FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

# Remote Administration Toolkits (RAT) für Android

Christian Esser

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

# Agenda

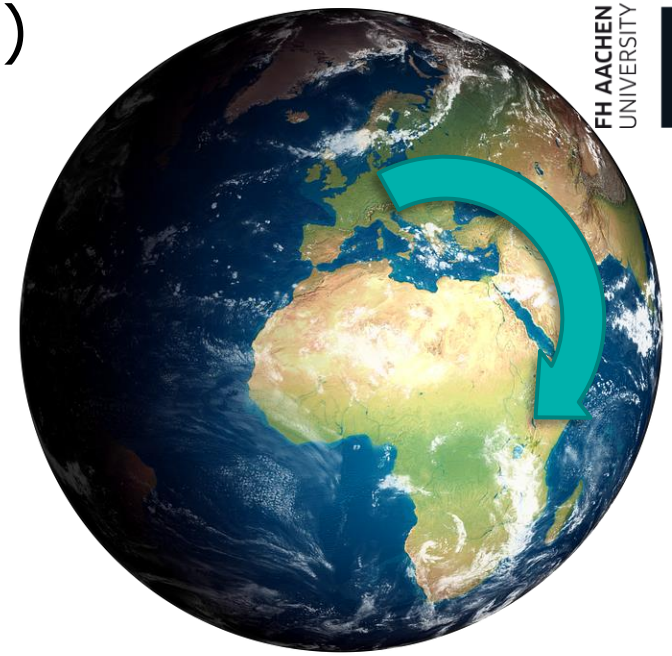
- Remote Administration Toolkit
- Android
- Aufgabenstellung
- Toolkits
- Bisherige Ergebnisse

# Hintergrundinformationen



Remote Administration Toolkit (RAT)

- Entfernter Zugriff auf ein System
- Einsatzmöglichkeiten
  - Fernwartung
    - Beseitigung von Störungen
  - Schadsoftware
    - Ausspähen von Benutzern/Daten

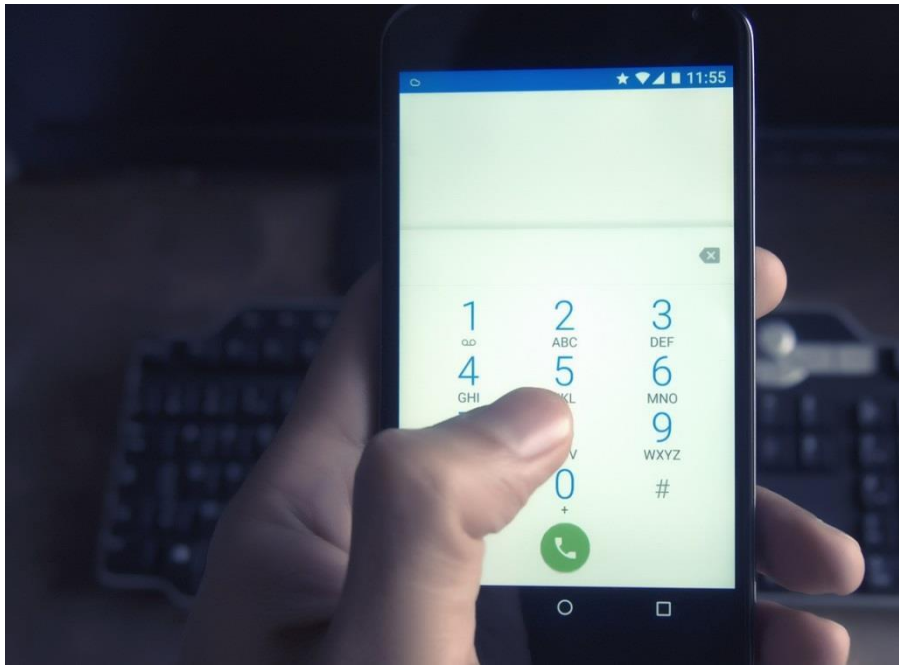


http://pixabay.com/de/erdkugel-erdball-weltkugel-planet-328140/

# Hintergrundinformationen



- Warum für Angreifer interessant?
  - kostenpflichtige Dienste aufrufbar
  - Bankgeschäfte
  - Industrie- / Wirtschaftsspionage
    - Kontakte
    - Konversationen (Messenger / Email)
    - Dateien
  - andere Daten




http://pixabay.com/de/smartphone-handy-telefon-564155/

# Hintergrundinformationen



Android

- Marktanteil (Stand 2014)
  - 1 Mrd. Absatz, ~80% der verkauften Geräte
- Höchste Verbreitung (Stand Dez. 2014)
  - 1,6 Mrd. genutzte Geräte, ~75%
- Einzug in Business Bereich
  - ersetzt zunehmend Blackberry, iPhone
- … für Angreifer interessantes OS

