FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensik großer Datenmengen

FH Aachen, 23. Mai 2018

Christian Schuch, B.Sc. Informatik
Philipp Wiesauer, M.Sc. in Engineering

IT Forensik
FH Aachen

Agenda

- Firmenvorstellung Warth & Klein Grant Thornton
- Vorstellung Philipp Wiesauer
- Grundidee zur Bachelorarbeit
- Einordnung im Forensik- und eDiscovery Prozess
- Theoretische Überlegungen
- Umsetzung
- Das Tool „Private Parts“
- Zusammenfassung

Profil Warth & Klein Grant Thornton

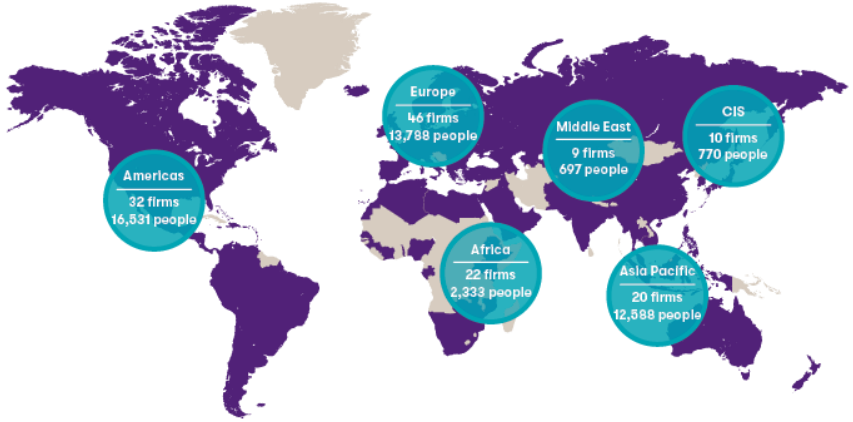
10
Standorte

~ 250
Berufsträger

~100
Partner

~96 mio. EUR
Umsatz in 2016/17

~900
Mitarbeiter



Grant Thornton LLP

Globales Netzwerk das zu den fünf größten Wirtschaftsprüfungsgesellschaften weltweit gehört.

130+
Länder

47.000+
Mitarbeiter

4.8 mrd. US$
Umsatz in 2016

Profil Philipp Wiesauer

Philipp Wiesauer ist im Bereich Governance, Risk & Compliance bei Warth & Klein Grant Thornton in Düsseldorf als Manager tätig

Philipp Wiesauer

ISO/IEC 27001 Lead Auditor

T +49 211 9524 8577
M +49 177 8952473
E philipp.wiesauer@wkgt.com

Ausgewählte Projekte

- Durchführung von IT Sicherheitsprüfungen sowie Penetrations-Tests inklusive Unterstützung bei der Beseitigung etwaiger gefundener Schwachstellen
- Erstellung von IT Sicherheitskonzepten hinsichtlich technischer und organisatorischer Maßnahmen inklusive Industrie 4.0 und IoT Sicherheit
- Durchführung von IT forensischen Sonderuntersuchungen zur Aufklärung von Fällen von Computerkriminalität, Wirtschaftskriminalität und Betriebsspionage in unterschiedlichen Branchen und Größenordnungen
- Durchführung und Leitung von zahlreichen eDiscovery Projekten aller Größenordnungen im Energie-, Finanz- und Automobilsektor
- Durchführung einer Incident Response Untersuchung im Rahmen einer andauernden Cyber-Attacke bei einem Telekommunikationsanbieter

Er verfügt über mehr als zehn Jahre Berufserfahrung als IT Specialist und IT Berater bei führenden IT Beratungs-unternehmen und Wirtschaftsprüfungsgesellschaften.

Beratungsschwerpunkte

Die Tätigkeitsschwerpunkte von Philipp Wiesauer liegen in der Beratung und Durchführung von Projekten in den Bereichen IT Sicherheit, IT Forensik und Incident Response. Zusätzlich berät er Unternehmen bei der Aufklärung von Wirtschaftskriminalität sowie der Aufarbeitung und Vermeidung von IT Sicherheitsvorfällen (Cybercrime).

Ein weiterer Tätigkeitsschwerpunkt von Philipp Wiesauer ist die Beratung von eDiscovery und Litigation Projekten aller Größenordnungen.

Qualifikation

Master of Science in Engineering
ISO/IEC 27001 Lead Auditor
Nuix eDiscovery Certified Specialist

