FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT First Responder App

Philipp Heischkamp

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik

IT Forensik
FH Aachen

Gliederung

- **Stand der Technik**
- Herausforderung
- Aufbau des ISO/IEC 27037:2012
- Realisierung als Applikation
- Fazit

Stand der Technik

Bereits große Auswahl an forensischer Tools zur Auswertung digitaler Geräte verfügbar

Aber: noch kein Tool, das einen IT First Responder durch den gesamten Ablauf an einem Tatort führt

aktuell nur einzelne Leitfäden in Textform:

- ISO/IEC 27037
- „Leitfaden IT Forensik“ des BSI

Gliederung

- Stand der Technik
- **Herausforderung**
- Aufbau des ISO/IEC 27037:2012
- Realisierung als Applikation
- Fazit

Herausforderung

Probleme von schriftlichen Leitfäden in der Praxis:

- sehr detailliert
  - z.B. „Leitfaden IT Forensik“ mit über 300 Seiten eher Nachschlagewerk
- manchmal umständlich
  - nicht besonders benutzerfreundlich

Lösung:

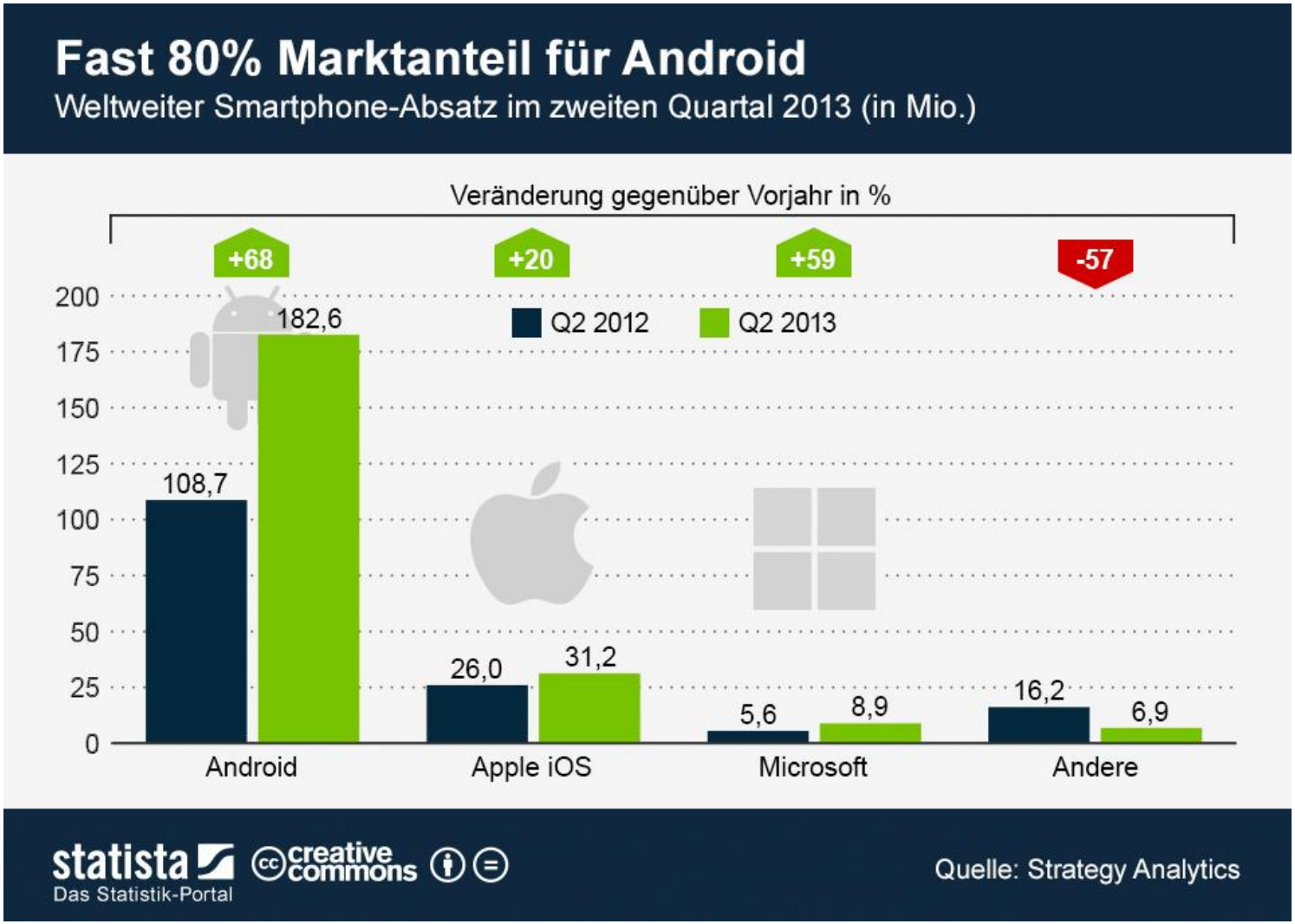
- Umsetzung des ISO/IEC 27037:2012 als Smartphone Applikation

