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

AGENDA

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

E-MAIL UND VERSCHLÜSSELUNG

- 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 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

- 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

- 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

- Alles gute Gründe E-Mails zu verschlüsseln.

  Aber -

Warum macht das niemand ?

E-MAIL UND VERSCHLÜSSELUNG

- 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.

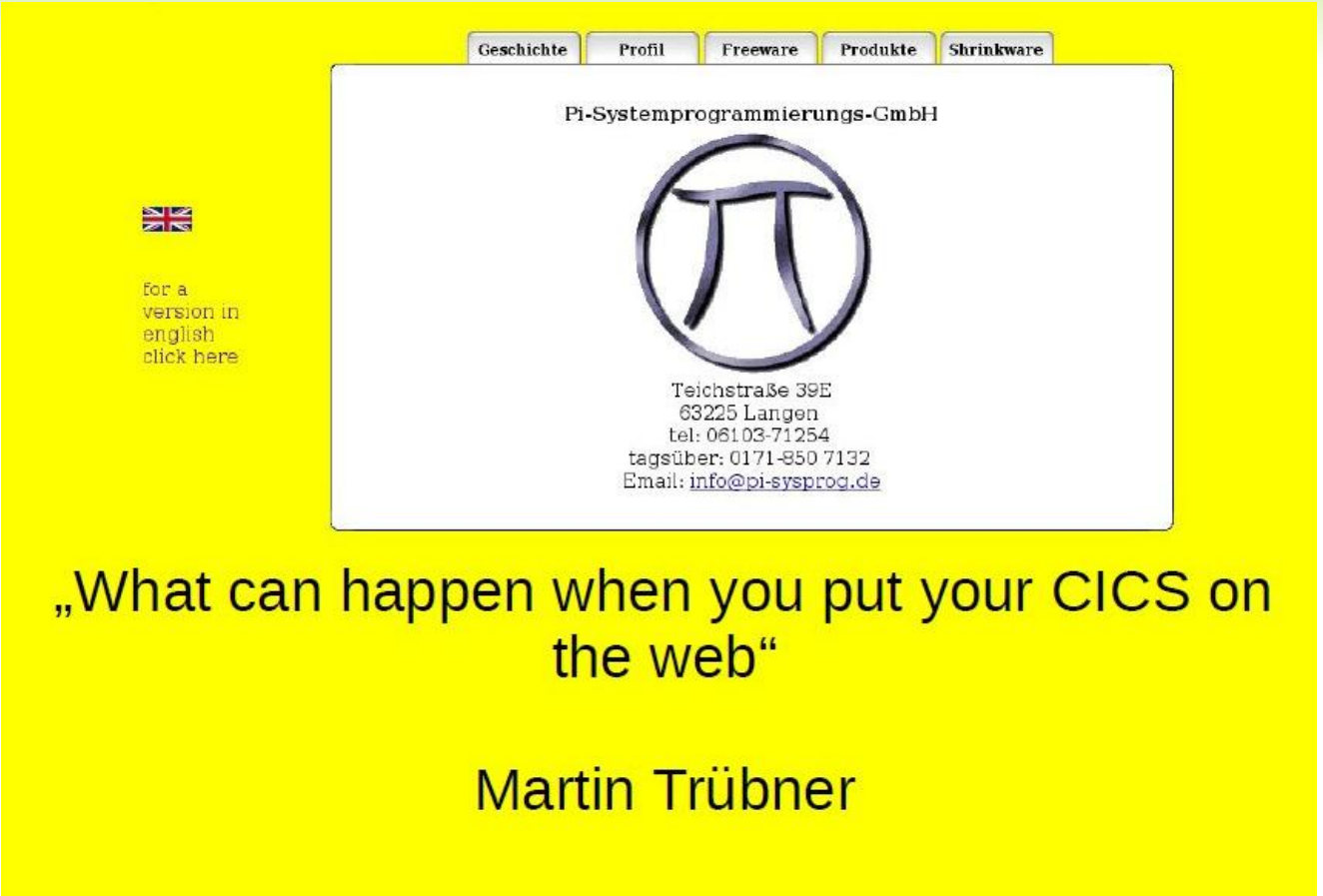
VORTRAG: MARTIN TRÜBNER 2010

