# 7IB/7CSB/7IMB: Digitale Forensik, Übung 5

**Lernziele:** Die Lernziele dieser Übung sind: a) das Kennenlernen von Werkzeugen zur Erzeugung von Dateisystemen Abbildern, b) das Arbeiten nach der IT-forensischen Vorgehensweise, c) die selbstständige Recherche und d) autodidaktische Erarbeitung von Wissen sowie die e) Vermittlung dieses Wissens nach Aufbereitung an Personen mit niedrigerem Wissensstand.

**Randbedingung:** Die Randbedingungen dieser Übung sind: Legen Sie für jede Aufgabe ein Logbuch Ihrer Bearbeitungsschritte an. Dies sollte insbesondere die abgesetzten Konsolenkommandos, die dazugehörigen Ausgaben sowie die Hashwerte und die verwendeten Werkzeuge und deren Versionen umfassen. Dokumentieren Sie ausführlich und sehr genau!

## Aufgabe 1: (Dateisysteme und Carving Tools)

1.1) Erstellen Sie ein Skript, welches einen Datenträger einer beliebigen Größe erzeugt und mit einem Dateisystem ihrer Wahl formatiert.
1.2) Sammeln Sie verschiedene Dateien unterschiedlicher Größe mit den folgenden Formaten:

- .png
- .jpeg, .jpg
- .doc, .docx, .xls, .xslx, .ppt, .pptx, .txt, .pdf
- .mpeg
- .mp3
- .py, .java
- .html, .xhtml, .xml

1.3) Fügen Sie auf dem erzeugten Datenträger die gesammelten Dateien per Skript hinzu.
1.4) Verwenden Sie zum einen Carving-Tool a) Scalpel und zum anderen b) Foremost, um die von Ihnen erzeugten Dateien von dem erzeugten Datenträger zu extrahieren.
1.5) Vergleichen Sie die Ergebnisse der beiden Carving-Tools mit der Liste Ihrer eingefügten Dateien. Vergleichen Sie weiterhin die Ergebnisse der beiden Werkzeuge miteinander.

# Aufgabe 2: (Dateisysteme und Carving Tools)

2.1) Verwenden Sie Ihr Skript aus Aufgabe 1 und erzeugen Sie einen Datenträger einer beliebigen Größe (mind. jedoch 15MB) und formatieren Sie diesen mit dem Dateisystem fat.
2.2) Füllen Sie den Datenträger, bis keine Speicherkapazität mehr vorhanden ist, mit Dateien verschiedener Größen und den folgenden unterschiedlichen Formaten:

- .png
- .jpeg, .jpg
- .doc, .docx, .xls, .xslx, .ppt, .pptx, .txt, .pdf
- .mpeg
- .mp3
- .py, .java
- .html, .xhtml, .xml

2.3) Erzeugen Sie einen Dump zur Sicherung des Zwischenstands. Legen Sie den Dump geeignet ab, so dass Sie diesen in den folgenden Übungen weiterhin verwenden können.
2.4) Sammeln Sie mindestens 5 Bilddateien in dem Format .jpeg bzw. .jpg.
2.5) Speichern Sie die gesammelten Bilddateien in dem Format .jpeg bzw. .jpg. auf den vollen Datenträger. Hierzu löschen Sie schrittweise zuvor abgelegte Dateien, solange bis für das zu speichernde Bild genügend freier Speicher vorhanden ist.
2.6) Erzeugen Sie erneut einen Dump zur Sicherung des Zwischenstands. Legen Sie den Dump geeignet ab, so dass Sie diesen in den folgenden Übungen weiterhin verwenden können.
2.7) Verwenden Sie zum einen Carving-Tool a) Scalpel und zum anderen b) Foremost, um die von Ihnen erzeugten Dateien von dem erzeugten Datenträger zu extrahieren.
2.8) Vergleichen Sie die Ergebnisse der beiden Carving-Tools mit der Liste Ihrer eingefügten Dateien. Vergleichen Sie weiterhin die Ergebnisse der beiden Werkzeuge miteinander.

# Aufgabe 3: (Dateiformate)

3.1) Verwenden Sie Ihr Skript aus Aufgabe 1 und erzeugen Sie einen Datenträger einer beliebigen Größe (mind. jedoch 15MB) und formatieren Sie dieses Dateisystem fat.
3.2) Füllen Sie den Datenträger mit Dateien verschiedener Größen und den folgenden unterschiedlichen Formaten:

- ein gültiges .doc
- ein gültiges .wav
- ein ungültiges .jpeg, in welchem nur ein Byte des Headers korrupt ist
- ein gültiges .jpeg
- ein gültiges .xls
- ein linearisiertes .pdf
- ein nicht-linearisiertes .pdf
- ein gültiges EXIF .jpeg
- ein gültiges .gif
- ein gültiges .mov
- ein gültiges .wmv
- ein gültiges .zip

3.3) Ermitteln Sie die Entropie der Dateien und vergleichen Sie diese miteinander. Welche Aussage lässt sich aus dem Ergebnis ableiten?
3.4) Verwenden Sie zum einen Carving-Tool a) Scalpel und zum anderen b) Foremost, um die von Ihnen erzeugten Dateien von dem erzeugten Datenträger zu extrahieren.
3.5) Vergleichen Sie die Ergebnisse der beiden Carving-Tools mit der Liste Ihrer eingefügten Dateien. Vergleichen Sie weiterhin die Ergebnisse der beiden Werkzeuge miteinander.