FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-forensische Analyse von Windows 10 Mobile

Simon Ebbers
Polizeipräsidium Münster
KK 35 Cybercrime

IT Forensik
FH Aachen

Gliederung

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

Motivation

- 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: Standartwerk auf dem Untersuchungen zu W10M aufbauen können

Stand der Technik (1/3)

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

Stand der Technik (2/3)

- 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

Stand der Technik (3/3)

- 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

Manuelle Untersuchung (1/4)

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

Manuelle Untersuchung (2/4)

- 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

Manuelle Untersuchung (3/4)

- 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\

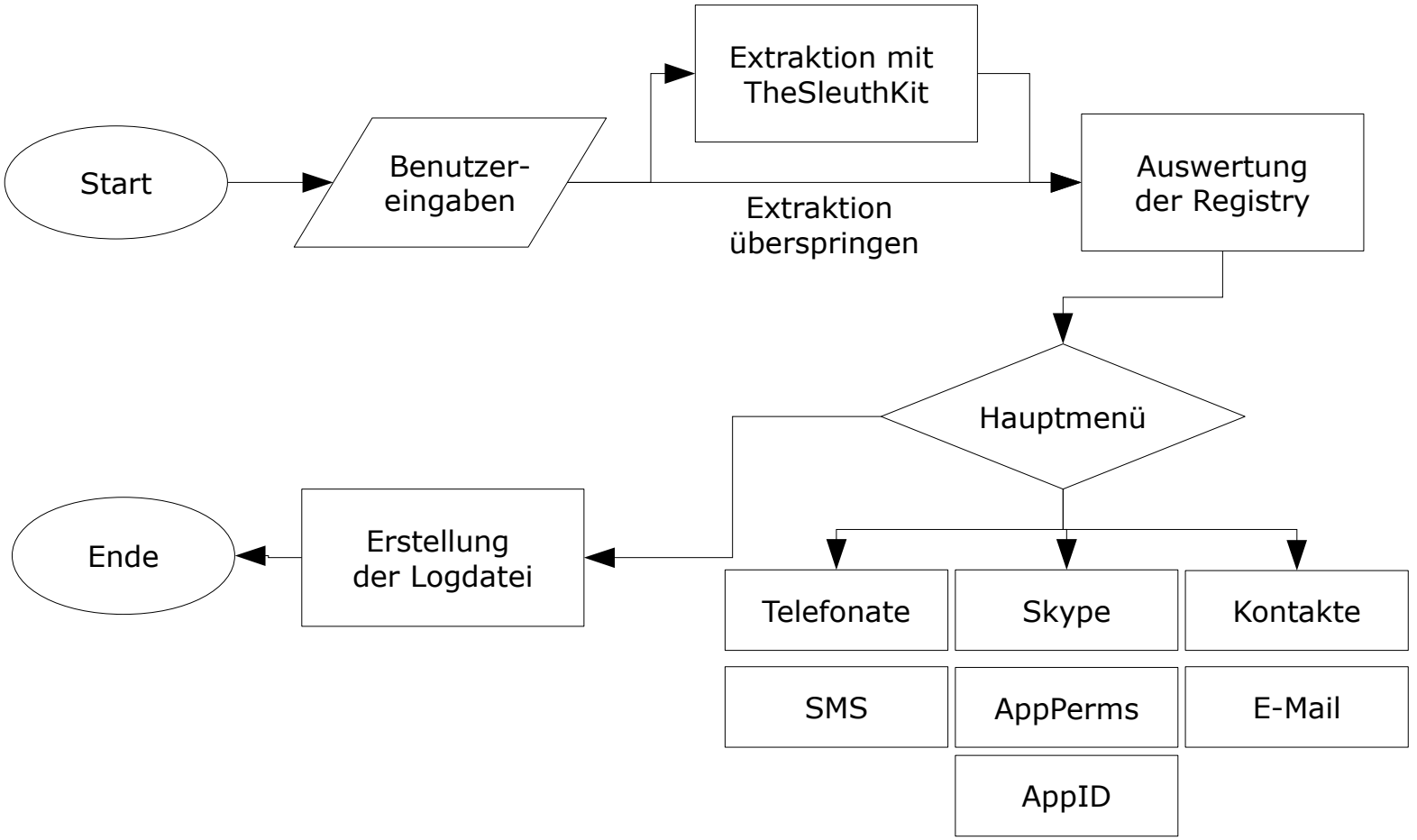
Manuelle Untersuchung (4/4)

