



Datenverarbeitungsgruppe

- Servicedienststelle
- in Niedersachsen pro Polizeiinspektion bzw. Zentraler Kriminalinspektion eine DVG
- **Ausnahme:** Polizeidirektion Hannover
- Zentraler Kriminaldienst, Kriminalfachinspektion 5

Aufgaben der Datenverarbeitungsgruppe

- Untersuchung/ Sicherung von Datenträgern, Handys,...
- Unterstützung bei Durchsuchungen, Datenkonvertierungen
- Amtshilfe BKA, LKA, StA...
- Sachverständiger Zeuge vor Gericht



Standardisierte Arbeitsweise

(am Beispiel der PD Hannover)

→ vorher

- Sicherstellung eines PC durch die Fachdienststelle
- Untersuchungsantrag / Informationsbeschaffung

Untersuchungshandlung

- Forensische Fertigung eines Image (Spiegelung)
→ Schreibschutzblocker
- Image in Untersuchungsprogramm einlesen
→ pers. Favorit / Workflow
- anschl. Untersuchung nur im Image

Vorbereitung des Image

- Grundstein für anschl. Untersuchung
→ Wurzel eines Baumes
- Je breiter die Basis desto sicherer der Stand



Dateiüberblick erweitern

- gelöschte Dateien wieder herstellen
- Finden/ Überprüfen von Dateien (Signaturen)
- Archive/ Datenbanken/ Dokumente entpacken
- Hautfarbenanteile errechnen (in Bilddateien)
- Hash-Werte errechnen



Dateisignatur

- legt intern den Typ einer Datei fest
- Hilfe bei Verschleierungstaktik
- Instrument zur Suche in Bereichen ohne Struktur

Hash-Wert

- digitaler Fingerabdruck
- archivierbar in Datenbanken/ Abgleich möglich

Dateiüberblick ist angereichert

- Konzentrierung auf mögl. strafrechtlich relevante Dateien (Videos/ Bilder)
- Stamm eines Baumes
- Kernstück weiterer Untersuchungen



Vorläufige Überprüfung

- Abgleich mit PERKEO Hash Datenbank
- Feststellung von strafbaren Inhalten
- Unterdrücken der bekannten Bilder vor der Sichtung



Sichtung von Bild- und Videodateien

Es werden **alle** Bild- und Videodateien gesichtet denn hinter jeder kinderpornografischen Bild- und Videodatei steht ein realer Missbrauch eines Kindes!

Dateiüberblick reduzieren

- Filtern der Dateien (Video, Bild, E-Mail,...)
- Immer noch mehrere hunderttausend Dateien
- irrelevante/ bekannte Dateien unterdrücken
- Duplikate unterdrücken
- Ordnen der Dateien (nach Pfad, Größe, Hautfarbenanteil,...)



Zeitansatz

Abhängig von:

- gespeicherten Inhalten
- Struktur und Ordnung der Daten
- Speicherort (Backup, Schattenkopie,...)
- Größe/ Beschaffenheit der Datei (z.B. Video)

Workflow

- Hardware
 - Monitorgröße
 - Rechenleistung,...
 - Datenträgergeschwindigkeit
- Software
 - Unterstützung von Tastaturabkürzungen
 - spezielle Filtertechniken,...



Sichtung ist abgeschlossen

- Verbindungen zu unterdrückten Duplikaten herstellen
- Zuordnung der relevanten Dateien in filterbare Berichtsstrukturen



Analyse der Speicherpfade

- Verbindungen der relevanten Dateien zu diversen Anwendungen: Tauschbörsen, Messenger Dienste, ...
- Äste des Baumes



Beispiele aus der Praxis

Zielrichtung bei der Analyse der Beziehungen der jeweiligen Programme mit den inkriminierten Daten ist nicht nur die Strafverschärfung (Verbreiten von Kinderpornografie), sondern auch die Feststellung weiterer Täter!

Fall 1:

ICQ Untersuchung mit mehreren Folgeverfahren

Fall 2:

Feststellung eines Trojaners und die folgenden Ermittlungsansätze



Ich hoffe nun weitere Fragen im offenen Dialog beantworten und gewünschte Themengebiete vertiefen zu können.

Vielen Dank für Ihre Aufmerksamkeit!