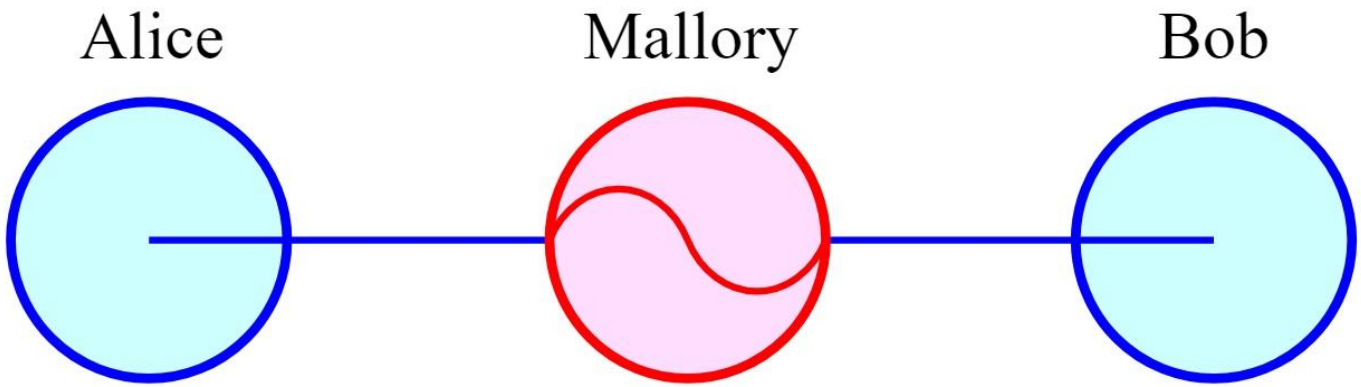

Alice
Mallory
Bob

Man-In-The-Middle

Attenberger, Bollenmiller, Schuster, Wilhelm

-Team J3A-

Hochschule München

29. September 2017

Inhalt

- **Projektziel**
- **Architektur**
  - **OpenBTS**
  - **Osmocom**
- **Umsetzung des Projektziels**
- **Probleme/ Lessons learned**
- **Live-Demo**