Sprachen

Deutsch
Englisch

Grundidee zur Bachelorarbeit

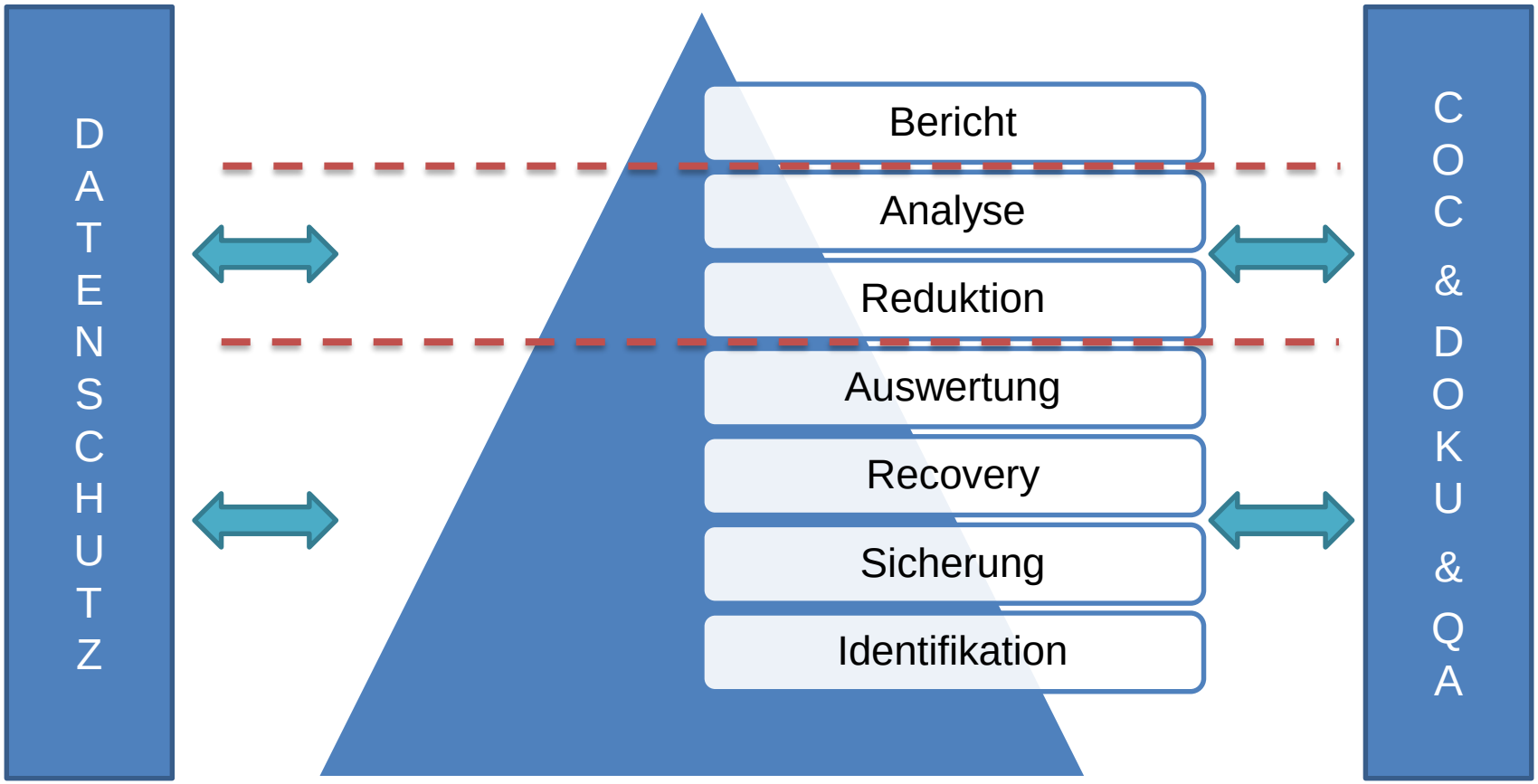
Ausgangssituation und Problemstellung

- Verarbeitung von zunehmend größeren Datenmengen bei Forensik- und eDiscovery-Projekten
- Einhaltung unterschiedlicher und sich ändernder **datenschutzrechtlicher** Anforderungen
- Aktuell halbautomatisierte (Skripte) und individuelle Lösungen im Einsatz

