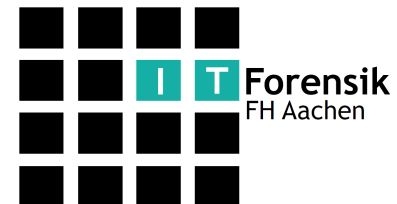


# IT-forensische Analyse von Windows 10 Mobile

Simon Ebbers  
Polizeipräsidium Münster  
KK 35 Cybercrime



- Motivation
- Stand der Technik
- Manuelle Untersuchung
- Automatisierte Analyse
- Ergebnisse und Fazit

- 3,3% Windows Smartphone in Deutschland
- 14% davon mit Windows 10 Mobile
- Keine Lösung von UFED und XRY zu W10M
- 95% eine Umfrage gaben an, dass mobilen Geräte wichtigste Datenquelle bei IT-forensischen Untersuchungen
  
- Ziel: Standardwerk auf dem Untersuchungen zu W10M aufbauen können

- Windows Phone/Mobile

- Adrian Leong - Cheeky4n6Monkey Blog
- Cindy Murphy - Windows Phone 8 Forensic Artifacts.
- Gabriele Zambelli - Windows Phone 7.8 Forensics

- Windows 10

- A. Majeed, H. Zia, R. Imran, S. Saleem - Forensic Analysis of three Social Media Apps in Windows 10
- Alex Parsons - Windows 10 Forensics Part 2: Facebook Forensics
- Brent Muir - Windows 10 Forensics: OS Evidentiary Artefacts

- Was vorherige Arbeiten anbieten
  - Wo werden welche Informationen gespeichert
  - Einzelne Auswertungen von Informationen
- Was vorherige Arbeiten nicht anbieten
  - Analyse von Windows 10 Mobile
  - Automatisierte Analyse

- Testgerät
  - Nokia Lumia 520 mit Windows 10.0.10568.107
- Datensammlung
  - Windows Phone Internals
- Datenanalyse
  - FTK Imager
  - Hexedit
  - ESEDatabaseView

- Windows Phone Internals
  - Bootloader entsperren
    - Full Flash Update (FFU) Image des aktuellen Systems
    - Emergency Flash Loader des aktuellen Systems
    - entsprechende Secure Boot Loader (SBL) 3 Partition
  - Backup durch Mass Storage Mode
    - Data.bin (NTFS), Anwendungen und Benutzerdaten
    - EFIESP.bin (FAT16), OS Loader und model-spezifische Einstellungen
    - MainOS.bin (NTFS), Betriebssystem, Treiber und Konfigurationen