Herausforderung

Warum als Smartphone Applikation?

- Nahezu jeder besitzt ein Smartphone
- Einfacher zu transportieren als Laptops
- Bieten zusätzliche Funktionen, die genutzt werden können (z.B. Kamera)

Herausforderung



Gliederung

- Stand der Technik
- Herausforderung
- **Aufbau des ISO/IEC 27037:2012**
- Realisierung als Applikation
- Fazit

Gliederung

Kompetenz:

- Ausreichende Ausbildung im Umgang mit forensischen Tools
- Ausreichendes rechtliches und technisches Verständnis

→Zielgruppe: autorisiertes, ausgebildetes und qualifiziertes Personal

Aufbau des ISO/IEC 27037:2012

ISO/IEC 27037 hat 4 Abschnitte:

- Generelle Informationen/Richtlinien
- Identifikation
  - Identifizieren der betroffenen Geräte
  - Dokumentieren der Geräte
- Collection und Acquisition
  - Beschlagnahmung/Auswertung der Geräte
  - Mögliches Vorgehen in Entscheidungsbaum dargestellt
- Preservation und Transport
  - Richtlinien die zur Aufbewahrung/Transport der Geräte beachtet werden müssen

Gliederung

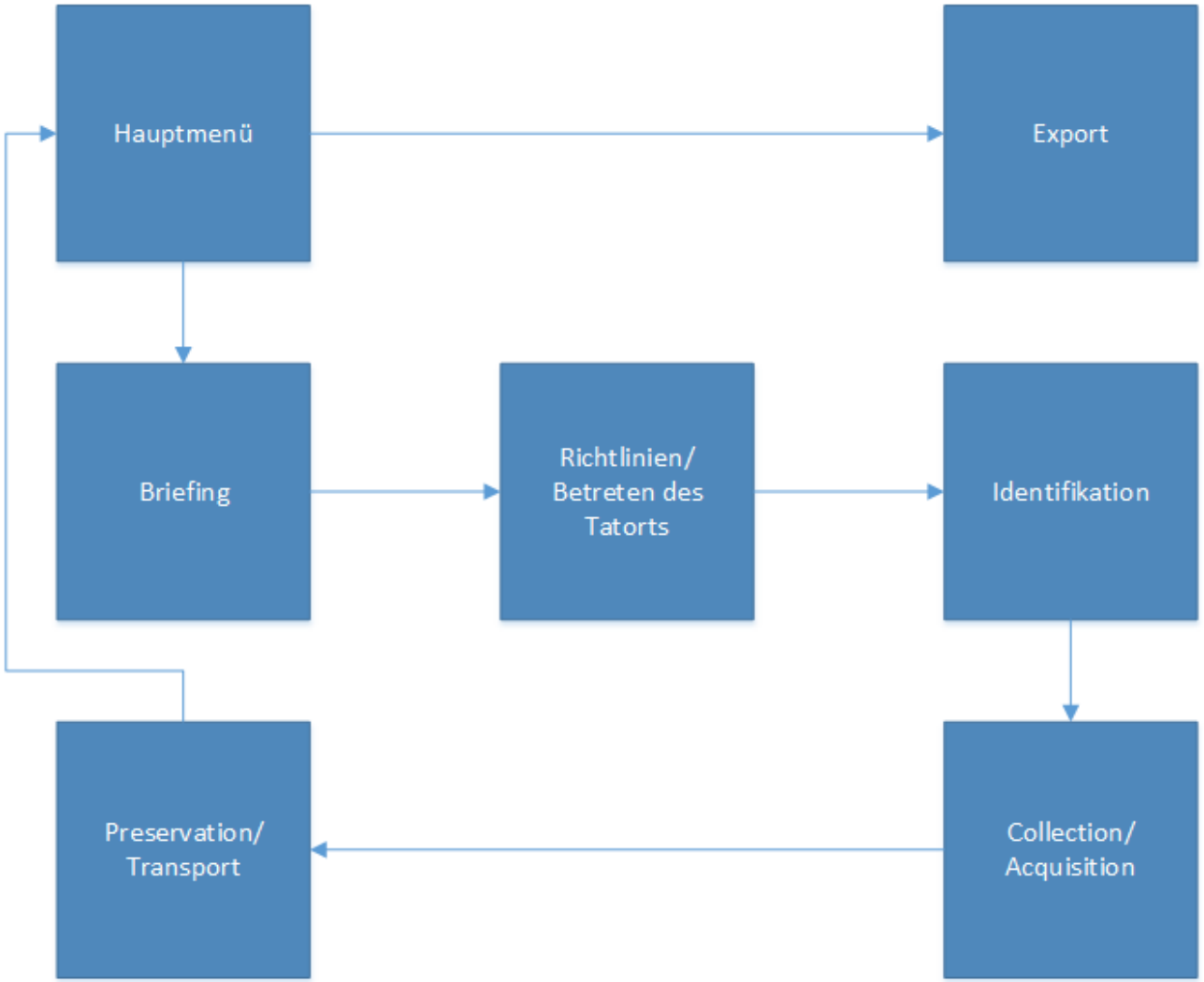
- Stand der Technik
- Herausforderung
- Aufbau des ISO/IEC 27037:2012
- **Realisierung als Applikation**
- Fazit

