Modulhandbuch

zum

Studiengang

Bachelor Digitale Forensik

16.02.2024

Inhaltsverzeichnis

Qualifikationsziele

Der Studiengang Digitale Forensik hat das Ziel, dass seine Absolventinnen und Absolventen in der Lage sind:

Grundlagen - Basiswissen

- die Grundlagen, den Aufbau und die Funktionsweise von Komponenten, die in der digitalen Forensik eine Rolle spielen wie Rechner, Netzwerke, Systemsoftware und Anwendungen zu verstehen und ihre Bedeutung für forensische Prozesse zu erläutern, [Informatik Grundlagen]
- Konzepte und Prinzipien der Cybersicherheit und der digitalen Forensik zu verstehen und einzusetzen und verschiedene Arten der Cyberkriminalität wie Hackerangriffen, Malware-Infektionen oder Datenlecks zu differenzieren, [fachliche Grundlagen]
- IT-Kriminalität im Sinne der Beweismittelführung und des Betrugs zu bewerten und relevante Prozessabläufe, insbesondere aus dem Bereich Cyberkriminalität, zu kennen, [rechtliche Grundlagen]

Anwendung

- Bedrohungen im Bereich IT-Sicherheit zu identifizieren und geeignete Reaktionen auf Cyberangriffe zu planen (Incident Response) und dabei die Korrektheit, Sicherheit und Angemessenheit einer von ihnen vorgeschlagenen Lösung überzeugend zu begründen,
- Angriffe auf IT-Systeme zu erkennen, diese zu analysieren und passende forensische Vorgehensweisen zu entwickeln und anzuwenden,
- mit wissenschaftlichen Methoden und Technologien digitale Spuren bei Einhaltung rechtlicher und ethischer Prinzipien unter fachgerechtem Einsatz forensischer Werkzeuge zu sichern, zu erfassen, zu untersuchen, zu analysieren, zu dokumentieren und zu präsentieren,

Softskills

- komplexe forensische Projekte zu planen, gemeinsam im Team zu bearbeiten und Teilaufgaben selbständig zu übernehmen,
- fachbezogene Positionen und Problemlösungen zu formulieren, argumentativ zu verteidigen und sich mit Fachvertreterinnen und -vertretern und Personen im beruflichen und wissenschaftlichen Umfeld über Informationen, Ideen, Probleme und Lösungen auszutauschen.

Studiengangarchitektur

Motivation für das Studium

In Gesellschaft, staatlichen Organen und in Unternehmen aller Branchen gibt es bei der aktuell immensen Zunahme von Cyberkriminalität ein stetig wachsender Bedarf an Absolventinnen und Absolventen aus dem Bereich IT-Sicherheit und insbesondere aus dem Themenkomplex ”Digitale Forensik”.

Die Aufklärung von Straftaten, die mittels Informationstechnik begangen werden und sich gegen IT-Infrastrukturen, Daten, Gesellschaft, Unternehmen oder Personen richten, erfordern Spezialisten im Bereich der Cyberabwehr, so wie sie nach unserem Studiengangskonzept ausgebildet werden.

Unsere Studierende erwartet ein anwendungsorientiertes Lernspektrum von den Grundlagen der Informatik, der Netzwerk- und Computertechnik, der Cybersicherheit und der Kriminalistik bis hin zu spezifischen Methoden und Vorgehensweisen zur Gewinnung und Präsentation von forensischen Beweisen, zur Aufklärung von Straftaten aber auch zur Vorbeugung und dem Schutz vor zukünftigen Cyberangriffen.

Kurzbeschreibung des Studienverlaufs

Das Studium der Digitalen Forensik zielt darauf ab, den Studierenden eine solide Grundlage in den Bereichen IT, Cybersicherheit und Kriminalistik zu vermitteln, um digitale Beweise forensisch zu untersuchen, mit den gewonnenen Erkenntnissen Verbrechen aufzuklären und damit auch vor zukünftigen Cyberattacken zu schützen. Das praxisorientierte Studium verknüpft die vermittelte Technik- und Methodenkompetenz stets mit der forensischen Fallarbeit.

Dazu gliedert sich das Studium in ein fachspezifisches Grundlagenstudium (Semester eins und zwei), das anwendungsbezogene Expertenstudium der digitalen Forensik (Semester drei und vier), ein individuelles Vertiefungssemester (Semester fünf) und einer Praxisphase inklusive der Bachelorarbeit (Semester sechs). Absolventinnen und Absolventen können sich im Rahmen wählbarer Module und Themen in den in jedem Semester angeboten Projekten bzw. durch die Praxisphase und ihre Abschlussarbeit ein individuelles fachspezifisches Kompetenzprofil erarbeiten.

Durch das Studium sind Lernpfade gezogen worden, die das Wissen ”von der Breite in die Tiefe” vermitteln. Der Lernpfad Forensik beispielsweise vermittelt die Grundlagen, danach die Anwendung im Alltag der Cyberkriminalisten und schließlich die Optimierung für Experten. Neben dem Lernpfad Forensik gibt es die Lernpfade für Softskills, Betriebssysteme, Netzwerke und Kriminalistik.

Sowohl die Zusammenstellung der für den Abschluss notwendigen Kompetenzen als auch die inhaltliche Gestaltung der Module erfolgt gemeinsam durch die Kompetenzträger (Hochschulen, Forschungseinrichtung, Polizei, Innenministerium). Der Studiengang ist praxisorientiert geplant, was sich an der hohen Anzahl der Prüfungsform ”Studien-, Projekt- oder Hausarbeit” widerspiegelt. Der Schwerpunkt des Studiengangs liegt jeweils auf der Anwendung spezifischer Methoden und Technologien im Zuge der forensischen Prozesse. Bspw. geht es im Modul Kryptografie praxisnah um die Datengewinnung von einem im Zuge einer Strafverfolgung in Beschlag genommenen verschlüsselten Datenträger und nicht um die Erstellung neuer kryptografischer Verfahren.

Um die Plan- und Studierbarkeit zu erhöhen sind die Module formal weitestgehend identisch aufgebaut. Alle Lehr-Module haben einen Umfang von fünf ECTS Punkten, die in vier SWS vermittelt werden. Zwei Unterrichtsstunden sind kombiniert mit zwei Übungsstunden, die aber in vielen Modulen als ”praktische Übung” geplant sind. Als Arbeitsgerät kommt dabei das den Studentinnen und Studenten gehörige Notebook zum Einsatz, so dass wenig Abhängigkeiten zu Geräten in der Hochschule bestehen und damit ein hoher Anteil an mobilen digitalen Lernformen möglich sind. Der potenziell mögliche hohe Anteil dieser digitalen Lernformen ist insbesondere für die im Beruf stehenden Teilzeit-Studierenden notwendig.

Der Studiengang wird in Kooperation von drei Fachbereichen an zwei Hochschulen und einer Forschungseinrichtung konzipiert und durchgeführt. Jeder Kooperationspartner bringt dediziert seine Stärken in der Vermittlung von Methoden, Informatik und Technik sowie der Anwendung ”Digitaler Forensik” in Lehre und Forschung in den Studiengang ein.

Modul	**BDF101 Informatik-Grundlagen der Forensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Jedes Studienjahr	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	1. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: Testat

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- die Struktur des Fachs Informatik und typische Fragestellungen seiner Teilgebiete zu beschreiben
- die Grundlagen, Prinzipien und Grenzen der Informatik zu erläutern
- fundamentale Konzepte der Informatik zu benennen, unterscheiden und auf verschiedene Gegenstandsbereiche zu übertragen
- einfache Informatik-Probleme zu modellieren und Algorithmen zur deren Lösung zu entwickeln
- die Eignung unterschiedlicher Programmierparadigmen und Programmiersprachen für verschiedene Anwendungsaufgaben zu untersuchen und zu beurteilen
- den Unterschied zwischen Übersetzung und Interpretation sowie die Aufgaben eines Laufzeitsystems abzugrenzen und zu erklären
- Korrektheitsbeweise auf der Basis von Schleifeninvarianten zu erklären
- für einfache algorithmische und datenstrukturorientierte Aufgabenstellungen Programme in verschiedenen Programmiersprachen und Programmierparadigmen unter Anwendung angemessener Techniken zu entwickeln
- kleinere Anwendungsprojekte im Team zu bearbeiten

Inhalte:

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

Lehrmethoden:

- Vorlesung, unterstützt durch Skript/Literatur zum Selbststudium. Der Stoff der Vorlesung wird vertieft durch Bearbeitung von Übungsaufgaben.
- Eigenständige, durch Betreuer/in unterstützte, und in Kleingruppen durchgeführte Projektarbeit zur Realisierung eines kleineren Anwendungsprojektes.