Projektziel

Projektziel

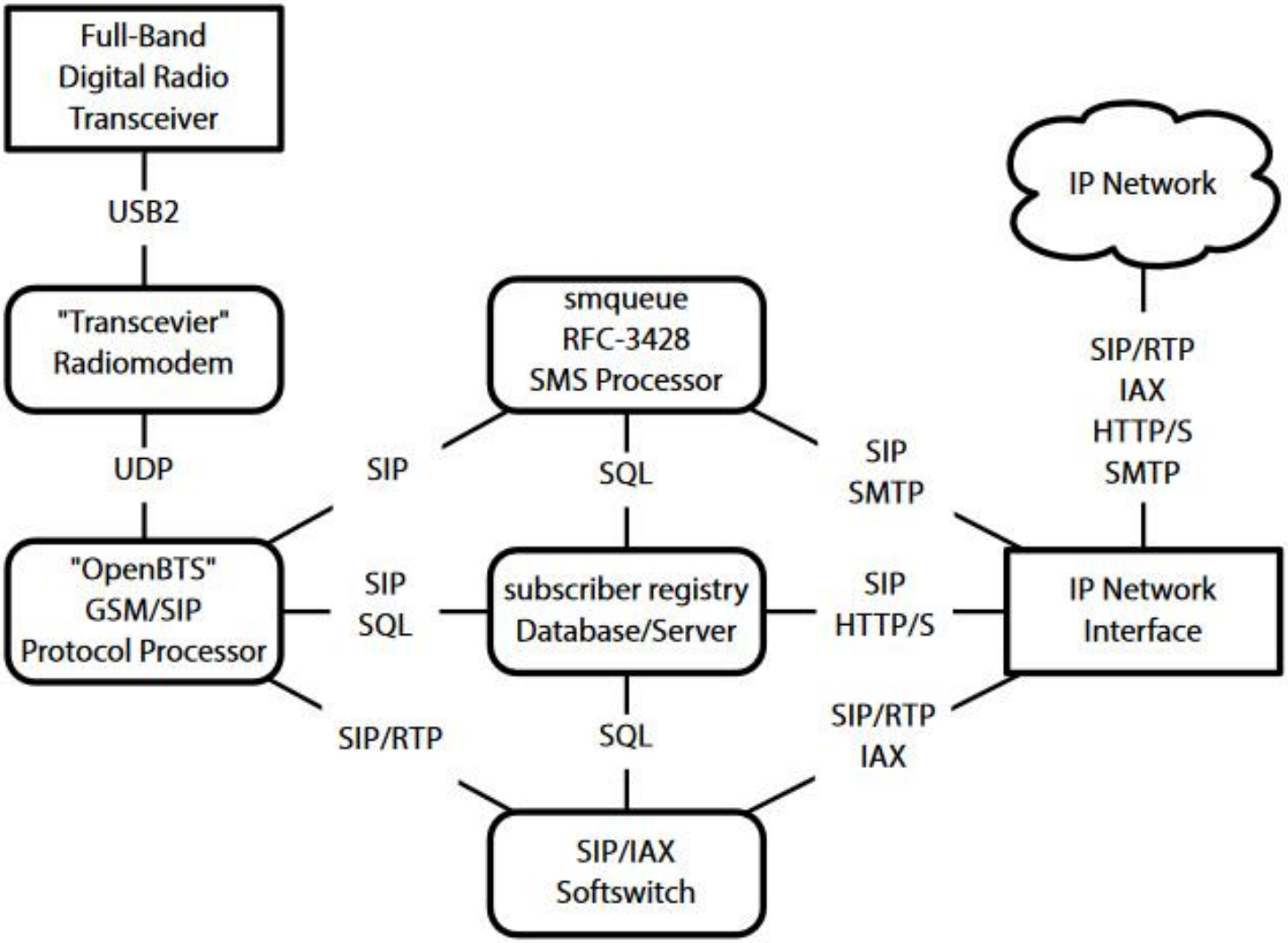
- Inbetriebnahme eines GSM Netzes
- Aufzeichnen und Abspeichern der Daten eines Telefongesprächs
- Lokales Abspielen des Gesprächs

Optionales Feature

- Hinterlegung einer Rufnummer
- Abspielen des Telefongesprächs bei Anruf der festgelegten Nummer


