Modul 1: Einführung in die Informatik – IT-Forensik

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Einführung in die Informatik – IT-Forensik
Kürzel	EI
Semester:	1 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	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
Arbeitsaufwand:	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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 • Kenntnisse über die Informatik-Schwerpunkte im Studiengang und die Inhalte der einzelnen Informatik-Lehrveranstaltungen • Befähigung zur Einordnung von forensischen Fragestellungen in Bezug auf den Nutzung des Computers
Inhalt:	• Einführung in das Fernstudium „IT-Forensik": Informatik im Kontext forensischer Fragestellungen • Was ist Informatik? • Historie und Teilgebiete der Informatik • Medieninformatik: die Medientypen Bild, Audio, Text, Video • Logik und Boolsche Algebra • Entwicklungsschritte eines Programmes und der Programmierwerkzeuge • Information und Daten • Programmiersprachen: Daten und Algorithmen • Algorithmen und Datenstrukturen • Grundlegende Aspekte der Automatentheorie • Grundlegende Probleme der Berechenbarkeit • Grundlegende Probleme der Komplexitätstheorie
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung o. Alternative Prüfungsleistung

Literatur:	🕮 H.-P. Gumm, M. Sommer: Einführung in die Informatik, Oldenburg Wissenschaftsverlag 2012 🕮 H. Herold, B. Lurz, J. Wohlrab: Grundlagen der Informatik, Pearson Studium, 2012 🕮 R. Malaka, A. Butz, H. Hussmann: Medieninformatik: Eine Einführung. Pearson Studium, 2009 🕮 R. Hattenhauer: Informatik für Schule und Ausbildung – Lehr und Lernbuch für Schule und Ausbildung. Pearson Studium, 2010 🕮 P. Levi, U. Rembold: Einführung in die Informatik – für Naturwissenschaftler und Ingenieure. Hanser Fachbuchverlag, 2002 🕮 R. Rechenberg, G. Pomberger (Hrsg.): Informatik-Handbuch, Hanser Fachbuchverlag, 2006 🕮 U. Schneider (Hrsg.): Taschenbuch der Informatik. Hanser Fachbuchverlag, 2012 🕮 P. A. Henning: Taschenbuch Multimedia. Hanser Fachbuchverlag, 2007 🕮 D. Hoffmann: Theoretische Informatik. Hanser Fachbuchverlag, 2011

Modul 2: Computersysteme I: Grundlagen der technischen Informatik

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Computersysteme I : Grundlagen technischer Systeme
Kürzel	CS I
Semester:	1 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	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
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 H.-P. Gumm, M. Sommer: Einführung in die Informatik, Oldenburg Wissenschaftsverlag 2012 🕮 H. Herold, B. Lurz, J. Wohlrab: Grundlagen der Informatik, Pearson Studium, 2012 🕮 R. Malaka, A. Butz, H. Hussmann: Medieninformatik: Eine Einführung. Pearson Studium, 2009 🕮 Taschenbuch Multimedia, P. A. Henning; Hanser Fachbuchverlag, 2007 🕮 Digitale Film- und Videotechnik, U. Schmidt, Hanser Fachbuchverlag, 2002

Modul 3: Zahlentheoretische Grundlagen

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Zahlentheoretische Grundlagen
Kürzel:	ZG
Semester:	1 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. habil. A. Ahrens
Dozent(in):	Prof. Dr.-Ing. habil. A. Ahrens
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Mathematische Grundkenntnisse
Lernziele / Kompetenzen:	• 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
Inhalt:	• Einführung in die lineare Algebra • Grundlagen der Algebra (Gruppen, Ringe, (endliche) Körper) • Grundlagen der Elementaren Zahlentheorie • Modulares Rechnen
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung

Literatur:	🕮 Schott, D.: Ingenieurmathematik mit MATLAB. Leipzig: Fachbuchverlag, 2004 🕮 Papula, L.: Mathematik für Ingenieure und Naturwissenschaftler, Band 1 – 3,Vieweg, 2001 🕮 Kurzweil, H.: Endliche Körper: Verstehen, Rechnen, Anwenden. Berlin, Heidelberg: Springer, 2008 🕮 Müller-Stach, S.; Piontkowski, J.: Elementare und algebraische Zahlentheorie: Ein moderner Zugang zu klassischen Themen. Wiesbaden: Vieweg+Teubner, 2011

Modul 4: Kriminalistik

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Kriminalistik
Kürzel	KRI
Semester:	1 Semester
Modulverantwortliche(r):	Prof. Dr. Roll/Verwaltungsfachhochschule Güstrow
Dozent(in):	Prof. Dr. Roll/Verwaltungsfachhochschule Güstrow
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Ackermann, R.: Kriminalistische Fallanalyse, Lehr- und Studienbriefe Kriminalistik Band 1; 3. Auflage Verlag Deutscher Polizeiliteratur, Hilden 2010 🕮 Ackermann, R.; Clages, H.; Roll, H.: Handbuch der Kriminalistik, 4. Auflage, Boorberg Stuttgart 2011

	🕮 Artkämper, H.; Clages, H.: Kriminalistik gestern – heute – morgen; Schriftenreihe der DGfK Band 4, Boorberg Stuttgart 2013 🕮 Berthel, R.; Mentzel, Th.; Neidhardt, K.; Schröder, D.; Spang, Th.: Grundlagen der Kriminalistik/Kriminologie, Lehr- und Studienbriefe Kriminalistik Band 1; 3. Auflage Verlag Deutscher Polizeiliteratur, Hilden 2008 🕮 Clages, H. (Hrsg.): Der rote Faden, 12. Auflage, Kriminalistik Verlag Heidelberg 2012 🕮 Wirth, I. (Hrsg.): Kriminalistik Lexikon; 4. Auflage, Kriminalistik Verlag Heidelberg 2011

