SMTP

Vortrag von Julius Hülsmann

Seminar 392023 Internet-Protokolle bei
Herrn Dr. Alexander Sczyrba
Herrn Dipl.-Inform. Jan Krüger

SMTP Überblick

- **S**imple **M**ail **T**ransfer **P**rotokoll
- Internetprotokoll
- Internet Standard für Email-Übermittlung

SMTP Überblick

- Geschichte
  - Entstanden in 1980er Jahren
  - RFC 821 (Jonathan Postel 1982)
  - RFC 5321 (aktuell von Oktober 2008, mit **E**xtended **SMTP**)

Vorteile Damals

- „Store and Foreward Protocol“
- Einfach zu benutzen
- Flexibel

Anforderungen an Mailversand

- **Composition:** Möglichkeit, Mails zu erstellen
- **Transfer:** Übermittlung der Mail
  - automatisch
  - Bereitstellen von Lösungsansätzen für Sonderfälle
- **Reporting:** Weitergabe von Informationen über Sendestatus an den Absender
  - Eingangsbestätigung, Lesebestätigung, Fehlermeldung und Andere

Beteiligt am Mailversand

- **Mail User Agents**
  - Komposition und Absenden der Nachricht an SMTP Relay Server
- **SMTP Relay** Server
  - Annahme und Weiterleitung von Mails

Wie die SMTP Server untereinander kommunizieren

KOMMUNIKATION

Kommunikation: Anfragen

- Minimaler SMTP Befehlssatz, wichtige Befehle
  - **HELO** [Identität]
    - Der Sender teilt Empfänger Identität (nach SMTP in Form des *Full Qualified Domain Name* (FQDM) mit
  - **MAIL FROM**: <[Adresse]>
  - **RCPT TO**: <[Adresse]>
  - **DATA** \n [Email Text] \n.\n
  - **QUIT**

Kommunikation: Anfragen

- Minimaler Befehlssatz
  - RSET
    - Bereits eingegebene Daten verwerfen
  - VRFY <[Adresse]>
    - Überprüft , ob die eingegebene Empfängeradresse gültig ist
  - NOOP („No operation“)
    - Nur Testantwort des Servers

Kommunikation: Antworten

Repy codes	*0*	*1*	*2*	*5*	
1**					Kein Fehler, abgeschlossen Weitere Eingabe notwendig
2**					Kein Fehler, abgeschlossen Weitere Eingabe optional
3**					Kein Fehler, nicht abgeschlossen, Weitere Eingaben notwendig
4**					Serverseitiger temporärer Fehler, Eingabe wiederholen
5**					Clientseitiger Fehler, Eingabe nicht korrekt
	Syntax	Allge-mein	Verbin-dung	Status	

Livepräsentation

Präsentation Einwahl via Telnet

@bonnie:~$ telnet smarthost.techfak.uni-bielefeld.de 25
Trying 2001:683:504:2014:ffff::24…
Connected to smarthost.techfkak.uni-bielefeld.de
Escape character is `^]`.
220 smarthost.techfak.uni-bielefeld.de ESMTP Postfix

HELO identity
250 smarthost.Techfak.Uni-Bielefeld.DE
MAIL FROM:<a1@ausgedacht.de>
250 2.1.0 Ok
RCPT TO:<jhuelsmann@techfak.uni-bielefeld.de>
250 2.1.5 Ok

Präsentation Einwahl via Telnet

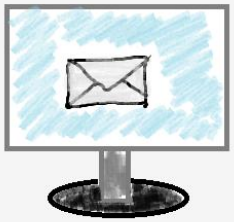
DATA
354 End data with <CR><LF>.<CR><LF>
From: <not_exists@ausgedacht.de
To: <not_exists2@ausgedacht.de>
Subject: Betreff
Message-ID: <0000000@techfak.uni-bielefeld.de>
In-Reply_to: <123456@example.com>
Hier ist Platz für den Inhalt der Mail.
.
250 2.0.0 Ok: queued as 34B9A8000F
QUIT
221 2.0.0 Bye
Connection closed by foreign host

Lebenslauf einer Email

ABLAUF DES EMAIL VERSANDS

Mail User Agent

MUA
Mail user Agent



Mail User Agent

- Erstellt Email nach ***Nachrichtenformat***, festgelegt in SMTP
  - **Header**
    - Notwendig: ***From*** und ***To***
    - Optional: Subject, Reply To, Date, mailID, User Agent uvm.
  - **Body**
    - Text und Anhänge