Initiator: Martin
à

Mal sehen ob es

noch mehr CICS

Websites gibt

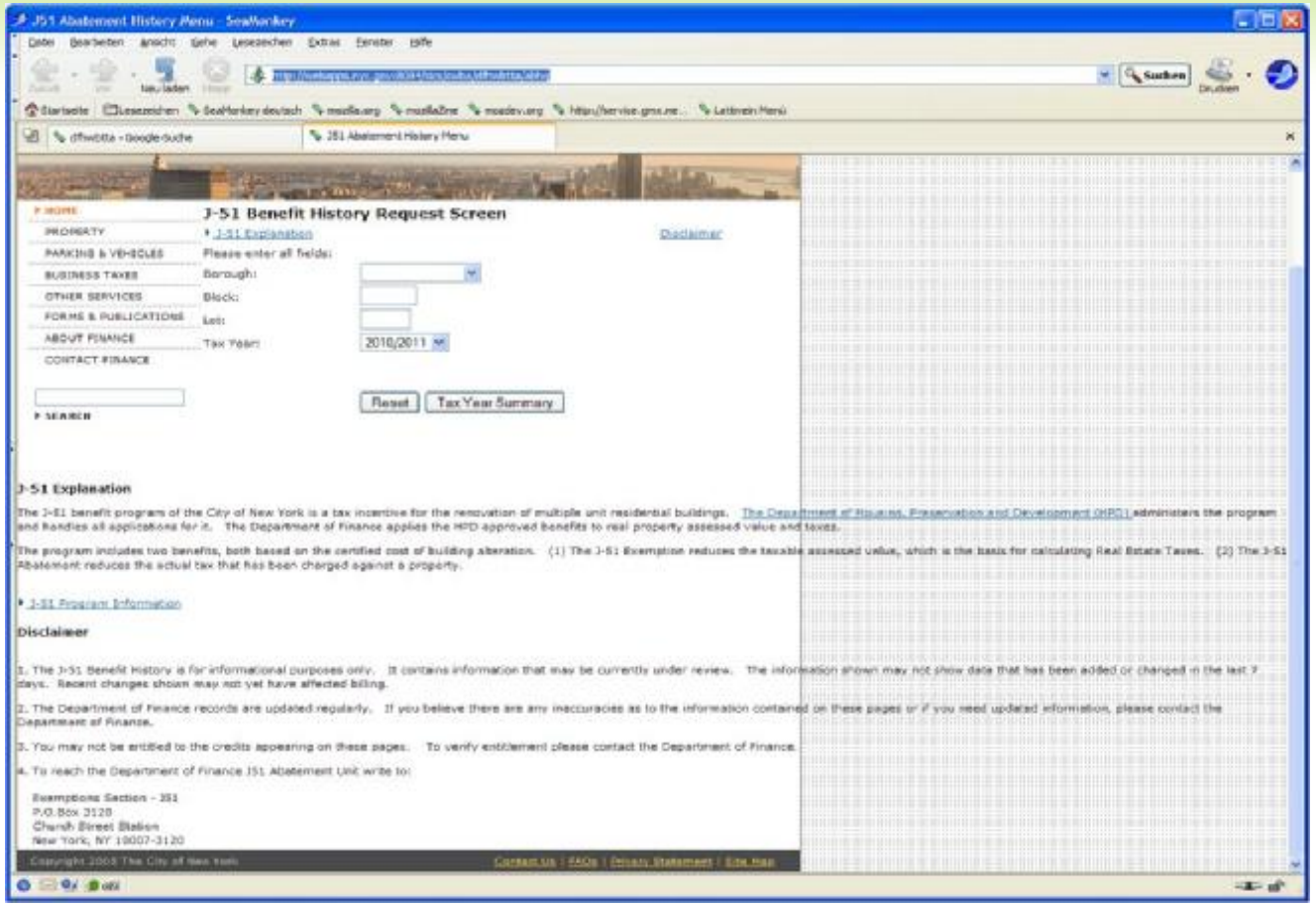


Auf der Suche nach VSE Servern im WWW

Reichlich, wenn man nach CICS/CWBA googelt.

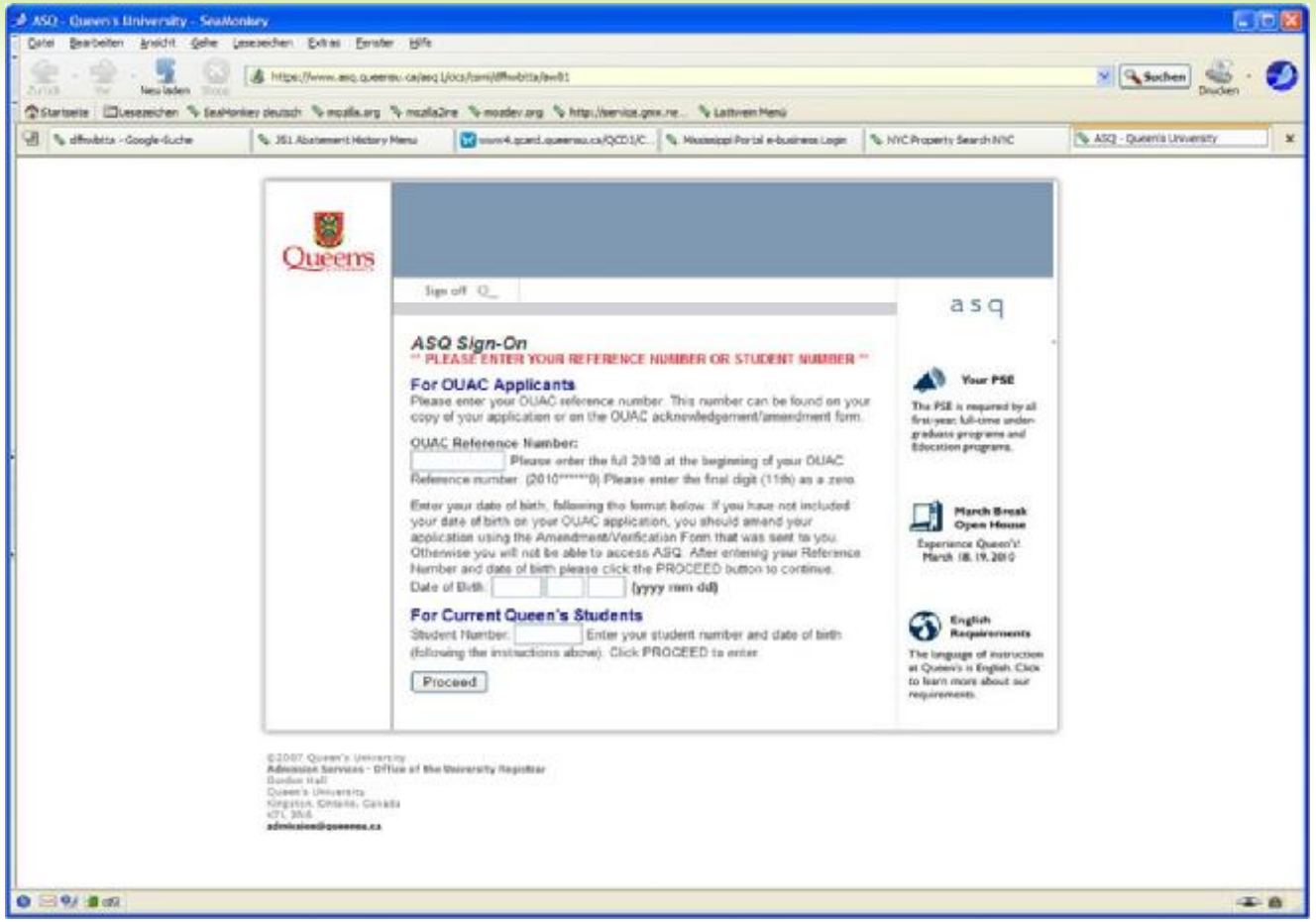
- Nur einige der 106000 Treffer bei CWBA oder 3660 Treffer auf DFHWBTTA
- http://webapps.nyc.gov:8084/cics/cwba/dfhwbtta/abhq
- http://xmarks.com/site/www4.qcard.queensu.ca/QCD3/CICS/CSMI/DFHWBTTA/CW01
- https://www.state.ms.gov/taxtitle/cics/dfhwbtta/TNIQ
- https://accounts.swbno.org:8084/cics/cwba/dfhwbtta/wa00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