Bezug zu anderen Fächern/Modulen:

Literatur: • Vorlesungsunterlagen • Helmut Herold, Bruno Lurz, Jürgen Wolrab, Matthias Hopf: Grundlagen der Informatik. Pearson, 2017 • Hans Peter Gumm, Manfred Sommer: Einführung in die Informatik, Oldenbourg-Verlag, 2011 • David Harel: Algorithmik. Die Kunst des Rechnens. Springer Verlag, 2010
Dozenten: tbd
Modulverantwortliche: Jonas, Stockmanns
Aktualisiert: 21.08.2023

Modul	**BDF102 Ethische und Menschliche Aspekte der Informationssicherheit**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	1. Semester		inkl. Prüfungsvorbereitung
Sem. LV + Vorlesung	2 + 2	60	90
Übung			
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Mündliche Prüfung (30 - 45 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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
- gesellschafltiche Problemfelder der Informationssicherheit zu benennen und im Lichte unterschiedlicher Interessen zu diskutieren
- Risiken automatisierter Entscheidungen zu erkennen
- eigenverantwortlich zu handeln

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 Aspekte.
- Psychologische Faktoren
- Ethische Dilemmata und moralische Entscheidungen
- Ethische Fragen in der Zusammenarbeit mit Strafverfolgungsbehörden oder Unternehmen

Lehrmethoden: Im Rahmen der Vorlesung werden Ethiktheorien vorgestellt und mit den Studentinnen und Studenten diskutiert.

- Im seminaristischen Teil werden ethische Theorien und Konzepte auf konkrete Fälle der digitalen Forensik angewendet und Lösungen zu den ethischen Problemen entwickelt (in Einzel- und in Gruppenarbeit).

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „IT-Sicherheit“ (BDF102 / BDF205 / BDF 304 / BDF 404). Das Modul kann für das Modul BCSM102 anerkannt werden.

Literatur: Birsch: ”Ethical Insights.” McGraw-Hill, 2001

- Heidenreich: ”Theorien der Gerechtigkeit.” Barbara Budrich, 2011
- OŃeil: ”Weapons of Math Destruction.” Penguin, 2017

Dozenten: tbd

Modulverantwortliche: Quade, Dalitz

Aktualisiert: 21.08.2023

Modul	**BDF103 Programmierung**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 1. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: Testat

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte:

- Algorithmen
- Entwicklungswerkzeuge und Standardbibliotheken
- Einführung in die Programmiersprache Python
- Grundlagen der Strukturierten Programmierung: Ablaufstrukturen, Datentypen und Funktionen, einfache Datenstrukturen wie verkettete Listen
- Elementare Ein- und Ausgabe, Dateisystem, Speicherverwaltung, rekursive Funktionen und Anwenden des Erlernten auf einfache Problemstellungen
- Softwareanalyse und Tests
- Grundlegende Elemente und Mechanismen der Softwareentwicklung und der strukturierten Programmierung werden anhand von kleinen Programmfragmenten und Modulen eingeführt und eingeübt.
- Die Übertragbarkeit des Erlernten wird durch die Nutzung von Bibliotheken und die Betrachtung des jeweiligen zweier Programmierparadigmen ermöglicht
- Grundlagen der Software-Entwicklung
- systematische Erstellung von Softwaresystemen o Phasen der Softwareentwicklung
- Grundlagen der strukturierten Programmierung:
- Ablaufstrukturen
- (rekursive) Funktionen
- elementare Datentypen
- einfache Datenstrukturen
- elementare Ein- und Ausgabe o Dateisysteme
- Anwendung des Erlernten auf einfache Algorithmen
- Grundlagen des objektorientierten Anwendungsentwurfs mit UML
- Grundlagen der objektorientierten und generischen Programmierung
- Nutzung von Bibliotheken

Lehrmethoden: Vorlesung, unterstützt durch Skript/Literatur zum Selbststudium. Der Stoff der Vorlesung wird vertieft durch Bearbeitung von Testaten, diese werden in Team von bis zu 5 Studierenden über das Semester als kleinere Programmierprojekte erarbeitet. Diese Aufgaben sind in den Teams selbständig unter Moderation des Lehrenden zu bearbeiten und die Ergebnisse sind vor einer Studierendengruppe zu präsentieren. An größeres Programmierprojekt wird in den Teams als Hausarbeit bearbeitet und präsentiert. Begleitendes, eigenverantwortliches Lernen in einer Softwarewerkstatt, unterstützt durch Tutorien.

Bezug zu anderen Fächern/Modulen: Das Modul kann für das Modul BCSM103 anerkannt werden.

Literatur:

- John Hunt: A Beginners Guide to Python 3 Programming Springer Verlag
- Balzert: Software-Technik Band 1 und 2
- Sommerville: Software-Engineering
- H. Balzert: Lehrbuch der Objektmodellierung. Spektrum.
- B. Oesterreich: Objektorientierte Softwareentwicklung. Oldenbourg.
- Passig, Jander: Weniger schlecht programmieren
- Sowie weitere aktuelle Literaturhinweise zu Beginn der Veranstaltung.

Dozenten: tbd

Modulverantwortliche: Stockmanns

Aktualisiert: 21.08.2023

Modul	**BDF104 Einführung in die Digitale Forensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 1. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Bereitschaft sich selbstständig in komplexe Themen einzuarbeiten

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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 selber durchführen zu können, in dem 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.

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)

Lehrmethoden: 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, 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.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Forensik“ (BDF104 / BDF204 / BDF 305 / BDF 405 / BDF 504a).

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben

Dozenten: tbd

Modulverantwortliche: Padilla

Aktualisiert: 21.08.2023

Modul	**BDF105 Rechtliche Grundlagen der Cyberkriminalistik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 1. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Testat

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

Inhalte: Verfassungsgrundsätze, insbesondere Demokratie und Rechtsstaatsprinzip

- Allgemeine Grundrechtslehren, insbesondere Funktionen, Schutzbereich, Eingriff, Schranken
- Einzelne Grundrechte
- Funktion der Strafe und des Strafrechts,
- Grundprinzipien des Strafrechts:
- Strafrechtliche Sanktionen im Überblick,
- Einteilung der Delikte
- Tatbestand: objektive und subjektive Tatbestandsmerkmale,
- Kausalität, Zurechenbarkeit, Vorsatz
- Schuld
- Formen von Täterschaft und Teilnahme
- Tatbestands- und Verbotsirrtum
- Ausgewählte IT-relevante Rechtsbereiche, z.B. DSGVO, Recht des elektronischen Geschäftsverkehrs, Immaterialgüterrecht, Telekommunikationsrecht
- Rechtsquellen
- Methodik der Fallbearbeitung: Gutachten- und Urteilsstil
- Methodik der juristischen, wissenschaftlichen Recherche: Gesetzes-, Rechtsprechungs- und Literaturquellen

Lehrmethoden: Skript bzw. Vorlesungsunterlagen. Ausgesuchte Beispielfälle zur Anwendung der erlernten Kompetenzen.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Kriminalistik“ (BDF 105 / BDF 203 / BDF 303 / BDF 403 / BDF 504b).

