

**GSE VM/VSE Tagung in  
Düsseldorf  
Vom 2.-4. Mai 2011**

**GEFAHREN IN DER IT - IST IHRE  
PRODUKTION SICHER VOR ANGRIFFEN?**

Heinz Peter Maassen – Lattwein GmbH

Überblick :

E-Mail

Telnet

FTP

HTTP Server mit z/VSE

- ¥ Rundum sorglos ?
- ¥ Sind Ihre Daten sicher ?
- ¥ Gefahren bei System z Umgebungen
- ¥ Machen Sie alles dicht - wie kann IBM hier helfen

# AKTUELLE MELDUNG

## 27.4.2011

The screenshot shows the 'heute.de computer' website interface. The main headline is 'PlayStation Network: Hacker klauen 77 Millionen Kundendaten'. Below the headline, there is a sub-headline 'Sony sperrt Online-Dienste - Racheakt aus der Szene?' and a short article snippet. To the right, there is a 'börsenkurs' section showing the SONY stock price at 19,91. Further right, there is a 'Passwörter ausgespäht' section with a short article snippet. The page also features a navigation menu on the left, a ZDFmediathek section, and a 'Links' section.

**heute.de computer**

**heute-Nachrichten**

- Startseite
- Schlagzeilen
- Politik
- Magazin
- Wirtschaft
- Computer**
- Sport
- Wetter
- Börse

**ZDFmediathek**

- Video iPhone speichert Positionsdaten
- Video Weiter viele Mängel beim Datenschutz
- Video "Digitaler Radiergummi"

**Links**

- Thema Daten in Gefahr
- Kundenkarten: Datenstriptease beim Wäschekauf
- Der Spion, der in der Kleidung steckt
- Wo Datenjäger im Alltag lauern

**Interaktiver Krimi**

- Sendung Wer rettet Dina Foxx?

**PlayStation Network: Hacker klauen 77 Millionen Kundendaten**

Sony sperrt Online-Dienste - Racheakt aus der Szene?

Gigantischer Datenklau: Hacker haben Passwörter, Adressen und möglicherweise auch Kreditkarten-Nummern von 77 Millionen Sony-Kunden gestohlen. Betroffen ist vor allem das PlayStation Network. Ist der Angriff eine Racheaktion aus der Hacker-Szene?

Drucken | Versenden | 27.04.2011

**börsenkurs**

**SONY**  
Kurs  
**19,91** ↓

Datum/Zeit  
27.04. 09:30:06

Vortag Änderung  
20,35 -2,19%

Börse: XETRA  
Kurs 15 min. verzögert  
Indices: realtime

Charts und weitere Informationen  
Quelle: Teledata / Innovative Software

**Passwörter ausgespäht**

Eine unbekannte Person habe sich Zugang zu persönlichen Daten wie Name, Adresse, E-Mail oder Geburtsdatum verschafft, schrieb Sony in Firmenblogs weltweit und informierte die Betroffenen. Auch Logins und Passwörter seien nach derzeitigem Kenntnisstand ausgespäht worden, möglicherweise auch die Liste der Käufe.

# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ✘ Herkömmliche E-Mails sind mit einer Postkarte vergleichbar.
- ✘ Der Inhalt liegt offen und kann von jedem mitgelesen werden.
- ✘ Auch beim Mail Dienstleister lassen sich die E-Mail Daten sogar einfach und automatisch per Programm auswerten oder als Kopie aufbewahren zur späteren Analyse.

# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ¥ E-Mail ersetzt heute immer häufiger den Brief, Telegramm, Fernschreiben und Teletex.
- ¥ 1. E-Mail in Deutschland – wurde am 24. 8. 1984 von Michael Rotert an der TH Karlsruhe empfangen.
- ¥ 2010 wurde 107 Mrd. E-Mails versendet (90 % SPAM).
- ¥ Das heute verwendete Protokoll ist SMTP zum senden und POP3 oder IMAP zum empfangen.

# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ¥ Beim Versand werden die Daten meist über SMTPS verschlüsselt zum Mailserver übertragen.
- ¥ Auch das Abholen der Mails erfolgt meistens über POP3S oder IMAPS Protokolle.
- ¥ Jedoch auf den Servern liegen die Mails – wenn nicht verschlüsselt – lesbar.
- ¥ Das gilt nicht nur für den Body der Mails, sondern auch für die Anhänge.

# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ¥ Die meisten Angriffe gegen Unternehmen erfolgen von Innen.
- ¥ Welchen Weg eine Mail über das Internet geht und auf welchen dieser Server Mails gespeichert und mitgelesen werden ist nicht bekannt.
- ¥ Auf dem Weg zum Empfänger kann eine Mail auch verändert und deren Inhalt verfälscht werden.

# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ¥ Alles gute Gründe E-Mails zu verschlüsseln.  
Aber -

## Warum macht das niemand ?



# E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ¥ Alle heutigen E-Mail Programme unterstützen die Verschlüsselung von Mails
- ¥ Man muss sich nur einen Public/Private Key generieren – und entsprechende Programme zur Verschlüsselung nutzen
- ¥ Aber je nach Mail Programm werden verschiedene Methoden verwendet.


# VORTRAG: MARTIN TRÜBNER 2010

Initiator: Martin  
à

Mal sehen ob es

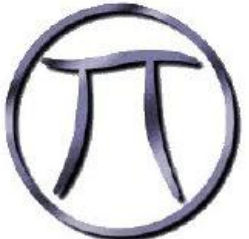
noch mehr CICS

Websites gibt



Geschichte Profil Freeware Produkte Shrinkware

Pi-Systemprogrammierungs-GmbH



Teichstraße 39E  
63225 Langen  
tel: 061.03-71254  
tagsüber: 0171-850 7132  
Email: [info@pi-sysprog.de](mailto:info@pi-sysprog.de)

for a version in english click here

„What can happen when you put your CICS on the web“

Martin Trübner

# AUF DER SUCHE NACH VSE SERVERN IM WWW

Reichlich, wenn  
man nach  
CICS/CWBA  
googelt.