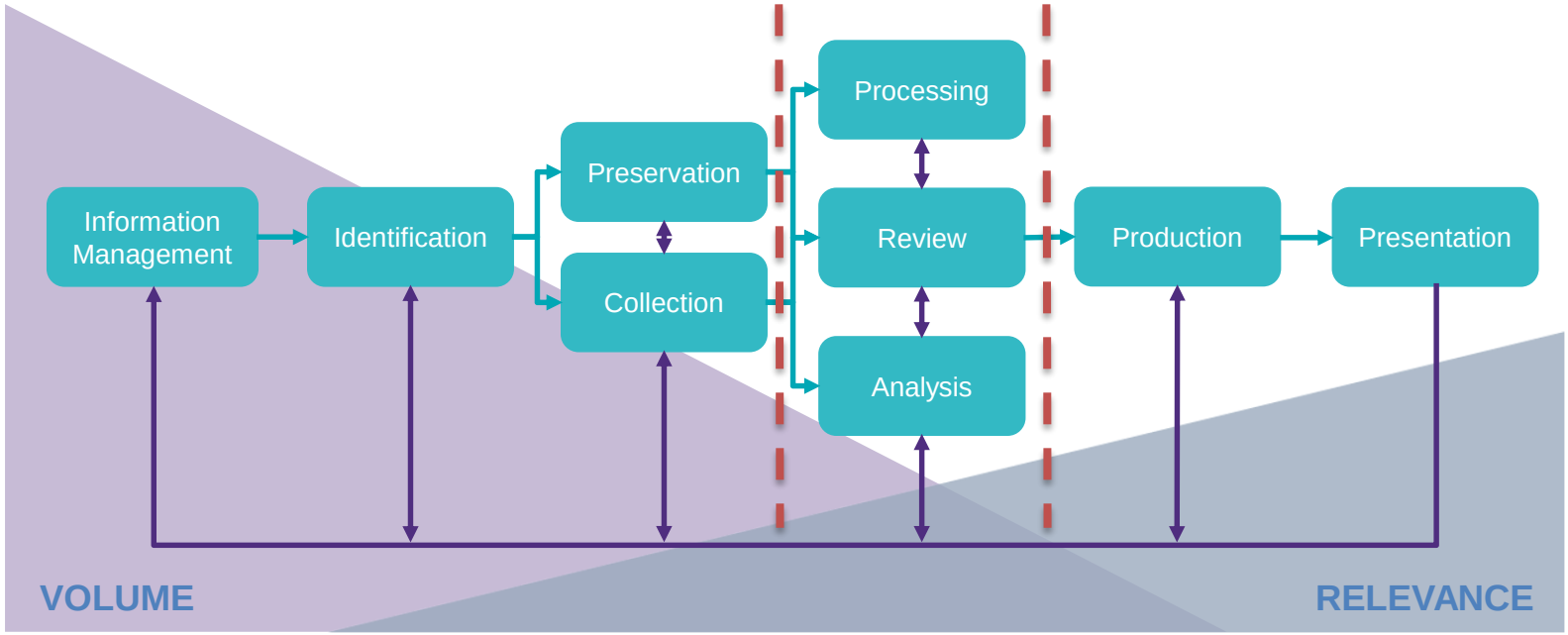
Anforderungen

- Automatisierte Filterung von in Nuix verarbeiteten Beweismitteldaten hinsichtlich **Datenschutz**
- Kompatibel zu IT-Forensik und eDiscovery Prozess von WKGT
- Automatisierte Dokumentation
- Automatisierte Qualitätssicherung

WKGT Forensik Prozess



eDiscovery EDRM Prozess



Quelle: vgl. EDRM.net

Theoretische Überlegungen

Ansatz:

- Filterung durch Suche von qualifizierenden Begriffen in der Menge der Beschreibungen aller Beweismittel oder bestimmter Teilmenge als Definitionsmenge (Item-Set)

- Einordnung in drei Ergebnismengen:

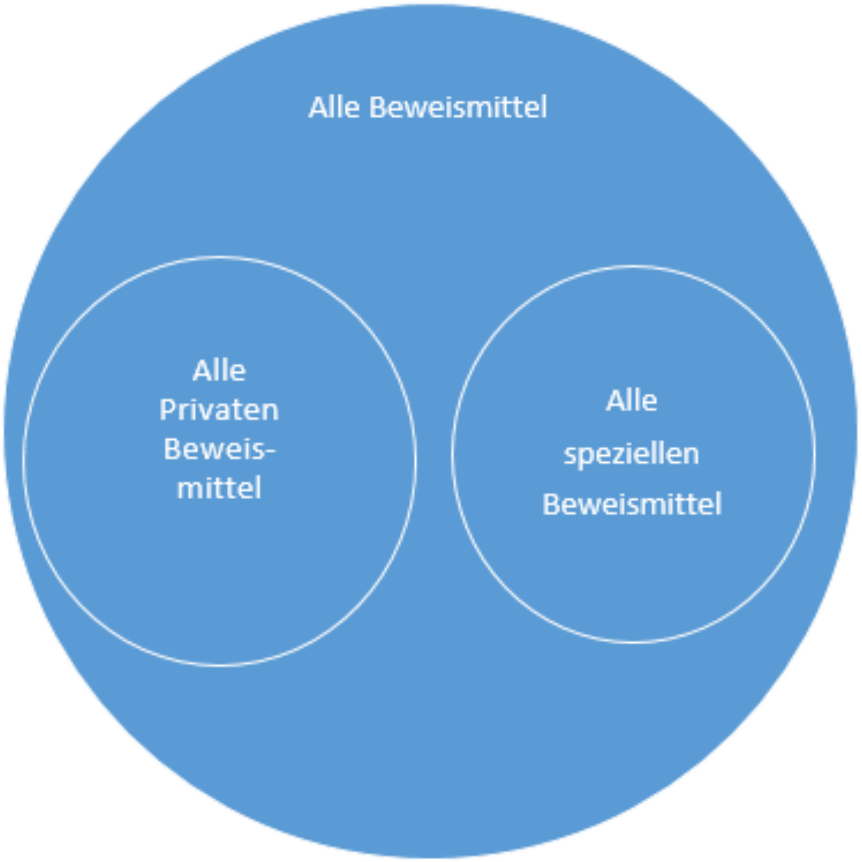
  – Vermutlich private Beweismittel
  – Beweismittel, die spezielle Kriterien erfüllen
  – manuell in der Analyse zu untersuchende Beweismittel

Theoretische Überlegungen

Beweismittelbeschreibungen zum Beispiel:
→ Metadaten
→ Textdaten
→ Custodians (Besitzer, Absender, Empfänger etc)

Analoges Verfahren bei den speziellen Kriterien (die zum Beipiel IP Adressen, oder eine Gruppe von Custodians sein könnten)

Theoretische Überlegungen



Die Restmenge beinhaltet die manuell zu untersuchenden Beweismittel

Umsetzung

- NUIX als IT-Forensik-Workstation
- GUI als Intranetseite
- Python als Programmiersprache
- Python für das Scripting von NUIX
- Django als Webframework

Umsetzung

Warum NUIX:

- Marktführer IT-forensik-Workstations
- Externer Vollzugriff auf nahezu alle Features durch Skripting schon in der Grundversion
- KI-basierte, sehr schnelle und variable Suche mit der Möglichkeit des Einsatzes von Fuzzy-Logic
- Vielfältige Möglichkeiten der Strukturierung der Daten
- Viele weitere Features, siehe www.nuix.com

Umsetzung

Vorteile Python:

- Glue-Language (leichte Verbindung zwischen mehreren Sprachen innerhalb desselben Projektes)
- Hochflexibel: Viele optionale Bibliotheken & Frameworks
- Einfache Lesbarkeit und klare Struktur, leichte Wartung/Anpassung
- Eine der drei mitgelieferten Skriptsprachen in NUIX, API für alle Zugriffe in NUIX in Standardausführung

Vorteile Django Framework:

- GUI als Webseite realisierbar (HTML/CSS/Template Language)
- Logikprogrammierung in Python →Hauptprogrammiersprache für ganzes Projekt
- Native API für DB-Zugriff auf z.B. SQLite
- Nachvollziehbare Projektstruktur

Das Tool

Suchbegriffe gespeichert (in SQLite-Datenbank):

Tabelle mit Begriffen, die private Items definieren (Metadaten, Textdaten, Custodians etc)

Tabelle mit Begriffen, die spezielle Items definieren

Attribute der Begriffe in der Datenbank:

Begriff, Suffix oder Präfix, Suchbereiche: alle Items, Emailanhänge, lose Dateien, irreguläre Items, Emailabsender, Metadaten

Sucheinstellungen (in Dateien):

Inklusions- Strategie, Deduplizierungsmethode, History in NUIX anlegen ?

