HOCHSCHULE MITTWEIDA
University of Applied Sciences

Digitale Forensik

Forensische Modelle, Prozesse und Methoden

Prof. Dr. Dirk Labudde

Bundeskriminalamt

Agenda

1. IT-Forensik
2. Modelle
3. Methoden
4. Forensische Datenarten

IT-Forensik

IT-Forensik

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems. [1]

→ IT-Forensik als Mittel der Strafverfolgung

→ BSI-Leitfaden als allgemeine Grundlage

Zeitpunkt der Untersuchung

Post-mortem-Analyse

- Vorfall nachträglich aufklären
- Untersuchung von Datenträgerabbildern
- Gewinnung/Untersuchung von gelöschten, versteckten, verschlüsselten Dateien (aber auch „normalen“)

Live-Forensik

- Untersuchung während des Vorfalls
- Flüchtige Daten gewinnen/untersuchen
- Hauptspeicherinhalt, bestehende Netzwerkverbindungen, gestartete Prozesse

Ziel der forensischen Untersuchung

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Später dann:

- Wer hat es getan?
- Was sind Präventionsmöglichkeiten?

Anforderungen an Vorgehensweisen

- Akzeptanz
- Glaubwürdigkeit
- Wiederholbarkeit
- Integrität
- Ursache und Auswirkung
- Dokumentation (Chain of Custody)

Anforderungen an die Vorgehensweise

- **Akzeptanz:** Die angewandten Methoden und Schritte müssen in der Fachwelt beschrieben und allgemein akzeptiert worden sein. Der Einsatz neuer Verfahren und Methoden ist zwar prinzipiell nicht ausgeschlossen, jedoch sollte dann ein Nachweis der Korrektheit dieser erfolgen.
- **Glaubwürdigkeit** - Die Robustheit und Funktionalität von Methoden wird gefordert und muss ggf. nachgewiesen werden.
- **Wiederholbarkeit** - Die eingesetzten Hilfsmittel und Methoden müssen bei der Anwendung Dritter auf dem gleichen Ausgangsmaterial dieselben Ergebnisse liefern.

Anforderungen an die Vorgehensweise

- **Integrität** - Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.
- **Ursache und Auswirkung** - Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. auch an Personen herzustellen.
- **Dokumentation (Chain of Custody)** - Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden. Lückenlose Nachweise über Verbleib/Verarbeitung/Herkunft von digitalen Spuren.

Modell, Prozess, Methode

Modell

Ein Modell beschreibt den groben Ablauf einer Untersuchung in stark vereinfachter, schematischer Weise.

Prozess

Der Prozess beschreibt den Ablauf in detaillierter Form und hilft dadurch, Reproduzierbarkeit zu gewährleisten und unterstützt, wesentliche Teile im definierten Prozess nach Möglichkeit nicht zu vergessen.

Methode

Die Methoden wiederum definieren die einzelnen Schritte bis hinunter zu den einzelnen Werkzeugen/Tools die man verwenden kann oder sollte.

