Hochschule Niederrhein
University of Applied Sciences

Ingenieurwissenschaften und Informatik
Faculty of Engineering and Computer Science

Digitale Forensik: Modulhandbuch

Bachelor Digitale Forensik (PO2023)

Herausgeber Fachbereich Ingenieurwissenschaften und Informatik
Stand 2026-08-10

Inhaltsverzeichnis

Einleitung

Dieses Modulhandbuch beschreibt den Bachelorstudiengang Digitale Forensik. Es macht transparent, welche fachlichen, methodischen, rechtlichen und überfachlichen Kompetenzen die Studierenden im Studienverlauf erwerben und wie diese Kompetenzen in Modulen, Lernpfaden, Projekten, Praxisphase und Bachelorarbeit aufgebaut, angewendet und vertieft werden.

Das Modulhandbuch dient Studierenden, Lehrenden und externen Interessierten als Orientierung über Aufbau, Ziele und Inhalte des Studiums. Die Modulbeschreibungen folgen einer einheitlichen Struktur und weisen insbesondere Lernergebnisse im Format Was-Womit-Wozu aus. Ergänzend macht die Ziele-Matrix sichtbar, welche Kompetenzbereiche in den einzelnen Modulen adressiert werden.

Studiengangsprofil

In Gesellschaft, staatlichen Organen und Unternehmen besteht ein wachsender Bedarf an Fachkräften aus den Bereichen IT-Sicherheit und Digitale Forensik. Straftaten, die mithilfe von Informationstechnik begangen werden oder sich gegen IT-Infrastrukturen, Daten, Organisationen oder Personen richten, erfordern Spezialistinnen und Spezialisten, die technische, methodische, rechtliche und kriminalistische Perspektiven verbinden können. Digitale Forensik ist dabei nicht nur eine technische Disziplin, sondern eine Schnittstelle zwischen Analyse, Beweissicherung, rechtlicher Bewertung und adressatengerechter Kommunikation.

Der Studiengang Digitale Forensik vermittelt ein anwendungsorientiertes Lernspektrum von den Grundlagen der Informatik, Netzwerk- und Computertechnik über Cybersicherheit und Kriminalistik bis zu spezifischen Methoden und Werkzeugen zur Gewinnung, Sicherung, Analyse, Dokumentation und Präsentation digitaler Beweise. Die Studierenden lernen, digitale Artefakte in unterschiedlichen technischen Umgebungen zu erkennen, ihre Aussagekraft kritisch zu bewerten und sie in einen nachvollziehbaren Gesamtzusammenhang einzuordnen. Ziel ist es, digitale Spuren fachgerecht zu untersuchen, Erkenntnisse für die Aufklärung von Straftaten nutzbar zu machen und zugleich einen Beitrag zur Vorbeugung und Abwehr zukünftiger Cyberangriffe zu leisten.

Das Profil des Studiengangs verbindet technische Grundlagen mit forensischer Fallarbeit. Dazu gehören der sichere Umgang mit Betriebssystemen, Netzwerken, Datenbanken, kryptografischen Verfahren und spezialisierten Analysewerkzeugen ebenso wie Kenntnisse über Tatortarbeit, Täterkommunikation, OSINT, Incident Response und rechtliche Rahmenbedingungen. Die Ausbildung ist praxisorientiert angelegt: Methoden und Technologien werden nicht isoliert betrachtet, sondern im Zusammenhang forensischer Prozesse angewendet, dokumentiert und reflektiert. Absolventinnen und Absolventen sollen dadurch in der Lage sein, technische Befunde belastbar aufzubereiten, Grenzen forensischer Untersuchungen einzuschätzen und Ergebnisse gegenüber fachlichen wie nichtfachlichen Adressaten verständlich zu vertreten.

Kurzporträt Studiengangsprofil

Worum geht es? Digitale Forensik verbindet Informatik, IT-Sicherheit, Betriebssysteme, Netzwerke, Kryptografie, Kriminalistik und Recht. Typische Themen sind digitale Spuren, forensische Werkzeuge, Incident Response, OSINT, Netzwerk- und Betriebssystemforensik, Malware-Analyse, Speichermedienforensik und rechtliche Rahmenbedingungen digitaler Ermittlungen.
Wofür braucht man es? Das Profil bereitet auf Tätigkeiten in Cyberabwehr, Ermittlungsunterstützung, IT-Sicherheitsanalyse, forensischer Untersuchung, Dokumentation und Präsentation digitaler Beweise vor.
Wieso ist es interessant? Digitale Forensik verbindet technische Analyse mit kriminalistischem Denken und rechtlicher Einordnung. Dadurch wird aus digitalen Spuren ein belastbares, nachvollziehbares Bild von Sicherheitsvorfällen oder Straftaten.

Aufbau des Studiums

Das Studium gliedert sich in ein fachspezifisches Grundlagenstudium in den ersten beiden Semestern, ein anwendungsbezogenes Expertenstudium der Digitalen Forensik im dritten und vierten Semester, ein individuelles Vertiefungssemester im fünften Semester sowie Praxisphase und Bachelorarbeit im sechsten Semester. Die Studierenden bauen zunächst tragfähige Grundlagen in Informatik, Programmierung, IT-Sicherheit, Recht, Kriminalistik und forensischem Arbeiten auf. Darauf aufbauend werden spezifische Methoden, Technologien und Vorgehensweisen der Digitalen Forensik anwendungsnah vertieft.

Durch das Studium ziehen sich Lernpfade, die Wissen von der Breite in die Tiefe entwickeln. Der Lernpfad Forensik führt von grundlegenden Konzepten über forensische Methoden und Werkzeuge bis zu vertiefenden Anwendungen wie Datenbanken-Forensik und forensischen Projekten. Ergänzend strukturieren Lernpfade und Modulbereiche die Themen Betriebssysteme, Netzwerke, Kriminalistik, IT-Sicherheit, Projekte, Wahlmodule sowie Praxisphase und Bachelorarbeit.

Der Studiengang ist praxisorientiert angelegt. Viele Module verbinden Vorlesungsanteile mit praktischen Übungen, Projektarbeiten oder anwendungsnahen Fallbeispielen. Das eigene Notebook der Studierenden ist dabei ein zentrales Arbeitsgerät, sodass digitale Lernformen, praktische Laboranteile und selbstständige Analyseaufgaben eng miteinander verbunden werden können. Die Wahlmodule, Projektmodule, Praxisphase und Bachelorarbeit ermöglichen eine individuelle fachliche Profilbildung.

Qualifikationsziele

Der Studiengang Digitale Forensik verfolgt das Ziel, Absolventinnen und Absolventen zu befähigen, digitale Sachverhalte technisch fundiert, methodisch kontrolliert, rechtlich reflektiert und adressatengerecht zu bearbeiten. Die übergreifenden Qualifikationsziele lassen sich in drei Bereiche gliedern.

Bereich	Qualifikationsziel
Grundlagen und Basiswissen	Z1: Die Studierenden verstehen Grundlagen, Aufbau und Funktionsweise von Komponenten, die in der Digitalen Forensik eine Rolle spielen, insbesondere Rechner, Netzwerke, Systemsoftware und Anwendungen, und können deren Bedeutung für forensische Prozesse erläutern.
Grundlagen und Basiswissen	Z2: Die Studierenden verstehen Konzepte und Prinzipien der Cybersicherheit und Digitalen Forensik und können unterschiedliche Formen der Cyberkriminalität wie Hackerangriffe, Malware-Infektionen oder Datenlecks differenzieren.
Grundlagen und Basiswissen	Z3: Die Studierenden können IT-Kriminalität im Sinne der Beweismittelführung und des Betrugs bewerten und relevante Prozessabläufe, insbesondere im Bereich Cyberkriminalität, rechtlich und fachlich einordnen.
Anwendung	Z4: Die Studierenden können Bedrohungen im Bereich IT-Sicherheit identifizieren, geeignete Reaktionen auf Cyberangriffe planen und die Korrektheit, Sicherheit und Angemessenheit vorgeschlagener Lösungen überzeugend begründen.
Anwendung	Z5: Die Studierenden können Angriffe auf IT-Systeme erkennen, analysieren und passende forensische Vorgehensweisen entwickeln und anwenden.
Anwendung	Z6: Die Studierenden können mit wissenschaftlichen Methoden und Technologien digitale Spuren unter Einhaltung rechtlicher und ethischer Prinzipien sichern, erfassen, untersuchen, analysieren, dokumentieren und präsentieren.
Softskills	Z7: Die Studierenden können komplexe forensische Projekte planen, gemeinsam im Team bearbeiten und Teilaufgaben selbstständig übernehmen.
Softskills	Z8: Die Studierenden können fachbezogene Positionen und Problemlösungen formulieren, argumentativ verteidigen und sich mit Fachvertreterinnen und Fachvertretern sowie Personen im beruflichen und wissenschaftlichen Umfeld über Informationen, Ideen, Probleme und Lösungen austauschen.

Ziele-Module-Matrix

Die Matrix zeigt, in welchen Pflichtmodulen die übergreifenden Qualifikationsziele aufgebaut und vertieft werden. A bedeutet Anwendung und Vertiefung, B kennzeichnet Transfer und Beherrschung auf einem höheren Integrationsniveau. Wahlpflichtmodule, etwa BDF512: Forensik von Speichermedien, sind nicht in der Matrix aufgeführt.

Legende: Z1 = Grundlagen, Aufbau und Funktionsweise relevanter IT-Komponenten verstehen; Z2 = Konzepte und Prinzipien der Cybersicherheit und Digitalen Forensik verstehen; Z3 = IT-Kriminalität, Beweismittelführung und Prozessabläufe rechtlich und fachlich einordnen; Z4 = Bedrohungen identifizieren, Reaktionen planen und Lösungen begründen; Z5 = Angriffe erkennen, analysieren und forensische Vorgehensweisen anwenden; Z6 = digitale Spuren rechtlich und ethisch kontrolliert sichern, analysieren, dokumentieren und präsentieren; Z7 = forensische Projekte planen, im Team bearbeiten und Teilaufgaben übernehmen; Z8 = fachbezogene Positionen und Problemlösungen formulieren, verteidigen und austauschen. A = vertiefen/anwenden; B = beherrschen/transferieren.

Modul	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8
BDF101: Informatik-Grundlagen der Forensik	A						A	
BDF102: Ethische und Menschliche Aspekte der Informationssicherheit		A				A		A
BDF103: Programmierung	A							
BDF104: Einführung in die Digitale Forensik		A	A		A	A		A
BDF105: Rechtliche Grundlagen der Cyberkriminalistik			A			A		A
BDF106: Erstsemesterprojekt		A		A	A	A	A	A
BDF201: Betriebssysteme: Anwendung	A	A		A				
BDF202: Einführung in Open Source Intelligence (OSINT)			A			A		A
BDF203: Einführung in die Kriminalistik			A			A		A
BDF204: Forensische Methoden und Werkzeuge	A				A	A		A
BDF205: IT-Sicherheit	A	A		A	A			
BDF206: Bedarfsorientierte Mikroprojekte	A	A		A			A	A
BDF301: Betriebssysteme: Technik	A	A			A	A		
BDF302: Rechnernetze und Rechnernetzsicherheit	A	A		A				
BDF303: Der Digitale Tatort und Täterkommunikation			A		A	A		A
BDF304: Web- und Browsersicherheit		A		A	A	A		A
BDF305: Datenbanken-Forensik	A	A			A	A		
BDF306: Security Incident Management		A		A	A	A		A
BDF401: Betriebssysteme: Forensik	A				B	B		A
BDF402: Netzwerkforensik	A	A			B	B		A
BDF403: Geschäftsmodelle im Internet		A	A	A	A			A
BDF404: Angewandte Kryptografie		A		A	A	A		A
BDF405: Forensikprojekt	A	A			B	B	B	B
BDF505: Hackathon	B	B		B	A		B	B
BDF601: Praxisphase und begleitendes Seminar	A	A		A	A	A	B	A
BDF602: Bachelorarbeit und Kolloquium	B	B	B	B	B	B	A	B

Modulbeschreibungen

Dieses Modulhandbuch beschreibt die Module des Bachelorstudiengangs Digitale Forensik mit Angaben zu Verwendbarkeit, Modultyp, Angebotshäufigkeit, Dauer, Credits, Benotung, Semesterwochenstunden, Workload, Voraussetzungen, Lernergebnissen, Inhalten, Prüfungsformen, Literatur und fachlicher Zuordnung. Die Modulbeschreibungen sind nach Modulbereichen und Lernpfaden geordnet und ermöglichen damit eine Orientierung über den Studienverlauf, die fachliche Profilbildung und die Verzahnung der Module mit den Qualifikationszielen.

So liest man eine Modulbeschreibung

Jede Modulbeschreibung folgt dem gleichen Aufbau: Zuerst stehen organisatorische Angaben wie Verantwortliche, Credits, Semesterwochenstunden (SWS) und Workload. Die **Lernergebnisse** sind im Format **WAS** (Kompetenz nach Abschluss), **WOMIT** (Inhalte und Tätigkeiten, mit denen die Kompetenz erworben wird) und **WOZU** (Nutzen für Studium und Beruf) beschrieben. Am Ende jedes Moduls gibt ein **Kurzporträt** einen schnellen Überblick. Unklare Abkürzungen wie ECTS, SWS oder V/Ü/P/S sind im Glossar am Ende des Handbuchs erklärt.

Allgemeine Grundlagen

Der Modulbereich Allgemeine Grundlagen befähigt die Studierenden, zentrale informatische, programmiertechnische und analytische Grundlagen der Digitalen Forensik zu verstehen und auf erste sicherheits- und forensikbezogene Aufgaben anzuwenden. Dabei entwickeln sie ein tragfähiges Fundament für den Umgang mit digitalen Systemen, offenen Informationsquellen, Sicherheitsvorfällen und strukturierten Problemlösungen.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können grundlegende Konzepte der Informatik, Programmierung, Open Source Intelligence und des Security Incident Managements beschreiben, einfache digitale Problemstellungen modellieren, technische Informationen auswerten und erste Handlungsansätze für sicherheitsrelevante Situationen ableiten.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Modulbereich
  - Grundlagen von Rechnern, Datenrepräsentation, Algorithmen und informatischen Arbeitsweisen erarbeiten,
  - Programme und einfache Softwarelösungen mit geeigneten Werkzeugen entwickeln, testen und nachvollziehbar strukturieren,
  - öffentlich verfügbare Quellen systematisch recherchieren, bewerten und für sicherheitsbezogene Fragestellungen nutzen,
  - Sicherheitsvorfälle einordnen, Incident-Response-Prozesse kennenlernen und organisatorische sowie technische Maßnahmen ableiten,
  - fachliche Ergebnisse dokumentieren und begründet kommunizieren.
- **WOZU**: Damit sie in den folgenden Modulen digitale Systeme, Daten, Programme, Informationsquellen und Sicherheitsereignisse fachlich fundiert einordnen können. Der Modulbereich schafft die Grundlage für vertiefende Lernpfade zu Betriebssystemen, Netzwerken, IT-Sicherheit, Kriminalistik und Forensik.

Kurzporträt Allgemeine Grundlagen

Worum geht es? Der Modulbereich Allgemeine Grundlagen führt in die informatischen und methodischen Grundlagen ein, die für Digitale Forensik benötigt werden. Die Studierenden lernen, wie digitale Systeme arbeiten, wie Programme entstehen, wie offene Quellen ausgewertet werden und wie Sicherheitsvorfälle strukturiert betrachtet werden können.
Wofür braucht man es? Diese Kompetenzen werden benötigt, um spätere forensische Aufgaben technisch nachvollziehen, digitale Spuren verstehen und einfache Analyse- oder Automatisierungsschritte selbst umsetzen zu können. Sie bilden die Basis für weiterführende Module in Forensik, Betriebssystemen, Netzwerken und IT-Sicherheit.
Wieso ist es interessant? Der Bereich zeigt, wie aus technischen Grundlagen konkrete forensische Handlungsfähigkeit entsteht. Wer digitale Spuren untersuchen will, muss verstehen, wie Informationen gespeichert, verarbeitet, recherchiert und in sicherheitsrelevanten Kontexten bewertet werden.

BDF101: Informatik-Grundlagen der Forensik

Modulverantwortung	Prof. Dr. Gudrun Stockmanns	**Lehrperson(en)**	Prof. Dr. Gudrun Stockmanns Prof. Dr. Jens Brandt
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Fundamentals of Computer Science for Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können grundlegende Konzepte, Strukturen und Arbeitsweisen der Informatik beschreiben, einfache informatische Problemstellungen modellieren und algorithmische Lösungen in unterschiedlichen Programmierparadigmen praktisch umsetzen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie

- Struktur, Kerngebiete, Anwendungsbereiche und typische Fragestellungen der Informatik kennenlernen,
- Grundlagen zu Information, Rechnerarchitektur, Zahlensystemen, Zeichenkodierungen, Bitoperationen und Digitaltechnik erarbeiten,
- zentrale Konzepte wie Syntax und Semantik, Nichtdeterminismus, Nebenläufigkeit, Übersetzung, Interpretation, Laufzeitsysteme, Invarianten und Korrektheit einordnen,
- grundlegende informatische Herangehensweisen wie Abstraktion, Modellierung, Modularisierung und Hierarchisierung anwenden,
- einfache Probleme algorithmisch modellieren und passende Datenstrukturen und Algorithmen entwickeln,
- verschiedene Programmierparadigmen und Programmiersprachen hinsichtlich ihrer Eignung für Anwendungsaufgaben untersuchen,
- einfache Programme in verschiedenen Programmiersprachen und Programmierparadigmen entwickeln,
- ein kleines Anwendungsprojekt in Kleingruppen bearbeiten.

WOZU. Damit sie in den folgenden Modulen der Digitalen Forensik informatische Systeme, Datenrepräsentationen, Algorithmen und Softwarestrukturen fachlich einordnen, analysieren und praktisch nutzen können. Die Kompetenzen bilden eine Grundlage für forensische Analyse-, Entwicklungs- und Automatisierungsaufgaben, bei denen digitale Spuren, Programme, Systeme und technische Abläufe verstanden und methodisch bearbeitet werden müssen.

