Modulhandbuch

IT-Forensik/Cybercrime (B.Sc.)

Modulübersicht

7601 03-FDVWD	Datenvirtualisierung und Wiederherstellen von Daten
7602 03-FEINF	Einführung in die Informatik
7603 03-FEITS	Einführung in die IT-Sicherheit
7604 03-FAFI	Allgemeine Forensik I
7605 03-FCYB1	Cybercrime I
7606 03-FPRO1	Programmierung I
7607 03-FREBS	Betriebssysteme
7608 03-FAFII	Allgemeine Forensik II
7609 03-FPRO2	Programmierung II Skriptsprachen
7610 03-FBUDS	Betriebssysteme und digitale Spuren
7611 03-FCYB2	Cybercrime II
7612 03-FBDFD	Big Data / Forensik in DBMS
7613 03-FGDMF	Grundlagen der Mobilfunkforensik
7614 03-FSEOS	Social Engineering und OSINT
7615 03-FEDSS	Entwicklung und Design sicherer Systeme
7616 03-FSWPM	Softwareprojekt Massendaten
7617 03-FIIHA	Internet und Internetartefakte Hacking, Angriffsanalyse
7618 03-FDNCF	Datennetze / Cloud Forensik
7619 03-FOSTM	Ontologie und Semantik / Textmining
7620 03-FSWPW	Softwareprojekt Werkzeuge
7621 03-FGDK	Grundlagen der Kryptologie
7622 03-FALGO	Algorithmen
7623 03-FDKMF	Datenkompression / Multimediaformate
7624 03-FFBVA	Forensische Bild und Videoanalyse
7625 03-FKPLX	Komplexpraktikum Forensische Methoden
7626 03-FKANA	Kryptoanalyse
7627 03-FESFS	Embedded Systems Forensics und Speichertechnologien
7628 03-FDSVG	Der Sachverständige vor Gericht
7629 03-FPPDU	Predicted Policing / Dunkelfeld
7630 03-FDWUG	Digitale Werte und Güter
7631 03-FPRAX	Praxisprojekt
7632 03-FBP	Bachelorprojekt

Hinweis zur Bestellung der Prüfer:

Die in dem Modulhandbuch genannten Verantwortlichen werden für die jeweilige Modulprüfung zum Prüfer bestellt.

Formen für Prüfungsvorleistungen (PVL) und Prüfungssleistungen (PL):

A = alternativ, AP = Arbeitsprobe, B = Beleg, BA = Bachelorarbeit, K = Kolloquium, LA = Laborarbeit, LB = Laborbericht, LT = Labortestat, M = mündlich, ME = Medienproduktion, PA = Projektarbeit, PB = Praxisbericht, PT = Präsentation, S = schriftlich, SA = Studienarbeit, T = Testat, TM = Testat mündlich, TS = Testat schriftlich, U = Übung, V = Vortrag, R = Referat, ZD = Zeichnungsdokumentation

Modulname:	**Datenvirtualisierung und Wiederherstellen von Daten**	*Sprache:*	*deutsch*
Modulnummer:	7601	*Abschluss:*	B.Sc.
Modulcode:	03-FDVWD	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	1