Modul 5: Kriminologie

Studiengang:	IT-Forensik
Modulbezeichnung:	Kriminologie
Kürzel	KR
Semester:	1 Semester
Modulverantwortliche(r):	PD Dr. iur. habil. M. Tamm
Dozent(in):	PD Dr. iur. habil. M. Tamm
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h, davon 8h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• Das Modul befähigt die Teilnehmer, das Begehen von Straftaten durch Menschen und deren Auswirken anhand unterschiedlicher wissenschaftlicher Erklärungsversuche soziologisch einordnen zu können.
Inhalt:	• 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.: Wirtschafts-kriminalität, Organisierte Kriminalität und die Kriminalität von Kindern) • Möglichkeiten und Grenzen sozialer und rechtlicher Kontrolle von Kriminalität
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Eisenberg, Kriminologie 🕮 Göppinger, Kriminologie

	🕮 Albrecht, Peter-Alexis: Kriminologie, 4. Aufl., Beck 2010 🕮 Meier, Bernd-Dieter: Kriminologie, 4. Aufl., Beck 201 🕮 Bock, Michael, Kriminologie, 4. Aufl., Vahlen, München 2013 🕮 Eisenberg, Ulrich: Kriminologie, 6. Aufl., Beck 2005

Modul 6: Betriebssysteme

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Betriebssysteme
Kürzel	BS
Semester:	2 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. E. Jonas
Dozent(in):	Prof. Dr.-Ing. E. Jonas
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h, davon 8h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I: Grundlagen der technischen Informatik
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung

Literatur:	🕮 Andrew S. Tannenbaum.: Moderne Betriebssysteme. 3. aktualisierte Auflage, Prentice Hall, 2009 🕮 W. Stallings: Operating Systems: Internals and Design Principles. Prentice-Hall 2001. (deutsch: Betriebssysteme - Prinzipien und Umsetzung. Pearson 2003) 🕮 Bengel, G.: Betriebssysteme. Hüthig – Verlag 1990 🕮 Rosen, K., Rosinski, R., Farber, J.: UNIX – System V Rel. 4. te-wi Verlag München 1993

Modul 7: Informationsrecherche im Internet

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Informationsrecherche im Internet
Kürzel:	IRI
Semester:	2 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h, davon 8h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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: o Precision and Recall o Stichwortidentifikation o Stoppworteliminierung • Suchmaschinen (Google, Bing, Yahoo u.a.) und ihre Suchoperatoren • Optimierung der Internet-Recherche • Beurteilung von Informationen aus Internet-Recherchen • Dark- und Deep-Web o Definition o Inhalte des Dark Webs o Systemische Recherche im Deep Web o Anonymes Verhalten im Deep Web

Studien- Prüfungsleistungen:	alternative Prüfungsleistung
Literatur:	🕮 R. Müller, J. Plieninger, C. Rapp: Recherche 2.0: Finden und Weiterverarbeiten in Studium und Beruf. Springer Verlag, 2013 🕮 P. Berger: Unerkannt im Netz: Sicher kommunizieren und recherchieren im Internet. UvK, 2008 🕮 T. Alby: Web 2.0 - Konzepte, Anwendungen, Technologien. Hanser Fachbuchverlag, 2008 🕮 D. Chung, A. Klünder: Suchmaschinen-Optimierung: Der schnelle Einstieg. mitp verlag, 2007 🕮 S: Erlhofer: Suchmaschinen-Optimierung: Das umfassende Handbuch: Aktuell zu Google Panda und Penguin, Galileo Computing, 2012 🕮 Handbuch Internet-Recherche auf http://www.werle.com/ (Januar 2014) 🕮 Suchmaschinen-Optimierung auf www.suchmaschinen-doktor.de (Januar 2014) 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 8: Programmierung I: Grundlagen der Programmierung

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Programmierung I: Grundlagen der Programmierung
Kürzel:	PRO I
Semester:	2 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. I. Müller
Dozent(in):	Prof. Dr.-Ing. I. Müller
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik
Lernziele / Kompetenzen:	• Befähigung zum Programmieren z.B. in C, C++
Inhalt:	• Einführung in die Entwicklungsumgebung • Elementare Sprachelemente • Steueranweisungen • Funktionen • Datenstrukturen • Fortgeschrittene Zeigertechnik • Ein-/ Ausgabeoperationen • Programmstrukturierung, Speicherklassen • Objektorientierte Programmierung (Klassen, Vererbung, • Polymorphie) • Anwendung WinAPI • MFC Programmierung

Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Kurzweil, H.: Endliche Körper: Verstehen, Rechnen, Anwenden. Berlin, Heidelberg: Springer, 2008 🕮 Goll, G.; Grüner, U.; Wiese, H.: C als erste Programmiersprache. 4. Auflage, B. G. Teubner Stuttgart Leipzig Wiesbaden 2003 🕮 Louis, D.: Easy C++: 1. Auflage, Verklag Markt + Technik München 2001 🕮 Mittelbach, H.: Einführung in C++. 2. Auflage, Fachbuchverlag Leipzig 2002 🕮 Helmke, H.; Isernhagen, R.: Softwaretechnik in C und C++ - Das Lehrbuch. Hanser Verlag München Wien 2001