Modelle

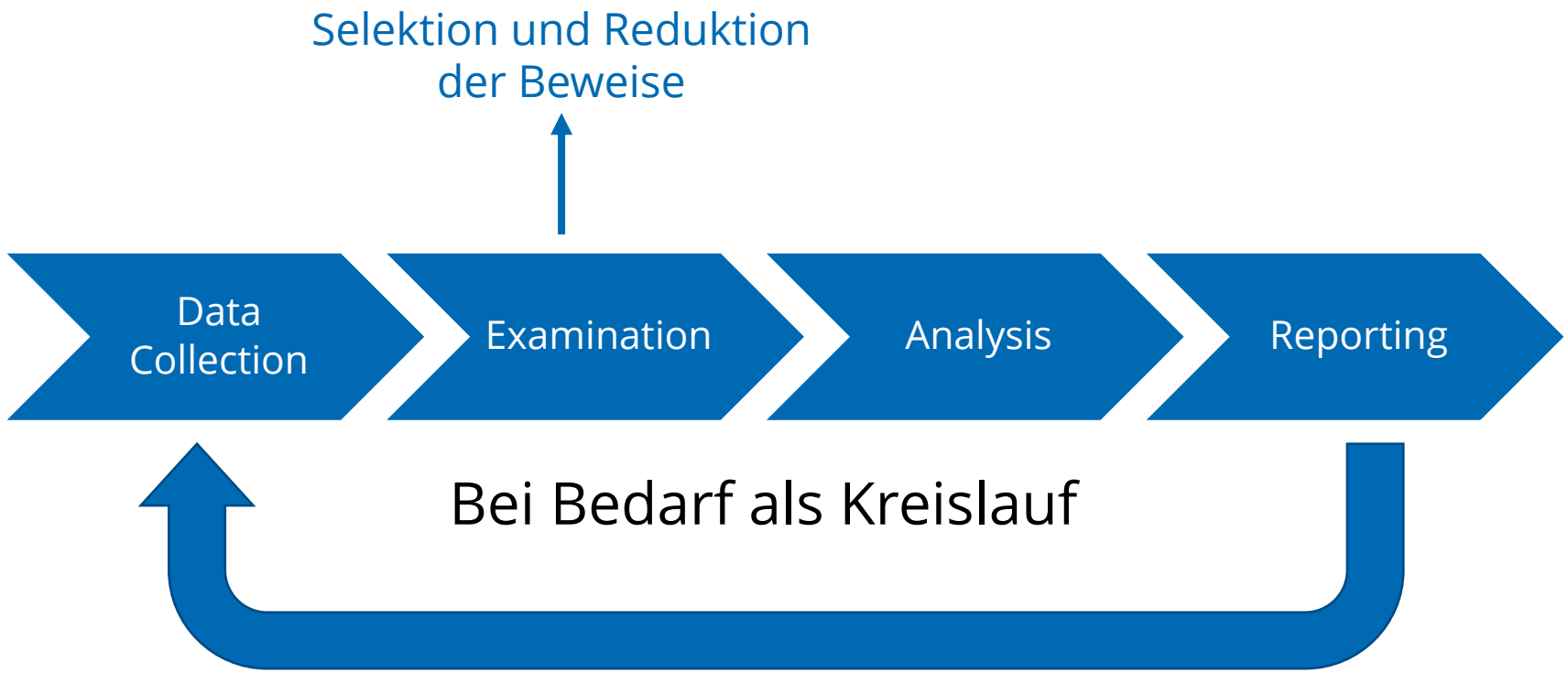
SAP – Ein forensisches Ablaufmodell

- Eine Grundlage für die Erhebung und Verwertung digitaler Spuren
- für die Untersuchung von Beweismitteln
- S(ecure)-A(nalyse)-P(resent) Modell

SAP – Ein forensisches Ablaufmodell

1. Phase, der so genannten Secure-Phase, hier werden strategische und operationale Vorbereitungen zur Erfassung aller relevanter Daten durchgeführt
2. Phase, der Analyse-Phase, hier werden die gesicherten Spuren und Beweise überprüfbar aufgearbeitet, sorgfältig überprüft und objektiv bewertet
3. Phase, die Present-Phase in der wird Ermittlungsprozess nachvollziehbar dargelegt (Präsentiert)

Modell nach Kent, Chevalier, Grace und Dang



Prozesse

Tipps zur Bestimmung einer konkreten Untersuchungsstrategie

1. Verstehen Sie die Ziele und den Zeitrahmen der Untersuchung.

2. Listen Sie Ihre Ressourcen auf, einschließlich Personal, Zeit und Ausrüstung.

3. Identifizieren Sie mögliche Beweisquellen.

4. Schätzen Sie für jede Beweisquelle den Wert sowie den Aufwand für deren Sicherstellung.

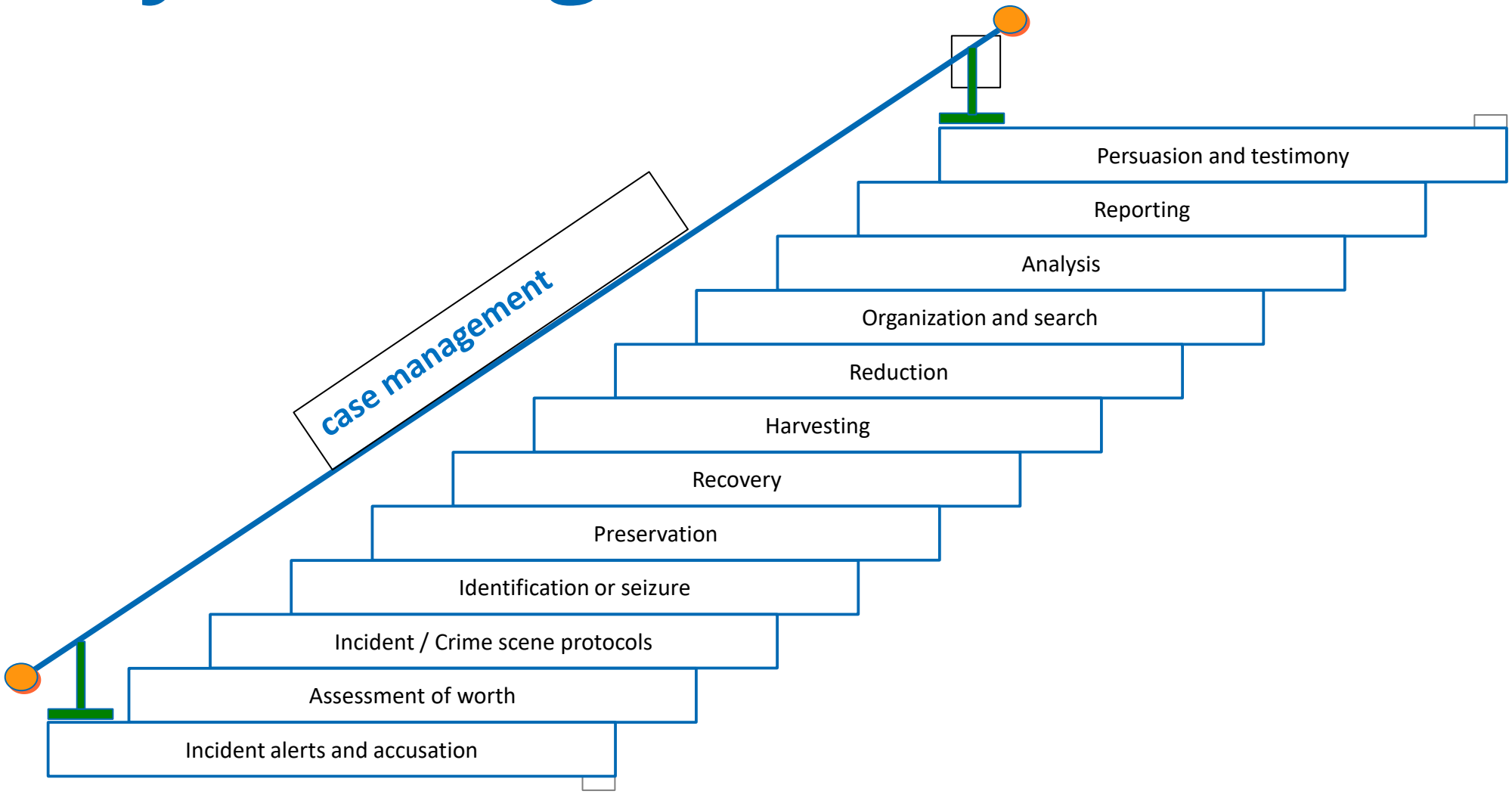
5. Priorisieren Sie Ihre Beweissicherung.