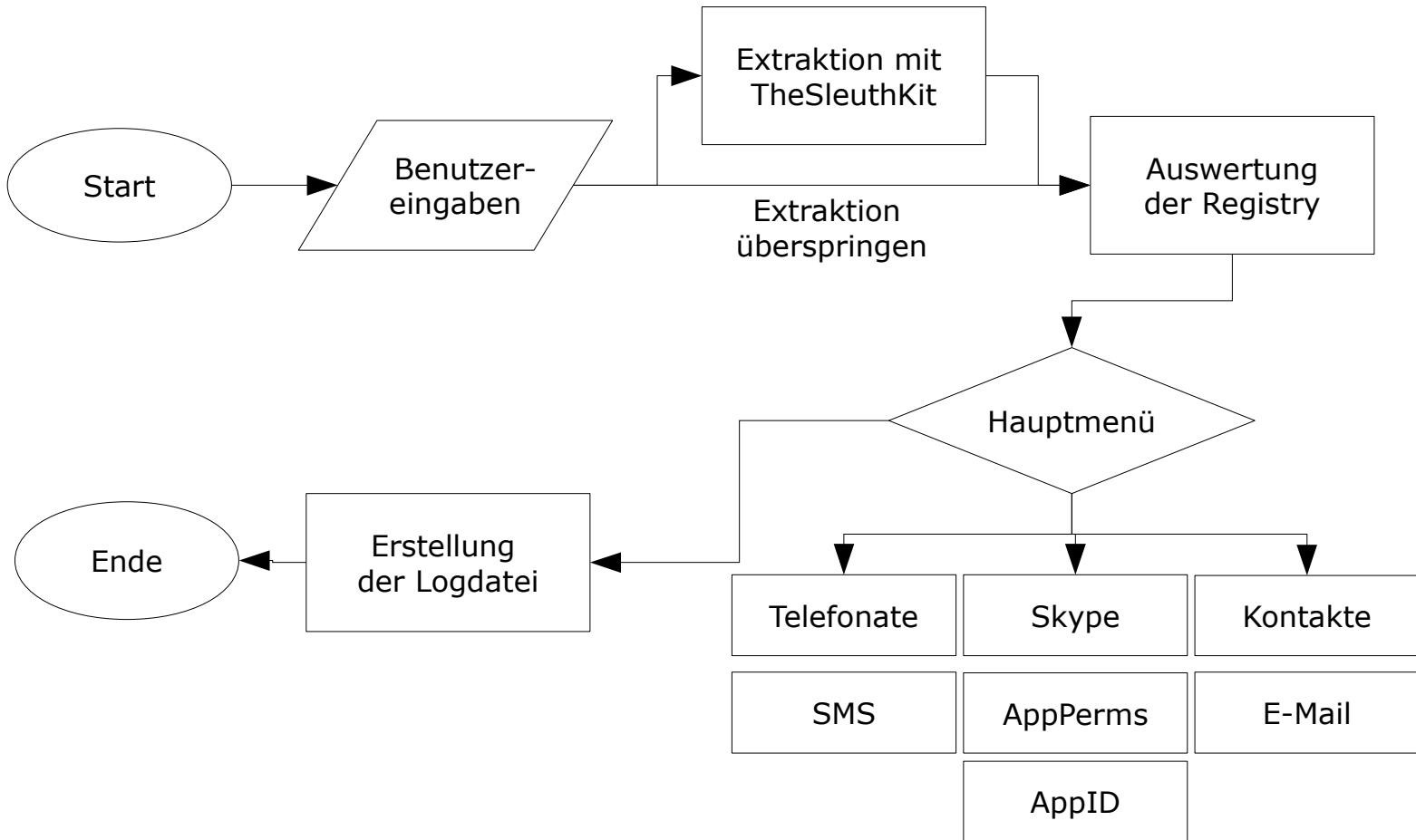


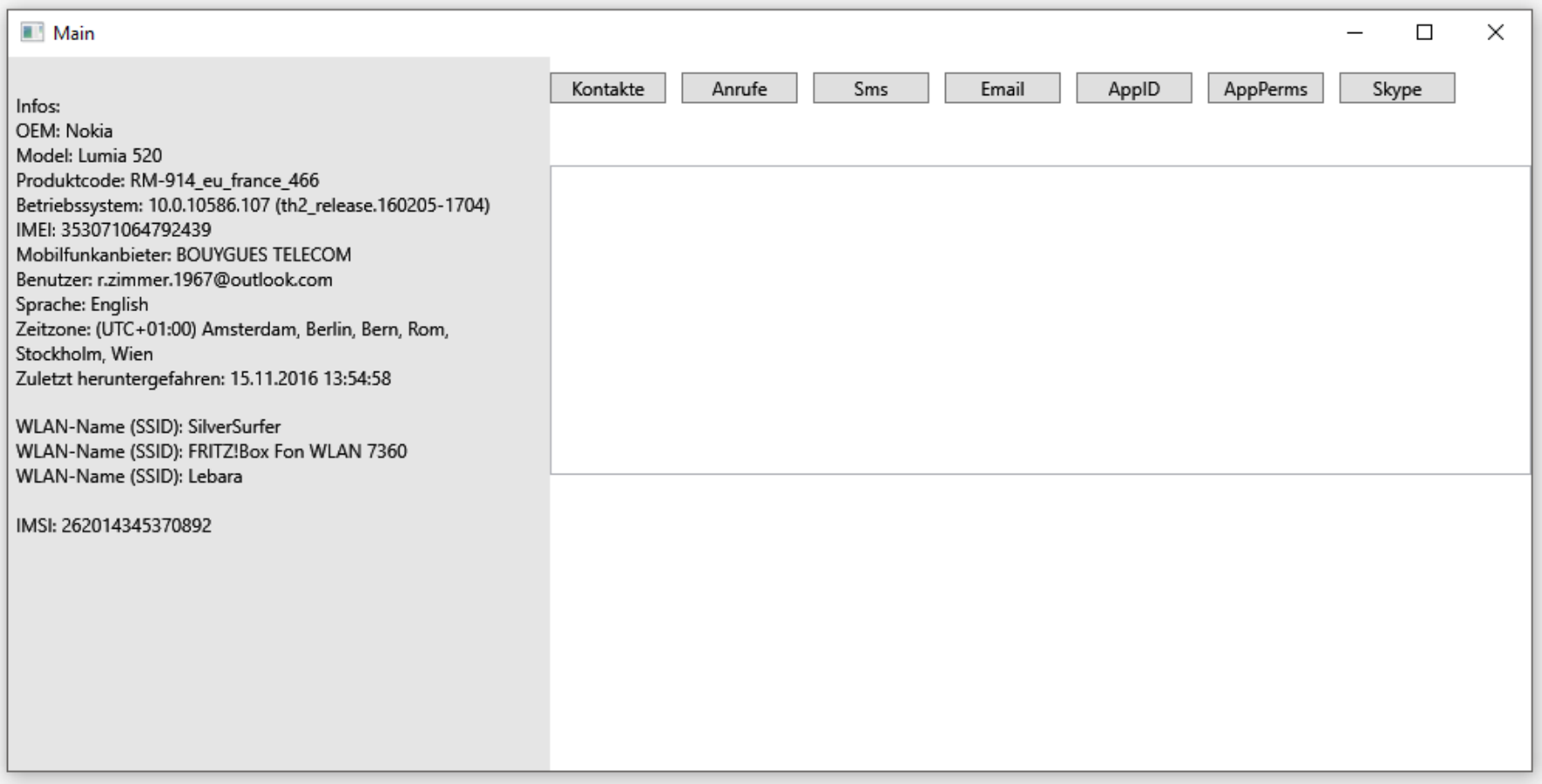
## ■ Data.bin

- Appverzeichnis
  - \PROGRAMS\
- Benutzerdaten der Apps
  - \Users\DefApps\APPDATA\Local\Packages\
- Multimediadateien des Benutzers
  - \Users\Public\
- Anruf-, SMS-, E-Mail- und Kontakte-Informationen
  - \Users\DefApps\APPDATA\Local\comms\UnistoreDB\store.vol
- E-Mail-Inhalte und -Anhänge
  - \SharedData\Comms\Unistore\data\

- MainOS.bin
  - Registry
    - \Windows\system32\

- Verwendete Software / Programmiersprachen
  - Windows Presentation Foundation (WPF)
  - C#
  - The SleuthKit 4.3.0
  - Python 2.7
  - Nirsoft ESEDatabaseView 1.42
  - Eric Zimmermann offline Registry parser





The screenshot shows a software window titled "Main" with a standard Windows-style title bar (minimize, maximize, close buttons). The interface is divided into two main sections. On the left is a grey sidebar containing device information under the heading "Infos:". On the right is a white main area with a horizontal menu of buttons at the top and a large empty space below.

**Infos:**  
OEM: Nokia  
Model: Lumia 520  
Produktcode: RM-914\_eu\_france\_466  
Betriebssystem: 10.0.10586.107 (th2\_release.160205-1704)  
IMEI: 353071064792439  
Mobilfunkanbieter: BOUYGUES TELECOM  
Benutzer: r.zimmer.1967@outlook.com  
Sprache: English  
Zeitzone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien  
Zuletzt heruntergefahren: 15.11.2016 13:54:58

WLAN-Name (SSID): SilverSurfer  