Ausbildungsziele:	Im Modul "Datenvirtualisierung und Wiederherstellen von Daten" werden den Studierenden die klassischen Kompetenzen eines IT-Forensikers vermittelt. Es werden die Aufgaben der IT-Forensik dargestellt und Lösungen vorgestellt. Die Studierenden sollen mit den Aufgaben und Werkzeugen des Fachgebiets vertraut gemacht werden und nach Abschluss des Moduls in der Lage sein selbstständig als IT-Forensiker zu arbeiten. Als Grundlage zur Datenauswertung soll zunächst auf die Datensicherung eingegangen werden. Hier werden verschiedene Techniken, nach dem vom BSI vorgegebenen Standard, und darüber hinausreichende Techniken besprochen. Es wird auch auf die besonderen Herausforderungen bei modernen Flash Speichern wie SSDs eingegangen. Nach der Datensicherung sollen Kompetenzen im Bereich der Datenrekonstruktion erworben werden. Hier wird auf die aus den Dateisystemen resultierenden Besonderheiten eingegangen und ein Ausblick in den Bereich Datenrettung vorgenommen. Im zweiten Teil des Moduls soll eingehend auf die Datenvirtualisierung eingegangen werden. Dazu werden verschiedenen Virtualisierungstechniken vorgestellt und Grenzen aufgezeigt.
Lehrinhalte:	• Sichern von Daten, verschiedene Arten von Schreibschutz, Probleme bei der Datensicherung, Umgang mit RAID Systemen • Gelöschte Daten, Überschriebene Daten, File Slacks, Datenrekonstruktion aus FAT/MFT • Dateiheader Signatursuche, Probleme, Footer, Dateirekonstruktion • Besonderheiten bei Flash Speichern, Wear leveling, JTAG, Chip off • Datenrettung • Virtualisieren von Images, Virtualisierungstechniken, Grenzen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden mögliche Datensicherungs- und Virtulaisierungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Im Praktikum sollen die Studierenden selbstständig Images auswerten und ihr erworbenes Wissen praktisch anwenden. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Steve Bunting: EnCase Computer Forensics. Sybex, 2012. • Leitfaden IT-Forensik. Bundesamt für Sicherheit in der Informationstechnik, 2011. • W.Curtis Preston: Backup & Recovery. O'Reilly, 2007. • Rino Micheloni: Inside Solid State Drives (SSDs). Spinger, 2013 • Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7601 Datenvirtualisierung und Wiederherstellen von Daten	0	2	1	1		S 90	1/36	5

Modulname:	**Einführung in die Informatik**	*Sprache:*	*deutsch*
Modulnummer:	7602	*Abschluss:*	B.Sc.
Modulcode:	03-FEINF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	1

Ausbildungsziele:	Behandelt werden die Grundzüge und Grundbegriffe der Informationsverarbeitung sowie deren Potenziale. Dabei steht zunächst die Vermittlung eines fundierten Fachwissens bezüglich der Komponenten und Teilsysteme integrierter Anwendungssysteme im Vordergrund (Analysekompetenz; Konzeptionskompetenz). Darauf aufbauend soll der Studierende in die Lage versetzt werden, Zusammenhänge der Gestaltung von Informationssystemen zu erkennen und anwendungsorientiert reflektieren zu können (Verstehen und Anwenden, Reflektieren). Hierzu sollen grundlegende Methodenkompetenzen in der Analyse und Beschreibung von Informationssystemen herausgebildet werden.
Lehrinhalte:	• Grundlegende Konzepte der Informatik • Komponenten und Aufbau moderner Personalcomputer • Hardware (Zahlensysteme und Codes, Rechnerarchitekturen, Datenein-/-ausgabe, Datenspeicherung, Hardwarekonfiguration • Systembetrieb (Betriebsarten, Nutzungsformen, Betriebssysteme) • Kommunikationssysteme (Grundlagen, Rechnernetze, Schnittstellen und Protokolle, Netzmanagement) • Dateioperationen, Datenorganisation (Grundbegriffe, Datei- und Datenbankorganisation, Text-, Retrieval- und Suchsysteme)
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen die Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Zusammenhänge offengelegt. Den Studierenden soll ein Überblick über die Informatik und die kommenden Themen vermittelt werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Gumm, Sommer: Einführung in die Informatik. Oldenbourg-Verlag • Küchlin, Weber: Einführung in die Informatik. Springer Verlag • Duden Informatik. Ein Sachlexikon für Studium und Praxis.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7602 Einführung in die Informatik	0	2	0	1		S 90	1/36	5

Modulname:	**Einführung in die IT-Sicherheit**	*Sprache:*	*deutsch*
Modulnummer:	7603	*Abschluss:*	B.Sc.
Modulcode:	03-FEITS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	1

Ausbildungsziele:

Ziel des Moduls ist es, den Studierenden grundlegende Kenntnisse über das Gebiet der IT-Sicherheit zu vermitteln.