6. Planen Sie die erste Erfassung / Analyse.

7. Legen Sie die Art und Weise bzw. Zeitpunkte für regelmäßige Kommunikation / Updates mit den Beteiligten fest.

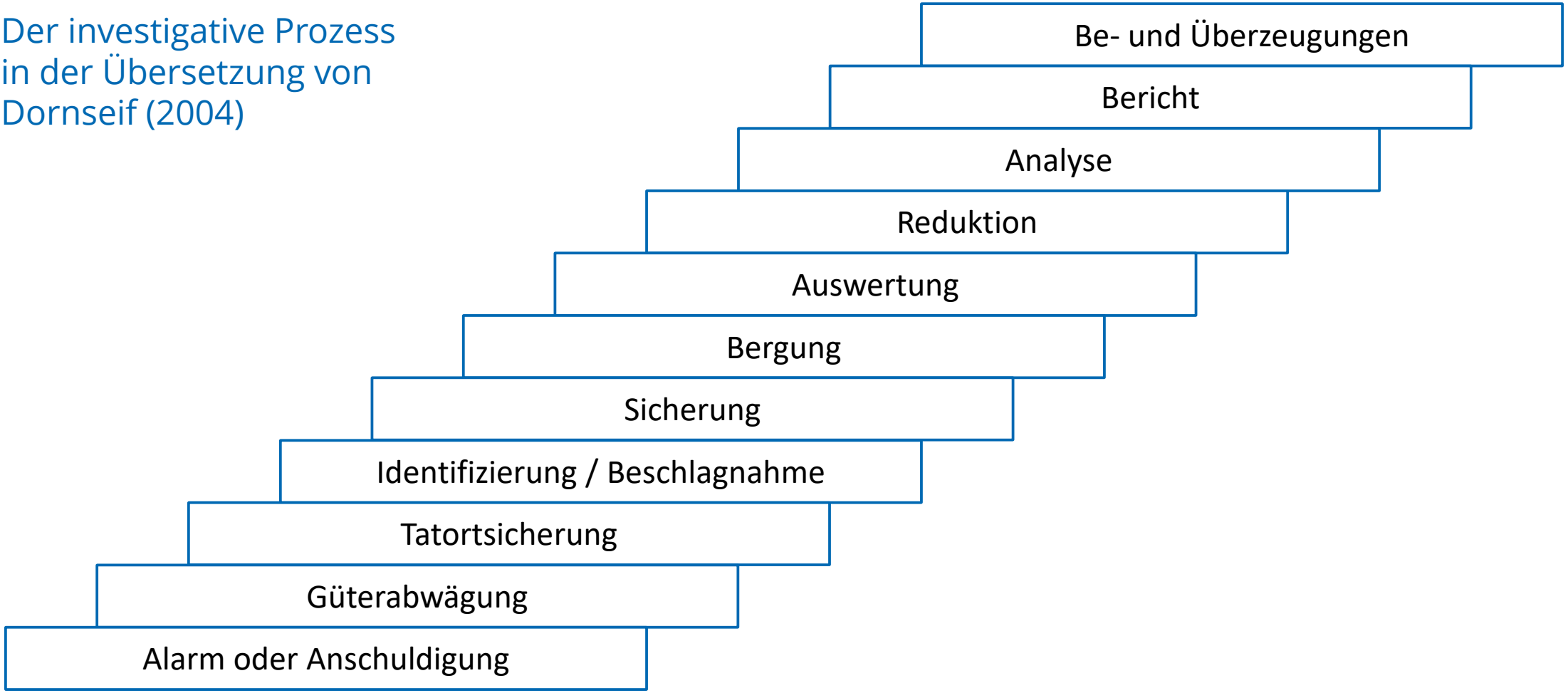
8. Denken Sie daran, dass Sie sich nach der ersten Analyse jederzeit entscheiden können, zurückzugehen, um weitere Beweise zu sammeln. Forensik ist ein iterativer Prozess!

Casey Investigative Prozess



Casey Modell übersetzt von Dornseif

Der investigative Prozess in der Übersetzung von Dornseif (2004)