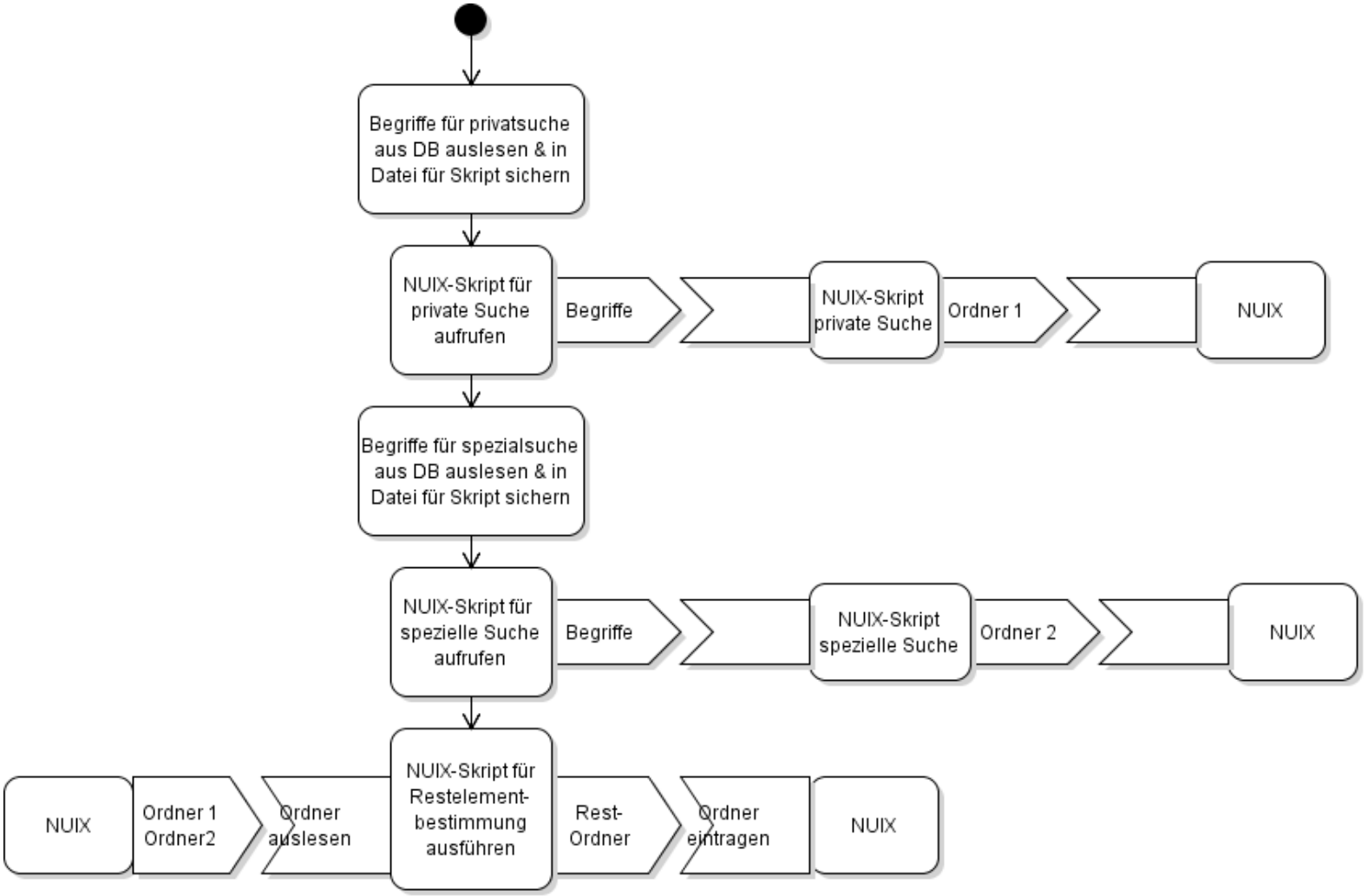
Das Tool

Django Framework:

- GUI als Webseite (HTML/CSS/Template Language)
- Logikprogrammierung in Python
- API aus Python heraus für DB-Zugriff auf SQLite - Datenbank
- Python-Code
  - → Inhalte des Datenmodells an Template übergeben
  - → Berechnungen durchführen
  - → Datenmodell, Webseitenstruktur & Files verwalten
  - → Aufruf NUIX-Skripte
- HTML-Templates
  - → Gestaltung der Webseiten, Darstellung der Modellinhalte
- → Aufruf der Logiken in Python-Code über Template-Language
- → Navigation durch Webseitenstruktur durch Links