Realisierung als Applikation

Features der Android Applikation:

- Umsetzung des ISO → durch Befolgen der Richtlinien sind Beweise gerichtsverwertbar
- Digitale Dokumentation aller Eingaben
- Smartphone-Kamera zur Dokumentation nutzen
- Erstellen eines Abschlussberichts, der alle eingegebenen Daten und Bilder enthält

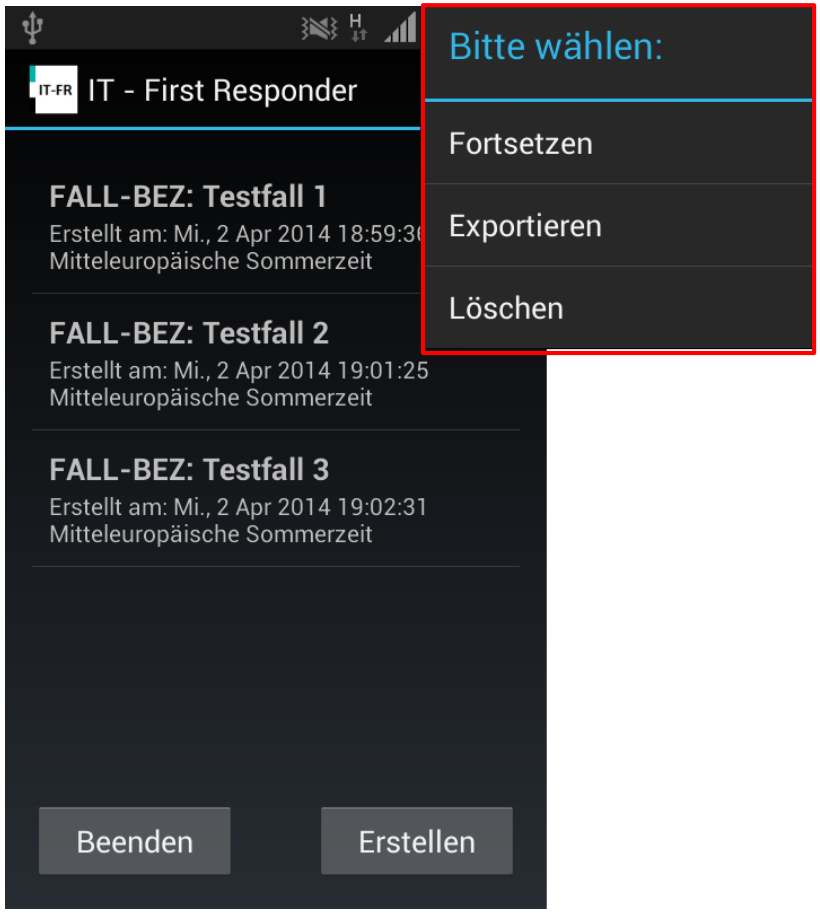
Realisierung als Applikation



Realisierung als Applikation

Hauptmenü:

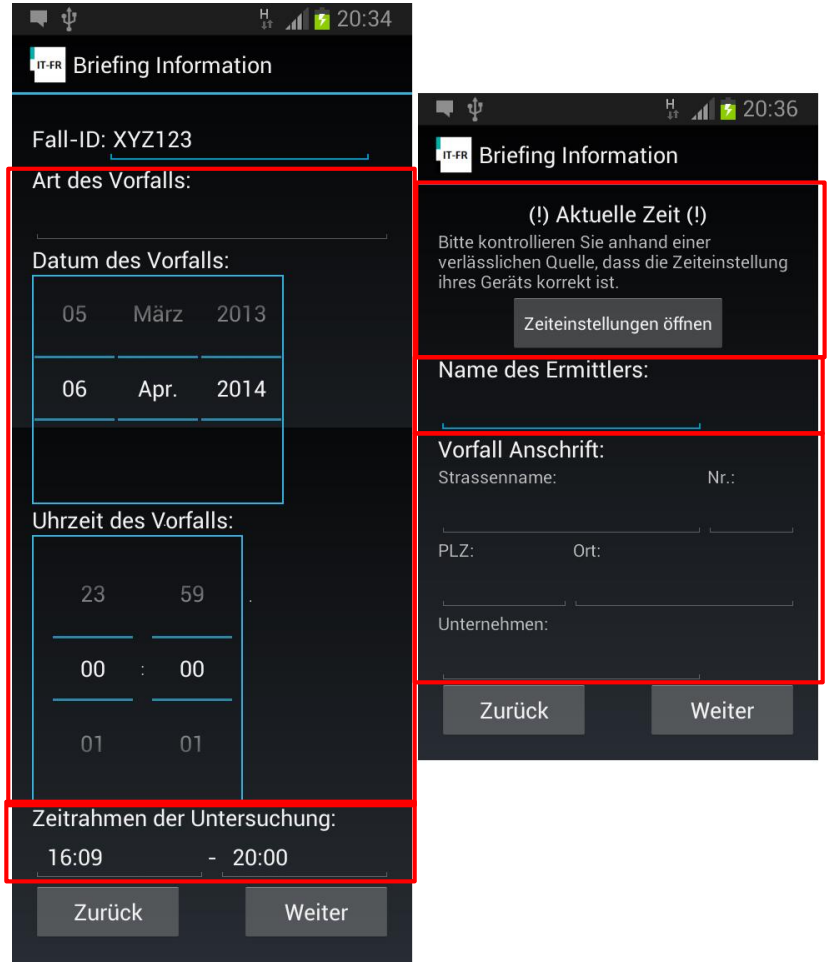
- Verwaltung der Fälle
  - Fortsetzen, Exportieren und Löschen möglich
- Neuer Fall kann hier erstellt werden



Realisierung als Applikation

Briefing Informationen:

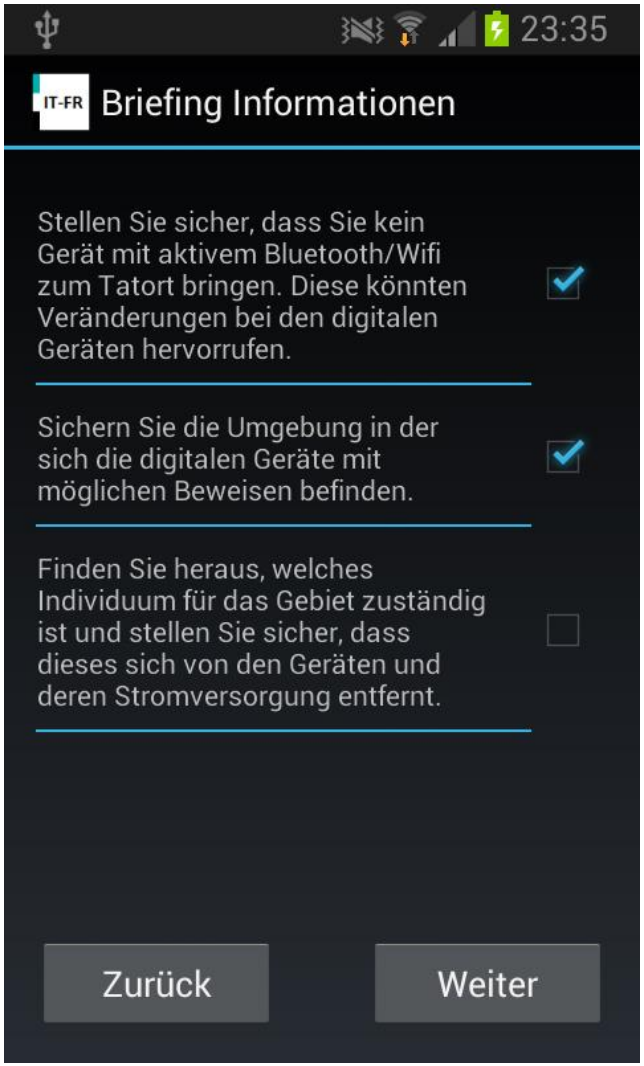
- Dokumentation aller Briefing Daten
  - Art, Datum und Uhrzeit des Vorfalls
  - Zeitrahmen der Untersuchung
  - Ermittler
  - Anschrift des Vorfalls
- Überprüfen der Zeiteinstellung
  - Dokumentierte Zeiten sind korrekt