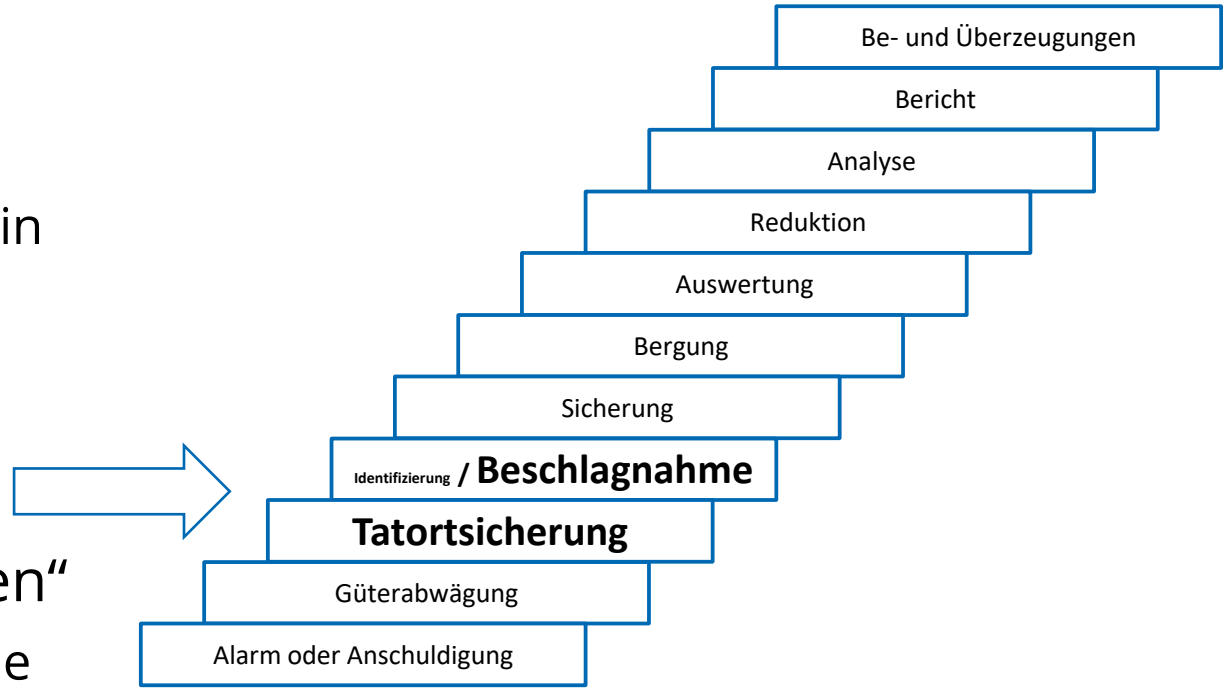
Beschlagnahme und Tatortsicherung

Beschlagnahme

- Traditionell: Einsacken, Absaugen, Abstauben
  - Einsacken ohne etwas zu verändern
  - Auch das „Drumherum“ kann wichtig sein
- Gefahren eindämmen

Tatortsicherung

- Ideal: „Den Tatort weiträumig absperren“
  - „freeze the evidence in place and provide ground truth for all activities that follow“ [Casey]
  - Versuchen Sie das mal im digitalen Raum!



Identifizierung

- Be- und Überzeugungen
- Bericht
- Analyse
- Reduktion
- Auswertung
- Bergung
- Sicherung
- **Identifizierung** / Beschlagnahme
- **Tatortsicherung**
- Güterabwägung
- Alarm oder Anschuldigung

Festplatten

Server

Fraunhofer Lernlabor Bundeskriminalamt | HOCHSCHULE MITTWEIDA

Sicherung

- Sicherstellen, dass Beweise unverändert bleiben
- Fotografieren, Versiegeln, Wegschließen
- Bei digitalen Spuren:
  - Kopien erstellen
  - Weitere Untersuchungen nur auf Kopien
  - Verwenden kryptografischer Hashes zum Nachweis der Echtheit
  - Verwendung von vertrauenswürdigen Tools
- Hier beginnt die Arbeit der Spezialisten!

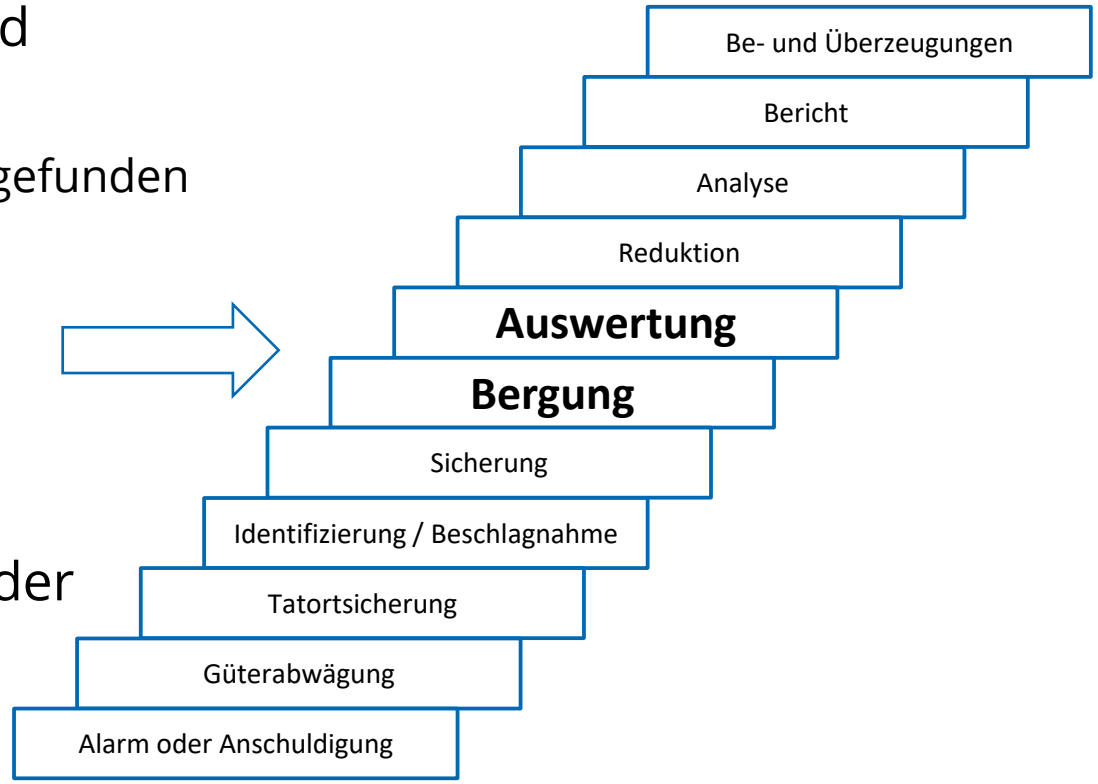
Bergung und Auswertung

Bergung

- Bergung von Daten, die gelöscht, versteckt, getarnt oder anderweitig unzugänglich gemacht worden sind
- Synergien mit anderen Beweismitteln nutzen
  - Beispiel: Ist ein Zettel mit Passwörtern am Tatort gefunden worden?