Inhalte

- Überblick über Struktur, Kerngebiete und Anwendungsbereiche der Informatik
- Information, Rechnerarchitektur und Digitaltechnik
- Zahlensysteme, Zeichenkodierungen und Bitoperationen
- Algorithmen, Konzepte verschiedener Programmierparadigmen und Programmiersprachen
- Grundlegende Informatik-spezifische Herangehensweisen an Probleme, insbesondere Abstraktion und Modellierung, Modularisierung und Hierarchisierung
- Einführung in grundlegende Konzepte, insbesondere Syntax und Semantik, Nichtdeterminismus, Nebenläufigkeit, Übersetzung und Interpretation, Invarianten und Korrektheit
- praktische Realisierung eines kleinen Anwendungsprojektes

Prüfungsvorleistung

Testat

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Helmut Herold, Bruno Lurz, Jürgen Wolrab und Matthias Hopf: Grundlagen der Informatik, Pearson, Hallbergmoos, 2017
- Hans Peter Gumm und Manfred Sommer: Einführung in die Informatik, De Gruyter Oldenbourg, Berlin, 2013, https://doi.org/10.1524/9783486723052
- David Harel und Yishai Feldman: Algorithmik: Die Kunst des Rechnens, Springer, Berlin, 2009, https://doi.org/10.1007/978-3-540-88740-9
- Andrew S. Tanenbaum und Todd Austin: Structured Computer Organization, Pearson, Boston, 2013

Kurzporträt BDF101: Informatik-Grundlagen der Forensik

Worum geht es? Dieses Modul führt in zentrale Grundlagen der Informatik ein, die für digitale Forensik benötigt werden. Studierende lernen, wie Informationen in Rechnern dargestellt werden, wie Rechner und digitale Schaltungen grundsätzlich funktionieren und wie Probleme durch Abstraktion, Modellierung und Algorithmen bearbeitet werden. Zusätzlich setzen sie einfache Programme und ein kleines Anwendungsprojekt praktisch um.
Wofür braucht man es? Die Kompetenzen werden benötigt, um digitale Systeme, Software, Datenrepräsentationen und algorithmische Abläufe in späteren forensischen Modulen fundiert verstehen und analysieren zu können. Sie bilden eine Grundlage für Aufgaben wie Datenanalyse, Werkzeugentwicklung, Betriebssystemverständnis und die strukturierte Untersuchung digitaler Spuren.
Wieso ist es interessant? Das Modul zeigt, was hinter digitalen Systemen grundsätzlich passiert: Wie aus Bits Informationen werden, wie Programme ausgeführt werden und wie sich Probleme so strukturieren lassen, dass Computer sie bearbeiten können. Wer digitale Forensik betreiben will, bekommt hier das informatische Fundament, um technische Spuren nicht nur zu finden, sondern auch zu verstehen.

BDF103: Programmierung

Modulverantwortung	Prof. Dr. Duc Duy Pham	**Lehrperson(en)**	Prof. Dr. Duc Duy Pham Prof. Dr. Gudrun Stockmanns
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Programming
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können grundlegende Programmierkonzepte anwenden, einfache Programme strukturiert entwickeln und Programmcode hinsichtlich Funktion, Qualität und Wiederverwendbarkeit beurteilen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Einfache Informatik-Probleme zu modellieren und Algorithmen zu deren Lösung zu entwickeln
- Die grundlegenden Sprachkonzepte wie primitive Datentypen und Kontrollstrukturen einer Programmiersprache (wie z.B. Python) zu beherrschen und sinnvoll einzusetzen
- Die Anwendbarkeit der grundlegenden Konzepte der objektorientierten Programmierung wie Klassen, Objekte, Vererbung, abstrakte Klassen und Schnittstellen, sowie die Fehlerbehandlung über Exceptions, für einfache und/oder begrenzt-umfangreiche Problemstellungen zu erkennen und diese auch in einer gängigen objektorientierten Programmiersprache zu implementieren
- Für einfache algorithmische und datenstrukturorientierte Aufgabenstellungen Programme in exemplarischer Programmiersprache und Programmierparadigma unter Anwendung angemessener Techniken zu entwickeln
- Aktuelle softwaretechnische Werkzeuge zielführend einzusetzen
- Für kleinere Programme einen Softwaretest mit seinen Anforderungen zu konzipieren
- Sich in vorhandene Programme einzuarbeiten und vorhandene Programmelemente oder Bibliotheken zu nutzen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Algorithmen und Modellierung einfacher Informatik-Probleme
- Entwicklungswerkzeuge, Standardbibliotheken und Einführung in Python
- Grundlagen der strukturierten Programmierung: Ablaufstrukturen, Datentypen, Funktionen und einfache Datenstrukturen
- Elementare Ein- und Ausgabe, Dateisystem, Speicherverwaltung und rekursive Funktionen
- Anwendung des Erlernten auf einfache Problemstellungen und kleine Programmfragmente
- Grundlagen der Softwareentwicklung, systematische Erstellung von Softwaresystemen und Phasen der Softwareentwicklung
- Softwareanalyse, Tests und Qualitätssicherung kleiner Programme
- Nutzung von Bibliotheken und Vergleich unterschiedlicher Programmierparadigmen

Prüfungsvorleistung

Testat

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- John Hunt: A Beginners Guide to Python 3 Programming, Springer, Cham, 2019, https://doi.org/10.1007/978-3-030-20290-3
- Allen B. Downey: Think Python: How to Think Like a Computer Scientist, O'Reilly Media, Sebastopol, 2015
- Mark Lutz: Learning Python, O'Reilly Media, Sebastopol, 2013
- Ian Sommerville: Software Engineering, Pearson, Harlow, 2016
- Bernd Oestereich und Axel Scheithauer: Analyse und Design mit UML 2.5, De Gruyter Oldenbourg, Berlin, 2013

Kurzporträt BDF103: Programmierung

Worum geht es? Dieses Modul behandelt Programmierung im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Algorithmen; Entwicklungswerkzeuge und Standardbibliotheken; Einführung in die Programmiersprache Python.
Wofür braucht man es? Programmierkompetenz ermöglicht es, forensische Auswertungen zu automatisieren, Datenquellen gezielt zu verarbeiten und eigene Analysewerkzeuge nachvollziehbar zu entwickeln.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF202: Einführung in Open Source Intelligence (OSINT)

Modulverantwortung	Prof. Dr. Thorsten Weber	**Lehrperson(en)**	Prof. Dr. Thorsten Weber Prof. Dr. Nils Kopal
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Introduction to Open Source Intelligence (OSINT)
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können öffentlich verfügbare Quellen systematisch recherchieren, bewerten und für forensische bzw. sicherheitsbezogene Fragestellungen auswerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die gesellschaftlichen und rechtlichen Rahmenbedingungen für einen OSINT-Einsatz zur Sammlung und Analyse von (sicherheits-)relevanten Information aus offenen, frei verfügbaren Quellen kritisch zu reflektieren
- ermittelte Daten hinsichtlich ihrer technischen und juristischen Verwertbarkeit zu beurteilen
- den Informationsgehalt der ermittelten Daten einzuschätzen
- OSINT Terminologien, Methoden, Techniken und Werkzeuge zu beschreiben
- die Methoden, Techniken und Werkzeuge bei zielgerichteten (anonymisierten) Recherchen anzuwenden

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Zielgerichtete Recherche
- (Online-)Quellen (Social Media, …)
- Quellen-Auswahl
- Anonymisierte Recherche
- Auswertemethoden
- Faktencheck
- Werkzeuge

Prüfungsvorleistung

Testat

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Nihad A. Hassan und Rami Hijazi: Open Source Intelligence Methods and Tools, Apress, Berkeley, 2018, https://doi.org/10.1007/978-1-4842-3213-2
- Michael Bazzell: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, IntelTechniques.com, 2023
- Rae L. Baker: Deep Dive: Exploring the Real-world Value of Open Source Intelligence, CRC Press, Boca Raton, 2023
- Babak Akhgar, P. Saskia Bayerl und Fraser Sampson: Open Source Intelligence Investigation: From Strategy to Implementation, Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-47671-1

Kurzporträt BDF202: Einführung in Open Source Intelligence (OSINT)

Worum geht es? Dieses Modul behandelt Einführung in Open Source Intelligence (OSINT) im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Zielgerichtete Recherche; (Online-)Quellen (Social Media, …); Quellen-Auswahl.
Wofür braucht man es? OSINT-Kompetenzen helfen, öffentlich zugängliche Informationen strukturiert zu recherchieren, ihre Aussagekraft einzuschätzen und sie rechtlich wie technisch verwertbar aufzubereiten.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF306: Security Incident Management

Modulverantwortung	Prof. Dr. Matthias Mehrtens	**Lehrperson(en)**	Prof. Dr. Matthias Mehrtens
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Security Incident Management
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Sicherheitsvorfälle strukturieren, Incident-Response-Prozesse anwenden und Maßnahmen zur Bewältigung und Nachbereitung von IT-Sicherheitsvorfällen planen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die Bedeutung des Incident Managements im Hinblick auf die Informationssicherheit zu erläutern und Methoden zur Reaktion kennen, so dass Schäden minimiert, die Verfügbarkeit der Systeme und die Integrität der Daten erhalten bleiben
- Maßnahmen zur Erkennung, Reaktion und Vorbeugung von Bedrohungen der IT-Sicherheit zu planen, zu dokumentieren und umzusetzen (Incident-Response-Plan) um zeitnah auf Bedrohungen und Angriffe reagieren zu können
- Sicherheitsrisiken zu bewerten und unter Berücksichtigung von Schwere und Auftrittswahrscheinlichkeiten zu priorisieren
- Bedrohungen zu identifizieren, indem beispielsweise Anomalien und Abweichungen in Datenverkehrsmustern oder im Systemverhalten erkannt werden
- Methoden und Werkzeuge wie Netzwerk-Scanner, Log-Analyse-Tools, Vulnerability-Scanner oder SIEMs zur Erfassung und Verarbeitung von Incidents, die in der Praxis für den Incident Management Prozess eingesetzt werden, zu bewerten und einzusetzen
- Regulatorische und gesetzliche Vorgaben im Zusammenhang mit Sicherheitsvorfällen und Incident-Response-Plänen berücksichtigen können, um sicherzustellen, dass alle Maßnahmen den gesetzlichen Vorgaben entsprechen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagen Security Incident Management (Strategien, Prozesse, Help Desk, Reporting, first level, second level, Krisensitzung, war room, …)
- Erstellung von Incident-Response-Plänen, Festlegung von Rollen und Verantwortlichkeiten, Identifizierung von Bedrohungen, Bewertung von Risiken und Entwicklung von Eskalationsprozessen
- Incident-Response-Tools, Systeme zur Netzwerküberwachung, Ticketsysteme, Sicherheitsinformations- und Event-Management-Systeme (SIEMs)
- Compliance und rechtliche Aspekte, (DSGVO, ISO 27035, ITIL, Informationspflichten)
- Dokumentation von Incident-Response-Aktivitäten und Erstellung von Berichten

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Paul Cichonski, Tom Millar, Tim Grance und Karen Scarfone: Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2, Gaithersburg, 2012, https://doi.org/10.6028/NIST.SP.800-61r2
- ENISA: Good Practice Guide for Incident Management, European Union Agency for Cybersecurity, Heraklion, 2010, https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
- ISO/IEC: ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process, ISO, Geneva, 2023
- Jason T. Luttgens, Matthew Pepe und Kevin Mandia: Incident Response and Computer Forensics, McGraw-Hill Education, New York, 2014

Kurzporträt BDF306: Security Incident Management

Worum geht es? Dieses Modul behandelt Security Incident Management im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlagen Security Incident Management (Strategien, Prozesse, Help Desk, Reporting, first level, second level, Krisensitzung, war room, …); Erstellung von Incident-Response-Plänen, Festlegung von Rollen und Verantwortlichkeiten, Identifizierung von Bedrohungen, Bewertung von Risiken und Entwicklung von Eskalationsprozessen; Incident-Response-Tools, Systeme zur Netzwerküberwachung, Ticketsysteme, Sicherheitsinformations- und Event-Management-Systeme (SIEMs).
Wofür braucht man es? Incident-Management-Kompetenzen werden benötigt, um Sicherheitsvorfälle einzuordnen, Reaktionsprozesse zu koordinieren und technische Erkenntnisse in belastbare Maßnahmen zu überführen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Lernpfad IT-Sicherheit

Der Modulbereich IT-Sicherheit befähigt die Studierenden, technische, ethische und kryptografische Grundlagen sicherer Informationsverarbeitung zu verstehen und auf web-, browser- und sicherheitsbezogene Fragestellungen anzuwenden. Dabei verbinden sie Schutzmaßnahmen, Angriffsmodelle, rechtliche und ethische Reflexion sowie praktische Sicherheitsanalysen.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können Sicherheitsrisiken digitaler Systeme erkennen, zentrale Schutzmechanismen erklären, ethische Fragestellungen der Informationssicherheit einordnen und ausgewählte Sicherheitsmechanismen in Web-, Browser- und Kryptografie-Kontexten anwenden und bewerten.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Modulbereich
  - ethische und menschliche Aspekte der Informationssicherheit analysieren und diskutieren,
  - grundlegende Bedrohungen, Schutzziele und Sicherheitsmaßnahmen der IT-Sicherheit erarbeiten,
  - Web- und Browsermechanismen hinsichtlich typischer Angriffe und Schutzkonzepte untersuchen,
  - kryptografische Verfahren anwendungsbezogen einsetzen und ihre Grenzen reflektieren,
  - technische und nichttechnische Sicherheitsentscheidungen nachvollziehbar begründen.
- **WOZU**: Damit sie forensische Analysen und sicherheitsbezogene Entscheidungen nicht nur technisch, sondern auch ethisch, rechtlich und organisatorisch angemessen einordnen können. Der Modulbereich liefert Grundlagen für Incident Response, Netzwerkforensik, Malware-Analyse, Kryptografieanwendungen und den Umgang mit sensiblen digitalen Spuren.

Kurzporträt Lernpfad IT-Sicherheit

Worum geht es? Der Modulbereich IT-Sicherheit behandelt, wie digitale Systeme geschützt, angegriffen und verantwortungsvoll betrieben werden. Dazu gehören ethische Fragen, Sicherheitsgrundlagen, Web- und Browsersicherheit sowie angewandte Kryptografie.
Wofür braucht man es? Die Kompetenzen werden benötigt, um Risiken einzuschätzen, Schutzmaßnahmen zu verstehen und forensische Befunde im Kontext realer Sicherheitsvorfälle zu bewerten. Sie helfen dabei, technische Analyse mit verantwortlichem Handeln zu verbinden.
Wieso ist es interessant? IT-Sicherheit ist die andere Seite digitaler Forensik: Wer Angriffe rekonstruieren will, muss auch verstehen, welche Schutzmechanismen existieren, wie sie versagen können und welche ethischen Fragen daraus entstehen.

BDF102: Ethische und Menschliche Aspekte der Informationssicherheit

Modulverantwortung	Prof. Dr. Jürgen Quade	**Lehrperson(en)**	Prof. Dr. Jürgen Quade
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | - Ü | - P | 2 SL	**Engl. Titel**	Ethical and Human Aspects of Information Security
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können zentrale Konzepte und Methoden des Moduls Ethische und Menschliche Aspekte der Informationssicherheit fachlich einordnen, anwenden und auf Aufgaben der Digitalen Forensik übertragen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- verschiedene ethische Theorien, deren Vor- und Nachteile und Kritikpunkte zu beschreiben (Utilitarismus, Deontologie (Kant), Verantwortungsethik (Jonas))
- ethische Fragen zu identifizieren und zu formulieren
- ethische Probleme zu analysieren und zu bewerten
- durch Abwägung der Optionen und Berücksichtigung der Auswirkungen auf verschiedene Interessengruppen ethische Entscheidungen zu treffen
- ethische Entscheidungen begründet zu kommunizieren
- gesellschaftliche Problemfelder der Informationssicherheit zu benennen und im Lichte unterschiedlicher Interessen zu diskutieren
- Risiken automatisierter Entscheidungen zu erkennen
- eigenverantwortlich zu handeln

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einführung in die Ethik
- Ethiktheorien (Kant, Utilitarismus, Rawls ”Theory of Justice”)
- Bedeutung von Information im ”Informationszeitalter”, Umgang mit sensiblen Daten
- Systemtheorie: Funktion von Ethik zur Verschleierung von Interessen
- automatisierte Entscheidungen: Objektivität und systematische Benachteiligung
- Persönlichkeitsrechte und Privatsphäre
- gesellschaftliche und psychologische Aspekte der Informationssicherheit
- ethische Dilemmata, moralische Entscheidungen und Fragen in der Zusammenarbeit mit Strafverfolgungsbehörden oder Unternehmen

Prüfungsvorleistung

Keine

Prüfungsleistung

Mündliche Prüfung (30 - 45 Minuten)

Literatur

- Michael J. Quinn: Ethics for the Information Age, Pearson, Boston, 2020
- Herman T. Tavani: Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, Wiley, Hoboken, 2016
- Richard A. Spinello: Cyberethics: Morality and Law in Cyberspace, Jones & Bartlett Learning, Burlington, 2020
- Sarah Spiekermann: Ethical IT Innovation: A Value-based System Design Approach, CRC Press, Boca Raton, 2015

Kurzporträt BDF102: Ethische und Menschliche Aspekte der Informationssicherheit

Worum geht es? Dieses Modul behandelt Ethische und Menschliche Aspekte der Informationssicherheit im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einführung in die Ethik; Ethiktheorien (Kant, Utilitarismus, Rawls ”Theory of Justice”); Bedeutung von Information im ”Informationszeitalter”, Umgang mit sensiblen Daten.
Wofür braucht man es? Ethische Reflexion ist notwendig, um technische Möglichkeiten verantwortungsvoll einzusetzen und Sicherheitsentscheidungen gegenüber Betroffenen, Organisationen und Ermittlungsstellen begründen zu können.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF205: IT-Sicherheit

Modulverantwortung	Prof. Dr. Martin Grothe	**Lehrperson(en)**	Prof. Dr. Martin Grothe
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	IT Security
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF101: Informatik-Grundlagen der Forensik: Rechnerarchitektur, Datenrepräsentation und informatische Grundbegriffe für Sicherheitsmechanismen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können grundlegende Konzepte, Bedrohungen und Schutzmaßnahmen der IT-Sicherheit erklären und einfache Sicherheitsmaßnahmen praktisch umsetzen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die Gefährdung in einem IT-System (Rechner, Netzwerk) zu analysieren (Risikoanalyse),
- Maßnahmen im Bereich Informations-Sicherheit kritisch zu reflektieren,
- sichere Netzstrukturen aus Hard- und Software im Hinblick auf IT-Sicherheit zu entwerfen,
- IT-Systeme mit Hilfe von Firewallregeln und VPN-Technik abzusichern,
- Software unter Berücksichtigung von IT-Sicherheit zu entwerfen und zu realisieren,
- geeignete Maßnahmen im Fall eines Angriffes zu ergreifen und
- Privatsphäre sicher zu stellen
- Dedizierte Sicherheitstechnologien wie beispielsweise Verschlüsselung und Authentifizierungsverfahren einzusetzen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Praxisorientierte Einführung in die Rechner- und Netzwerksicherheit
- Einführung in Schutzziele, Gefährdungen und rechtliche Rahmenbedingungen
- Grundlagen der Kryptografie, symmetrische und asymmetrische Verschlüsselung
- Authentifizierung, digitale Signaturen und Public-Key-Infrastrukturen (PKI)
- Angriffsarten
- Elemente der Systemsicherheit (Rechtemanagement und Zugriffskontrolle, Virenschutz, Firewall, IDS/IPS)
- Sicherheits-Architekturen basierend auf Netzhierarchien und VPN
- Sicherung der Privatsphäre und Sicherheit in Betriebssystemen