- ¥ Nur einige der 106000 Treffer bei CWBA oder 3660 Treffer auf DFHWBTTA
- ¥ <http://webapps.nyc.gov:8084/cics/cwba/dfhwbtta/abhq>
- ¥ <http://xmarks.com/site/www4.qcard.queensu.ca/QCD3/CICS/CSMI/DFHWBTTA/CW01>
- ¥ <https://www.state.ms.gov/taxtitle/cics/dfhwbtta/TNIQ>
- ¥ <https://accounts.swbno.org:8084/cics/cwba/dfhwbtta/wa00>
- ¥ <https://techmvs.technion.ac.il/cics/CWBA/WGRNSE1?SUB=134065>

# NY GOV APPLICATION

**J-51 Abatement History Menu**

**J-51 Benefit History Request Screen**

**PROPERTY** [J-51 Explanation](#) [Disclaimer](#)

**PARKING & VEHICLES** Please enter all fields:

**BUSINESS TAXES** Borough:

**OTHER SERVICES** Block:

**FORMS & PUBLICATIONS** Lot:

**ABOUT FINANCE** Tax Year:

**CONTACT FINANCE**

**SEARCH**

**J-51 Explanation**

The J-51 benefit program of the City of New York is a tax incentive for the renovation of multiple unit residential buildings. The Department of Housing, Preservation and Development (HPD) administers the program and handles all applications for it. The Department of Finance applies the HPD approved benefits to real property assessed value and taxes.

The program includes two benefits, both based on the certified cost of building alteration. (1) The J-51 Exemption reduces the taxable assessed value, which is the basis for calculating Real Estate Taxes. (2) The J-51 Abatement reduces the actual tax that has been charged against a property.

**J-51 Program Information**

**Disclaimer**

- The J-51 Benefit history is for informational purposes only. It contains information that may be currently under review. The information shown may not show data that has been added or changed in the last 7 days. Recent changes shown may not yet have affected billing.
- The Department of Finance records are updated regularly. If you believe there are any inaccuracies as to the information contained on these pages or if you need updated information, please contact the Department of Finance.
- You may not be entitled to the credits appearing on these pages. To verify entitlement please contact the Department of Finance.
- To reach the Department of Finance J51 Abatement Unit write to:

Exemptions Section - J51  
P.O. Box 3128  
Chambers Street Station  
New York, NY 10007-3128

Copyright 2008 The City of New York [CONTACT US](#) / [FAQS](#) / [DISCLAIMER](#) / [JOB VAC](#)

# WWW.STATE.MS.GOV



# QUEEN UNIVERSITY CA

ASQ - Queen's University - SeaMonkey

https://www.asq.queensu.ca/req/1/ocs/any/dffvbita/4=81

Startseite | Lesesuchen | SeaMonkey deutsch | mozilla.org | mozilla2re | mozilla.org | http://service.gov.n... | Latvian Mail

dffvbita - Google-Duche | 351 Abatement History Menu | www4.queensu.ca/QCD1/C... | MoodlePortal for al e-business Login | NYC Property Search NYC | ASQ - Queen's University

Sign off: Q\_

**ASQ Sign-On**  
\*\* PLEASE ENTER YOUR REFERENCE NUMBER OR STUDENT NUMBER \*\*

**For OUAC Applicants**  
Please enter your OUAC reference number. This number can be found on your copy of your application or on the OUAC acknowledgement/amendment form.

**OUAC Reference Number:**  
 Please enter the full 2010 at the beginning of your OUAC Reference number. (2010\*\*\*\*\*) Please enter the final digit (11th) as a zero.

Enter your date of birth, following the format below. If you have not included your date of birth on your OUAC application, you should amend your application using the Amendment/Verification Form that was sent to you. Otherwise you will not be able to access ASQ. After entering your Reference Number and date of birth please click the PROCEED button to continue.

Date of Birth:    (yyyy mm dd)

**For Current Queen's Students**  
Student Number:  Enter your student number and date of birth (following the instructions above). Click PROCEED to enter.

**Your PSE**  
The PSE is required by all first-year, full-time undergraduate programs and Education programs.

**March Break Open House**  
Experience Queen's!  
March 18, 19, 2010

**English Requirements**  
The language of instruction at Queen's is English. Click to learn more about our requirements.

©2007 Queen's University  
Admission Services - Office of the University Registrar  
Bardie Hall  
Queen's University  
KINGSTON, ONTARIO, CANADA  
K7L 3N6  
admission@queensu.ca

# NEW ORLEANS: ACCOUNTS.SWBNO.ORG:8010

**Find Account Number**

In an effort to make your information more secure, we have disabled the online Find Account Number feature. To find your account number, please retrieve a recent water bill and locate your account number in one of the two locations outlined on the sample bill below.