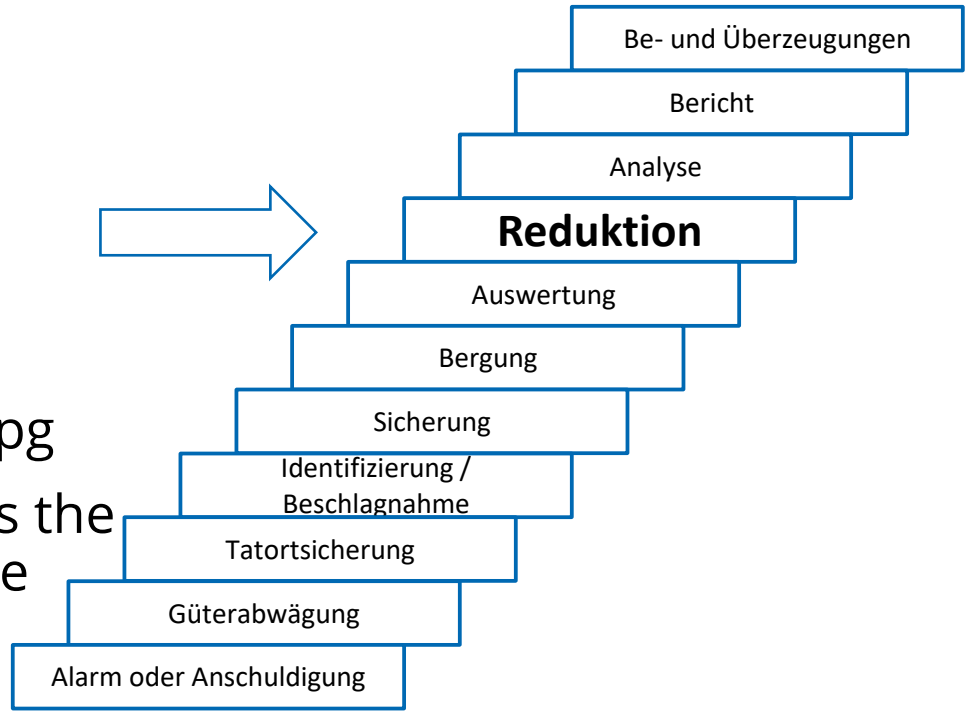
Auswertung

- Organisation der großen Datenmenge
- Zunächst Untersuchung von Meta-Daten statt der eigentlichen Daten
- Gruppierung von Daten
  - Nach Dateityp
  - Nach Zugriffszeiten
  - ...



Reduktion

- Irrelevante Daten eliminieren
- Weiter ohne die eigentlichen Daten anzuschauen
  - Reduktion nach Datentyp
  - Beispiel: Anschuldigung „Besitz von Kinderpornographie“
  - Reduktion auf Dateien mit Endungen .gif und .jpg
  - Ziel: „Smallest set of digital information that has the highest potential of containing data of probative value“ [Casey]
  - Hilfreich: Hash-Datenbanken von bekannten Dateien



Strukturierung, Analyse, Bericht

Strukturierung/ Suche

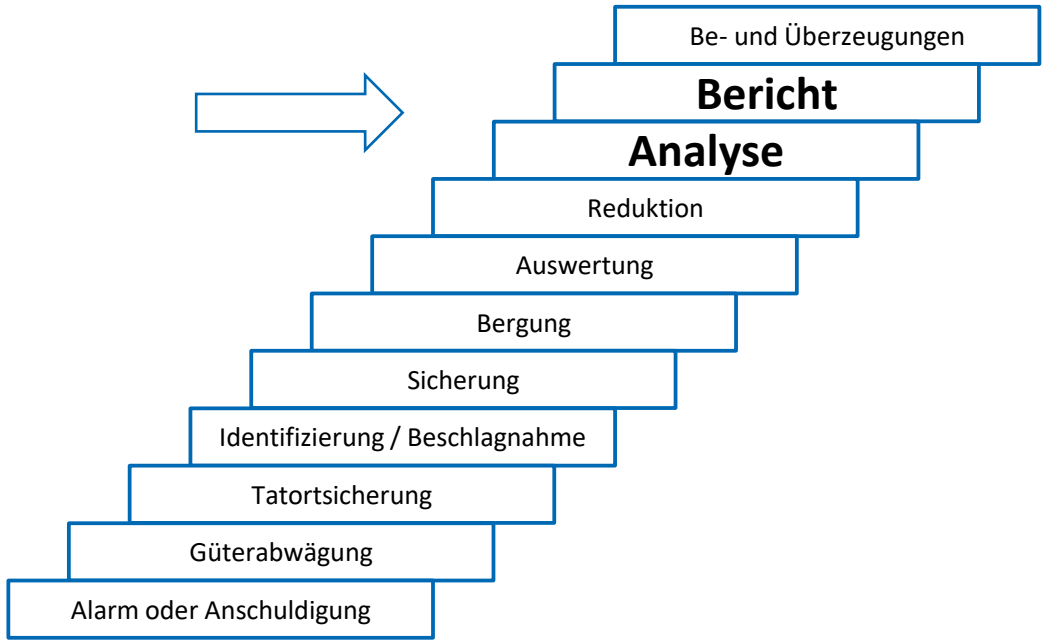
- Organisation der Daten nach der Reduktion
- Oftmals Erstellung von Indizes und Übersichten
- Macht die Referenzierung der Daten in den folgenden Schritten einfacher

