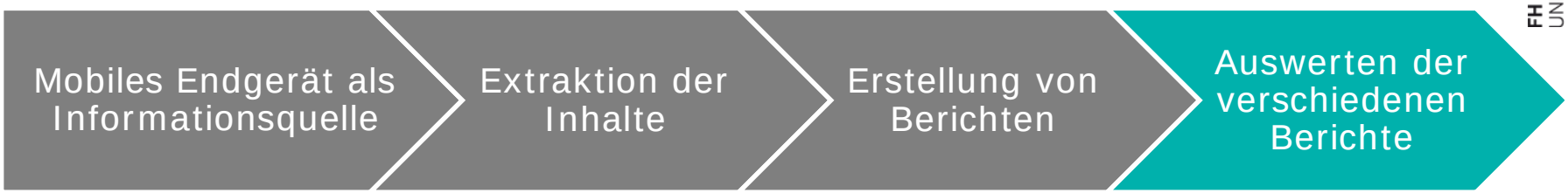
FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Korrelationstool für forensische Berichte (DIRECT)

Martin Pfeiffer
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Problemstellung



- Kontakte, SMS, IM, E-Mail, MMS
- Dateien, Fotos, Videos, Musik
- Positionsdaten
- Backups
- …

- Logisch-, Physikalisch-, Filesystemanalyse
- Verschiedene Tools

- XML
- Schnittstellen zur Extraktions-software

- Zusammenfassen
- Korrelation

Aktuell großer Aufwand durch das Zusammenfassen und die Korrelation.

Aufgabenstellung

- Zusammenfassen von Berichten
  - in gemeinsames Datenformat
  - Duplikate ausblenden
  - für verschiedene Extraktionsarten
  - für Extraktionen von verschieden Zeitpunkten
  - von unterschiedlichen Tools
- Visualisierung
  - Wer kennt wen?
  - Wer hat wie häufig mit wem kommuniziert?
  - Timeline

Grundsätzliche Idee - Import

UFED: Logische, Physikalische, und Filesystemextraktionen

XRY LOGICAL

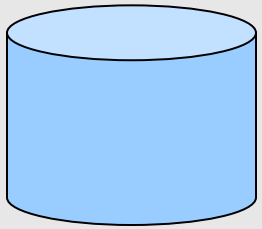
XRY PHYSICAL

Paraben - Device Seizure

Import der Berichte:

- XML
- Plugins

DIRECT



...