**Sewerage and Water Board of New Orleans**

1117 SANDYBAY STREET  
NEW ORLEANS, LA 70119-0001  
www.swbno.org

Please pay by MAY 31, 2007

Account No. 10488-02-0

Account No.	Water Meter	Water Meter	Rate	Water Meter	Water Meter	Water Meter
1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET
THIS BILL 05/01/07	4,800	0	0.00	00	0.00	0.00
LAST BILL 04/01/07	4,800	0	0.00	00	0.00	0.00
LAST YEAR 05/01/06	4,800	0	0.00	00	0.00	0.00

Account 10488-02-0

Account No.	Water Meter	Water Meter	Water Meter	Water Meter	Water Meter
1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET
1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET	1117 SANDYBAY STREET

City of New Orleans



# MUNICIPALITY OF ANCHORAGE

MUNICIPALITY OF ANCHORAGE

Home Residents Businesses Government Visitors Departments Public Safety

Departments - Finance - Property Taxes - New Results - results

← back Pay Account Property Approval

Account Key: 976-021-21-000 Tax Year: 2009

Name: WEAYE SHELBY C

Transaction Type	Effective Date	Thru Date	Payment	Principal	Interest	Penalty	Cost	Total
FULL YEAR TAX			.00	5,456.75	.00	.00	.00	5,456.75
SRVET EXEMPTION			.00	-1,724.99	.00	.00	.00	-1,724.99
REND EXEMPTION			.00	+236.80	.00	.00	.00	+236.80
TAX CREDIT			.00	-172.39	.00	.00	.00	-172.39
TAX PAYMENT	04-01-09		1,564.10	-1,564.10	.00	.00	.00	-1,564.10
TAX PAYMENT	05-10-09		1,564.10	-1,564.10	.00	.00	.00	-1,564.10
<b>BALANCE</b>		01-25-11	.00	.00	.00	.00	.00	.00

632 W. 60th Avenue Anchorage, Alaska 99501  
PO Box 196550 Anchorage, Alaska 99519



# STATE OF NEVADA



The screenshot displays a web browser window titled "UI Internet Claims Login Screen - SeaMonkey". The browser's address bar shows the URL "https://sec.nvdeir.org/claims/forhrtdr/auis". The browser's menu bar includes "Datei", "Bearbeiten", "Ansicht", "Gehe", "Lesezeichen", "Extras", "Einstellungen", and "Hilfe". The browser's toolbar includes "Startseite", "Lesezeichen", "SeaMonkey deutsch", "mozilla.org", "mozilla2.de", "mozilla.org", "http://services.gov.nv...", "Lithuan Manu", "dfliville - Gey...", "JSL Abonnement", "www-fairaid.a...", "Hilfsmap Part...", "ASQ - Queen's...", "accounts.enr...", "hilfe/7... RD-2009", "Ask a question...", "12308\_Okt\_Ge...", "Gua BS (14) A...", and "UE Internet Cl...".

The main content area of the browser displays the "State of Nevada" logo and the text "Department of Employment, Training & Rehabilitation" and "Nevada Internet Claims". Below this, the "UI Login" section is visible, featuring a key icon. The login form includes the following fields and buttons:

- Social Security Number:** A field with a hyphen and two sub-fields.
- Personal Identification Number (PIN):** A field with a "Help" button.
- Security Verification:** A field with a "Refresh Image" button.
- Buttons:** "EXIT", "Back", "Print", and "LOGIN".
- Link:** "Forgot Your PIN or need a new PIN? Click to get a new PIN."

The browser's status bar at the bottom shows the system tray with icons for "SeaMonkey", "Gnome", and "Gnome 2.26.1".

# UND WIE SICHER SIND UNSERE STANDARD ANWENDUNGEN

- ¥ Auch Inhouse Anwendungen sind nicht sicher!
- ¥ Sei es CICS Sign-ON über Telnet
- ¥ FTP von oder zum z/VSE
- ¥ Email im zVSE versendet

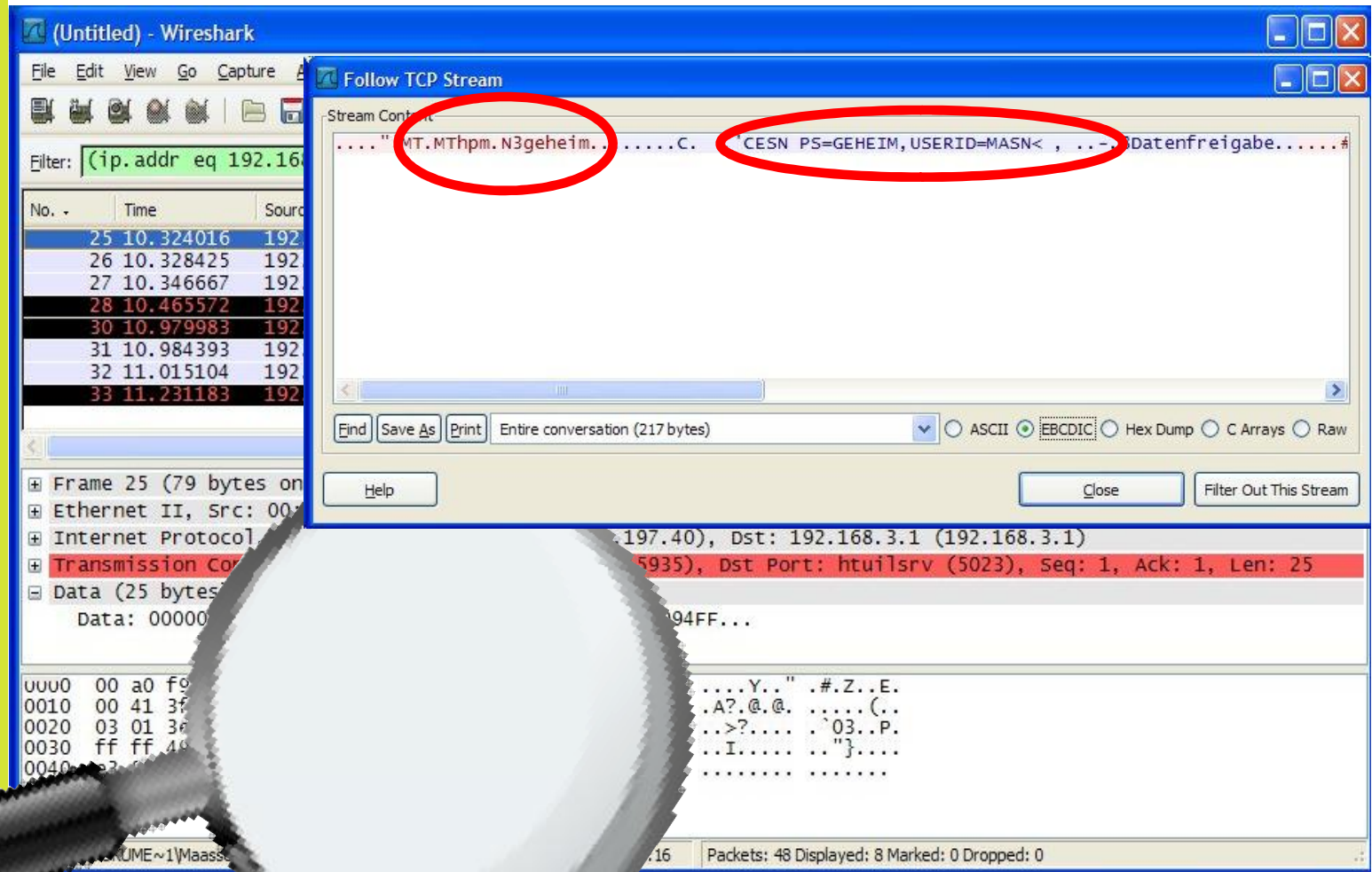
Diese Folien sollen nicht dazu auffordern VSE Systeme auszuspionieren. Sie wollen auf die Gefahren hinweisen, die vorhanden sind. Obwohl die Verwendung von Traces sowie Wireshark normalerweise verboten sind- richtet sich auch derjenige sich nicht daran, der ein System ausspionieren will!