Analyse

- Detailanalyse unter Beachtung der Dateiinhalte
- Verbindung Herstellen
- Verantwortliche ermitteln
- Bewertung von Inhalt und Kontext
- „Means, motivation, opportunity“
- Zusammenführung und Korrelation
- Überprüfung (Wissenschaftliche Methodik**)**

Bericht

- Nicht nur Ergebnisse präsentieren… sondern auch wie man dazu kommt
- Immer über die befolgten Regeln und Standards berichten
- Schlüsse begründen
- Alternative Erklärungsmodelle erörtern



Erweiterter forensischer Prozess

Strategische Vorbereitung: Identifizierung und Bereitstellung geeigneter Werkzeuge, Tests und Sicherungstools, Vorgehensplanung, Vorbereitung von Hardware und Software, Maßnahmen seitens des Anlagenbetreibers (proaktiv)

Operative Vorbereitung: nach dem Eintreten des Vorfalls, vor der Datensammlung, z.B. Identifikation potentieller Datenquellen (auch Datenträger oder mobile Endgeräte)

Erweiterter forensischer Prozess

Datensammlung: wichtige Daten von potentiell betroffenen Systemen/Komponenten, vollständige Erfassung und Speicherung, Verfälschungen vermeiden, Fehler und Lücken dokumentieren (und rechtfertigen), Flüchtigkeitsreihenfolge beachten

Datenreduktion: wichtige (forensisch wertvolle) Daten/Spuren identifizieren, unwichtige aus Untersuchung ausschließen

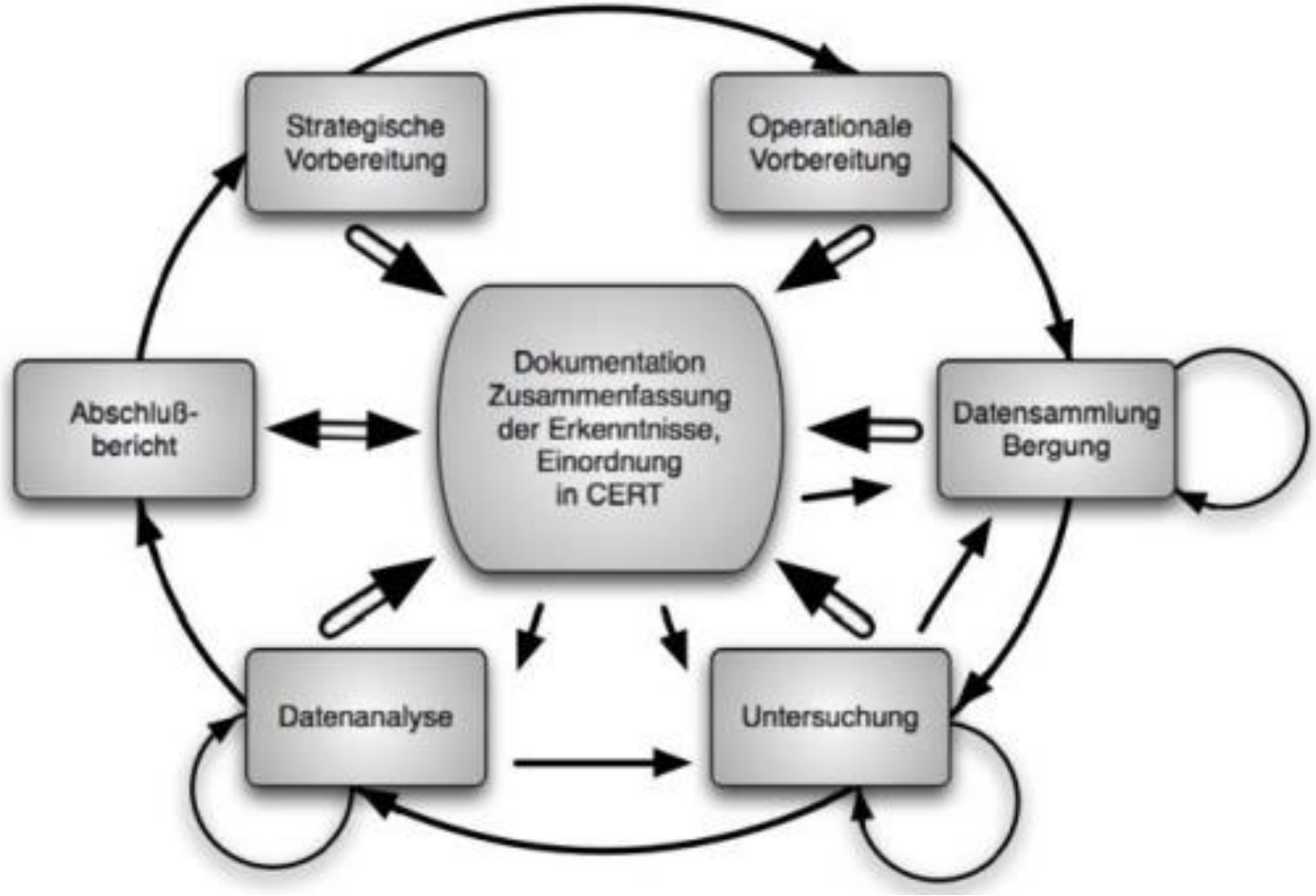
Erweiterter forensischer Prozess

Datenanalyse: Ergebnisse der reduzierten Daten in logischen Zusammenhang bringen, einheitlichen Zeitverlauf generieren,