# Aufgabenstellung



Was plane ich für meine Abschlussarbeit

- Analyse der RAT Software
  - Wie funktioniert sie?
  - Was kann sie?
- Typischer Angriffsablauf
- Erkennung von Angriffen
- Analyse der Aktivitäten
- Schutzmaßnahmen

# Existierende Toolkits



## AndroRAT

- Entwickelt von 4 Studenten
  - Veröffentlicht November 2012
  - Idee: Fernwartung
  - Erweiterbarkeit
- Erweitert von Crackern
  - Integration eines APK Binders
  - Idee: Schadsoftware als Trojaner

# Existierende Toolkits



## Dendroid

- reine Schadsoftware
  - APK tarnt sich als „Adobe Flash“
- Besondere Features
  - Unterbinden von SMS Empfang
  - DoS Attacken (Smartphone Botnet)

# Toolkit - Vergleich

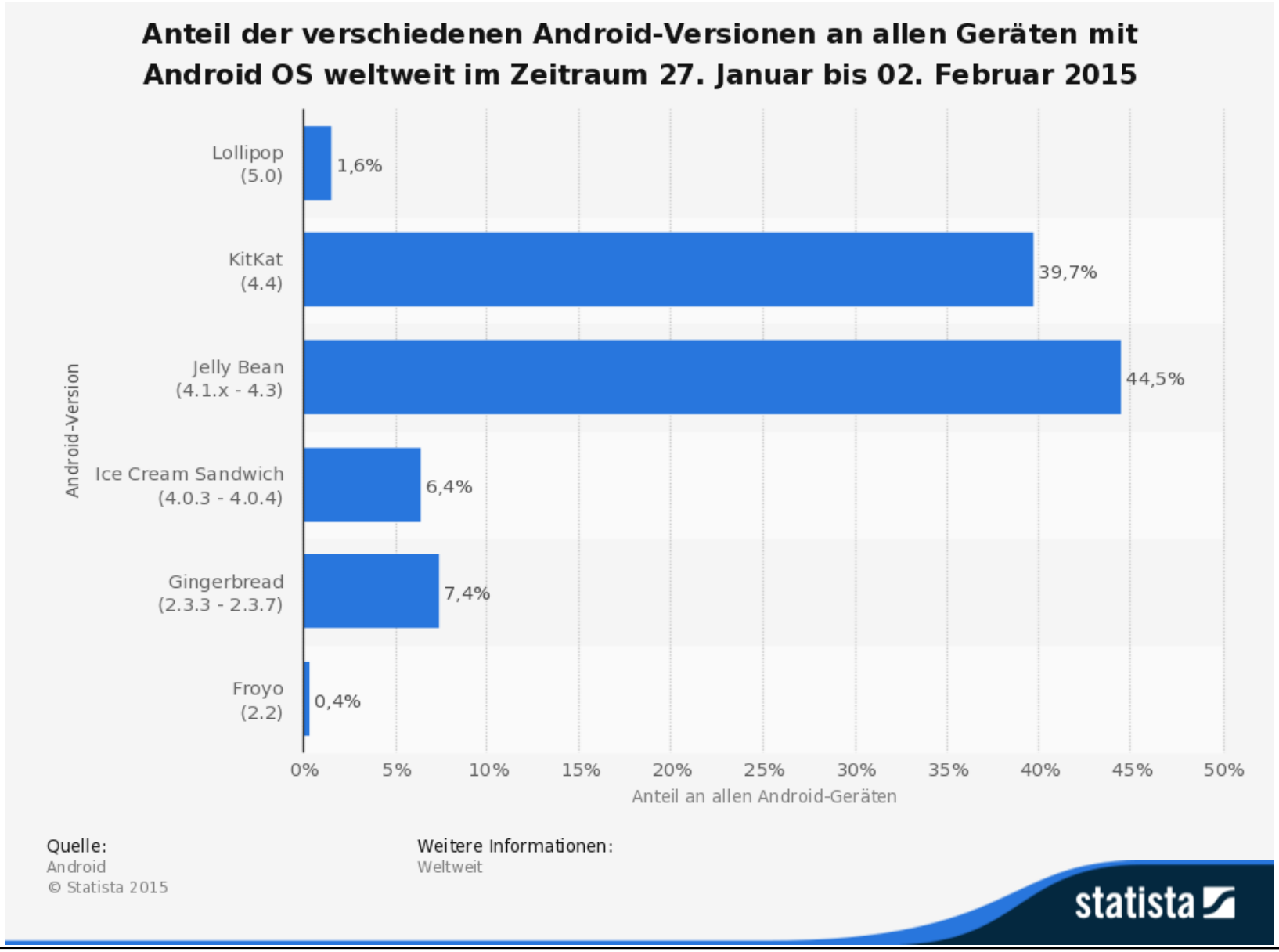
| Merkmal | AndroRAT | Dendroid |
|---|---|---|
| Detaillierte Informationen | X | |
| **SMS senden/lesen** | **X** | **X** |
| SMS löschen | | X |
| **Anruf initiieren** | **X** | **X** |
| Anruf aufnehmen | X | X |
| Anruf History lesen | X | X |
| Anruf History löschen | | X |
| Kontakte auslesen | X | X |
| **Webseite öffnen** | **X** | **X** |
| Foto aufnehmen | X | X |
| Video aufnehmen | X | X |
| **Audio aufnehmen** | **X** | **X** |
| Position bestimmen | X | X |
| SD Karte auslesen | X | |

