Die E-Mail, die durch die Zeit sprang

Ein Raspberry Pi Projekt für Zeitreisende

Zu erreichende Weltenlinien

- Was ist und woher kam das Projekt
- Bedienungsanleitung
- Live Demonstration

Zu erreichende Weltenlinien

- Wie funktioniert:
  - Die Fernsteuerung
    - DTMF-Empfang und Verarbeitung
      - Voice over IP
    - Ausführung der Steuerbefehle
      - ATmega8-Aufgaben
  - E-Mail in die Vergangenheit
    - E-Mail-Filter
      - Details
      - Angreifbare E-Mail-Clients

Zu erreichende Weltenlinien

- Was ist (noch) fehlerhaft
- Call for Action
- Weiterführende Ressourcen

Woher kam die Idee

- PhoneWave
  - mod. Mikrowelle
    - Fernsteuerung
    - Zeitreise von E-Mails
- Steins;Gate
  - Visual Novel/Anime

Disclaimer

- Erhitzungsfunktion ausgebaut
- Alles ausgebaut bis auf
  - 220V Netzteil
  - Display
  - Drehtellermotor
  - Licht

Bedienungsanleitung

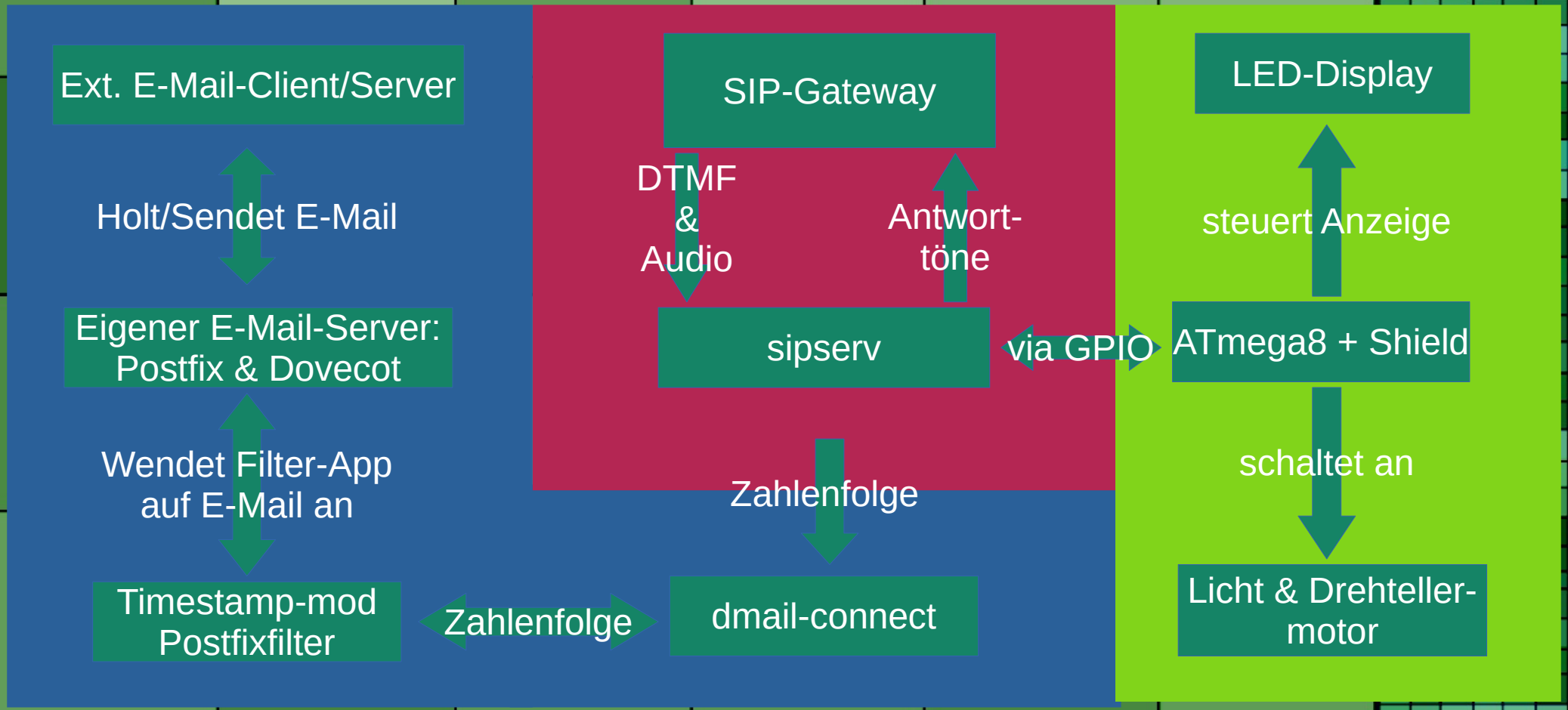
- Gerät anrufen
- Im Anruf:
  - Zahlen eingeben (Ziffernfolge der gewünschten Laufzeit in Sekunden)
    - Anzahl der eingestellten Sekunden = Anzahl der Stunden, die die E-Mail in der Zeit „zurückreist“
  - # drücken → Prozess startet
  - E-Mail senden an: dmail@futuregadgetlab.de
  - * drücken, um Timer zu löschen

Everybody can watch...

- Heute versendete E-Mails werden hier gezeigt
  - Inkl. Absenderadresse & Name
  - Bleibt auch in Aufzeichnung des Talks erhalten!

