 15 13:07:12 GMT 2004	10.28.2.37	admin	logged out	
Firewall	Tue Mar 16 08:11:12 GMT 2004	10.28.2.37	admin	logged in	
Network Services	Tue Mar 16 08:12:33 GMT 2004	10.28.2.37	admin	Reconstructed data at 03/16/2004 08:11:30 of POS1-001.GTEN.COM/sf3 filter: top and host 216.136.227.56 and port 28680 and host 213.217.105.66 and port 25	
Logs & Jobs	Tue Mar 16 08:12:33 GMT 2004	10.28.2.37	admin	Reconstructed data at 03/16/2004 08:11:30 of POS1-001.GTEN.COM/sf3 filter: top and host 216.136.227.56 and port 28680 and host 213.217.105.66 and port 25	
Activities Log	Tue Mar 16 08:16:57 GMT 2004	10.28.2.37	admin	logged out	
Export Log	Tue Mar 16 09:31:42 GMT 2004	10.28.2.37	admin	logged in	
Job Queue	Tue Mar 16 09:41:39 GMT 2004	10.28.2.37	admin	Data Imported from 10.28.2.29 in MAR_R_*.pcap	
	Tue Mar 16 09:44:00 GMT 2004	10.28.2.37	admin	Data Imported from 10.28.2.29 in heag.pcap	
	Tue Mar 16 10:01:23 GMT 2004	10.28.2.37	admin	Reconstructed data at 03/16/2004 09:12:43 of POS1-001.GTEN.COM/sf3 filter: top and host 213.217.105.66 and port 51488 and host 62.146.57.114 and port 80	
	Tue Mar 16 10:01:26 GMT 2004	10.28.2.37	admin	Reconstructed data at 03/16/2004 09:12:41 of POS1-001.GTEN.COM/sf3 filter: top and	



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
[G]

- 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