NY Gov Application

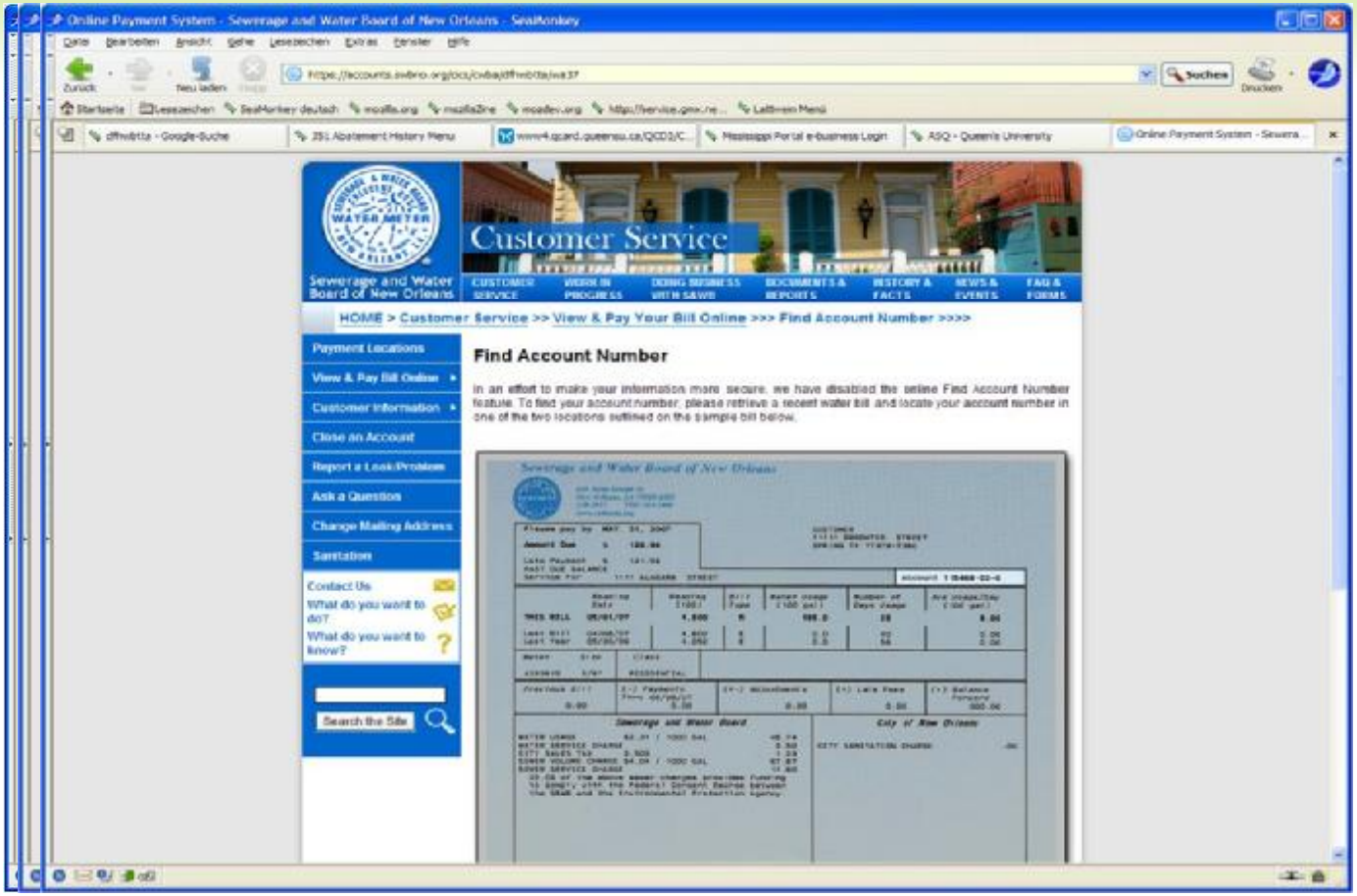


WWW.STATE.MS.GOV

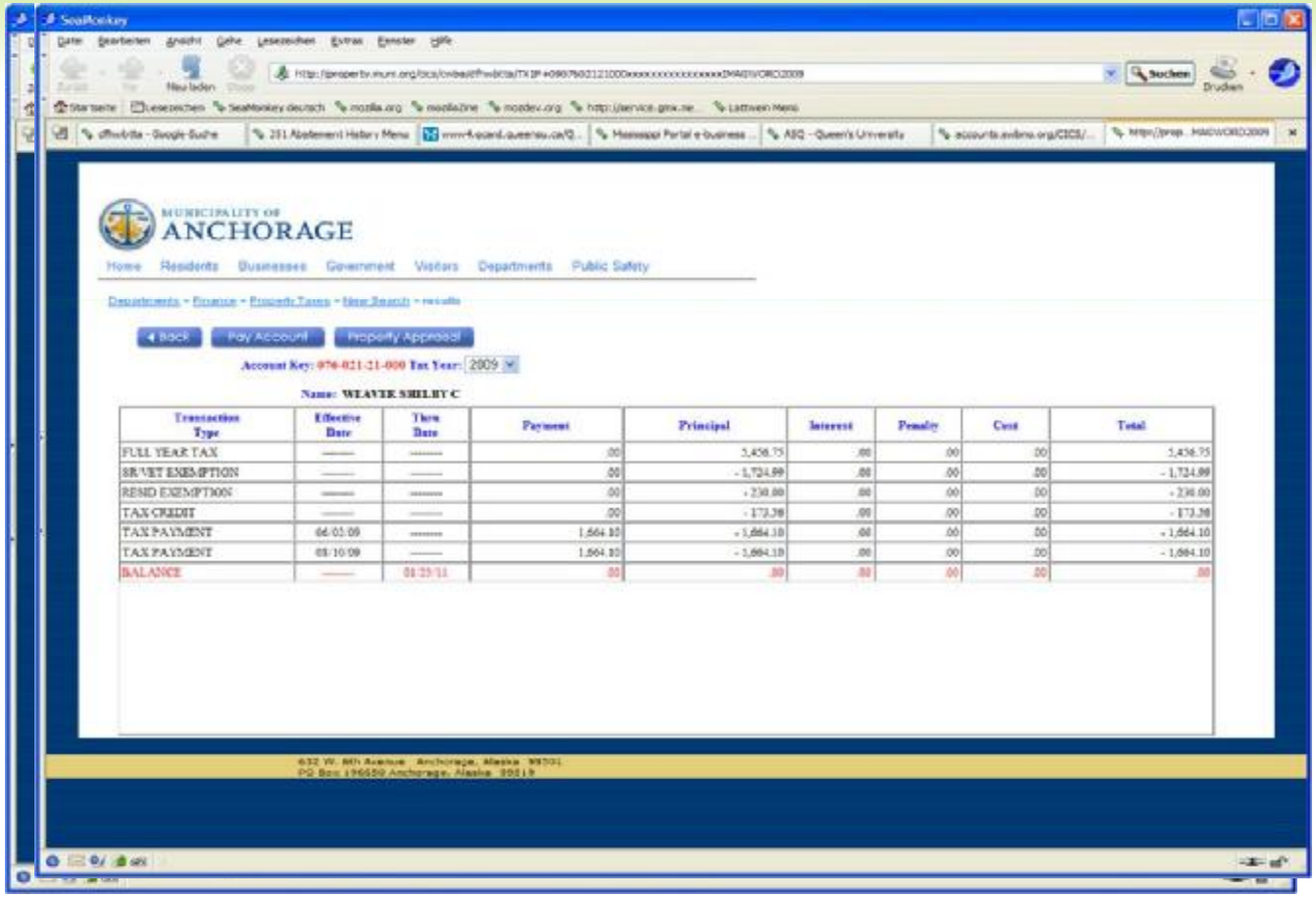
QUEEN UNIVSERSITY CA



NEW ORLEANS: ACCOUNTS.SWBNO.ORG:8010



MUNICIPALITY OF ANCHORAGE



State of Nevada

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 normaler-weise 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

