Open C^{3}S
Open Competence Center for Cyber Security

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Modulbeschreibung: Mobilfunkforensik

Modulbezeichnung:	Mobilfunkforensik (Smartphone Forensics)
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Modulverantwortliche(r):	Dr. Michael Spreitzenbarth
Dozent(in):	Dr. Michael Spreitzenbarth
Zeitraum:	Nächster Angebotszeitraum: April bis Juli 2023
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten mit Interesse im Bereich mobiler Endgeräte
Studien- und Prüfungsleistungen:	Hausarbeit
Notwendige Voraussetzungen:	• Programmierkenntnisse in Python und Java • gute Linux-/UNIX-Kenntnisse • gute Englischkenntnisse
Empfohlene Voraussetzungen:	• Kenntnisse der forensischen Grundsätze
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	50	Zeitstunden
davon Online-Betreuung:	15	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

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 • Das Mobilfunkforensik-Framework ADEL **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 smali, dex2jar und JD-GUI **Obfuskierung** • Einführung in Obfuskierung • String-Obfuskierung (XOR, Crypt, ...) • Junkbytes zum Verwirren der Disassembler • Kollision mehrerer Apps zum Verschleiern der Schadfunktion **Projekt (Hausarbeit):** • Im Rahmen des Projekts wird eine vollständige forensische Analyse eines Mobiltelefons durchgeführt. Dabei werden sowohl die installierten Applikationen selbst als auch ihre verwendeten Datenstrukturen analysiert. Die durchgeführte Untersuchung soll in einem möglichst gerichtsverwertbaren Bericht zusammengefasst werden.

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. *Sozialkompetenz:* Durch das gemeinsame Lösen von Aufgaben erlangen die Studierenden die Fähigkeit eigene Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und ihre Teamfähigkeit zu stärken. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Lehrveranstaltungen und Lehrformen:	*Präsenzveranstaltung:* Vorlesung, Übungen, Präsentation von Übungsergebnissen *Onlineveranstaltung:* Flexible Vertiefung wichtiger Themen, Lernen im Dialog, Fragen zu Übungen
Medienformen:	• Studienbriefe in schriftlicher und elektronischer Form • Onlinematerial in Lernplattform • Übungen und Projekt über Lernplattform • Online-Konferenzen, Chat und Forum • Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.