- Innerhalb dieser Einführung sammeln die Teilnehmer Wissen über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und Sicherheitssystemen.
- Die Studierenden verfügen über grundlegendes Verständnis in Bezug auf mögliche Angriffe und geeignete Gegenmaßnahmen auf IT-Systeme (Fachkompetenz).
- Sie kennen die wichtigsten Bedrohungen und Schwachstellen heutiger IT-Systeme.
- Innerhalb der Übung im Computerlabor erlangen die Studierenden praktische Erfahrungen bezogen auf die Nutzung bzw. Wirkung von Sicherheitssystemen (Methodenkompetenz). - Die Übungen werden vorzugsweise in kleinen Gruppen durchgeführt (Förderung der Team- und Sozialkompetenz).
- Jeder Modulteilnehmer ist für Sicherheitsprobleme im beruflichen genauso wie im privaten Umfeld sensibilisiert.
- Der Studierende erlebt hautnah die Notwendigkeit und Bedeutung der IT-Sicherheit und ist darin geschult, bestehende Sicherheitslösungen zu analysieren bzw. mögliche Schwachstellen identifizieren.

Lehrinhalte:

IT-Sicherheit Grundlegende Begriffe und Definition, Sicherheitsprobleme, Sicherheitsbedürfnisse, Bedrohungen, Angriffe, Schadenskategorien, Sicherheitsmodelle, Sicherheitsbasismechanismen und technologische Grundlagen für Schutzmaßnahmen: Private-Key-Verfahren, Public-KeyVerfahren, Kryptoanalyse, Hashfunktionen, Schlüsselgenerierung, Smartcards; Grundprinzip, Formen und Ausgestaltung von Authentikationsverfahren, Zugriffs- und Nutzungskontrolle, Netzwerksicherheit (Grundlagen), Anwendungssicherheit, Überblick zu Viren-,Würmer, Trojaner, Rootkits, Intrusion Dedection Systeme (IDS), Netzwerk-Sicherheit (Einstieg), Frühwarnsysteme (Grundlagen), Trusted Computing (Grundlagen), Sniffer-Tools, Digital Fingerprinting, Digitale Forensik

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.

Literatur:

- Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle.7. Auflage, Oldenbourg-Verlag, 2012.
- Bishop, M. : Computer Security: Art and Science, Addison-Wesley, 2003.
- Erickson, J.: Hacking: Die Kunst des Exploits, dpunkt.Verlag, 2008.

Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7603 Einführung in die IT-Sicherheit	0	2	0	1		S 90	1/36	5

Modulname:	**Allgemeine Forensik I**	*Sprache:*	*deutsch*
Modulnummer:	7604	*Abschluss:*	B.Sc.
Modulcode:	03-FAFI	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	1

Ausbildungsziele:	Die Studierenden lernen Grundprinzipien der Biometrie und deren Verwendung in der forensischen Fallarbeit kennen. Ausgehend vom Spurenbegriff wird im Prozess der Analyse der Unterschied zwischen Identifizierung und Authentifizierung durch die Verwendung von biometrischen Merkmalen des Menschen deutlich. Somit erhalten die Studierende Einblick in die Prozesskette der klassischen Fallanalyse.
Lehrinhalte:	• Begriffsbestimmung Forensik und Kriminalwissenschaften • Tatort - Spur und Einteilung, Kategorisierung (Materialspuren, Formspuren, Gegenstandsspuren und Siuationsspuren) • Tatortarbeit • Statistische und bioinformatische Grundlagen sowie Biometrische Verfahren • Digitale Forensik (Einteilung und Vorgehen) • Techniken der Tatortvermessung • Der Mensch als Spurenträger und Prozess der Spurenübertragung • Physikalische und biologische Eigenschaften von Blut • Tropfen und Musteranalyse • Biometrie • Eigenschaften biometrischer Parameter • Iriserkennung, Finger und Gesicht • Identifizierung und Authentifizierung • Aktive und passive Merkmale • Schrifterkennung und Stimmenanalyse • Morphognostik und Morphometrie - Begrifflichkeiten und Definitionen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt und Literatur zur Verfügung gestellt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten forensischen Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Grundlagen der Kriminalistik/ Kriminologie. Lehr- und Studienbriefe • Kriminalistik/Kriminologie, Band 1 Berthel, R.; Mentzel, Th.; Neidhardt, K.White (ed),Crime Scene to Court, The Essentials of Forensic Science, The Royal Society of Chemistry, London, 2004 M. Benecke, Dem Täter auf der Spur. So arbeitet die moderne Kriminalbiologie - Forensische Entomologie und Genetische Fingerabdrücke, Lübbe Verlag, 2006 B. Herrmann, K.S. Saternus, Biologische Spurenkunde , Bd.1, Kriminalbiologie 1; Springer Verlag, Berlin, 2007 • Alan Gunn: Essential ForensicBiology, 2009, Wiley Introduction to Statistics for Forensic Scientists, David Lucy, Wiley, 2006 • Ralph Rapley, David Whitehouse: Molecular Forensics, 2007, Wiley
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7604 Allgemeine Forensik I	0	2	0	1		S 90	1/36	5

