1 Klassische Forensik

Autor: Julian Kotzur - Das ist eine sehr sehr grobe Zusammenfassung. Ich habe einen Bericht geschrieben und wollte hier nur kurz die mMn. wichtigsten Begriffe zusammentragen. Es sind somit sehr viele Lücken (ggf. auch Fehler) enthalten!

1.1 Forensische Wissenschaft

Klassische vs. digitale Forensik

- **Klassische Forensik**: Physische Spuren
- **Digitale Forensik**: Digitale Spuren

Wichtige Grundbegriffe

- **Kriminalistik**: „Lehre von der Bekämpfung der Kriminalität durch die Strafverfolgungsorgane in der Lebenswirklichkeit“, d.h. Straften mit technischen und organisatorischen Maßnahmen aufklären
- **Forensische Wissenschaften**: Synonym für Kriminalistik
- **Kriminologie**: „Lehre von den Ursachen und den Erscheinungsformen der Kriminalität“, d.h. sozialwissenschaftliche und psychologische Analyse von Kriminalität

Gebiete der Kriminalistik

- **Verbrechenstechnik**: Phänomenologie kriminellen Verhaltens
- **Kriminaltechnik**: Erbringung von Sachbeweisen
- **Kriminaltaktik**: Anwendung kriminaltechnischer Methoden in einem größeren Zusammenhang
- **Organisation** (der Verbrechensbekämpfung)

Bezug zum Rechtssystem

- Forensische Wissenschaft abstrahiert rechtliche Fragen zu wissenschaftlichen

1.2 Spuren und ihre Entstehung

Wichtige Begriffe

- **Spur**: „materielle Veränderungen der Umwelt, die im Zusammenhang mit der Begehung einer Straftat entstanden sind“, d.h. hinterlassene Zeichen am Tatort
- **Beweismittel**: Dienen vor Gericht als Argumentationsgrundlage. Spuren sind ein Beispiel
- **Austauschprinzip**: Jeder und alles am Tatort nimmt etwas mit und lässt etwas zurück

Bemerkung 1.1.

- Die Spuren werden von Ermittlern am Tatort ermittelt und sichergestellt und zur Analyse an ein Labor weitergeleitet

Klassifikation von Spuren

- **Nach Straftat**
- **Nach chemischer/biologischer Zusammensetzung**
- **Nach Zusammenhang zur Straftat**: Unterscheidung zw. echten und falschen (gefälschten) Spuren
- **Nach Flüchtigkeit**: Transiente Spuren existieren nur temporär (z.b. Temperaturen, Gerüche). Meist nur schriftliches Festhalten möglich
- **Nach Wahrnehmbarkeit**: Auch winzige Spuren (z.b. Haare für DNA-Analysen) sind wichtig

Spuren ohne Austausch von Materie

- **Austausch von Mustern**: Allein die Veränderung von Materie durch Interaktion von Objekten kann eine Spur liefern
- Beispiel: Pistolenlauf verformt das Projektiel. Damit kann man beide einander zuordnen

Fazit

Sowohl Physischer Austausch als auch Musteraustausch kann zu Spuren führen. In beiden

Fällen entsteht ein Austausch von Informationen. Somit gibt es in der echten Welt kein perfektes Verbrechen, bestenfalls gut verborgene Spuren.

1.3 Rekonstruktion des Tatverlaufs

Wichtige Begriffe

- **Rekonstruktion**: Ereignisse in einen räumlich/zeitlichen Zusammenhang bringen
- **Ereignisse**: Festgestellter Kontakt von Objekten auf Basis einer Spur. Entsteht durch Assoziation
- **Assoziation**: Vorgang der Feststellung eines Kontaktes zwischen zwei Objekten. Herleitung und Begründung sind essentiell
- **Quantifizierung**: Wahrscheinlichkeitsanalyse für Assoziationen (nicht immer notwendig)

Vorgehen bei Assoziation

1. Spur erkennen und von anderen abgrenzen
2. Spur **Identifizieren** und Tauglichkeit als Beweismittel feststellen (Was liegt vor?)
3. **Klassifizierung** der Spur (Zu welcher Klasse von Gegenständen gehört das Objekt?)
4. **Individualisierung** der Spur (Spezifizierende Analyse)

Bemerkung 1.2.