Demonstration

Signalweg


Ext. E-Mail-Client/Server
Holt/Sendet E-Mail
Eigener E-Mail-Server:
Postfix & Dovecot
Wendet Filter-App
auf E-Mail an
Timestamp-mod
Postfixfilter
Zahlenfolge
dmail-connect
SIP-Gateway
DTMF
&
Audio
Antwort-
töne
sipserv
Zahlenfolge
via GPIO
LED-Display
steuert Anzeige
ATmega8 + Shield
schaltet an
Licht & Drehteller-
motor

DTMF (aka MFV)

- dual-tone multi-frequency
  - dt. Mehrfrequenzwahlverfahren
  - Verwendet bei:
    - Analogtelefon: Mitteilen der Zielrufnummer
    - Generell: Signalübermittlung während Verbindung

Frequenzen	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

DTMF via SIP (Eingehend)

- Inband Audio
  - Als Audiosignal, nur über lossless Codec
- Inband (RFC 2833)
  - Im Medienstream, Datenpaket mit Infos
- DTMF INFO (RFC 2976)
  - Außerhalb Medienstream, Paket mit Infos
- Überführung in RFC-Formate im Gateway
  - sipgate
  - GSM (mit chan_dongle via Asterisk)

Gateway und Client

- Verbindung zum restlichen Telefonnetz
  - „Umwandler“ zwischen VoIP und Außennetz
    - Handelsüblicher VoIP-Provider
    - Mobilnetz über :
      - Asterisk & Huawei & chan_dongle
- sipserv als VoIP-Client („Telefon“)
  - VoIP-Anruf annehmen
    - DTMF-Signale des Anrufs auswerten, weitergeben

Asterisk und chan_dongle

- Asterisk
  - VoIP-Telefonanlage
  - Leitungen in Channels unterteilt, z.B:
    - VoIP-Channels
    - chan_dongle Channel
      - Verbindung mit Mobilfunknetz
  - Anrufvermittlung mittels Dialplans
    - Unterteilung durch Context

Beispiel-Dialplan

```
[kontextname]
exten => _.,1,Dial(SIP/4001)
exten => _.,n,Hangup()
```

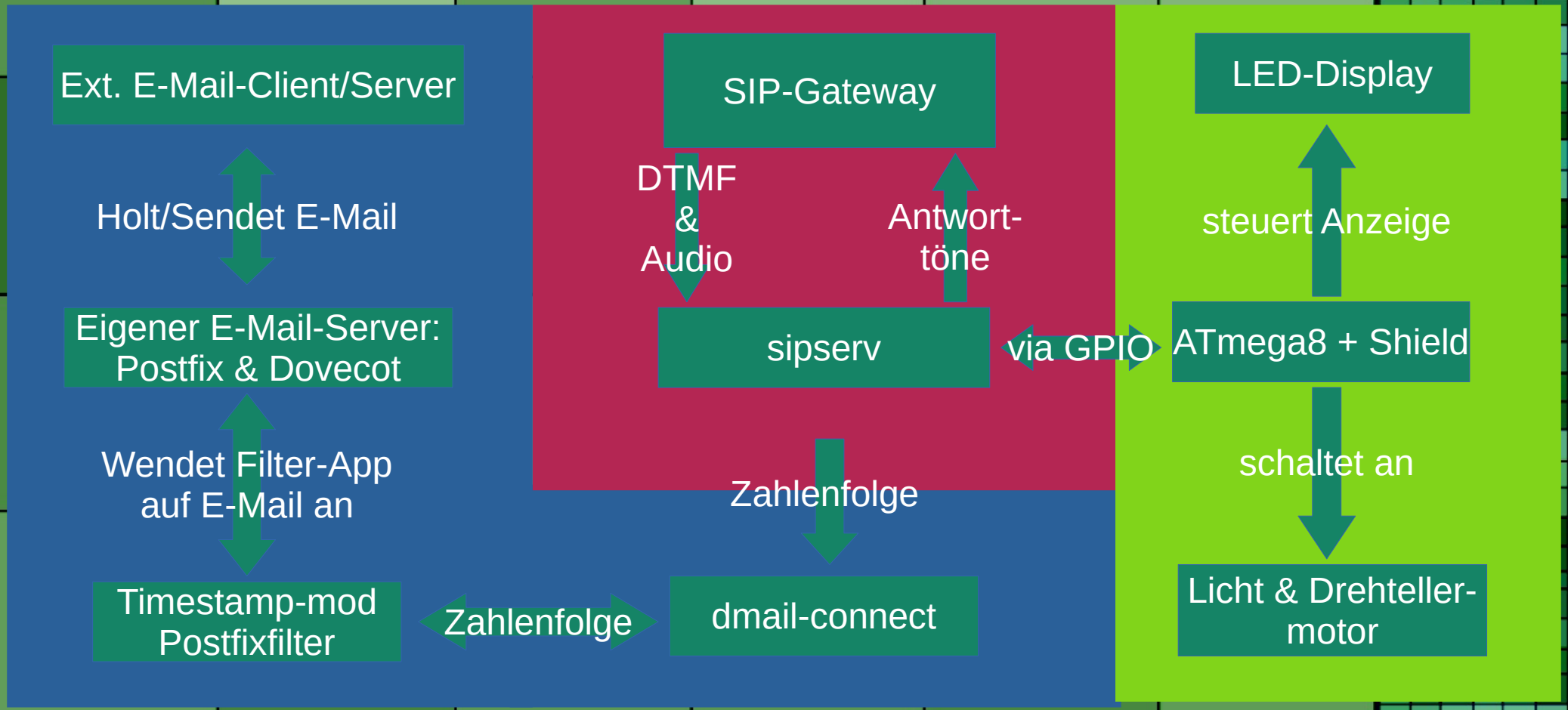
GSMagic mit chan_dongle und mehr

- USB-3G-Stick von Huawei
  - Sprachfunktion
    - Im Einsatz: K3520
  - Mit chan_dongle als Asterisk-Channel nutzbar
    - Asterisk als GSM-Gateway
  - Parallel auch als Internetmodem nutzbar
    - wvdial