Modul 9: Datenschutzrecht

Studiengang:	IT-Forensik
Modulbezeichnung:	Datenschutzrecht
Kürzel	DSR
Semester:	2 Semester
Modulverantwortliche(r):	PD Dr. iur. habil. M. Tamm
Dozent(in):	PD Dr. iur. habil. M. Tamm
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung ohne Note
Literatur:	🕮 Simitis, Siros: Bundesdatenschutzgesetz (Kommentar), 8. Aufl., Nomos, Baden-Baden 2014

	🕮 Gohla, Peter/Schomerus, Rudolf (Hrsg.), BDSG: Bundesdatenschutzgesetz (Kommentar), 11. Aufl. Beck, München 2012 🕮 Däubler, Wolfgang: Kompaktkommentar zum BDSG, 4. Aufl., Bund Verlag, Frankfurt/M. 2011 🕮 Kühling, Jürgen, Datenschutzrecht, 2. Aufl., C.F. Müller, Heidelberg 2011 🕮 Leupold, Andreas/Glosser, Silke: Münchner Anwaltshandbuch IT-Recht, Beck 2011

Modul 10: Algorithmen und Datenstrukturen

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Algorithmen und Datenstrukturen
Kürzel	ADS
Semester:	3 Semester
Modulverantwortliche(r):	Prof. Dr. -Ing. M. Kreuseler
Dozent(in):	Prof. Dr. -Ing. M. Kreuseler
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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

Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Sedgewick, R.: Algorithmen. Addison-Wesley, Pearson-Studium, 2002 🕮 Cormen, T.H.; Leiserson, C.E.; Rivest, R.L.: Introduction to Algorithms. The MIT Press, 2009

Modul 11: Computersysteme II: Software-Architekturen

Studiengang:	IT-Forensik
Modulbezeichnung:	Computersysteme II: Software-Architekturen
Kürzel	CS II
Semester:	3 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. O. Zukunft (HAW Hamburg)
Dozent(in):	Prof. Dr.-Ing. O. Zukunft (HAW Hamburg)
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik
Lernziele / Kompetenzen:	• 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
Inhalt:	• Pattern und Muster für SW-Architekturen (Design Pattern) • Modellierung von SW-Architekturen (MVC, PAC, Test driver architecture) • Evaluation von SW-Architekturen • Software-Qualität o Definitionen und Standards o Funktionstest, Überdeckungsmaße o HiL-, Integrations- und Abnahmetests o Verifikation und Validierung • Architecture Design and Reliability
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 *Reussner, Ralf, Handbuch der Software-Architekturen, dpunkt Verlag, 2008* 🕮 *Starke, Gernot, Effektive Software-Architekturen, Hanser Verlag, 2011* 🕮 *Bass, Clements, and Kazman. Software Architecture in Practice. Addison-Wesley, 2nd edition, 2003.* 🕮 *Starke, Gernot, Patterns kompakt, Springer Vieweg 2013*

Modul 12: Systemnahe Programmierung

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Systemnahe Programmierung
Kürzel:	SysProg
Semester:	3 Semester
Modulverantwortliche(r):	Dr. O. Hagendorf
Dozent(in):	Dr. O. Hagendorf
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden wie Internet-based teaching; Abschlussveranstaltung zur Prüfungsvorbereitung und Klärung offener Fragen bzw. Vorstellung der APL (online)
Arbeitsaufwand:	125 h, davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CP
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 6: Betriebssysteme • Modul 8: Programmierung I: Grundlagen der Programmierung
Lernziele / Kompetenzen:	Befähigung zur Administration von Linux und Programmierung systemnaher Anwendungen
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung oder 120-minütige schriftliche Prüfung
Literatur:	🕮 Hagendorf: Studienanweisung Systemnahe Programmierung 🕮 Kofler: Linux Kommandoreferenz: Shell-Befehle von A bis Z. Rheinwerk Computing, 5. Auflage, 2020 (ISBN: 978-3836278584) 🕮 Glatz: Betriebssysteme: Grundlagen, Konzepte, System-programmierung. dpunkt.verlag GmbH, 4.Auflage, 2019 ISBN: 978-3864907050) 🕮 Ehses, Köhler, Riemer, Stenzel, Victor: Systemprogrammierung in UNIX. Vieweg+Teubner Verlag, 1.Auflage, 2012 (ISBN: 978-3834814180) 🕮 Rago, Stevens: Advanced Programming in the UNIX Environment; Addison Wesley. 3. Auflage, 2013 (ISBN: 978-0321637734)

Modul 13: Cybercrime I: Computerkriminalität im engeren Sinne

Studiengang:	IT-Forensik
Modulbezeichnung:	Cybercrime I: Computerkriminalität im engeren Sinne
Kürzel	CC I
Semester:	3 Semester
Modulverantwortliche(r):	PD Dr. iur. habil. M. Tamm
Dozent(in):	PD Dr. iur. habil. M. Tamm
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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.
Inhalt:	• 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.
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Annette Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl.., Beck, München 2010 🕮 Marco Gercke/ Phillip W. Bruns, Praxishandbuch Internetstrafrecht, Kohlhammer, Stuttgart 2009