- Es kann Klassifizierung ohne Individualisierung ausreichen (z.b. Besitz illegaler Objekten)
- Individualisierung ist nötig, wenn man einen Zusammenhang bei vorliegenden Objekten finden muss (z.b. zu welcher Pistole gehört eine Kugel)

Beispiel 1.3. (Assoziation bei Schusswechsel)

- Spur am Tatort: metallisches Objekt
- Identifizierung: Kugel einer Schusswaffe
- Klassifikation: Kugel hat Kaliber X
- Individualisierung: Beobachtung der Kratzspuren

2 Digitale Spuren

Spuren

- **Wo fallen digitale Spuren an**: Caches, Logs, History, Zeitstempel, etc.
- **Digitale Spuren**: Basieren auf Daten, die in Computersystemen gespeichert oder übertragen wurden
- **Spurenbeschreibung**: Spurenmetadaten
- **Spurenträger**: z.b. Festplatte
- **Spureninformation**: Die Informationen die aus der Interpretation einer Spur entstehen
- **Aufbau**: CSI: Claim (Metadaten), Support (Materie, auch Authentizität), Information (Interpretation der Daten, auch Integrität)
- **Klassifikation**: Entstehungsort (z.b. Rechner, lokales Netz), Flüchtigkeit (z.b. RAM vs. HDD), Semanti (Primär, Sekundärdaten, Logdaten), Vermeidbarkeit (vermeidbare (Logs) vs. unvermeidbare Spuren (gewisse Metadaten))

3 Dokumentation und Vorgehensmodelle

3.1 Forensische Dokumentation

Definition 3.1 (Aufgabentrennung)

- **Polizeiliche Ermittlungsperson**: Treibt Ermittlungsverfahren voran, bildet und prüft Hypothesen
- **Ersteinschreiter, Spurensicherung, Kriminaltechnik**: Sichert Spuren und leitet diese ans Labor weiter
- **Forensische Wissenschaftler, Sachverständiger**: Untersucht die weitergeleiteten Spuren
- Viele weitere mögliche Akteure

Definition 3.2 (Überdeckte Wissensbereiche)

- Kommunikation zwischen Ermittlern und Wissenschaftlern ist wichtig
- Wissenschaftler braucht Verständnis für das Untersuchungsziel (Welche Frage soll beantwortet werden, welcher Kontext liegt vor)
- Ermittler braucht Verständnis für Spurenart, ihre Auffindewahrscheinlichkeit und Aussagekraft (Können die gefundenen Spuren die Fragen beantworten)

Welche Spuren/Ergebnisse sind relevant?

- Frage nach den „richtigen“ Untersuchungsergebnissen
- **Schlechtes Beispiel**: Prüfen sie X nach Strafbarkeit Y! Problem ist zum einen das Finden der richtigen Auslegung des Gesetzes. Zum anderen kann durch die Frage leicht ein Rechtsurteil die antwort sein, was ein Befangenheitsgrund sein kann
- **Besseres Beispiel**: Befinden sich auf dem Datenträger Dateien mit potentiellem Inhalt X? Bei wie vielen Daten kann man Annehmen, dass Y davon wusste? Der Sachverständiger kann die fragen wörtlich beantworten ohne ein Urteil oder eine Bewertung zu treffen
- **Ziel**: Diskrete, nicht wertende, neutrale, fachlich korrekte und exakte Beantwortung der Fragestellung

Wie beschreibt man die Ergebnisse, sodass sie nicht missverstanden werden?

- Sprache des Zielpublikums sprechen (z.b. keinen Informatikersprech)
- Worte so wählen, dass man nicht angreifbar ist
- Zweifel einbauen, ggf. diese Widerlegen und zu Überzeugung kommen
- Eigene Arbeit mehrmals auf Inhalt und Sprache kontrollieren
- Glaubwürdig bleiben: Fehler eingestehen, auf Fachdiskussion einlassen

3.2 Vorgehensmodelle

Grundlegendes

- **Dokumentieren**: Alles Dokumentieren
- **Allgemein**: Alarm, Güterabwägung, Tatortsicherung, Identifikation/Beschlagnahmung, Sicherung/Bergung, Auswertung, Reduktion, Strukturierung/Suche, Analyse, Bericht, Bezeugen
- **Sachverständiger**: Meist zuständig ab Auswertung
- **Grundlegendes Mindset**: Nichts verändern, alles nachvollziehbar beschreiben, dokumentieren!