Den Anruf auswerten

- Client: sipserv
  - Audioantwort auf DTMF-Nachricht
    - Text to Speech (espeak)
    - Wav-Datei (Microsoft WAV (signed 16 bit) Mono, 22 kHz)
  - Weiterleitung der Ziffern an:
    - ATmega8
      - Shield
    - dmail-connect (für E-Mail-Server)

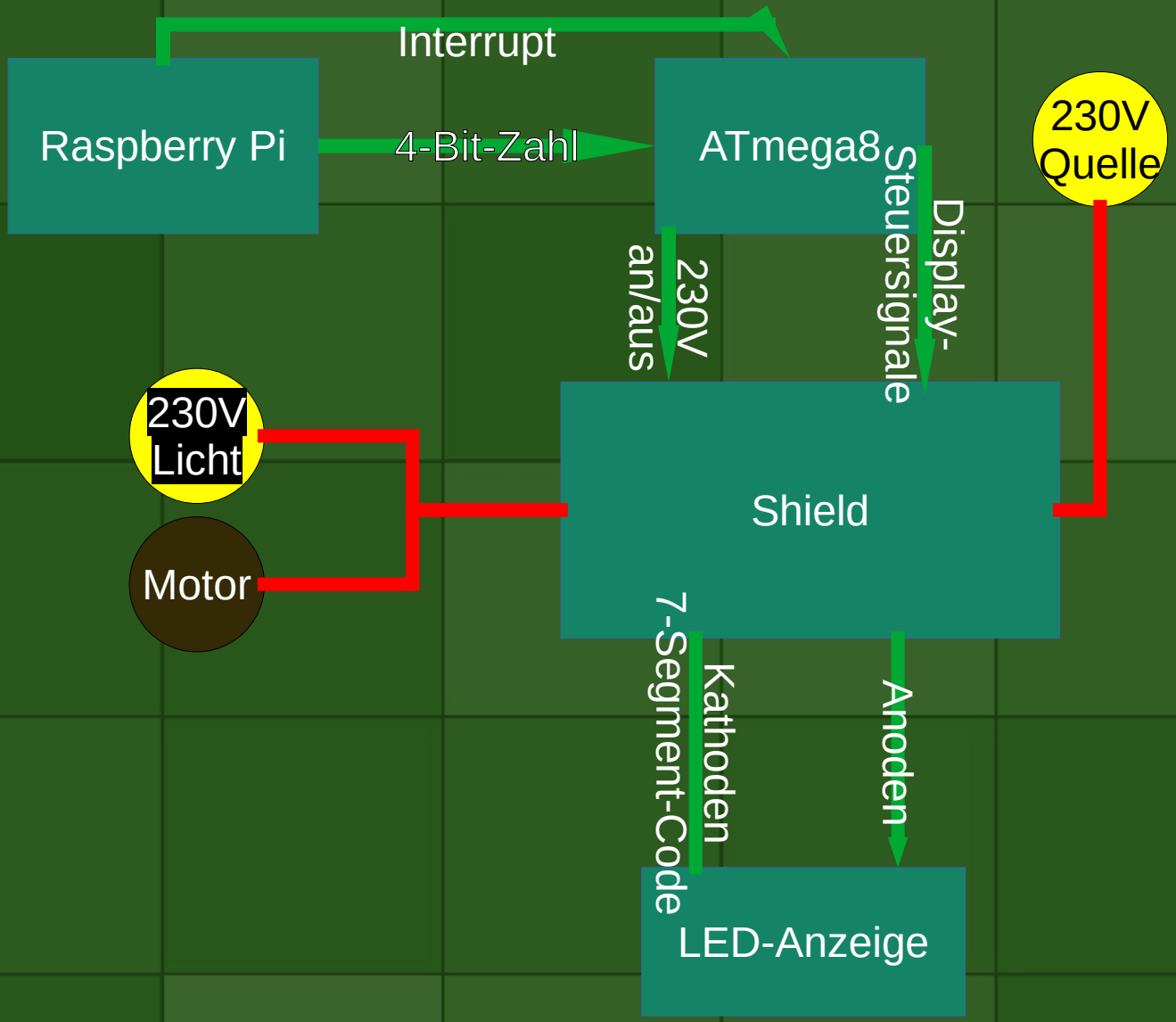
SIP-DTMF kontrolliert alles



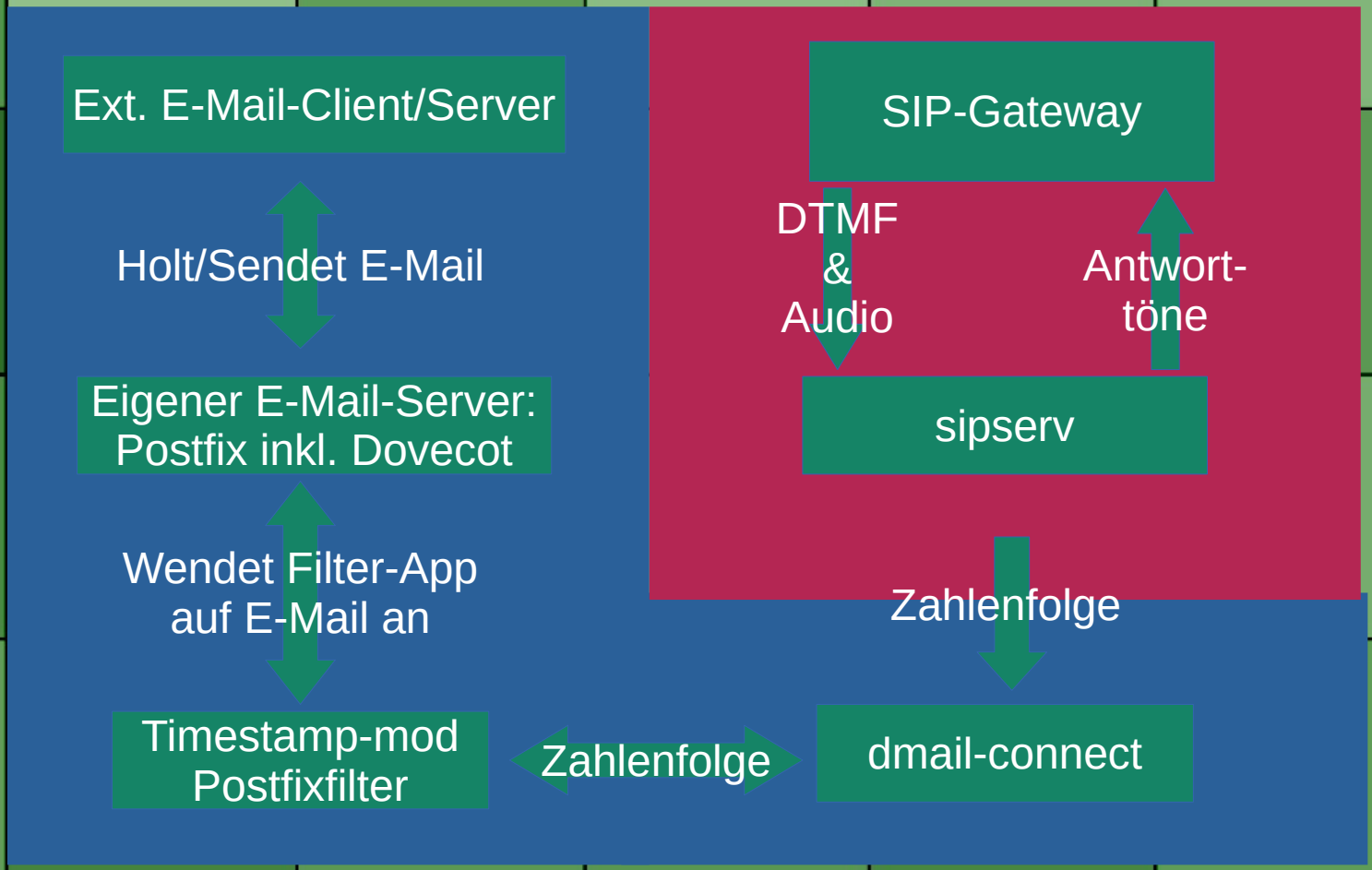
ATmega8-Aufgaben

- Countdown-Timer
  - Eingabe vom Pi
- Ansteuerung Display
  - Sekundenzahl auf Display aktualisieren
- 230V Geräte managen
  - Während Countdown