Modulname:	**Cybercrime I**	*Sprache:*	*deutsch*
Modulnummer:	7605	*Abschluss:*	B.Sc.
Modulcode:	03-FCYB1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	2

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime I soll auf die sogenannte IuK-Kriminalität im engeren Sinne (Computerkriminalität) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden alle relevanten Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären. Gegen Ende des Moduls wird auf die Bedeutung der Computerkriminalität im internationalen Kontext eingegangen und internationale Normen und Verfahren dargelegt.
Lehrinhalte:	IuK Kriminalität im engeren Sinne: • Computerbetrug (§ 263a StGB) • Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB) • Datenveränderung (§ 303a) • Computersabotage (§ 303b StGB) • Ausspähen von Daten (§ 202a StGB) • Abfangen von Daten (§ 202b StGB) • Datenhehlerei (§ 202d StGB) • Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. "Hacker-Werkzeugen", die illegalen Zwecken dienen (§ 202c StGB) Cybercrime im Internationalen Kontext • Die EU-Cybercrime Richtlinie • Computer Fraud and Abuse Act und Nachfolgende Regelungen in Vereinigten Staaten • Zwischenstaatliche Vereinbarungen, G8, UN, ITU
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Dieter Kochheim: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. C.H.Beck, 2015 • Michael Büchel, Peter Hirsch: Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention (Grundlagen der Kriminalistik, Band 48). Kriminalistik, 2014. • BKA, Cybercrime: Bundeslagebild (jährlich neu) • Chuck Easttom, Jeff Taylor: Computer Crime, Investigation, and the Law. Cengage Learning PTR, 2010. • United Nations: Comprehensive Study on Cybercrime. 2013 • ITU: Understanding cybercrime: Phenomena, challenges and legal response. 2012

Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7605 Cybercrime I	0	2	0	1		S 90	1/36	5

Modulname:	**Programmierung I**	*Sprache:*	*deutsch*
Modulnummer:	7606	*Abschluss:*	B.Sc.
Modulcode:	03-FPRO1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	2

Ausbildungsziele:

Am Ende dieses Moduls kennt jeder Kursteilnehmer den grundlegenden Aufbau und die Funktionsweise eines Rechnersystems und kann die Verfahren zur rechnerinternen Darstellung von Daten und Zahlen erläutern.

Die Studierenden kennen darüber hinaus wesentliche Konzepte und Verfahren moderner Programmiersprachen, angefangen von einfachen Datentypen, über Kontrollstrukturen bis hin zu den Themen Klassen, Objekte und Vererbung.

Jeder Teilnehmende beherrscht wesentliche Bestandteile der Syntax und Semantik der Programmiersprache C. Somit ist es den Studierenden möglich, einfache praxisrelevante Problemstellungen selbständig zu analysieren und anschließend programmiertechnisch umzusetzen.

Gemeinsam können die Studierenden Lösungen für neue unbekannte Problemstellungen aus dem Bereich der Programmierung erarbeiten.

Die Studenten besitzen die notwendigen theoretischen Grundkenntnisse und praktischen Fähigkeiten und Fertigkeiten für das systematische Programmieren im Kleinen als Voraussetzung für alle weiteren Informatik Module.

