Prüfungsmodalitäten – IT-Forensik Projekt

Das Modul wird mit einer Gruppen-Projektarbeit und einer Gruppen-Programmieraufgabe abgeschlossen. Die Prüfung ist bestanden, wenn bei beiden Prüfungsteile mit mindestens 50% der zu vergebenen Punkte erreicht wurden. Die Gesamtnote ermittelt sich zu 70% aus der Note der Projektarbeit und zu 30% aus der Note der Programmieraufgabe.

1. **Projektarbeit / Hausarbeit (70% Notenanteil)**

   Das Ziel der Projektarbeit besteht darin, …

   - unter Verwendung zweier erhaltener Mobiltelefone einen fiktiven Tathergang durchzuspielen und dabei digitale Spuren zu erzeugen, wie beispielsweise mittels Mediendateien, Kommunikations-Apps (WhatsApp, o.ä.), Standortdaten, etc.
   - dokumentieren Sie hierbei Ihr Vorgehen
   - beide Spurenträger (Mobiltelefone) physikalisch zu sichern (Erstellen einer Image-Datei)
   - und diese Images unter Nutzung eine spezieller Forensik Software (CellebriteReader und/oder Mobile Revelator) zu analysieren
   - und die Tat-relevanten digitalen Spuren in einem Bericht im Gutachtenstil zu präsentieren

   Orientierungshilfe:

   https://it-forensik.fiw.hs-wismar.de/images/5/5e/Handout_Wurzler_und_Blank_Forensik.pdf

   Die Hausarbeit soll folgende Bestandteile enthalten
   - Aufgabenstellung/-beschreibung
   - Szenariobeschreibung
   - Szenarioumsetzung
   - Forensische Untersuchung im Gutachtenstil
     - Auftragsspezifikation (Fragestellung an die IT-Forensik)
     - Erlangte Erkenntnisse
     - Verwendet Werkzeuge
     - Untersuchungsobjekte
     - Untersuchung der Asservate
       - Datensicherung
       - Analyse
   - Manöverkritik / Leasons Learned
   - Anhang (z.B. für Datenpräsentation für Ergebnisse aus dem Gutachten)

   Abgabetermin Hausarbeit: 15. März 2022

2. **Programmierungsaufgabe / Präsentation**

   Das Ziel der Programmieraufgabe besteht darin gleichartige digitale Spuren / Artefakte aus unterschiedlichen Spurenträgern (forensischen Sicherung), z.B. den zwei verwendeten Mobiltelefonen, gemeinsam für die Ermittlungsarbeiten geeignet automatisiert aufzuarbeiten / zu visualisieren / präsentieren.

   Als **Datenbasis** ist folgendes **zulässig**:

- original Image-Datei
- original extrahiertes Artefakt (z.B. die konkreten Bilder, Datenbanken, etc.)
- erstellter Export aus dem Analyse-Werkzeug

Fokussieren Sie sich auf die Lösung **eines** konkreten Analyse-Problems. Beispiele entnehmen Sie bitte den Unterlagen der Vorlesung 30.11.2021

Das Ergebnis **muss granular** und **transportabel** sein, d.h. das Ergebnis sollte ohne Ihre Programmierlösung mittels einem gängigen Viewer/Programm (Excel, Browser, etc.) betrachtet werden können.

Die Wahl Ihrer Programmierlösung (Tool, Sprache) obliegt Ihnen, hier gibt es keine Vorgabe.

Abgabe / Präsentationstermin: 1. Februar 2022

Am Präsentationstermin demonstrieren Sie als Gruppe Ihre Lösung, inklusive Vorstellung Ihrer Überlegungen (ca. 20 Minuten). Alle Gruppenmitglieder sollten hierbei einen Vergleichbaren Präsentationsanteil haben.

Am Präsentationstermin geben Sie folgendes ab:

- Programmierlösung inkl. Quellcode
- Präsentation

Bei konkreten Fragen oder Unklarheiten, sprechen Sie mich gerne an.