- ursprünglich für Betrieb mit MT8870D

Funktionen


Interrupt
Raspberry Pi
4-Bit-Zahl
ATmega8
230V Quelle
230V an/aus
Steuersignale
Display-
230V Licht
Motor
Shield
7-Segment-Code
Kathoden
Anoden
LED-Anzeige

Der Zeitsprung



Die Herausforderung beim Zeitsprung

- Zeitstempel aus der Vergangenheit!
  - Contentfilter
- Durch Spamfilter kommen!
  - DKIM
    - Signatur, als Contentfilter
  - SPF
  - DMARC

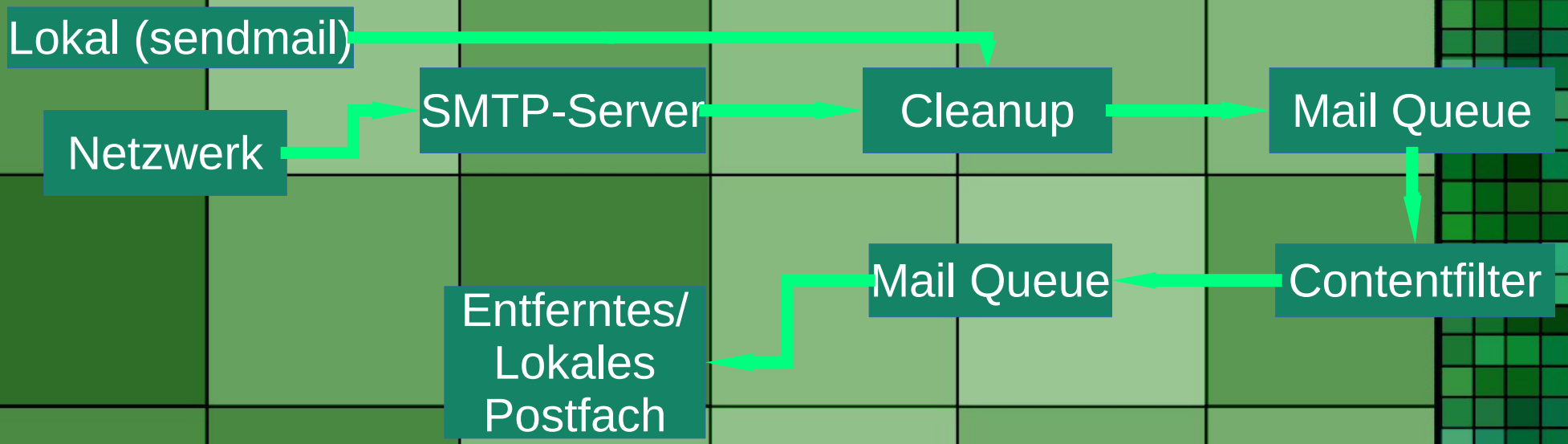
Der Zeitsprung-Filter

- Postfix Contentfilter:
  - Before Queue
  - After Queue
    - Unser Zeitsprungfilter
  - Milter
    - OpenDKIM