MUA Header Beispiel

X-Mozilla-Status:	*0002 (erfolgreich versendet)*
X-Mozilla-Status2:	*10000000 (Dateien an Mail angehängt)*
Content-transfer-encoding:	7BIT
Content-type: text/plain;	CHARSET=US-ASCII
X-EnvFrom:	from@techfak.uni-bielefeld.de
Message-id:	<534FF67D.1030802@uni-bielefeld.de>
Date:	Thu, 17 Apr 2014 17:42:53 +0200
From:	**displayNamen@techfak.uni-bielefeld.de**
To:	**jhuelsmann@techfak.uni-bielefeld.de**
Subject:	tea

User Agent zu Mail Submission Agent

User Agent zu Mail Submission Agent

- Kommunikation
  - auch PIPING genutzt (darauf gehen wir nicht ein)
  - SMTP
- Ablauf
  - MUA sucht Mailserver (z.B. host gmx.mi)
  - Antwort: *Handled by mailserver x* , Priorität (z.B.10)
  - SMTP Befehle

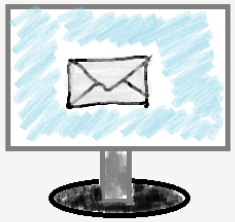
Submission - / Transfer Agent

Submission - / Transfer Agent

- MSA ***prüft*** ob alle ***Angaben*** korrekt sind
- Erstellt aus Header sog. **Envelope**
  - Enthält ***wichtige Infos*** für den *weiteren Versand der Email*
  - Wird editiert von zukünftigen Relays
- MSA reicht Mail incl. Header weiter zu MTA

Transfer Agent zu exchanger

MUA
Mail user Agent



MSA
Mail Submission Agent

MTA
Mail Transfer Agent

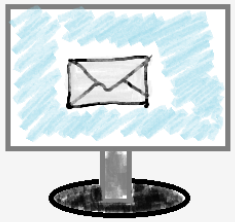
MX
Mail eXchange

Submission/Transfer Agent ->Mail eXchange

- MTA-> MX
  - Baut Verbindung auf
  - Reiht Mail in FIFO Queue ein
  - Zustellungsversuch
    - *Scheitern*: noch mal in FIFO, ggf. Fehlermail (von MTA gesendet)
    - *Erfolg*: Kommunikation wie im Beispiel via telnet präsentiert (Port 25 bzw. 465, 587)

Mail Exchange

MUA
Mail user Agent



MSA
Mail Submission Agent

MTA
Mail Transfer Agent

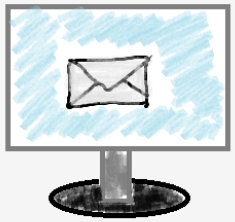
MX
Mail eXchange

Mail Exchange

- Annahme der Mail (incl. Header)
- Schaut ob alles korrekt ist
  - *Andere Empfängerdomain*: theoretisch Weiterleitung an MXer anderer Domain (**open Relay**)
  - *Eigene Domain* und alle *Angaben korrekt*: Zustellung der Mail an MDA