4 Digitale Ermittlung

Klassische Kriminalistik

- **Objektivität**: Der Ermittler muss immer objektiv bleiben
- **Erfahrungsfalle**: Ähnliche Fälle können objektivität beeinträchtigen
- **Kriminalistisches Denken**: Zuordnen einer Tat zu einem konkreten Menschen. Ausgangspunkt ist der Verdacht
- **Verdacht**: Entsteht z.b. durch Zeugenaussage oder Anzeige. Verdacht kann zu Beweis führen. Unterschiedlich starke Verdachtsfälle möglich (einfach, dringend, hinreichend)
- **Kriminalistische Fallanalyse**: Sammeln und Prüfen von Fakten um Hypothesen zu bilden

Analyse von Datenträgerabbildern

- **Selektion und Priorisierung**: Was gesichtert werden soll wird anhand einer Priorisieurng selektiert.
- **Priorisierung**: kann überall stattfinden, auch bei der Analyse der Daten (welche zuerst?)

Analyse von Log-Dateien

- **Timelining**: Darstellung von Dateien nach ihren Zeitstempeln
- **Quellen für Zeitinformationen**: Log-Dateie, Caches, Dateiinformationen, etc.
- **Manipulation**: Zeitinformationen können manipuliret sein, daher sollte man versuchen Hinweise für/gegen Manipulation zu finden

5 Forensischer Zugriff und Partitionssysteme

Grundlegende Begriffe

- **Laufwerk**: Menge an adressierbaren Sektoren, die ein BS oder Programm zur Speicherung von Daten verwenden kann
- **Partition**: Menge aufeinanderfolgender Sektoren in einem Laufwerk
- **Partitionssysteme**: DOS oder GPT(weiterentwicklung für größere Partitionen) ist eine minimale Verwaltung von Partitionen für den Boot-Vorgang und ähnliche grundlegende Vorgänge

Regeln für die Extraktion von Daten

- So tief wie nötig, so hoch wie möglich (z.b. sqlite3 besser als hexdump)
- Weg durch die Hierarchiestufen dokumentieren
- Nichts verändern!

Qualitätssicherung bei forensischem Zugriff

1. **Konsistenzprüfung der Partitionstabelle**
2. **Extraktion der Partitionen**: Image in Dateiform als Kopie
3. **Dokumentation der Integrität**: Nutzung von kryptographischen Hashfunktionen

Strikt und Partiell essentielle Daten

- **Essentielle Daten**: Notwendig für grundlegend Funktionalität des BS (z.b. lesen von Daten)
- **Strikt Essentiell**: Alle Programme benötigen diese Daten um grundlegend Funktionalität zu gewährleisten
- **Partiell Essentiell**: Manche Anwendungen benötigen diese Daten

6 Weiteres

6.1 Wichtigste Befehle aus der Übung

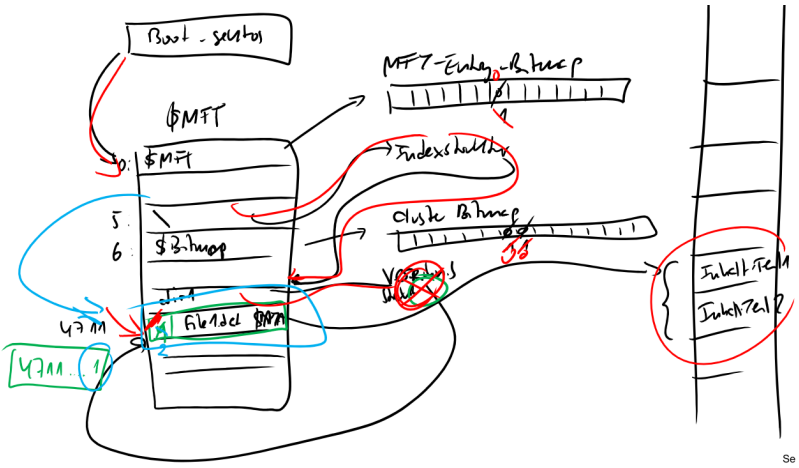
- **Hashsummen**: md5, sha256
- **Partitionstyp**: mmstat Image
- **Partitionstabelle**: mmls Image
- **Dateisystemanalyse**: fls Image (Inode)
- **Metainfos**: istat file
- **Datenextraktion**: icat part Inode
- **Dateiformatanalyse**: file part Inode
- **File-Carving**: scalpel, photorec Image/part
- **Outputstream bescheiden**: | grep!
- sqlite HerauskopierteDatei: Öffnen von Logdateien