→ Detailanalyse; (Möglicherweise Wiederholung von Schritt 3 und 4)

Dokumentation: Zusammenfassung aller Abläufe zu einem Bericht

Erweiterter forensischer Prozess



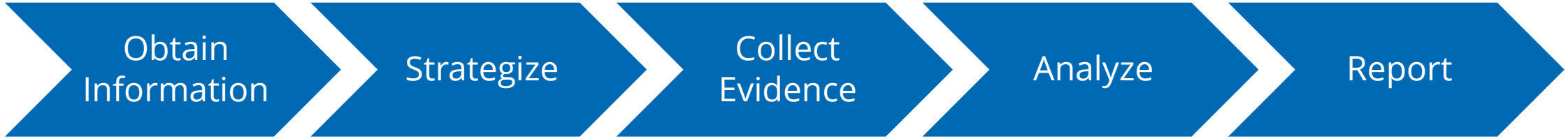
Dokumentation im forensischen Prozess

- Prozessbegleitende Dokumentation und abschließende Dokumentation
- Prozessbegleitend: parallel zur Durchführung, Protokollierung der gewonnenen Daten und durgeführten Prozesse, auch Parameter der Durchführung
- Abschließend: Erstellen eines Gesamtbildes aus Daten, welche Information gewonnen, Ablauf der Untersuchung (für Dritte nachvollziehbar) → Voraussetzung zur Abschätzung der Beweiskraft der Ergebnisse

Anforderungen an Vorgehensweisen

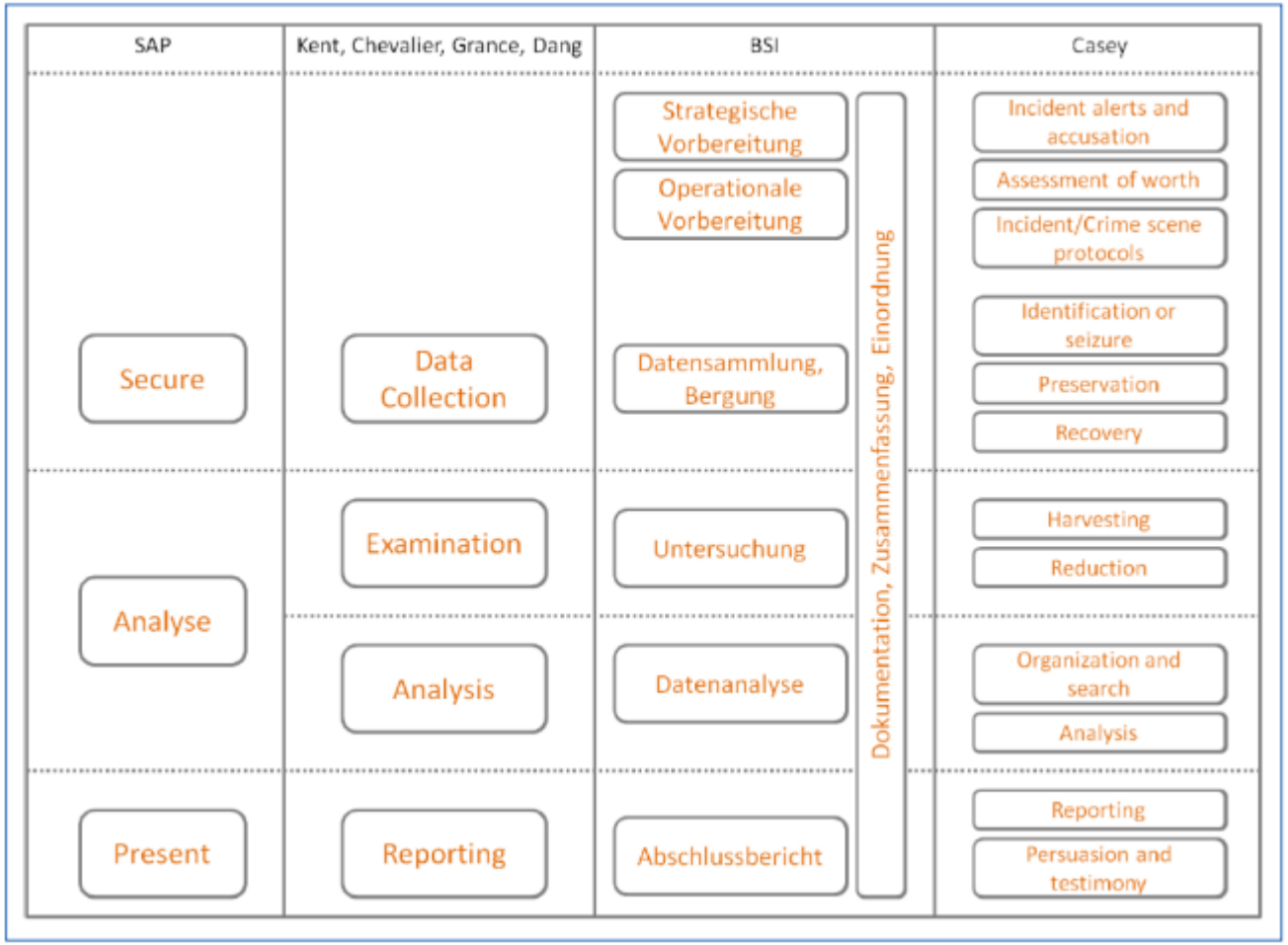
- Akzeptanz
- Glaubwürdigkeit
- Wiederholbarkeit
- Integrität
- Ursache und Auswirkung
- Dokumentation (Chain of Custody)

OSCAR-Modell



- Methodik der zur Durchführung einer netzwerkforensischen Untersuchung
- Ermittlungsprozess setzt sich aus 5 Schritten zusammen

Verschiedene Modelle/Prozesse



Methoden

Grundlegende Methoden

- Methoden des Betriebssystems;
- Methoden des Dateisystems;
- Explizite Methoden der Einbruchserkennung;
- Methoden einer IT-Anwendung;
- Methoden der Skalierung von Beweismöglichkeiten;
- Methoden der Datenbearbeitung und Auswertung.