Wikipedia

Wireshark (engl. „wire“: Draht, Kabel; „shark“: Hai; alte Bezeichnung: Ethereal) ist ein freies Programm zur Analyse von Netzwerk-Kommunikationsverbindungen („Sniffer“).

# TELNET LOGIN DATA

LOGIN über  
Benutzer  
Programm  
Und anschließend  
CESN



(Untitled) - Wireshark

Filter: (ip.addr eq 192.168.3.1)

No.	Time	Source
25	10.324016	192.168.3.1
26	10.328425	192.168.3.1
27	10.346667	192.168.3.1
28	10.465572	192.168.3.1
30	10.979983	192.168.3.1
31	10.984393	192.168.3.1
32	11.015104	192.168.3.1
33	11.231183	192.168.3.1

Stream Content: ...."MT.MThpm.N3geheim.....C. CESN PS=GEHEIM, USERID=MASN< , ... Datenfreigabe....."

Find Save As Print Entire conversation (217 bytes) ASCII  EBBCDIC  Hex Dump  C Arrays  Raw

Close Filter Out This Stream

Help

Frame 25 (79 bytes on wire (1000 bytes captured) on interface 0:0:0:0:0:0 (10.324016), Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.3.1 (192.168.3.1))

Ethernet II, Src: 08:00:00:08:00:00 (192.168.3.1), Dst: 08:00:00:08:00:00 (192.168.3.1)

Internet Protocol Version 4, Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.3.1 (192.168.3.1)

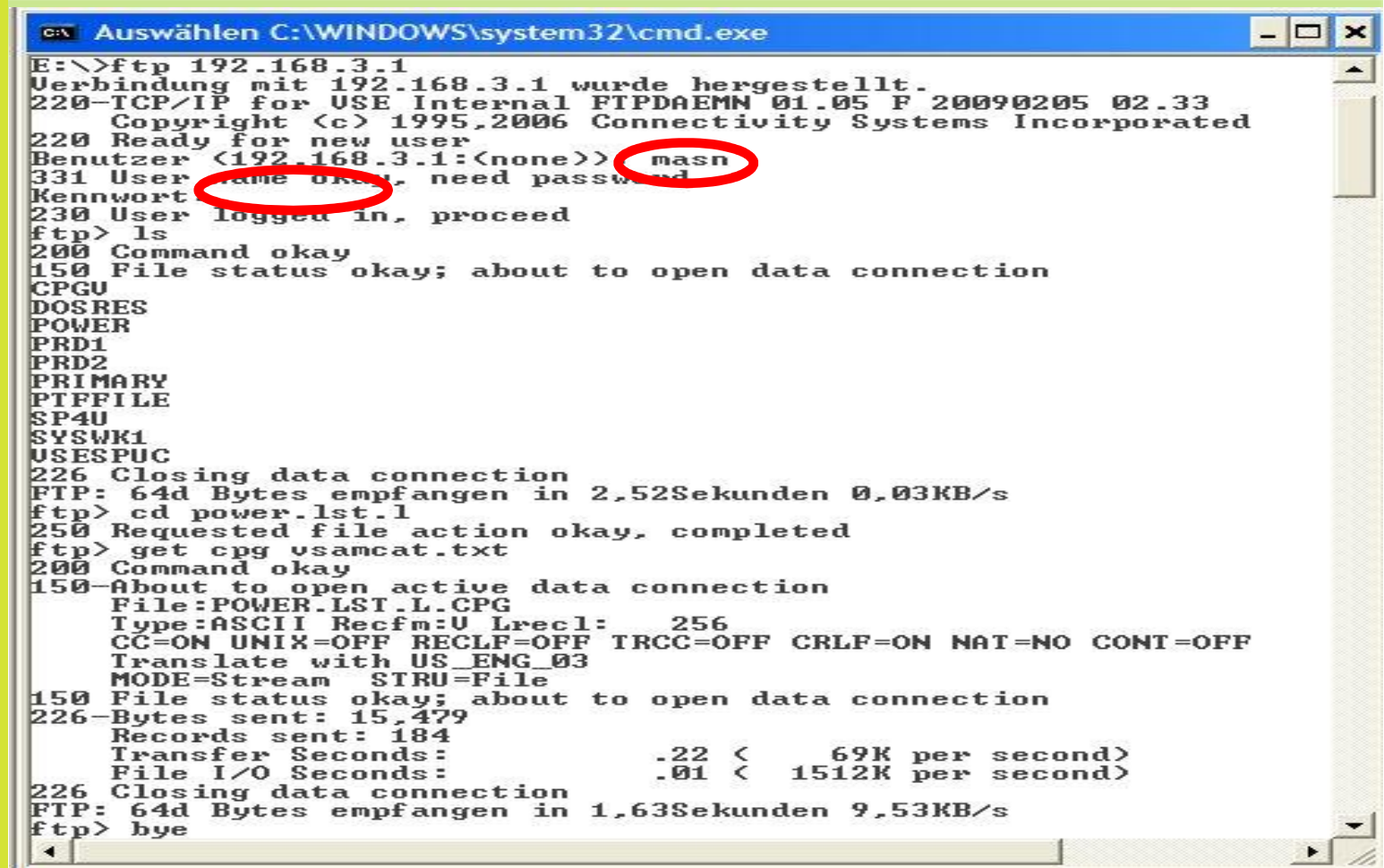
Transmission Control Protocol, Src Port: 5935, Dst Port: htuilsrv (5023), Seq: 1, Ack: 1, Len: 25