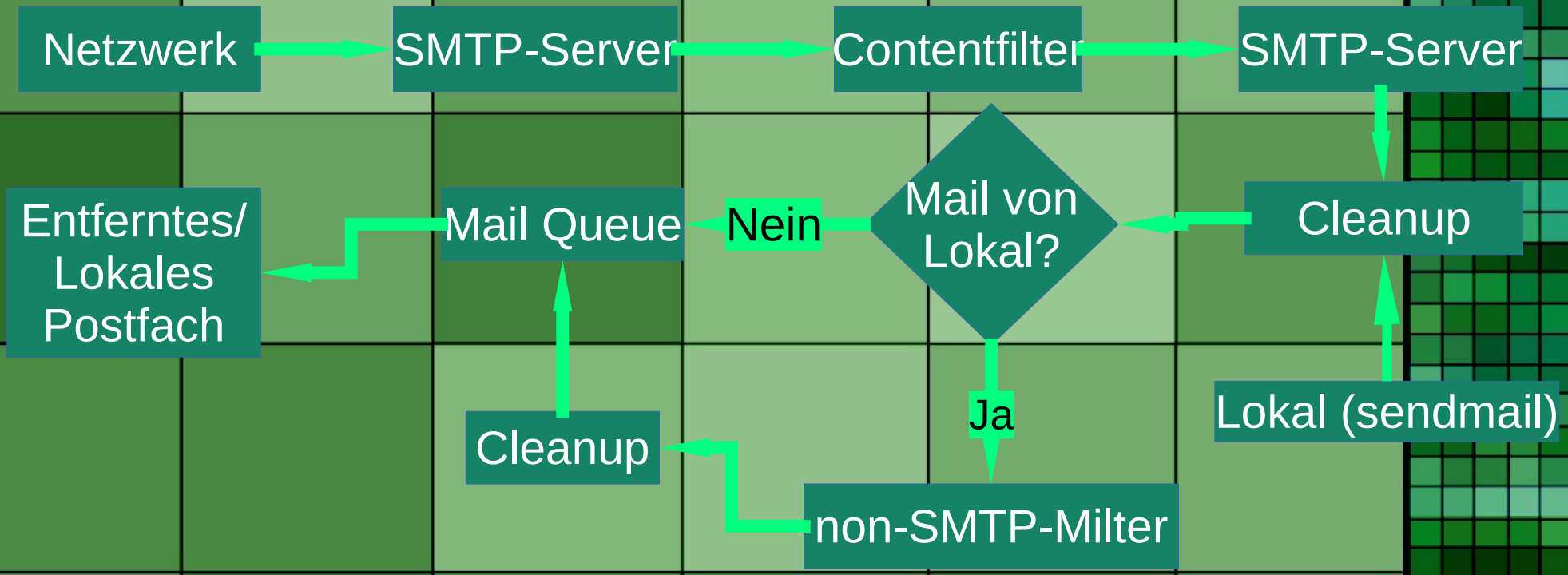
Der Zeitsprung-Filter

- Skipt & Programm
- Arbeit am Zeitstempel
  - Zurechtrichten
  - In Unix-Zeit wandeln
  - Stunden abziehen
  - Alte Zeitstempel ersetzen

