

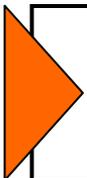
Korrelationstool für forensische Berichte (DIRECT)

Martin Pfeiffer
Lehrgebiet Datennetze





- Kontakte, SMS, IM, E-Mail, MMS
 - Dateien, Fotos, Videos, Musik
 - Positionsdaten
 - Backups
 - ...
- Logisch-, Physikalisch-, Filesystemanalyse
 - Verschiedene Tools
- XML
 - Schnittstellen zur Extraktionssoftware
- Zusammenfassen
 - Korrelation

 Aktuell großer Aufwand durch das Zusammenfassen und die Korrelation.

- Zusammenfassen von Berichten
 - in gemeinsames Datenformat
 - Duplikate ausblenden
 - für verschiedene Extraktionsarten
 - für Extraktionen von verschiedenen Zeitpunkten
 - von unterschiedlichen Tools

- Visualisierung
 - Wer kennt wen?
 - Wer hat wie häufig mit wem kommuniziert?
 - Timeline



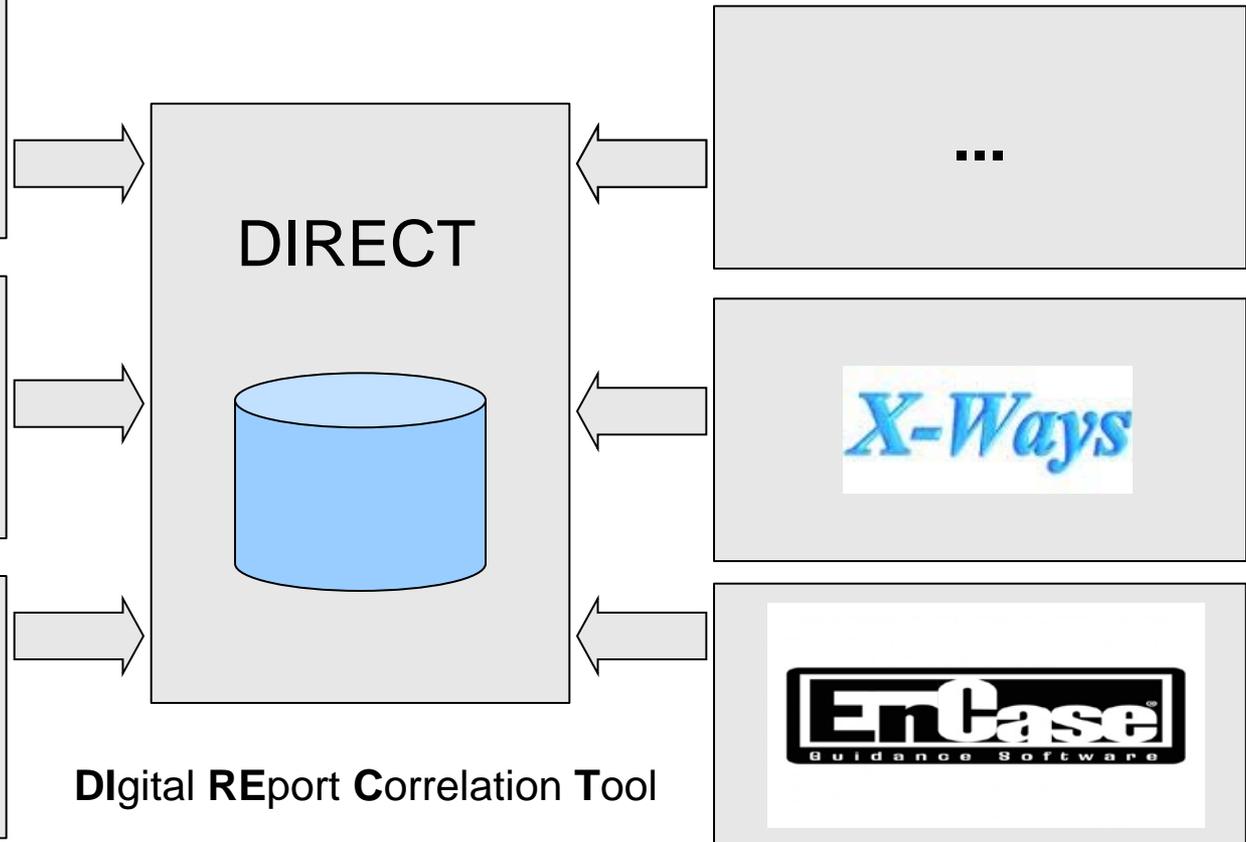
UFED: Logische, Physikalische, und Filesystemextraktionen