Data (25 bytes captured on interface 0:0:0:0:0:0 (10.324016))

Data: 00000000 00010000 00020000 00030000 00040000 00050000 00060000 00070000 00080000 00090000 000A0000 000B0000 000C0000 000D0000 000E0000 000F0000 00100000 00110000 00120000 00130000 00140000 00150000 00160000 00170000 00180000 00190000 001A0000 001B0000 001C0000 001D0000 001E0000 001F0000 00200000 00210000 00220000 00230000 00240000 00250000 00260000 00270000 00280000 00290000 002A0000 002B0000 002C0000 002D0000 002E0000 002F0000 00300000 00310000 00320000 00330000 00340000 00350000 00360000 00370000 00380000 00390000 003A0000 003B0000 003C0000 003D0000 003E0000 003F0000 00400000 00410000 00420000 00430000 00440000 00450000 00460000 00470000 00480000 00490000 004A0000 004B0000 004C0000 004D0000 004E0000 004F0000 00500000 00510000 00520000 00530000 00540000 00550000 00560000 00570000 00580000 00590000 005A0000 005B0000 005C0000 005D0000 005E0000 005F0000 00600000 00610000 00620000 00630000 00640000 00650000 00660000 00670000 00680000 00690000 006A0000 006B0000 006C0000 006D0000 006E0000 006F0000 00700000 00710000 00720000 00730000 00740000 00750000 00760000 00770000 00780000 00790000

VM/VSE GSE-4 16 Packets: 48 Displayed; 8 Marked; 0 Dropped: 0

Command Fenster  
mit FTP zum  
z/VSE.  
TCPIP 1.5.F



```
C:\WINDOWS\system32\cmd.exe
E:\>ftp 192.168.3.1
Verbindung mit 192.168.3.1 wurde hergestellt.
220-TCP/IP for USE Internal FTPDAEMN 01.05 F 20090205 02.33
    Copyright (c) 1995,2006 Connectivity Systems Incorporated
220 Ready for new user
Benutzer (192.168.3.1:(none)) masn
331 User name okay, need password
Kennwort
230 User logged in, proceed
ftp> ls
200 Command okay
150 File status okay; about to open data connection
CPGU
DOSRES
POWER
PRD1
PRD2
PRIMARY
PTFFILE
SP4U
SYSWK1
USESPUC
226 Closing data connection
FTP: 64d Bytes empfangen in 2,52Sekunden 0,03KB/s
ftp> cd power.lst.1
250 Requested file action okay, completed
ftp> get cpg vsamcat.txt
200 Command okay
150-About to open active data connection
File:POWER.LST.L.CPG
Type:ASCII Recfm:U Lrecl: 256
CC=ON UNIX=OFF RECLF=OFF TRCC=OFF CRLF=ON NAT=NO CONT=OFF
Translate with US_ENG_03
MODE=Stream STRU=File
150 File status okay; about to open data connection
226-Bytes sent: 15,479
Records sent: 184
Transfer Seconds: .22 < 69K per second>
File I/O Seconds: .01 < 1512K per second>
226 Closing data connection
FTP: 64d Bytes empfangen in 1,63Sekunden 9,53KB/s
ftp> bye
```

# FTP DAEMON RESPONSE

Im Wireshark  
sieht man die  
Konversation vom  
z/VSE zum Client

The screenshot shows a Wireshark capture of an FTP session. The packet list pane displays the following entries:

No.	Time	Source	Destination	Protocol	Info
9	4.515284	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT]
10	4.521980	192.168.3.1	192.168.197.40	FTP	Response: 220-TCP/IP for VSE Internal FTPDAEMN 01.05 F 20090205
11	4.531205	192.168.3.1	192.168.197.40	TCP	htuilsrv > 16603 [PSH, ACK] Seq=1 Ack=1 Win=65534 Len=106
12	4.653894	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=62 Win=65474 [TCP CHECKSUM INCORRECT]
13	4.654904	192.168.197.40	192.168.3.1	TCP	16603 > htuilsrv [ACK] Seq=1 Ack=107 Win=65429 [TCP CHECKSUM INCORRECT]
14	4.658183	192.168.3.1	192.168.197.40	FTP	Response: Copyright (c) 1995,2006 Connectivity Systems Inc
15	4.855059	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=125 Win=65411 [TCP CHECKSUM INCORRECT]
16	4.858590	192.168.197.40	192.168.197.40	FTP	Response: 220 ready for new user