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- William Stallings und Lawrie Brown: Computer Security: Principles and Practice, Pearson, Harlow, 2023
- Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, Indianapolis, 2020
- Matt Bishop: Computer Security: Art and Science, Addison-Wesley, Boston, 2019
- Claudia Eckert: IT-Sicherheit: Konzepte, Verfahren, Protokolle, De Gruyter Oldenbourg, Berlin, 2018, https://doi.org/10.1515/9783110563900

Kurzporträt BDF205: IT-Sicherheit

Worum geht es? Dieses Modul behandelt IT-Sicherheit im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Praxisorientierte Einführung in die Rechner- und Netzwerksicherheit; Einführung in Schutzziele, Gefährdungen und rechtliche Rahmenbedingungen; Grundlagen der Kryptografie.
Wofür braucht man es? Grundlegende IT-Sicherheitskompetenz ist Voraussetzung, um Angriffe, Schutzmaßnahmen und Systemrisiken zu verstehen und forensische Befunde in ihren Sicherheitskontext einzuordnen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF304: Web- und Browsersicherheit

Modulverantwortung	Prof. Dr. Marcus Niemietz	**Lehrperson(en)**	Prof. Dr. Marcus Niemietz
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Web and Browser Security
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF103: Programmierung: grundlegende Programmierkonzepte, Softwareanalyse und Tests als Grundlage für Web- und Browser-Sicherheitsanalysen.
- BDF205: IT-Sicherheit: Schutzziele, Angriffsarten, Schutzmaßnahmen und Grundlagen sicherer System- und Netzarchitekturen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können zentrale Angriffs- und Schutzmechanismen im Web- und Browserkontext erklären, praktisch untersuchen und sicherheitsbezogen bewerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die technischen Aspekte von Web- und Browsersicherheit zu verstehen
- ein Systemverständnis über komplexe Webanwendungen zu verfügen
- zu verstehen wie angreifende Parteien Webapplikationen und Webbrowser untersuchen
- Probleme im Bereich der Web- und Browsersicherheit zu analysieren
- Sicherheitsuntersuchungen zu verstehen und durchzuführen
- Risiken (u. a. OWASP TOP-10) zu identifizieren und diese zu bewerten
- Forensische Analysen nach und während Webangriffen durchzuführen
- Maßnahmen zum Schutz gegen Cyberangriffe auf Webapplikationen zu implementieren und den Nutzen der erarbeiteten Lösungen argumentativ zu begründen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Browserbasierte Sicherheitskonzepte (bspw. Same-Origin-Policy)
- Front-End- sowie Back-End-Sicherheit von Webanwendungen
- Best-Practices zur Härtung von Webanwendungen

Prüfungsvorleistung

Testat

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Dafydd Stuttard und Marcus Pinto: The Web Application Hacker's Handbook, Wiley, Indianapolis, 2011
- OWASP Foundation: Web Security Testing Guide, OWASP, 2024, https://owasp.org/www-project-web-security-testing-guide/
- PortSwigger: Web Security Academy, PortSwigger, 2024, https://portswigger.net/web-security
- Michal Zalewski: The Tangled Web: A Guide to Securing Modern Web Applications, No Starch Press, San Francisco, 2011

Kurzporträt BDF304: Web- und Browsersicherheit

Worum geht es? Dieses Modul behandelt Web- und Browsersicherheit im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Browserbasierte Sicherheitskonzepte (bspw. Same-Origin-Policy); Front-End- sowie Back-End-Sicherheit von Webanwendungen; Best-Practices zur Härtung von Webanwendungen.
Wofür braucht man es? Web- und Browsersicherheit ist relevant, um typische Angriffspfade in Webanwendungen zu erkennen, Spuren solcher Angriffe auszuwerten und Schutzmaßnahmen fachlich zu beurteilen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF404: Angewandte Kryptografie

Modulverantwortung	Prof. Dr. Nils Kopal	**Lehrperson(en)**	Prof. Dr. Nils Kopal
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Applied Cryptography
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF101: Informatik-Grundlagen der Forensik: Zahlensysteme, Bitoperationen, Datenrepräsentation und algorithmische Grundlagen.
- BDF103: Programmierung: grundlegende Programmierkonzepte zur praktischen Umsetzung kryptografischer Verfahren.
- BDF104: Einführung in die Digitale Forensik: forensische Fragestellungen und rechtlich-ethischer Kontext digitaler Beweise.
- BDF205: IT-Sicherheit: Kryptografiegrundlagen, Authentifizierung, digitale Signaturen und Sicherheitsziele.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können kryptografische Verfahren anwendungsbezogen erklären, einsetzen und hinsichtlich ihrer forensischen und sicherheitstechnischen Bedeutung bewerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- verschiedene Verschlüsselungsverfahren zu identifizieren
- bekannte Schwächen zur Entschlüsselung zu nutzen
- die Kryptoanalyseverfahren zur Entschlüsselung von bekannten Verfahren zu abstrahieren und auf neue Verfahren anzuwenden
- ausgewählte mathematischen Grundlagen moderner Kryptografie auf einfachen Beispielen anzuwenden
- die Funktionsweise moderner Verschlüsselung mittels DES / AES zu erläutern und die Algorithmen von historischen Verfahren hinsichtlich ihrer Sicherheit abgrenzen
- neben den technischen Grundlagen der modernen Kryptografie die sozialen und gesellschaftlichen Fragestellungen, die aus dem Einsatz von Verschlüsselungsverfahren resultieren, zu kennen
- auf affektiver Ebene sich eine eigene Meinung zu diesen Fragestellungen zu bilden und diese zu begründen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Geschichtliche Entwicklung der Kryptografie
- Mathematische Grundlagen der Kryptografie
- Signaturen, Ende-zu-Ende-Verschlüsselung in der Kommunikation
- Blockchains, Distributed Ledgers und Kryptowährungen
- Nachweis perfekter Sicherheit und Postquanten-Kryptografie
- Methoden zum Brechen von Kryptografie (Krypto-Analyse, Häufigkeitsanalyse, Brute-Force)
- Einführung in Werkzeuge (z.B. John the Ripper, Hashcat, Medusa, Aircrack)
- Ethische und rechtliche Aspekte (Privatsphäre versus Sicherheitsinteressen)

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Christof Paar und Jan Pelzl: Understanding Cryptography, Springer, Berlin, 2010, https://doi.org/10.1007/978-3-642-04101-3
- Jonathan Katz und Yehuda Lindell: Introduction to Modern Cryptography, CRC Press, Boca Raton, 2021
- Niels Ferguson, Bruce Schneier und Tadayoshi Kohno: Cryptography Engineering, Wiley, Indianapolis, 2010
- Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996, https://-cacr.uwaterloo.ca/hac/

Kurzporträt BDF404: Angewandte Kryptografie

Worum geht es? Dieses Modul behandelt Angewandte Kryptografie im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Geschichtliche Entwicklung der Kryptografie; Mathematische Grundlagen der Kryptografie; Signaturen, Ende-zu-Ende-Verschlüsselung in der Kommunikation.
Wofür braucht man es? Kryptografisches Verständnis hilft, Verschlüsselung, Signaturen und Schlüsselmaterial in Sicherheits- und Forensikfällen korrekt einzuordnen und Grenzen technischer Schutzverfahren zu erkennen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Lernpfad Betriebssysteme

Der Lernpfad Betriebssysteme befähigt die Studierenden, Betriebssysteme von der Anwendung über technische Grundlagen bis zur forensischen Untersuchung systematisch zu verstehen. Dabei entwickeln sie Kompetenzen im Umgang mit Betriebssystemdiensten, Systemarchitekturen, Artefakten, Protokollen und Analysewerkzeugen.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können Betriebssysteme bedienen, zentrale technische Konzepte erklären und betriebssystembezogene Spuren forensisch erfassen, analysieren, interpretieren und dokumentieren.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Lernpfad
  - Betriebssysteme aus Anwendersicht nutzen und administrative Grundaufgaben durchführen,
  - Prozesse, Speicher, Dateisysteme, Benutzer- und Rechtemodelle sowie Systemdienste untersuchen,
  - technische Betriebssystemmechanismen hinsichtlich Funktion und Sicherheitsrelevanz analysieren,
  - forensisch relevante Artefakte in Betriebssystemen identifizieren und sichern,
  - geeignete Werkzeuge zur Betriebssystemforensik einsetzen und Ergebnisse nachvollziehbar dokumentieren.
- **WOZU**: Damit sie digitale Spuren auf Endgeräten und Servern fachgerecht verstehen und auswerten können. Der Lernpfad bildet eine wichtige Grundlage für Malware-Analyse, Speichermedienforensik, Embedded-Systems-Forensik und die Entwicklung forensischer Werkzeuge.

Kurzporträt Lernpfad Betriebssysteme

Worum geht es? Der Lernpfad Betriebssysteme zeigt, wie Betriebssysteme genutzt, technisch verstanden und forensisch untersucht werden. Die Studierenden arbeiten sich von der Anwendung über interne Mechanismen bis zur Analyse konkreter Systemspuren vor.
Wofür braucht man es? Betriebssysteme sind zentrale Quellen digitaler Spuren. Wer Benutzerhandlungen, Prozesse, Dateien, Protokolle oder Systemzustände rekonstruieren will, benötigt ein fundiertes Verständnis ihrer technischen Grundlagen.
Wieso ist es interessant? Betriebssysteme verbinden sichtbare Nutzung mit vielen unsichtbaren technischen Abläufen. Der Lernpfad macht nachvollziehbar, wie aus diesen Abläufen forensisch verwertbare Hinweise entstehen.

BDF201: Betriebssysteme: Anwendung

Modulverantwortung	Prof. Dr. Peter Davids	**Lehrperson(en)**	Prof. Dr. Peter Davids
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Operating Systems: Application
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF101: Informatik-Grundlagen der Forensik: Rechnerarchitektur, Datenrepräsentation und informatische Grundbegriffe.
- BDF103: Programmierung: grundlegende Programmier- und Scripting-Konzepte zur Automatisierung administrativer Aufgaben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Betriebssysteme aus Anwendersicht bedienen, zentrale Dienste nutzen und einfache administrative Aufgaben sicher durchführen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Fachbegriffe im Bereich der Betriebssysteme zu verstehen, um sie aktiv anzuwenden
- Architektur- und Systemkonzepte sowie Verfahren und Funktionen unterschiedlicher Betriebssysteme zu beschreiben
- Betriebssysteme hinsichtlich ihres Leistungsvermögens und ihrer Einsetzbarkeit in verschiedenen Umgebungen zu vergleichen
- Betriebssysteme zu administrieren, insbesondere in Bezug auf IT-Sicherheit
- Aufgaben über Kommandozeile durchzuführen und per Scripting zu automatisieren
- Aufwände und Wirkungen administrativer Maßnahmen und sich daraus ergebende Notwendigkeiten einzuschätzen
- Sicherheitsprobleme von Betriebssystemen und darauf abzielende Angriffe zu beschreiben
- Sicherheitstechnische Schwächen aufzudecken, zu beheben und Schutzmechanismen moderner Betriebssysteme entsprechend einer Security-Policy zu konfigurieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundbegriffe und Grundprinzipien von Betriebssystemen werden im Kontext der Cyber Sicherheit erläutert
- die Funktionsweise von Betriebssystemen werden eingeübt
- die Nutzung und Administration von Betriebssystemen aus Usersicht wird in der Praxis angewandt

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Andrew S. Tanenbaum und Herbert Bos: Moderne Betriebssysteme, Pearson, Hallbergmoos, 2016
- Abraham Silberschatz, Peter B. Galvin und Greg Gagne: Operating System Concepts, Wiley, Hoboken, 2018
- Brian Ward: How Linux Works: What Every Superuser Should Know, No Starch Press, San Francisco, 2021
- Æleen Frisch: Essential System Administration, O'Reilly Media, Sebastopol, 2002

Kurzporträt BDF201: Betriebssysteme: Anwendung

Worum geht es? Dieses Modul behandelt Betriebssysteme: Anwendung im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundbegriffe und Grundprinzipien von Betriebssystemen werden im Kontext der Cyber Sicherheit erläutert; die Funktionsweise von Betriebssystemen werden eingeübt; die Nutzung und Administration von Betriebssystemen aus Usersicht wird in der Praxis angewandt.
Wofür braucht man es? Sichere Betriebssystemnutzung bildet die Grundlage, um spätere Analysen auf Endgeräten und Servern nachvollziehbar vorzubereiten und administrative Eingriffe fachgerecht zu bewerten.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF301: Betriebssysteme: Technik

Modulverantwortung	Prof. Dr. Thorsten Weber	**Lehrperson(en)**	Prof. Dr. Jörg Helbach Prof. Dr. Thorsten Weber
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	V | - Ü | - P | 4 SL	**Engl. Titel**	Operating Systems: Technology
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF201: Betriebssysteme: Anwendung: Bedienung, Administration, Kommandozeile, Scripting und grundlegende Betriebssystemkonzepte.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können technische Grundlagen von Betriebssystemen erklären und Betriebssystemmechanismen hinsichtlich Aufbau, Funktion und sicherheitsrelevanter Eigenschaften analysieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- den Aufbau von und die Abläufe in gängigen Betriebssystemen zu analysieren
- Manipulationen in Betriebssystemen, z.B. durch Malware/Spionagesoftware zu erkennen und zu beheben
- Betriebssystemarchitekturen zu unterscheiden, zu analysieren,
- Datenträger und In-Memory-Verschlüsselung zu verstehen und wenn möglich aufzubrechen
- die technischen Grundlagen zur gerichtsverwertbaren Sicherung von Spuren in Betriebssystemen zu beherrschen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Dateisysteme (FAT,FAT32,NTFS, HFS, APFS, EXT4, ZFS, NFS, et.al.)
- Datenträgerverschlüsselung
- Backup- und Recovery Mechanismen
- Authentifizierungs- und Autorisierungsmechanismen
- Audit-Subsysteme und Sicherheits-Mechanismen / Secure Boot
- Prozessmanagement, IO-Management und Memory-Management
- Interprozess-Kommunikation und Netzwerk-Kommunikation

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Andrew S. Tanenbaum und Herbert Bos: Modern Operating Systems, Pearson, Harlow, 2023
- Abraham Silberschatz, Peter B. Galvin und Greg Gagne: Operating System Concepts, Wiley, Hoboken, 2018
- Robert Love: Linux Kernel Development, Addison-Wesley, Boston, 2010
- Maurice J. Bach: The Design of the UNIX Operating System, Prentice Hall, Englewood Cliffs, 1986

Kurzporträt BDF301: Betriebssysteme: Technik

Worum geht es? Dieses Modul behandelt Betriebssysteme: Technik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Dateisysteme (FAT,FAT32,NTFS, HFS, APFS, EXT4, ZFS, NFS, et.al.); Datenträgerverschlüsselung; Backup- und Recovery Mechanismen.
Wofür braucht man es? Technisches Betriebssystemwissen ist zentral, um Prozesse, Speicher, Dateisysteme und Schutzmechanismen als Quellen digitaler Spuren verstehen und analysieren zu können.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF401: Betriebssysteme: Forensik

Modulverantwortung	Prof. Dr. Martin Grothe	**Lehrperson(en)**	Dr. Markus Schneider
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Operating Systems: Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF104: Einführung in die Digitale Forensik: forensischer Prozess, Beweissicherung und Dokumentation.
- BDF204: Forensische Methoden und Werkzeuge: Akquise, Auswertung und Interpretation von Datenträger-, Arbeitsspeicher- und Netzwerkdaten.
- BDF205: IT-Sicherheit: Schutzmechanismen, Angriffsarten und Systemsicherheit.
- BDF301: Betriebssysteme: Technik: Dateisysteme, Prozesse, Speicher, Rechte, Logging und Betriebssystemarchitekturen.
- BDF302: Rechnernetze und Rechnernetzsicherheit: TCP/IP, Netzwerkdienste und Grundlagen der Netzwerksicherheit.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Betriebssysteme mit forensischen Methoden untersuchen, relevante Artefakte identifizieren und Analyseergebnisse nachvollziehbar bewerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- selbständig mittels IT-forensischer Methoden digitale Spuren aus gängigen Betriebssystemen (Linux, Windows, MacOS, iOS, Android) unter Einbeziehung von Hintergrundspeicher, Arbeitsspeicher und Netzwerk auf rechtssichere Weise zu extrahieren
- digitale Beweise, beispielsweise durch Wiederherstellung von vermeintlich gelöschten Dateien (File Carving) oder durch Auswertung von Metadaten (MAC-Spur), rechtssicher zu gewinnen
- notwendige forensische Werkzeuge wie FTK Imager, EnCase oder Sleuth Kit effektiv zu nutzen
- aus einem Betriebssystem extrahierte, digitale Beweise zu analysieren, zu bewerten und zu dokumentieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagen der Betriebssystemforensik (Analysemethoden, Klassifizierung digitaler Spuren, Kernel, Userland, Dateiverwaltung, Logging)
- Rechtssichere Datenextraktion und Datensicherung in gängigen Betriebssystemen (Windows, Linux, MacOS, iOS, Android)
- Wiederherstellung von Daten, beispielsweise gelöschter, beschädigter oder verschlüsselter Dateien (Artefakte)
- Analyse von Logdateien und sonstigen Systeminformationen, um Informationen über die Aktivitäten des Systems und der Benutzer zu erhalten
- Anti-Forensik-Techniken, die Aktivitätsspuren verwischen
- Werkzeuge der digitalen Forensik
- Implementierungstechnische Auswirkungen auf forensische Auswertungen

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Bruce Nikkel: Practical Linux Forensics: A Guide for Digital Investigators, No Starch Press, San Francisco, 2021
- Harlan Carvey: Windows Forensic Analysis Toolkit, Syngress, Waltham, 2018
- Brian Carrier: File System Forensic Analysis, Addison-Wesley, Boston, 2005
- Cory Altheide und Harlan Carvey: Digital Forensics with Open Source Tools, Syngress, Waltham, 2011

Kurzporträt BDF401: Betriebssysteme: Forensik

Worum geht es? Dieses Modul behandelt Betriebssysteme: Forensik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlagen der Betriebssystemforensik (Analysemethoden, Klassifizierung digitaler Spuren, Kernel, Userland, Dateiverwaltung, Logging); Rechtssichere Datenextraktion und Datensicherung in gängigen Betriebssystemen (Windows, Linux, MacOS, iOS, Android); Wiederherstellung von Daten, beispielsweise gelöschter, beschädigter oder verschlüsselter Dateien (Artefakte).
Wofür braucht man es? Betriebssystemforensik wird benötigt, um Artefakte aus Windows-, Linux-, macOS- und mobilen Systemen zu sichern, auszuwerten und gerichtsfest zu dokumentieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Lernpfad Netzwerke

Der Lernpfad Netzwerke befähigt die Studierenden, Rechnernetze technisch zu verstehen, sicherheitsrelevante Kommunikationsprozesse zu beurteilen und Netzwerkdaten forensisch auszuwerten. Dabei entwickeln sie Kompetenzen im Analysieren von Protokollen, Angriffsszenarien, Netzwerksicherheitsmechanismen und Netzwerkspuren.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können Aufbau und Funktion von Rechnernetzen erklären, Netzwerksicherheitsmechanismen einordnen und Netzwerkkommunikation forensisch erfassen, analysieren, interpretieren und dokumentieren.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Lernpfad
  - Netzwerkarchitekturen, Protokolle und Kommunikationsmodelle erarbeiten,
  - typische Netzwerkdienste, Routing, Adressierung und Paketverarbeitung analysieren,
  - Bedrohungen und Schutzmaßnahmen in Rechnernetzen untersuchen,
  - Netzwerkverkehr mitschneiden, filtern und mit geeigneten Werkzeugen auswerten,
  - sicherheitsrelevante Kommunikationsmuster erkennen und forensische Ergebnisse nachvollziehbar darstellen.
- **WOZU**: Damit sie Angriffe, Datenabflüsse, Kommunikationsbeziehungen und technische Abläufe in vernetzten Systemen rekonstruieren können. Der Lernpfad unterstützt insbesondere Netzwerkforensik, Incident Response, IoT-Security und Untersuchungen verteilter digitaler Infrastrukturen.