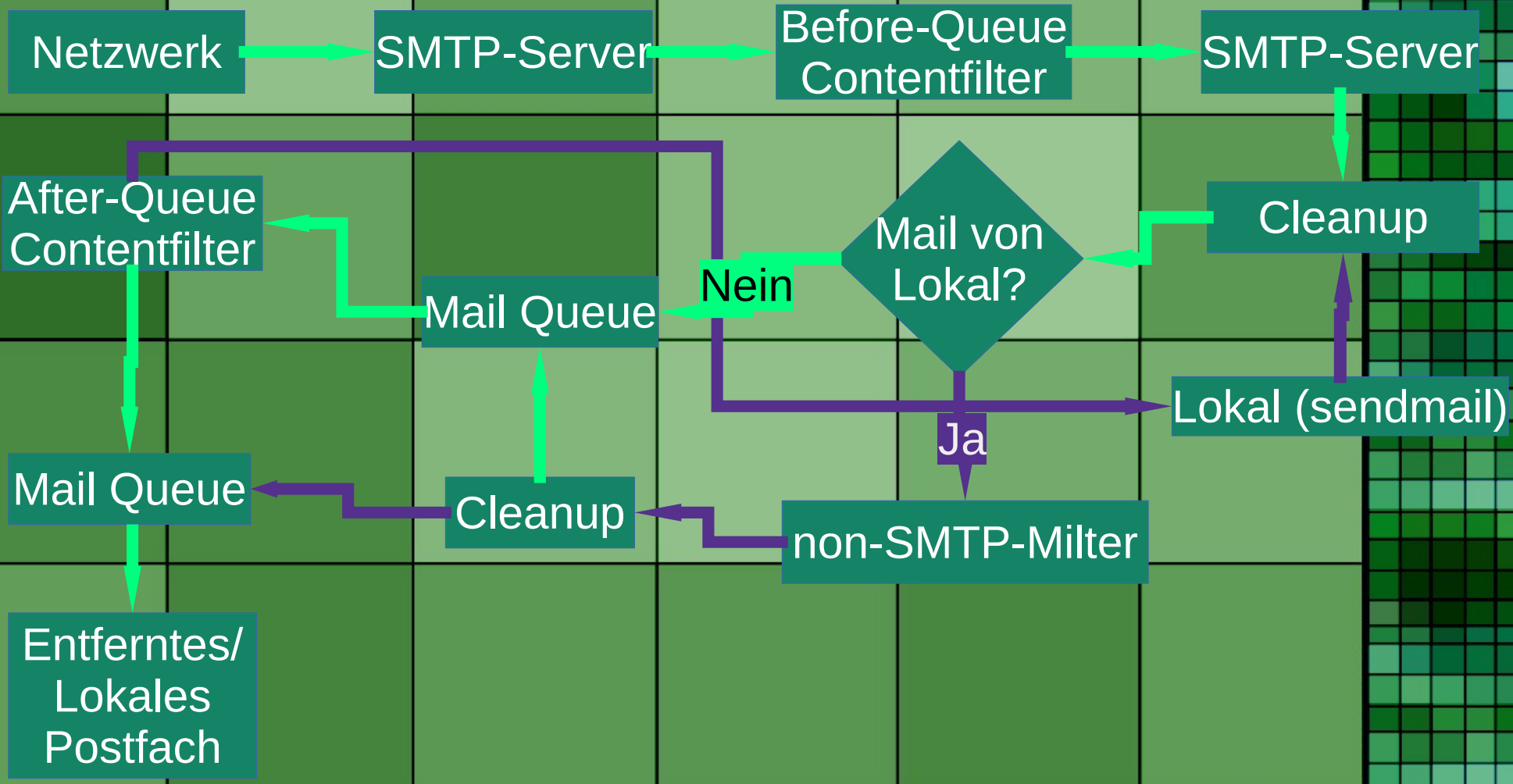
After-Queue


Lokal (sendmail)
Netzwerk
SMTP-Server
Cleanup
Mail Queue
Contentfilter
Mail Queue
Entferntes/
Lokales
Postfach

Before-Queue/Milter



Kombiniert


Netzwerk
SMTP-Server
Before-Queue Contentfilter
SMTP-Server
Cleanup
Mail von Lokal?
Nein
Ja
Lokal (sendmail)
After-Queue Contentfilter
Mail Queue
Mail Queue
Cleanup
non-SMTP-Milter
Entferntes/ Lokales Postfach