Betriebssystem

- generell umfangreiche Möglichkeiten, forensisch wertvolle Informationen zu liefern
- Verwaltet Netzwerk (z.B. Netzwerkverbindungen, Konfigurationsvorgaben)
- Sitzungsdaten, Daten über geöffnete Dateien, Daten über laufende Prozesse…
- Betriebssysteme verstehen

Dateisystem

- Dateisystem der Datenträger einer der bedeutsamsten Orte
- nichtflüchtige Daten
- Dateisystem muss eine Reihe von Informationen über die gespeicherten Daten enthalten, damit beim Mehrbenutzerbetrieb nur derjenige auf die Daten zugreifen kann, der auch die nötigen Rechte besitzt. Diese Details über Daten beinhalten u. a. das Erstellungsdatum einer Datei, das Datum des letzten Zugriffs, das Datum der letzten Modifikation, den Eigentümer und die Zugriffsrechte.
- Verwaltung des Dateinamens (bzw. des Verzeichnisnamens); Verwaltung des Dateianfangs; Verwaltung der Dateilänge zusammen mit Metadaten (z. B. Dateirechte, Zeitstempel); Verwaltung der von der Datei benutzten Speichereinheiten (Cluster); Verwaltung der belegten und freien Cluster

Explizite Methoden der Einbruchserkennung

- Maßnahmen, die weitestgehend automatisiert und routinemäßig ausgeführt werden
- Zwischenfälle in einem IT-System zu bemerken (z.B. Intrusion Detection Systeme)
- Besonders im Bereich der strategischen Vorbereitung

  → Funktionalität zur Detektion von Zwischenfällen um eine forensische Untersuchung anzustoßen oder einer forensischen Untersuchung durch die von ihnen erstellten Log-Dateien zu unterstützen

IT-Anwendung

- die eigentlichen Anwendungen eines IT-Systems
- Tabellenkalkulationen, Datenbanksoftware, Webbrowser, Chatclients oder auch Spiele

→ Aus der Ausführung von Anwendungen werden forensisch nutzbare Daten gewonnen

Skalierung von Beweismitteln

- nur im konkreten Verdachtsfall eines Zwischenfalls durchgeführt
- Z.B. zum Vermeiden unübersichtlich großer Datenmengen
- Im Bereich der Datensammlung und Reduktion

Datenbearbeitung und Auswertung

- forensische Untersuchung zu unterstützen, indem sie Ausgangsdaten analysieren und aus ihnen Daten extrahieren oder rekonstruieren
- Sachverhalte aus forensischer Sicht anschaulicher darstellen
- Betrifft sowohl Auswertung, als auch Präsentation
- Nicht im Bereich der Vorbereitung anzutreffen

Grundlegende Methoden – Einfluss auf das Vorgehen

	SV Strategische Vorbereitung	OV Operationale Vorbereitung	DS Daten-sammlung	US Untersuchung	DA Datenanalyse	DO Dokument-ation
BS Betriebs-system	X	X	X	X	X	
FS Dateisystem			X	X		
EME Explizite Methoden der Einbruchs-erkennung	X		X			
ITA IT-Anwendungen	X		X			
SB Skalierung von Beweis-möglichkeiten			X	X		
DBA Daten-bearbeitung und Auswertung			X	X	X	X

Forensische Datenarten

DIGITALE SPUREN - BEGRIFFSBESTIMMUNG

Spuren sind alle materiellen Veränderungen an Personen und / oder Sachen bzw. Objekten, die im Zusammenhang mit einem relevanten Ereignis entstanden sind und zur Tataufklärung beitragen können, da Rückschlüsse auf den Tatablauf, die Tatumstände sowie Hinweise auf den / die Täter gezogen werden können. Entscheidend ist das der Spur innewohnende objektive Informationspotential, dieses muss relativ beständig sein (Beibehaltung bis zur Begutachtung). Die materiellen Spuren bestimmen den Gegenstand der Spurenkunde unter anderem in der Kriminaltechnik. Grundsätzlich gilt: Es gibt keinen Tatort ohne Spuren!

DIGITALE SPUREN - BEGRIFFSBESTIMMUNG

Digitale Spuren basieren auf Daten, die in Computersystemen gespeichert sind oder zwischen Ihnen übertragen wurden. Dabei sind digitale Spuren nicht mit materiellen Spuren gleichzusetzen. Digitale Spuren werden erst durch ihre Interpretation von physischen Spuren über unterschiedliche Interpretationsebenen zu einer verwertbaren digitalen Spur.

Forensische Datenarten

- Hardwaredaten
- Rohdateninhalte
- Details über Daten
- Konfigurationsdaten
- Kommunikationsprotokolldaten
- Prozessdaten
- Sitzungsdaten
- Anwenderdaten

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik: Leitfaden IT-Forensik

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

dirk.labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de