Paraben -
Device Seizure

Import der Berichte:

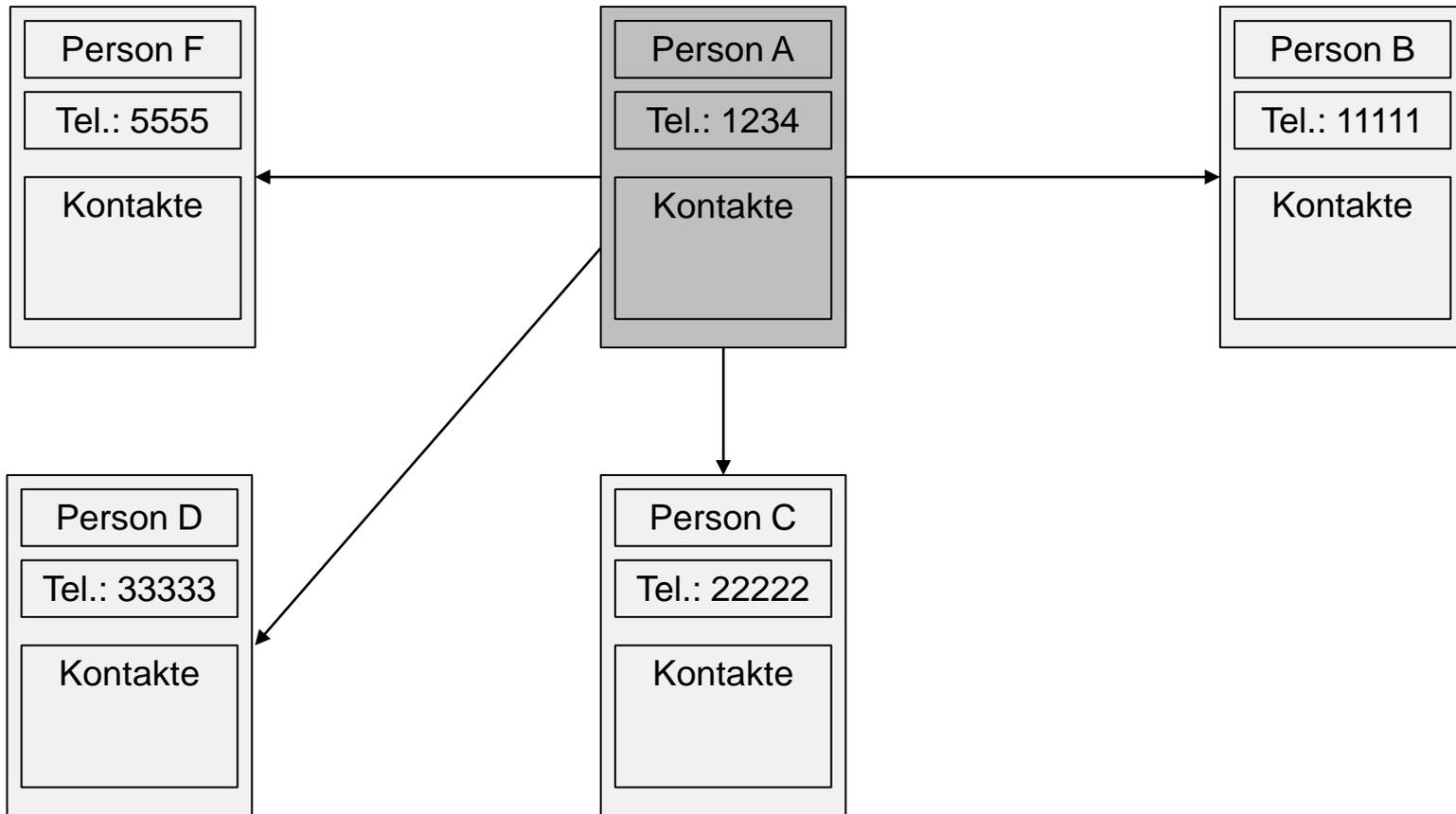
- ▣ XML
- ▣ Plugins

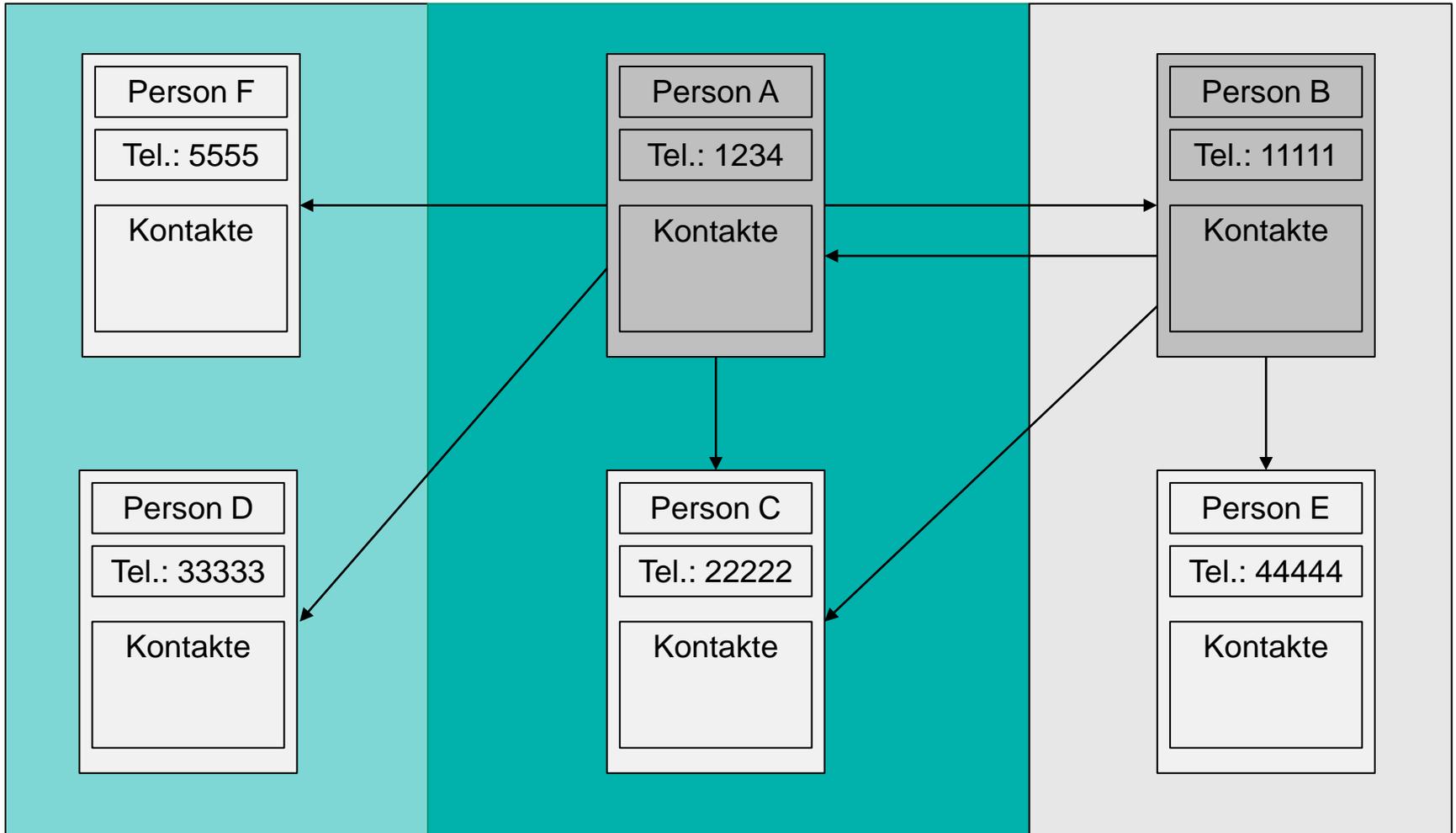


- Merge
 - Fasse mehrere Berichte einer Organisationsgruppe zusammen
 - Organisationsgruppen dabei: Endgerät, Person, Gruppe, Fall
 - Alle Quellen bleiben referenziert

- Filter
 - einfache Filter anwendbar
 - Im Export ersichtlich, dass und worauf gefiltert wurde

- Sortieren





- 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

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

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

The screenshot shows the website interface for IT Forensik FH Aachen. On the left is a navigation menu titled "HAUPTMENÜ" with the following items: Startseite, Veranstaltungen, **Projekte** (highlighted), DIRECT, VOLIX, Archiv, Pressemeldungen, Kontakt, and Impressum. Below the menu is a login section with fields for "Benutzername" and "Passwort". The main content area features a large banner image of a server room with glowing blue lines. Below the banner is a diagram for the "DIRECT" (Digital Report Correlation Tool). The diagram shows a central box labeled "DIRECT" with "Digital Report Correlation Tool" written below it. Four arrows point from this central box to four different devices: a smartphone, a laptop, a desktop monitor, and a tablet. The FH Aachen logo is visible in the bottom left corner of the diagram area.

Digital REport Correlation Tool

Fragen?

Vorschläge & Ergänzungen willkommen!