Realisierung als Applikation

Richtlinien:

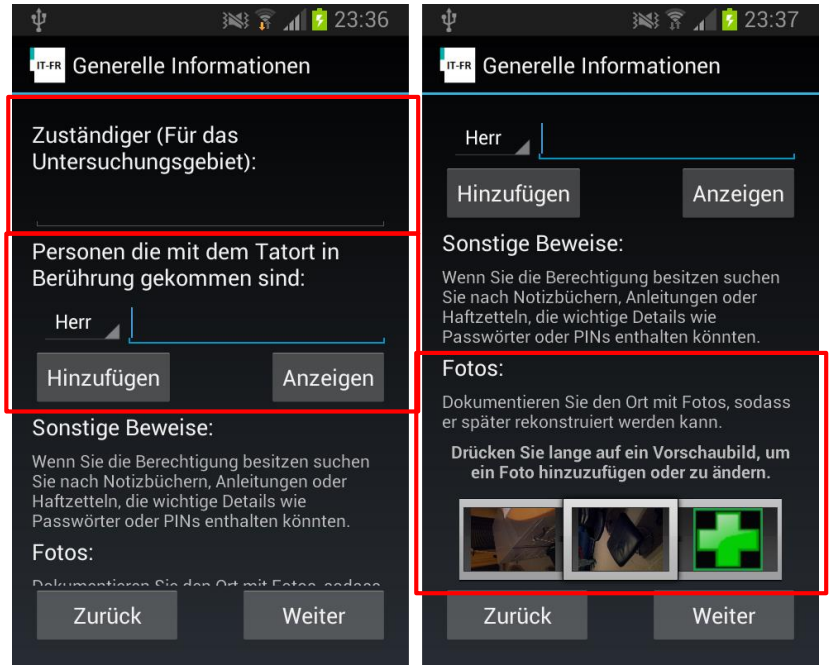
- Stellen richtiges Verhalten sicher
- Müssen bestätigt werden



Realisierung als Applikation

Dokumentation des Tatorts:

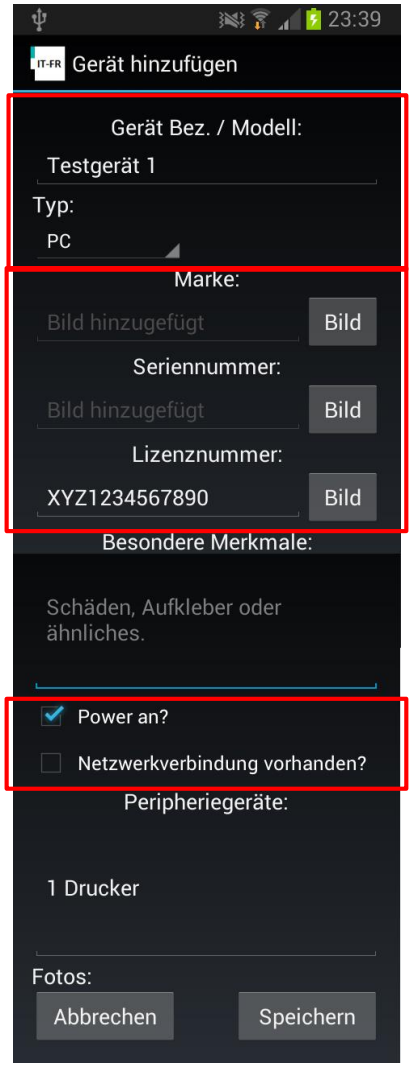
- Zuständiger vor Ort
- Personen die Kontakt mit Geräten hatten
- Fotos des Tatorts zur Rekonstruktion