Darüber hinaus wird im Rahmen des Moduls eine Harmonisierung der informatikbezogenen Kenntnisse und Fertigkeiten der Studierenden bedingt durch weiter auseinander gehende Ausgangsniveaus angestrebt.

Lehrinhalte:

- Grundbegriffe der Informatik, Rechneraufbau nach v.Neumann
- Grundkonstrukte für die Formulierung und Darstellung von Algorithmen und ihre programmiersprachliche Umsetzung
- elementare Daten und Datenstrukturen von Programmiersprachen und ihre konkrete Realisierung
- Hilfsmittel zur systematischen Programmentwicklung (grafischer Entwurf, einfache Entwurfsmuster)
- Verwendung und Erstellung von Dokumentationen als integraler Bestandteil des Programmierens

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Programmieraufgaben werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.

Literatur:

H. Balzert: Lehrbuch Grundlagen der Informatik, Heidelberg, 2005

H. Herold et al: Grundlagen der Informatik, Pearson Studium IT, 2012.

- Online-Dokumentationen und Tutorien der verwendeten Programmiersprache

Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7606 Programmierung I	0	2	1	1		S 90	1/36	5

Modulname:	**Betriebssysteme**	*Sprache:*	*deutsch*
Modulnummer:	7607	*Abschluss:*	B.Sc.
Modulcode:	03-FREBS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	2

Ausbildungsziele:	Die Studierenden erwerben umfangreiche Kenntnisse zu typischen Architekturkonzepten und zur grundlegenden Funktionsweise von Betriebssystemen. Sie kennen wichtige Hilfsmittel (Dienste, API-Funktionen/system calls), die von modernen Betriebssystemen zur Lösung typischer Aufgabenstellungen in komplexen Anwendungssystemen paralleler Prozesse/Threads angeboten werden. Dabei erwerben sie zunächst Wissen (Fachkompetenz) und die Fähigkeit, verschiedene Betriebssysteme hinsichtlich ihres Leistungsvermögens und ihrer Einsetzbarkeit in verschiedenen Gebieten (Arbeitsplatz, Server, mobil, Echtzeitsystem,...) einschätzen und vergleichen zu können (Analyse- und Evaluationskompetenz). Sie sind außerdem in der Lage, typische Probleme beim Entwurf und der Implementierung konkreter Anwendungen in Form von Multitaskingsystemen zu erkennen und zu ihrer Lösung geeignete Mittel vorhandener Betriebssysteme auszuwählen und zu benutzen, wobei hier vor allem der Entwurf und nicht die praktische Implementierung im Vordergrund steht. Insofern bietet der Modul hier vorrangig informatische und technologische Fachkompetenzen, aber ebenso analytische Methodenkompetenzen.
Lehrinhalte:	• Bedeutung und Aufgaben von Betriebssystemen; • Architekturkonzepte; Anforderungen an Entwurf und Implementierung; • Verwaltung paralleler/nebenläufiger Prozesse (Multitasking, Multithreading); Application Programming Interface API, Diensterbringung durch ein Betriebssystem; • Konkurrenz-Probleme zwischen Prozessen und Lösungsmöglichkeiten (wechselseitiger Ausschluss); • Kooperation von Prozessen und Lösungsmöglichkeiten • Betriebsmittel-Verwaltung (Scheduling); • Verklemmungen in Prozess-Systemen und mögliche Gegenmaßnahmen; • Speicherverwaltung; • Ein-/Ausgabesystem; • Dateiverwaltung; • Sicherheitsaspekte An ausgewählten Stellen (z.B. Multithreading, Virtueller Speicher) wird ergänzend auf die zugrundeliegenden Prinzipien der Rechnerarchitektur eingegangen.
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Studienhefte/Lehrmaterialien versandt, in denen die wichtigsten theoretische und praxisrelevante Grundlagen des Moduls vermittelt werden. Dabei werden ausgewählte Probleme (z.B. Prozess-/Threadverwaltung, Prozess-Synchronisation und - Kommunikation) vertiefend diskutiert und typische Algorithmen bzw. Strategien von Betriebssystemen an Beispielaufgaben aufgezeigt (z.B. Scheduling). Das Lehrmaterial enthält zusätzliche didaktische Hinweise und Anregungen zur schrittweisen erfolgreichen Bearbeitung sowie Fragen/Aufgaben zur Selbstkontrolle (mit Lösungshinweisen). Im Rahmen der Präsenzveranstaltungen werden ausgewählte Schwerpunkte sowie ggf. Übungsaufgaben diskutiert, dies dient gleichzeitig der Prüfungsvorbereitung.
Literatur:	Betriebssysteme: • Achilles, A.: Betriebssysteme. Berlin: Springer, 2006 • Brause, R. : Betriebssysteme: Grundlagen und Konzepte. Berlin: Springer, 3. Aufl. 2004 • Ehses, E. u.a.: Betriebssysteme. München: Pearson Studium, 2005 • Glatz, E.: Betriebssysteme. Heidelberg: dpunkt.Verlag, 2. Aufl. 2010 • Mandel,P.: Grundkurs Betriebssysteme. Wiesbaden: Vieweg, 4. Aufl. 2014 • Schneider, U. (Hrsg.): Taschenbuch der Informatik. München: Hanser (Leipzig: Fachbuchverlag), 7. Auflage, 2012