Kurzporträt Lernpfad Netzwerke

Worum geht es? Der Lernpfad Netzwerke behandelt, wie digitale Systeme miteinander kommunizieren und wie diese Kommunikation abgesichert, beobachtet und forensisch ausgewertet werden kann. Die Studierenden verbinden Netzwerktechnik mit praktischer Analyse von Netzwerkdaten.

Wofür braucht man es? Viele digitale Spuren entstehen in der Kommunikation zwischen Systemen. Die Kompetenzen helfen, verdächtigen Netzwerkverkehr, Angriffswege und Kommunikationsbeziehungen technisch fundiert zu verstehen.

Wieso ist es interessant? Netzwerke machen digitale Handlungen sichtbar, oft in Form einzelner Pakete, Protokolle und Verbindungen. Der Lernpfad zeigt, wie daraus ein nachvollziehbares Bild eines Sicherheits- oder Forensikfalls entsteht.

BDF302: Rechnernetze und Rechnernetzsicherheit

Modulverantwortung	Prof. Dr. Martin Grothe	**Lehrperson(en)**	Prof. Dr. Martin Grothe
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Computer Networks and Network Security
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Rechnernetze und grundlegende Netzwerksicherheitsmechanismen erklären, konfigurieren und hinsichtlich typischer Risiken beurteilen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Kernelemente von Rechnernetzen mit korrekten Fachtermini zu erklären
- Struktur, Komponenten, Protokolle und Funktion des Internets zu erklären
- grundlegende Anforderungen an Netzwerkstrukturen zu bestimmen
- kleinere Unternehmens-LANs zu konzipieren
- typische Fehlersituationen in Netzwerken zu untersuchen
- die vielfältigen Sicherheitsprobleme sowie Techniken und Verfahren zur Sicherung von Unternehmensnetzen zu demonstrieren
- die Administration im Betrieb von Rechnernetzen durchzuführen
- moderne Trends in Rechnernetzen darzustellen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einsatz von und Anforderungen an Datennetze
- Netzkomponenten, insbesondere Switche und Router, sowie TCP/IP-Protokollfamilie
- Management der IPv4/IPv6-Adressierung; IP-Services (DHCP/NAT)
- Grundlagen des Routings, Switching und VLANs
- WLAN-Technologien, ihr Einsatz und WLAN-Sicherheit
- Design, Aufbau und Betrieb redundanter LANs
- Sichere Anbindung von Unternehmensnetze an das Internet, insb. VPN
- Netzwerkmanagement und Netzwerksicherheit: SNMP, Absicherung der Netzwerkgeräte, Authentifizierung, Autorisierung, Abrechnung, Firewall-Technologien und IPS/IDS-Implementierungen

Prüfungsvorleistung

Testat

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- James F. Kurose und Keith W. Ross: Computer Networking: A Top-Down Approach, Pearson, Harlow, 2021
- Andrew S. Tanenbaum und David J. Wetherall: Computer Networks, Pearson, Boston, 2011
- Larry L. Peterson und Bruce S. Davie: Computer Networks: A Systems Approach, Morgan Kaufmann, Cambridge, 2021, https://book.systemsapproach.org/
- William Stallings: Network Security Essentials: Applications and Standards, Pearson, Harlow, 2020

Kurzporträt BDF302: Rechnernetze und Rechnernetzsicherheit

Worum geht es? Dieses Modul behandelt Rechnernetze und Rechnernetzsicherheit im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einsatz von und Anforderungen an Datennetze; Netzkomponenten, insb. Switche und Router; TCP/IP-Protokollfamilie.
Wofür braucht man es? Netzwerkgrundlagen sind notwendig, um Kommunikation zwischen Systemen zu verstehen, Fehlkonfigurationen und Angriffe zu erkennen und Sicherheitsarchitekturen beurteilen zu können.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF402: Netzwerkforensik

Modulverantwortung	Prof. Dr. Martin Grothe	**Lehrperson(en)**	Prof. Dr. Martin Grothe
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | - Ü | 2 P | - S	**Engl. Titel**	Network Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF204: Forensische Methoden und Werkzeuge: forensische Akquise, Auswertung, Korrelation und Dokumentation digitaler Spuren.
- BDF205: IT-Sicherheit: Angriffsarten, Schutzmaßnahmen, IDS/IPS und Sicherheitsarchitekturen.
- BDF301: Betriebssysteme: Technik: Betriebssystemartefakte, Logging, Prozesse und Netzwerkkommunikation.
- BDF302: Rechnernetze und Rechnernetzsicherheit: TCP/IP, Routing, Switching, Netzwerkdienste und Netzwerksicherheitsmechanismen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Netzwerkdaten forensisch erfassen, analysieren und sicherheitsrelevante Kommunikation nachvollziehbar interpretieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- auf forensisch saubere Art und Weise digitale Spuren zu sichern und auszuwerten
- forensische Spuren zu finden, sie zu extrahieren und sinnvoll zu korrelieren
- mit dem Wissen der zugrundeliegenden Theorie den Umgang mit ausgewählten Werkzeugen der IT-Forensik praktisch anzuwenden
- die wichtigsten Schritte einer forensischen Untersuchung zu kennen und durchführen zu können
- die für einen IT-Forensiker wichtigen Soft-Skills zu kennen
- die Möglichkeiten und Grenzen der modernen IT-Forensik zu verstehen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- In der Veranstaltung werden zunächst die wichtigsten Grundlagen für die forensisch saubere Arbeitsweise vorgestellt. Hierbei werden theoretische Modelle und Anforderungen und ihre Anwendung in der Praxis beleuchtet
- Weiterhin wird betrachtet, welche Voraussetzungen für eine erfolgreiche forensische Ermittlung gegeben sein müssen
- Mit diesem Wissen ausgestattet, wird im weiteren Verlauf die Extraktion von digitalen Artefakten beschrieben. Insbesondere werden hier im Detail die Methoden der Netzwerkforensik vermittelt. Es wird das notwendige Hintergrundwissen zu den entsprechenden Technologien eingeführt, bevor im Anschluss mögliche Analysemethoden vorgestellt werden
- Anschließend werden weitere Datenquellen für digitale Spuren dargestellt. Hierzu zählen beispielsweise Log-Daten, Betriebssystemdateien, wie z.B. die Windows-Registry, anwendungsspezifische Daten, wie bspw. Exif-Daten in Bildern oder Browser-Daten, sowie Inhalte und Metadaten von Datenbanksystemen
- Nachdem vermittelt wurde, wie und wo digitale Spuren extrahiert und gesichert werden können, wird im nächsten Block vertieft, wie diese gesammelten Daten zur Beantwortung typischer Fragestellungen im Kontext von IT-forensischen Untersuchungen verwendet werden können. Hierzu werden Techniken zur Korrelation von digitalen Spuren aufgezeigt. Gleichzeitig werden Methoden zur schnellen Erstanalyse (Triage) vorgestellt sowie die Grundlagen des Similarity-Hashings. Darüber hinaus werden Techniken aus dem Bereich der Anti-Forensik vorgestellt und den Umgang hiermit
- Für alle Inhalte werden neben den theoretischen Grundlagen stets auch die praktische Anwendbarkeit vermittelt. Daneben sind aber auch für die digitale Forensik eminente Soft-Skills wichtig, wie das zielgruppengerechte Präsentieren von Ermittlungsergebnissen, die Fähigkeit, Thesen mithilfe von digitalen Artefakten zu untermauern oder zu widerlegen, sowie eine strukturierte Vorgehens- und Denkweise bei forensischen Analysen

Prüfungsvorleistung

Testat

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Chris Sanders und Jason Smith: Applied Network Security Monitoring, Syngress, Waltham, 2014
- Richard Bejtlich: The Practice of Network Security Monitoring, No Starch Press, San Francisco, 2013
- Laura Chappell: Wireshark Network Analysis, Protocol Analysis Institute, San Jose, 2012
- Gerald Combs und Ulf Lamping: Wireshark User's Guide, Wireshark Foundation, 2024, https://www.wireshark.org/docs/wsug_html_chunked/

Kurzporträt BDF402: Netzwerkforensik

Worum geht es? Dieses Modul behandelt Netzwerkforensik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere In der Veranstaltung werden zunächst die wichtigsten Grundlagen für die forensisch saubere Arbeitsweise vorgestellt. Hierbei werden theoretische Modelle und Anforderungen und ihre Anwendung in der Praxis beleuchtet; Weiterhin wird betrachtet, welche Voraussetzungen für eine erfolgreiche forensische Ermittlung gegeben sein müssen; Mit diesem Wissen ausgestattet, wird im weiteren Verlauf die Extraktion von digitalen Artefakten beschrieben. Insbesondere werden hier im Detail die Methoden der Netzwerkforensik vermittelt. Es wird das notwendige Hintergrundwissen zu den entsprechenden Technologien eingeführt, bevor im Anschluss mögliche Analysemethoden vorgestellt werden.
Wofür braucht man es? Netzwerkforensik macht Kommunikationsspuren auswertbar und hilft, Angriffswege, Datenabflüsse und Zusammenhänge zwischen Systemen technisch nachvollziehbar zu rekonstruieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Lernpfad Kriminalistik

Der Lernpfad Kriminalistik befähigt die Studierenden, digitale Spuren und technische Befunde in kriminalistische, rechtliche und gesellschaftliche Zusammenhänge einzuordnen. Dabei entwickeln sie Kompetenzen im Verstehen von Ermittlungsprozessen, Täterkommunikation, Geschäftsmodellen im Internet und rechtlichen Grundlagen der Cyberkriminalistik.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können kriminalistische Grundlagen, rechtliche Rahmenbedingungen, digitale Tatorte, Täterkommunikation und internetbasierte Geschäftsmodelle beschreiben, analysieren und auf Fragestellungen der Digitalen Forensik beziehen.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Lernpfad
  - rechtliche Grundlagen der Cyberkriminalistik und typische Prozessabläufe erarbeiten,
  - kriminalistische Denk- und Vorgehensweisen auf digitale Sachverhalte übertragen,
  - digitale Tatorte, Kommunikationsspuren und Täterkommunikation analysieren,
  - internetbasierte Geschäftsmodelle und deren sicherheits- bzw. kriminalitätsrelevante Aspekte untersuchen,
  - Befunde adressatengerecht dokumentieren, begründen und kommunizieren.
- **WOZU**: Damit sie technische Spuren nicht isoliert betrachten, sondern in Ermittlungs-, Beweis- und Handlungskontexte einordnen können. Der Lernpfad schafft die Verbindung zwischen technischer Forensik, rechtlicher Bewertung und kriminalistischer Fallarbeit.

Kurzporträt Lernpfad Kriminalistik

Worum geht es? Der Lernpfad Kriminalistik verbindet digitale Technik mit Ermittlungslogik, Recht und Fallverständnis. Die Studierenden lernen, digitale Spuren als Teil eines Tatgeschehens, einer Kommunikationssituation oder eines rechtlich relevanten Prozesses zu betrachten.
Wofür braucht man es? Forensische Ergebnisse müssen in Ermittlungen belastbar, verständlich und rechtlich verwertbar sein. Die Kompetenzen helfen, technische Analyseergebnisse sinnvoll einzuordnen und für unterschiedliche Adressaten aufzubereiten.
Wieso ist es interessant? Digitale Forensik endet nicht beim technischen Fund. Der Lernpfad zeigt, wie technische Hinweise zu kriminalistischen Erkenntnissen werden und welche Rolle Kommunikation, Recht und digitale Geschäftsmodelle dabei spielen.

BDF105: Rechtliche Grundlagen der Cyberkriminalistik

Modulverantwortung	Prof. Dr. Timo Schwarzwälder	**Lehrperson(en)**	Prof. Dr. Timo Schwarzwälder
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Legal Fundamentals of Cybercrime Investigation
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können zentrale rechtliche Grundlagen der Cyberkriminalistik einordnen und typische straf-, strafprozess- und datenschutzrechtliche Fragestellungen auf digitale Sachverhalte anwenden.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- den Inhalt, die Bedeutung und die Funktion von Grundrechten zu beschreiben
- mit den Grundlagen des formellen und materiellen Strafrechts zum Schutz unterschiedlicher Rechtsgüter vertraut zu sein
- einfache Sachverhalte eigenständig hinsichtlich Tatbestand, Rechtswidrigkeit und Schuld zu bewerten und dabei auch Formen der Deliktsbegehung zu differenzieren
- insbesondere IT-relevante Sachverhalte vertiefend zu behandeln
- ausgewählte Grundlagen des IT-Rechts, wie z.B. datenschutzrechtliche Aspekte oder privatrechtliche Besonderheiten des elektronischen Geschäftsverkehrs zu erfassen
- mit juristischen Prüfmethoden und Arbeitsweisen vertraut zu sein, die ihnen erlauben, ihr berufliches Handeln vor dem Hintergrund der oben genannten Rechtsbereiche zu reflektieren
- den Umgang mit rechtswissenschaftlichen Quellen zur Beurteilung der Sachverhalte zu kennen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Verfassungsgrundsätze, insbesondere Demokratie und Rechtsstaatsprinzip
- Allgemeine Grundrechtslehren, einzelne Grundrechte, Schutzbereich, Eingriff und Schranken
- Funktion der Strafe und des Strafrechts sowie Grundprinzipien des Strafrechts
- Strafrechtliche Sanktionen und Einteilung der Delikte
- Tatbestand: objektive und subjektive Tatbestandsmerkmale, Kausalität, Zurechenbarkeit und Vorsatz
- Schuld, Formen von Täterschaft und Teilnahme sowie Tatbestands- und Verbotsirrtum
- Ausgewählte IT-relevante Rechtsbereiche, z.B. DSGVO, Recht des elektronischen Geschäftsverkehrs, Immaterialgüterrecht, Telekommunikationsrecht
- Rechtsquellen, Methodik der Fallbearbeitung sowie juristische und wissenschaftliche Recherche

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Eric Hilgendorf und Brian Valerius: Computer- und Internetstrafrecht, Springer, Berlin, 2012, https://doi.org/10.1007/978-3-642-16895-6
- Ulrich Sieber, Nicolas von zur Mühlen und Jan Pohle: Cybercrime und Strafrecht in der Informationsgesellschaft, Duncker & Humblot, Berlin, 2021
- Lutz Meyer-Goßner und Bertram Schmitt: Strafprozessordnung mit GVG und Nebengesetzen, C.H.Beck, München, 2024
- Alexander Roßnagel: Datenschutzrecht, C.H.Beck, München, 2023

Kurzporträt BDF105: Rechtliche Grundlagen der Cyberkriminalistik

Worum geht es? Dieses Modul behandelt Rechtliche Grundlagen der Cyberkriminalistik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Verfassungsgrundsätze, insbesondere Demokratie und Rechtsstaatsprinzip; Allgemeine Grundrechtslehren, insbesondere Funktionen, Schutzbereich, Eingriff, Schranken; Einzelne Grundrechte.
Wofür braucht man es? Rechtskenntnisse sind erforderlich, um digitale Ermittlungen an Grundrechten, Strafrecht, Datenschutz und Verwertbarkeit auszurichten und eigenes Handeln rechtlich abzusichern.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF203: Einführung in die Kriminalistik

Modulverantwortung	Prof. Dr. Nils Kopal	**Lehrperson(en)**	Dr. Sinan Eroglu
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Introduction to Criminalistics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können kriminalistische Grundbegriffe, Vorgehensweisen und Denkmodelle beschreiben und auf digitale Ermittlungs- und Spurenlagen beziehen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die Kriminalwissenschaften innerhalb der Studienfächer einzuordnen
- Aufbau und Organisation der Kriminalitätsbekämpfung zu erläutern und Bezüge zwischen kriminalistischer Beweisführung im Ermittlungsverfahren und gerichtlicher Beweisführung herzustellen
- die kriminalistische Verdachtslehre auf Sachverhalte anzuwenden
- die Organisation der Kriminaltechnik zu erläutern
- die Zuständigkeiten für die polizeiliche Spurensuche, Spurensicherung und Spurenauswertung auf die jeweiligen Stadien der polizeilichen Ermittlungsarbeit zu erläutern
- kriminalistisch relevante Spuren nach der Grundeinteilung jeweils systematisch zuzuordnen
- die Möglichkeiten und Grenzen einer ersten Spurensuche an Tatorten zu bewerten
- Spuren hinsichtlich Relevanz, Beweiskraft und Beweiswert zu interpretieren, zu klassifizieren und auf Sachverhalte zu übertragen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einordnung der Fächer Kriminalistik, Kriminaltechnik und Kriminologie in den Bereich der Kriminalwissenschaften, Differenzierung der Fächer untereinander und Aufzeigen der Querbezüge zu den übrigen Studienfächern
- Aufbau und Organisation der Kriminalitätsbekämpfung sowie Zusammenarbeit zwischen Staatsanwaltschaft und Polizei im Ermittlungsverfahren
- fachliche Entwicklung, Anforderungen und formelle Beweismittel der Beweisführung im Ermittlungsverfahren und vor Gericht
- Verdachtsfindung und Verdachtsqualifizierung im Ermittlungsverfahren
- Kriminalwissenschaftliche Analysemethoden und kriminalistische Fallanalyse zur Aufklärung von Einzeldelikten und Tatserien
- polizeiliche Zuständigkeiten, kriminaltechnische Grundeinteilung und Grundtechniken zur Suche, Sicherung und Auswertung von Spuren
- Relevanz, Beweiskraft und Beweiswert gefundener oder möglicher Spuren für die weitere Beweisführung
- kriminalistischer und juristischer Tatort, weitere relevante Ereignisorte und Aussage als Zeuge vor Gericht