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

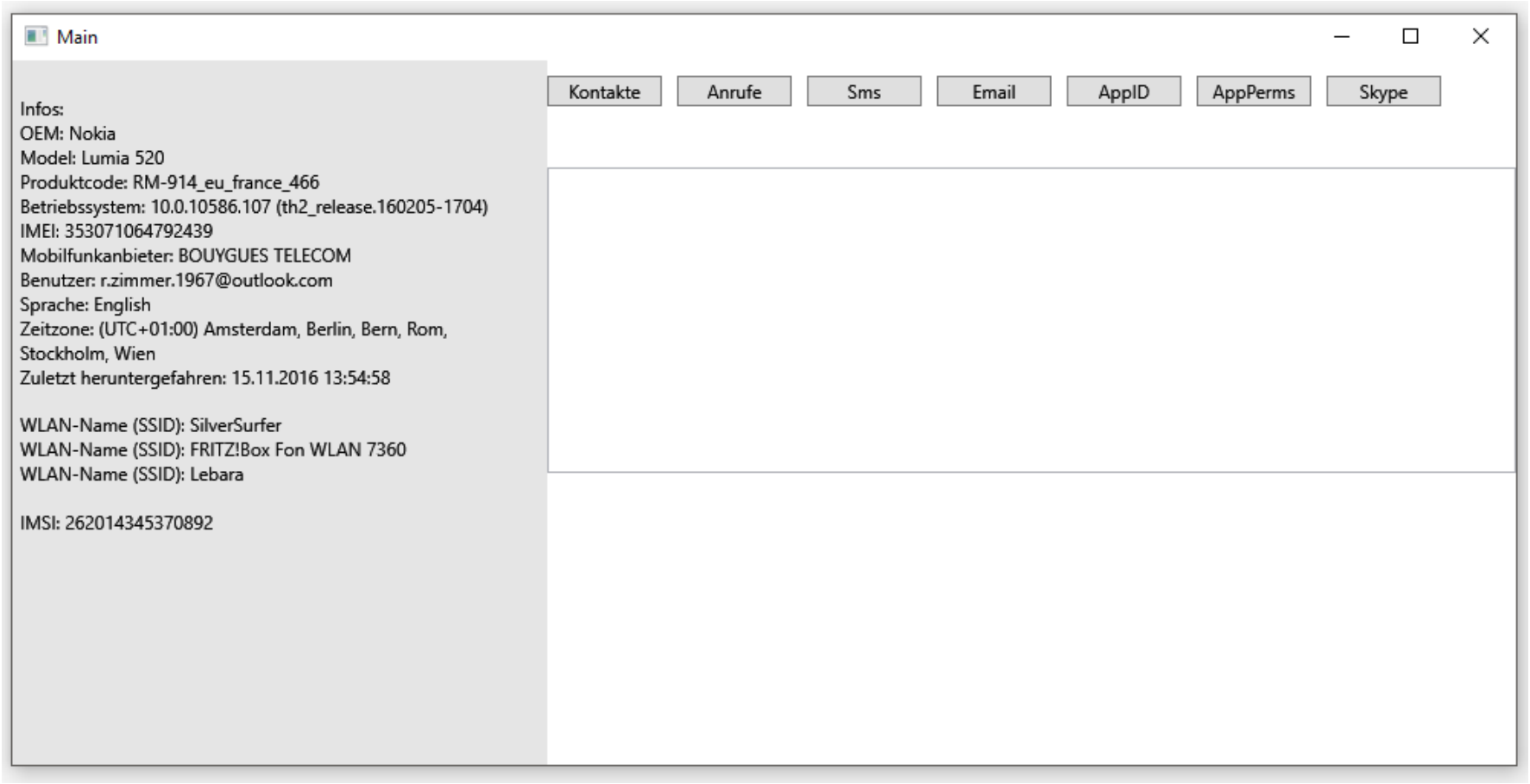
Automatisierte Analyse (1/4)

