FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Vergleich von XRY, UFED und anderen Analysetools

Adam Pospiech

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik

IT Forensik
FH Aachen

Aufgabenstellung

- Analysesoftware vergleichen
  - Gemeinsamkeiten
  - Unterschiede
  - Alternativen
- Report-Korrelation (DIRECT)
  - Korrelation mehrerer Reports
    - Gleiches Gerät
    - Unterschiedliche Geräte
  - Unterstützung durch zusätzliche Software

Software

- Kommerzielle
  - Cellebrite - UFED
    - Physical Analyzer
    - Logical Analyzer
  - Micro Systemation (MSAB) - XRY
    - Physical
    - Logical

Software

- Kostenlose
  - Cryptic Bit - iPhone Analyzer
    - Apple Only (bis iOS 5)
  - ViaForensics - AFLogical
    - Android Only
  - TULP2G
    - C# Framework
  - BitPim

Geräte

- Ebay
  - Sony Xperia U (Android)
    - Privat
  - Nokia Lumia 800 (16GB) (Windows Phone)
    - ReBuy
  - BlackBerry Curve 8520 (BlackBerry OS)
    - Privat
  - iPhone 3GS/4 (iOS)
    - Privat

DIRECT-Integration

- **DI**gital **RE**port **C**orrelation **T**ool
  - Aktueller Stand
    - Dynamische Korrelation von Daten forensischer Berichte
      - Christoph Beckmeyer
    - Projekt-Seite:
      - http://www.it-forensik.fh-aachen.de/projekte/direct
  - Erweiterung
    - Freeware
    - Anrufe
    - Multimedia

Ende

Noch Fragen?