Prüfungsvorleistung

Keine

Prüfungsleistung

Testat

Literatur

- Rolf Ackermann, Horst Clages und Holger Roll: Handbuch der Kriminalistik, Boorberg, Stuttgart, 2019
- Robert Weihmann: Kriminalistik: Ein Grundriss für Studium und Praxis, Boorberg, Stuttgart, 2022
- Hans-Dieter Schwind: Kriminologie und Kriminalpolitik, Kriminalistik Verlag, Heidelberg, 2021
- Jochen Neuhaus und Artur R. Müller: Kriminalistische Fallanalyse, C.F. Müller, Heidelberg, 2020

Kurzporträt BDF203: Einführung in die Kriminalistik

Worum geht es? Dieses Modul behandelt Einführung in die Kriminalistik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einordnung der Fächer Kriminalistik, Kriminaltechnik und Kriminologie in den Bereich der Kriminalwissenschaften, Differenzierung der Fächer untereinander und Aufzeigen der Querbezüge zu den übrigen Studienfächern; Aufbau und Organisation der Kriminalitätsbekämpfung; Verhältnis zwischen Staatsanwaltschaft und Polizei sowie die Bedeutung für die Zusammenarbeit im Ermittlungsverfahren.
Wofür braucht man es? Kriminalistisches Grundverständnis hilft, technische Spuren in Ermittlungslogik, Beweiswert und Tatortarbeit einzuordnen und Ergebnisse adressatengerecht aufzubereiten.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF303: Der Digitale Tatort und Täterkommunikation

Modulverantwortung	Prof. Dr. Nils Kopal	**Lehrperson(en)**	Dr. Thomas Jansen Dr. Philip Schütz Jens Berger Karsten Brodkorb
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	The Digital Crime Scene and Perpetrator Communication
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF104: Einführung in die Digitale Forensik: forensisch saubere Arbeitsweise, Sicherung digitaler Beweise und Untersuchungsprozess.
- BDF105: Rechtliche Grundlagen der Cyberkriminalistik: straf-, strafprozess- und datenschutzrechtliche Grundlagen digitaler Ermittlungen.
- BDF203: Einführung in die Kriminalistik: Tatortbegriff, Spurensuche, Spurensicherung, Beweiskraft und Beweiswert.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können digitale Tatorte und Täterkommunikation kriminalistisch einordnen sowie digitale Spuren sichern, interpretieren und dokumentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- den Begriff Tatort rechtlich sowie kriminalistisch einzuordnen und auf cyberkriminalistische Sachverhalte anzuwenden
- potentielle Spurenträger am Tatort zu identifizieren und situationsangepasste und integritätswahrende Sicherungsmethoden zu bestimmen und anzuwenden
- gesicherte Daten mit forensischen Werkzeugen auszuwerten und zu interpretieren
- unterschiedliche Kommunikationsformen von Cyberkriminellen und die ihnen zugrunde liegenden technischen Hintergründe erläutern zu können
- Anonymisierungstechniken erläutern und anwenden zu können sowie Möglichkeiten der Deanonymisierung aufzuzeigen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Rechtliche und kriminalistische Grundlagen zum Tatortbegriff
- Akteure und Verhalten am Tatort
- Zuständigkeiten für die Suche, Sicherung und Auswertung von digitalen Spuren
- Forensische Live-Sicherung von digitalen Spuren in unterschiedlichen IT-Systemen
- Zielgerichtete Suche und Interpretation von Spuren in IT-Systemen
- Aufbereitung von forensischen Datensicherungen
- Beweiswert, Beweiskraft und Dokumentation von (digitalen) Spuren am Tatort
- Täterseitige Kommunikationsmittel sowie Anonymisierungs- und Deanonymisierungstechniken

Prüfungsvorleistung

Keine

Prüfungsleistung

Mündliche Prüfung (30 - 45 Minuten)

Literatur

- Eoghan Casey: Digital Evidence and Computer Crime, Academic Press, Waltham, 2011
- Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, Heidelberg, 2014
- Brian Carrier: File System Forensic Analysis, Addison-Wesley, Boston, 2005
- Angus M. Marshall: Digital Forensics: Digital Evidence in Criminal Investigation, Wiley, Chichester, 2008

Kurzporträt BDF303: Der Digitale Tatort und Täterkommunikation

Worum geht es? Dieses Modul behandelt Der Digitale Tatort und Täterkommunikation im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Rechtliche und kriminalistische Grundlagen zum Tatortbegriff; Akteure und Verhalten am Tatort; Zuständigkeiten für die Suche, Sicherung und Auswertung von digitalen Spuren.
Wofür braucht man es? Kenntnisse zu digitalen Tatorten und Täterkommunikation unterstützen dabei, Spurenträger zu identifizieren, Kommunikationswege zu verstehen und digitale Befunde kriminalistisch zu interpretieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF403: Geschäftsmodelle im Internet

Modulverantwortung	Prof. Dr. Thorsten Weber	**Lehrperson(en)**	Dr. Sven Thielen Prof. Dr. Peter Davids Prof. Dr. Jürgen Quade
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Business Models on the Internet
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF203: Einführung in die Kriminalistik: kriminalistische Einordnung, Ermittlungslogik und Bewertung von Beweisspuren.
- BDF302: Rechnernetze und Rechnernetzsicherheit: netzwerkzentrierte Anwendungen, Internetdienste und Kommunikationsgrundlagen.
- BDF303: Der Digitale Tatort und Täterkommunikation: digitale Tatorte, Täterkommunikation, Anonymisierungstechniken und Interpretation digitaler Spuren.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können internetbasierte Geschäftsmodelle analysieren und deren technische, wirtschaftliche und sicherheitsbezogene Rahmenbedingungen einordnen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Geschäftsprozesse und Geschäftsmodelle im Internet einzuordnen, sie zu identifizieren und nachzuvollziehen
- ihr Missbrauchspotential für kriminelle Zwecke einzuschätzen und zu beschreiben
- Ermittlungsmethoden bei ausgewählten Geschäftsprozessen im Internet anzuwenden
- Techniken zur Anonymisierung von Geschäftsvorfällen und Zahlungsmethoden im Internet aufzuzeigen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einordnung der Geschäftsprozesse im Internet in den Bereich der Kriminalwissenschaften, Differenzierung der Fächer untereinander und Aufzeigen von Querbezügen zu den übrigen Studienfächern
- Kriminalistische Betrachtung ausgewählter Geschäftsprozesse im Internet sowie aktuelle Trends und Entwicklungen
- Nutzung von netzwerkzentrierten Anwendungen, wie beispielsweise Browser, Messenger, EMail, Cloud-Dienste und soziale Netzwerke
- Foren- und Handelsplattformen, Registrierung bei Internetdiensten und Hosting von Diensten
- Virtuelle private Netzwerke, Botnetze, Proxy-Dienste, Clearnet und Darknet
- Underground Economy, Tätergruppierungen und Cybercrime-as-a-Service
- Angriffs- und Angreifertypen sowie Verbreitung von Malware vom initialen Zugriff bis zur Exfiltration von Daten
- Bezahldienste, Zahlungsmethoden, Bonussysteme und Zugang zu Opferdaten über Spam, Phishing oder ausgenutzte Schwachstellen

Prüfungsvorleistung

Keine

Prüfungsleistung

Mündliche Prüfung (30 - 45 Minuten)

Literatur

- Alexander Osterwalder und Yves Pigneur: Business Model Generation, Campus, Frankfurt am Main, 2011
- Bernd W. Wirtz: Electronic Business, Springer Gabler, Wiesbaden, 2021, https://doi.org/10.1007/978-3-658-34349-1
- Kenneth C. Laudon und Carol Guercio Traver: E-Commerce: Business, Technology, Society, Pearson, Harlow, 2023
- Dave Chaffey, Fiona Ellis-Chadwick und Richard Mayer: Digital Business and E-Commerce Management, Pearson, Harlow, 2019

Kurzporträt BDF403: Geschäftsmodelle im Internet

Worum geht es? Dieses Modul behandelt Geschäftsmodelle im Internet im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einordnung der Geschäftsprozesse im Internet in den Bereich der Kriminalwissenschaften, Differenzierung der Fächer untereinander und Aufzeigen von Querbezügen zu den übrigen Studienfächern; Kriminalistische Betrachtung ausgewählter Geschäftsprozesse im Internet sowie aktuelle Trends und Entwicklungen; Nutzung von netzwerkzentrierten Anwendungen, wie beispielsweise Browser, Messenger, EMail, Cloud-Dienste und soziale Netzwerke.
Wofür braucht man es? Das Verständnis internetbasierter Geschäftsmodelle erleichtert es, Missbrauchsformen, Zahlungswege, Plattformstrukturen und kriminelle Ökosysteme im digitalen Raum zu analysieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Lernpfad Forensik

Der Lernpfad Forensik befähigt die Studierenden, digitale Beweise methodisch zu sichern, mit geeigneten Werkzeugen zu untersuchen und Analyseergebnisse nachvollziehbar zu dokumentieren. Dabei entwickeln sie Kompetenzen im forensischen Prozess, in der Werkzeugauswahl, in der Datenbankanalyse und in projektförmiger Fallbearbeitung.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können grundlegende Konzepte der Digitalen Forensik erklären, forensische Methoden und Werkzeuge anwenden, Datenbanken forensisch untersuchen und komplexere forensische Aufgaben in Projekten bearbeiten.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Lernpfad
  - Prozesse, Grundbegriffe und typische Aufgaben der Digitalen Forensik erarbeiten,
  - Methoden zur Sicherung, Analyse, Dokumentation und Präsentation digitaler Spuren anwenden,
  - forensische Werkzeuge auswählen, einsetzen und deren Ergebnisse kritisch bewerten,
  - Datenbanksysteme hinsichtlich relevanter Artefakte und Spuren untersuchen,
  - im Forensikprojekt eine zusammenhängende Aufgabenstellung planen, durchführen und präsentieren.
- **WOZU**: Damit sie digitale Spuren fachgerecht, reproduzierbar und nachvollziehbar bearbeiten können. Der Lernpfad bildet den Kern der forensischen Handlungskompetenz im Studiengang und verbindet technische Analyse mit methodischem Vorgehen und Ergebnisdarstellung.

Kurzporträt Lernpfad Forensik

Worum geht es? Der Lernpfad Forensik behandelt den Weg von der Einführung in digitale Forensik über Methoden und Werkzeuge bis zur forensischen Untersuchung konkreter Datenquellen und Projektaufgaben. Im Mittelpunkt steht das kontrollierte Arbeiten mit digitalen Beweisen.
Wofür braucht man es? Die Kompetenzen werden benötigt, um digitale Spuren nicht nur zu finden, sondern korrekt zu sichern, auszuwerten, zu dokumentieren und zu präsentieren. Sie sind zentral für forensische Praxis, Ermittlungsunterstützung und sicherheitsbezogene Analyseaufgaben.
Wieso ist es interessant? Digitale Forensik macht verborgene technische Spuren sichtbar und interpretierbar. Der Lernpfad zeigt, wie aus Daten belastbare Hinweise entstehen und wie diese in nachvollziehbare Ergebnisse überführt werden.

BDF104: Einführung in die Digitale Forensik

Modulverantwortung	Prof. Dr. Christofer Fein	**Lehrperson(en)**	Prof. Dr. Christofer Fein
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Introduction to Digital Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Grundbegriffe, Prozesse und typische Aufgaben der Digitalen Forensik erklären und einfache forensische Fragestellungen methodisch einordnen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Konzepte und Technologien, ethische und rechtliche Standards der digitalen Forensik zu benennen und zu erläutern
- die Phasen in einem Untersuchungsprozess wie das Sammeln der Beweismittel, der Analyse und der Berichterstattung zu kennen
- fundiert die Möglichkeiten und Ergebnisse forensischer Untersuchungen zu bewerten und in einen Gesamtkontext einzuordnen
- rudimentäre Untersuchungen selbst durchführen zu können, indem digitale Beweise gesammelt, dokumentiert und aufbewahrt werden, so dass diese für Gerichte und Strafverfolgungsbehörden verwertbar sind,
- Forensische Werkzeuge und -Technologien einzusetzen, um digitale Geräte und Kommunikationssysteme zu untersuchen und Beweise zu sammeln

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagen der digitalen Forensik und der forensisch sauberen Arbeitsweise
- Modelle und ihre Anwendung in der Praxis
- Anforderungen, Voraussetzungen, Rechtsrahmen, Zielsetzung (Fragestellungen)
- Digitale Artefakte und deren Konfidenz im Kontext der Zielsetzung
- Vorgehensmodelle zur Sicherung digitaler Beweise
- Kriminelle Vorgehensweisen, Monetarisierungsmöglichkeiten und deren technische Basis aus dem Bereich Cyberkriminalität (Erpressung mittels Ransomware, Cybercrime as a Service)

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, Heidelberg, 2014
- Eoghan Casey: Digital Evidence and Computer Crime, Academic Press, Waltham, 2011
- John Sammons: The Basics of Digital Forensics, Syngress, Waltham, 2015
- Bill Nelson, Amelia Phillips und Christopher Steuart: Guide to Computer Forensics and Investigations, Cengage Learning, Boston, 2019

Kurzporträt BDF104: Einführung in die Digitale Forensik

Worum geht es? Dieses Modul behandelt Einführung in die Digitale Forensik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlagen der digitalen Forensik und der forensisch sauberen Arbeitsweise; Modelle und ihre Anwendung in der Praxis; Anforderungen, Voraussetzungen, Rechtsrahmen, Zielsetzung (Fragestellungen).
Wofür braucht man es? Die Einführung schafft Orientierung im forensischen Prozess und hilft, Beweise von Beginn an methodisch sauber, nachvollziehbar und rechtlich verwertbar zu behandeln.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF204: Forensische Methoden und Werkzeuge

Modulverantwortung	Prof. Dr. Christofer Fein	**Lehrperson(en)**	Prof. Dr. Christofer Fein
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Forensic Methods and Tools
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF104: Einführung in die Digitale Forensik: forensischer Prozess, Beweissicherung, Dokumentation und grundlegende Werkzeugnutzung.
- BDF106: Erstsemesterprojekt: erste praktische Erfahrungen mit Sicherheitsaspekten, forensischer Analyse und Berichterstellung.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können grundlegende forensische Methoden und Werkzeuge auswählen, anwenden und Ergebnisse nachvollziehbar dokumentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- selbständig einfache forensische Auswertungen von Datenträgern, Arbeitsspeicher und Netzwerkdaten durchzuführen
- die gewonnenen Erkenntnisse angemessen zu dokumentieren
- die Aussagekraft der Ergebnisse einer gegebenen forensischen Analyse fundiert zu bewerten
- einzuschätzen, ob bzw. mit wie viel Aufwand weiterführende Erkenntnisse mittels zusätzlicher Analysen möglich wären

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einführung in die Teilbereiche Datenträger-, Arbeitsspeicher- und Netzwerkforensik
- Datenrepräsentation auf Datenträgern, im Arbeitsspeicher und im Netzwerk sowie deren Zugriff und Auswertbarkeit
- forensische Methoden zur Akquise, Auswertung und Interpretation der gewonnenen Daten
- Herausforderungen der unterschiedlichen forensischen Teildisziplinen (Schreibschutz bei Datenträgern, Akquise von Hauptspeicher, Aufzeichnung von Netzwerkverkehr)
- Werkzeuge der digitalen Forensik

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Eoghan Casey: Digital Evidence and Computer Crime, Academic Press, Waltham, 2011
- Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, Heidelberg, 2014
- Cory Altheide und Harlan Carvey: Digital Forensics with Open Source Tools, Syngress, Waltham, 2011
- John Sammons: The Basics of Digital Forensics, Syngress, Waltham, 2015

Kurzporträt BDF204: Forensische Methoden und Werkzeuge

Worum geht es? Dieses Modul behandelt Forensische Methoden und Werkzeuge im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einführung in die Teilbereiche Datenträger-, Arbeitsspeicher- und Netzwerkforensik; Datenrepräsentation auf Datenträgern, im Arbeitsspeicher und im Netzwerk sowie deren Zugriff und Auswertbarkeit; forensische Methoden zur Akquise, Auswertung und Interpretation der gewonnenen Daten.
Wofür braucht man es? Methoden- und Werkzeugkompetenz ist nötig, um Daten aus unterschiedlichen Quellen sachgerecht zu akquirieren, auszuwerten und die Aussagekraft der Ergebnisse kritisch zu bewerten.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF305: Datenbanken-Forensik

Modulverantwortung	Prof. Dr. Nils Kopal	**Lehrperson(en)**	Prof. Dr. Nils Kopal Prof. Dr. Thorsten Weber
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Database Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF101: Informatik-Grundlagen der Forensik: Datenmodellierung, Abstraktion und informatische Grundbegriffe.
- BDF103: Programmierung: grundlegende Programmierkonzepte für SQL-Abfragen und datenbezogene Analyseaufgaben.
- BDF204: Forensische Methoden und Werkzeuge: forensische Auswertung, Dokumentation und Bewertung digitaler Spuren.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Datenbanksysteme hinsichtlich forensisch relevanter Informationen analysieren und Datenbankspuren sichern, auswerten und dokumentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- anhand eines einheitliches Begriffsgebäudes die Datenbankthematik erklären
- Unterschiede zwischen relationalen und NoSQL Datenbank-Managementsystemen (DBMS) zu verstehen und abzugrenzen
- einschlägige Methoden der Datenmodellierung, wie z. B. das Entity-Relationship-Modell (ER), anzuwenden
- ein Datenbankschema aus dem ER-Modell in das Relationenmodell zu transformieren
- komplexere Datenbankabfragen, Datendefinitionen und Datenänderungen über SQL zu programmieren
- den Transaktionsbegriff, Mehrbenutzersynchronisation und Verfahren zur Sicherung der Datenintegrität zu erläutern, zu vergleichen und im Hinblick auf forensische Analysen zu beurteilen
- Sicherheitsaspekte wie Zugriffskontrollen und Multilevel-Datenbanken zu verstehen und anzuwenden
- NoSQL Datenbanksysteme zu verstehen und zu implementieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlegende Strukturen von Datenbanksystemen
- konzeptionelle und logischen Datenmodellierung
- SQL-API
- NoSQL-API
- Transaktionsmanagement
- DB-Architekturen im Kontext der IT-Sicherheit
- forensische Analysen von Datenbanken

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Kevin Kline, Regina Obe und Leo Hsu: SQL in a Nutshell, O'Reilly Media, Sebastopol, 2022
- Ramez Elmasri und Shamkant B. Navathe: Fundamentals of Database Systems, Pearson, Harlow, 2016
- Paul M. Wright: SQL Server Forensic Analysis, Rampant TechPress, Kittrell, 2007
- David Litchfield: The Oracle Hacker's Handbook, Wiley, Indianapolis, 2007

Kurzporträt BDF305: Datenbanken-Forensik

Worum geht es? Dieses Modul behandelt Datenbanken-Forensik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlegende Strukturen von Datenbanksystemen; konzeptionelle und logischen Datenmodellierung; SQL-API.
Wofür braucht man es? Datenbankforensik unterstützt Untersuchungen, bei denen strukturierte Daten, Transaktionen, Zugriffsspuren oder Datenbankarchitekturen als Beweis- und Erkenntnisquellen dienen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Projekte

Die Projektmodule befähigen die Studierenden, fachliche Inhalte der Digitalen Forensik in offenen, praxisnahen und teamorientierten Aufgabenstellungen anzuwenden. Dabei entwickeln sie Kompetenzen in Projektplanung, Selbstorganisation, Recherche, Teamarbeit, Dokumentation, Präsentation und kreativer Problemlösung.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können forensische, sicherheitsbezogene und informatische Projektaufgaben strukturieren, im Team bearbeiten, fachliche Lösungen entwickeln und Ergebnisse nachvollziehbar dokumentieren und präsentieren.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Modulbereich
  - einfache forensische Aufgabenstellungen in frühen Projektformaten bearbeiten,
  - bedarfsorientierte Mikroprojekte planen, durchführen und reflektieren,
  - fachliche Inhalte selbstständig recherchieren und mit vorhandenen Kompetenzen verknüpfen,
  - im Forensikprojekt komplexere Untersuchungs- oder Entwicklungsaufgaben bearbeiten,
  - im Hackathon kreative Lösungsansätze unter begrenzten Rahmenbedingungen entwickeln und präsentieren.
- **WOZU**: Damit sie die im Studium aufgebauten Kompetenzen in realitätsnahen Arbeitsformen anwenden und auf offene Problemstellungen übertragen können. Die Projektmodule stärken insbesondere Selbstständigkeit, Teamarbeit, Kommunikation und transferfähige Handlungskompetenz.