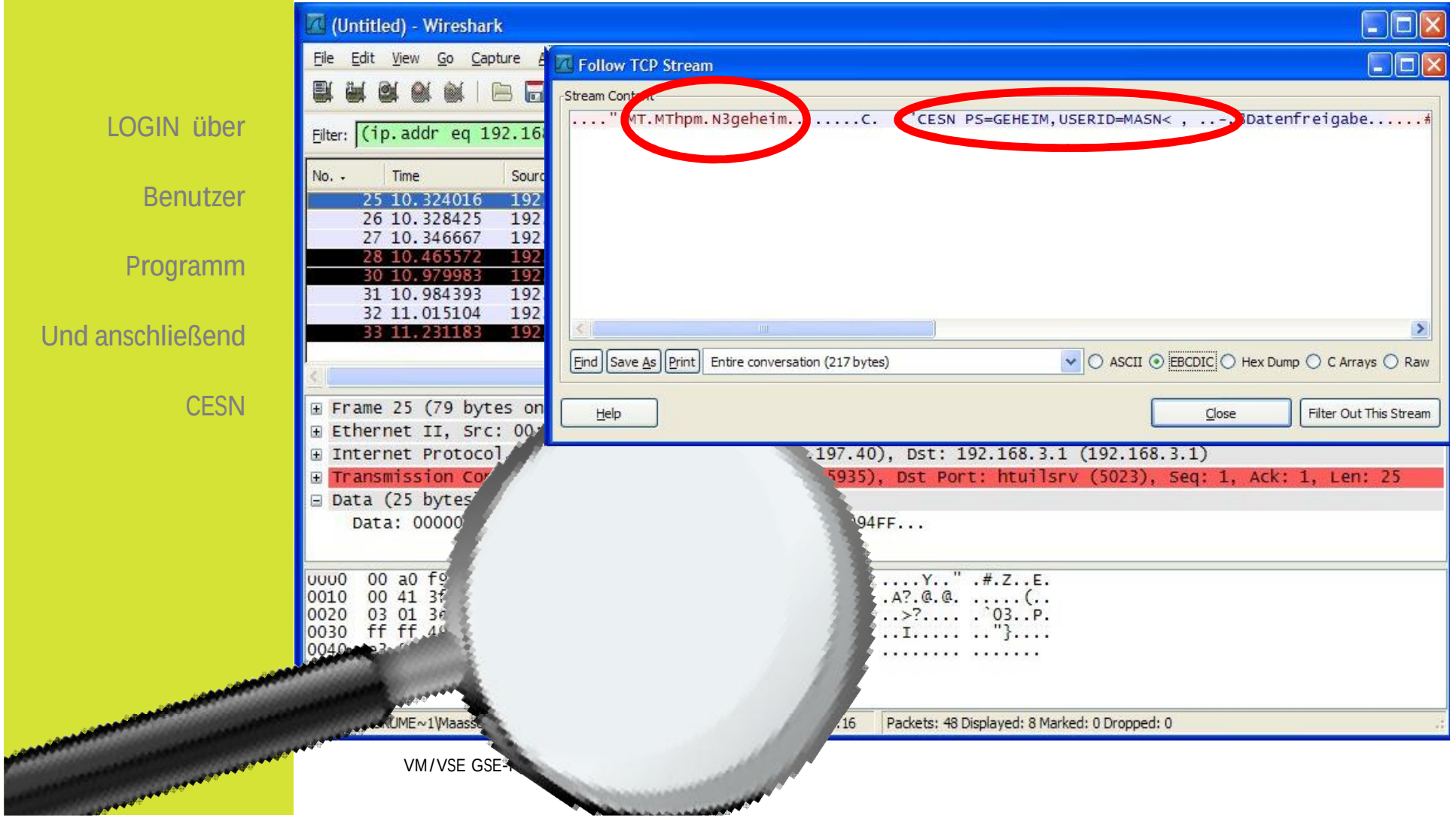
LOGIN über

Benutzer

Programm

Und anschließend

CESN