Mail Delivery Agent

MUA
Mail user Agent



MSA
Mail Submission Agent

MTA
Mail Transfer Agent

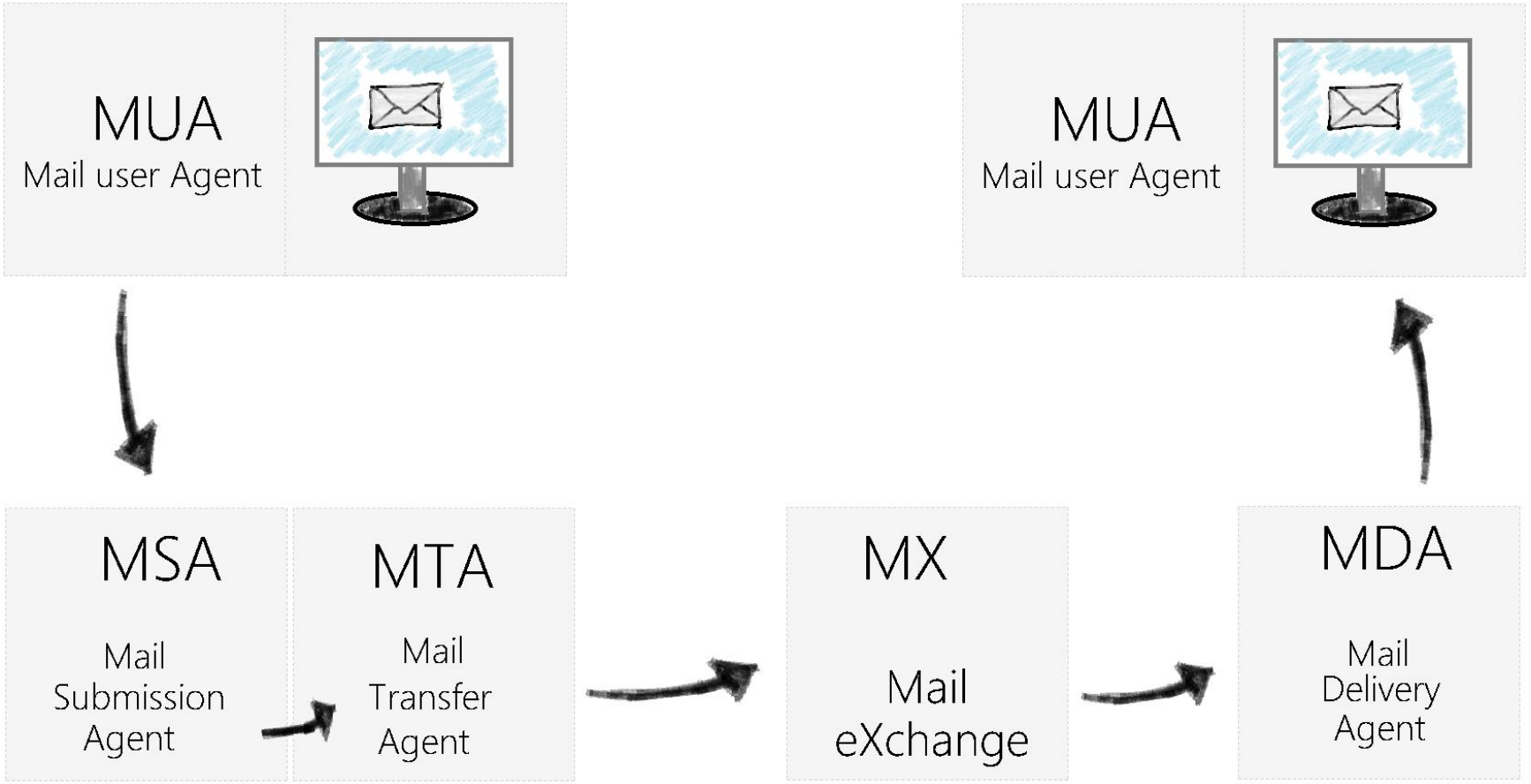
MX
Mail eXchange

MDA
Mail Delivery Agent

Mail Delivery Agent

- Zustellungsversuch
  - *Fehler*: Kenne User nicht / Postfach voll etc.
    - „Zurückbouncen“ der Nachricht an MTA, der dann wiederum eine Informations- Email zurückschickt
  - *Erfolg*: User kann dann per POP3/IMAP/HTTP die Mails abrufen!

Gesamtbild


MUA
Mail user Agent
MUA
Mail user Agent
MSA
Mail Submission Agent
MTA
Mail Transfer Agent
MX
Mail eXchange
MDA
Mail Delivery Agent

Lebenslauf im Header

- Von einzelnen Relays werden Informationen in den Header geschrieben
- Header wird von Hinten nach Vorne gelesen
- Ist „per Hand“ analysierbar
- Scenario:
  - Mail von user@gmail.com
  - Mail an user@techfak.uni-bielefeld.de

