Handy - Forensik

Lars Wolleschensky
Seminar ITS
Ruhr-Universität Bochum
SS 2007

Gliederung

1. Einleitung
2. Prozess
3. Entwicklung

Einleitung (1)

Forensik

kriminelle Handlungen werden systematisch identifiziert, analysiert oder rekonstruiert (wikipedia)

Relevanz

- hoher Verbreitungsgrad
  - mindestens ein Handy in mehr als 80% aller Haushalte
  - 84% der 13- bis 22-Jährigen
  - 32,6 Millionen umgesetzte Mobiltelefone pro Jahr
- mehr als “simples” telefonieren
  - 34 SMS pro Nutzer und Monat
  - Digitalkamera
  - Terminplaner

Einleitung (2)

Beweisstücke

- Adressbuch
- ein- und abgehende Anrufe
- SMS (gesendet / empfangen)
- Kalender
- Photos/Video
- GSM Location Register

... und andere

Konservierung und Dokumentation

- andere Spuren auf dem Handy sichern
- Dokumentation!!!

Erfassung

- Daten müssen zugänglich gemacht werden
    - Screenshots
    - Software
    - Bit exakte Speicherkopie

- Telefon vs. SIM Karte

Prozess

Analyse

- Suche nach relevanten Informationen
- zum Teil automatisiert

Dokumentation

- was, wie, wann, wo gemacht
- warum
- zum Teil Jahre zwischen Untersuchung und Strafprozess
- nachvollziehbar für die Gegenseite (Wiederholbarkeit)

Probleme in der Praxis

Probleme

Vielfalt

- Handy identifizieren
  - Webseiten, die helfen (gsmarena.com, phonescoop.com)
- Kabel finden oder kaufen (Strom, Daten)
- vertraut machen
- kompatible Software einsetzten
- auf dem neusten Stand bleiben

PIN/PUK

- Personal Identifikation Nummer
- Personal Unblocking Key
  - mit dem Verdächtigen sprechen
  - Netzbetreiber

On vs. Off

On
- keine PIN
- Datenverlust auf SIM Karte

Off
- kein Datenverlust im Datenbereich
- Remotewipe
- SMS überschreiben
- kein Faradaykäfig
- mehr Zeit, um Stromversorgung zu garantieren
- ist Tradition ...

Probleme

Software

- Produktvielfalt
- Kompatibilität
- Zuverlässigkeit
- Features
- SIM Karte
- Preis
- Zertifikate

JTAG

Joint Test Action Group

- direkte Kommunikation mit dem Schaltkreis
- kein Betriebssystem

Aber

- fragmentierte, HEX Daten
- kein Dateisystem
- individuelle Befehle für jeden Chipsatz
- keine Unterstützung durch die Hersteller

Flasher Boxen

- herstellerspezifisch
- zum Teil offiziell unterstützt
- lesen Speicher direkt aus

Aber:

- illegale Zielsetzung (Unlock)
- Black Box
- Datenintegrität?
- vor Gericht nicht zugelassen

Fragen, Kommentare?

Quellen

Bitte lesen!

Paolo Gubian Antonio Savoldi. Sim and Usim Lesesystem: a forensics perspective. Proceedings of the 2007 ACM symposium on Applied computing, 2007.

Michael Harrington. Hex Dumping Primer. 2004.

Coert klaver Ronal van der Knij
Marcel Breeuwsma, martien de Jongh
and Mark Roelos. Forensic data recovery from Fash memory. Small Scale Digital Device Forensics Journal, 1, 2007.

Rick Ayers Wayne Jansen. Guidelines on Cell Phone Forensics. 2007.

Probleme in der Praxis

Vielfalt (1)

- Hersteller (Nokia, Siemens, Motorola …)
- Modelle
- Betriebssysteme
- Anschlüsse
- Stromversorgung
- Software
- Features (Kamera, Office ...)
- Netzbetreiber (Features sperren)

Viele neue Produkte!

Zukunft

Hardware

- Moore's Law
    - Speicher
        - 4 Gigabyte SIM Karte
        - Festkörper Festplatten
- Prozessoren

DRM

- verschlüsseltes Betriebssystem (Motorola)
- verschlüsselte Daten
- DRM