Kurzporträt Projekte

Worum geht es? Die Projektmodule bringen Studierende früh und wiederholt in anwendungsnahe Arbeitssituationen. Sie bearbeiten forensische, sicherheitsbezogene oder informatische Aufgaben im Team, dokumentieren ihr Vorgehen und präsentieren Ergebnisse.
Wofür braucht man es? Digitale Forensik ist häufig projektförmig, interdisziplinär und zeitkritisch. Die Kompetenzen helfen, Aufgaben zu planen, Rollen zu klären, Wissen selbstständig aufzubauen und Ergebnisse überzeugend zu vertreten.
Wieso ist es interessant? In Projekten wird sichtbar, wie Wissen aus einzelnen Modulen zusammenwirkt. Die Studierenden erleben, wie aus Recherche, Analyse, Umsetzung, Dokumentation und Präsentation eine tragfähige Lösung entsteht.

BDF106: Erstsemesterprojekt

Modulverantwortung	Prof. Dr. Thomas Meuser	**Lehrperson(en)**	Prof. Dr. Thomas Meuser
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	V | - Ü | 2 P | 2 SL	**Engl. Titel**	First-Semester Project
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können eine einfache fachbezogene Projektaufgabe im Team strukturieren, bearbeiten, dokumentieren und präsentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- am Beispiel eines praxisnahen, aber dennoch einfachen Untersuchungsobjektes eine forensische Aufgabenstellung in einem Team zu bearbeiten
- selbständig spezielle Kenntnisse und Fertigkeiten, die zur erfolgreichen Bearbeitung der Projektaufgabe erforderlich sind, zu erkennen, zu recherchieren und zu erarbeiten
- eine persönliche Selbstorganisation und eigene Lernstrategie zu entwickeln
- in einem interdisziplinären und heterogen zusammengesetzten Team selbständig und teamorientiert zu arbeiten und zu kommunizieren
- Vorteile und Grenzen von Teamarbeit zu erkennen
- ein gemeinsames Projekt zu planen, durchzuführen und zu kontrollieren
- eine Dokumentation des Projektes zu erstellen und die Projektergebnisse einem breiteren Publikum zu präsentieren
- motiviert das nachfolgende wissenschaftliche Studium fortzusetzen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagenwissen zu verschiedenen Sicherheitsaspekten
- Identifizierung von Angriffen auf die Sicherheit sowie von Symptomen, Prozessen und Gegenmaßnahmen
- Erwerb von Fertigkeiten in den Bereichen Sicherheitsmanagement, Kontrollen, Schutz und Eindämmungstechnologien
- Werkzeuge der forensischen Analyse
- Prozess einer digitalen forensischen Untersuchung
- Auswerten der digitalen Spuren
- Erstellen eines Berichts

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Die Informationsrecherche erfolgt über das Internet und im Laufe des Semesters wird ein Online-Curriculum durchgearbeitet

Kurzporträt BDF106: Erstsemesterprojekt

Worum geht es? Dieses Modul behandelt Erstsemesterprojekt im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlagenwissen zu verschiedenen Sicherheitsaspekten; Identifizierung von Angriffen auf die Sicherheit sowie von Symptomen, Prozessen und Gegenmaßnahmen; Erwerb von Fertigkeiten in den Bereichen Sicherheitsmanagement, Kontrollen, Schutz und Eindämmungstechnologien.
Wofür braucht man es? Das Erstsemesterprojekt führt früh an teamorientierte Fallbearbeitung heran und verbindet Recherche, Analyse, Dokumentation und Präsentation in einem überschaubaren Rahmen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF206: Bedarfsorientierte Mikroprojekte

Modulverantwortung	Prof. Dr. Jens Brandt	**Lehrperson(en)**	Prof. Dr. Jens Brandt
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | - Ü | 2 P | - S	**Engl. Titel**	Demand-Driven Micro Projects
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

Keine angegeben.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können kleine bedarfsorientierte Projektaufgaben analysieren, passende technische Lösungsansätze entwickeln und prototypisch umsetzen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Kenntnisse aus einem vorgegeben und eng abgegrenzten fachlichen Themengebiet aus dem Grundlagenbereich eigenständig zu erkennen, zu recherchieren und zu erarbeiten
- eine persönliche Selbstorganisation und eigene Lernstrategie zu entwickeln
- selbständig erworbenes Fachwissen in ein Projekt oder Team einzubringen
- die erarbeiteten Inhalte mit bisher gelernten Inhalten oder mit zu erlernenden Inhalten aus anderen Gebieten selbständig zu verknüpfen und in diesen Gebieten anzuwenden
- ein Projekt zu planen, durchzuführen und zu kontrollieren
- gemeinsame Projekte koordiniert, teamorientiert und agil zu bearbeiten
- eine Dokumentation des Projektes zu erstellen und die Projektergebnisse vor einem Fachpublikum teilweise auch in Englisch zu präsentieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Anwendungsbezogene Grundlagen der Netzwerktechnik
- Anwendungs- und Kontextbezogene Grundlagen der Informatik,
- Grundlagen der Mathematik im anwendungsbezogenen Kontext
- Anwendungsbezogene Sprachkenntnisse (Deutsch und Englisch)

Prüfungsvorleistung

Testat

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Sydsaeter K.; Hammond P. Strom, A.; Carvajal, A.: Mathematik für Wirtschaftswissenschaftler. Mit eLearning-Zugang ”MyLab, Pearson Studium - Economic BWL (Deutsch) aktuelle Ausgabe Bereitgestellte Unterlagen zu jedem Projektinhalt
- Balzert, H.: Lehrbuch der Softwaretechnik: Softwaremanagement. Spektrum-Verlag, aktuelle Auflage
- Hanser, E.: Agile Prozesse: Von XP über Scrum bis MAP, Springer-Verlag, aktuelle Auflage
- Meinel, C./Mundhenk, M.: Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung, aktuelle Auflage

Kurzporträt BDF206: Bedarfsorientierte Mikroprojekte

Worum geht es? Dieses Modul behandelt Bedarfsorientierte Mikroprojekte im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Anwendungsbezogene Grundlagen der Netzwerktechnik; Anwendungs- und Kontextbezogene Grundlagen der Informatik,; Grundlagen der Mathematik im anwendungsbezogenen Kontext.
Wofür braucht man es? Mikroprojekte trainieren, begrenzte Aufgaben selbstständig zu strukturieren, fehlendes Wissen gezielt aufzubauen und Ergebnisse in kurzen Projektzyklen nutzbar zu machen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF405: Forensikprojekt

Modulverantwortung	Prof. Dr. Jürgen Quade	**Lehrperson(en)**	Prof. Dr. Martin Grothe Prof. Dr. Nils Kopal Prof. Dr. Jürgen Quade Prof. Dr. Matteo Zella
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Sommersemester	**Dauer**	1 Semester
Credits	10 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	V | - Ü | 3 P | 1 SL	**Engl. Titel**	Forensics Project
Workload	• Präsenz: 45 Std. • Selbst: 225 Std.		

Empfohlene Voraussetzungen

- BDF104: Einführung in die Digitale Forensik: forensischer Prozess und methodische Einordnung digitaler Beweise.
- BDF204: Forensische Methoden und Werkzeuge: Werkzeugauswahl, Akquise, Analyse und Dokumentation.
- BDF305: Datenbanken-Forensik: datenbankbezogene Analysekompetenzen für projektbezogene forensische Fragestellungen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können eine forensische Projektaufgabe im Team methodisch planen, durchführen, dokumentieren und präsentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- erlernte wissenschaftliche Methoden, Verfahren und Anwendungen aus dem Bereich der IT-Forensik im Rahmen von Teamarbeit zu koordinieren und praktisch anzuwenden
- eine abgegrenzte praktische Problemstellung aus dem Bereich der IT-Forensik eigenständig, mittels einer Analyse der Problemstellung, der Durchführung von wissenschaftlichen (Literatur)recherchen und der Erarbeitung kreativer Lösungen, wissenschaftlich fundiert zu bearbeiten
- eine persönliche Selbstorganisation und eigene Lernstrategie zu entwickeln und selbständig erworbenes Fachwissen zielorientiert in ein Projekt einzubringen
- auf der Basis einer wissenschaftlichen Vorgehensweise (klassisch und agiles Projektmanagement) ein Projekt zu planen, durchzuführen und zu kontrollieren
- gemeinsame interdisziplinäre Projekte koordiniert und teamorientiert zu bearbeiten
- das erlernte Wissen über wissenschaftliche Methoden und Vorgehensweisen anzuwenden, um eine technische Dokumentation des Projektes zu erstellen und die Projektergebnisse vor einem Fachpublikum zu präsentieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Vertiefung der bisher gewonnen Fachkenntnisse im Bereich IT-Forensik
- Wissenschaftliches Vorgehen und Arbeiten
- Zielgerichteter Werkzeugeinsatz
- Präsentationsfähigkeiten (Dokumentation, Ergebnispräsentation)

Prüfungsvorleistung

Testat

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Mark B.: Basiswissen IT Forensik: DE; ISBN 978-3755758976
- Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären; ISBN 978-3864901331
- Weiterführende Quellen werden in der Vorlesung gegeben

Kurzporträt BDF405: Forensikprojekt

Worum geht es? Dieses Modul behandelt Forensikprojekt im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Vertiefung der bisher gewonnen Fachkenntnisse im Bereich IT-Forensik; wissenschaftliches Vorgehen und Arbeiten; zielgerichteter Werkzeugeinsatz.
Wofür braucht man es? Im Forensikprojekt werden zuvor erworbene Kompetenzen zusammengeführt, um komplexere Aufgaben im Team wissenschaftlich fundiert zu planen, umzusetzen und zu präsentieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF505: Hackathon

Modulverantwortung	Prof. Dr. Thomas Meuser	**Lehrperson(en)**	Dr. Markus Schneider
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	10 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	V | - Ü | 3 P | 1 SL	**Engl. Titel**	Hackathon
Workload	• Präsenz: 45 Std. • Selbst: 225 Std.		

Empfohlene Voraussetzungen

- BDF101-BDF106: Module des ersten Fachsemesters: informatische, ethische, programmiertechnische, forensische, rechtliche und projektbezogene Grundlagen.
- BDF201-BDF206: Module des zweiten Fachsemesters: Betriebssystemanwendung, OSINT, Kriminalistik, forensische Methoden, IT-Sicherheit und Mikroprojektkompetenzen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können unter zeitlich und organisatorisch herausfordernden Rahmenbedingungen praxisnahe IT-Sicherheits- oder Forensik-probleme kreativ im Team lösen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Eine definierte praxisnahe Aufgabenstellung, die ein konkretes Problem der IT-Sicherheit bzw. IT-Forensik adressiert, zu bearbeiten und eigenständig unter erschwerten Rahmenbedingungen wie beispielsweise begrenzte Zeit zu lösen
- Neben einem zu erlangenden fachlichen Wissen Methoden und Werkzeuge zur Aggregation von Wissen und der Zusammenarbeit untereinander einzusetzen
- Die Kreativität und Kommunikation durch eine Zusammenarbeit mit anderen Studierenden zu verstärken, sodass Weiterentwicklungen bzw. Optimierungen durchgeführt werden können
- Problemlösungen mit der Hilfe einer Präsentation gegenüber Publikum anhand einer klaren Struktur sowie hohen Verständlichkeit wissenschaftlich vorzutragen und zu visualisieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Kreative Problemlösungen und schnelles Prototyping in interdisziplinären Projekten
- Bedarfsanalyse
- Anwendung der in den Fachmodulen erworbenen, multidisziplinären Fähigkeiten zur Identifikation und zur Lösung von Problemen aus der realen Welt
- Konzeption, Entwurf und prototypische Realisierung sicherer IT-Lösungen für Unternehmen oder Gesellschaften
- Präsentation

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Andreas Kohne, Volker Wehmeier: Hackathons: Von der Idee zur erfolgreichen Umsetzung; ISBN 978-3658260279
- Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären; ISBN 978-3864901331
- Weitere Unterlagen werden in der Vorlesung bekanntgegeben

Kurzporträt BDF505: Hackathon

Worum geht es? Dieses Modul behandelt Hackathon im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Kreative Problemlösungen und schnelles Prototyping in interdisziplinären Projekten; Bedarfsanalyse; Anwendung der in den Fachmodulen erworbenen, multidisziplinären Fähigkeiten zur Identifikation und zur Lösung von Problemen aus der realen Welt.
Wofür braucht man es? Der Hackathon stärkt die Fähigkeit, unter Zeitdruck tragfähige Lösungsansätze zu entwickeln, Prototypen zu erstellen und technische Ergebnisse überzeugend zu vermitteln.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Wahlpflichtmodule

Der Modulbereich Wahlmodule ermöglicht den Studierenden eine individuelle fachliche Vertiefung innerhalb der Digitalen Forensik und angrenzender Sicherheitsfelder. Die Module erweitern das Pflichtcurriculum um spezialisierte Themen wie Malware-Analyse, Speichermedienforensik, Embedded Systems, Werkzeugentwicklung, Künstliche Intelligenz, Eingriffsrecht und IoT-Security.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können ausgewählte Spezialgebiete der Digitalen Forensik und IT-Sicherheit vertieft analysieren, geeignete Methoden und Werkzeuge anwenden und fachliche Ergebnisse für anspruchsvollere Untersuchungs- oder Sicherheitskontexte aufbereiten.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Modulbereich je nach Wahl
  - Malware statisch und dynamisch analysieren,
  - Speichermedien und Dateisysteme forensisch untersuchen,
  - eingebettete Systeme und IoT-Umgebungen sichern und analysieren,
  - eigene Werkzeuge zur Auswertung digitaler Spuren entwickeln,
  - KI-Verfahren auf forensische Fragestellungen anwenden und kritisch reflektieren,
  - besondere Rechtsfragen des Eingriffsrechts und IoT-Sicherheitsfragen bearbeiten.
- **WOZU**: Damit sie ein individuelles Kompetenzprofil aufbauen und sich gezielt auf spezialisierte Aufgabenfelder der Digitalen Forensik, Cyberabwehr, Sicherheitsanalyse oder Ermittlungsunterstützung vorbereiten können. Der Modulbereich eröffnet fachliche Vertiefung über das Pflichtcurriculum hinaus.

Kurzporträt Wahlpflichtmodule

Worum geht es? Die Wahlmodule bieten vertiefende und spezialisierende Themen der Digitalen Forensik und IT-Sicherheit. Die Studierenden können eigene Schwerpunkte setzen und sich mit aktuellen oder besonders anwendungsnahen Fragestellungen beschäftigen.
Wofür braucht man es? Die Kompetenzen unterstützen die individuelle Profilbildung und bereiten auf spezialisierte Tätigkeiten vor, etwa in Malware-Analyse, Speichermedienforensik, IoT-Security, Werkzeugentwicklung oder rechtlich geprägten Ermittlungsfragen.
Wieso ist es interessant? Der Wahlbereich zeigt die Breite der Digitalen Forensik. Er ermöglicht es, eigene Interessen zu vertiefen und aktuelle technische, rechtliche oder methodische Entwicklungen in das Studium einzubeziehen.