Ettus Research
USRP N210

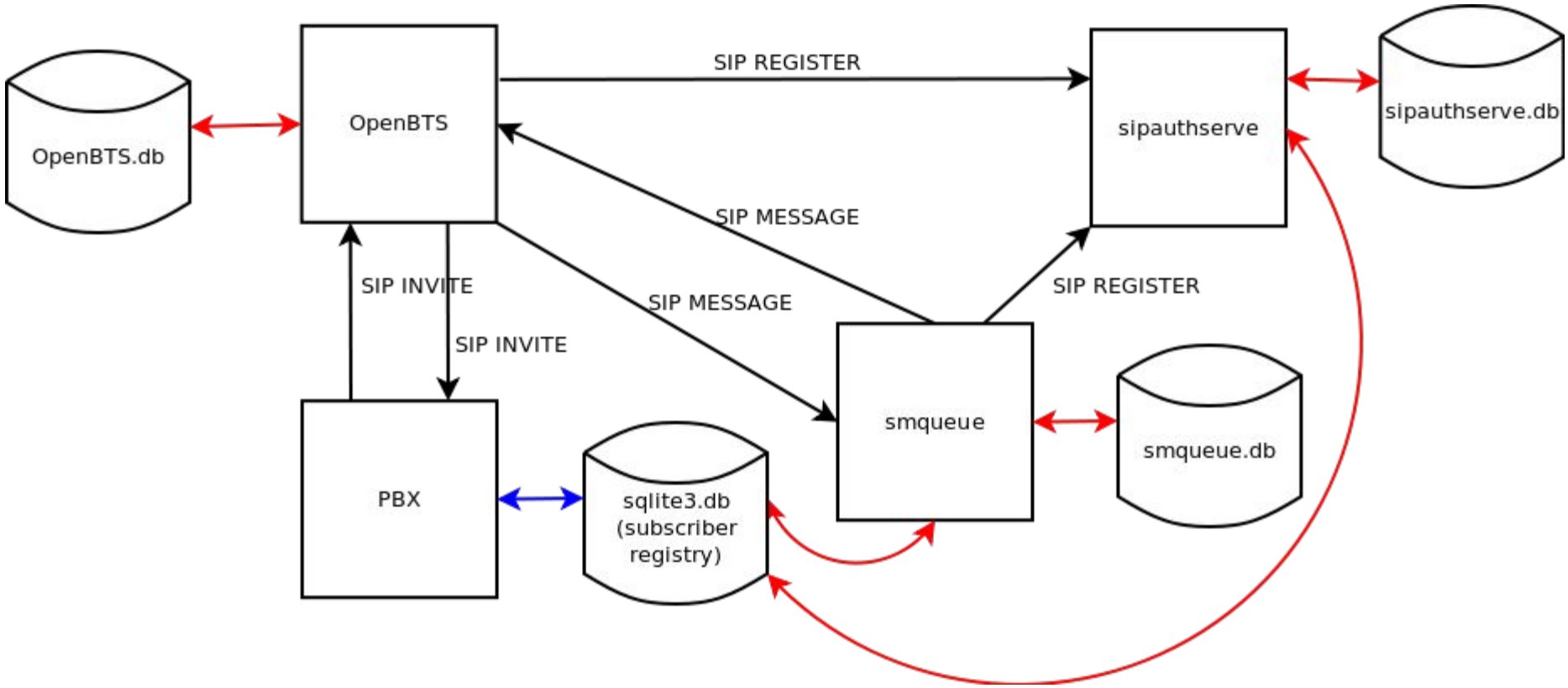
Architektur OpenBTS


Full-Band
Digital Radio
Transceiver
USB2
"Transcevier"
Radiomodem
UDP
"OpenBTS"
GSM/SIP
Protocol Processor
SIP
SQL
SIP/RTP
smqueue
RFC-3428
SMS Processor
SQL
subscriber registry
Database/Server
SQL
SIP/IAX
Softswitch
SIP
SMTP
SIP
HTTP/S
SIP/RTP
IAX
IP Network
SIP/RTP
IAX
HTTP/S
SMTP
IP Network
Interface

Systemarchitektur eines GSM-Netzes mit OsmoBTS

Bestandteile von OpenBTS:

- OpenBTS: Die eigentliche OpenBTS-Anwendung, die den Großteil des GSM-Stacks oberhalb des Radiomodems realisiert
- Transceiver: Software-Radiomodem und Hardware-Kontrollsystem, welches für die Anbindung des USRP N210 SDR zuständig ist
- Asterisk: Private Branch Exchange (PBX), der Hauptfunktionen des Mobile Switching Center (MSC) übernimmt
- SIPAuthServe: Verwaltung einer Subscriber Registry Datenbank, die dem Home Location Register (HLR) ähnelt
- SMQueue: Store-and-Forward Message Service für die Übertragung und Speicherung von SMS-Nachrichten