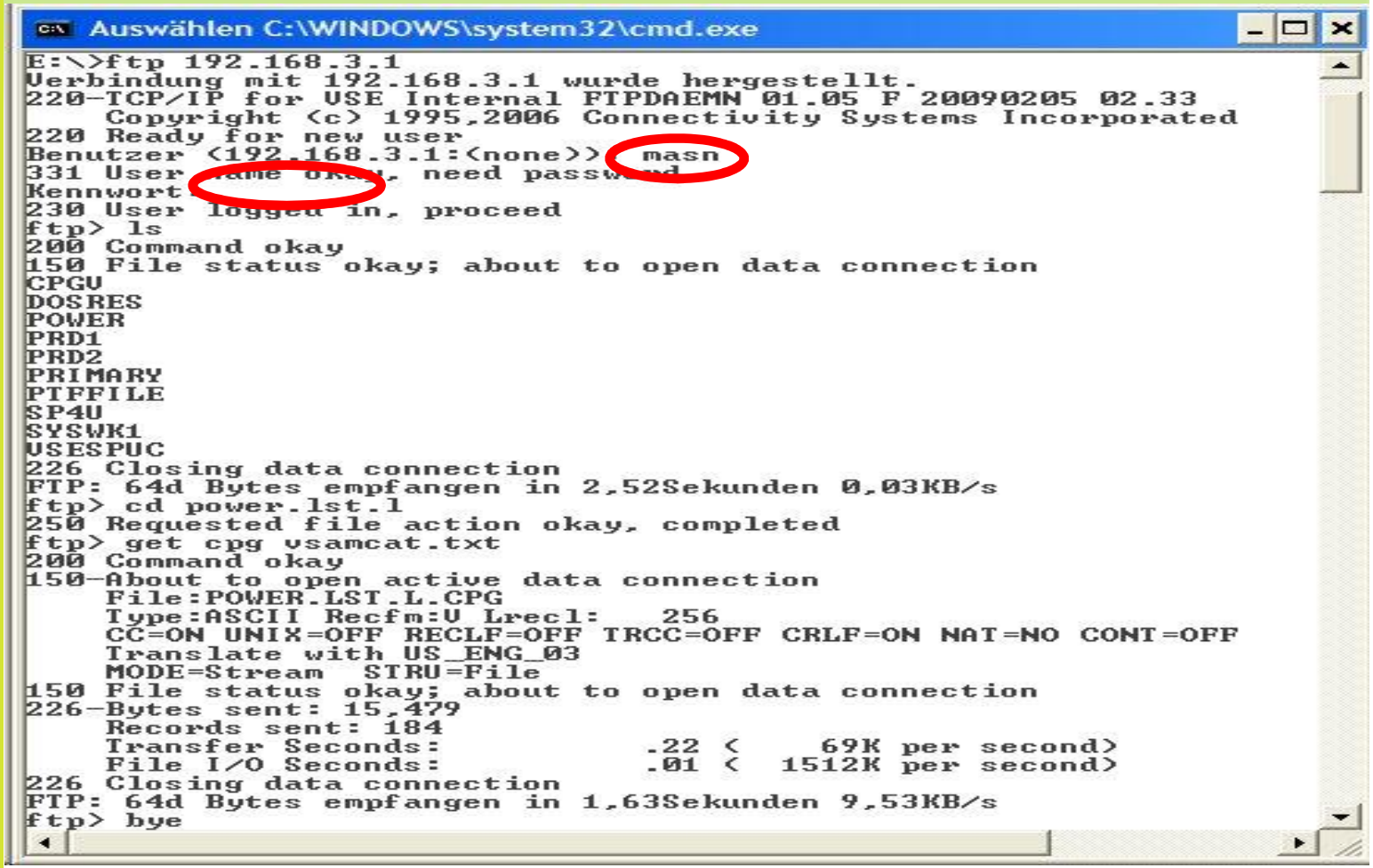
FTP

Command Fenster

mit FTP zum

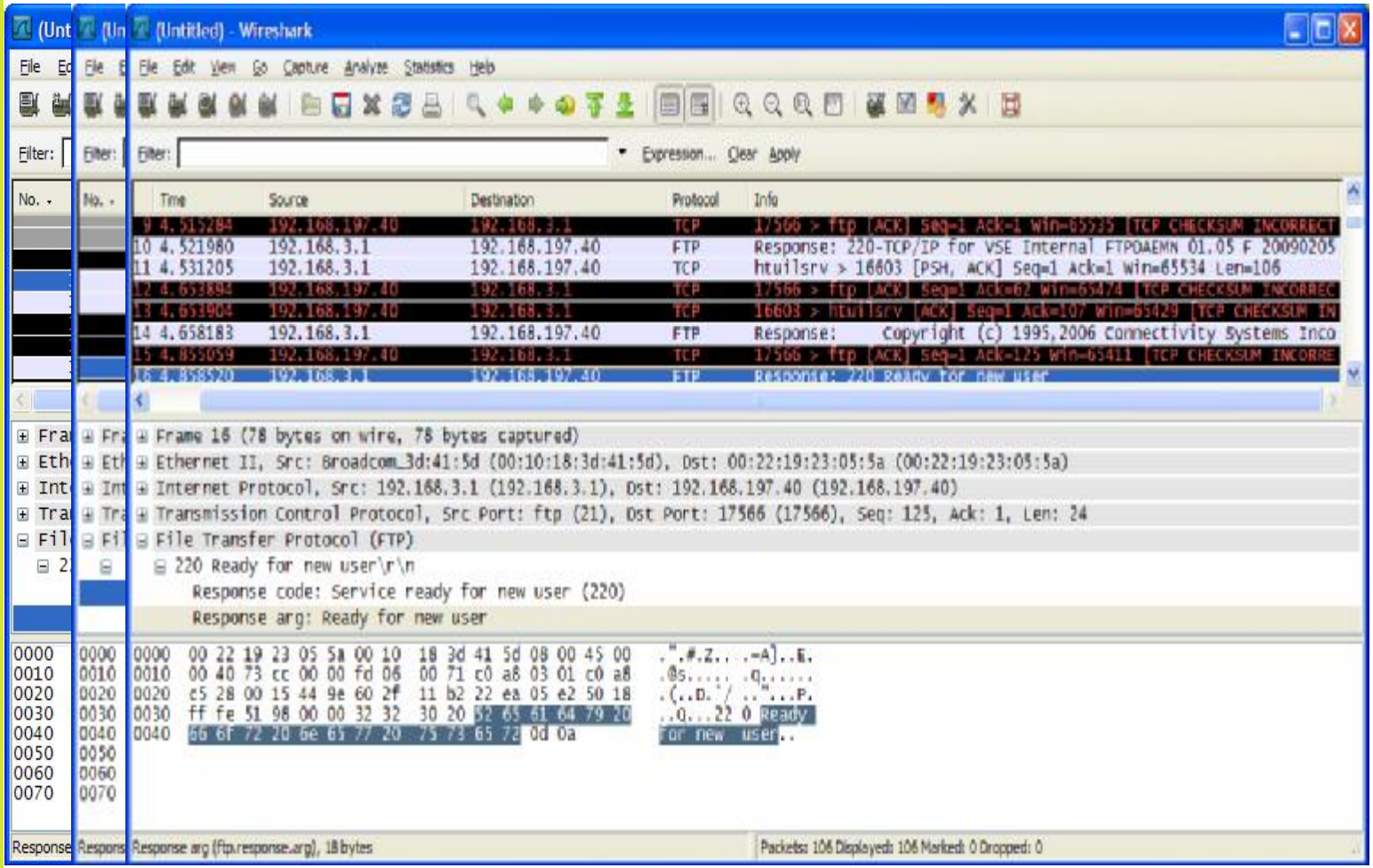
z/VSE.