BDF511: Malware-Analyse

Modulverantwortung	Prof. Dr. Martin Grothe	**Lehrperson(en)**	Prof. Dr. Martin Grothe
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Malware Analysis
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF101: Informatik-Grundlagen der Forensik: Rechnerarchitektur, Datenrepräsentation und Algorithmen.
- BDF103: Programmierung: Programmierkonzepte, Softwareanalyse und Tests.
- BDF201: Betriebssysteme: Anwendung: Betriebssystemnutzung, Administration und Scripting.
- BDF205: IT-Sicherheit: Angriffsarten, Schutzmechanismen und Systemsicherheit.
- BDF301: Betriebssysteme: Technik: Prozesse, Speicher, Dateisysteme, Systemcalls und Betriebssystemarchitekturen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Malware klassifizieren, statisch und dynamisch analysieren und Ergebnisse für Erkennung und Gegenmaßnahmen auswerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- verschiedenen Arten von Malware zu klassifizieren und deren Eigenschaften bezüglich Funktion, Verbreitung und Stealth-Techniken zu benennen
- Malware statisch und dynamisch zu analysieren
- Quellcode abzuleiten und die Funktionsweise und Ziele der Software zu verstehen
- Tools und Techniken der Malware Analyse (Debugger, Disassembler, Emulatoren) zu kennen und einzusetzen
- Erkennungsmechanismen und Gegenmaßnahmen zu entwickeln

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einführung in die Thematik (Definition, Klassifikation, Eigenschaften, Funktionsweise)
- Informationstechnische Grundlagen (Betriebssysteme, Dateiformate, Programmaufbau, Systemcalls)
- Technische Grundlagen der Malware (Stealth-Techniken, Verschlüsselung)
- Werkzeuge (Disassembler, Debugger, Emulator)
- Reverse Engineering (Disassembling, Decompiling)
- Statische Analyse über Quellcode-Untersuchung
- Dynamische Analyse (Runtime-Debugging)
- Verhaltensanalyse

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Michael Sikorski und Andrew Honig: Practical Malware Analysis, No Starch Press, San Francisco, 2012
- Monnappa K. A.: Learning Malware Analysis, Packt Publishing, Birmingham, 2018
- Eldad Eilam: Reversing: Secrets of Reverse Engineering, Wiley, Indianapolis, 2005
- Alexey Kleymenov und Amr Thabet: Mastering Malware Analysis, Packt Publishing, Birmingham, 2022

Kurzporträt BDF511: Malware-Analyse

Worum geht es? Dieses Modul behandelt Malware-Analyse im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einführung in die Thematik (Definition, Klassifikation, Eigenschaften, Funktionsweise), informationstechnische Grundlagen wie Betriebssysteme, Dateiformate, Programmaufbau und Systemcalls sowie technische Grundlagen der Malware.
Wofür braucht man es? Malware-Analyse hilft, Schadsoftware zu verstehen, Indikatoren abzuleiten und technische Befunde für Erkennung, Reaktion und forensische Bewertung nutzbar zu machen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF512: Forensik von Speichermedien

Modulverantwortung	Prof. Dr. Peter Davids	**Lehrperson(en)**	Prof. Dr. Peter Davids Dr. Bastian Feldkeller
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Storage Media Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF104: Einführung in die Digitale Forensik: forensisch saubere Beweissicherung und Dokumentation.
- BDF204: Forensische Methoden und Werkzeuge: Akquise und Auswertung von Datenträgern.
- BDF301: Betriebssysteme: Technik: Dateisysteme, Datenträgerverschlüsselung, Backup/Recovery und Betriebssystemartefakte.
- BDF401: Betriebssysteme: Forensik: Extraktion und Analyse betriebssystembezogener digitaler Spuren.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Dateisysteme und Speichermedien forensisch untersuchen, relevante Daten extrahieren und Analyseergebnisse dokumentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- mittels fundierter Kenntnisse zu aktuellen Dateisystemen Quellen für forensische Analyse relevante Daten in diesen Dateisystemen zu finden
- für forensische Analyse relevante Daten zu extrahieren
- tiefgreifende forensische Untersuchungen auf Speichermedien durchzuführen, zu dokumentieren und zu interpretieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- grundlegende Konzepte von Dateisystemen
- Relevanz von Dateisystemen für verschiedene Klassen von Speichermedien (Festplatten, Speicherkarten/-sticks, Heimassistenten, Armbänder, Uhren)
- Aufbau und Architektur ausgewählter Dateisysteme (zum Beispiel NTFS, ext4, APFS, ZFS)
- Ablageorte forensisch relevanter Information und deren Extraktion und Sicherung

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Brian Carrier: File System Forensic Analysis, Addison-Wesley, Boston, 2005
- Bruce Nikkel: Practical Linux Forensics: A Guide for Digital Investigators, No Starch Press, San Francisco, 2021
- Eoghan Casey: Digital Evidence and Computer Crime, Academic Press, Waltham, 2011
- Joachim Metz: libyal Documentation and File Format Notes, libyal project, 2024, https://github.com/libyal

Kurzporträt BDF512: Forensik von Speichermedien

Worum geht es? Dieses Modul behandelt Forensik von Speichermedien im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere grundlegende Konzepte von Dateisystemen; Relevanz von Dateisystemen für verschiedene Klassen von Speichermedien (Festplatten, Speicherkarten/-sticks, Heimassistenten, Armbänder, Uhren); Aufbau und Architektur ausgewählter Dateisysteme (zum Beispiel NTFS, ext4, APFS, ZFS).
Wofür braucht man es? Speichermedienforensik ist wichtig, um Dateisysteme, gelöschte Daten und speicherbezogene Artefakte systematisch zu untersuchen und nachvollziehbar zu dokumentieren.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF513: Embedded Systems Forensik

Modulverantwortung	Prof. Dr. Matteo Zella	**Lehrperson(en)**	Prof. Dr. Jürgen Quade Prof. Dr. Matteo Zella
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Embedded Systems Forensics
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF201: Betriebssysteme: Anwendung: grundlegende Betriebssystembedienung, Administration und Scripting.
- BDF205: IT-Sicherheit: Sicherheitsziele, Angriffsarten und Schutzmechanismen.
- BDF302: Rechnernetze und Rechnernetzsicherheit: Netzwerkprotokolle, Dienste und Netzwerksicherheit.
- BDF401: Betriebssysteme: Forensik: Sicherung und Auswertung betriebssystembezogener Artefakte.
- BDF402: Netzwerkforensik: Analyse von Netzwerkkommunikation und Kommunikationsartefakten.
- BDF404: Angewandte Kryptografie: Verschlüsselung, Signaturen und kryptografische Schutzmechanismen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können eingebettete Systeme und IoT-Systeme forensisch sichern, analysieren und die gewonnenen Spuren dokumentieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Eingebettete Systeme in die Kategorien Deeply Embedded und Open Embedded zu klassifizieren und Unterschiede zu Standardsystemen benennen zu können,
- Technische Basiskonzepte, Sicherheitsarchitekturen, Betriebsabläufe und Kommunikationsprotokolle, die im Bereich eingebetteter Systeme und IoT Anwendung finden, zu beschreiben,
- Eingebettete Systeme zur forensischen Analyse sicherzustellen und von diesen relevante Daten zu extrahieren,
- Werkzeuge zur forensischen Analyse einzusetzen,
- Datenspuren der Systeme statisch zu untersuchen
- das Verhalten aktiver Systeme und der Kommunikation über verschiedene Protokolle zu beobachten und auszuwerten
- Ergebnisse der forensischen Analyse zu dokumentieren und zu präsentieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagen und Architektur Eingebetteter- und IoT-Systeme (Klassifizierung: Deeply-Embedded, Open-Embedded, Besonderheiten)
- Technische Basiskonzepte (Sicherheitsarchitekturen, Betriebsabläufe wie Bootprozess, Updateprozess oder Normalbetrieb, spezifische Kommunikationsprotokolle wie beispielsweise LoraWAN, IoT - Technologien)
- Möglichkeiten der Sicherstellung und der Daten-Extraktion
- Statische Analyse (Logdateien, Speicheranalyse)
- Dynamische Analyse (Aktive Prozesse, Kommunikationsbeziehungen, Debugging)
- Verhaltens Analyse (z.B. über Kommunikation)
- Dokumentation und Präsentation

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- David Kleidermacher und Mike Kleidermacher: Embedded Systems Security, Elsevier, Amsterdam, 2012
- Joseph Yiu: The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors, Newnes, Oxford, 2013
- Michael Barr und Anthony Massa: Programming Embedded Systems, O'Reilly Media, Sebastopol, 2006
- NIST: Foundational Cybersecurity Activities for IoT Device Manufacturers, NISTIR 8259, Gaithersburg, 2020, https://doi.org/10.6028/NIST.IR.8259

Kurzporträt BDF513: Embedded Systems Forensik

Worum geht es? Dieses Modul behandelt Embedded Systems Forensik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Grundlagen und Architektur Eingebetteter- und IoT-Systeme (Klassifizierung: Deeply-Embedded, Open-Embedded, Besonderheiten); Technische Basiskonzepte (Sicherheitsarchitekturen, Betriebsabläufe wie Bootprozess, Updateprozess oder Normalbetrieb, spezifische Kommunikationsprotokolle wie beispielsweise LoraWAN, IoT - Technologien); Möglichkeiten der Sicherstellung und der Daten-Extraktion.
Wofür braucht man es? Embedded-Systems-Forensik erweitert forensische Methoden auf Geräteklassen, in denen Speicher, Schnittstellen und Kommunikationsprotokolle anders funktionieren als bei Standardsystemen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF514: Erstellung forensischer Werkzeuge

Modulverantwortung	Prof. Dr. Jens Brandt	**Lehrperson(en)**	Prof. Dr. Jens Brandt Prof. Dr. Nils Kopal
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Development of Forensic Tools
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF103: Programmierung: Python, strukturierte Programmentwicklung, Tests und Softwareanalyse.
- BDF201: Betriebssysteme: Anwendung: Betriebssystemdienste, Kommandozeile, Dateisystem und Scripting.
- BDF204: Forensische Methoden und Werkzeuge: forensische Arbeitsabläufe, Datenquellen und Werkzeugnutzung.
- BDF205: IT-Sicherheit: sicherheitsbezogene Anforderungen an Software und Werkzeuge.
- BDF302: Rechnernetze und Rechnernetzsicherheit: Netzwerkprotokolle und Netzwerkverkehr als Grundlage für die Auswertung von Netzwerkdaten.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können eigene Skripte und Werkzeuge zur Auswertung digitaler Spuren entwickeln, testen und in forensische Arbeitsabläufe integrieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- mit Skriptsprachen wie Python oder Lua Programme zur Auswertung digitaler Spuren zu schreiben,
- mit den erstellten Programmen Dienste des Betriebssystems zu nutzen,
- fortgeschrittene Konzepte zur Auswertung von Log-Dateien, Analyse verschiedener Dateiformate oder von Netzwerktraffic und das Auswerten von Netzwerkprotokollen in Software umsetzen zu können
- Werkzeuge zur Datenanalyse, Extraktion von Informationen und zur Automatisierung von Prozessen zu entwickeln
- Skripte in vorhandene Werkzeuge wie beispielsweise Wireshark zu integrieren
- Skripte zu debuggen und zu testen, um sicherzustellen, dass sie korrekt und effektiv funktionieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Einführung in Skriptsprachen wie beispielsweise Python und Lua
- Parsing von Log-Dateien, Extraktion von Daten aus verschiedenen Dateiformaten wie z.B. CSV, JSON, XML
- Verarbeitung von Datenpaketen, Extraktion von Metadaten und anderen Informationen
- Erstellung von Skripten zur Automatisierung von Aufgaben und Prozessen
- Methoden und Möglichkeiten zur Datenanalyse und -visualisierung
- Integration von Skripten mit anderen Tools und Frameworks, wie z.B. Datenbanken und anderen Forensik-Tools
- Verwendung von Debugging-Tools und Techniken, Schreiben von Unit-Tests und Durchführen von manuellen Tests
- IT-Sicherheitstechnische Aspekte der Programmierung und Einsatz in der Praxis

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Preston Miller und Chapin Bryce: Learning Python for Forensics, Packt Publishing, Birmingham, 2019
- Chet Hosmer: Python Forensics, Syngress, Waltham, 2014
- David Beazley und Brian K. Jones: Python Cookbook, O'Reilly Media, Sebastopol, 2013
- Al Sweigart: Automate the Boring Stuff with Python, No Starch Press, San Francisco, 2019

Kurzporträt BDF514: Erstellung forensischer Werkzeuge

Worum geht es? Dieses Modul behandelt Erstellung forensischer Werkzeuge im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Einführung in Skriptsprachen wie beispielsweise Python und Lua; Parsing von Log-Dateien, Extraktion von Daten aus verschiedenen Dateiformaten wie z.B. CSV, JSON, XML; Verarbeitung von Datenpaketen, Extraktion von Metadaten und anderen Informationen.
Wofür braucht man es? Eigene Werkzeuge ermöglichen wiederholbare Auswertungen, passgenaue Datenextraktion und die Automatisierung forensischer Arbeitsschritte in konkreten Untersuchungssituationen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF515: KI in der Cyberkriminalistik

Modulverantwortung	Prof. Dr. Jürgen Quade	**Lehrperson(en)**	Prof. Dr. Jürgen Quade Prof. Dr. Michael Gref Prof. Dr. Duc Duy Pham
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	AI in Cybercrime Investigation
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF102: Ethische und Menschliche Aspekte der Informationssicherheit: ethische Bewertung automatisierter Entscheidungen, Bias und verantwortlicher Umgang mit sensiblen Daten.
- BDF103: Programmierung: Python-Grundlagen, Bibliotheksnutzung und einfache Implementierung datenverarbeitender Programme.
- BDF305: Datenbanken-Forensik: datenbezogene Analyseaufgaben, strukturierte Datenquellen und forensische Auswertung größerer Datenbestände.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Methoden der Künstlichen Intelligenz auf forensische Fragestellungen anwenden und deren Grenzen, Risiken und Einsatzbedingungen kritisch reflektieren.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Grundlagen der KI (insb. Decision Trees, Neuronale Netze, LLMs) erklären und auf forensische Problemstellungen anwenden
- Praktische KI-Werkzeuge (z.B. Python, Scikit-learn, TensorFlow, YOLO, LLM-APIs) für forensische Analysen nutzen (z.B. Bilderkennung in Beweismitteln, Textanalyse in Logfiles)
- Grenzen und Risiken von KI in der Forensik kritisch reflektieren (z.B. Bias, Overfitting, Halluzinationen bei LLMs)
- Einfache KI-Modelle (z.B. Decision Trees, Tiny-LLMs) selbst implementieren und trainieren
- Prompt-Engineering und LLM-APIs für forensische Recherche oder Datenaufbereitung einsetzen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Praktische KI-Programmierung: Python-Bibliotheken (z.B. Pandas, NumPy, Scikit-learn), Jupyter Notebooks
- Decision Trees & Neuronale Netze: Aufbau, Training, Anwendung auf forensische Datensätze (z.B. Klassifikation von Angriffsmustern)
- Objekterkennung: YOLO für Bild-/Videoforensik (z.B. Erkennung von Tatwerkzeugen)
- Large Language Models (LLMs): Architektur, Training, Einsatz in der Forensik (z.B. Auswertung von Chatprotokollen, automatisiertes Reporting)
- Ethik & Risiken: Diskussion von Fehlerquellen, Datenschutz, Manipulationsgefahren

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 90 Minuten

Literatur

- Stuart Russell und Peter Norvig: Artificial Intelligence: A Modern Approach, Pearson, Hoboken, 2021
- Aurélien Géron: Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, O'Reilly Media, Sebastopol, 2022
- Ian Goodfellow, Yoshua Bengio und Aaron Courville: Deep Learning, MIT Press, Cambridge, 2016, https://www.deeplearningbook.org/
- Christopher M. Bishop und Hugh Bishop: Deep Learning: Foundations and Concepts, Springer, Cham, 2024, https://doi.org/10.1007/978-3-031-45468-4

Kurzporträt BDF515: KI in der Cyberkriminalistik

Worum geht es? Dieses Modul behandelt KI in der Cyberkriminalistik im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Praktische KI-Programmierung: Python-Bibliotheken (z.B. Pandas, NumPy, Scikit-learn), Jupyter Notebooks; Decision Trees & Neuronale Netze: Aufbau, Training, Anwendung auf forensische Datensätze (z.B. Klassifikation von Angriffsmustern); Objekterkennung: YOLO für Bild-/Videoforensik (z.B. Erkennung von Tatwerkzeugen).
Wofür braucht man es? KI-Kompetenzen helfen, datenintensive forensische Aufgaben zu unterstützen und zugleich Risiken wie Verzerrungen, Fehlklassifikationen oder nicht nachvollziehbare Ergebnisse kritisch zu bewerten.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF516: Besondere Rechtsfragen im Eingriffsrecht

Modulverantwortung	Prof. Dr. Nils Kopal	**Lehrperson(en)**	Dr. Sinan Eroglu
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	Special Legal Issues in Intervention Law
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF105: Rechtliche Grundlagen der Cyberkriminalistik: Grundrechte, Strafrecht, Strafprozessrecht, Datenschutz und juristische Fallbearbeitung.
- BDF203: Einführung in die Kriminalistik: Ermittlungsverfahren, Beweisführung und kriminalistische Bewertung von Spuren.
- BDF205: IT-Sicherheit: Verschlüsselung, Authentifizierung, Kommunikationssicherheit und sicherheitsbezogene technische Rahmenbedingungen.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können besondere Rechtsfragen des Eingriffsrechts, insbesondere zur Telekommunikationsüberwachung, fallbezogen einordnen und gutachterlich bearbeiten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die verfassungsrechtlichen Grundlagen der Telekommunikationsüberwachung (Art. 10 GG, Rechtsprechung des BVerfG, EMRK) kennen und anwenden können,
- die einschlägigen einfachgesetzlichen Regelungen (insb. §§ 100a ff. StPO, Polizeigesetz NRW, TKÜV) sicher beherrschen,
- zwischen repressiven und präventiv-polizeilichen Befugnissen differenzieren können,
- typische Problemfelder wie Kernbereichsschutz, Verhältnismäßigkeit, Datenverwertung und Transparenzpflichten rechtlich einordnen,
- praktische Handlungssicherheit im Umgang mit TKÜ-Maßnahmen entwickeln (Ablauf, Zuständigkeiten, Dokumentationspflichten),
- aktuelle Entwicklungen (z. B. Quellen-TKÜ, digitale Kommunikation, Verschlüsselung) kritisch reflektieren,
- gutachterliche Falllösungen erstellen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Strafprozessuale TKÜ-Befugnisse: Voraussetzungen, Katalogtaten, Richtervorbehalt, Dauer und Dokumentation (§§ 100a–100f StPO)
- Polizeirechtliche TKÜ-Befugnisse: Rechtsgrundlagen im PolG NRW, präventiv-polizeiliche Zielrichtungen, Abgrenzung zu repressiven Maßnahmen
- Rechtsprechung: Leitentscheidungen des BVerfG und des BGH (z. B. Urteil zur Quellen-TKÜ 2008, Entscheidung zu Online-Durchsuchungen 2008)
- Technische und praktische Umsetzung: Abläufe, Zuständigkeiten, Kooperation mit TK-Anbietern, Beweisverwertung
- Datenschutzrechtliche Aspekte: Löschung, Zweckbindung, Informationspflichten, Kernbereichsschutz
- Aktuelle Herausforderungen: Messenger-Dienste, Verschlüsselung, Ende-zu-Ende-Kommunikation, europäische Entwicklungen

Prüfungsvorleistung

Keine

Prüfungsleistung

Klausur, 120 Minuten

Literatur

- Lutz Meyer-Goßner und Bertram Schmitt: Strafprozessordnung mit GVG und Nebengesetzen, C.H.Beck, München, 2024
- Rolf Hannich: Karlsruher Kommentar zur Strafprozessordnung, C.H.Beck, München, 2023
- Ulrich Sieber, Nicolas von zur Mühlen und Jan Pohle: Cybercrime und Strafrecht in der Informationsgesellschaft, Duncker & Humblot, Berlin, 2021
- Dirk Heckmann und Anne Paschke: juris PraxisKommentar Internetrecht, juris, Saarbrücken, 2024

Kurzporträt BDF516: Besondere Rechtsfragen im Eingriffsrecht

Worum geht es? Dieses Modul behandelt Besondere Rechtsfragen im Eingriffsrecht im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Strafprozessuale TKÜ-Befugnisse: Voraussetzungen, Katalogtaten, Richtervorbehalt, Dauer und Dokumentation (§§ 100a–100f StPO); Polizeirechtliche TKÜ-Befugnisse: Rechtsgrundlagen im PolG NRW, präventiv-polizeiliche Zielrichtungen, Abgrenzung zu repressiven Maßnahmen; Rechtsprechung: Leitentscheidungen des BVerfG und des BGH (z. B. Urteil zur Quellen-TKÜ 2008, Entscheidung zu Online-Durchsuchungen 2008).
Wofür braucht man es? Eingriffsrechtliche Kenntnisse sind notwendig, um Überwachungsmaßnahmen, Beweisverwertung und technische Ermittlungsbefugnisse rechtssicher einzuordnen.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF519: IoT-Security

Modulverantwortung	Prof. Dr. Thomas Meuser	**Lehrperson(en)**	Prof. Dr. Jörg Helbach
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Wahl	**Sprache**	Deutsch
Angebot	Wintersemester	**Dauer**	1 Semester
Credits	5 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	2 V | 2 Ü | - P | - S	**Engl. Titel**	IoT Security
Workload	• Präsenz: 45 Std. • Selbst: 90 Std.		

