Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

M116 Wahlpflichtmodul – Master Digitale Forensik

WS 2021/22

Mobilfunkforensik - Modulbeschreibung

Dr. Michael Spreitzenbarth

Modulbezeichnung:	Mobilfunkforensik
Lehrveranstaltungen und Lehrformen:	• **Präsenzveranstaltung:** Vorlesung, Übungen, Präsentation der Übungsergebnisse • **Onlineveranstaltungen:** flexible Vertiefung wichtiger Themen, Lernen im Dialog, Fragen zu Übungen
Modulverantwortliche(r):	Dr.-Ing. Michael Spreitzenbarth
Lehrende:	Dr.-Ing. Michael Spreitzenbarth
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen	Klausur
Notwendige Voraussetzungen	• Programmierkenntnisse in Python und Java • gute Linux-/UNIX-Kenntnisse • gute Englischkenntnisse
Empfohlene Voraussetzungen:	Kenntnisse der forensischen Grundsätze
Unterrichts- und Prüfungssprache:	Deutsch
Generelle Zielsetzung des Moduls:	Vertiefung des Wissens von forensischen Ermittlern und Sicherheitsanalysten mit Interesse im Bereich mobile Endgeräte
Arbeitsaufwand bzw. Gesamtworkload:	• **Präsenzzeit:** 15 h – Vorlesungsteil: 5 h – Übungsteil: 10 h • **Eigenstudium:** 135 h – Durcharbeiten der Studienbriefe: 75 h – Online Betreuung und Beratung: 10 h – Ausarbeiten von Aufgaben: 50 h
Lerninhalte	• Einführung in Android – Aufbau des Android-Systems – Unterschiede zwischen der Java-VM und der Dalvik-VM – Das Android SDK • Einführung in iOS – Aufbau des iOS-Systems

	– Sicherheitskonzept und Secure-Boot – Verschlüsselung und Datenschutz • Einführung in Mobilfunkforenisk für Android – Wie kommt man an die wichtigen Daten? – Rooting, Recovery und andere Zugriffsstrategien – Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie? – Einführung in SQLite • Einführung in Mobilfunkforenisk für iOS – Wie kommt man an die wichtigen Daten? – Jailbreaking und andere Zugriffsstrategien – Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie? • Aufbau und Analyse von Android-Applikationen – Bestandteile einer Android-Applikation (Manifest, Dalvik-Bytecode, Zertifikate, native Bibliotheken usw.) – Einführung in das Dekompilieren und Reversen von Android-Applikationen – Automatisierte Analysetechniken: Überblick, Einführung und Diskussion statische vs. Dynamische Analyse – Einführung in die Tools: Android Studio, JadX, Hashcat • Obfuskierung – Einführung in Obfuskierung – String-Obfuskierung (XOR, Crypt, ...) – Junkbytes zum Verwirren der Disassembler – Kollision mehrerer Apps zum Verschleiern der Schadfunktion
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über den Aufbau des Android und iOS Betriebssystems. Sie sind in der Lage Android und iOS Mobiltelefone zu analysieren und Spuren auf diesen Geräten zu sichern. Ebenso sind sie in der Lage Android-Applikationen zu analysieren und verdächtiges Verhalten zu identifizieren. *Methodenkompetenz:* Die Studierenden beherrschen die Arbeitstechnik, mit bekannten Tools und Werkzeugen im Bereich Forensik und Android-Applikations-Analyse umzugehen. Weiter beherrschen sie die Problemlösefähigkeit, ein Android-Programm auf sein Verhalten zu untersuchen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Literatur:	Siehe Verweise innerhalb der einzelnen Studienbriefe

Ablauf/Termine:

- Online Meeting 20.09.2021 um 19.00 Uhr
- Online Meeting 04.10.2021 um 19.00 Uhr
- Präsenzwochenende 16./17.10.2021 je nach Infektionslage in Albstadt bzw. online
- Klausur
  Haupttermin 05.11.2021 in Saarbrücken bzw. online
  Nachtermin 04.02.2022 in Erlangen bzw. online