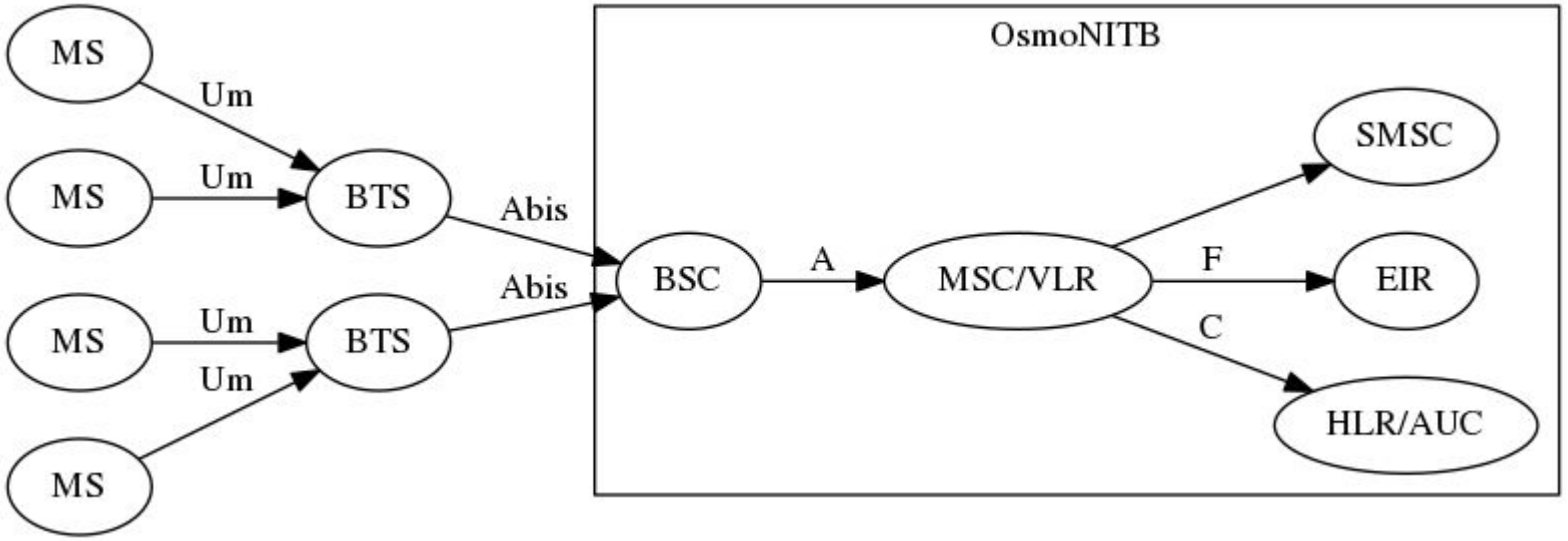

OpenBTS.db
OpenBTS
SIP REGISTER
sipauthserve
sipauthserve.db
SIP MESSAGE
SIP INVITE
SIP MESSAGE
SIP REGISTER
SIP INVITE
smqueue
smqueue.db
PBX
sqlite3.db
(subscriber
registry)

Architektur Osmocom

Systemarchitektur eines GSM-Netzes mit OsmoNITB

OsmoNITB ist ein Projekt aus dem OsmocomBB-Umfeld.

OsmoNITB implementiert das Network Switching Subsystem (NSS) im GSM-Netz, aber mit OpenBSC auch Teile des Base Station Subsystems (BSS).



Systemarchitektur eines GSM-Netzes mit OsmoNITB

Bestandteile von OsmoNITB:

- BSC: Basisstation-Controller; Überwacht Mobilfunkverbindung und regelt die Leistung; Löst einen Zellenwechsel (Handover), falls erforderlich, aus

- MSC/ VLR: Mobile-service switching center ist Vermittlungsstelle im GSM/GPRS-Netz; Übernimmt die Anrufverwaltung/ Authentifizierung und Gebührenerfassung.
  Visitor Location Register (VLR) → Datenbank, die verwaltet, in welcher BTS ein MS zuletzt eingebucht war

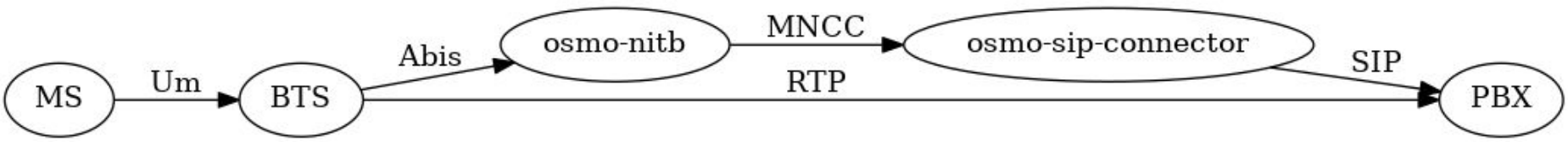
- SMSC: Server für SMS-Dienste; Verarbeitung von Textmitteilungen

- EIR (Equipment Identity Register) → Optional; Datenbank für Seriennummern der Mobilgeräte (IMEI) gespeichert → Sperren verlorener oder gestohlener Endgeräte