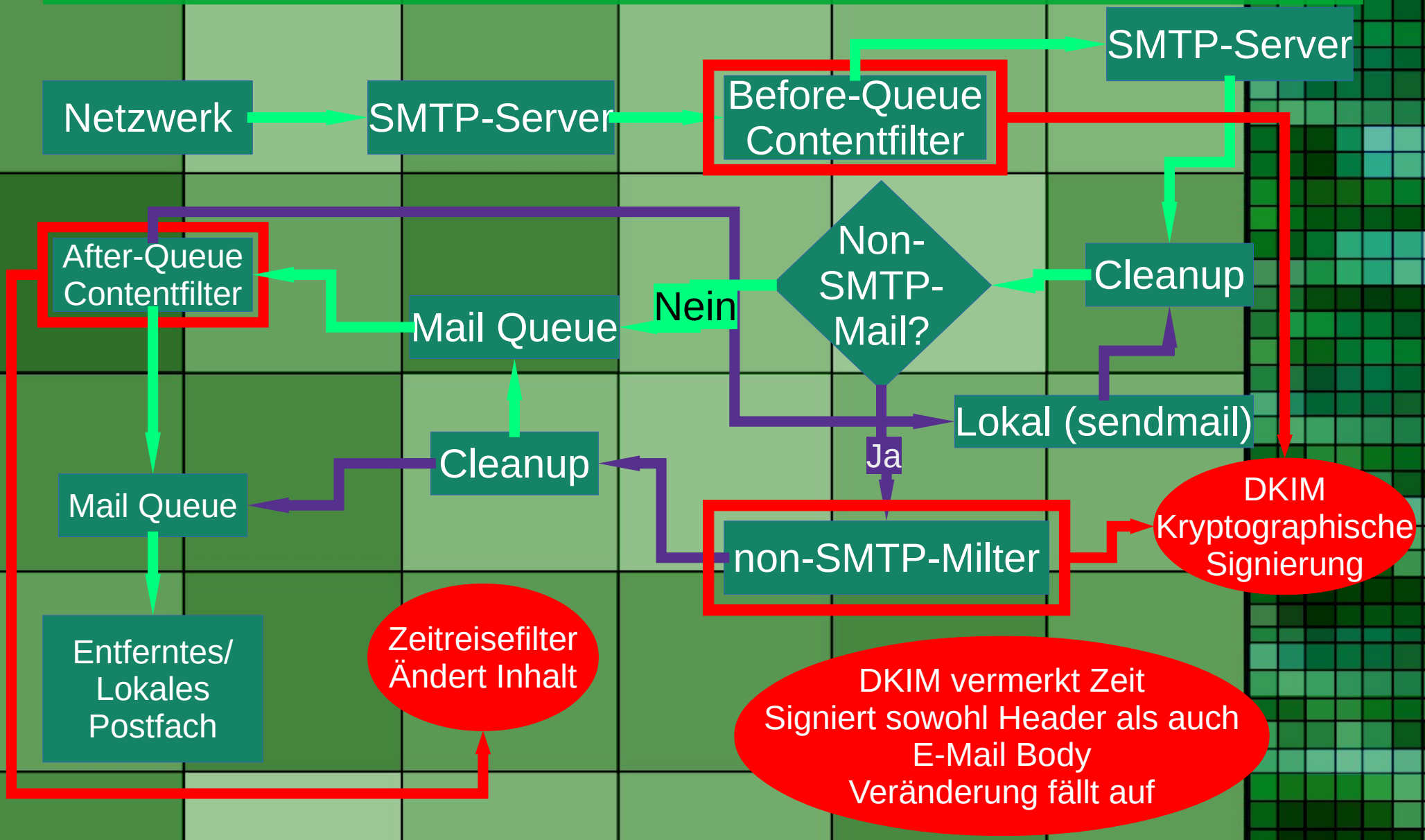
Und jetzt

Fügen wir zur Spamfilterdurchdringung DKIM ein!

DKIM

- DomainKeys Identified Mail
  - Asymmetrisches kryptographisches Verfahren zur Signatur von Mails
  - Schlüssel dazu im DNS TXT

Autsch!


Netzwerk
SMTP-Server
Before-Queue Contentfilter
SMTP-Server
After-Queue Contentfilter
Mail Queue
Nein
Non-SMTP-Mail?
Cleanup
Lokal (sendmail)
Ja
Cleanup
Mail Queue
non-SMTP-Milter
DKIM Kryptographische Signierung
Entferntes/ Lokales Postfach
Zeitreisefilter Ändert Inhalt
DKIM vermerkt Zeit
Signiert sowohl Header als auch E-Mail Body
Veränderung fällt auf

SPF

- Sender Policy Framework
- Welche IP‘s dürfen im Namen der Domain mailen
  - DNS TXT

Wo kam ich durch Spamfilter

- Nein:
  - Yahoo
  - Microsoft
    - Blacklistete mich
    - Wenn nicht, kommts durch
- Ja:
  - Hochschule Niederrhein
  - Google Mail
  - GMX

Et voila

Originalnachricht

Nachrichten-ID	<akzclc1zg1w6-3xu9t1-s5xtdvqvydzbutji12rdr7sfqqy0x3-111yg1j14dkw60jf8h-baedlx-n1xsxcgupxj7-82sf05qdvh7my5u2welb66n-stmo5fozp32f783z96o811c-lqrl4a-19z00h.1554311776241@email.android.com>
Erstellt am:	29. März 2019 um 17:16 (Nach 435602 Sekunden zugestellt)
Von:	"dmail@futuregadgetlab.de" <dmail@futuregadgetlab.de>
An:	
Betreff:	Status der Forschung
SPF:	PASS mit IP-Adresse 2a03:4000:1d:5d7:0:0:0:1 Weitere Informationen
DKIM:	'PASS' mit Domain futuregadgetlab.de Weitere Informationen
DMARC:	'PASS' Weitere Informationen

- Googlemail sagt:
  - Alles Okay!
  - Webmail zeigt Empfangszeit an
    - Nicht beeinflussbar

Und die E-Mail-Header:

From - **Wed Apr 3 19:21:08 2019**
Delivered-To: xxxxxxxx@gmail.com
Received: by 2002:a02:5588:0:0:0:0:0 with SMTP id [redacted];
        Wed, 3 Apr 2019 10:16:19 -0700 (PDT)
X-Received: by 2002:adf:eac9:: with SMTP id
        [redacted];
        Wed, 03 Apr 2019 10:16:18 -0700 (PDT)
smtp.mailfrom=dmail@futuregadgetlab.de;
       dmarc=pass (p=NONE sp=NONE dis=NONE)
header.from=futuregadgetlab.de
Return-Path: <dmail@futuregadgetlab.de>
Received: from futuregadgetlab.de (futuregadgetlab.de. [2a03:4000:1d:5d7::1])
        by mx.google.com with ESMTPS id
x3si9767240wmj.173.2019.04.03.10.16.18
        for <xxxxxxxx@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-CHACHA20-POLY1305
bits=256/256);
        Wed, 03 Apr 2019 10:16:18 -0700 (PDT)