The packet details pane for packet 16 shows the following structure:

- Frame 16 (78 bytes on wire, 78 bytes captured)
- Ethernet II, Src: Broadcom\_3d:41:5d (00:10:18:3d:41:5d), Dst: 00:22:19:23:05:5a (00:22:19:23:05:5a)
- Internet Protocol, Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.197.40 (192.168.197.40)
- Transmission Control Protocol, Src Port: ftp (21), Dst Port: 17566 (17566), Seq: 125, Ack: 1, Len: 24
- File Transfer Protocol (FTP)
  - 220 Ready for new user\r\n
    - Response code: Service ready for new user (220)
    - Response arg: Ready for new user

The packet bytes pane shows the raw data for the selected packet:

```

0000 0000 0000 00 22 19 23 05 5a 00 10 18 3d 41 5d 08 00 45 00  . . # . z . . . . - A ) . . E .
0010 0010 0010 00 40 73 cc 00 00 fd 06 00 71 c0 a8 03 01 c0 a8  . @ s . . . . . . q . . . . .
0020 0020 0020 e5 28 00 15 44 9e 60 2f 11 b2 22 ea 05 e2 50 18  . ( . . D . / . . . . . P .
0030 0030 0030 ff fe 51 98 00 00 32 32 30 20 52 65 61 64 79 20  . . . . 22 0 Ready
0040 0040 0040 66 6f 72 20 6e 65 77 20 75 73 65 72 0d 0a      for new user..
  
```



# FTP USER MASN

Userid und  
Passwort im  
Klartext !

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.3.1 and ip.addr eq 192.168.197.40) Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
9	4.953591	192.168.3.1	192.168.197.40	FTP	Response: 220 Ready for new user
10	5.168833	192.168.197.40	192.168.3.1	TCP	16693 > ftp [ACK] Seq=1 Ack=149 win=65535
14	8.834804	192.168.197.40	192.168.3.1	FTP	Request: USER masn
15	8.839620	192.168.3.1	192.168.197.40	TCP	ftp > 16693 [ACK] Seq=149 Ack=12 win=65535
16	8.840910	192.168.3.1	192.168.197.40	FTP	Response: 331 User name okay, need password
25	9.106232	192.168.197.40	192.168.3.1	TCP	16693 > ftp [ACK] Seq=12 Ack=184 win=65535
38	12.866749	192.168.197.40	192.168.3.1	FTP	Request: PASS geheim
39	12.874149	192.168.3.1	192.168.197.40	TCP	ftp > 16693 [ACK] Seq=184 Ack=25 win=65535
40	12.875698	192.168.3.1	192.168.197.40	FTP	Response: 230 User logged in, proceed

Frame 40 (83 bytes on wire, 83 bytes captured)

- Ethernet II, Src: Broadcom\_3d:41:5d (00:10:18:3d:41:5d), Dst: 00:22:19:23:05:5a (00:22:19:23:05:5a)
- Internet Protocol, Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.197.40 (192.168.197.40)
- Transmission Control Protocol, Src Port: ftp (21), Dst Port: 16693 (16693), Seq: 184, Ack: 25, Len: 29
- File Transfer Protocol (FTP)

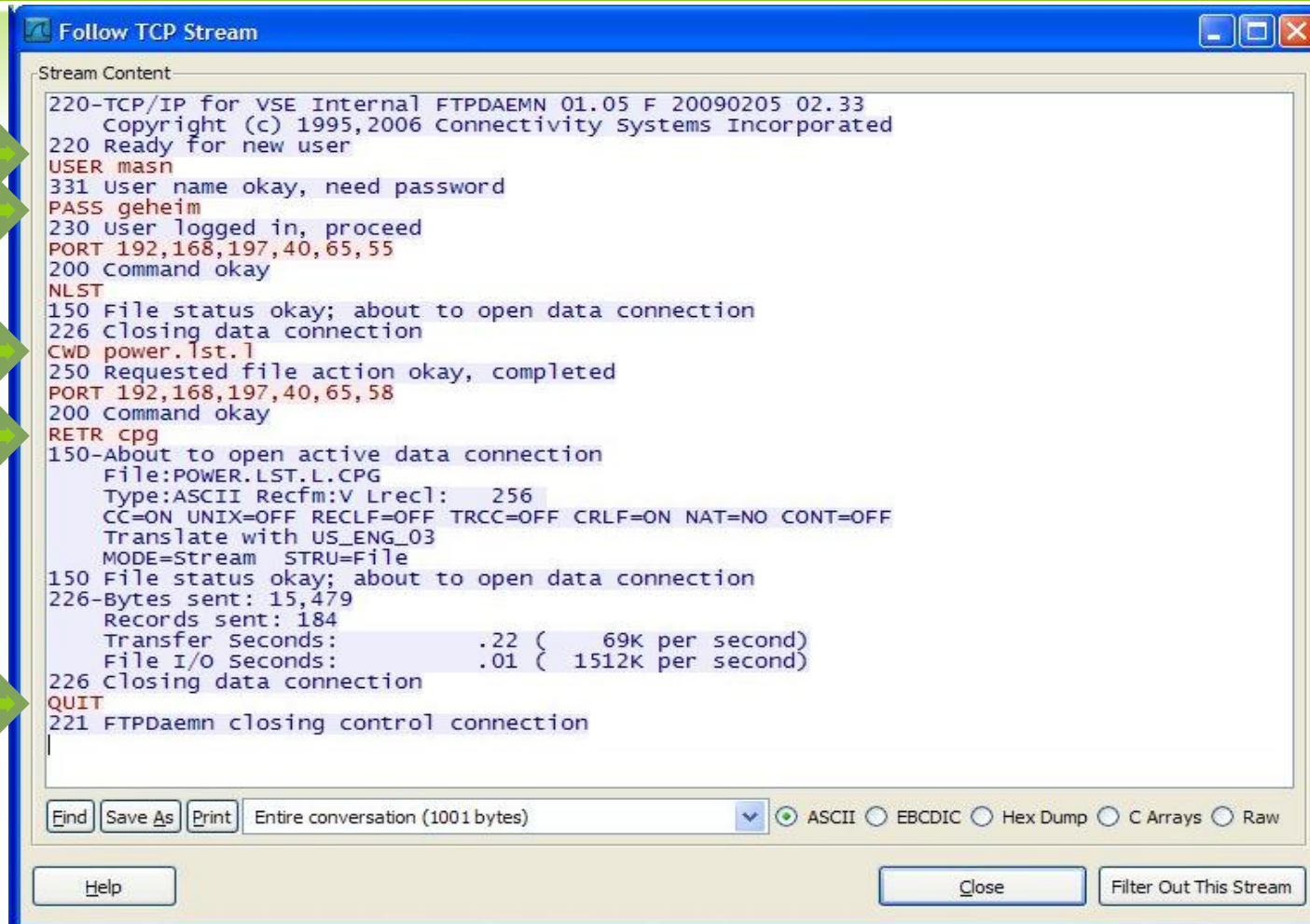
```

0000  00 22 19 23 05 5a 00 10 18 3d 41 5d 08 00 45 00  ."#.Z.. .=A]..E.
0010  00 45 d9 b9 00 00 fd 06 9a 7e c0 a8 03 01 c0 a8  .E..... ~.....
0020  c5 28 00 15 41 35 40 43 dd 7b cb ac 51 0e 50 18  .(..A5@C .{..Q.P.
0030  ff fe 29 08 00 00 32 33 30 20 55 73 65 72 20 6c  ..)...23 0 User |
0040  6f 67 67 65 64 20 69 6e 2c 20 70 72 6f 63 65 65  ogged in , procee
0050  64 0d 0a                                     d..
  