- HLR/AUC: Home Location Register ist Datenbank in der die Rufnummer, IMSI & TMSI eines Mobiltelefons hinterlegt ist.
  Authentification Center (AUC): Authentifizierungszentrale; Ort, an dem Authentifizierungsschlüssel Ki abgelegt ist; Authentifizierung der SIM-Karte gegenüber Mobilfunknetz

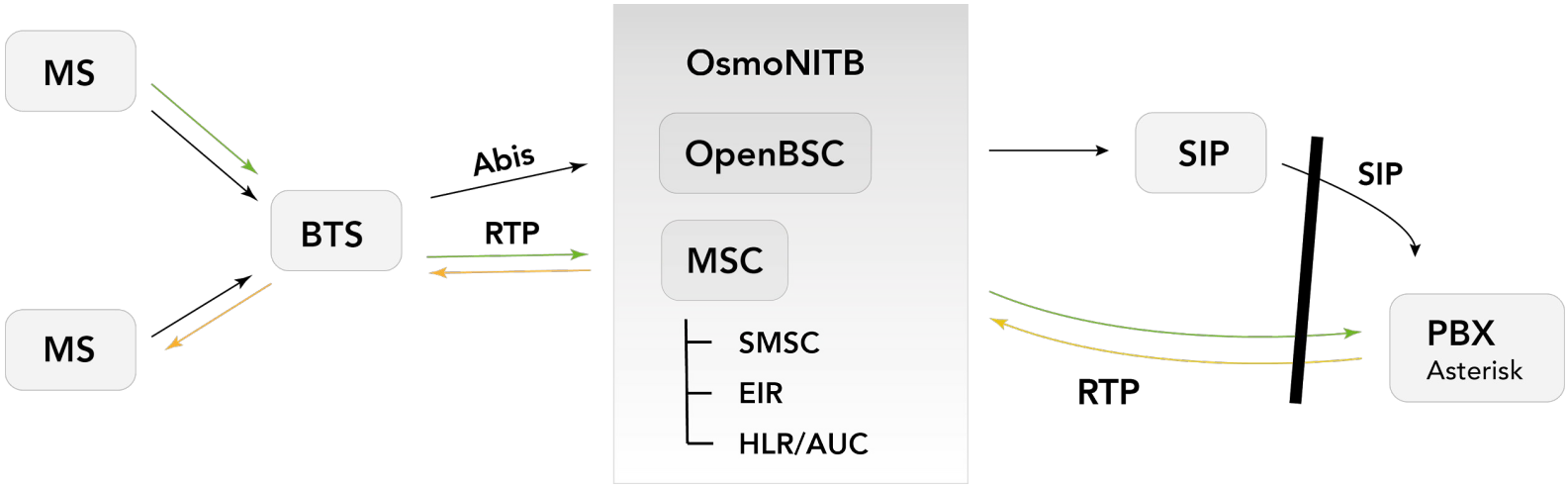
VoIP im GSM-Netzes

- Osmocom-SipConnector wirkt als vermittler der klassischen ISDN-Anrufsteuerungsprotokoll (MNCC) und dem SIP-Protokoll
- Connector ist notwendig um eine Verbindung mit Asterisk aufzunehmen
- Asterisk ist eine virtuelle Telefonanlage, die als Vermittlungsstelle genutzt werden kann