Literatur: Beulke, Werner: Strafrecht Allgemeiner Teil: Die Straftat und ihr Aufbau, 49. Auflage 2019

- Fischer, Thomas, Strafgesetzbuch, 69. Auflage, München 2022
- Michael Hettinger / Armin Engländer: Strafrecht Besonderer Teil / 1: Straftaten gegen Persönlichkeits- und Gemeinschaftswerte, 45. Auflage 2021
- Thomas Hillenkamp / an C. Schuh: Strafrecht Besonderer Teil/2: Straftaten gegen Vermögenswerte, 44. Auflage 2021
- Elmar Erhardt (Autor): Strafrecht für Polizeibeamte (Recht und Verwaltung), 7. Auflage 2021
- Basten, Eingriffsrecht der Polizei in NRW – Band 1: Grundlagen des polizeilichen Eingriffsrechts, Frankfurt a.M. 2020
- Basten, Eingriffsrecht der Polizei in NRW - Band 2: Grundstudium, Frankfurt a.M. 2021 Basten, Eingriffsrecht der Polizei in NRW – Fälle, Frankfurt a.M. 2021
- Beulke, Werner/ Swoboda, Sabine: Strafprozessrecht (Schwerpunkte Pflichtfach), 15. Auflage 2020
- Hilgendorf, Eric, Valerius, Brian, Kusche, Carsten: Computer- und Internetstrafrecht – Ein Grundriss, 3. Auflage 2022 (erscheint im Herbst 2022), Springer
- Kochheim, Dieter: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage 2018, C.H.Beck

Dozenten: tbd

Modulverantwortliche: Freund, Godry, Schwarzwälder

Aktualisiert: 21.08.2023

Modul	**BDF106 Erstsemesterprojekt**		**Credits: 05**
Studiengang	Bachelor		
Modultyp	Pflichtmodul		
Sprache	Deutsch		
Turnus des Angebots	Wintersemester		

	Semesterwochenstunden 1. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung	2	30	
Übung			
Praktikum/Projekt	2		120
Arbeitsaufwand in Stunden		30	120

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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

Lehrmethoden: Ein Team von bis zu 5 Studierenden erhält über das Semester Aufgaben zur Erarbeitung von Grundbegriffen und Konzepten, der Darstellung von aktuellen Cybervorfällen und der Herleitung von technischen Grundlagen. Sie bearbeiten selbständig einen fiktiven Fall und präsentieren die Ergebnisse vor anderen Studierendengruppen, beispielsweise in Form einer Beweisführung.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Softskills“ (BDF 106 / BDF 206 / BDF 505 / BDF 601). Das Modul kann für das Modul BCSM106 anerkannt werden.

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

Dozenten: Meuser

Modulverantwortliche: Meuser

Aktualisiert: 21.08.2023

Modul	**BDF201 Betriebssysteme: Anwendung**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	2. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	30
Übung	2	30	60
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Softwareentwicklung, Informatik-Grundlagen

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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 in der Systemkonfiguration aufzudecken und zu beheben.
- Sicherheitskonzepte und Schutzmechanismen moderner Betriebssysteme zu kennen, zu konfigurieren und IT-Systeme entsprechend einer Security-Policy abzusichern.

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

Lehrmethoden: Vorlesung mit Foliensammlung, Skript, Literatur und Beispielprogrammen zum Selbststudium.

- Den Studierenden stehen virtuelle Server zur Verfügung mit deren Hilfe die praktischen Übungen und Aufgaben durchgeführt werden können.
- Kollaborationswerkzeuge (gitlab und Chatsysteme) sollen Gruppenarbeiten in diesem Modul unterstützen.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Betriebssysteme“ (BDF 201 / BDF 301 / BDF 401 / BDF 503a). Das Modul kann für das Modul BCSM 201 anerkannt werden.

Literatur:

- A. S. Tanenbaum: Moderne Betriebssysteme; Pearson Studium, 2016.
- E. Glatz: Betriebssysteme, dpunkt Verlag, 2015.
- R. Bause: Betriebssysteme, Grundlagen und Konzepte, Springer Vieweg, 2017
- P. Mandl: Grundkurs Betriebssysteme, Springer Vieweg, 2014

Dozenten: Davids

Modulverantwortliche: Davids

Aktualisiert: 21.08.2023

Modul	**BDF202 Einführung in Open Source Intelligence (OSINT)** **Credits: 05**
Studiengang	Bachelor
Modultyp	Pflichtmodul
Sprache	Deutsch
Turnus des Angebots	Sommersemester

	Semesterwochenstunden 2. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: Testat

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte:

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

Lehrmethoden: Vorlesung unterstützt durch Skript/Literatur zum Selbststudium. Der Stoff der Vorlesung wird vertieft durch Bearbeitung von Testaten. Diese werden in Teams von bis zu 5 Studierenden über das Semester als kleinere Anwendungsprojekte erarbeitet. Diese Aufgaben sind in den Teams selbständig unter Moderation des Lehrenden zu bearbeiten und die Ergebnisse sind vor einer Studierendengruppe zu präsentieren. An größeres Projekt wird in den Teams als Hausarbeit bearbeitet und präsentiert.

Bezug zu anderen Fächern/Modulen:

Literatur: Foliensammlung, Literatur zum Selbststudium

Dozenten: tbd

Modulverantwortliche: Stockmanns

Aktualisiert: 21.08.2023

Modul	**BDF203 Einführung in die Kriminalistik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden 2. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Testat

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- die Kriminalwissenschaften innerhalb der Studienfächer einzuordnen.
- Aufbau und Organisation der Kriminalitätsbekämpfung zu erläutern.
- zwischen der kriminalistischen Beweisführung im Ermittlungsverfahren und der späteren gerichtlichen Beweisführung eine Beziehung 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 bezüglich ihrer möglichen Relevanz für die Aufklärung kriminalistischer Sachverhalte zu interpretieren und zu klassifizieren.
- Beziehungen zwischen Beweiskraft und Beweiswert einer Spur herzustellen und diese auf Sachverhalte zu übertragen.
- die Bedeutung des Tatortes für die Ermittlungsarbeit zu identifizieren.
- die Rolle des Cyber-Kriminalisten im Strafverfahren einzuordnen.
- den Beweiswert verschiedener Spuren/-komplexe zu interpretieren und den Bezug zum Sachbeweis herzustellen.
- naturwissenschaftliche Erkenntnisse und kriminaltechnische Verfahren auf konkrete Sachverhalte anzuwenden.
- geeignete Spurensicherungsmaßnahmen zu übertragen und die Bedeutung der Dokumentation für das Ermittlungsverfahren zu erläutern.
- die Sachbearbeitung in Straftaten besonderer Kriminalitätsbereiche, wie zum Beispiel Sexualdelikte, zu erläutern.
- Besonderheiten bei der Sachbearbeitung der Cyber-Kriminalität zu identifizieren.

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
- Verhältnis zwischen Staatsanwaltschaft und Polizei sowie die Bedeutung für die Zusammenarbeit im Ermittlungsverfahren
- fachliche Entwicklung der spezifischen Möglichkeiten der Beweisführung
- Anforderungen an die Beweisführung im Ermittlungsverfahren und vor Gericht
- Formelle Beweismittel zur Urteilsfindung
- Verdachtsfindung und Verdachtsqualifizierung im Ermittlungsverfahren
- Kriminalwissenschaftliche Analysemethoden und Verdeutlichung deren Zielrichtung und Bedeutung für die Praxis
- Analytische Bewertung von Straftaten in Form der kriminalistischen Fallanalyse zur Erlangung von Ansatzpunkten für die Aufklärung von Einzeldelikten/Tatserien
- polizeiliche Zuständigkeiten für die Suche, Sicherung und Auswertung von kriminalistischen Spuren
- kriminaltechnische Grundeinteilung relevanter Spuren
- Grundtechniken zur Suche von Spuren
- Differenzierung der Relevanz gefundener und möglicher Spuren für die weitere Beweisführung
- Beweiskraft und Beweiswert wesentlicher kriminalistischer Spuren an Tatorten
- kriminalistischer und juristischer Tatort und weitere relevante Ereignisorte und deren Bedeutung für die polizeiliche Ermittlungsarbeit
- Aussage als Zeuge vor Gericht
- Beweiswert und Beweiskraft wesentlicher Spuren an Tatorte
- Suche und Sicherung relevanter Spuren
- aktuelle naturwissenschaftliche Auswertungsmöglichkeiten von Spuren und deren Beweiswert bei einer konkreten Straftat
- Zusammenwirken von Personal- und Sachbeweis
- Bedeutung der Spuren und der Dokumentation des Spurensicherungsverfahrens für das Strafverfahren
- Kriminalistische Maßnahmen zur Aufklärung von Straftaten besonderer Kriminalitätsbereiche, wie zum Beispiel Sexualdelikte
- Erscheinungsformen und Maßnahmen zur Verfolgung der Cyber-Kriminalität

Lehrmethoden: Vorlesung mit Unterlagen, Übungen anhand von Praxisbeispielen

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Kriminalistik“ (BDF 105 / BDF 203 / BDF 303 / BDF 403 / BDF 504b).

