Modulhandbuch

Fernstudium

Bachelor

IT-Forensik

Stand: 13.05.2024

WINGS-FERNSTUDIUM
AN DER HOCHSCHULE WISMAR

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Inhaltsverzeichnis

Modulbezeichnung Deutsch: PM 1 Einführung in die Informatik – IT-Forensik	
Modulbezeichnung Englisch: Introduction in Computer Science - Digital Forensics	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Einführung in das Fernstudium „IT-Forensik“: Informatik im Kontext forensischer Fragestellungen Was ist Informatik? Historie und Teilgebiete der Informatik Logik und Boolsche Algebra Information und Daten Programmiersprachen: Daten und Algorithmen Grundlegende Probleme der theoretischen Informatik Grundlegende Begriffe der IT-Forensik: Digitale Spur, Artefakt, W-Fragen, Gerichtsverwertbarkeit Vorgehensmodelle in der IT-Forensik
Qualifikationsziele des Moduls	Beherrschen von Informatik-Grundlagen: • Kenntnisse über die Informatik-Schwerpunkte im Studiengang und die Inhalte der einzelnen Informatik-Lehrveranstaltungen • Kenntnisse über die Teilgebiete der Informatik • Befähigung zum Verständnis von zentralen Fragestellungen der Informatik • Kenntnisse über die Boolsche Algebra • Befähigung zum Erstellen eines Algorithmus • Kenntnisse über die Beschreibbarkeit und Berechenbarkeit von Problemen Beherrschen von IT-Forensik-Grundlagen: • Kenntnisse über grundlegende Begriffe und Normen • Kenntnisse über die Befähigung zur Einordnung von IT-forensischen Fragestellungen Grundlegende Begriffe der IT-Forensik: Digitale Spur, Artefakt, W-Fragen, Gerichtsverwertbarkeit • Vorgehensmodelle in der IT-Forensik
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen Grundlegende Begriffe der IT-Forensik: Digitale Spur, Artefakt, W-Fragen, Gerichtsverwertbarkeit
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik

Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120 o. APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 2 Computersysteme I: Grundlagen der technischen Informatik	
Modulbezeichnung Englisch: Computer Systems I - Basics of Technical Computer Science	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Repräsentation von Informationen: Kanäle, Codes und Medien Repräsentation von Informationen: Zahlensysteme und Konvertierung Transistoren, Chips, logische Bausteine Prozessorarchitektur und Speicher Rechnernetze und das Internet Bussysteme und Datenübertragung Codierung, Kompression Signaltheoretische und physikalische Grundlagen der Digitalgrafik; Farbräume und Konvertierung
Qualifikationsziele des Moduls	Beherrschen und Anwenden von technologischen Grundlagen (Hardware und Software) multimedialer Systeme und Anlagen. Weitreichende Kenntnisse über multimediale Datenstrukturen und Dateiformate einschließlich ihrer technischen und physikalischen Grundlagen. Grundlegende Fähigkeiten, IT-forenische Fragenstellungen und technische Aspekte von Computersystemen in Beziehung zu setzen.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 3 Zahlentheoretische Grundlagen	
Modulbezeichnung Englisch: Mathematics	
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Andreas Ahrens
Inhalte des Moduls	Einführung in die lineare Algebra Grundlagen der Algebra (Gruppen, Ringe, (endliche) Körper) Grundlagen der Elementaren Zahlentheorie Modulares Rechnen
Qualifikationsziele des Moduls	Befähigung komplexe wissenschaftliche, technologische und organisatorische Problemstellungen in mathematische Formulierungen zu übertragen, die Lösungen methodisch richtig durchzuführen und die gewonnenen Ergebnisse kritisch zu beurteilen Beherrschung der grundlegenden algebraischen und zahlentheoretischen Strukturen zum Verstehen von Verfahren der IT-Sicherheit und Forensik Beherrschung der grundlegenden Denkweise der modernen Algebra
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Mathematische Grundkenntnisse
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 4 Kriminalistik	
Modulbezeichnung Englisch: Criminalistics	
Modulverantwortliche(r)	Stefan Kellermann, M.A.
Inhalte des Moduls	System der Kriminalistik und ihrer Bezugswissenschaften Kriminalistischer Erkenntnis- und Beweisführungsprozess Kriminalistisches Denken (Version- und Hypothesenbildung; Logische Methoden; Verdacht, Zweifel, Kriminalistische Entscheidungsprozesse) Informationsbewertung nach 4x4 Modell, wahrscheinlichkeitstheoretische Aspekte Kriminalistische Analyse und Synthese Kriminaltaktisches Konzept
Qualifikationsziele des Moduls	Kenntnisse zum wissenschaftlichen System der Kriminalistik und tangierender Wissenschaftsgebiete Beherrschung der theoretischen Grundlagen kriminalistischer Erkenntnis- und Beweisprozesse Kenntnisse zu Verdachtsarten und Beherrschung von Verdachtsschöpfungsstrategien sichere Beherrschung der Grundmethoden kriminalistischen Denkens und der kriminalistischen Informationsbewertung Vermögen, kriminalistische Lagen zu beurteilen und darauf basierend Ermittlungsansätze abzuleiten und entsprechende Untersuchungshandlungen vorzuschlagen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt

Modulbezeichnung Deutsch: PM 5 Kriminologie	
Modulbezeichnung Englisch: Criminology	
Modulverantwortliche(r)	Prof. Dr. iur. habil. Marina Tamm
Inhalte des Moduls	Einführung in den kriminologischen Verbrechensbegriff und in das Aufgabenfeld der Kriminologie Besprechung der Kriminalstatistik der letzten Jahre und der diesbezüglichen Datenerhebung Berührung mit dem „Dunkelfeld“ von Kriminalität Wissensvermittlung zu allgemeinen biologischen, psychologischen und sozialstrukturellen Kriminalisierungstheorien speziellen Kriminalitätstheorien wie der Kriminalität i.V.m. Massenmedien, Ursachen der Kriminalität von besonderen Personengruppen und von fremdenfeindlicher Gewalt. Überblick über die sog. Viktimologie Kriminologische Einführung in spezielle Kriminalitätsbereiche (z.B.: Wirtschaftskriminalität, Organisierte Kriminalität und die Kriminalität von Kindern) Möglichkeiten und Grenzen sozialer und rechtlicher Kontrolle von Kriminalität
Qualifikationsziele des Moduls	Das Modul befähigt die Studierenden, das Begehen von Straftaten durch Menschen und deren Auswirken anhand unterschiedlicher wissenschaftlicher Erklärungsversuche soziologisch einordnen zu können.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL (ohne Note)
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 6 Betriebssysteme	
Modulbezeichnung Englisch: Operating Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. Olaf Hagendorf
Inhalte des Moduls	Grundlagen, Prinzipien und Architekturen von Rechnerarchitekturen und Betriebssystemen, Aufbau, Komponenten und Wirkungsweise des Betriebssystemkerns, Scheduling und Schedulingstrategien, Synchronisation und Kommunikation von Diensten und Prozessen, Hauptspeicherverwaltung und virtuelle Speicherververwaltung, Geräteverwaltung und Deadlookbehandlung, Filesysteme und Dateiverwaltung, Handhabung und Administration des Betriebssystems UNIX/LINUX, Einführung in die Shellprogrammierung
Qualifikationsziele des Moduls	Kenntnisse über Rechnerarchitekturen, Strukturierungsprinzipien, Fähigkeiten und Betriebsarten von modernen Betriebssysteme sowie über deren Realisierungsprinzipien und innere Funktionsweise, Befähigung zur applikationsspezifischen Auswahl von Betriebssystemen und Plattformen, Befähigung zum Verstehen und Bewerten von Mechanismen und Strategien von Betriebssystemen und deren Anwendung, Befähigung zur Handhabung und zur Administration des Betriebssystems UNIX Befähigung, komplexe Zusammenhänge in Betriebssystemen zu verstehen und für die systemnahe Programmierung anwenden zu können, Grundlegende Kenntnisse in der Administration von Betriebssystemen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester

Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 7 Informationsrecherche im Internet	
Modulbezeichnung Englisch: Information Investigations Using the Internet	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Überblick über Such-Werkzeuge im Internet Maßnahmen zur Suchmaschinenoptimierung von Web-Inhalten Systemische Recherche im Web Architektur und Arbeitsweise von Suchmaschinen Grundkonzepte des Information Retrievals: Precision and Recall Stichwortidentifikation Stoppworteliminierung Suchmaschinen (Google, Bing, Yahoo u.a.) und ihre Suchoperatoren Optimierung der Internet-Recherche Beurteilung von Informationen aus Internet-Recherchen Dark- und Deep-Web Definition Inhalte des Dark Webs Systemische Recherche im Deep Web Anonymes Verhalten im Deep Web
Qualifikationsziele des Moduls	Kenntnisse über OSINT (Open Source Intelligent)-Recherchen Vermittlung von grundlegendem Wissen bzgl. einer Internet-Recherche Vermittlung von Kenntnissen über Suchtechnologien und Suchstrategien im Internet Befähigung zur detaillierten Nutzung von Suchmaschinen, Internet-Katalogen und sozialen Netzen zur Gewinnung von Informationen Befähigung zur Bewertung von Informationen aus Internet-Recherchen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL

Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 8 Programmierung I: Grundlagen der Programmierung	
Modulbezeichnung Englisch: Programming I - Basics of Programming	
Modulverantwortliche(r)	Prof. Dr.-Ing. Ingo Müller
Inhalte des Moduls	Einführung in die Entwicklungsumgebung Elementare Sprachelemente Steueranweisungen Funktionen Datenstrukturen Fortgeschrittene Zeigertechnik Ein-/ Ausgabeoperationen Programmstrukturierung, Speicherklassen Objektorientierte Programmierung (Klassen, Vererbung, Polymorphie) Anwendung WinAPI MFC Programmierung
Qualifikationsziele des Moduls	Befähigung zum Programmieren z.B. in C, C++
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 9 Datenschutzrecht	
Modulbezeichnung Englisch: Data Privacy Laws	
Modulverantwortliche(r)	Prof. Dr. iur. habil. Marina Tamm
Inhalte des Moduls	Einführung in den nationalen und europäischen Grundlagen des Datenschutzrechts deutsches und europäisches Grundrecht auf informationelle Selbstbestimmung und auf Integrität computergestützter Systeme, nationale und europäische Bestimmungen zum Datenschutz inkl. der einschlägigen Rechtsprechung internationale Vorgaben zum Datenschutz (insbesondere Datenschutzabkommen mit Drittstaaten) aktuelle Justizkonflikte etwa im Zusammenhang mit der Vorratsdatenspeicherung
Qualifikationsziele des Moduls	Befähigung zur sicheren Anwendung polizeilicher bzw. strafverfolgungsrechtlicher Handlungsbefugnisse im Grenzbereich zum Datenschutzrecht Wissen zu datenschutzrechtlichen Vorgaben des Verfassungsrechts sowie des deutschen und europäischen Sekundärrechts und Wissen um internationale Abkommen zum Datenschutz sowie den diesbzgl. Anwendungsvorgaben der Rechtsprechung
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL (ohne Note)
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt

Modulbezeichnung Deutsch: PM 10 Algorithmen und Datenstrukturen	
Modulbezeichnung Englisch: Algorithm and Data Structures	
Modulverantwortliche(r)	Prof. Dr. -Ing. Matthias Kreuseler
Inhalte des Moduls	Algorithmenbegriff, Beschreibungsmöglichkeiten für Alg. einfache und zusammengesetzte Datenstrukturen: Feld, Stapel, Liste, Baum Sortieren (1): selection sort, bubble sort asymptotische Algorithmenanalyse: worst case, average case, Rechenzeitbedarf vs. Speicherbedarf Sortieren (2): quick sort, merge sort, heap sort Datenstrukturen und Algorithmen für Graphen: Traversierung, Backtracking, kürzeste Wege, Minimale Spannbäume Klassische Probleme hoher Komplexität und Generische Optimierungsalgorithmen Algorithmen zur Fehlerkorrektur und Kompression
Qualifikationsziele des Moduls	Kenntnis und Verständnis des Begriffs Algorithmus Verständnis und Befähigung zur Anwendung wichtiger Algorithmen (z.B. Sortieren, Suchen) wichtige Datenstrukturen verstehen und anwenden (z.B. Arrays, Stapel, Bäume) Befähigung, Effizienz von Algorithmen zu analysieren und zu bewerten Befähigung, geeignete Algorithmen für neue Problemstellungen zu erarbeiten Grundlegende Kenntnisse von Umsetzungsmöglichkeiten für die Programmiersprachen C++, Java und .NET
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 11 Computersysteme II: Software-Architekturen	
Modulbezeichnung Englisch: Computer Systems II - Software Architectures	
Modulverantwortliche(r)	Michael Mundt
Inhalte des Moduls	Pattern und Muster für SW-Architekturen (Design Pattern) Modellierung von SW-Architekturen (MVC, PAC, Test driver architecture) Evaluation von SW-Architekturen Software-Qualität Definitionen und Standards Funktionstest, Überdeckungsmaße HiL-, Integrations- und Abnahmetests Verifikation und Validierung Architecture Design and Reliability Vermittlung von IT-forensischen Auswertungsstrategien von komplexen Softwaresystemen
Qualifikationsziele des Moduls	Vermittlung von Kenntnissen über Architekturen von Softwaresystemen Befähigung zur Bewertung der Softwarearchitekturen hinsichtlich sicherheitsrelevanter Aspekte, Befähigung zur Bewertung von Sicherheitslücken in Softwaresystemen Befähigung zum Verstehen und Bewerten von Softwarestrukturen und modellbasierten Ansätzen Befähigung zur Bewertung von Softwaretest und von Softwarequalität Befähigung zur Analyse von Softwaresystemen in Bezug auf die IT-Forensische Analyse
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester

Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 12 Systemnahe Programmierung	
Modulbezeichnung Englisch: System Programming	
Modulverantwortliche(r)	Prof. Dr. Olaf. Hagendorf
Inhalte des Moduls	Linuxinstallation und -administration Shell, C und Assembler Programmierung Dateihandling mittels Low- und Highlevelfunktionen Betriebssystemschnittstellen Prozesssystem und –Handling Prozesssynchronisation und -kommunikation Erweiterte Interprozesskommunikation über Nachrichtenwarteschlangen, Semaphore, Gemeinschaftsspeicher und Netzwerkschnittstellen
Qualifikationsziele des Moduls	Befähigung zur Administration von Linux und Programmierung systemnaher Anwendungen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120 o. APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 13 Cyber Crime I	
Modulbezeichnung Englisch: Cyber Crime I	
Modulverantwortliche(r)	Prof.Dr. iur. habil. Marina Tamm
Inhalte des Moduls	Einführung in die Cyberkriminalität als Querschnittsmaterie zwischen Verfassungs-, Zivil-, Polizei-, Ordnungs- und Strafrecht. Schwerpunkt auf dem materiellen Strafrecht mit Bezugnahme der klassischen Straftaten, die „gegen“ den Computer bzw. informationstechnische Systeme begangen werden (z.B.: Computerbetrug, Ausspähen und Abfangen von Daten, Datenveränderung, Computersabotage). Verfolgbarkeit der Straftatbestände über das deutsche Hoheitsgebiet hinaus.
Qualifikationsziele des Moduls	Befähigung dazu, die klassischen Delikte, die „gegen“ den Computer bzw. informationstechnische Systeme begangen werden, zu erkennen. Befähigung, die Verfolgbarkeit der Delikte über die Grenzen des deutschen Hoheitsgebietes hinaus abschätzen zu können.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 14 Programmierung II: Skript-Sprachen	
Modulbezeichnung Englisch: Programming II - Script Languages	
Modulverantwortliche(r)	Dr.-Ing. Markus Berg
Inhalte des Moduls	Einführung in den Aufbau von HTML Einführung in die Erstellung von Webseiten Einführung in die Clientseitige Script-Programmierung mit Javascript: - allgemeine und anwendungsbedingte Sprachelemente - spezielle Bibliotheken (JQuery, -UI, -Mobile) Einführung in die Serverseitige Script-Programmierung mit PHP: - allgemeine Sprachelemente - Sessionverwaltung - Datenbank-Zugriff Einführung in das Konzept AJAX Programmierpraktische Übungen
Qualifikationsziele des Moduls	Beherrschung von Client- und Serverseitigen Scriptsprachen Befähigung zum Programmieren von dynamischen Webseiten Befähigung zum Analysieren von Skripten in Webseiten
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 15 Datenbanken I: Grundlagen von DBS	
Modulbezeichnung Englisch: Database Systems I - Basics of Database Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Grundlagen, Prinzipien und Architekturen von Datenbankmanagementsystemen Konzepte relationaler DBS, Relationale Algebra SQL: Datendefinition, Anfragen, Join, Unteranfragen, Datenmanipulation Einführung in die Datenbankprogrammierung Prinzipien des Datenbank-Zugriffes aus Programmiersprachen Grundlagen der Administration von Datenbankmanagementsystemen Beispielhafte Übungen mit einem DBMS, z.B. MySQL
Qualifikationsziele des Moduls	Kenntnisse von Architektur und Grundlagen von Datenbanksystemen (DBS) Befähigung zum Verständnis von relationalen Datenbanken Befähigung, einfache SQL-Anfragen zu formulieren Grundlegende Kenntnisse in der Administration von Datenbankmanagementsystemen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120 o. APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 16 Ethical Hacking	
Modulbezeichnung Englisch: Ethical Hacking	
Modulverantwortliche(r)	Prof. Dr.-Ing. Meiko Jensen
Inhalte des Moduls	Grundlagen, Prinzipien und Architekturen von Computersystemen und Rechnernetzen, Ethical Hacking und Penetrationstests Strukturierungsprinzipien von Rechnernetzen, Rechner- und Internet-Unsicherheit, Klassifikation, Mechanismen und Wirkprinzipien von Bedrohungen und Angriffen, Schutz vor Bedrohungen und Abwehr von Angriffen
Qualifikationsziele des Moduls	Kenntnisse über Strukturierungsprinzipien von Betriebssystemen und Rechnernetzen, Befähigung zur Klassifikation von Hackern Vermittlung von Kenntnissen über Bedrohungen und Angriffsmechanismen Befähigung zum Verstehen und Bewerten von Mechanismen und Strategien von Hackern im Kontext von Ethical Hacking Befähigung zur Durchführung von Penetrationstests in Netzwerken Grundlegende Kenntnisse über gängige Werkzeuge und Rahmenbedingungen zur Durchführung von Penetrationstests Befähigung, komplexe Zusammenhänge in Betriebssystemen und Netzwerken zu verstehen und für die Abwehr von Bedrohungen anwenden zu können, Grundlagen der Ethik in der IT-Sicherheit
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 17 Computer Forensik I: Grunlagen der IT-Forensik	
Modulbezeichnung Englisch: Computer-Forensics I - Basic of Digital Forensics	
Modulverantwortliche(r)	Hans-Peter Merkel
Inhalte des Moduls	Einführung Überblick über die IT-Forensik Aktuelle Herausforderungen an die IT-Forensik Ziele einer IT-Forensischen Untersuchung Grundsätze einer forensischen Arbeitsweise Vorgehensweise bei einer IT-Forensischen Untersuchung Zu berücksichtigende rechtliche Aspekte Identifizierung und Datensicherung von relevanten Datenquellen Wiederherstellung von gelöschten und geänderten Daten Umgang mit Verschlüsselung Dateianalyse: Allocated, Unallocated, Carving Einsatz der Virtualisierung in der Forensik Parallelen und Gemeinsamkeiten der Forensik zu mobilen Geräten Kennenlernen von IT-Forensik-Werkzeugen Zeitstempel Informationen einbinden (Timelines und Supertimelines) Windows spezifische Artefakte (VSS, Prefetch, Registry)
Qualifikationsziele des Moduls	Das Modul befähigt Studierende dazu, die Möglichkeit und die Erfolgsaussichten der Computer Forensik abschätzen zu können. Sie kennen Anwendungsszenarien, Maßnahmen und die prinzipiellen Vorgehensweisen und können die Möglichkeiten der Computer Forensik nutzen. Sie wissen, wie die forensisch erfassten Daten als Beweismittel in Form eines Reports gerichtsverwertbar zu sichern und zu dokumentieren sind.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)

Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 18 Cyber Cime II	
Modulbezeichnung Englisch: Cyber Crime II	
Modulverantwortliche(r)	Prof. Dr. iur. habil. Marina Tamm
Inhalte des Moduls	Vermittlung von Kenntnissen zu Straftatbeständem, die typischerweise „mit“ dem Computer begangen werden (als Computerkriminalität im weiteren Sinne), z.B.: Betrug, unerlaubte Veranstaltung eines Glückspiels, Besitz und Verbreitung pornographischer Schriften, Anleitung zu Straftaten, Volksverhetzung und Gewaltdarstellung, Beleidigung, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, Nachstellung, Urheber- und Markenrechtsrechtsverletzung, Verrat von Geschäfts- und Betriebsgeheimnissen. Verfolgbarkeit der Delikte über die Grenzen des deutschen Hoheitsgebietes hinaus.
Qualifikationsziele des Moduls	Befähigung dazu, die klassischen Delikte, die „mit“ dem Computer bzw. informationstechnischen Systemen begangen werden, zu erkennen. Befähigung, die Verfolgbarkeit der Delikte über die Grenzen des deutschen Hoheitsgebietes hinaus abschätzen zu können.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 19 IT-Forensik-Projekt I	
Modulbezeichnung Englisch: Digital Forensics Project I	
Modulverantwortliche(r)	Prof. Dr. iur. habil. Marina Tamm
Inhalte des Moduls	Ausgabe bzw. Wahl eines Projektthemas aus dem Gebiet „IT-Forensik“ Aufteilung der Projektinhalte auf die Team-Mitglieder Literaturrecherche zu forensischen Fragestellungen Entwicklung einer Strategie/ eines Konzeptes zur Lösung der Fragestellungen im Projektthema Ausarbeitung einer schriftlichen Analyse Präsentation der Ergebnisse des Projektes
Qualifikationsziele des Moduls	Praktische Kenntnisse in der strategischen Aufarbeitung forensischer Fragestellungen, insbesondere juristische Aspekte Befähigung zur eigenständigen Aufarbeitung von forensischen Fragestellungen Befähigung im Team forensische Fragestellungen zu bearbeiten Befähigung forensische Fragestellungen zu dokumentieren und zu präsentieren
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K 120 o. APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 20 Kryptografie I	
Modulbezeichnung Englisch: Cryptography I	
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Andreas Ahrens
Inhalte des Moduls	Einführung in die mathematischen Grundlagen und Konzepte der klassischen und modernen Kryptologie sowie in Grundwissen über deren Algorithmen, Protokolle und Verfahren Beschreibung und symmetrischer Verschlüsselungsverfahren und aktueller symmetrischer Algorithmen Behandlung wichtiger asymmetrischer Verfahren sowie digitaler Zertifikate
Qualifikationsziele des Moduls	Kenntnisse von grundlegenden Problemen der IT-Sicherheit Befähigung zur Durchführung wichtiger kryptographischer Verfahren und deren mathematischer Grundlagen Befähigung zur Nutzung von Techniken zur Konstruktion und Analyse ausgewählter kryptografischer Algorithmen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 21 Datenbanken II: Forensik in DBS	
Modulbezeichnung Englisch: Database Systems II - Forensics in Database Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. A. Raab-Düsterhöft
Inhalte des Moduls	Administration von verschieden, konkreten DBMS Auslesen einer Datenbank-Struktur und von Datenbank-Inhalten Formulierung komplexer SQL-Anfragen Erweiterte Datenbankprogrammierung: Prozeduren, Funktionen, Trigger Analyse von internen Informationen wie z.B. LOG-Files Systematischen, nachvollziehbarer Datenbank-Zugriff aus verschiedenen Programmiersprachen heraus, Injected SQL Beispielhafte und vergleichende Übungen mit mehreren DBMS, z.B. MySQL, MSSQLServer, PostgreSQL u.a.
Qualifikationsziele des Moduls	Erweiterte Kenntnisse in der Administration von Datenbankmanagementsystemen Befähigung, komplexe SQL-Anfragen und DB-Skripte zu formulieren Befähigung zur Gewinnung von Informationen aus Datenbanken unter Ausnutzung interner Informationen Erweiterte Befähigung zum Anfragen von Datenbanken aus Programmiersprachen heraus
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt

Modulbezeichnung Deutsch: PM 22 Forensik auf mobilen Geräten	
Modulbezeichnung Englisch: Mobile Forensics	
Modulverantwortliche(r)	Hans-Peter Merkel
Inhalte des Moduls	Das Modul befasst sich mit der Forensik von mobilen Geräten als Ermittlungsmaßnahme in Form von rechtlich verwendbaren Datenerfassungen, der Analyse und der Sicherung von Daten von mobilen Geräten und der Erfassung der forensischen Daten. In einem ersten Abschnitt geht es um die unterschiedlichen Formen von Betriebssystemen auf mobilen Geräten, die forensischen Möglichkeiten digitale Daten von unterschiedlichen Betriebssystemen zu identifizieren und zu erfassen. Dabei werden die Unterschiede zur klassischen PC Forensik aufgezeigt. Es geht ferner um die Vermittlung von Grundlagen zur Durchführung forensischer Analysen auf mobilen Geräten mit proprietärer und Open Source Software. Schlussendlich werden anhand praktischer Beispiele logische und physikalische Auswertungen von SQLite Datenbanken durchgeführt, die in einem gerichtsverwertbaren Bericht dokumentiert werden.
Qualifikationsziele des Moduls	Das Modul befähigt die Studierenden dazu, die Möglichkeit und die Erfolgsaussichten der Forensik auf mobilen Geräten abschätzen zu können. Sie kennen Anwendungsszenarien- und Maßnahmen und können die Möglichkeit der Forensik auf mobilen Geräten nutzen. Sie wissen wie Smartphone-Daten physikalisch oder logisch gesichert werden. Sie kennen die Unterschiede und Grenzen zur traditionellen PC-Forensik und wissen welche Informationen gerichtsverwertbar genutzt werden können.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester

Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 23 Malware Analyse	
Modulbezeichnung Englisch: Malware Analysis	
Modulverantwortliche(r)	Prof. Dr.-Ing. Olaf Hagendorf
Inhalte des Moduls	Malware Analyse Tools und Umgebungen Malwarearten und deren Erkennung Reverse Engineering Statische und dynamische Analyse Verschleierung von Funktionalitäten
Qualifikationsziele des Moduls	Kenntnisse zu Malware Arten und Analysetechniken Befähigung zur statischen und dynamischen Erkennung und Analyse von Malware Grundkenntnisse in Assembler- und LowLevel-Programmierung
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120 o. APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 24 Computer Forensik II: Praxis Aspekte	
Modulbezeichnung Englisch: Computer Forensic II - Practical Aspects	
Modulverantwortliche(r)	Gilbert Löhr
Inhalte des Moduls	Das Modul befasst sich mit der Forensik von Computern als Ermittlungsmaßnahme in Form von rechtlich verwendbaren Datenerfassungen, der Analyse und der Sicherung von Daten von Computern und der Erfassung der forensischen Daten in Form einer gerichtlich verwendbaren Beweissicherung „Forensic Engineer Evidence Report“. In einem ersten Abschnitt geht es um die unterschiedlichen Formen von Computer Betriebssystemen, die forensischen Möglichkeiten digitale Daten von unterschiedlichen Betriebssystemen zu identifizieren und zu erfassen. Es werden ferner Grundlagen zur Durchführung der Forensik von Computern vermittelt. Schlussendlich werden anhand spezifischer Prozesse die Vorgehensweisen dargestellt, um Daten aus forensisch erfassten Computern als Beweismittel zu sichern und in einem Bericht die forensische Datenerhebung und somit die Beweisführung gerichtsverwertbar zu dokumentieren. Einbezogen sind typische Herangehensweisen zur Forensik von Computern und die Anwendung von geeigneten Software- und Hardwaretools.
Qualifikationsziele des Moduls	Das Modul befähigt die Teilnehmer dazu, die Möglichkeit und die Erfolgsaussichten der Computer Forensik abschätzen zu können. Sie kennen Anwendungsszenarien- und Maßnahmen und können die Möglichkeit der Computer Forensik nutzen. Sie wissen, wie die forensisch erfassten Daten als Beweismittel in Form eines „Forensic Engenieer Evidence Report“ gerichtsverwertbar zu sichern und zu dokumentieren sind.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL (ohne Note)
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester

Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 25 Kryptografie II	
Modulbezeichnung Englisch: Cryptography II	
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Andreas Ahrens
Inhalte des Moduls	Kryptographische Techniken, Verfahren und Systeme Kryptoanalytische Betrachtungen möglicher Angriffe auf kryptographische Verfahren An definierten Beispielen werden die Grenzen kryptografischer Verfahren praktisch ausgelotet
Qualifikationsziele des Moduls	Kenntnisse über grundlegende kryptographische Techniken, Verfahren und Systeme Grundlegende Kenntnisse zum Brechen kryptographische Verfahren
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik: PM 3: Zahlentheoretische Grundlagen Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik – IT-Forensik Grundkenntnisse in Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung Grundlagen kryptografischer Systeme: PM 20: Kryptografie I
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 26 Grundlagen Bild- und Videoverarbeitung	
Modulbezeichnung Englisch: Basics of Image Processing	
Modulverantwortliche(r)	Prof. Dr. rer. nat. Herbert Litschke
Inhalte des Moduls	Grundlagen der Optik und Fotografie Speicherung und Kompression von Bilddaten Statistische Bildverarbeitung Punktoperationen, Nachbarschaftsoperationen und Filter Geometrische Transformationen Fourier-Analyse von Bilddaten Grundlagen der Objekterkennung und Segmentierung Algorithmen zur Merkmalsextraktion Softwarebibliotheken des Maschinellen Sehens
Qualifikationsziele des Moduls	Verständnis optischer Systeme. Speicherung von Farben. Kenntnisse grafischer Dateiformate. Umfangreiche Fähigkeiten in der Manipulation und Analyse digitaler Bilder mittels eigener Programme und selbst entworfener Filter-Algorithmen. Klassifizierung und Korrektur von Abbildungsfehlern. Grundzüge der Objekterkennung und des maschinellen Sehens
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in der Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik – IT-Forensik PM 2: Computersysteme I: Grundlagen der technischen Informatik
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester

Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 27 Staatsphilosophie	
Modulbezeichnung Englisch: Commonwealth Philosophy	
Modulverantwortliche(r)	Prof. Dr. iur. Bodo Wiegand-Hoffmeister
Inhalte des Moduls	Besprechung der Teleologie staatlicher Gemeinschaften und politischen Handelns Vermittlung von Staatstheorien und der Idee der modernen am Gemeinwohl orientierte Staatsphilosophie (bonnum commune) Grundlagen der demokratischen Legitimierung politischer Macht und ihrer Akteure im modernen Wohlfahrtsstaat Gewaltenteilung, föderales System, Rechtsstaats- und Sozialstaatlichkeit als Staatsstrukturprinzipien der Bundesrepublik und der EU Notwendigkeit gesetzlicher Absicherung staatlicher Eingriffsbefugnisse Bedrohungen für das demokratische Gemeinwesen durch undemokratische Herrschaftssysteme und deren Grundlagen
Qualifikationsziele des Moduls	Verständnis zur Legitimation des modernen Staates und seiner demokratischen am Gemeinwohl orientierten Grundlagen Wissen um Gefährdungslagen für die demokratische Grundordnung und Freiheitsrechte einzelner durch undemokratische Herrschaftsorganisationen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120 (ohne Note)
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 28 IT-Forensik Projekt II	
Modulbezeichnung Englisch: Digital Forensics Project II	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Wahl eines Projektthemas aus dem Gebiet „IT-Forensik“ Aufteilung der Projektinhalte auf die Team-Mitglieder Literaturrecherche zu forensischen Fragestellungen Entwicklung einer Strategie/ eines Konzeptes zur Lösung der Fragestellungen im Projektthema Ausarbeitung einer schriftlichen Analyse Vermittlung von Wissen zur korrekten Nutzung von Systemen der Künstlichen Intelligenz für die Bearbeitung von wissenschaftlichen und forensischen Fragestellungen Präsentation der Ergebnisse des Projektes
Qualifikationsziele des Moduls	Praktische Kenntnissen in der strategischen Aufarbeitung forensischer Fragestellungen Befähigung zur eigenständigen Aufarbeitung von forensischen Fragestellungen Befähigung im Team forensische Fragestellungen zu bearbeiten Befähigung zur korrekten Nutzung von KI-Systemen Befähigung forensische Fragestellungen zu dokumentieren und zu präsentieren
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik – IT-Forensik PM 2: Computersysteme I: Grundlagen der technischen Informatik Grundkenntnisse in der Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse in Betriebssysteme: PM 6: Betriebssysteme Grundkenntnisse in der IT-Forensik PM 17: Computer Forensik I: Grundlagen der IT-Forensik PM 22: Forensik auf mobilen Geräten PM 24: Computer Forensik II: Praxis-Aspekte

Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz oder Online)
Leistungspunkte	5
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 29 Künstliche Intelligenz	
Modulbezeichnung Englisch: Artificial Intelligence	
Modulverantwortliche(r)	Prof. Dr. rer. nat. Jürgen Cleve
Inhalte des Moduls	Veranstaltung behandelt einen wichtigen Teilbereich der KI: Wissensextraktion, also die automatische Extraktion von Zusammenhängen in Massendaten. Zunächst werden die Grundprinzipien der Wissensextraktion mittels Data Mining erläutert. Es wird Data Mining über strukturierten, semistrukturierten und unstrukturierten Daten diskutiert. Es wird der lassische Ablauf einer Datenanalyse vorgestellt: Datenvorverarbeitung, Analyse, Interpretation. Verschiedene Verfahrensklassen des Data Mining (Klassifikation, Vorhersage, Clustering, Assoziationsregeln) werden anhand typischer Probleme eingeführt. Ein Schwerpunkt ist die Datenvorverarbeitung. Anhand realer Daten werden alle Teilthemen behandelt.
Qualifikationsziele des Moduls	Die Studierenden erwerben Kompetenzen im Einsatz von Analysetechniken, hier speziell auf dem Gebiet der Datenanalyse auf Massendaten. Sie erwerben die Fähigkeit, Data-Mining-Systeme zur Lösung von Analyseaufgabe einzusetzen. Durch Projektbasiertes Lernen wird die typische Sichtweise auf ein zu lösendes Problem gestärkt. Die Studierenden können: • die Relevanz der Wissensextraktion aus großen Datenmengen beurteilen; • mit großen Datenmengen umgehen, diese für Data-Mining-Verfahren vorbereiten; • verschiedene Data-Mining-Techniken anwenden; • die Resultate interpretieren; • • die Leistungsfähigkeit, die Einsatzmöglichkeiten und Grenzen der DM-Verfahren einschätzen.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Mathematik PM 3: Zahlentheoretische Grundlagen Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik – IT-Forensik

