Open C³S
Open Competence Center for Cyber Security

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Modulbeschreibung:

Weiterführende Themen der Computerforensik

Modulbezeichnung:	Weiterführende Themen der Computerforensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Dozent(in):	Prof. Dr. Harald Baier
Zeitraum:	Nächster Angebotszeitraum: Sommersemester 2024 Dauer ca. 5 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten, Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Digitaler Forensik und Cyber-Sicherheit weiterbilden möchten.
Studien- und Prüfungsleistungen:	IT-forensisches Gutachten (Hausarbeit) und Präsentation
Notwendige Voraussetzungen:	Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII), Grundkenntnisse im Umgang mit Betriebssystemen (insbesondere Linux), Sicherheit im Umgang mit der Linux-Kommandozeile, grundlegende Kenntnisse zu Partitionsschemata und Dateisystemen, grundlegende Programmierkenntnisse
Empfohlene Voraussetzungen:	
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	90	Zeitstunden
davon Aufgaben und Hausarbeit:	30	Zeitstunden
davon Online-Betreuung:	15	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalte	In diesem Modul werden die folgenden Themengebiete behandelt: • Gutachtenerstellung • Aufbau und forensische Untersuchung der Windows-Registry • Windows Artefakte • Möglichkeiten und Techniken der Anti-Forensik • Sicherung und forensische Analyse des Hauptspeichers • Forensische Analyse von SQLite Datenbanken
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erlernen die Analyse und Auswertung der grundlegenden forensischen Artefakte innerhalb des Windows Betriebssystems und haben Kenntnisse in der Untersuchung anwendungsspezifischer Daten. Des Weiteren sind die Studierenden mit den weiterführenden Techniken der Hauptspeicherforensik vertraut. Sie kennen weiter gängige antiforensische Maßnahmen und sind sich deren Auswirkungen auf den Untersuchungsprozess bewusst. Darüber hinaus werden den Studierenden Konzepte für die Erstellung gerichtsverwertbarer Gutachten vermittelt. Zudem erlernen die Studierenden den Aufbau und die forensische Analyse von gängigen SQLite Datenbanken. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit weiterführenden Themen und Konzepten der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischer Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebundene Diskussionen lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übungen Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, 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:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Michael Hale Ligh, et al.: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons, 2014, ISBN 978-1118825099 • Harlan Carvey: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. Elsevier, 2011, ISBN 978-0128032916 • Paul Sanderson, et al.: SQLite Forensics. Independently published, 2018, ISBN 978-1980293071 • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Else-vier Academic

	Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.