

3. Forensic Technology

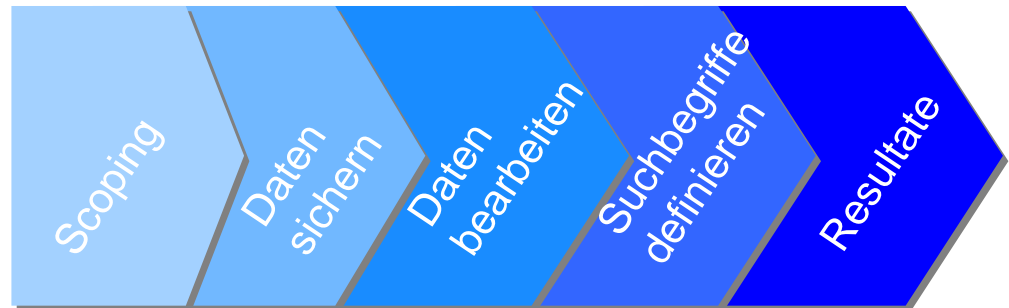
Sicherung elektronischer Daten - Übersicht

Beschreibung

- Datenbestände, Abteilungen, Personen lokalisieren und identifizieren
- Sicherung elektronischer Daten (Laptops, Handhelds, E-Mails, Server etc.)
- Gelöschte und versteckte Dateien wiederherstellen
- Daten klassifizieren und vereinheitlichen
- Daten nach gemeinsam definierten Suchbegriffen filtern
- Ergebnisse werden in gewünschtem Format bereitgestellt


Vorteile

- Einheitliche Methodologie
- Breites Spektrum an IT Mitteln für die Sicherung verschiedenster Geräte
- Aktuellste Software, welche langwieriges manuelles Bearbeiten umgeht



3. Forensic Technology

Das „Natürlich Werden“ von Dokumenten

Epoche	vorhandene Datenträger	Medium für die Review	Mass
Papier (linear) <i>Bis - 1990</i>			Schachteln ? Seiten/Stunde
E - Papier (linear) <i>1990 - 2000</i>			Lineare Review 30 Dokumente/Std
Concept/ Analytics <i>2000 -</i>			200+ Entscheidungen/Std

3. Forensic Technology

Ein Meer von Daten

- Papier (Berichte, Broschüren, Dokumente jeder Art)
- E-Mail (persönliche Internet-Mails wie yahoo, g-mail)
- Festplatten (Laptop, Desktop)
- Mailserver (Mail, Public Folders)
- Applikationen und Datenbanken
- Instant messages (SMS, MMS)
- Word, Excel, etc.
- Server (Abteilungs-, Gruppen-, Public-Folders)
- Clouds
- Web pages / blogs
- Netzwerke wie Facebook, XING, LinkedIn
- PDAs, Blackberry, DVD, externe Festplatten, USB-Sticks, Telefone
- Fax, Faxserver
- Backup Medien
- Voice mail
- Microfiche und -film
- Fernsehaufzeichnungen
- Radiosendungen



3. Forensic Technology

Stolpersteine und wichtige Aspekte



3. Forensic Technology

Stolpersteine und wichtige Aspekte

Sprachen



- „andere“ Schriftarten (Kyrillisch, Asiatisch, Arabisch)

Daten-
Format



- Lesbarmachen von Backup-Tapes
- Kompatibilität
- Verschlüsselung

Gesetze



- Datenschutz
- Schweizerisches Strafgesetzbuch Art. 271

Datum



- Unterschiedliche Schreibweisen für Datum

Menge



- Das Rechenzentrum auf dem Pult

3. Forensic Technology

Von der Front 1

Flaschenhalse

- Aussagen:
 - Aufbewahrungsrichtlinien bestehen
 - Ca. 300 Backup Tapes sind vorhanden
- Tatsache
 - 6000 Backups im Archiv (...von der 5 ¼ Zoll Diskette bis zu den modernsten Medien)

Flaschenhalse

- IT 3 Jahre vor der Untersuchung an Outsourcer übergeben
 - Eigenes Produktivsystem in Testumgebung bei Outsourcer migriert
 - Testumgebung in Produktivsystem migriert
- Im Rahmen der Abgrenzung der zu sichernden Daten für die Untersuchung stellt sich heraus, dass die Testumgebung beim Outsourcer nicht gelöscht wurde
- Nicht gelöschte Daten:
 - Ca. 20 Terrabytes
 - Zur Zeit der Untersuchung bedeutet dies den Aufbau eines mittelgrossen Rechenzentrums.....

3. Forensic Technology

Von der Front 2

Flaschenhalse

- Durchführung Hausdurchsuchung simultan an sieben Standorten - Forensic Technology Equipment sowie Forensic Technology Spezialisten entsprechend zahlreich (Zweierteams vor Ort, begleitet durch Polizei)
- Elektronische Datenbestände verschiedenster Arten gesucht und identifiziert (Standalone PC, Fileserver, Faxserver, Mailserver, USB-Stick, Fotokamera-Chip, Laptop, CDs, Disketten, Bänder)
- Imaging (Sicherung vor Ort) und Sicherstellung von Geräten (über 130 PCs, Server, und verschiedenste Datenträger...)
- Start um 07.00 Uhr, Ende 23.00 Uhr

5. Fragen

