Open C³S
Open Competence Center for Cyber Security

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Modulbeschreibung:

Einführung in die digitale Forensik

Modulbezeichnung:	Einführung in die digitale Forensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Dozent(in):	Prof. Dr. Harald Baier
Zeitraum:	Nächster Angebotszeitraum: Wintersemester 2024 / 2025 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:	Mündliche Online-Prüfung (30 Minuten)
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 Programmierkenntnisse
Empfohlene Voraussetzungen:	Grundkenntnisse in IT-Sicherheit
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: • Klassische forensische Wissenschaften und digitale Forensik • Grundlagen der digitalen Forensik • Digitale Spuren ◦ Entstehung ◦ Manipulier- und Kopierbarkeit ◦ Personenbezogenheit • Datenträgeranalyse ◦ DOS / GPT Partitionsschema ◦ HPA, DCO • Einführung in die Dateisystemanalyse ◦ Generelles Konzept ◦ FAT ◦ NTFS ◦ Slack-Spaces • Analyse mit forensischen Tools ◦ Sleuthkit ◦ Autopsy ◦ DFF ◦ Filecarver • Vorgehensmodelle, Gutachtenerstellung **Übungen:** • Zur Vertiefung der theoretisch vermittelten Kenntnisse werden im Rahmen der Online-Seminare mehrere praktische Aufgaben bearbeitet.
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften der gängigen Dateisysteme FAT und NTFS und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines IT-Forensikers und können mit allgemeinen und speziellen forensischen Werkzeugen sicher umgehen. Des Weiteren sind die Studierenden mit der grundlegenden Funktionsweise kryptographischer Hashfunktionen, sowie deren Rolle in der digitalen Forensik vertraut. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien 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 forensischen Untersuchungen im Team zu arbeiten und können auftretende Prolleme, Fragen und Aufgaben durch fachgebundene Diskussion 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: Analyse verschleierter Binaries, Analyse von Malware, Vorbereitung auf die Hausarbeit 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 • Brian Carrier: File System Forensic Analysis, 5th Printing. Addison-Wesley Longman, Amsterdam (17. März 2005), ISBN 978-0321268174 • Dan Farmer, Wietse Venema: Forensic Discovery. 2nd Printing. Addison-Wesley, Boston u. a. 2006, ISBN 0-201-63497-X, (Addison-Wesley professional computing series) • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier 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 • BSI: Leitfaden 'IT-Forensik', herausgegeben vom BSI im März 2011 (v. 1.0.1) Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.