Arbeitsblatt – **SMTP** Klasse: Name:

**Arbeitsauftrag 1**

1. Markieren Sie im RFC und im nachfolgenden Text die SMTP-Befehle und Namen von Headerzeilen.
2. Erklären Sie die Bedeutung von HELO/EHLO, MAIL FROM, RCPT TO
3. Erläutern Sie den Beriff "Mail-Spoofing".

Auszug aus **RFC 2821: "Simple Mail Transfer Protocol"**, 2001, 79 Pages

4.1.1.1 Extended HELLO (EHLO) or HELLO (HELO)

These commands are used to identify the SMTP client to the SMTP server. […] The SMTP server identifies itself to the SMTP client in the connection greeting reply and in the response to this command.

A client SMTP SHOULD start an SMTP session by issuing the EHLO command. […]

These commands, and a "250 OK" reply to one of them, confirm that both the SMTP client and the SMTP server are in the initial state, that is, there is no transaction in progress and all state tables and buffers are cleared.

Syntax:

```
ehlo            = "EHLO" SP Domain CRLF
helo            = "HELO" SP Domain CRLF
```

[…]

4.1.1.2 MAIL (MAIL)

This command is used to initiate a mail transaction […] The argument field contains a reverse-path and may contain optional parameters.
[…]

Syntax:

```
"MAIL FROM:" ("<>" / Reverse-Path)
                 [SP Mail-parameters] CRLF
```

4.1.1.3 RECIPIENT (RCPT)

This command is used to identify an individual recipient of the mail data; […]

For example, […]

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<userc@d.bar.org>
```

[…]

4.1.1.4 DATA (DATA)

[…]

When the SMTP server accepts a message either for relaying or for final delivery, it inserts a trace record (also referred to interchangeably as a "time stamp line" or "Received" line) at the top of the mail data. This trace record indicates the identity of the host that sent the message, the identity of the host that received the message (and is inserting this time stamp), and the date and time the message was received. Relayed messages will have multiple time stamp lines. Details for formation of these lines, including their syntax, is specified in section 4.4.

## Aufbau und Zustellung einer E-Mail (Quelle, gekürzt: https://th-h.de/net/usenet/faqs/headerfaq/)

**Eine E-Mail besteht aus mehreren Teilen. Wenn man den Vergleich mit einem konventionellen Brief suchen möchte, könnte man sagen, es gibt einen Umschlag (SMTP-Envelope), einen Briefkopf (Header) und den eigentlichen Brieftext oder -inhalt (Body).**

Den **SMTP-Envelope** bekommt der Nutzer im Normalfall nicht zu sehen. Man bezeichnet so die für die E-Mail-Zustellung relevanten Informationen, die einem Mailserver beim Versand vor der eigentlichen E-Mail übergeben werden. Diese Informationen gehen beim Einsortieren ins Postfach des Empfängers normalerweise verloren. Nur Header und Body der Mail erreichen den Empfänger. Allerdings werden Daten aus dem Umschlag oft in den Header der E-Mail übernommen.

Die Daten für den Umschlag erhält ein Mailserver ganz zu Anfang der Verbindungsaufnahme mit dem Einlieferer. Diese Verbindung wird als SMTP-Dialog bezeichnet. SMTP besteht aus festgelegten (englischen) Schlüsselworten oder Befehlen. Dabei stellt der einliefernde Server sich vor (mittels HELO/EHLO), gibt den Absender an (*Envelope-From*) und nennt den oder die Empfänger (*Envelope-To*). Danach folgt nach dem Kommando DATA die E-Mail mit Header und Body.

Der Dialog beginnt damit, dass der sendende Mailserver oder -client Kontakt mit dem empfangenden aufnimmt. Darauf folgt dann die eigentliche Vorstellung und Begrüßung. Die Angabe des einliefernden Servers nach HELO wird dabei weder überprüft noch hat sie heutzutage besondere Bedeutung. Der sendende Mailserver kann über seinen Namen lügen. Danach gibt der Sender per MAIL FROM die **Absenderadresse** an, der Empfänger bestätigt; gleiches gilt für die **Empfangsadresse** (RCPT TO). Die Absenderadresse kann auch hier gelogen sein. (Mail-Spoofing!)

Die Angaben im **Header** sind völlig beliebig durch den Absender einstellbar und müssen nicht mit den Angaben im Umschlag übereinstimmen. Außer dem Briefkopf, der schon vom Absender mitgeschickt wird, finden sich aber auch noch Headerzeilen, die von jedem an der Übertragung beteiligten Mailserver eingetragen werden, wenn die E-Mail befördert wird. *Diese* Headerzeilen sind für die Rückverfolgung einer E-Mail entscheidend.

Die Zeile Return-Path sollte, wenn sie existiert, ganz am Anfang der E-Mail stehen. Sie enthält den *Envelope-From* und bringt für eine Rückverfolgung herzlich wenig. Die "eigentlichen" Zustellvermerke sind die "Received:"-Headerzeilen, die jeweils vor dem Weiterschicken einer E-Mail vom Mailserver vorne angefügt werden. Man muss sie also rückwärts lesen: die letzte Received:-Zeile ist die oberste. Wenn "mittendrin" noch einmal "Received:"-Zeilen auftauchen, handelt es sich mit hoher Wahrscheinlichkeit um Fälschungen, die einfach vom Absender schon vor dem ersten Versenden eingefügt wurden. Gleiches gilt, wenn sich "Lücken" zwischen einzelnen "Received:"-Zeilen auftun.

**Arbeitsauftrag 2: Wählen Sie eine der beiden folgenden Aufgaben.**

1. Erläutern Sie folgenden SMTP-Dialog:

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to
meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... ok
C: DATA
S: 354 Enter mail, end with "." on a
line by itself
C: ...
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connec-
tion
```

2. Erläutern Sie folgenden Mailquelltext:

```
Return-Path: <user31232@t-online.de>
Received: from mailout06.t-online.de
([194.25.134.19]) by mx-ha.foo.net (mxfoo114
[133.217.17.5])
for <you@foo.com>; Fri, 24 Jul 2020 08:59:50
+0200
Received: from fwd37.aul.t-online.de
(fwd37.aul.t-online.de [172.20.27.137])by
mailout06.t-online.de
for <you@foo.com>; Fri, 24 Jul 2020 08:59:49
+0200 (CEST)
Received: from 110.235.250.208
([110.235.250.208]) by fwd37.t-online.de; Fri,
24 Jul 2020 08:59:46 +0200
From: "WhatsApp.de" <user31232@t-online.de>
To: you@foo.com
Subject: Dein WhatsApp-Konto ist deaktiviert -
635016
Date: Fri, 24 Jul 2020 08:59:12 +0200
Organization: WhatsApp
```