Modul 14: Programmierung II: Script Sprachen

Studiengang:	Fernstudiengang IT-Forensik
Modulbezeichnung (Deutsch):	Programmierung II: Skript Sprachen
Kürzel:	PRO II
Semester:	3 Semester
Modulverantwortliche(r):	Dr.-Ing. M. Berg
Dozent(in):	Dr.-Ing. M. Berg
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in der Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung
Lernziele / Kompetenzen:	• Beherrschung von Client- und Serverseitigen Scriptsprachen • Befähigung zum Programmieren von dynamischen Webseiten • Befähigung zum Analysieren von Skripten in Webseiten
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 David Flanagan: JavaScript – kurz und gut, O'Reilly 2012 🕮 Maximilian Vollendorf, Frank Bongers: JQuery – das Praxisbuch, Galileo Computing 2012 🕮 Stefan Reimers, Gunnar Thies: PHP 5.4 & MySql 5.5, Galileo Computing 2012 🕮 Ralph Steyer: AJAX mit PHP, addison wesley 2006

Modul 15: Datenbanken I: Grundlagen von Datenbanksystemen

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Datenbanken I: Grundlagen von Datenbanksystemen
Kürzel	DB I
Semester:	4 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung o. Alternative Prüfungsleistung
Literatur:	🕮 A. Kemper, A. Eickler.: Datenbanksysteme – Eine Einführung, Oldenbourg Verlag, 2013 🕮 R. A. Elmasr, S. B. Navathe: Grundlagen von Datenbanksystemen, 3. Auflage, Pearson Studium, 2009 🕮 A. Heuer, K. Sattler, G. Saake: Datenbanken –Konzepte und Sprachen. MITP Verlag, 2013 🕮 Vossen, G.; Datenbankmodelle, Datenbanksprachen und Datenbankmanagement-Systeme. Oldenbourg, München, 2008 🕮 A. Heuer, G. Saake, K. Sattler; Datenbanken: Implementierungskonzepte mitp-Verlag, Bonn, 2011 🕮 Dokumentation MySQL, MSSQLServer bzw. PostgreSQL-Datenbanksysteme

Modul 16: Ethical Hacking

Studiengang:	IT-Forensik
Modulbezeichnung:	Ethical Hacking
Kürzel	EH
Untertitel	Bedrohungen und Angriffstechniken in Computersystemen
Semester:	4 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. E. Jonas
Dozent(in):	Prof. Dr.-Ing. E. Jonas
Sprache:	Deutsch
Zuordnung zum Curriculum	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform / SWS:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h, davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I • Modul 6: Betriebssysteme
Lernziele / Kompetenzen:	• Kenntnissen über Strukturierungsprinzipien von Betriebssystemen und Rechnernetzen, • Vertiefte Kenntnissen über Aufbau, Funktion und Wirkmechanismen von Betriebssystemen, insbesondere der der Netzwerkschnittstelle • 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, komplexe Zusammenhänge in Betriebssystemen zu verstehen und für die Abwehr von Bedrohungen anwenden zu können, • Grundlegende Kenntnisse in der Administration von Betriebssystemen
Inhalt:	• Grundlagen, Prinzipien und Architekturen von Computersystemen und Rechnernetzen, • Ethical Hacking • Strukturierungsprinzipien von Rechnernetzen, • Rechner- und Internet-Unsicherheit, • Klassifikation, Mechanismen und Wirkprinzipien von Bedrohungen und Angriffen, • Schutz vor Bedrohungen und Abwehr von Angriffen,
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Andrew S. Tannenbaum.: Moderne Betriebssysteme. 3. aktualisierte Auflage, Prentice Hall, 2009 🕮 W. Stallings: Operating Systems: Internals and Design Principles. Prentice-Hall 2001. (deutsch: Betriebssysteme - Prinzipien und Umsetzung. Pearson 2003)

	🕮 Bengel, G.: Betriebssysteme. Hüthig – Verlag 1990 🕮 *Claudia Eckert: IT-Sicherheit, 5. Auflage, Oldenbourg-Verlag, 2007* 🕮 *Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate: Praxisbuch Sicherheit für Linux-Server und –Netze, Hanser-Verlage, 2004* 🕮 *Charles P. Pfleeger, Sharie L. Pfleeger: Security in Computing, Pearson 2006/2008* 🕮 *Simson Garfikel, Gene Spafford: Practical UNIX & Security, O'Reilly, 2003* 🕮 *Charly Kaufman, Radia Perlman, Mike Speciner: Network Security, Prentice Hall, 2002*

Modul 17: Computer Forensik I: Grundlagen

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Computer Forensik I: Grundlagen
Kürzel	CFI
Semester:	4 Semester
Modulverantwortliche(r):	H.-P. Merkel
Dozent(in):	H.-P. Merkel
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik Betriebssystem-Grundkenntnisse: • Modul 6: Betriebssysteme
Lernziele / Kompetenzen:	Das Modul befähigt Teilnehmer 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.
Inhalt:	1. 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 2. Identifizierung und Datensicherung von relevanten Datenquellen 3. Wiederherstellung von gelöschten und geänderten Daten 4. Umgang mit Verschlüsselung

	5. Dateianalyse: Allocated, Unallocated, Carving 6. Einsatz der Virtualisierung in der Forensik 7. Parallelen und Gemeinsamkeiten der Forensik zu mobilen Geräten 8. Kennenlernen von IT-Forensik-Werkzeugen 9. Zeitstempel Informationen einbinden (Timelines und Supertimelines) 10. Windows spezifische Artefakte (VSS, Prefetch, Registry)
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Carrier, B.: File System Forensic Analysis. Addison-Wesley 🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 18: Cybercrime II: Computerkriminalität im weiteren Sinne