Literatur:

Dozenten: tbd

Modulverantwortliche: Jens Brandt

Aktualisiert: 21.08.2023

Modul	**BDF204 Forensische Methoden und Werkzeuge**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	2. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Grundkenntnisse zu Betriebssystemen und zu Rechnernetzen; Grundlagen der IT-Sicherheit aus dem ESP - BDF106; erfolgreiche Teilnahme an Veranstaltung Einführung in die Digitale Forensik BDF104

Prüfungsvorleistung:

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte:

- Einführung in die Teilbereiche Datenträger-, Arbeitsspeicher- und Netzwerkforensik
- Datenrepräsentation auf Datenträgern, im Arbeitsspeicher und im Netzwerk und 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

Lehrmethoden: 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, 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.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Forensik“ (BDF104 / BDF204 / BDF305 / BDF405 / BDF 504a). Pro Teildisziplin (Datenträger-, Arbeitsspeicher- und Netzwerkforensik) werden jeweils grundlegende Konzepte und Überlegungen vorgestellt und anhand einfacher Beispiele verdeutlicht. Eine fachlich tiefergehende Behandlung der Teildisziplinen erfolgt jeweils in weiterführenden Modulen.

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben

Dozenten: tbd

Modulverantwortliche: Padilla

Aktualisiert: 21.08.2023

Modul	**BDF205 IT-Sicherheit**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden 2. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Grundlagen der Informatik (BDF101)

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Die Studierenden beschäftigen sich mit dem Vorbeugen, Erkennen und der Reaktion auf Ereignisse, die die Integrität von Daten, die Nutzbarkeit von Systemen und die Privatsphäre gefährden. Mit dem erfolgreichen Absolvieren des Moduls sind die Studierenden in der Lage

- 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.

Inhalte:

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

Lehrmethoden: Rechnergestützte Vorlesung mit Unterlagen zum Selbststudium; praktisch orientierte Übung am eigenen oder am zur Verfügung gestelltem Rechner (Verschlüsselter EMail-Versand, Aufbau PKI, VPN, Firewall aufbauen, etc.)

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „IT-Sicherheit“ (BDF102 / BDF205 / BDF 304 / BDF 404). Das Modul kann für das Modul BCSM203 anerkannt werden.

Literatur: Unterlagen zur Vorlesung in der jeweils aktuelle Auflage

- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, De Gruyter Oldenbourg, 2018.

Dozenten: Quade, Meuser

Modulverantwortliche: Quade

Aktualisiert: 21.08.2023

Modul	**BDF206 Bedarfsorientierte Mikroprojekte**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden 2. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	30
Übung			
Praktikum/Projekt	2	30	60
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: kei ne

Prüfungsvorleistung: Testat

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte: Anwendungsbezogene Grundlagen der Netzwerktechnik

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

Lehrmethoden: Ein Team von bis zu 5 Studierenden erhält über das Semester kleinere Aufgaben zu anwendungsbezogenen Grundlagen. Herleitung von Grundlagen und deren Anwendung in einem Praxisprojekt. Diese Aufgaben sind im Team selbständig unter Moderation des Lehrenden zu bearbeiten und die Ergebnisse sind vor einer Studierendengruppe zu präsentieren.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Softskills”. (BDF 106 / BDF 206 / BDF 505 / BDF 601). Das Modul kann für das Modul BCSM206 anerkannt werden.

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 Ausflage
- Meinel, C./Mundhenk, M.: Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung, aktuelle Auflage

Dozenten: tbd

Modulverantwortliche: Stockmanns

Aktualisiert: 21.08.2023

Modul	**BDF301 Betriebssysteme: Technik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	3. Semester		inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung	4	60	90
Übung			
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Betriebssysteme Anwendungen (BDF201)

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

Inhalte:

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

Lehrmethoden: Vorlesung mit Foliensammlung, Skript, Literatur und Beispielprogrammen zum Selbststudium. Den Studierenden stehen virtuelle Server zur Verfügung, mit deren Hilfe die praktischen Übungen und Aufgaben durchgeführt werden können.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Betriebssysteme“ (BDF 201 / BDF 301 / BDF 401 / BDF503a), es ist weiterhin Grundlage für die Module „Malwareanalyse“ und „Forensik von Speichermedien“.

Literatur:

- S. Tanenbaum: Moderne Betriebssysteme; Pearson Studium, 2016.
- E. Glatz: Betriebssysteme, dpunkt Verlag, 2015.
- R. Bause: Betriebssysteme, Grundlagen und Konzepte, Springer Vieweg, 2017
- P. Mandl: Grundkurs Betriebssysteme, Springer Vieweg, 2014
- J. Quade, E. Kunst: Linux-Treiber entwickeln: Eine systematische Einführung in die Gerätetreiber- und Kernelprogrammierung, dpunkt Verlag, 2015

Dozenten: tbd

Modulverantwortliche: Davids

Aktualisiert: 21.08.2023

Modul	**BDF302 Rechnernetze und Rechnernetzsicherheit**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	3. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	30
Übung	2	30	60
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Netzwerkthema aus dem Modul BDF 206

Prüfungsvorleistung: Testat

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte: Die Vernetzung ist die Plattform für die IT-Systeme, aber auch für Sicherheits-Attacken. Daher müssen die Prinzipien, Konzepte und Techniken von Rechnernetzen bekannt sein. Mit diesem Wissen können Angriffsgefahren und -strukturen verstanden werden. Daraus leiten sich abschließend ein sicherer Netzwerkbetrieb, die Meldung von Sicherheitsvorfällen und die gängigen Gegenmaßnahmen der Netzwerksicherheit ab.

- Einsatz von und Anforderungen an Datennetze
- Netzkomponenten, insb. Switche und Router
- TCP/IP-Protokollfamilie
- Management der IPv4/IPv6-Adressierung; IP-Services (DHCP/NAT)
- Grundlagen des Routings; statisches und dynamisches Routing
- Grundlagen des 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, insb. mit SNMP
- Grundlagen der Netzwerksicherheit
- Absicherung der Netzwerkgeräte
- Authentifizierung, Autorisierung und Abrechnung
- Firewall-Technologien; IPS/IDS-Implementierungen

Lehrmethoden: Seminaristische Vorlesung mit Übungsanteilen; begleitender Online-Kurs

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Netzwerke“ (BDF 302 / BDF 402 / BDF 502a). Das Modul kann für das Modul BCSM 303 anerkannt werden.

Literatur: Riggert, Lübben: Rechnernetze – ein einführendes Lehrbuch; 6., aktualisierte und erweiterte Auflage. 2020 • A.S. Tanenbaum: Computer Networks, Pearson New International Edition, Juli 2013, Prentice Hall In-ternational, ISBN 978-1292024226 • Cisco Press: Networking Essentials Companion Guide, 2022 (ISBN: 978-0137660483) • CCNA Security Lab Manual Version 2, 2015 (ISBN: 978-1587133503) • M. Kappes: Netzwerk- und Datensicherheit: Eine praktische Einführung, Springer-Verlag, erscheint August 2020 (ISBN-13: 978-3658161262) • C. Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Studium, August 2018 (ISBN-13: 978-3110551587
Dozenten: tbd
Modulverantwortliche: Meuser
Aktualisiert: 21.08.2023

Modul	**BDF303 Der Digitale Tatort und Täterkommunikation**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 3. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Mündliche Prüfung (30 - 45 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

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
- Zielgerichte Suche und Interpretation von Spuren in IT-Systemen
- Aufbereitung von forensischen Datensicherungen
- Beweiswert und Beweiskraft von (digitalen) Spuren am Tatort
- Dokumentation der Tatortarbeit
- Täterseitige Kommunikationsmittel (z. B. E-Mail, Messenger im Clear- und Darknet)
- Anonymisierungs- und Deanonymisierungstechniken

Lehrmethoden: Vorlesung mit Foliensammlung, Skript und Literatur zum Selbststudium. Falldiskussionen und praktische Übungen zur Tatortarbeit, Spurensuche, -sicherung und -auswertung.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Kriminalistik“ (BDF 105 / BDF 203 / BDF 303 / BDF 403 / BDF 504b).

