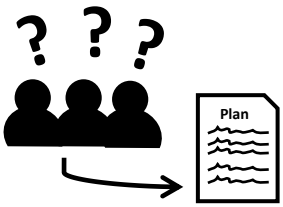
SOP zur Durchführung einer IT-forensischen Untersuchung

Sachverhalt: _____ Bearbeiter: _____

Gemeldet durch: _____ Datum: _____

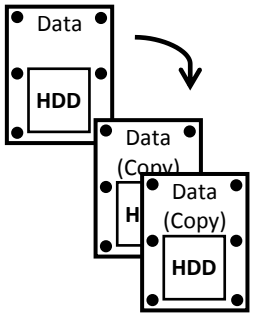
Do…	Do NOT…
• Ruhe bewahren! • Alle Schritte dokumentieren! • 4-Augen-Prinzip anwenden!	• Keine Live-Analysen! • Keine Arbeiten am Live-System! • Keine Arbeiten an der Masterkopie!

1. Vorbereitung – Rahmenbedingungen klarstellen



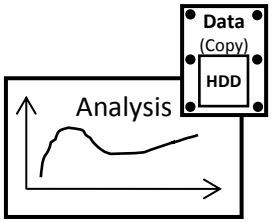
- ☐ Initiierung durch Auftraggeber
- ☐ Übersicht über Sachverhalt verschaffen
- ☐ Identifizierung potentiell relevanter Datenquellen
- ☐ Aufstellen einer Hypothese und Zieldefinition
- ☐ Ermitteln personeller/finanzieller Ressourcen
- ☐ Aufstellen eines Teams, Informieren der Unternehmensleitung, DSB

2. Absicherung – Beweismittel und Untersuchungsbereich



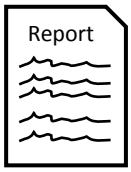
- ☐ Schutz potentieller Beweismittel vor Fremdeinwirkung
- ☐ Dokumentieren des Tatorts und der Umgebung
- Beweisaufnahme:
  - ☐ Strom-/ Netzwerkverbindung trennen (situationsbedingt)
  - ☐ Sichern relevanter Daten und Informationen, Eigentumsverhältnisse/Datenschutz beachten
  - ☐ Erzeugen von Master- und Arbeitskopien relevanter Datenquellen
  - ☐ Erstellte Kopien kryptografisch verschlüsseln
  - ☐ Sichern von Metadaten
  - ☐ Originaldatenträger sicher verwahren

3. Analyse – Auswertung der Beweismittel



- ☐ Keine Analyse aus dem Original; nur aus den Arbeitskopien!
- ☐ Vergleich der Kopien durch Bildung von Hash-Werten
- ☐ Beweisspurensicherung
- ☐ Objektive Bewertung der Daten und deren Bezug zum Vorfall
- ☐ Datenrettung durchführen (situationsbedingt)
- ☐ Suchindex für Daten erstellen
- ☐ Kategorisieren der Daten sofern zweckmäßig

4. Reporting – Dokumentation der Maßnahmen!



- ☐ Informationen aus der prozessbegleitenden Dokumentation verwenden
- ☐ Erstellen eines Gesamtbildes
- ☐ Erarbeitung einer Zusammenfassung und der Ergebnisse
- ☐ Vergleich der forensischen Ergebnisse mit dem Anfangsverdacht
- ☐ Beweissichere Aufbereitung der Ergebnisse
- ☐ Formulieren eines Ergebnisprotokolls

Ziel/Ergebnisse:

- **Gerichtsfeste Informationen! Was/wann/wie** durch **wen/welche** Systeme.
- **Transparente Aufbereitung der Arbeitsweise**

Type	Responsibility	Autoren	Matrikelnummer
Standard Operation Procedure	Forensics	D. Dressler, H. Müller	20201720, 20202183