Realisierung als Applikation

Identifikation:

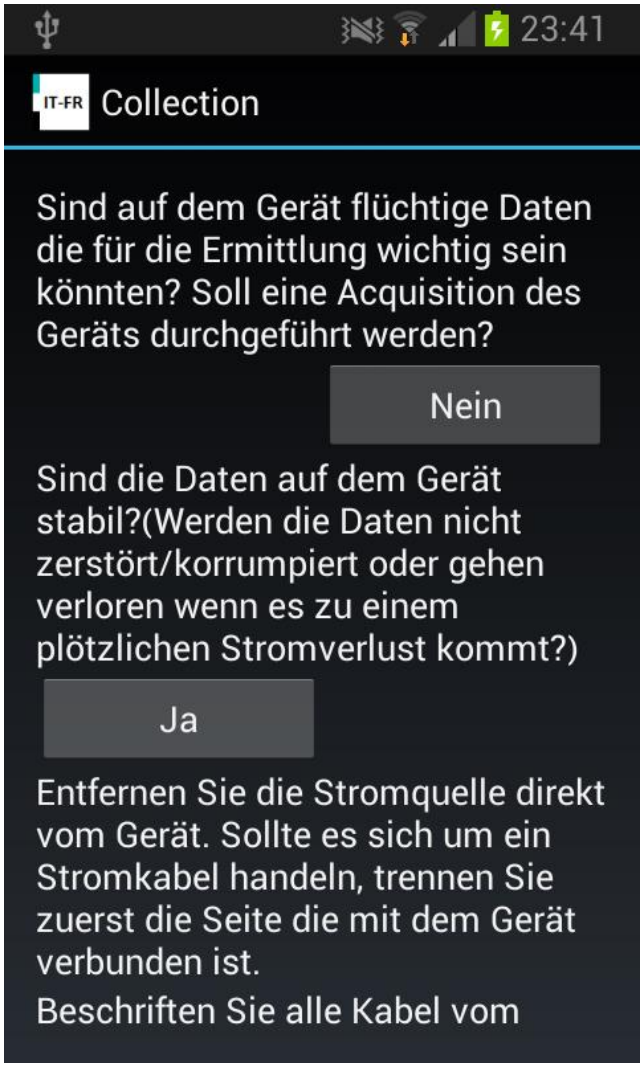
- Übersicht aller Geräte
- Identifikationsdialog für jedes Gerät
  - Bezeichnung und Typ des Geräts wählen
  - Marke, Serien- und Lizenznummer per Foto
  - Power-/Netzwerkstatus wichtig für weitere Bearbeitung
  - Fotos des Geräts z.B. der Verkabelung



Realisierung als Applikation

Collection/Acquisition:

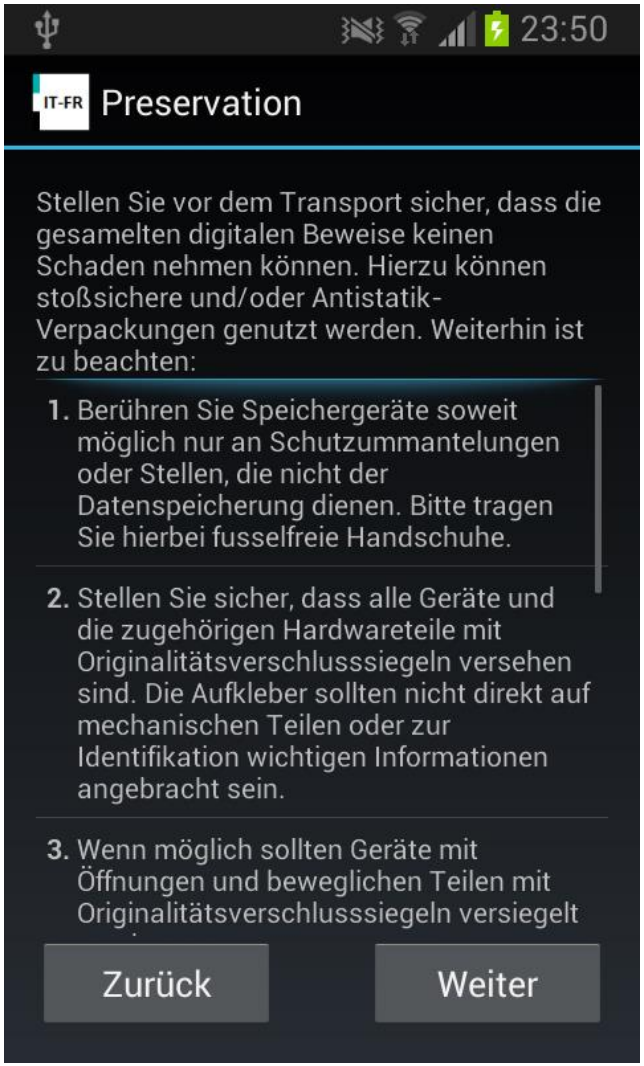
- jedes Geräts wird einzelnd bearbeitet
- Entscheidungsbäume wie im ISO
- Power- & Netzwerk-status entscheiden über mögliche Wege
- Eigene Bearbeitung von CCTV-Systemen