Empfohlene Voraussetzungen

- BDF103: Programmierung: grundlegende Programmierkonzepte und Softwareentwicklungswerkzeuge als Basis hardwarenaher Entwicklung.
- BDF201: Betriebssysteme: Anwendung: Betriebssystemnutzung, Administration und Scripting.
- BDF205: IT-Sicherheit: Bedrohungen, Schutzmaßnahmen und Sicherheitsarchitekturen.
- BDF302: Rechnernetze und Rechnernetzsicherheit: Netzwerkprotokolle, Dienste, Routing und Netzwerksicherheit.
- BDF404: Angewandte Kryptografie: Verschlüsselung, Authentifizierung und kryptografische Schutzmechanismen für vernetzte Systeme.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können Sicherheitsrisiken von IoT-Systemen analysieren und grundlegende Schutzmaßnahmen praktisch konfigurieren und bewerten.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- Die grundlegenden Konzepte und Herausforderungen der IoT-Sicherheit verstehen
- Sicherheitsrisiken und Angriffsszenarien für IoT-Geräte identifizieren und bewerten können
- Praktische Fähigkeiten zur Implementierung und Konfiguration von Sicherheitsmaßnahmen in IoT-Geräten entwickeln
- Wissen über aktuelle Technologien und Best Practices im Bereich der IoT-Sicherheit besitzen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Grundlagen, Architektur und typische Einsatzszenarien von IoT-Systemen
- Vernetzung, Kommunikationsprotokolle und Betriebsmodelle von IoT-Geräten
- Sicherheitsrisiken, Bedrohungen und Angriffsszenarien im Internet der Dinge
- Sicherheitsmaßnahmen und Best Practices zur Absicherung von IoT-Geräten
- Praktische Arbeit mit Arm-Cortex-M-Prozessoren und Echtzeitbetriebssystemen
- Bewertung und Dokumentation von Schutzmaßnahmen in konkreten IoT-Umgebungen

Prüfungsvorleistung

Keine

Prüfungsleistung

Studien-, Projekt- oder Hausarbeit (10 - 15 Seiten)

Literatur

- Brian Russell und Drew Van Duren: Practical Internet of Things Security, Packt Publishing, Birmingham, 2018
- ENISA: Baseline Security Recommendations for IoT, European Union Agency for Cybersecurity, Heraklion, 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
- NIST: IoT Device Cybersecurity Capability Core Baseline, NISTIR 8259A, Gaithersburg, 2020, https://doi.org/10.6028/NIST.IR.8259A
- Joseph Yiu: The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors, Newnes, Oxford, 2013

Kurzporträt BDF519: IoT-Security

Worum geht es? Dieses Modul behandelt IoT-Security im Kontext vernetzter eingebetteter Systeme. Im Mittelpunkt stehen Architektur, Kommunikation und Absicherung von IoT-Geräten sowie praktische Untersuchungen an hardwarenahen Plattformen.
Wofür braucht man es? IoT-Sicherheitskompetenzen werden benötigt, um vernetzte Geräte, Sensoren und eingebettete Systeme gegen typische Angriffe abzusichern und sicherheitsrelevante Schwachstellen fundiert zu bewerten.
Wieso ist es interessant? IoT-Geräte verbinden Software, Hardware und Netzwerke auf engem Raum. Dadurch entstehen Sicherheitsfragen, bei denen technische Details unmittelbare Auswirkungen auf reale Umgebungen haben.

Praxisphase und Bachelorarbeit

Der Modulbereich Praxisphase und Bachelorarbeit befähigt die Studierenden, die im Studium erworbenen Kompetenzen in berufspraktischen und wissenschaftlich-anwendungsorientierten Kontexten eigenständig einzusetzen. Dabei entwickeln sie ihre Fähigkeit weiter, komplexe Aufgaben zu planen, durchzuführen, zu dokumentieren, zu reflektieren und fachlich zu verteidigen.

Zusammenfassung der Lernziele / Kompetenzen

- **WAS**: Die Studierenden können forensische, sicherheitsbezogene oder informatische Aufgabenstellungen in der Praxis bearbeiten und eine eigenständige wissenschaftlich orientierte Abschlussarbeit planen, umsetzen, dokumentieren, präsentieren und im Fachgespräch begründen.
- **WOMIT**: Die Studierenden erreichen dieses Lernergebnis, indem sie im Modulbereich
  - in Dienststellen, Unternehmen oder Organisationen an konkreten Aufgaben aus Cyber Security und Digitaler Forensik mitarbeiten,
  - berufliche Arbeitsabläufe, Kommunikation und organisatorische Zusammenhänge reflektieren,
  - eine praxisorientierte Aufgabenstellung selbstständig nach wissenschaftlichen und anwendungsorientierten Methoden bearbeiten,
  - Ergebnisse schriftlich dokumentieren und mündlich präsentieren,
  - Vorgehen, Lösungsansätze und Ergebnisse im Kolloquium fachlich begründen und diskutieren.
- **WOZU**: Damit sie den Übergang vom Studium in berufliche oder weiterführende wissenschaftliche Tätigkeiten fundiert gestalten können. Der Modulbereich führt Fachkompetenz, Selbstorganisation, wissenschaftliches Arbeiten, Praxisbezug und Kommunikation auf Abschlussniveau zusammen.

Kurzporträt Praxisphase und Bachelorarbeit

Worum geht es? In Praxisphase und Bachelorarbeit wenden die Studierenden ihre Kompetenzen in realen oder realitätsnahen Aufgabenstellungen an. Sie arbeiten in beruflichen Kontexten mit, bearbeiten eine eigenständige Abschlussaufgabe und stellen ihre Ergebnisse nachvollziehbar dar.
Wofür braucht man es? Diese Module zeigen, dass Studierende fachliche, methodische und kommunikative Kompetenzen eigenständig einsetzen können. Sie bereiten auf berufliche Aufgaben in Digitaler Forensik, Cyber Security und angrenzenden IT-Feldern vor.
Wieso ist es interessant? Der Bereich verbindet Studium und Praxis unmittelbar. Die Studierenden bearbeiten konkrete Fragestellungen, erleben berufliche Anforderungen und zeigen mit der Bachelorarbeit, dass sie ein Thema selbstständig wissenschaftlich und anwendungsbezogen durchdringen können.

BDF601: Praxisphase und begleitendes Seminar

Modulverantwortung	Studiendekan:in	**Lehrperson(en)**	Alle Lehrende des Studiengangs
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Jedes Studienjahr	**Dauer**	1 Semester
Credits	15 ECTS	**Benotung**	unbenotet
SWS	V | - Ü | - P | 1 S	**Engl. Titel**	Practical Phase and Accompanying Seminar
Workload	450 Stunden		

Empfohlene Voraussetzungen

- BDF101-BDF106: Module des ersten Fachsemesters: informatische, ethische, programmiertechnische, forensische, rechtliche und projektbezogene Grundlagen.
- BDF201-BDF206: Module des zweiten Fachsemesters: Betriebssystemanwendung, OSINT, Kriminalistik, forensische Methoden, IT-Sicherheit und Mikroprojektkompetenzen.
- BDF301-BDF306: Module des dritten Fachsemesters: Betriebssystemtechnik, Rechnernetze, digitale Tatorte, Web- und Browsersicherheit, Datenbanken-Forensik und Incident Management.
- BDF401-BDF405: Module des vierten Fachsemesters: Betriebssystemforensik, Netzwerkforensik, Geschäftsmodelle im Internet, Kryptografie und projektförmige forensische Fallbearbeitung.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können erworbene Kompetenzen in einer berufspraktischen Aufgabenstellung anwenden, Arbeitsprozesse koordinieren und Praxiserfahrungen reflektiert darstellen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- zu erkennen, wie bestimmte berufliche Tätigkeiten in den organisatorischen und sozialen Zusammenhang eines Unternehmens oder einer Organisation einzuordnen sind
- Kommunikation mit Kolleg:Innen und Vorgesetzen im beruflichen Umfeld zu führen
- Routineaufgaben, die eigenen Projektarbeiten und die im Berufsalltag ad hoc anfallenden Tätigkeiten für sich zu koordinieren

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Die Studierenden werden durch praktische Mitarbeit in Dienststellen, Unternehmen und Organisationen an die Berufspraxis und ihre zukünftige berufliche Tätigkeit herangeführt. Sie wenden ihre erworbenen Kenntnisse und Fähigkeiten auf konkrete vom Unternehmen formulierte und vom betreuenden Professor akzeptierte Aufgabenstellungen im Bereich Cyber Security, insb. der Digitalen Forensik an. Die Studierende sollen beruflichen Alltag mit Routineaufgaben, Kommunikation mit anderen Mitarbeiter:Innen und der Bearbeitung eigener Aufgabenstellungen erleben

Prüfungsvorleistung

Keine

Prüfungsleistung

Testat

Literatur

- Die verwendete aktuelle Literatur orientiert sich an den vom Unternehmen formulierten Aufgabenstellungen

Kurzporträt BDF601: Praxisphase und begleitendes Seminar

Worum geht es? Dieses Modul behandelt Praxisphase und begleitendes Seminar im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Die Studierenden werden durch praktische Mitarbeit in Dienststellen, Unternehmen und Organisationen an die Berufspraxis und ihre zukünftige berufliche Tätigkeit herangeführt. Sie wenden ihre erworbenen Kenntnisse und Fähigkeiten auf konkrete vom Unternehmen formulierte und vom betreuenden Professor akzeptierte Aufgabenstellungen im Bereich Cyber Security, insb. der Digitalen Forensik an. Die Studierende sollen beruflichen Alltag mit Routineaufgaben, Kommunikation mit anderen Mitarbeiter:Innen und der Bearbeitung eigener Aufgabenstellungen erleben.
Wofür braucht man es? Die Praxisphase verbindet Studium und Berufspraxis und zeigt, wie fachliche Kompetenzen in realen Organisationen, Abläufen und Kommunikationssituationen eingesetzt werden.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

BDF602: Bachelorarbeit und Kolloquium

Modulverantwortung	Studiendekan:in	**Lehrperson(en)**	Alle Lehrende des Studiengangs
Verwendbarkeit	Bachelor Digitale Forensik	**Fächergruppe**	Informatik
Modultyp	Pflicht	**Sprache**	Deutsch
Angebot	Jedes Studienjahr	**Dauer**	1 Semester
Credits	15 ECTS	**Benotung**	Deutsche Notenskala 1-5
SWS	V | - Ü | 6 P | - S	**Engl. Titel**	Bachelor's Thesis and Colloquium
Workload	450 Stunden		

Empfohlene Voraussetzungen

- BDF101-BDF106: Module des ersten Fachsemesters: informatische, ethische, programmiertechnische, forensische, rechtliche und projektbezogene Grundlagen.
- BDF201-BDF206: Module des zweiten Fachsemesters: Betriebssystemanwendung, OSINT, Kriminalistik, forensische Methoden, IT-Sicherheit und Mikroprojektkompetenzen.
- BDF301-BDF306: Module des dritten Fachsemesters: Betriebssystemtechnik, Rechnernetze, digitale Tatorte, Web- und Browsersicherheit, Datenbanken-Forensik und Incident Management.
- BDF401-BDF405: Module des vierten Fachsemesters: Betriebssystemforensik, Netzwerkforensik, Geschäftsmodelle im Internet, Kryptografie und projektförmige forensische Fallbearbeitung.
- BDF505-BDF519: Wahl- und Vertiefungsmodule des fünften Modulblocks: spezialisierte Kompetenzen passend zum Thema der Bachelorarbeit.

Lernergebnisse / Kompetenzen

WAS. Die Studierenden können eine praxisorientierte wissenschaftliche Aufgabenstellung selbstständig bearbeiten, dokumentieren, präsentieren und fachlich verteidigen.

WOMIT. Die Studierenden erreichen dieses Lernergebnis, indem sie insbesondere folgende im PDF genannten Kompetenzen aufbauen:

- die erlernten Fachkenntnisse und wissenschaftliche Methoden im Rahmen einer konkreten anwendungsorientierten Themenstellung selbstständig anzuwenden
- die Umsetzung der eigenen Arbeitsergebnisse zu beurteilen
- eigenverantwortliches Handeln auf Grundlage einer selbständigen Projektorganisation zu zeigen
- die Untersuchungen und Ergebnisse der Bachelorarbeit verständlich zu präsentieren,
- die betrachteten Lösungsansätze in einer fachwissenschaftlichen Diskussion zu erläutern
- die gewählte Vorgehensweise zur Bearbeitung der Problemstellung zu begründen

WOZU. Damit sie in späteren Modulen, Projekten und beruflichen Aufgaben der Digitalen Forensik fachliche Entscheidungen begründet treffen, digitale Sachverhalte systematisch untersuchen und Ergebnisse nachvollziehbar kommunizieren können.

Inhalte

- Die Bachelorarbeit soll zeigen, dass der Prüfling befähigt ist, innerhalb einer vorgegebenen Frist von höchstens drei Monaten eine praxisorientierte Aufgabenstellung aus einem Fachgebiet des Studiengangs sowohl in fachlichen Einzelheiten als auch in fachübergreifenden Zusammenhängen nach wissenschaftlichen und anwendungsorientierten Methoden selbständig zu bearbeiten. Das abschließende Kolloquium dient der Feststellung, ob der Prüfling befähigt ist, die Ergebnisse der Bachelorarbeit, ihre fachlichen Zusammenhänge und außerfachlichen Bezüge mündlich darzustellen, selbständig zu begründen und ihre Bedeutung für die Praxis einzuschätzen

Prüfungsvorleistung

Keine

Prüfungsleistung

Benotete Prüfung – Abschlussarbeit (40-70 Seiten) mit Kolloquium (mündliche Prüfung, 30-45 Minuten)

Literatur

- Die verwendete aktuelle Literatur orientiert sich an den vom Unternehmen oder der Organisation formulierten Aufgabenstellung

Kurzporträt BDF602: Bachelorarbeit und Kolloquium

Worum geht es? Dieses Modul behandelt Bachelorarbeit und Kolloquium im Kontext der Digitalen Forensik. Im Mittelpunkt stehen insbesondere Die Bachelorarbeit soll zeigen, dass der Prüfling befähigt ist, innerhalb einer vorgegebenen Frist von höchstens drei Monaten eine praxisorientierte Aufgabenstellung aus einem Fachgebiet des Studiengangs sowohl in fachlichen Einzelheiten als auch in fachübergreifenden Zusammenhängen nach wissenschaftlichen und anwendungsorientierten Methoden selbständig zu bearbeiten. Das abschließende Kolloquium dient der Feststellung, ob der Prüfling befähigt ist, die Ergebnisse der Bachelorarbeit, ihre fachlichen Zusammenhänge und außerfachlichen Bezüge mündlich darzustellen, selbständig zu begründen und ihre Bedeutung für die Praxis einzuschätzen.
Wofür braucht man es? Bachelorarbeit und Kolloquium weisen nach, dass eine fachliche Fragestellung eigenständig bearbeitet, wissenschaftlich dokumentiert und im Fachgespräch verteidigt werden kann.
Wieso ist es interessant? Das Modul verbindet fachliche Grundlagen mit anwendungsnahen Fragestellungen und zeigt, wie die behandelten Konzepte in realen digitalen Untersuchungs- und Sicherheitskontexten wirksam werden.

Glossar

Dieses Glossar erklärt Abkürzungen und wiederkehrende Begriffe, die in den Modulbeschreibungen verwendet werden.

ECTS European Credit Transfer System. Ein ECTS-Punkt (auch „Credit") entspricht etwa 30 Stunden studentischem Arbeitsaufwand (Workload) und ist die europaweit vergleichbare Maßeinheit für den Umfang eines Moduls.

SWS Semesterwochenstunden. Gibt an, wie viele Zeitstunden Lehrveranstaltung pro Woche während der Vorlesungszeit eines Semesters stattfinden, aufgeschlüsselt nach Veranstaltungsart (siehe V, Ü, P, S/SL).

V Vorlesung. Lehrveranstaltungsform, in der fachliche Inhalte überwiegend im Vortrag vermittelt werden.

Ü Übung. Lehrveranstaltungsform zur Vertiefung und Einübung der in der Vorlesung vermittelten Inhalte, häufig anhand von Aufgaben.

P Praktikum. Praktische Lehrveranstaltung, in der Inhalte im Labor oder an Versuchsaufbauten selbst durchgeführt werden.

S Seminar. Lehrveranstaltungsform mit stärker eigenständiger, oft projekt- oder präsentationsorientierter Arbeitsweise.

SL Seminaristischer Unterricht. Lehrveranstaltungsform, die das freie Vortragen von Inhalten (wie in einer Vorlesung) mit dem interaktiven Dialog kombiniert.

Workload Der geschätzte studentische Gesamtarbeitsaufwand für ein Modul, aufgeteilt in Präsenzstudium (Teilnahme an Lehrveranstaltungen) und Selbststudium (eigenständige Vor- und Nachbereitung, Prüfungsvorbereitung).

Modultyp Kennzeichnet, ob ein Modul verpflichtend zu belegen ist (**Pflicht**) oder aus einem Angebot ausgewählt werden kann (**Wahlpflicht**).

WAS / WOMIT / WOZU Format zur Beschreibung von Lernergebnissen: **WAS** die Studierenden nach dem Modul können, **WOMIT** (mit welchen Inhalten und Tätigkeiten) sie dieses Lernergebnis erreichen und **WOZU** sie diese Kompetenzen im weiteren Studium oder Beruf benötigen.

Ziele-Module-Matrix Übersicht, die zeigt, in welchen Modulen die übergreifenden Qualifikationsziele eines Studiengangs aufgebaut und vertieft werden.

Capstone-Modul Abschließendes Modul eines Lernpfads, in dem die zuvor erworbenen fachlichen und methodischen Kompetenzen in einer größeren, integrierenden Projektaufgabe zusammengeführt und angewendet werden.

Lernpfad Thematisch gebündelte Abfolge von Pflichtmodulen, die inhaltlich aufeinander aufbauen und in einem Capstone-Modul münden. Lernpfade orientieren sich an einem typischen Berufs- bzw. Tätigkeitsprofil des Studiengangs.

Kurzporträt Kurzbeschreibung eines Moduls oder Lernpfads entlang der Fragen „Worum geht es¿', „Wofür braucht man es?" und „Wieso ist es interessant?", gedacht als schneller Einstieg für Studierende.