	Grundkenntnisse in Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 30 Grundlagen und Anwendungen biometrischer Systeme	
Modulbezeichnung Englisch: Basics and Applications of Biometrical Systems	
Modulverantwortliche(r)	Prof. Dr.-Ing. Matthias Kreuseler
Inhalte des Moduls	Entwicklung der Fingerabdruckerkennung und ihr Einsatz in Kriminalistik und Forensik Grundlegende Anforderungen an die Auswahl biometrischer Merkmale zur Personenidentifikation Vermittlung der drei derzeit am stärksten verbreiteten Verfahren: Fingerabdruckerkennung, Gesichtserkennung und Iriserkennung und der jeweiligen Teilprozesse Aufbau automatisierter biometrischer Systeme vertiefende Betrachtung Automatischer Fingerabdruck Identifikationssysteme Unterschiede zwischen Criminal- und Civil AFIS Weitere wichtige ausgewählte biometrische Anwendungen: ePassport-biometrische ID-Dokumente, eBorder – elektronische biometrische Grenzsysteme, biometrische Wählerregistrierung) Biometrische Standards und Standarddatenformate (BioAPI 2.0, CBEFF, ISO 19794, NIST)
Qualifikationsziele des Moduls	Kenntnisse über die Historie der Biometrie und ihr Einsatz in Kriminalistik und Forensik Verständnis biometrischer Grundbegriffe, wie Identifikation, Verifikation, etc. Kenntnisse des Grundaufbaus biometrischer Systeme Übersicht über die wichtigsten biometrischen Verfahren (Fingerabdruck-, Gesichts- und Iriserkennung) Umsetzung dieser Verfahren in automatisierten Biometriesystemen (Schwerpunkt AFIS) Kenntnisse wichtiger Grundgrößen zur Evaluierung der Performanz biometrischer Systeme, wie False Acceptance Rate, False Reject Rate, Equal-Error-Rate, etc. Grundkenntnisse biometrischer Standards
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik – IT-Forensik

	Grundkenntnisse in Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse der Bildverarbeitung PM 26: Grundlagen der Bild- und Videoverarbeitung
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 31 Netzwerktechnik und Sicherheitsmanagement	
Modulbezeichnung Englisch: Network- and Security Management	
Modulverantwortliche(r)	Prof. Dr. Nils Gruschka
Inhalte des Moduls	Sicherheitsprobleme und Angriffe in Netzwerken Angewandte Kryptographie Kryptographische Schlüsselaustauschverfahren Zertifikate und Public-Key-Infrastructure Transport Layer Security E-Mail-Sicherheit
Qualifikationsziele des Moduls	Befähigung zur Bewertung der Sicherheitsarchitektur vernetzter Rechnersysteme, Befähigung zur Bewertung von Angriffsmechanismen und sicherheitsrelevanten Aspekten von vernetzten Rechnersystemen, Befähigung zum Verstehen und Bewerten von Mechanismen und Strategien zur Erhöhung der Sicherheit von Rechnernetzen, Befähigung zur Administration sicherheitsspezifischer Mechanismen in Rechnernetzen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in Informatik: PM 2 Computersysteme I: Grundlagen der technischen Informatik PM 6 Betriebssysteme
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 32 Forensische Analyse Bilder und Videos	
Modulbezeichnung Englisch: Forensic Analysis of Images and Videos	
Modulverantwortliche(r)	Prof. Dr. rer. nat. Herbert Litschke
Inhalte des Moduls	Inbetriebnahme einer angepassten Programmierumgebung für das maschinelle Sehen Kriterien zum Erkennen von Bildmanipulationen Grundlagen der Beleuchtung Repräsentation von Bildinhalten durch Frequenzen Keypoint-orientierte Verfahren zur Objekterkennung Methoden zur Beschreibung / Erkennung von Bewegungen
Qualifikationsziele des Moduls	Aufbauend auf den erlernten Grundlagen der Bildverarbeitung werden ausgesuchte Aspekte hinsichtlich der forensischen Verwendung vertieft und an einfachen Beispielen selbst programmiert. Schwerpunkte sind sowohl Methoden der Erkennung von Bildmanipulationen als auch der Einsatz der Bildanalyse zum Finden von Objekten oder zum Erkennen und Verfolgen von Bewegungen
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	Grundkenntnisse in der Programmierung: PM 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse in Informatik: PM 1: Einführung in die Informatik Grundkenntnisse der Bildverarbeitung PM 26: Grundlagen der Bild- und Videoverarbeitung
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung K120
Arbeitsaufwand	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	5
Angebotsturnus	Wintersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 33 Technischer Datenschutz	
Modulbezeichnung Englisch: Technical Privacy	
Modulverantwortliche(r)	Hon.-Prof. Dipl. Ing.(FH) Ulf Glende
Inhalte des Moduls	Einführung in die nationalen und europäischen Grundlagen des Datenschutzrechts, vor allem den technischen und organisatorischen Maßnahmen BDSG (§9) bzw. der europäischen Datenschutz-Grundverordnung Aufnahme und Bewertung der technischen und organisatorischen Abläufe in Unternehmen unter Einbeziehung der Anforderungen des Datenschutzes und der Vorgaben der Datenschutzaufsichtsbehörden technische Anforderungen an eine Datenschutzkonforme Verarbeitung von personenbezogenen Daten Überschneidungen von IT-Sicherheit und TOM (Datenschutz) Nutzen des Standard-Datenschutzmodell als Vorgabe der Datenschutzbehörden
Qualifikationsziele des Moduls	Verständnis zur Umsetzung der datenschutzrechtlichen Vorgaben in der IT Wissen zu technischen und organisatorischen Anforderungen im europäischen Datenschutz und BDSG Befähigung zu Prüfungen im Bereich des technischen Datenschutzes auf der Grundlage der europäischen Datenschutz-Grundverordnung und des BDSG (§9)
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL
Arbeitsaufwand	75 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	3
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 34 Thesis Seminar	
Modulbezeichnung Englisch: Thesis Seminar	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Grundsätze und Techniken wissenschaftlichen Arbeitens, selbständiges Verfassen wissenschaftlicher Texte und ihrer Dokumentation, Grundlagen der Rhetorik und Präsentation, Präsentation von Arbeitsergebnissen (face-to-face, online, offline), effektiver Umgang mit persönlichkeitsspezifischen Sach- und Sozialkompetenzen unter Bezug auf die Fragestellungen aus dem Gebiet der IT-Forensik.
Qualifikationsziele des Moduls	Die Studierenden beherrschen die Grundsätze wissenschaftlicher Arbeit bezüglich der Dokumentation und Nachvollziehbarkeit wissenschaftlicher Arbeiten (insbes. Zitierweise, Quellenangaben, Gliederungsstruktur). Sie kennen die gängigen Verfahren der Quellenrecherche und sind in der Lage, eigenständig Texte zu verfassen, die den üblichen akademischen Anforderungen entsprechen. Auch können sie ihre Arbeitsergebnisse situationsadäquat und unter Nutzung aktueller Medien und Techniken präsentieren. Sie haben gelernt, die dazu nötigen Sach- und sozialen Kompetenzen persönlichkeits- und situationsadäquat zu nutzen. Die Studierenden sind in Bezug auf ihre rhetorische Kompetenz sensibilisiert, was sie in die Lage versetzt, komplexe Sachverhalte zunehmend verständlicher zu vermitteln und in Diskussionen Standpunkte argumentativ zu begründen. Die Studierenden sind informiert über die Aufbereitung von Arbeitsergebnissen und über die rhetorische Gestaltung einer Präsentation (Vortrag).
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bestehen der Modulprüfung APL (z. B. 15minütige Präsentation (Vortrag))
Arbeitsaufwand	50 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Leistungspunkte	2
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben

Modulbezeichnung Deutsch: PM 35 Bachelor-Thesis + Kolloqium	
Modulbezeichnung Englisch: Bachelor's Thesis	
Modulverantwortliche(r)	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Inhalte des Moduls	Es handelt sich um eine praxisbezogene theoretische Auseinandersetzung mit aktuellen Fragestellungen aus einem Teilgebiet des Studiums. Die Thesis sollte inhaltlich anspruchsvoll, wissenschaftlich theoretisch fundiert und zugleich praxisbezogen ausgerichtet sein. Mit Hilfe der Analyse und Auswertung aktueller Erkenntnisse des Fachgebietes, sollen die Studierenden auf der Basis ihres Wissens eigene Standpunkte aufstellen, Lösungsansätze entwickeln und diese in geeigneter Weise darstellen. Wesentlicher Inhalt des Kolloquiums ist die mündliche Präsentation der Inhalte und Ergebnisse der vorangegangenen Thesis der Studierenden. Im Anschluss an die mündliche Präsentation erfolgt eine Diskussion über eventuelle Unklarheiten oder Schwachstellen der Thesis sowie über themenübergreifende, das Studium betreffende Inhalte.
Qualifikationsziele des Moduls	Der Anspruch eines Studiums ist es, neben der fachspezifischen Vermittlung von berufspraktischen Inhalten, Studierende zur selbstständigen wissenschaftlichen und interdisziplinären Recherche und Problemanalyse zu befähigen. Im Rahmen einer Thesis soll dokumentiert werden, dass die Studierenden in der Lage sind, innerhalb einer vorgegebenen Frist ein fachspezifisches Problem selbstständig mit dem im Studium erlernten Fach- und Methodenwissen nach wissenschaftlichen Methoden zu bearbeiten sowie einen Themenbereich vertieft analysieren und weiterentwickeln zu können und gewonnene Ergebnisse in die wissenschaftliche und fachpraktische Diskussion einzuordnen. Die Thesis wird durch das Kolloquium ergänzt. Im Rahmen des Kolloquiums soll festgestellt werden, ob die Studierenden in der Lage sind, die Ergebnisse ihrer Thesis in überzeugender Weise, unter Berücksichtigung der fachlichen Grundlagen und interdisziplinären Zusammenhänge, mündlich zu präsentieren und selbstständig zu begründen sowie ggf. die Bedeutung für die Praxis mit einzubeziehen. Ebenso erhalten die Studierenden die Möglichkeit auf eventuelle Unklarheiten und Schwachstellen ihrer Thesis einzugehen und diese richtig zu stellen. Themenfindung der Thesis erfolgt in Absprache mit dem Betreuer unter Berücksichtigung folgender Punkte: • Einordnung in den Studiengang • Umfang

	• wissenschaftlicher Anspruch • Praxisrelevanz • ausreichendes Vorhandensein entsprechender Literatur Das Kolloquium behandelt das Thema der jeweiligen Thesis der Studierenden sowie angrenzende, das Studium betreffende Inhalte.
ggf. Sprache	Deutsch
Lehr- und Lernformen	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Präsenzveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen
Voraussetzung für die Teilnahme	keine
Verwendbarkeit des Moduls	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Voraussetzungen für die Vergabe von Leistungspunkten	Bachelor-Thesis Kolloquium (mündliche Verteidigung der Bachelor-Thesis)
Arbeitsaufwand	375 h Selbststudium
Leistungspunkte	15
Angebotsturnus	Sommersemester
Dauer des Moduls	1 Semester
Literaturangaben	Die Literatur wird zu Beginn des Semesters bekannt gegeben