Realisierung als Applikation

Preservation/Transport:

- Auflistung von Richtlinien um Schaden zu verhindern
  - Tragen von Handschuhen
  - Fortführen der Chain of Custody



Realisierung als Applikation

Export:

- Automatisches Erstellen eines Berichts
  - HTML und XML
- Erstellen von SHA-256 Hashes zu allen Bildern
- Automatisches Zusammenfügen aller Bilder und Berichte
  - Als ZIP-Archiv

Realisierung als Applikation

Aufgenommene Geräte
Anzahl: 2

1. Gerät: Testgerät 1
Eingetragen: Tue May 06 13:56:45 MESZ 2014

Typ:	PC
Marke:	IT_FirstResponder_29_20140506_135528.jpg
Seriennummer:	XYZ1234567890
Lizenznummer:	IT_FirstResponder_29_20140506_135544.jpg
Netzwerkverbindung:	Deaktiviert
Power:	An
Merkmale:	keine besonderen Merkmale
Peripheriegeräte:	
Weiter bearbeitet:	Tue May 06 13:58:05 MESZ 2014
Weg der Bearbeitung:	Es sind keine flüchtigen Daten auf dem Gerät für die eine Acquisition durchgeführt werden muss. --Die Daten auf dem Gerät sind nicht stabil und es kann, bei plötzlichem Stromverlust, zu Datenverlust kommen. --Das Gerät wurde ordnungsgemäß heruntergefahren. --Alle Kabel des Geräts wurden beschriftet und anschliessen entfernt. Tape wurde über den Stromschalter platziert um versehentliches verstellen zu verhindern. --CD/DVD/Disketten Laufwerke wurden (falls vorhanden) mit Tape verschlossen.

Gerät Fotos: 4

Dateiname	Aufnahmezeit
IT_FirstResponder_29_20140506_135528.jpg	Tue May 06 13:55:40 MESZ 2014
IT_FirstResponder_29_20140506_135544.jpg	Tue May 06 13:55:51 MESZ 2014
IT_FirstResponder_29_20140506_135625.jpg	Tue May 06 13:56:33 MESZ 2014
IT_FirstResponder_29_20140506_135636.jpg	Tue May 06 13:56:42 MESZ 2014

Realisierung als Applikation

Applikations-Daten:

- Ab Android-Version 3.0.0
  - Deckt circa 80% aller Geräte ab
- Einfach zu lokalisieren
  - Aktuell in Deutsch und Englisch
- Applikations-Größe nur 1,4 MB
  - Schnelles Nachladen auf ein Gerät möglich

Realisierung als Applikation

Getestete Geräte:

- Samsung Nexus S
- Samsung Galaxy S2
- Samsung Galaxy S3
- Motorola Moto G

Gliederung

- Stand der Technik
- Herausforderung
- Aufbau des ISO/IEC 27037:2012
- Realisierung als Applikation
- **Fazit**

Fazit

Probleme gelöst durch:

- Benutzerfreundliche Umsetzung als Applikation
- Unterstützung des IT First Responders durch
  - digitale Dokumentation
  - Nutzen der Kamerafunktion
  - automatisches Erstellen eines Abschlussberichts
- Nur mögliche Schritte bei Bearbeitung der Geräte angezeigt

Vielen Dank für Ihre Aufmerksamkeit!

http://www.it-forensik.fh-aachen.de/projekte/itfirstresponder