# Bisherige Ergebnisse

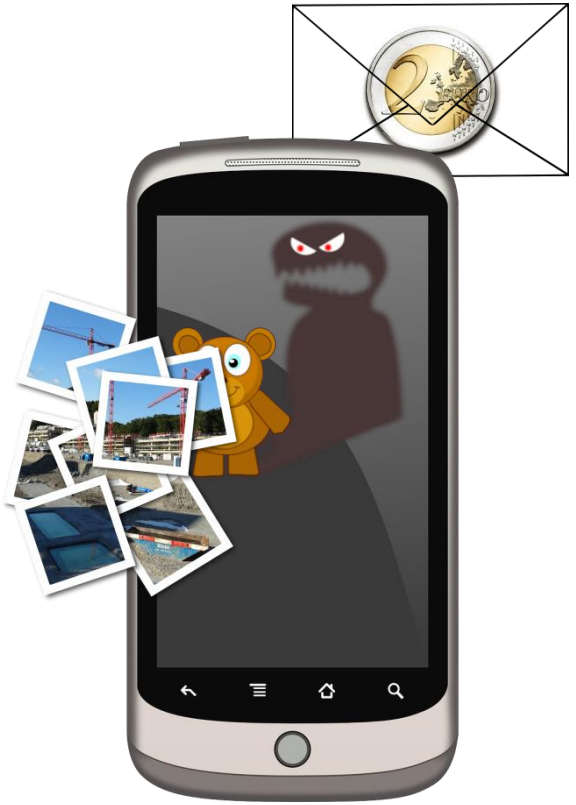


- Aufbau der notwendigen Client-Server-Umgebung
- Erstellen der Schadsoftware
  - bei AndroRAT: *.apk (APK Binder nicht trivial)
  - bei Dendroid: mit Toolkit geliefert
- Wie wird das Smartphone infiziert?
  - Google Play Store
  - Alternativer App Store
  - *.apk installieren
  - Manipulierte Webseite
  - System Sicherheitslücke