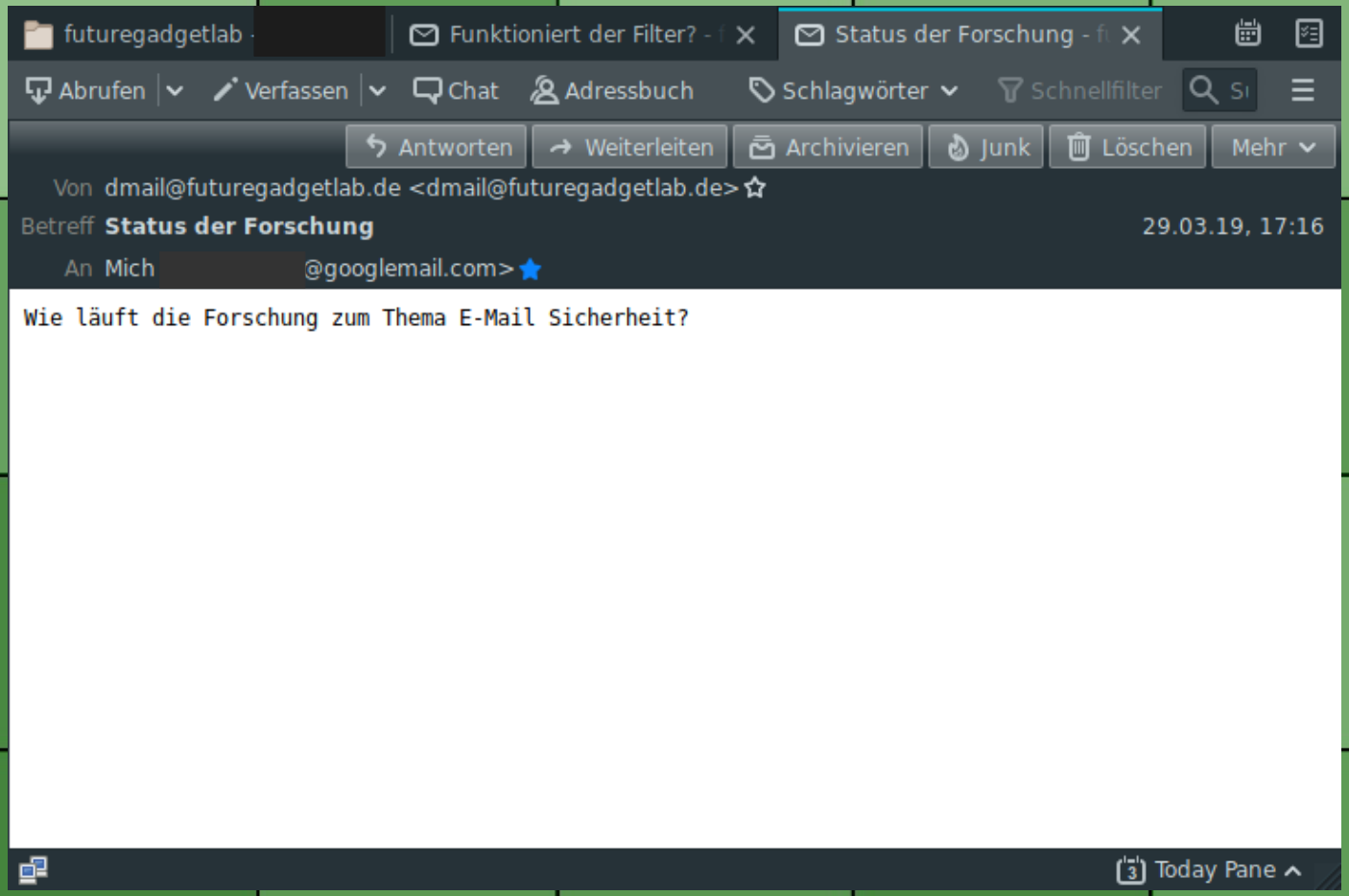
Und die E-Mail-Header:

Received-SPF: pass (google.com: domain of dmail@futuregadgetlab.de designates 2a03:4000:1d:5d7::1 as permitted sender) client-ip=2a03:4000:1d:5d7::1;
Authentication-Results: mx.google.com;
dkim=pass header.i=@futuregadgetlab.de header.s=201806 header.b=r4P0TVfB;
spf=pass (google.com: domain of dmail@futuregadgetlab.de designates 2a03:4000:1d:5d7::1 as permitted sender) smtp.mailfrom=dmail@futuregadgetlab.de;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=futuregadgetlab.de
Received: by futuregadgetlab.de (Postfix, from userid 1005)
id 6556741F63; **Wed, 3 Apr 2019 19:16:18 +0200 (CEST)**
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=futuregadgetlab.de;
s=201806; **t=1554311778**;
bh=U1TA6T/0LXNMJBX/r9dZwSdFWsnGobxCnFQ7bnw5RXU=;
h=Date:Subject:From:To:From;
b=[Hash des Bodys]

Und die E-Mail-Header:

Received: from [IPv6:] (unknown [IPv6:])
(using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256)
(No client certificate requested)
(Authenticated sender: dmail)
by futuregadgetlab.de (Postfix) with ESMTPSA id [redacted]
for <xxxxxx@googlemail.com>; **Fri, 29 Mar 2019 18:16:17 +0200 (CEST)**
Date: **Fri, 29 Mar 2019 18:16:16 +0200**
Subject: Status der Forschung
Message-ID: <[redacted]@email.android.com>
From: "dmail@futuregadgetlab.de" <dmail@futuregadgetlab.de>
To: xxxxxxx <xxxxxxxx@googlemail.com>

Und Thunderbird so:



Welche Clients sind austricksbar

- Betroffen
  - Thunderbird
  - Huawei E-Mail-App
- Nicht betroffen:
  - Webseiten der Anbieter
  - Gmail-App
  - Mail for Windows 10
- Ungetestet:
  - Microsoft Office Outlook
  - Opera Mail
  - Und viele mehr

Was ist fehlerhaft

- Letzte Zeitstempel des eigenen Servers
  - DKIM-Zeitstempel:
    - OpenDKIM modifizieren
- dmail-connect:
  - Crasht, wenn Verbindung durch zu lange Latenzen gestört wird
    - Keepalive macht Probleme

Versuchskaninchen gesucht

- Mitstreiter gesucht
  - Testen von Clients
    - Siehe QR-Code
  - Verbesserung des Filters

Ressourcen

- Software & Layouts
  - github.com/kaitocross
- chan_dongle & Asterisk:
  - www.raspberry-asterisk.org
  - https://wiki.e1550.mobi/
  - github.com
    - /bg111/asterisk-chan-dongle/wiki
    - /wdoekes/asterisk-chan-dongle

Bauanleitung, Blog & Mehr Infos: futuregadgetlab.de

Vielen Dank!

Vielen Dank für eure Aufmersamkeit!

Credits

Präsentationstemplate „green-box“
von Marcin Miłkowski

Fragerunde

- Ask me anything (about the project)