Unser System

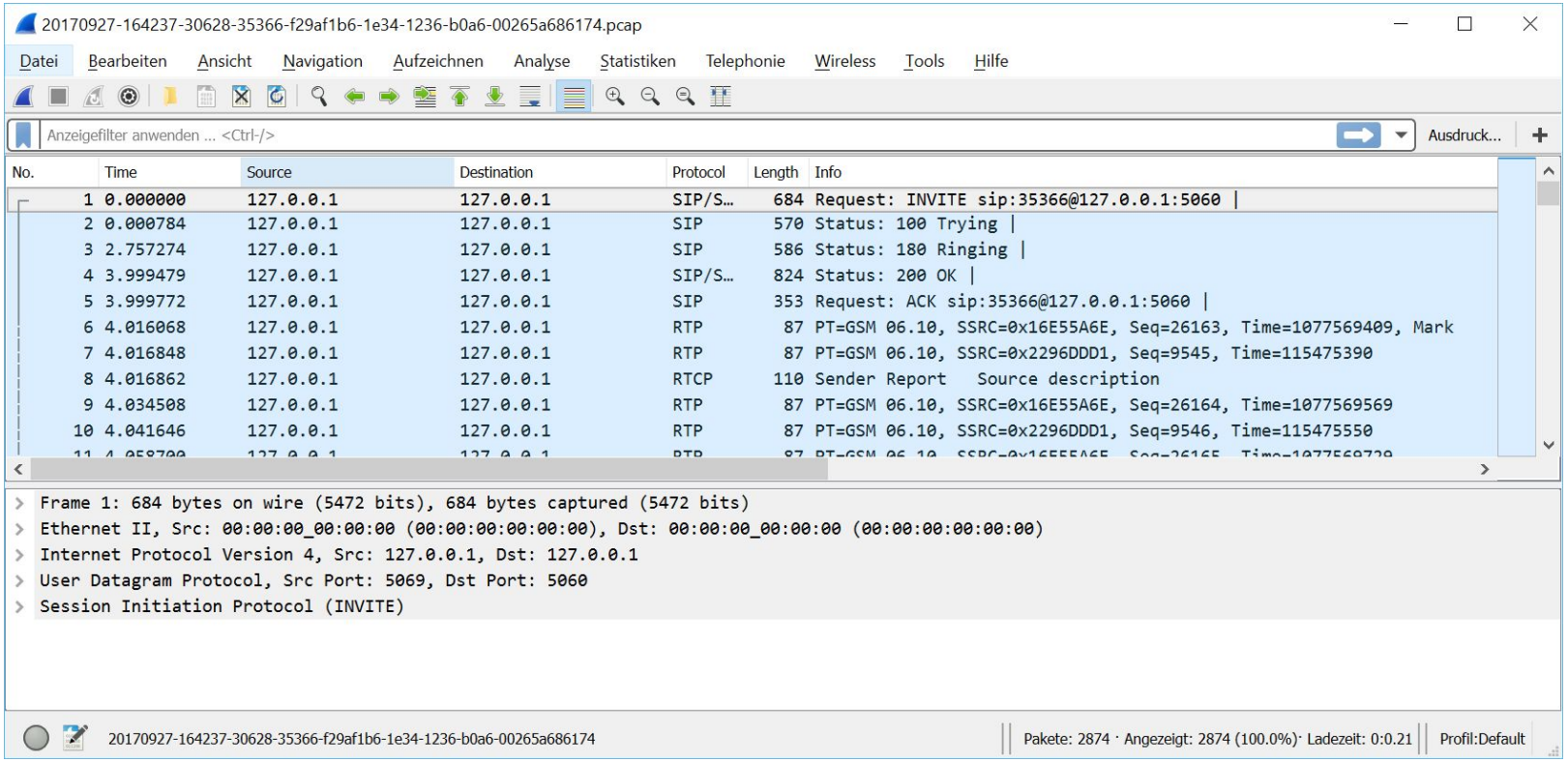
- Eine BTS, Osmocom-Abis-Interface, OsmoNITB, OsmocomSipConnector, Asterisk
- Abgriff der Gespräche am schwarzen Balken