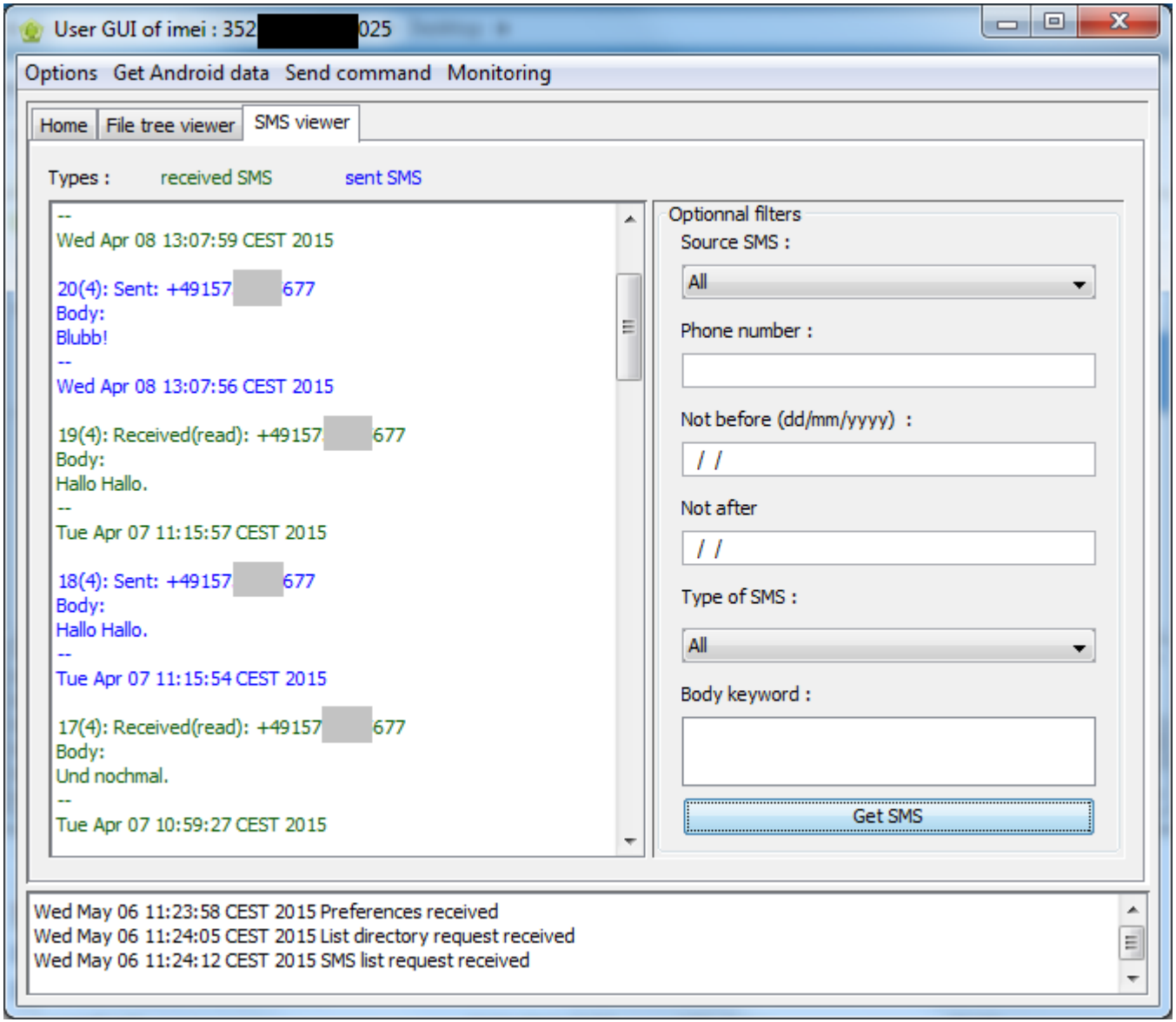
# Bisherige Ergebnisse



# Bisherige Ergebnisse

# Sicht des Angreifers



# Bisherige Ergebnisse



- Wie könnte eine Infektion erkannt werden?
  - Installierte App ohne Funktion
  - Standortermittlung aktiv