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben.

Dozenten: tbd

Modulverantwortliche: Thomas Meuser

Aktualisiert: 21.08.2023

Modul	**BDF304 Web- und Browsersicherheit**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	3. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Studierende haben die wesentlichen in dem Modul Programmierung BDF103 vermittelten Lehrinhalte und Kompetenzen erfolgreich in ihren Wissens- und Fähigkeitskanon übernommen.

Prüfungsvorleistung: Testat

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.
- den Nutzen der erarbeiteten Lösungen argumentativ zu begründen.

Inhalte:

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

Lehrmethoden: Rechnergestützte Vorlesung mit Unterlagen zum Selbststudium; praktisch orientierte Übung am eigenen oder am zur Verfügung gestelltem Rechner.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „IT-Sicherheit“ (BDF102 / BDF205 / BDF 304 / BDF 404).

Literatur:

- Zalewski: Tangled Web - Der Security-Leitfaden für Webentwickler; dpunkt.verlag
- Heiderich et al.: Browser Security White Paper; Cure53
- Rohr: Sicherheit von Webanwendungen in der Praxis: Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse; Springer Vieweg

Dozenten: tbd

Modulverantwortliche: Niemietz

Aktualisiert: 21.08.2023

Modul	**BDF305 Datenbanken-Forensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 3. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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

Lehrmethoden: Vorlesung mit theoretischen und praktischen Übungen

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Forensik“ (BDF104 / BDF204 / BDF 305 / BDF 405 / BDF 504a).

Literatur: Foliensammlung, Literatur zum Selbststudium:

- Kemper, Eickel: Datenbank-Systeme - eine Einführung. 10. Auflage, De Gruyter, 2015.
- Studer: Relationale Datenbanken: Von den theoretischen Grundlagen zu Anwendungen mit PostgreSQL. Springer Vieweg, 2016.
- Trelle: MongoDB: Der praktische Einstieg. dpunkt.verlag, 2014.

Dozenten: tbd

Modulverantwortliche: Niemietz

Aktualisiert: 21.08.2023

Modul	**BDF306 Security Incident Management**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 3. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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, Sicherheits-Informationen- und Event-Management-Systemen (SIEMs)
- Compliance und rechtliche Aspekte, (DSGVO, ISO 27035, ITIL, Informationspflichten)
- Dokumentation von Incident-Response-Aktivitäten und Erstellung von Berichten

Lehrmethoden: Klassische Wissensvermittlung wird mit praktisch orientierten Übungen gekoppelt. In den Übungen werden (simulierte) Unternehmen und Sicherheitsvorfälle behandelt. Incident Management Werkzeuge werden exemplarisch auf (eigenen) Rechnern installiert und eingesetzt.

Bezug zu anderen Fächern/Modulen: Das Modul kann für das Modul BCSM502-2 anerkannt werden.

Literatur:

- DIN EN ISO/IEC 27035
- Colby A. Clark: Cybersecurity Incident Management Masters Guide. Volume 1, Juni 2020.

Dozenten: tbd

Modulverantwortliche: Quade, Padilla

Aktualisiert: 21.08.2023

Modul	**BDF401 Betriebssysteme: Forensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	4. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: - Grundkenntnisse zu Betriebssystemen (Hauptspeicherverwaltung, Dateisystem, ...) - Grundkenntnisse zu Rechnernetzen (Ethernet, TCP, IP, UDP, ...) - Grundlagen der IT-Sicherheit (Sicherheitstests, Kryptographie, Angriffserkennung, Programmanalyse, ...) - Erfolgreiche Teilnahme an Veranstaltung Einführung in die Digitale Forensik - Erfolgreiche Teilnahme an Veranstaltung Forensische Methoden und Werkzeuge - Bereitschaft sich selbstständig in komplexe Themen einzuarbeiten

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

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

Lehrmethoden: Für die Auswertungen werden jeweils Open Source Werkzeuge eingeführt und durch die Studierenden in praktischen Übungen erprobt. Es werden für alle Inhalte neben den theoretischen Grundlagen stets auch die praktische Anwendbarkeit vermittelt. Durch die Praxisnähe und zielgruppengerechte Präsentationen von Ermittlungsergebnissen werden die für die digitale Forensik eminenten Soft-Skills vermittelt, wie beispielsweise die Fähigkeit, Thesen mithilfe von digitalen Artefakten zu untermauern oder zu widerlegen sowie eine strukturierte Vorgehens- und Denkweise bei forensischen Analysen anzuwenden.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Betriebssysteme“ (BDF 201 / BDF 301 / BDF 401 / BDF503a).

Literatur: Bruce Nikkel: Practical Linux Forensics: A Guide for Digital Investigators, No Starch Press 21. Dezember 2021.

Dozenten: tbd

Modulverantwortliche: Padilla

Aktualisiert: 21.08.2023

Modul	**BDF402 Netzwerkforensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Jedes Studienjahr	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	4. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung			
Praktikum/Projekt	2	30	45
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Inhalte der LV Rechnernetze, Betriebssystem Technik, IT-Sicherheit

Prüfungsvorleistung: Testat

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

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, 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.

Lehrmethoden: Präsentation, interaktive Übungsaufgaben auf eigener Plattform, Übungen zum Selbststudium

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Netzwerke”. (BDF 302 / BDF 402 / BDF 502a); weiterhin vertieft es Inhalte aus den Modulen Kryptografie, Betriebssystem Technik, IT-Sicherheit und wendet diese an.

Literatur: • Geschonneck: Computer-Forensik, ISBN-13: 978-3864901331 • Kävrestad: Fundamentals of Digital Forensics, ISBN-13: 978-3030389536 • Veröffentlichungen in dem Journal Forensic Science International: Digital Investigation (vormals Digital Investigation) • Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
Dozenten: tbd
Modulverantwortliche: Meuser
Aktualisiert: 21.08.2023

Modul	**BDF403 Geschäftsmodelle im Internet**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	4. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Mündliche Prüfung (30 - 45 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

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, E-Mail, Cloud-Dienste und soziale Netzwerke
- Foren- und Handelsplattformen
- Registrierung bei bekannten Internetdiensten
- Hosting von Diensten
- Virtuelle private Netzwerke, Botnetze und Proxy-Dienste
- Clearnet und Darknet
- Underground Economy
- Angriffs- und Angreifertypen
- Verbreitung von Malware, beispielsweise ausgehend vom initialen Zugriff, der Privilegieneskalation, der lateralen Bewegung und dem Exfiltration von Daten
- Tätergruppierungen und Cybercrime-as-a-Service
- Bezahldienste und -methoden sowie Bonussystem
- Zugang zu Opferdaten über Spam- und Phishing oder dem Ausnutzen von Schwachstellen

Lehrmethoden: Vorlesung mit Foliensammlung, Skript und Literatur zum Selbststudium

- Präsentationen
- Gruppenarbeit

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Kriminalistik“ (BDF 105 / BDF 203 / BDF 303 / BDF 403 / BDF 504b).

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben.

Dozenten: tbd

Modulverantwortliche: Jürgen Quade

Aktualisiert: 21.08.2023

Modul	**BDF404 Angewandte Kryptografie**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Sommersemester	

	Semesterwochenstunden 4. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: keine

Vorkenntnisse: Lehrstoff der beiden ersten Semester, insbesondere Informatik-Grundlagen der IT-Forensik, Programmieren, Einführung in die Digitale Forensik, IT-Sicherheit

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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
- Postquanten Krypto
- 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)

Lehrmethoden: Vorlesung mit Foliensammlung, Skript, Literatur und Beispielprogrammen zum Selbststudium. Den Studierenden stehen virtuelle Server zur Verfügung mit deren Hilfe die praktischen Übungen und Aufgaben durchgeführt werden können.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „IT-Sicherheit“ (BDF102 / BDF205 / BDF 304 / BDF 404).