- 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

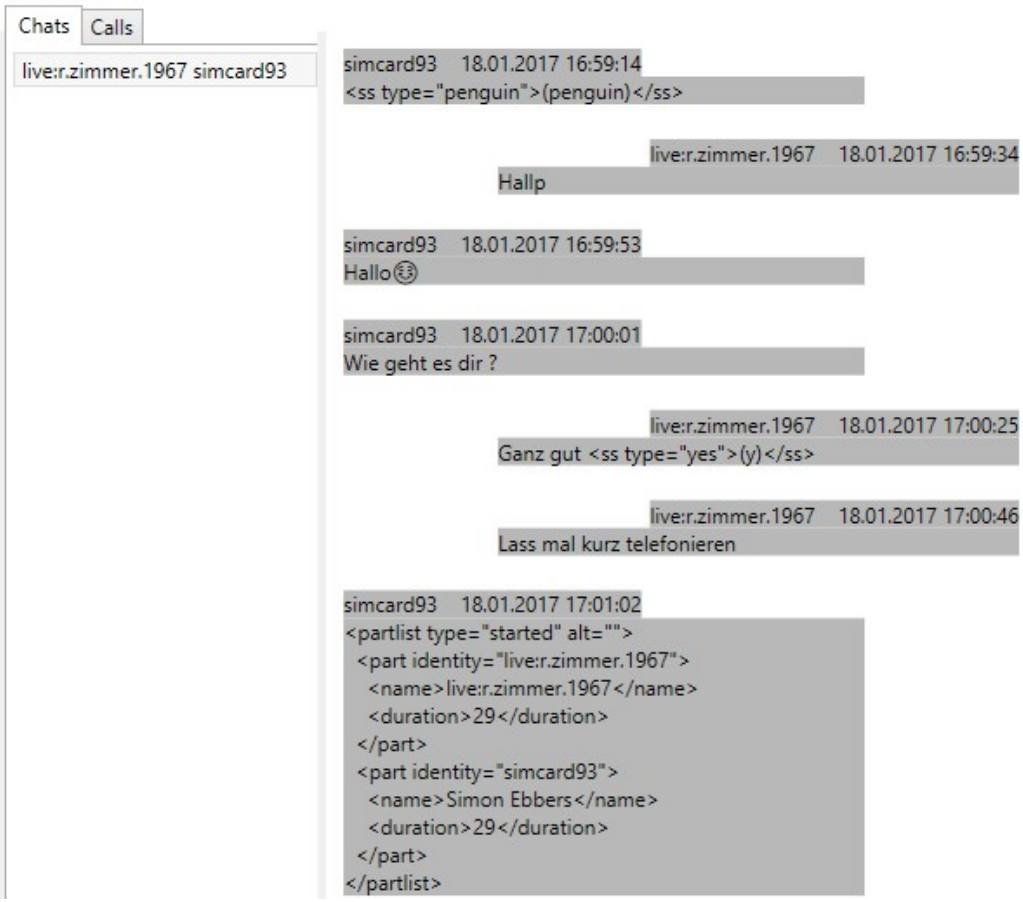
Automatisierte Analyse (2/4)



Automatisierte Analyse (3/4)



Automatisierte Analyse (4/4)



Ergebnisse und Fazit (1/2)

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

Ergebnisse und Fazit (2/2)

- 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