TCPIP 1.5.F



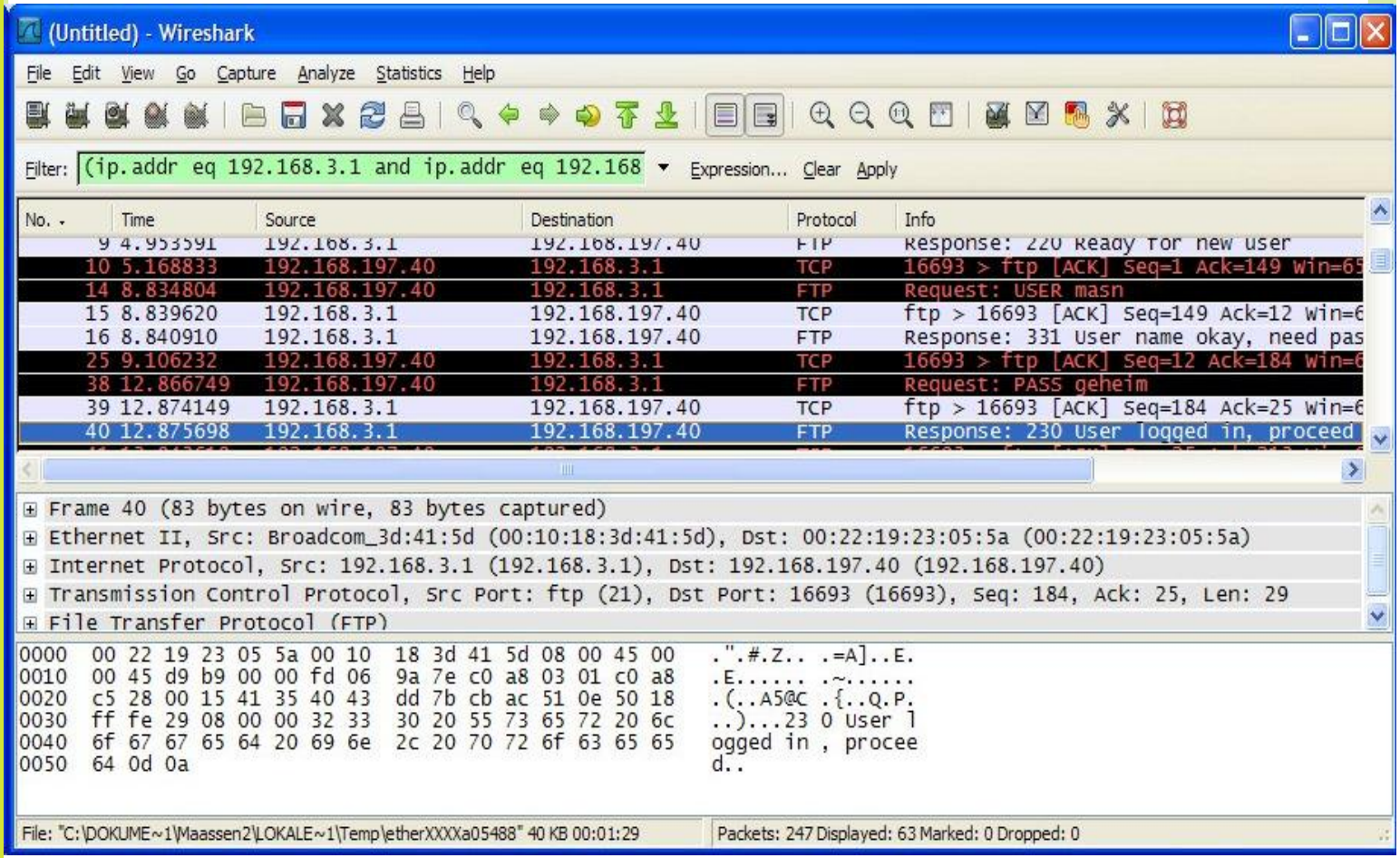
FTP DAEMON RESPONSE

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



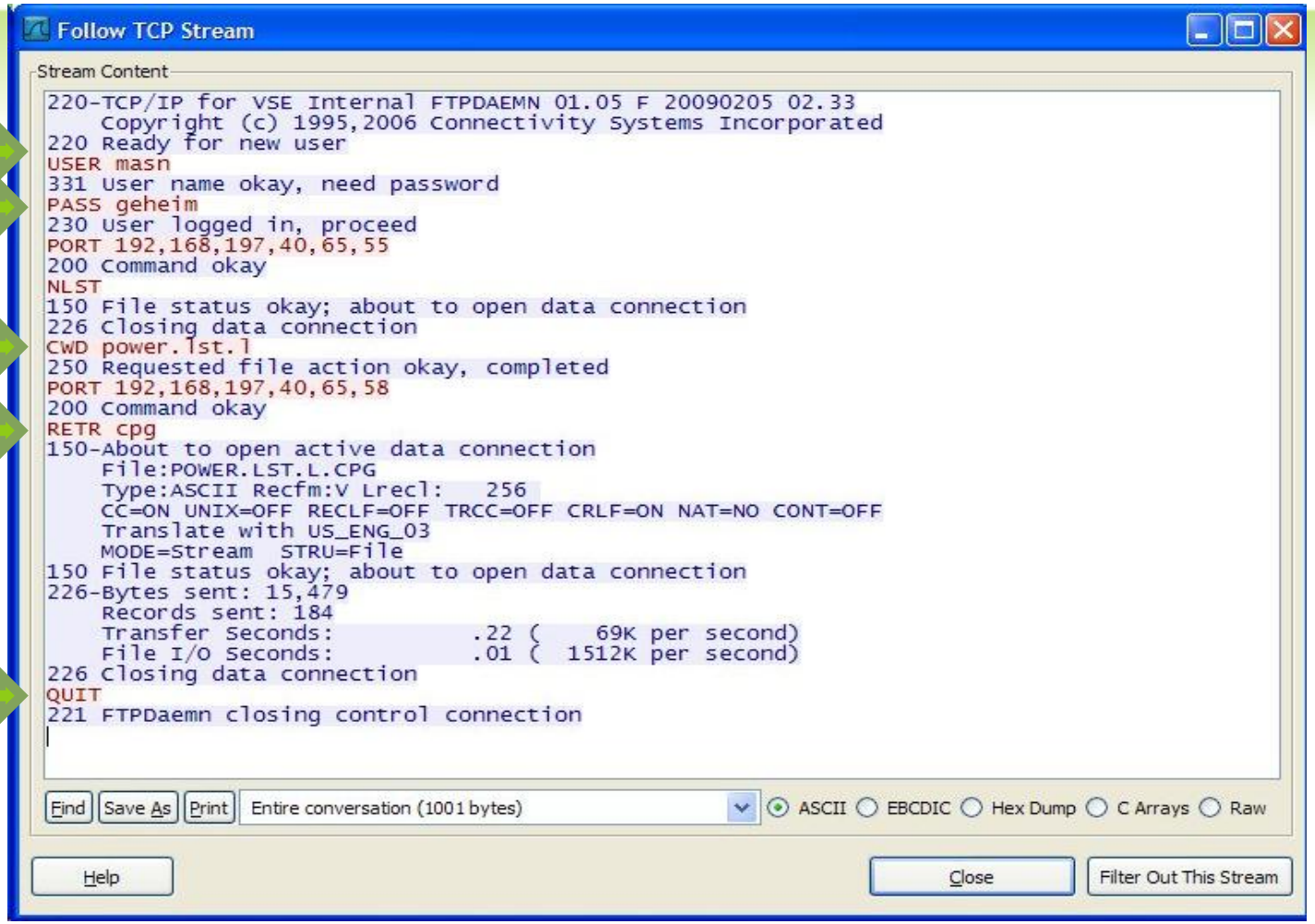
FTP USER MASN

Userid und Passwort im Klartext !