Umsetzung des Projektziels

Umsetzung des Projektziel

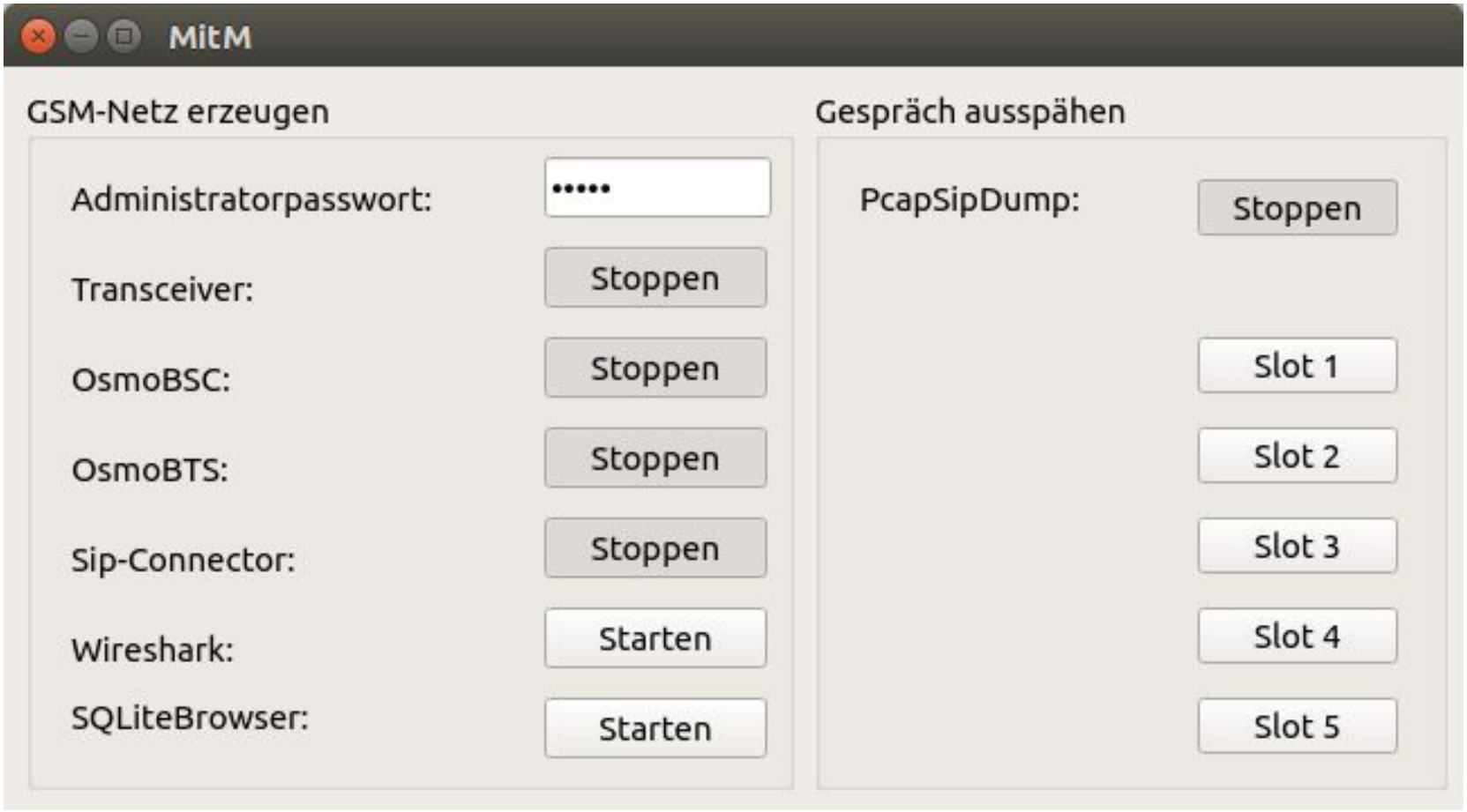
- Aufzeichnen und Abspeichern der Daten
  - pcapsipdump



Umsetzung des Projektziel

- Aufzeichnen und Abspeichern der Daten
  - pcapsipdump
- Extrahieren und konvertieren der Daten
  - pcap2wav
- vollständige Automatisierung
  - Incron

- Feature - Abhören der Nachricht
  - Bestimmte Rufnummer hinterlegen
  - Abspielen des Gesprächs bei Anruf der definierten Nummer


MitM
GSM-Netz erzeugen
Administratorpasswort:
•••••
Transceiver:
Stoppen
OsmoBSC:
Stoppen
OsmoBTS:
Stoppen
Sip-Connector:
Stoppen
Wireshark:
Starten
SQLiteBrowser:
Starten
Gespräch ausspähen
PcapSipDump:
Stoppen
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5

Probleme/ Lessons learned

Probleme/ Lessons learned

- Konfiguration von OpenBsc und Osmo-Bts ✓
- Installation sämtlicher Abhängigkeiten ✓
- Backup-System → parallele Inbetriebnahme zweier Systeme ✓
- Automatisierung des Abspeicherns und Abhörens ✓
- Aufzeichnen und Abspeichern des Telefongesprächs → Systemperformanz ✓
- Hinterlegen der Rufnummer ✓

Live-Demo

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?