	• Stallings, W.: Betriebssysteme - Prinzipien und Umsetzung. 4. Aufl., Pearson Studium, 2003 • Tanenbaum, A.S.: Moderne Betriebssysteme, 3. Aufl., Pearson Studium, 2009 • Vogt, C.: Betriebssysteme. Heidelberg: Spektrum Akademischer Verlag, 2001 Ergänzend zu Rechnerarchitektur: • Tanenbaum, A.S.; Austin, T.: Rechnerarchitektur. 6. Aufl., Pearson Studium, 2014
Dozententeam:	Prof. Dr.-Ing. Schneider, Uwe (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7607 Betriebssysteme	0	2	0	1		S 90	1/36	5

Modulname:	**Allgemeine Forensik II**	*Sprache:*	*deutsch*
Modulnummer:	7608	*Abschluss:*	B.Sc.
Modulcode:	03-FAFII	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	2

Ausbildungsziele:	Aufbauend auf die Morphognostik und Morphometrie werden spezielle Analyseverfahren der Forensik (forensische Entomologie, Phonetik) kennengelernt. Schwerpunkt bildet das Verständnis von biologischen Spuren, insbesondere DNA-Spuren aus unterschiedlichen biologischen Materialien. Im Praktikum stellen die Studierenden Beziehungen zu anderen Modulen durch die Erstellung von Datenbanken und weiteren Analysewerkzeugen her. Das Wissen aus der Allgemeinen Forensik I wird in speziellen Feldern vertieft.
Lehrinhalte:	• Weichteilgesichtsrekonstruktion (Schwerpunkt computergestützte Weichteilgesichtsrekonstruktion) • Forensische Entomologie • Forensische Linguistik und Phonetik • Formspuren (Fuß- und Schuhabdrücke, Handschuhabdrücke und Materialspuren und deren Einordnung sowie Bedeutung mit dem Schwerpunkt der Digitalisierung und computergestützten Analyse • Ganganalyse • Biologische Spuren und Materialien (DNA-Spuren) • Abstammungsgutachten basierend auf dem Hardy-Weinberg Gesetz
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Weiterführende Themen der Allgemeinen Forensik werden in aller Tiefe behandelt und Lösungen für Sonder- und Spezialfälle diskutiert.Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Grundlagen der Kriminalistik/ Kriminologie. Lehr- und Studienbriefe • Berthel, R.; Mentzel, Th.: Kriminalistik/Kriminologie, Band 1 • Neidhardt, K.White (ed),Crime Scene to Court, The Essentials of Forensic Science, The Royal Society of Chemistry, London, 2004 • Benecke, M.: Dem Täter auf der Spur. So arbeitet die moderne Kriminalbiologie - Forensische Entomologie und Genetische Fingerabdrücke, Lübbe Verlag, 2006 • Herrmann, B.; K.S. Saternus: Biologische Spurenkunde , Bd.1, Kriminalbiologie 1; Springer Verlag, Berlin, 2007 • Alan Gunn: Essential ForensicBiology, 2009, Wiley Introduction to Statistics for Forensic Scientists, David Lucy, Wiley, 2006 • Ralph Rapley, David Whitehouse: Molecular Forensics, 2007, Wiley
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	7604 Allgemeine Forensik I
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7608 Allgemeine Forensik II	0	2	0	1		S 90	1/36	5