FTP Follow TCP Stream

FTP LS Data



PASSWORT SCHUTZ

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.

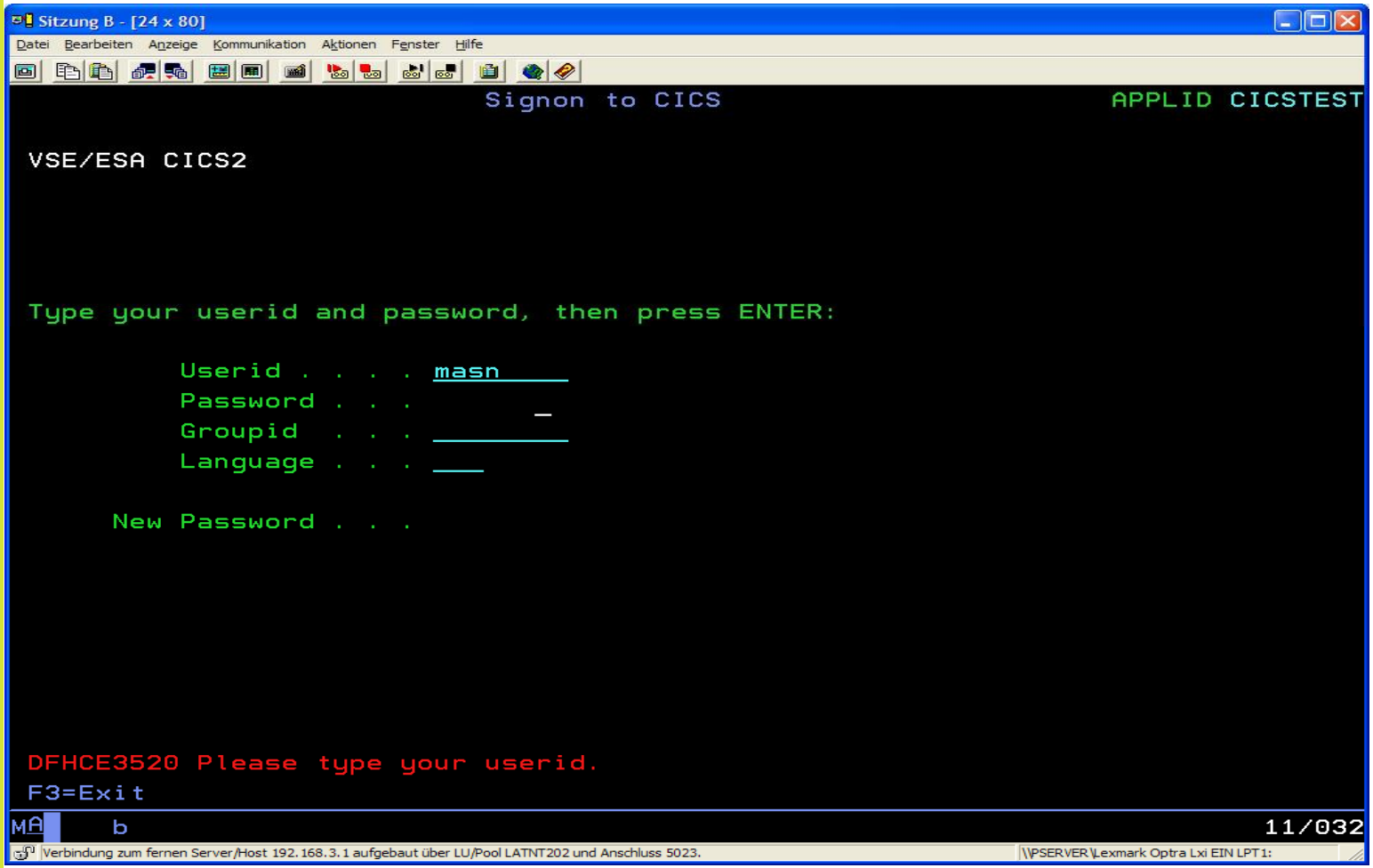
Sind diese denn sicher ?

CESN DATA

CESN:

SignOn to CICS

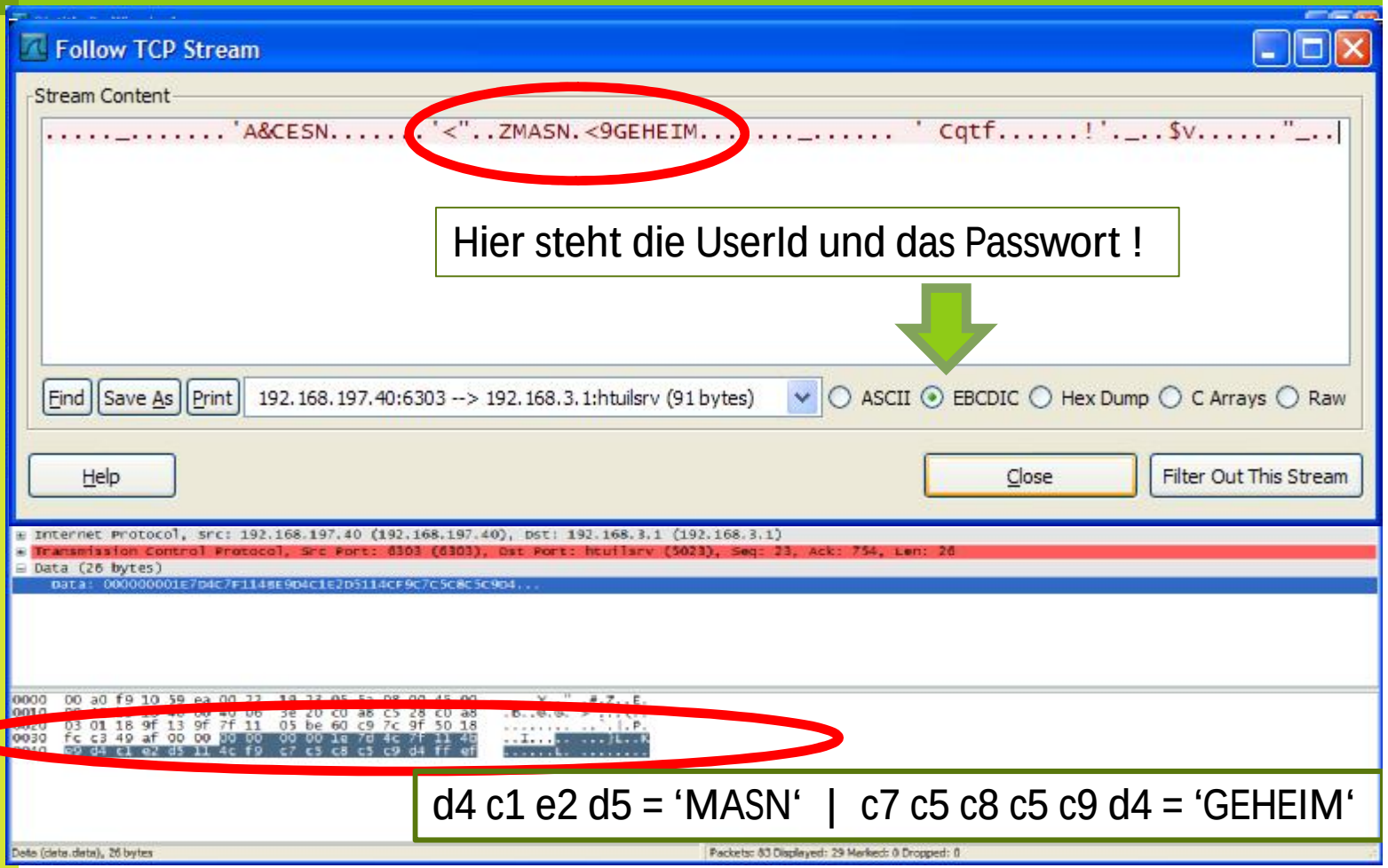
Alles geheim - da keine Anzeige im 3270 erfolgt ?



CESN USER / PASSWORD

Nicht falls man EBCDIC Hex lesen kann !

Geht aber auch im Klartext . . .



EMAIL IM zVSE TRACE

- Wie bei IPTRACE dokumentiert, kann Email Trafic 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:

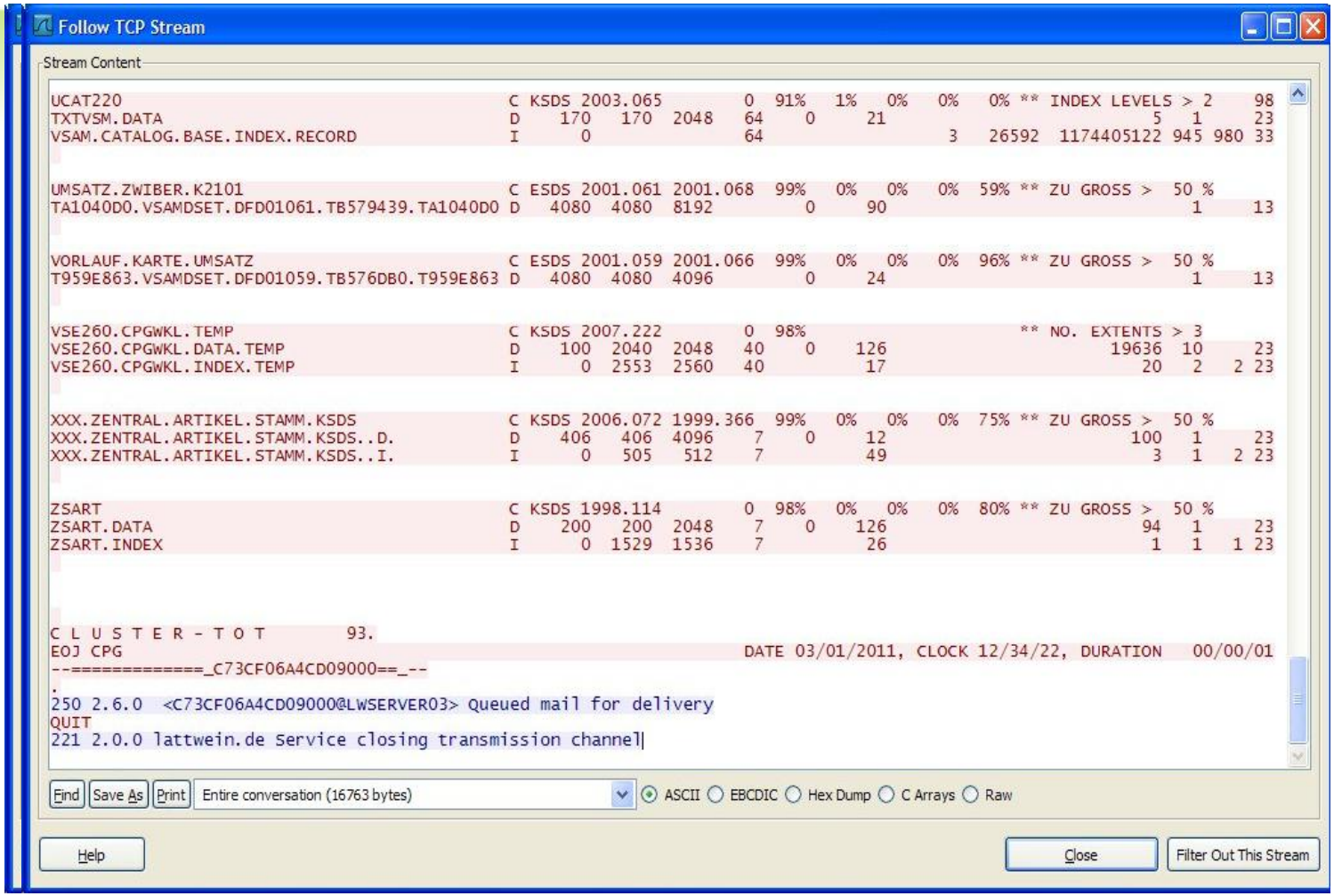
MSG xx (xx = partition ID of target TCP/IP partition)
DEFINE TRACE,ID=xxxx, IPADDR=ipaddr-of-target-system
--> recreate the problem
DUMP TRACES SEGMENT NEW
DELETE TRACE,ID=xxxx
Download the SYSLST output containing the trace data to your PC in ASCII format.
Now you can use the IP Trace Tool to convert 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



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.