Literatur:

- Buchmann, J: Einführung in die Kryptographie Rothe, J: Komplexitätstheorie und Kryptologie, Springer
- David Kahn: The Codebreakers
- Klaus Schmeh: The Codeknacker gegen Codemacher - die faszinierende Geschichte der Verschlüsselung
- Jonathan Katz & Yehuda Lindell: Introduction to Modern Cryptography
- Dan Boneh & Victor Shoup. A Graduate Course in Cryptography

Dozenten: Tipp

Modulverantwortliche: Tipp, Quade
Aktualisiert: 21.08.2023

Modul	**BDF405 Forensikprojekt**		**Credits: 10**
Studiengang	Bachelor		
Modultyp	Pflichtmodul		
Sprache	Deutsch		
Turnus des Angebots	Sommersemester		

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	4. Semester		inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung	1	15	30
Übung			
Praktikum/Projekt	3	45	210
Arbeitsaufwand in Stunden		60	240

Zulassungsvoraussetzungen: keine

Vorkenntnisse: keine

Prüfungsvorleistung: Testat

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

Inhalte:

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

Lehrmethoden: Ein Team von bis zu 5 Studierenden erhält Aufgaben zur Ausarbeitung eines wissenschaftlichen Forensikprojekts. Diese Aufgaben sind im Team selbständig unter Moderation des Lehrenden zu bearbeiten und die Ergebnisse sind vor einer Studierendengruppe zu präsentieren.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Forensik“ (BDF104 / BDF204 / BDF 305 / BDF 405 / BDF 504a).

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

Dozenten: tbd

Modulverantwortliche: Niemietz

Aktualisiert: 21.08.2023

Modul	**BDF501a Malewareanalyse**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Wahlpflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: - Betriebssysteme - Programmierung

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- verschiedenen Arten von Malware zu klassifizieren und deren Eigenschaften bezüglich Funktion, Verbreitung und Stealth-Techniken zu benennen
- Malware statisch und dynamisch zu analyisieren
- 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

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

Lehrmethoden: Rechnergestützte Vorlesung mit Vorlesungsunterlagen zum Selbststudium; Praktische Übungen am eigenen oder zur Verfügung gestellten Notebook (learning by doing).

Bezug zu anderen Fächern/Modulen: Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Kleymenov, Thabet: Mastering Malware Analysis: A malware analystś practical guide to combating malicious software, APT, cybercrime, and IoT attacks. Packt Publishing, 2nd Edition 2022.

- Andriesse: Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. No Starch Press, 2018.

Dozenten: tbd

Modulverantwortliche: Quade, Padilla

Aktualisiert: 13.09..2023

Modul	**BDF501b Forensik von Speichermedien**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: Grundkenntnisse zu Betriebssystemen (Hauptspeicherverwaltung, Dateisystem, ...) Grundkenntnisse zu Rechnernetzen (Ethernet, TCP, IP, UDP, ...) Grundlagen der IT-Sicherheit (Sicherheitstests, Kryptographie, Angriffserkennung, Programmanalyse, ...) Erfolgreiche Teilnahme an Veranstaltung Einführung in die Digitale Forensik Erfolgreiche Teilnahme an Veranstaltung Forensische Methoden und Werkzeuge Bereitschaft sich selbstständig in komplexe Themen einzuarbeiten

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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

Lehrmethoden: Es werden jeweils Open Source Werkzeuge für die Extraktion und Auswertung vorgestellt und durch die Studierenden erprobt. Es werden also für alle Inhalte neben den theoretischen Grundlagen stets auch die praktische Anwendbarkeit vermittelt. Daneben sind aber auch für die digitale Forensik eminente Soft-Skills, 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.

Bezug zu anderen Fächern/Modulen: Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben

Dozenten: tbd

Modulverantwortliche: Padilla

Aktualisiert: 13.09.2023

Modul	**BDF502a Mobilfunk- und Kommunikationsforensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: Inhalte insbesondere der LV Netzwerkforensik/Abwehr von IT-Angriffen, Betriebssystemforensik und digitale Spuren, Kryptografie, Rechnernetze

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- Konzepte, Architekturen und Geräte der technischen Kommunikation, insbsondere der Mobilfunktechnik zu beschreiben,
- die Funktionsweise unterschiedlicher Kommunikationsprotokolle (u.a. GSM, UMTS, LTE; WLAN) zu erläutern,
- Meta- und Inhaltsdaten aus der Kommunikation aufzuzeichnen und zu analysieren
- Datenspuren (Kommunikationsparameter, Kontaktdaten, Anruflisten, SMS, E-Mails Messenger, soziale Medien) auf mobilen Endgeräten zu identifizieren, zu sichern und zu analyiseren
- Korrelationen zwischen Analyseergebnissen aus unterschiedlichen Quellen zu erstellen, um daraus Indizien abzuleiten
- Werkzeuge wie Wireshark oder FTK anzuwenden

Inhalte:

- Einführung in die Grundlagen der Kommunikations- und
- Mobilfunktechnik, in Netzwerktypen, Protokolle und
- Kommunikationsstandards
- Methoden und Techniken zur forensischen Untersuchung
- von Kommunikations- und Mobilgeräten, insbesondere
- der Extraktion und Auswertung von Daten
- Einführung in mobile Betriebssysteme, insbesondere Android
- und iOS unter Berücksichtigung der eingebauten Sicherheitsfunktionen
- Analyse von Mobilkommunikation
- Einsatz von Werkzeugen zur Sicherung und Analyse von
- Kommunikationsdaten, einschließlich der Verwendung von
- Netzwerkprotokollanalysatoren
- Gerichtsfeste Dokumentation und Präsentation der Analyseergebnisse

Lehrmethoden: Präsentation, Literaturanalyse (insbes. aktuelle Journal-Artikel und Konferenzbeiträge), Diskussion, praktische Anwendung in Testinfrastrukturen

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Netzwerke”. (BDF 302 / BDF 402 / BDF 502a); weiterhin vertieft es Inhalte aus den Modulen Betriebssysteme: Forensik und Kryptografie und wendet diese an. Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Martin Sauter: Grundkurs Mobile Kommunikationssysteme: 5G New Radio und Kernnetz, LTE-Advanced Pro, GSM, Wireless LAN und Bluetooth; ISBN-13: 978-3658369620 • Alexander Geschonneck: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären; ISBN-13: 978-3864901331 • Reza Montasari: Digital Forensic Investigation of Internet of Things (IoT) Devices; ISBN-13: 978-3030604240 • Marcel Mangel: Praktische Einführung in Hardware Hacking: Sicherheitsanalyse und Penetration Testing für IoT-Geräte und Embedded Devices; ISBN-13: 978-3958458161
Dozenten: tbd
Modulverantwortliche: Jonas
Aktualisiert: 13.09.2023

Modul	**BDF502b Social Engineering**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Mündliche Prüfung (30 - 45 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- Grundlagen der Mensch-Maschine-Interaktion mit Hinblick auf die Grundwerte der Informationssicherheit zu verstehen
- den Faktor „Mensch“ als gezielten Angriffsvektor zu definieren
- Social Engineering-Methoden zu erkennen
- neue Methoden bzw. Angriffsvektoren wie Emotet / CEO Fraud zu verstehen und zu analysieren
- gängige Techniken und psychologische Grundlagen der einzelnen Angriffsmuster zu bewerten
- Abwehrstrategien gegen Social Engineering zu entwickeln und umzusetzen
- Sicherheitsrichtlinien und Schulungen in Bezug auf Verhalten in Sicherheitszonen, Telearbeitsumgebungen zu entwickeln

Inhalte:

- Grundlagen des Social Engineering wie Reziprozität, Konsistenz und Commitment
- Andere Techniken wie Phishing und Dumpster Diving
- Abwehrstrategien gegen Social Engineering
- Grundlagen der Informationssicherheit in der Mensch-Maschine-Interaktion (MMI)
- Grundlagen der Psychologie und weiterer sozialer Faktoren (Vertrauen, Recht) zur effektiven Sicherheit von Informationssystemen
- Praktische Beispiele und Hackmethoden

Lehrmethoden: Seminaristische Vorlesung mit Übungsanteilen; Präsentation zu ausgewählten Aufgabenstellungen, Literaturanalyse aktueller Veröffentlichungen und Studien

Bezug zu anderen Fächern/Modulen: Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006

- Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007
- Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010
- Cranor, Garfinkel: Security and Usability: Designing Secure Systems that People Can Use, OŔeilly, 2005

Dozenten: tbd

Modulverantwortliche: Treibert

Aktualisiert: 13.09.2023

Modul	**BDF503a Embedded Systems Forensik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Wahlpflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	5. Semester		inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: Vorkenntnisse aus den Themenfeldern Netzwerkforensik/Abwehr von IT-Angriffen, Betriebssystemforensik und digitale Spuren, Kryptografie, Rechnernetze

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- Eingebettete Systeme in die Kategorie Depply 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 sicher zu stellen und von diesen relevante Daten zu extrahiere,
- 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

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

Lehrmethoden: Rechnergestützte Vorlesung mit Unterlagen zum Selbststudium; praktisch orientierte Übungen an eingebetteten-, IoT- oder Smart-Home-Geräten.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Betriebssysteme”. (BDF 201 / BDF 301 / BDF 401 / BDF503a). Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur:

Dozenten: tbd

Modulverantwortliche: Jonas, Quade

Aktualisiert: 13.09.2023

Modul	**BDF503b IT-Kriminaltaktik**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Mündliche Prüfung (30 - 45 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- den Begriff Kriminaltaktik im cyberkriminalistischen Kontext einzuordnen
- den Modus Operandi ausgewählter Delikte aus den Bereichen Cybercrime im engeren und weiteren Sinne beschreiben zu können
- Grundsätze der strukturierten Beschuldigten- und Zeugenvernehmungen unter besonderer Berücksichtigung möglicher Beweis- und Beweisverwertungsverbote sowie bestehender Opferrechte zu beurteilen
- psychologische Einflussfaktoren vor, während und nach der Vernehmung zu bewerten und eine Vernehmung entsprechend zu konzipieren
- Durchsuchungsmaßnahmen rechtlich einzuordnen und ihre taktischen Grundlagen zu kennen
- die Sicherstellung von IT-Asservaten aus juristischer Sicht einordnen zu können und die relevanten Verfahrensvorschriften aufzuzeigen
- Maßnahmen zu verdeckten personalen Ermittlungen benennen und sie kriminaltaktisch und juristisch bewerten zu können

Inhalte:

- Einordnung der IT-Kriminaltaktik in den Bereich der Kriminalwissenschaften, Differenzierung der Fächer untereinander und Aufzeigen von Querbezügen zu den übrigen Studienfächern
- Modus Operandi einzelner Delikte aus den Bereichen Cybercrime im engeren und weiteren Sinne, wie zum Beispiel von Sexualdelikten, politisch motivierter Kriminalität, organisierter Kriminalität, Kapitalverbrechen, Urheberrecht, kriminelle Handelsplattformen
- Taktisches Vorgehen im Ermittlungsverfahren bei einschlägigen Cybercrime-Delikten
- Vorbereitung, Durchführung und Dokumentation von Vernehmungen, Rechts- und Aussagepsychologie: Psychologische Grundsätze der Befragung von Auskunftspersonen, Einflüsse auf die Entstehung polizeilicher (Zeugen-)Aussagen (z.B. absichtliche und unabsichtliche Falschaussagen)
- Rechtliche Grundlagen sowie Vorbereitung, Durchführung und Dokumentation von Durchsuchungen und Sicherstellungen
- Verdeckte Maßnahmen im Ermittlungsverfahren, wie z. B. Observationen, Telekommunikationsüberwachung, verdecke Ermittler

Lehrmethoden: Vorlesung mit Foliensammlung, Skript und Literatur zum Selbststudium

- Präsentationen
- Gruppenarbeit

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Kriminalistik”. (BDF 203 / BDF 303 / BDF 403 / BDF 503a) Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Weiterführende Quellen werden in der Vorlesung gegeben.

Dozenten: tbd

Modulverantwortliche: Jens Brandt

Aktualisiert: 13.09.2023

Modul	**BDF504a Erstellung forensicher Werkzeuge**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Wahlpflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: - Basis-Kenntisse der Programmierung (BDF103, Software Entwicklung) - Grundkenntnisse über Betriebssysteme (BDF201, Betriebssysteme Anwendung) - IT-Sicherheit (BDF205)

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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, Durchführen von manuellen Tests.
- IT-Sicherheitstechnische Aspekte der Programmierung.
- Einsatz in der Praxis

Lehrmethoden: Vorlesung

- Praktische Übungen, in denen Werkzeuge erstellt werden

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Forensik”. (BDF104 / BDF204 / BDF 305 / BDF 405 / BDF 504a); es baut zudem auf BDF103 ”Software Entwicklung” auf. Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Preston Miller, Chapin Bryce: Learning Python for Forensics: Leverage the power of Python in forensic investigations, 2nd Edition. Packt Publishing 2019.

Dozenten: tbd

Modulverantwortliche: Stockmanns, Quade

Aktualisiert: 13.09.2023

Modul	**BDF504b Strafverfahren in der Cyberkriminalität**	**Credits: 05**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Wintersemester	

	Semesterwochenstunden 5. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Vorlesung	2	30	45
Übung	2	30	45
Praktikum/Projekt			
Arbeitsaufwand in Stunden		60	90

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Klausurarbeit (90 Minuten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- Grundsätze und Grundprinzipien des Strafprozessrechts (StPO) zu kennen und die verschiedenen Stufen des Strafverfahrens zu unterscheiden.
- die verschiedenen Möglichkeiten der Beweiserhebung sowie bestehende Beweisverbote zu erläutern
- Grundsätze, Methoden und Taktiken der Vernehmung von Zeugen und Beschuldigten sowie verschiedene Ansätze zur Beurteilung von Glaubhaftigkeit von Aussagen. zu beherrschen
- die Grundsätze einer Durchsuchung und der Sicherstellung bzw. Beschlagnahme von Asservaten zu beherrschen
- die Besonderheiten im Umgang mit IT-Asservaten zu kennen

Inhalte:

- Grundlagen und Grundprinzipien der StPO
- Ablauf des Strafverfahrens
- Beweiserhebung
- Grundsätze der Beweiserhebung
- Beweisverbote
- Vernehmungsmethoden und -taktiken
- Durchsuchung und Beschlagnahme
- Besonderheiten beim Umgang mit IT-Asservaten
- Faires Verfahren
- Phasen der Informationsgewinnung
- Rechtssichere Planung und Durchführung von Beweissicherungsmaßnahmen

Lehrmethoden: Skript bzw. Vorlesungsunterlagen. Ausgewählte Fälle zur Anwendung der erlernten Kompetenzen.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Kriminalistik”. (BDF 105 / BDF 203 / BDF 303 / BDF 403 / BDF 504b) Zukünftig als Modul im Wahlpflichtkatalog des Studiengangs BCSM/BCSMT vorgesehen.

Literatur: Bender, Rolf/ Häcker, Robert/ Schwarz, Volker: Tatsachenfeststellung vor Gericht, 5. Auflage 2021

- Beulke, Werner/ Swoboda, Sabine: Strafprozessrecht (Schwerpunkte Pflichtfach), 15. Auflage 2020
- Meyer-Goßner /Schmitt: Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen (Beckśche Kurz-Kommentare), 65. Auflage 2022
- Rodorf, Alfred: Strafprozessrecht - Strafverfolgung durch die Polizei, Polizeikurse.de - für Studium und Praxis - Studienheft StPO / Strafprozessordnung: ...
- Beschlagnahme, vorläufige Festnahme u.a. Taschenbuch, 2022
- Walter, T.: Strafprozessrecht: Ein Lehrbuch für Studenten und angehende Praktiker, utb, 2020

Dozenten: tbd

Modulverantwortliche: Freund, Godry
Aktualisiert: 13.09.2023

Modul	**BDF505 Hackathon**		**Credits: 10**
Studiengang	Bachelor		
Modultyp	Pflichtmodul		
Sprache	Deutsch		
Turnus des Angebots	Wintersemester		

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	5. Semester		inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung	1	15	30
Übung			
Praktikum/Projekt	3	45	210
Arbeitsaufwand in Stunden		60	240

Zulassungsvoraussetzungen: Die Studierenden in BDF haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 Kreditpunkte erreicht.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

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

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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.