Analyse

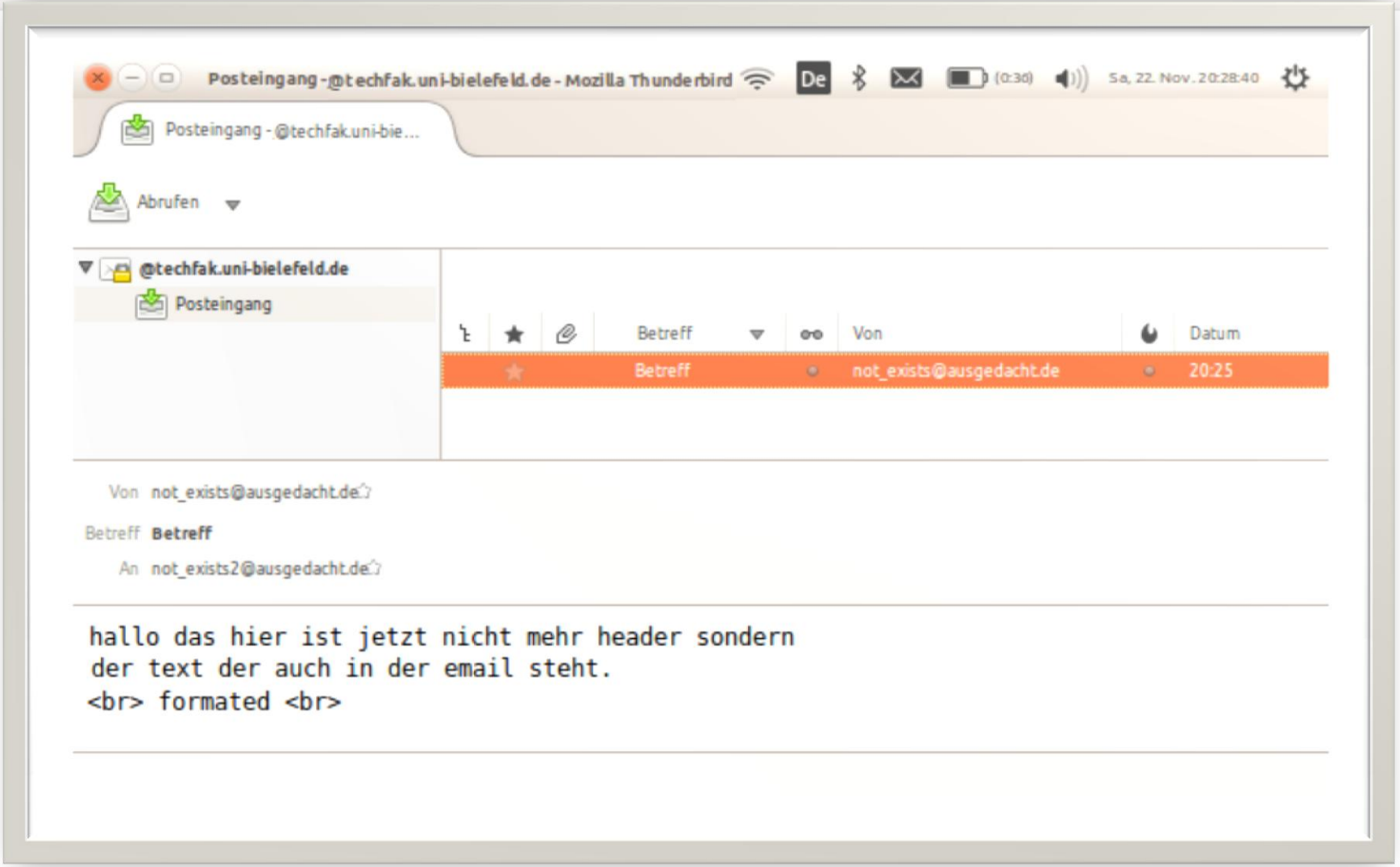
#	Delay	From *			To *
0	60 mins	ubi-1-234-89.dhcp.uni-bielefeld.de	→		mx17.freenet.de
1		mx17.freenet.de	→		mjail0.freenet.de
2	2 mins	localhost	→		mjail0.freenet.de
3		[195.4.92.140]	→		mout3.freenet.de
4	1 sec	mout3.freenet.de	→		mailin.techfak.uni-bielefeld.de
5		mailin.techfak.uni-bielefeld.de	→		imap.TechFak.Uni-Bielefeld.DE