X-Ways

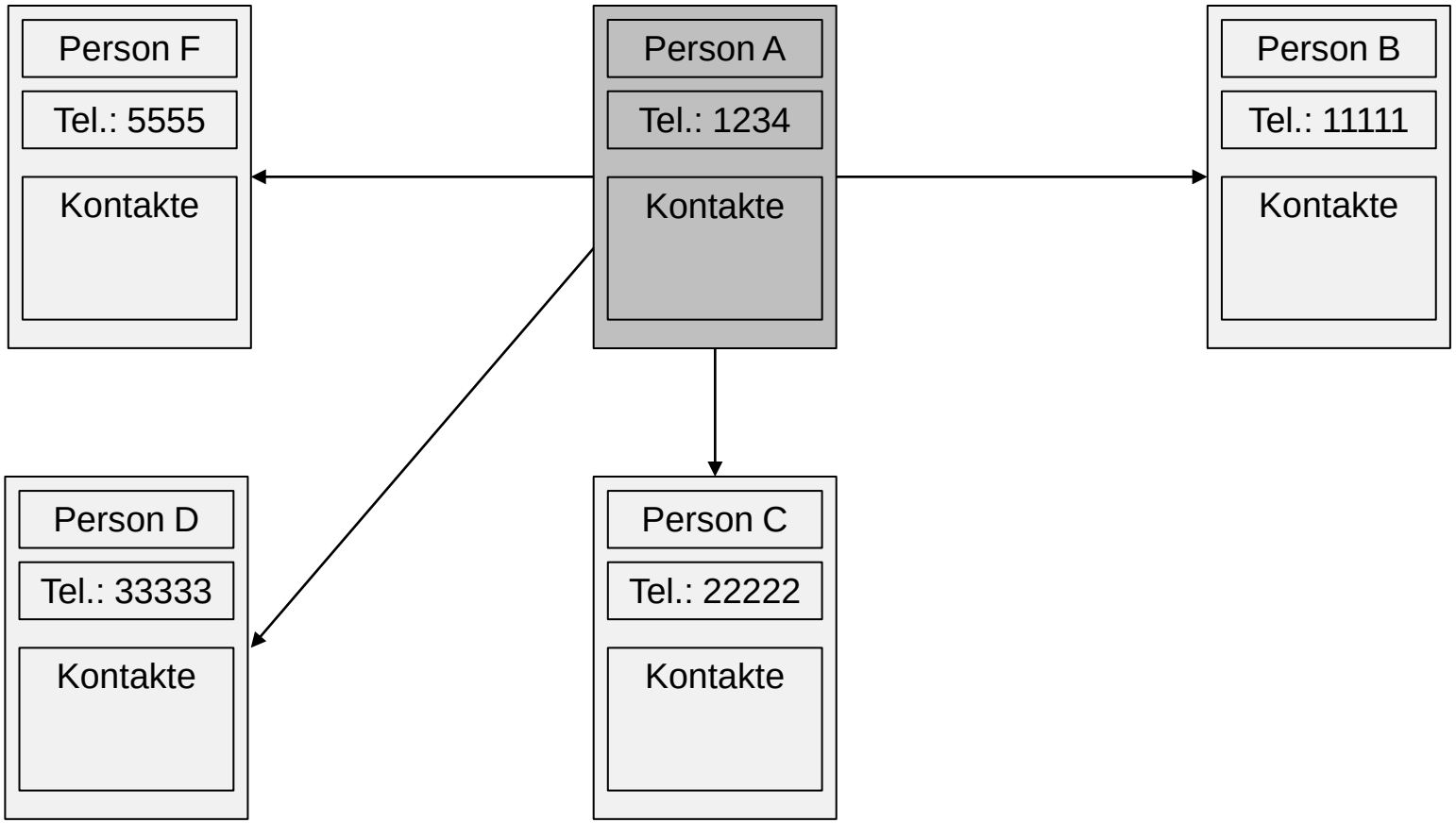
EnCase Guidance Software

DIgital **RE**port **C**orrelation **T**ool

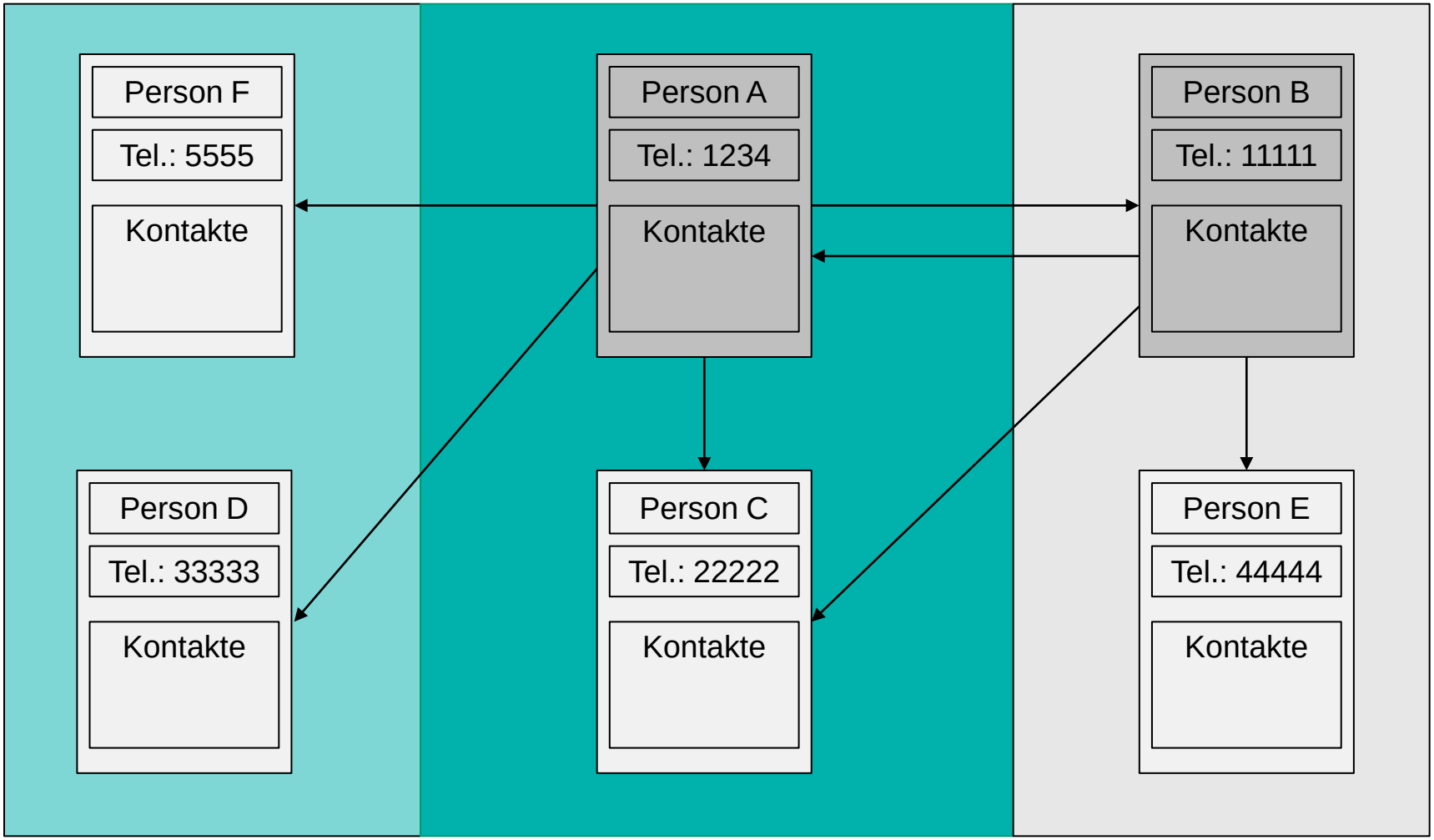
Vorgehen - Verarbeitung

- Merge
  - Fasse mehrere Berichte einer Organisationsgruppe zusammen
  - Organisationsgruppen dabei: Endgerät, Person, Gruppe, Fall
  - Alle Quellen bleiben referenziert
- Filter
  - einfache Filter anwendbar
  - Im Export ersichtlich, dass und worauf gefiltert wurde
- Sortieren

Vorgehen - Verarbeitung



Vorgehen - Verarbeitung



Vorgehen - Export

- XML
  - Im Format wie eingelesen
  - Externe Report Engine
- PDF
  - Dann eigene Reporting Engine
  - Flexibler
- Plugin, um Reporting Engine z.B. von Physical Analyzer 2 zu nutzen

Fortschritt

- Datenbank fertig
- Import von Daten
  - XMLs von Physical Analyzer 2

Projekt-Webseite

- http://www.it-forensik.fh-aachen.de/
  - im Menü „Projekte“

Fragen

Fragen?

Vorschläge & Ergänzungen willkommen!