Studiengang:	IT-Forensik
Modulbezeichnung:	Cybercrime II: Computerkriminalität im weiteren Sinne
Kürzel	CC II
Semester:	4 Semester
Modulverantwortliche(r):	PD Dr. iur. habil. M. Tamm
Dozent(in):	PD Dr. iur. habil. M. Tamm
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Recht: • Modul 13: Cybercrime I: Computerkriminalität im engeren Sinne
Lernziele / Kompetenzen:	• 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.
Inhalt:	• Vermittlung von Kenntnissen zu Straftatbestände, 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.
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Annette Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl.., Beck, München 2010 🕮 Marco Gercke/ Phillip W. Bruns, Praxishandbuch Internetstrafrecht, Kohlhammer, Stuttgart 2009

Modul 19: IT-Forensik-Projekt I

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	IT-Forensik-Projekt I
Kürzel	P I
Semester:	4 Semester
Modulverantwortliche(r):	PD Dr. iur. habil. M. Tamm
Dozent(in):	PD Dr. iur. habil. M. Tamm
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Recht • Modul 4: Kriminalistik • Modul 5: Kriminologie • Modul 9: Datenschutzrecht • Modul 13: Cybercrime I: Computerkriminalität im engeren Sinne
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung oder 120-minütige schriftliche Prüfung
Literatur:	🕮 Spezielle Literatur ausgerichtet auf das Projektthema

Modul 20: Kryptografie I

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Kryptographie I
Kürzel:	KR I
Semester:	5 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. habil. A. Ahrens
Dozent(in):	Prof. Dr.-Ing. habil. A. Ahrens
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform / SWS:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Mathematik: • Modul 3: Zahlentheoretische Grundlagen Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I: Grundlagen der technischen Informatik)
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Beutelsbacher, A.; Schwenk,J.;Wolfenstetter, K.-D.: Moderne Verfahren der Kryptographie. Wiesbaden: Vieweg+Teubner, 2010 🕮 Beutelspacher, A.; Neumann, H.B.; Schwarzpaul, T.: 🕮 Kryptografie in Theorie und Praxis. Wiesbaden: Vieweg+Teubner, 2009

	🕮 Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners.Berlin, Heidelberg: Springer, 2009. 🕮 Delfs, H., Knebl, H.: Introduction to Cryptography. Principles and Applications. Berlin, Heidelberg: Springer, 2002. 🕮 Mollin, R.A.: RSA and Public-Key Cryptography. Boca Raton, London, New York: CRC Press, 2003. Boca Raton, London, New York: CRC Press, 2003.

Modul 21: Datenbanken II: Forensik in DBS

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Datenbanken II: Forensik in DBS
Kürzel:	DB II
Semester:	5 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Datenbanken • Modul 15: Datenbanken I
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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.
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung

Literatur:	🕮 A. Kemper , A. Eickler: Datenbanksysteme – Eine Einführung, Oldenbourg Verlag, 2013 🕮 R. A. Elmasr, S. B. Navathe: Grundlagen von Datenbanksystemen, 3. Auflage, Pearson Studium, 2009 🕮 A. Heuer, K. Sattler, G. Saake: Datenbanken –Konzepte und Sprachen. MITP Verlag, 2013 🕮 Vossen, G.; Datenbankmodelle, Datenbanksprachen und Datenbankmanagement-Systeme. Oldenbourg, München, 2008 🕮 A. Heuer, G. Saake, K. Sattler; Datenbanken: Implementierungskonzepte mitp-Verlag, Bonn, 2011 🕮 Dokumentation MySQL, MSSQLServer bzw. PostgreSQL-Datenbanksysteme 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 22: Forensik auf mobilen Geräten

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Forensik auf mobilen Geräten
Kürzel	FMG
Semester:	5 Semester
Modulverantwortliche(r):	H.P.-Merkel
Dozent(in):	H.-P. Merkel
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I: Grundlagen der technischen Informatik Grundkenntnisse in der Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse in Betriebssysteme: • Modul 6: Betriebssysteme
Lernziele / Kompetenzen:	Das Modul befähigt die Teilnehmer 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.
Inhalt:	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.
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Andrew Hoog: Android Forensics. Syngress Verlag 2011 🕮 C. Altheide und H. Carvey: Digital Forensics with Open Source Tools Syngress Verlag 2011 🕮 R.Tamma: Learning Android Forensics. Puckt Publishing 2015 🕮 Carrier, B.: File System Forensic Analysis. Addison-Wesley 🕮 T. Fuchß: Mobile Computing – Grundlagen und Konzepte für mobile Anwendungen. Hanser Fachbuchverlag, 2009 🕮 T. Alby: Das mobile Web, Hanser Fachbuchverlag, 2008 🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 23: Malware-Analyse

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Malware-Analyse
Kürzel:	MalAn
Semester:	5. Semester
Modulverantwortliche(r):	Dr. O. Hagendorf
Dozent(in):	Dr. O. Hagendorf
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht
Arbeitsaufwand:	125 h, davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CP
Voraussetzungen:	Grundkenntnisse in Informatik und Programmierung: • Modul 1: Einführung in die Informatik • Modul 6: Betriebssysteme • Modul 8: Programmierung I: Grundlagen der Programmierung • Modul 12: Systemnahe Programmierung
Lernziele / Kompetenzen:	• Kenntnisse zu Malware Arten und Analysetechniken • Befähigung zur statischen und dynamischen Erkennung und Analyse von Malware • Grundkenntnisse in Assembler- und LowLevel-Programmierung
Inhalt:	• Malware Analyse Tools und Umgebungen