https://toolbox.googleapps.com/apps/messageheader/analyzeheader

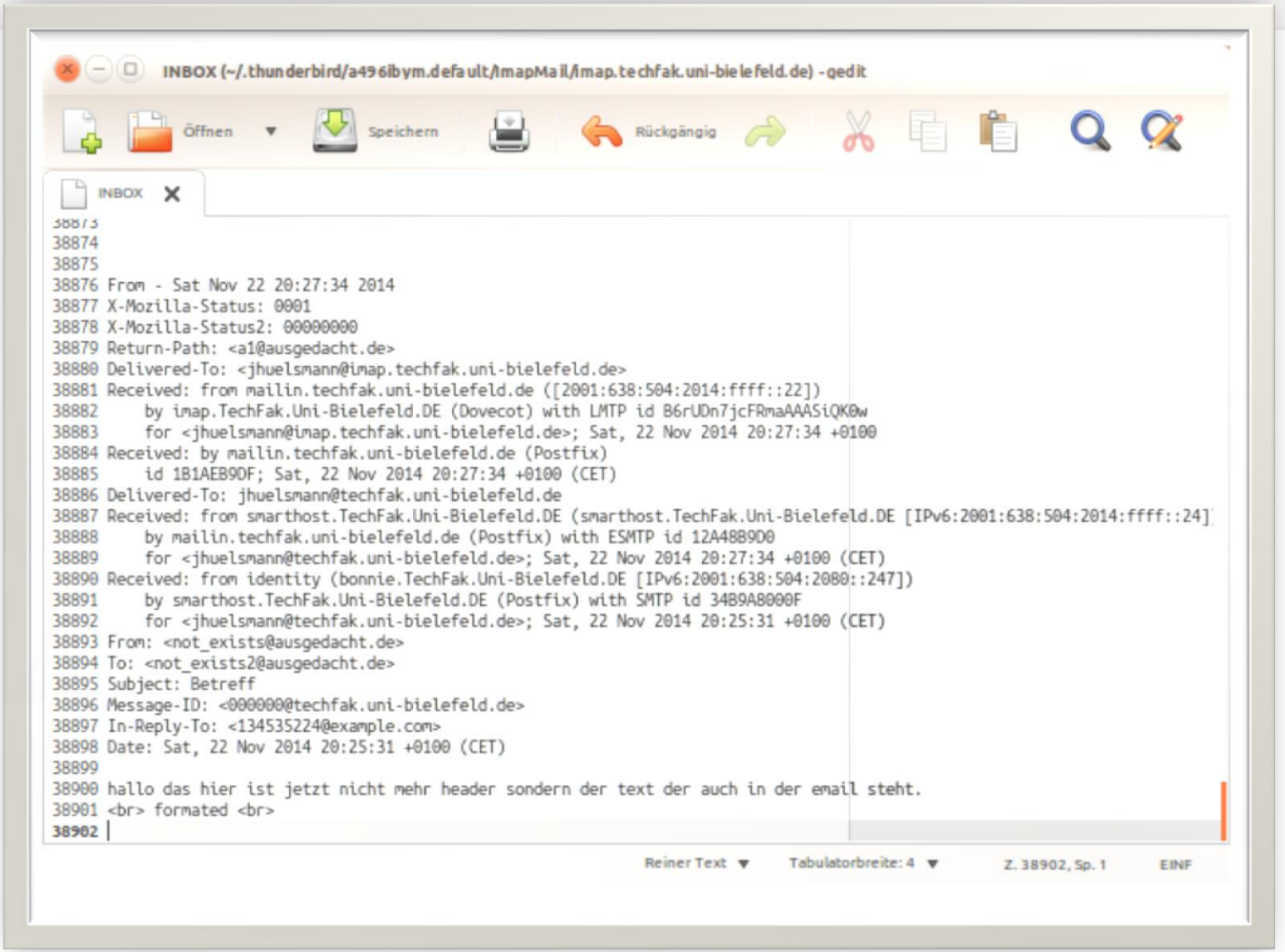
Die Grenzen von SMTP

INFORMATIONSMANIPULATION

Präsentation Mail Eingang



Präsentation Header



Worauf kann sich der Empfänger verlassen?

- Absender?
- Empfänger?
- Inhalt?
- Wegprotokoll?

Alle diese Daten können während der Übertragung abgeändert werden!

Warum trotzdem so entwickelt

- **Flexibel**
- **Einfach**

Trotzdem Datenintegrität nachbesserbar (nicht in SMTP definiert)

- PGP(*Public Key Infrastructure mit Diffie Hellman Schlüsselaustausch*)
- *Signatur mit privatem Schlüssel* für Senderintegrität

ESMTP

- Extended SMTP oder Enhanced SMTP
- Abwärtskompatibel
- Definiert in November 1995 in RGC 1869

ESMTP

- Ersetzt HELO durch EHLO
  - Antwort: 250 OK und Liste von Erweiterungen die unterstützt werden
- Gängige Erweiterungen
  - STARTTLS (secure SMTP over TLS)
  - 8BITMIME
  - DSN (Delivery status notification)
  - SMTP-Auth

Weiterführende Informationen

- Weblinks

  SMTP
  - http://tools.ietf.org/html/rfc821
  - http://www.kubieziel.de/computer/email.html
  - http://www.eyrich-net.org/mozilla/X-Mozilla-Status.html
  - http://www.elektronik-kompendium.de/sites/net/0903081.htm
  - http://www.daniel-rehbein.de/rfc2821.html
  - http://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
  - https://tools.ietf.org/html/rfc5321
  - http://wiki.dreamhost.com/Viewing_Full_Headers
  - https://toolbox.googleapps.com/apps/messageheader/analyzeheader

  Spam
  - http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches

Weiterführende Informationen

Authentifizierung:

- http://de.wikipedia.org/wiki/SMTP-Auth
- http://tools.ietf.org/html/rfc6409

ESMTP

- http://www.iana.org/assignments/mail-parameters/mail-parameters.xhtml (Liste von SMTP Erweiterungen)
- http://en.wikipedia.org/wiki/Extended_SMTP

Sonstiges

- http://en.wikipedia.org/wiki/Fully_qualified_domain_name

Danke für die
Aufmerksamkeit!