6.2 Allgemein wichtiger Hinweis

- Findet man in den Berichten ein Rechtsurteil (z.b. Die Person ist schuldig), überschreitet man meist die eigene Kompetenz, was ein Befangenheitsgrund sein kann

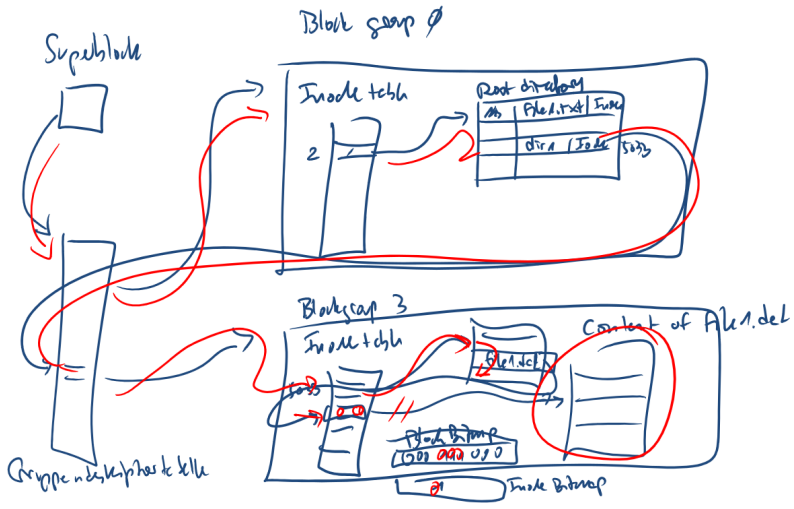
7 Grundlagen Dateisysteme

7.1 NTFS Dateisystem



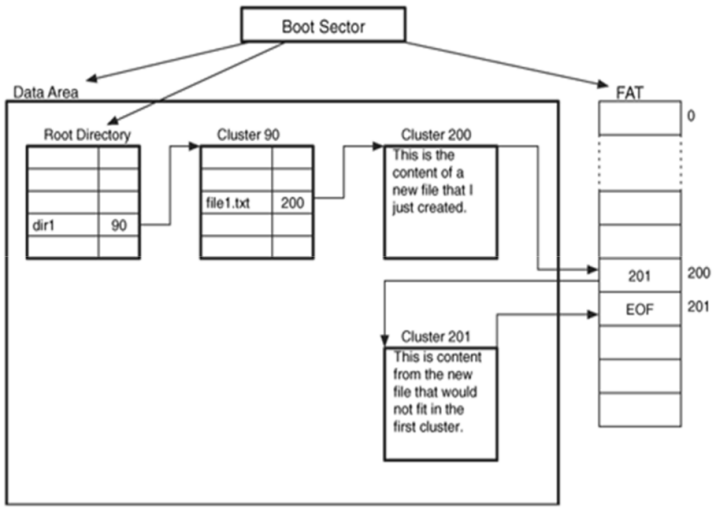
- Alles ist eine Datei
- Master File Table (MFT) als grundlegende Struktur
- Dateien sind als Metadaten-Einträge im MFT gespeichert
- Meist bei Windows

7.2 EXT Dateisystem



- Meist bei Linux: Achtung, da dem Standard abweichende Konfigurationen leicht möglich sind

7.3 FAT Dateisystem



- FAT steht für File Allocation Table
- Meist bei externen Datenträgern wie USB Sticks vorhanden
- Bild zeigt Erstellen einer Datei