```

File: "C:\DOKUME~1\Maassen2\LOKALE~1\Temp\etherXXXa05488" 40 KB 00:01:29 Packets: 247 Displayed: 63 Marked: 0 Dropped: 0

# FTP FOLLOW TCP STREAM

FTP LS Data



```
220-TCP/IP for VSE Internal FTPDAEMN 01.05 F 20090205 02.33
Copyright (c) 1995,2006 Connectivity Systems Incorporated
220 Ready for new user
USER masn
331 User name okay, need password
PASS geheim
230 User logged in, proceed
PORT 192,168,197,40,65,55
200 Command okay
NLST
150 File status okay; about to open data connection
226 Closing data connection
CWD power.lst.1
250 Requested file action okay, completed
PORT 192,168,197,40,65,58
200 Command okay
RETR cpg
150-About to open active data connection
File:POWER.LST.L.CPG
Type:ASCII Recfm:V Lrecl: 256
CC=ON UNIX=OFF RECLF=OFF TRCC=OFF CRLF=ON NAT=NO CONT=OFF
Translate with US_ENG_03
MODE=Stream STRU=File
150 File status okay; about to open data connection
226-Bytes sent: 15,479
Records sent: 184
Transfer Seconds: .22 ( 69K per second)
File I/O Seconds: .01 ( 1512K per second)
226 Closing data connection
QUIT
221 FTPDaemn closing control connection
```

Find Save As Print Entire conversation (1001 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Close Filter Out This Stream

# PASSWORT SCHUTZ

## Passwörter

Was ein sicheres Passwort ist:

*Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 157*

*Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 157*

*Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 157*

Passwörter sind im z/VSE normalerweise nur 8 Stellen lang, es sei  
Denn man verwendet LDAP Anmeldung- dann bis zu 64 Stellen.

Passwörter sind normalerweise in Uppercase und bestehen aus  
Buchstaben, Ziffern und Sonderzeichen.

Sind diese denn sicher ?



# CESN DATA

CESN:

SignOn to CICS

Alles geheim - da  
keine Anzeige im  
3270 erfolgt ?

```
Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
Signon to CICS APPLID CICSTEST

VSE/ESA CICS2

Type your userid and password, then press ENTER:

  Userid . . . . masn
  Password . . . .
  Groupid . . . .
  Language . . . .

New Password . . . .

DFHCE3520 Please type your userid.
F3=Exit

MA b 11/032
Verbindung zum fernen Server/Host 192.168.3.1 aufgebaut über LU/Pool LATNT202 und Anschluss 5023. \\PSEVER\lexmark Optra Lxi EIN LPT1:
```

# CESN USER/PASSWORD

Nicht falls man  
EBCDIC Hex lesen  
kann !

Geht aber auch  
im Klartext . . .

Follow TCP Stream

Stream Content

..... 'A&CESN.....' <'"..ZMASN.<9GEHEIM... ..' cqtF.....!'...\$v....."....|

Hier steht die UserId und das Passwort !

Find Save As Print 192.168.197.40:6303 --> 192.168.3.1:htuilsrv (91 bytes) ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help Close Filter Out This Stream

Internet Protocol, Src: 192.168.197.40 (192.168.197.40), Dst: 192.168.3.1 (192.168.3.1)  
Transmission Control Protocol, Src Port: 6303 (6303), Dst Port: htuilsrv (5023), Seq: 23, Ack: 754, Len: 26  
Data (26 bytes)  
data: 000000001E7D4C7F1148E9D4C1E2D5114CF9C7C5C8C5C9D4...