WLAN-Name (SSID): FRITZ!Box Fon WLAN 7360  
WLAN-Name (SSID): Lebara

IMSI: 262014345370892

Navigation buttons: Kontakte, Anrufe, Sms, Email, AppID, AppPerms, Skype

**Simon Ebbers**

16:59



**Ich**

Hallp

**Simon Ebbers**

Hallo 😊

Wie geht es dir ?

**Ich**

Ganz gut 👍

Lass mal kurz telefonieren

📞 Anruf begonnen

17:01

Chats Calls

live:r.zimmer.1967 simcard93

simcard93 18.01.2017 16:59:14  
<ss type="penguin">(penguin)</ss>

live:r.zimmer.1967 18.01.2017 16:59:34  
Hallp

simcard93 18.01.2017 16:59:53  
Hallo 😊

simcard93 18.01.2017 17:00:01  
Wie geht es dir ?

live:r.zimmer.1967 18.01.2017 17:00:25  
Ganz gut <ss type="yes">(y)</ss>

live:r.zimmer.1967 18.01.2017 17:00:46  
Lass mal kurz telefonieren

simcard93 18.01.2017 17:01:02  
<partlist type="started" alt="">  
  <part identity="live:r.zimmer.1967">  
    <name>live:r.zimmer.1967</name>  
    <duration>29</duration>  
  </part>  
  <part identity="simcard93">  
    <name>Simon Ebbers</name>  
    <duration>29</duration>  
  </part>  
</partlist>

- Aktuelle Version der Analysesoftware
  - SMS, Kontakte, Telefonate, E-Mails
  - Multimediadateien
  - IMSI, IMEI, SSIDs, Systemzeit
  - Chats und Telefonate der Skypeapp
  - unterstützende Funktionen für weitere Appanalysen

- Unterstützung bei Untersuchung, Datenanalyse und Dokumentation
- Standardwerk, auf dem Untersuchungen zu W10M aufbauen können
- Erweiterungsmöglichkeiten:
  - Weitere Geräte überprüfen und ggf. anpassen
  - Weitere OS- und App-Versionen überprüfen und ggf. anpassen