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

Lehrmethoden: Ein Team von bis zu 5 Studierenden erhält Aufgaben zur Ausarbeitung einer im Rahmen eines Hackathons definierten Aufgabenstellung. Diese Aufgaben sind im Team selbständig unter Moderation der Lehrperson zu bearbeiten und die Ergebnisse sind vor einer Studierendengruppe zu präsentieren.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads „Softskills“ (BDF 106 / BDF 206 / BDF 505 / BDF 601). Das Modul kann für das Modul BCSM 505 anerkannt werden.

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

Dozenten: tbd

Modulverantwortliche: Pentang, Niemietz

Aktualisiert: 13.09.2023

Modul	**BDF601 Praxisphase und begleitendes Seminar**	**Credits: 15**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Jedes Studienjahr	

	Semesterwochenstunden	**Präsenzzeit**	**Selbststudium**
	6. Semester		inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung	1	15	15
Übung			
Praktikum/Projekt			420
Arbeitsaufwand in Stunden		15	435

Zulassungsvoraussetzungen: Die Studierenden in BDF und BDFT haben alle Module des 1. und 2. Fachsemesters gemäß BDF-Studienverlaufsplan erfolgreich abgeschlossen und somit alle 60 cp erreicht. Zudem haben sie mindestens 30 Kreditpunkte in den Modulen des 3. und 4. Fachsemesters gemäß BDF-Studienverlaufsplan erlangt.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Testat

Notensystem: bestanden / nicht bestanden

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- 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

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.

Lehrmethoden: Die Studierenden arbeiten in Dienststellen, im Unternehmen oder einer Organisation im Team der Mitarbeiter:Innen an der konkret formulierten Aufgabenstellungen aus dem Bereich Cyber Security, insb. Digitaler Forensik. Dazu wenden sie ihre bisher erworbenen Kenntnisse und Fähigkeiten auf eben diese Aufgabenstellung an. In dem begleitenden Seminar werden mit anderen Studierenden die Erfahrungen ausgetauscht und im Endbericht die Tätigkeiten, das Betätigungsumfeld und die erworbenen Kompetenzen beschrieben.

Bezug zu anderen Fächern/Modulen: Das Modul ist Teil des Lernpfads ”Softskills”. (BDF 106 / BDF 206 / BDF 505 / BDF 601)

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

Dozenten: Professorinnen und Professoren der HSNR (FB03, FB08) und der HBRS (FB Informatik)

Modulverantwortliche: Meuser

Aktualisiert: 21.08.2023

Modul	**BDF602 Bachelorarbeit und Kolloquium**	**Credits: 15**
Studiengang	Bachelor	
Modultyp	Pflichtmodul	
Sprache	Deutsch	
Turnus des Angebots	Jedes Studienjahr	

	Semesterwochenstunden 6. Semester	**Präsenzzeit**	**Selbststudium** inkl. Prüfungsvorbereitung
Sem. Lehrveranstaltung			90
Übung			
Praktikum/Projekt			360
Arbeitsaufwand in Stunden		0	450

Zulassungsvoraussetzungen: Für die Zulassung zur Bachelorarbeit haben die Studierenden in BDF und BDFT alle Module des 1., 2., 3. und 4. Fachsemesters gemäß BDF-Studienverlaufsplan sowie die Praxisphase erfolgreich abgeschlossen und somit mindestens 135 Kreditpunkte erreicht.

Vorkenntnisse: keine

Prüfungsvorleistung: keine

Prüfungsform: Benotete Prüfung - Abschlussarbeit (40 - 70 Seiten)

Notensystem: deutsche Notenskala 1-5

Lernziele/Kompetenzen: Mit dem erfolgreichen Absolvieren des Moduls sind Studierende in der Lage,

- die erlernten Fachkenntnisse und wissenschaftliche Methoden im Rahmen einer konkreten anwendungsorientierten Themenstellung selbstständig anzuwenden
- umzusetzen 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.

Inhalte: Die Bachelorarbeit soll zeigen, dass der Prüfling befähigt ist, innerhalb einer vorgegebenen Frist 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 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.
- Selbständige Bearbeitung einer Aufgabenstellung aus der betriebswirtschaftlichen Forschung und/oder Praxis nach wissenschaftlichen Methoden innerhalb eines Zeitraums von höchstens drei Monaten.

Lehrmethoden: Wissenschaftliche Aufarbeitung bzw. systematische Dokumentation und Präsentation eines komplexen Themas erfordert eine fachspezifische Methodenkompetenz. Präsentation der Ergebnisse der Bachelorarbeit, Verteidigung und Diskussion der Ergebnisse im Fachgespräch. Im wissenschaftlichen Diskurs der Arbeitsergebnisse im Kolloquium zeigt der Student seine Kritik- und Argumentationsfähigkeit.

Bezug zu anderen Fächern/Modulen:

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

Dozenten: Professorinnen und Professoren der HSNR (FB03, FB08) und der HBRS (FB Informatik)

Modulverantwortliche: Meuser

Aktualisiert: 21.08.2023

Modulname	Kürzel	Analyse-Kompetenz	Design-Kompetenz	Fachübergreifende Kompetenzen	Formale, algorithmische, mathematische Komp.	Methoden-Kompetenzen	Projektmamagement-Kompetenz	Realisierungs-Kompetenz	Soziale Kompetenzen und Selbstkompetenz	Technologische Kompetenzen
Informatik-Grundlagen der Forensik	BDF101	x			x			x		
Ethische und Menschliche Aspekte der Informationssicherheit	BDF102	x		x					x	
Programmierung	BDF103				x	x		x		
Einführung in die Digitale Forensik	BDF104	x				x				x
Rechtliche Grundlagen der Cyberkriminalistik	BDF105			x		x			x	
Erstsemesterprojekt	BDF106						x	x	x	
Betriebssysteme: Anwendung	BDF201							x		x
Einführung in Open Source Intelligence (OSINT)	BDF202	x				x		x		
Einführung in die Kriminalistik	BDF203	x		x		x				
Forensische Methoden und Werkzeuge	BDF204			x		x				x
IT-Sicherheit	BDF205								x	x
Bedarfsorientierte Mikroprojekte	BDF206				x	x				x
Betriebssysteme: Technik	BDF301	x	x							x
Rechnernetze und Rechnernetzsicherheit	BDF302	x						x		x
Der Digitale Tatort und Täterkommunikation	BDF303	x		x					x	
Web- und Browsersicherheit	BDF304		x			x		x		
Datenbanken-Forensik	BDF305	x				x				x
Security Incident Management	BDF306	x				x	x			
Betriebssysteme: Forensik	BDF401	x				x				x
Netzwerkforensik	BDF402	x			x					x
Geschäftsmodelle im Internet	BDF403	x								x
Angewandte Kryptografie	BDF404				x	x		x		
Forensikprojekt	BDF405		x				x		x	
Malewareanalyse	BDF501a	x				x				x
Forensik von Speichermedien	BDF501b	x						x		x
Mobilfunk- und Kommunikationsforensik	BDF502a	x				x				x
Social Engineering	BDF502b					x		x	x	
Embedded Systems Forensik	BDF503a	x						x		x
IT-Kriminaltaktik	BDF503b			x		x			x	
Erstellung forensicher Werkzeuge	BDF504a					x		x		x
Strafverfahren in der Cyberkriminalität	BDF504b	x		x					x	
Hackathon	BDF505					x			x	x
Praxisphase und begleitendes Seminar	BDF601			x					x	x
Bachelorarbeit und Kolloquium	BDF602	x				x				x