	• Malwarearten und deren Erkennung • Reverse Engineering • Statische und dynamische Analyse • Verschleierung von Funktionalitäten
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung oder 120-minütige schriftliche Prüfung
Literatur:	🕮 Mohanta, Saldanha: Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress, 1. Auflage, 2020 (ISBN: 978-1484261927) 🕮 Monnappa: Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing, 1.Auflage, 2018 (ISBN: 978-1788392501) 🕮 Dang: Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. Wiley, 1. Auflage, 2014 (ISBN: 978-1118787311) 🕮 Eagle, Nance: The Ghidra Book: The Definitive Guide. No Starch Press, 1.Auflage, 2020 (ISBN: 978-1718501027)

Modul 24: Computer Forensik II: Praxis-Aspekte

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Computer Forensik II: Praxis-Aspekte
Kürzel	CFI
Semester:	5 Semester
Modulverantwortliche(r):	Gilbert Löhr
Dozent(in):	Gilbert Löhr
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 15: Computer Forensik I: Grundlagen
Lernziele / Kompetenzen:	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.
Inhalt:	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.
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Carrier, B.: File System Forensic Analysis. Addison-Wesley 🕮 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press 🕮 Geschonneck, A.: Computer Forensik. dpunkt Verlag 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 25: Kryptografie II

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Kryptographie II
Kürzel:	KR
Semester:	6 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. habil. A. Ahrens
Dozent(in):	Prof. Dr.-Ing. habil. A. Ahrens
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform / SWS:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Mathematik: • Modul 1: Zahlentheoretische Grundlagen Grundkenntnisse in Informatik: • Modul 2: Einführung in die Informatik Grundkenntnisse in Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung Grundlagen kryptografischer Systeme: • Modul 20: Kryptografie I
Lernziele / Kompetenzen:	• Kenntnisse über grundlegende kryptographische Techniken, Verfahren und Systeme • Grundlegende Kenntnisse zum Brechen kryptographische Verfahren

Inhalt:	• Kryptographische Techniken, Verfahren und Systeme • Kryptoanalytische Betrachtungen möglicher Angriffe auf kryptographische Verfahren • An definierten Beispielen werden die Grenzen kryptografischer Verfahren praktisch ausgelotet
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 *Schmeh, K.: Kryptografie: Verfahren-Protokolle-Infrastrukturen. Heidelberg: dpunkt-Verlag, 2013* 🕮 *Beutelsbacher, A.; Schwenk,J.;Wolfenstetter, K.-D.: Moderne Verfahren der Kryptographie. Wiesbaden: Vieweg+Teubner, 2010* 🕮 *Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners.Berlin, Heidelberg: Springer, 2009.* 🕮 *Delfs, H., Knebl, H.: Introduction to Cryptography. Principles and Applications. Berlin, Heidelberg: Springer, 2002.* 🕮 *Mollin, R.A.: RSA and Public-Key Cryptography. Boca Raton, London, New York: CRC Press, 2003.*

Modul 26: Grundlagen der Bild- und Videoverarbeitung

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Grundlagen der Bildverarbeitung
Kürzel	BV
Semester:	6 Semester
Modulverantwortliche(r):	Prof. Dr. rer. nat. H. Litschke
Dozent(in):	Prof. Dr. rer. nat. H. Litschke
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in der Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I: Grundlagen technischer Systeme
Lernziele / Kompetenzen:	Verständnis optischer Systeme. 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
Inhalt:	• Grundlagen der Optik und Fotografie • Statistische Bildverarbeitung • Punktoperationen, Nachbarschaftsoperationen und Filter

	• Geometrische Transformationen • Fourier-Analyse von Bilddaten • Grundlagen der Objekterkennung und Segmentierung • Algorithmen zur Merkmalsextraktion • Softwarebibliotheken des Maschinellen Sehens
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 C. Demant, B. Streicher-Abel, P. Waszkewitz: Industrielle Bildverarbeitung, Springer, 2002 🕮 A. Nischwitz, P. Haberäcker: Computergrafik und Bildverarbeitung – Band II, Vieweg+Teubner 2011 🕮 B. Jähne: Digitale Bildverarbeitung und Bildgewinnung, Springer, 2012 🕮 H. Handels: Medizinische Bildverarbeitung, 2. Auflage, Vieweg+Teubner, 2009 🕮 Taschenbuch Multimedia, P.A.Henning; Hanser Fachbuchverlag, 2007

Modul 27: Staatsphilosophie

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Staatsphilosophie
Kürzel	SE
Semester:	6 Semester
Modulverantwortliche(r):	Prof. Dr. iur. B. Wiegand-Hoffmeister
Dozent(in):	Prof. Dr. iur. B. Wiegand-Hoffmeister
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung ohne Note
Literatur:	🕮 Ullrich, Carsten G., Soziologie des Wohlfahrtsstaates, Campus-Verlag, Frankfurt/M. 2005 🕮 Zippelius, Reinhold, Allgemeine Staatslehre. Politikwissenschaft, ein Studienbuch, 16. Aufl., Beck München 2010 🕮 Anter, Andreas/Bleck, Wilhelm: Staatskonzepte. Die Theorie der bundesdeutschen Politikwissenschaft, Campus Verlag, Frankfurt/M./New York 2013 🕮 Kriele, Martin: Einführung in die Staatslehre. Die geschichtlichen Legitimationsgrundlagen des demokratischen Verfassungsstaates, 6. Aufl., Kohlhammer, Stuttgart 2003 🕮 Voigt, Rüdiger/Weiß, Ulrich (Hrsg.): Handbuch der Staatsdenker, Franz Steiner Verlag, Stuttgart 2010

Modul 28: IT-Forensik Projekt II

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	IT-Forensik Projekt II
Kürzel	FEP II
Semester:	6 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik • Modul 2: Computersysteme I: Grundlagen der technischen Informatik Grundkenntnisse in der Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung

	Grundkenntnisse in Betriebssysteme: • Modul 6: Betriebssysteme Grundkenntnisse in der IT-Forensik • Modul 17: Computer Forensik I: Grundlagen der IT-Forensik • Modul 22: Forensik auf mobilen Geräten • Modul 24: Computer Forensik II: Praxis-Aspekte
Lernziele / Kompetenzen:	• Praktische Kenntnissen in der strategischen Aufarbeitung forensischer Fragestellungen • Befähigung zur eigenständigen Aufarbeitung von forensischen Fragestellungen • Befähigung im Team forensische Fragestellungen zu bearbeiten • Befähigung forensische Fragestellungen zu dokumentieren und zu präsentieren
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Spezielle Literatur ausgerichtet auf das Projektthema

Modul 29: Künstliche Intelligenz

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Künstliche Intelligenz
Kürzel:	DM
Semester:	7 Semester
Modulverantwortliche(r):	Prof. Dr. rer. nat. J. Cleve/ NN
Dozent(in):	Prof. Dr. rer. nat. J. Cleve/ NN
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD’s, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Mathematik • Modul 3: Zahlentheoretische Grundlagen Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik

	Grundkenntnisse in Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung
Lernziele / Kompetenzen:	Die Studierenden erwerben Kompetenzen im Einsatz von Analysetechniken, hier speziell auf dem Gebiet der Datenanlyse auf Massendaten. Sie erwerben die Fähigkeit, Data-Mining-Systeme zur Lösung von Analyseaufgabe einzusetzen. Durch Projekt-basiertes Lernen wird die typische Sichtweise auf ein zu lösendes Problem gestärkt. Die Teilnehmer 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.
Inhalt:	Die 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 klassische 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.
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Cleve, J.; Lämmel, U.: Data Mining. DeGruyter. 2020 Weitere Literaturhinweise werden zum Semesterbeginn bekanntgegeben.

Modul 30: Grundlagen und Anwendungen biometrischer Systeme

Studiengang:	IT-Forensik
Modulbezeichnung:	Grundlagen und Anwendungen biometrischer Systeme
Kürzel	GBS
Semester:	7 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. Matthias Kreuseler
Dozent(in):	Prof. Dr.-Ing. Matthias Kreuseler
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensic
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik

	Grundkenntnisse in Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse der Bildverarbeitung • Modul 26: Grundlagen der Bild- und Videoverarbeitung
Lernziele / Kompetenzen:	• 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
Inhalt:	• 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) • Risikobehandlung und Grundprinzipien des Datenschutzes beim Umgang mit Biometriedaten
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 A. Jain, A.A. Ross, K. Nandakumar. Introduction to Biometrics. Springer 2011 🕮 M. Behrens, R. Roth. Biometrische Identifikation. Vieweg+Teubner Verlag, 2013. 🕮 V. Nolde, L. Leger. Biometrische Verfahren. Verlag Deutscher Wirtschaftsdienst 2008. 🕮 D. Maltoni, D. Maio, A. Jain, S. Prabhakar. Handbook of Fingerprint Recognition. Springer, 2009. 🕮 Behrens, M./Roth, R. (Hrsg.), Biometrische Identifikation, Grundlagen, Verfahren, Perspektiven, Vieweg DuD-Fachbeiträge 2001, ISBN 3-528-05786-6 🕮 Stan Z. Li, Anil K. Jain. Handbook of Face Recognition. Springer, 2005.

Modul 31: Netzwerktechnik und Sicherheitsmanagement

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Netzwerktechnik und Sicherheitsmanagement
Kürzel	NWTS
Semester:	7 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. E. Jonas

Dozent(in):	Prof. Dr.-Ing. E. Jonas
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang Forensic Engineering
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik (Modul 2), Betriebssysteme (Modul 6)
Lernziele / Kompetenzen:	• Kenntnisse über Aufbau, Struktur und die Funktionsweise von Rechnernetzen, • 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
Inhalt:	• Motivation und OSI-Sicherheitsarchitektur, • Security Engineering: Vorgehensmodell, Sicherheitsprobleme, Bedrohungen • Kryptologie, symmetrische und asymmetrische Kroptosysteme und –verfahren • Kryptografische Hashfunktionen (MD4/5, Wirpool) • Sicherheitsmechanismen • WLAN-Sicherheit • Komplexe Sicherheitsmechanismen (IPSec, SSL/TSL, ssh) • Firewallsysteme • Forensic in Rechnernetzen (Logfileanalyse, IDS, IPS)
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 Claudia Eckert: IT-Sicherheit, 5. Auflage, Oldenbourg-Verlag, 2007 🕮 Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate: Praxisbuch Sicherheit für Linux-Server und –Netze, Hanser-Verlage, 2004 🕮 Charles P. Pfleeger, Sharie L. Pfleeger: Security in Computing, Pearson 2006/2008 🕮 Simson Garfikel, Gene Spafford: Practical UNIX & Security, O'Reilly, 2003 🕮 Seymour Bosworth, M. E. Kabay: Computer Security Handbook, John Willey & Sons, 2003 🕮 Bruce Schneider: Angewandte Kryptographie, Pearson Studium, 2005 🕮 Charly Kaufman, Radia Perlman, Mike Speciner: Network Security, Prentice Hall, 2002 🕮 Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman: Building Internet Firewalls, O'Reilly, 2002 🕮 Martin Kappes: Netzwerk- und Datensicherheit, Eine praktische Einführung, Springer Vieweg, 2013. 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 32: Forensische Analyse von Bildern und Videos