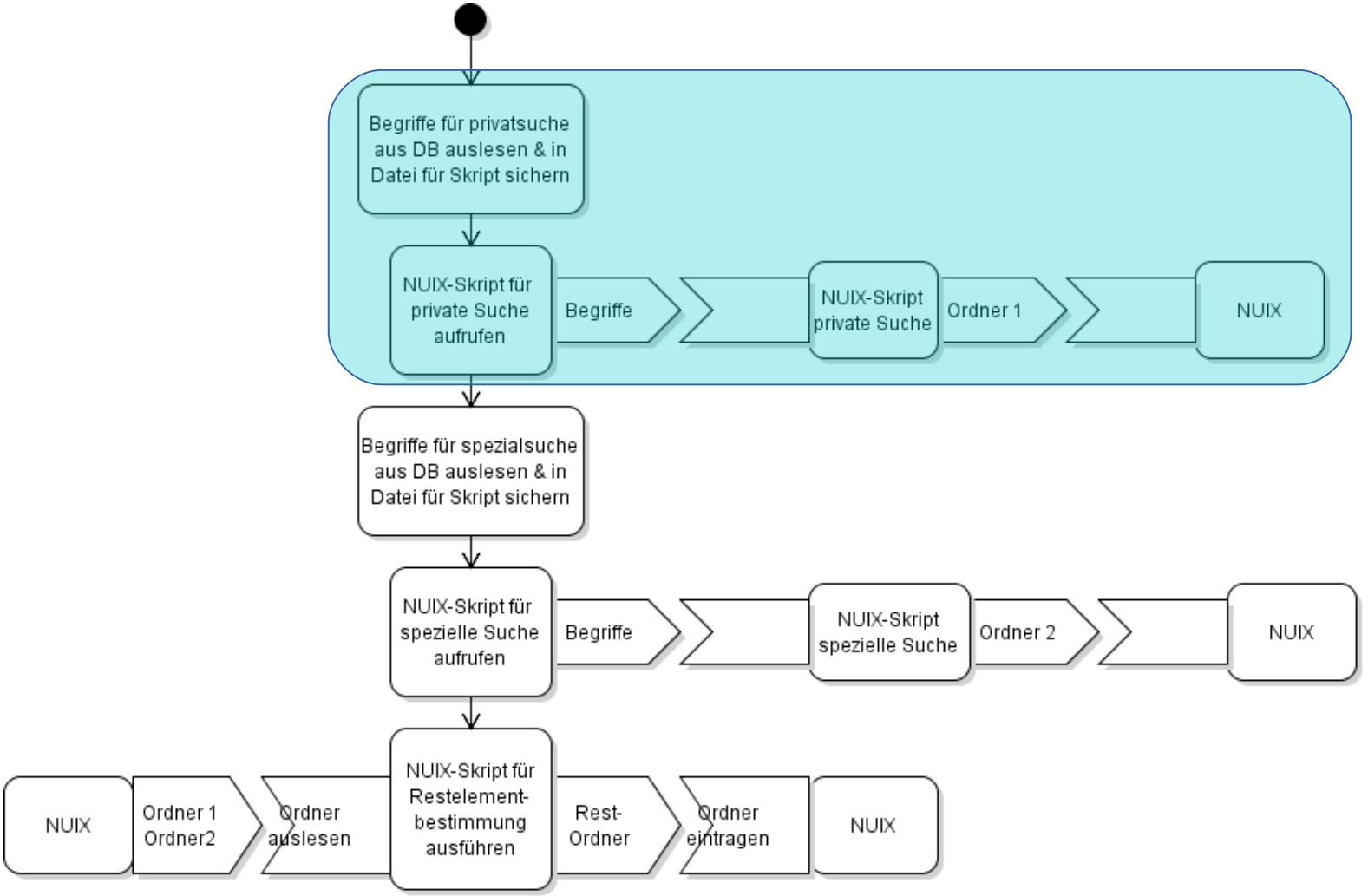
Das Tool

Algorithmus:



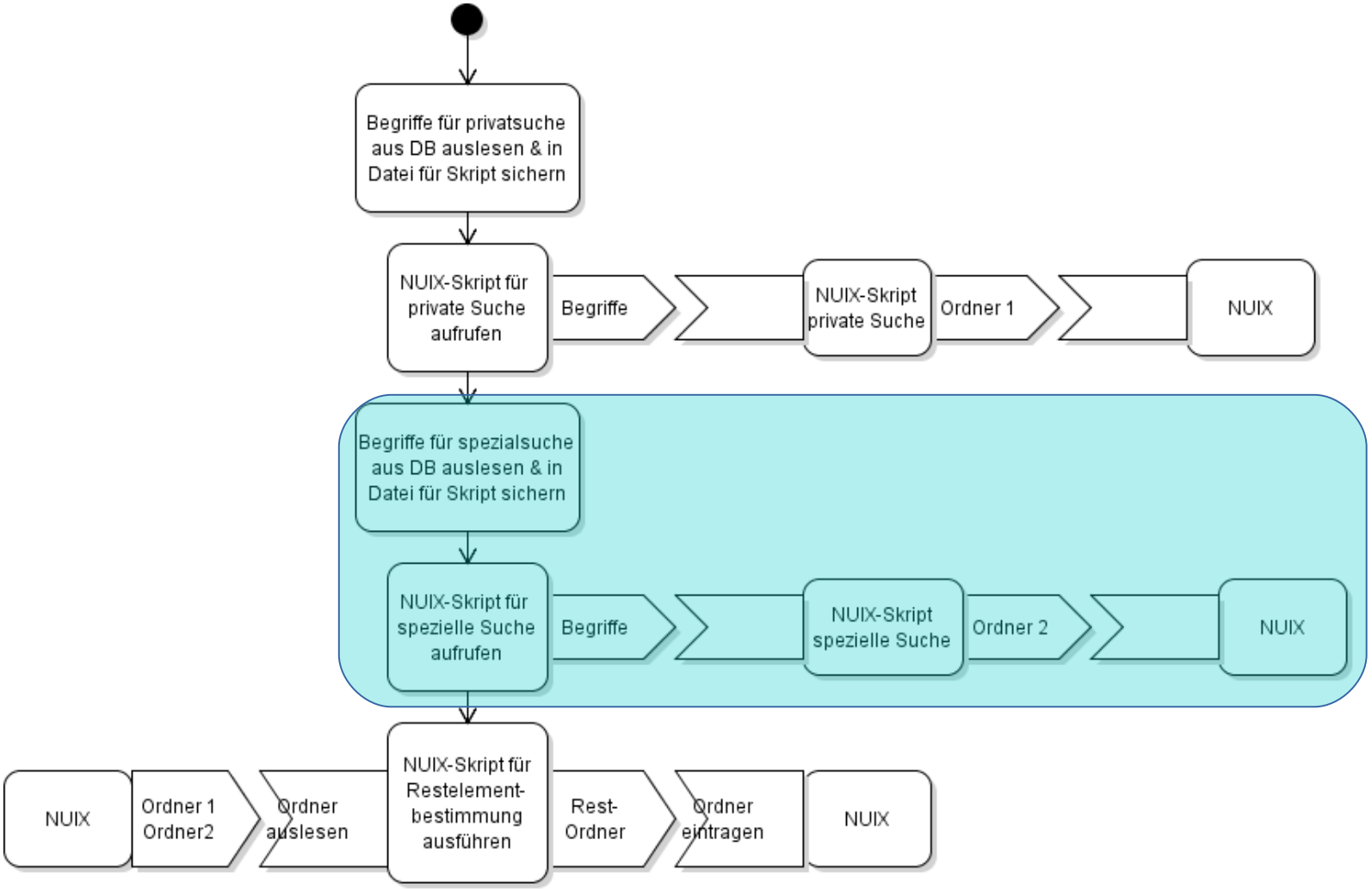
Das Tool

Private Items:



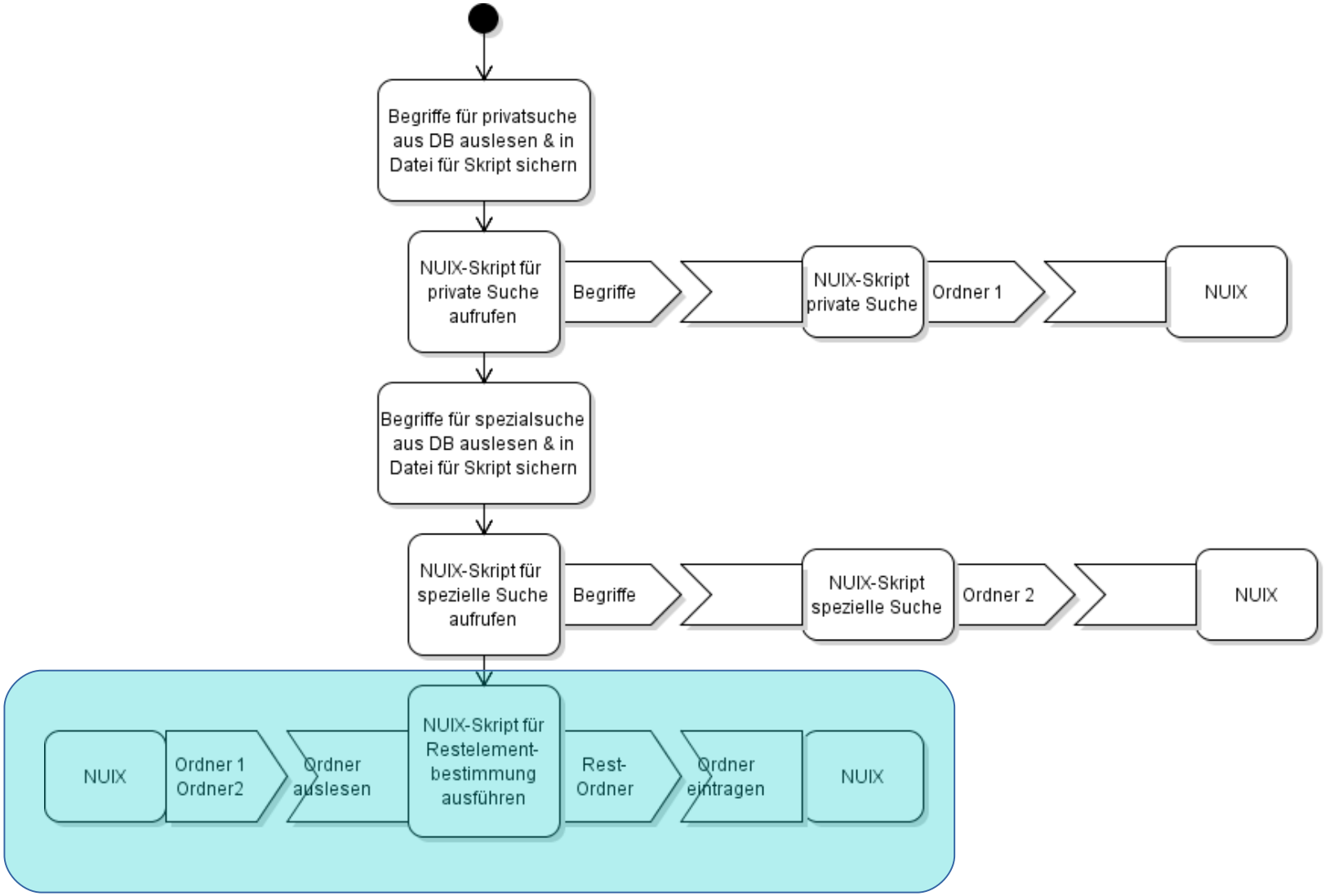
Das Tool

Spezielle Items:



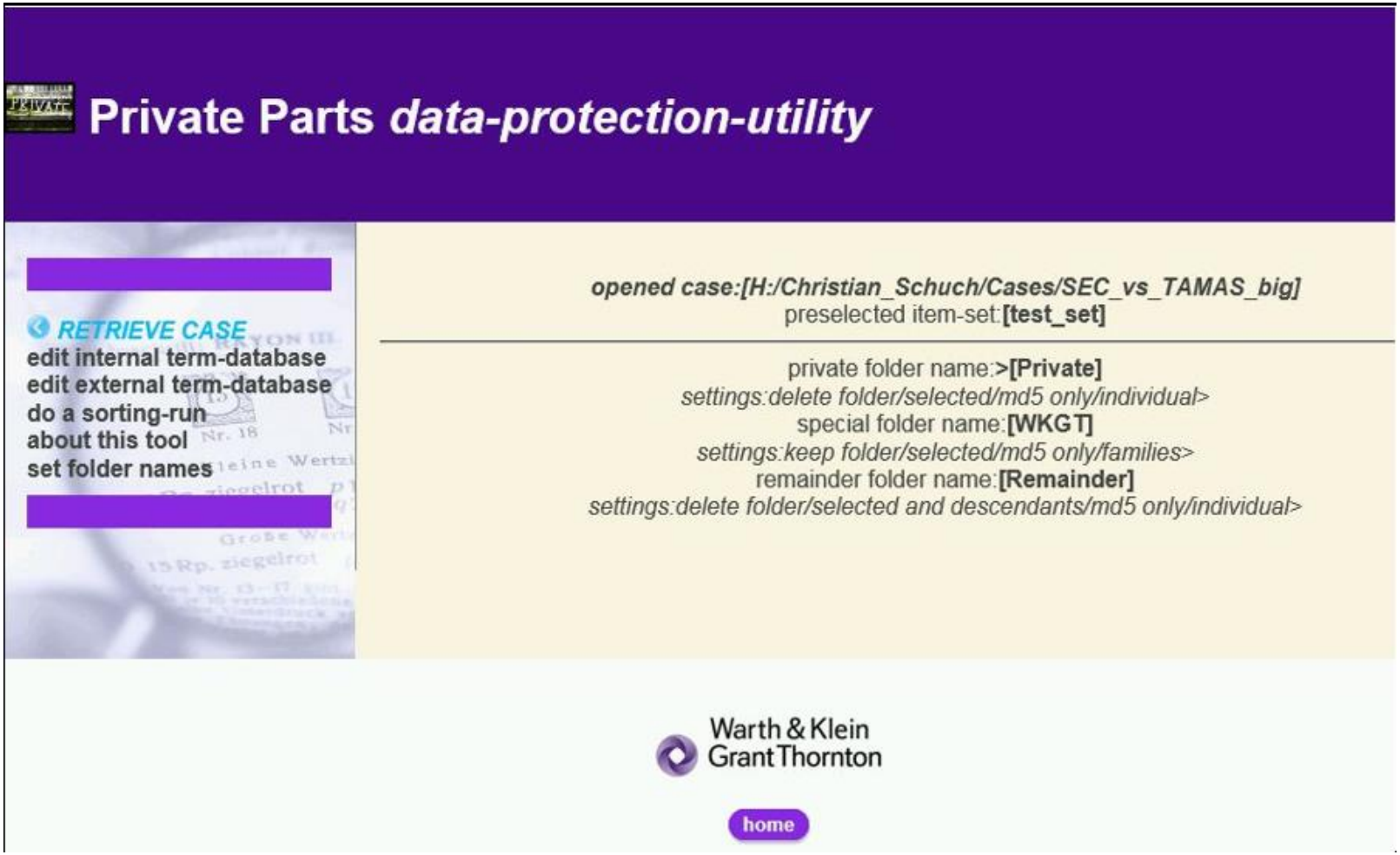
Das Tool

Ermittlung des Manuell zu untersuchenden Restes:



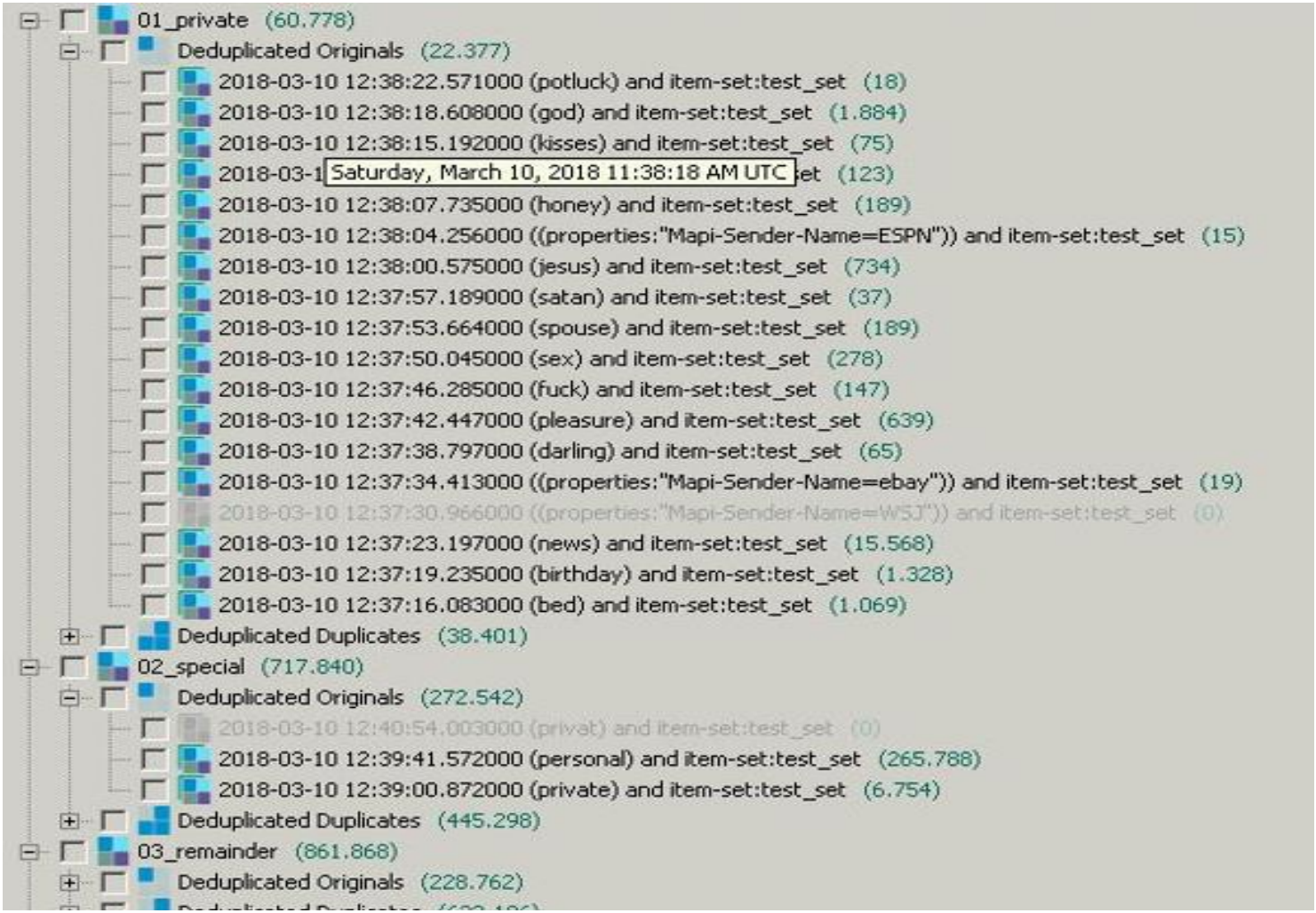
Das Tool

Die GUI / Weboberfläche:



Das Tool

Erzeugte Struktur im NUIX-Case:



Das Tool

Erzeugter Eintrag in History:

```
------------------------------------------------------------
internal search:2018-03-10 12:37:10.421000

delete folder:True
inclusion strategy:SELECTED_ITEMS
deduplication method:md5
deduplicate by:INDIVIDUAL

command:(bed) and item-set:test_set hits:2537
command:(birthday) and item-set:test_set hits:3759
command:(news) and item-set:test_set hits:42888
command:((properties:"Mapi-Sender-Name=WSJ")) and item-set:test_set hits:7
command:((properties:"Mapi-Sender-Name=iTunes") (properties:amazon)) and item-set:test_set hits:0
command:((properties:"Mapi-Sender-Name=ebay")) and item-set:test_set hits:34
command:(darling) and item-set:test_set hits:351
command:(pleasure) and item-set:test_set hits:2128
command:(fuck) and item-set:test_set hits:414
command:(sex) and item-set:test_set hits:1157
command:((properties:"Mapi-Sender-Name=facebook")) and item-set:test_set hits:0
command:(spouse) and item-set:test_set hits:675
command:((properties:"Mapi-Sender-Name=iTunes")) and item-set:test_set hits:0
command:(satan) and item-set:test_set hits:114
command:(jesus) and item-set:test_set hits:2212
command:((properties:"Mapi-Sender-Name=ESPN")) and item-set:test_set hits:20
command:(honey) and item-set:test_set hits:784
command:(kicks) and item-set:test_set hits:447
command:(kisses) and item-set:test_set hits:214
command:(god) and item-set:test_set hits:7276
command:(potluck) and item-set:test_set hits:40
****************************************
special search:2018-03-10 12:38:32.324000

delete folder:True
inclusion strategy:TOP-LEVEL_ITEMS
deduplication method:md5
deduplicate by:FAMILY

command:(private) and item-set:test_set hits:15609
command:(personal) and item-set:test_set hits:717840
command:(persönlich) and item-set:test_set hits:0
command:(persoenlich) and item-set:test_set hits:0
command:(privat) and item-set:test_set hits:32
****************************************
remainder search:2018-03-10 12:41:04.911000

delete folder:True
inclusion strategy:SELECTED_ITEMS
deduplication method:md5
deduplicate by:INDIVIDUAL

remainder:(item-set:test_set) and (not item-set:01_private) and (not item-set:02_special) hits:293411
Process finished at:2018-03-10 12:41:15.472000
------------------------------------------------------------
```

Zusammenfassung

- Filterung zwischen zulässigen/unzulässigen Beweismitteln oft umständlich → Entwicklung Methode/Tool zur Automatisierung
- NUIX bietet schnelle, variable & Effektive Suche
- Nutzung NUIX-Engine über Python-API → Python/Django
- Komfortable Nutzung durch GUI / Webseite
- Effektive Sortierung
- Anpassbarkeit
- Automatisierte Dokumentation

Vielen Dank für Ihre Aufmerksamkeit !