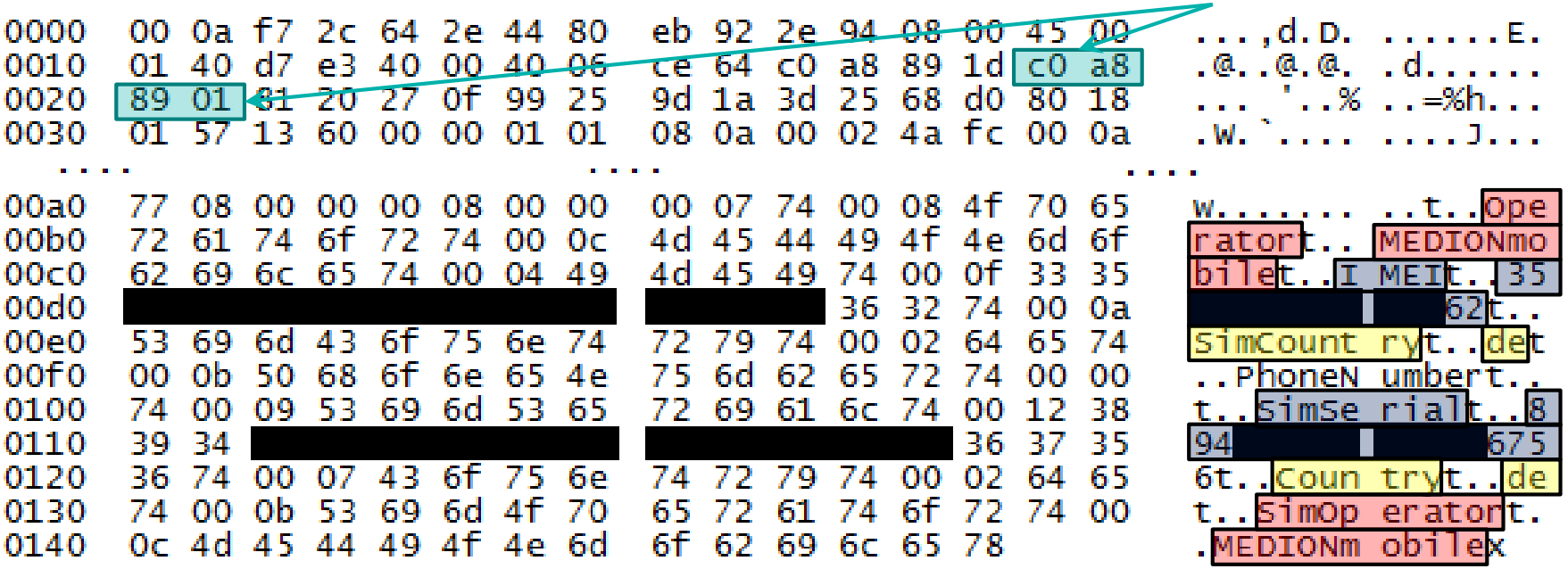

  - Unbekannte Audio-, Video- oder Bilddateien
  - Virenscanner App
    - Erkennungsrate ~ 86% (AndroRAT)
  - Intrusion Detection System
    - Business Bereich
  - Analyse Datenverkehr (beide unverschlüsselt)
  - Analyse RAM-Image

# Bisherige Ergebnisse



- Ermitteln aus Datenverkehr:
  - Wer hat mich infiziert?

IP Adresse AndroRAT Server




Netzbetreiber

IMEI & Sim Seriennummer

Ländercode

# Bisherige Ergebnisse



- Ermitteln aus Datenverkehr:
  - Welche Aktivitäten werden ausgeführt?

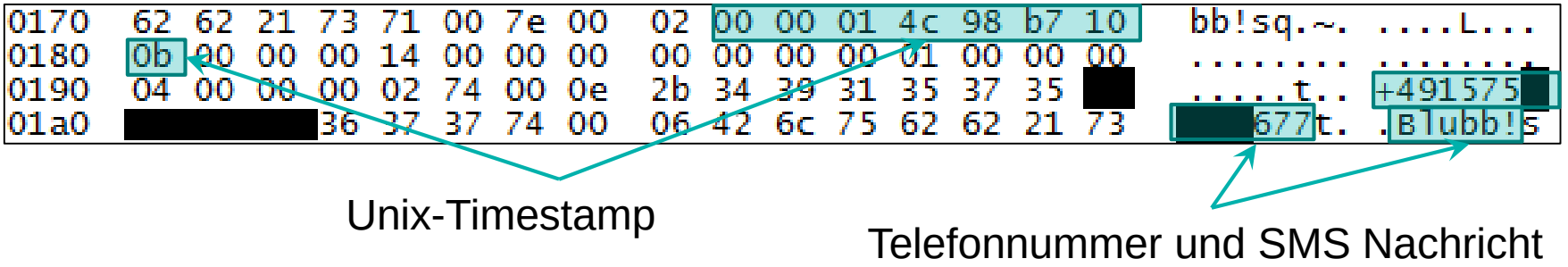
```
0040   df 24 00 00 00 06 00 00   00 06 01 00 00 00 00 00   .$...... ........
0050   00 00 71 00 00 00 92                               ..q....
```

Identifikationsnummer der Anfrage (hier: Alle SMS zusenden)

# Bisherige Ergebnisse



- Ermitteln aus Datenverkehr:
  - Welche Daten werden mir geklaut?



# Ausstehend Ergebnisse



- Ermittlung aus RAM Dump
- Wie kann ich mein Smartphone bereinigen?
- Wie kann ich die Infektion verhindern?

# Fragen?



Vielen Dank für ihre Aufmerksamkeit!