0000 00 a0 f9 10 59 ea 00 22 18 22 05 5a 08 00 48 00 .Y."#Z.E.  
0010 03 01 18 9f 13 9f 7f 11 05 be 60 c9 7c 9f 50 18 ..b..>T..P.  
0020 f3 c3 49 af 00 00 00 00 00 00 18 78 4c 7f 11 48 ..I...:..L..P.  
0030 00 00 01 c7 c5 c8 c5 c9 d4 ff ef ..:..:..:..:..

d4 c1 e2 d5 = 'MASN' | c7 c5 c8 c5 c9 d4 = 'GEHEIM'

Data (data.data), 26 bytes | Packets: 83 Displayed: 29 Marked: 0 Dropped: 0

# EMAIL IM ZVSE TRACE

- ¥ Wie bei IPTRACE dokumentiert, kann Email Traffic im VSE aufgezeichnet und anschließend von Wireshark ausgewertet werden.

Dieser Text stammt aus  
der HTML Dokumentation:  
~/doc/ipTraceTool.html

How to take a trace

Enter the following commands on your VSE console:

MSG xx (xx = partition ID of target TCP/IP partition)

DEFINE TRACE,ID=xxxx, IPADDR=ipaddr-of-target-system

--> recreate the problem

DUMP TRACES SEGMENT NEW

DELETE TRACE,ID=xxxx

Download the SYSLST output containing the trace data to your PC in ASCII format.

Now you can use the IP Trace Tool to convert and view this trace in Wireshark.

Note: The trace data is taken in the TCP/IP partition GETVIS.

# EMAIL NOCH EINFACHER IM KLARTEXT

Email von VSE

mit Anhang

```

Follow TCP Stream
Stream Content
UCAT220          C KSDS 2003.065    0 91%  1%  0%  0%  0% ** INDEX LEVELS > 2  98
TXTVSM . DATA  D   170  170  2048  64  0  21  0  5  1  23
VSAM . CATALOG . BASE . INDEX . RECORD  I    0    64    3  26592  1174405122  945  980  33

UMSATZ . ZWIBER . K2101          C ESDS 2001.061  2001.068  99%  0%  0%  0%  59% ** ZU GROSS >  50 %
TA1040D0 . VSAMDSET . DFD01061 . TB579439 . TA1040D0  D  4080  4080  8192    0  90    1  13

VORLAUF . KARTE . UMSATZ          C ESDS 2001.059  2001.066  99%  0%  0%  0%  96% ** ZU GROSS >  50 %
T959E863 . VSAMDSET . DFD01059 . TB576DB0 . T959E863  D  4080  4080  4096    0  24    1  13

VSE260 . CPGWKL . TEMP            C KSDS 2007.222    0 98%                ** NO . EXTENTS >  3
VSE260 . CPGWKL . DATA . TEMP    D   100  2040  2048  40  0  126  19636  10  23
VSE260 . CPGWKL . INDEX . TEMP    I    0  2553  2560  40    17    20  2  2  23

XXX . ZENTRAL . ARTIKEL . STAMM . KSDS  C KSDS 2006.072  1999.366  99%  0%  0%  0%  75% ** ZU GROSS >  50 %
XXX . ZENTRAL . ARTIKEL . STAMM . KSDS . . D         406  406  4096  7  0  12  100  1  23
XXX . ZENTRAL . ARTIKEL . STAMM . KSDS . . I          0  505  512  7  49    3  1  2  23

ZSART          C KSDS 1998.114    0 98%  0%  0%  0%  80% ** ZU GROSS >  50 %
ZSART . DATA  D   200  200  2048  7  0  126  94  1  23
ZSART . INDEX  I    0  1529  1536  7  26    1  1  1  23

CLUSTER - TOT          93.
EOJ CPG                DATE 03/01/2011, CLOCK 12/34/22, DURATION 00/00/01
-----_C73CF06A4CD09000==_--
.
250 2.6.0 <C73CF06A4CD09000@LWSERVER03> Queued mail for delivery
QUIT
221 2.0.0 lattwein.de service closing transmission channel|

Find Save As Print Entire conversation (16763 bytes)
 ASCII  EBCDIC  Hex Dump  C Arrays  Raw
Help Close Filter Out This Stream
  
```

# CICS TRANSACTION DUMP

Name/

Password

im CICS DUMP

Auch im CICS Transaction DUMP können UserId's und Passwörter im Klartext stehen.

Deshalb Vorsicht, wenn man Dumps weiterreicht oder ausgedruckt jemandem zur Ansicht gibt.

```
TRANSACTION STORAGE-USER24                ADDRESS 00681770 TO 0068276F    LENGTH
00000000  C2F0F0F2 F0F7F9F2 85000000 00000000 000F5DD2 11D4E3C8 D7D411D5 F3C7
00000020  C5C9D400 00000000 00000000 00000000 00000000 00000000 00000000 0000
00000040  00000000 00000000 00000000 00000000 00000000 00000000 00000000 0000
00000060  LINES TO 00000B20 SAME AS ABOVE
```

```
1770 TO 0068276F    LENGTH 00001000
DD2 11D4E3C8 D7D411D5 F3C7C5C8  *B0020792E.....)K.MTHPM.N3GEH* 00681770
000 00000000 00000000 00000000  *EIM.....* 00681790
000 00000000 00000000 00000000  *.....* 006817B0
```

Das sind Terminal Input Daten – das kann auch in der Common Area oder in Temporary Storage Records stehen.

# CICS TRANSACTION DUMP

Positiv:

Bei CEDF wird das  
Password  
unterdrückt!

¥ Nur bei CEDF wird das Passwort beim EXEC CICS SIGNON unterdrückt.

¥ When processing an EXEC CICS SIGNON command, CEDF suppresses display of the password value to reduce the risk of accidental disclosure.