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Forensische Analyse von Bildern und Videos
Kürzel	FABV
Semester:	7 Semester
Modulverantwortliche(r):	Dr. Dima Pröfrock
Dozent(in):	Dr. Dima Pröfrock
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	125 h davon 8 h Seminaristischer Unterricht (Präsenz)
Kreditpunkte:	5 CR
Voraussetzungen:	Grundkenntnisse in Informatik: • Modul 1: Einführung in die Informatik Grundkenntnisse in Programmierung: • Modul 8: Programmierung I: Grundlagen der Programmierung Grundkenntnisse der Bildverarbeitung • Modul 26: Grundlagen der Bild- und Videoverarbeitung
Lernziele / Kompetenzen:	In dem Modul wird ein Verständnis relevante, in der forensischen Bildanalyse häufig eingesetzter Softwaresysteme für die forensische Bildauswertung vermittelt. Im Anschluss sind die Studierenden befähigt, diese Softwaresysteme informiert und gezielt auszuwählen und gegebenenfalls zu bedienen.
Inhalt:	Basierend auf dem Modul "Grundlagen der Bildverarbeitung" wird die dort behandelte Liste von Algorithmenklassen wie beispielsweise Bildverbesserung, Segmentierung, Rauschminderung erweitert um Lern- und Klassifikationsverfahren. Alle Lehrinhalte werden anhand relevanter Auswertungs-Szenarien wie beispielsweise Täter- und Opfer-Identifikation sowie Wiedererkennung von Tatorten und Tatwerkzeugen vermittelt.
Studien- Prüfungsleistungen:	120-minütige schriftliche Prüfung
Literatur:	🕮 R. Szelisky, "Computer Vision: Algorithms and Applications", Springer; 2011. 🕮 D.L. Baggio, S. Emami, D.M. Escrivá, K. Ievgen, N. Mahmood, J. Saragih, R. Shilkrot, "Mastering OpenCV with Practical Computer Vision Projects", Packt Publishing, 2012. 🕮 Weitere fachspezifische Literatur wird in den Lehrunterlagen aufgeführt.

Modul 33: Technischer Datenschutz

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Technischer Datenschutz
Kürzel	TD
Semester:	8 Semester
Modulverantwortliche(r):	Hon.-Prof. Dipl. Ing.(FH) U. Glende
Dozent(in):	Hon.-Prof. Dipl. Ing.(FH) U. Glende
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	75 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	3 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	• 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)
Inhalt:	• 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
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung
Literatur:	🕮 Simitis, Siros: Bundesdatenschutzgesetz (Kommentar), 8. Aufl., Nomos, Baden-Baden 2014 🕮 Gierschmann, Saeugling (Hrsg.): Systematischer Praxiskommentar Datenschutzrecht, Köln, 2014, 🕮 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: EU Datenschutz-Grundverordnung, BfDi-Info 6, 2. Aufl., Mai 2016 🕮 AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell, V1.0, November 2016

Modul 34: Thesis Seminar

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Bachelor Thesis Seminar
Kürzel	BTS
Semester:	8 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Selbststudium anhand von Lehrbriefen und Literatur, ggf. weitere Lehrmaterialien und Lehrmethoden, wie CD's, Vorlesungen auf DVD und Internet-based teaching; Seminaristischer Unterricht zur Prüfungsvorbereitung und Klärung offener Fragen
Arbeitsaufwand:	50 h davon 8 h Seminaristischer Unterricht (Online)
Kreditpunkte:	2 CR
Voraussetzungen:	keine
Lernziele / Kompetenzen:	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).
Inhalt:	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.
Studien- Prüfungsleistungen:	Alternative Prüfungsleistung (z. B. 15minütige Präsentation (Vortrag))
Literatur:	🕮 wird entsprechend des Themas gewählt

Modul 35: Bachelor Thesis

Studiengang:	IT-Forensik
Modulbezeichnung (Deutsch):	Bachelor Thesis
Kürzel	BT
Semester:	8 Semester
Modulverantwortliche(r):	Prof. Dr.-Ing. A. Raab-Düsterhöft
Dozent(in):	Prof. Dr.-Ing. A. Raab-Düsterhöft (verantw.)
Sprache:	Deutsch
Verwendbarkeit:	Pflichtmodul im Bachelor-Studiengang IT-Forensik
Lehrform:	Bei der Thesis handelt es sich um die eigenständige, durch Beratung unterstützte, individuelle Verfassung einer wissenschaftlichen Abschlussarbeit. Das Kolloquium (– mündliche Präsentation und Verteidigung der Inhalte der Thesis) findet in Form einer hochschulöffentlichen Veranstaltung statt, sofern der/ die Studierende nicht widerspricht bzw. das jeweilige Thema unter Ausschluss der Öffentlichkeit behandelt werden muss.
Arbeitsaufwand:	160 Stunden Selbststudium und 45 min. Kolloquium
Kreditpunkte:	15 CR (12 CR für die Bachelor Thesis, 3 CR für das Kolloquium)
Voraussetzungen:	Das Thema der Thesis wird ausgegeben, wenn Credits gemäß Prüfungsordnung nachgewiesen werden können. Voraussetzung für die Teilnahme am Kolloquium ist das erfolgreiche Bestehen der Thesis.
Lernziele / Kompetenzen:	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.

Inhalt:	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.
Studien- Prüfungsleistungen:	Wiss. Arbeit (Bachelor-Thesis) und 45min Kolloquiums (30min Präsentation und 15min Diskussion zum Bachelor-Thema)
Literatur:	🕮 wird entsprechend des Themas gewählt