Modulname:	**Programmierung II Skriptsprachen**	*Sprache:*	*deutsch*
Modulnummer:	7609	*Abschluss:*	B.Sc.
Modulcode:	03-FPRO2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	3

Ausbildungsziele:

Bei Skriptsprachen handelt es sich um Programmiersprachen, die zumeist dazu dienen, Abläufe in Betriebssystemen oder Anwendungsprogrammen zu steuern. Sie verfügen in der Regel über sehr mächtige Mechanismen (z.B. Mustersuche) und Softwarebibliotheken (z.B. Systemschnittstellen oder Internet-Programmierung). Ziel des Moduls ist das Erlernen der Skriptsprache Python und der Erwerb der Methodenkompetenz, typische Problemstellungen der digitalen Forensik mittels eigener Python-Projekte zu lösen. Dazu zählen u.a. die Entwicklung kurzer Skripte für alltägliche Aufgaben, die Suche in Textdokumenten und Dateisystemen sowie die Entwicklung von Plugins für forensische Anwendungsprogramme. Dabei wird auf die in vorangehenden Semestern erworbenen Kenntnisse im Umgang mit Betriebssystemen und Konzepte der Programmierung aufgebaut.

Lehrinhalte:

- Grundlagen der Sprache Python (Datentypen, Kontrollstrukturen, Objektorientierte Aspekte)
- Standardbibliotheken für Systemschnittstellen, mathematische Operationen, Datenbankzugriff, XML-Verarbeitung, Datenvisualisierung etc.
- Textmatching, reguläre Ausdrücke
- CGI-Programmierung
- Plugin-Entwicklung am Beispiel einer Computerforensik-Software

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. Die Ausgabe und Kontrolle von Übungsaufgaben erfolgt mittels eines E-Learning-Systems. Es sollen regelmäßige Konsultationen abgehalten werden.

Literatur:

J. Ernesti, P. Kaiser: "Python 3: Das umfassende Handbuch", Galileo Computing, 2012

M. Pilgrim: "Python 3 - Intensivkurs", Springer, 2010

M. L. Hetland: "Python Algorithms: Mastering Basic Algorithms in the Python Language", Springer, 2010

- Offizielle Dokumentation der Python Foundation: https://docs.python.org

Dozententeam: Dipl.-Informatiker (FH) Stockmann, Daniel (Hauptverantwortlicher)

Voraussetzungen: keine

Vorausges. Module: 7606 Programmierung I

Arbeitslast: *- workload*

150 Stunden, davon
45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7609 Programmierung II Skriptsprachen	0	2	0	1		S 90	1/36	5

Modulname:	**Betriebssysteme und digitale Spuren**	*Sprache:*	*deutsch*
Modulnummer:	7610	*Abschluss:*	B.Sc.
Modulcode:	03-FBUDS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	3

Ausbildungsziele:	Betriebssysteme liefern generell umfangreiche, forensisch wertvolle Informationen. Dies liegt darin begründet, dass forensische Datenquellen in der Regel grundsätzlich durch Betriebssysteme verwaltet werden. Dies bezieht sich sowohl auf die flüchtigen Daten im Arbeitsspeicher, wie auch auf die nichtflüchtigen Daten auf Massenspeichern. Im Modul sollen Kenntnisse der Protokollierungs- und Konfigurationsdaten der vorgestellten Betriebssysteme MS Windows, OSX und Linux vorgestellt werden. Für das Betriebssystem MS Windows sollen Kenntnisse über den Aufbau und die Inhalte der zentralen Registrierungsdatenbank vermittelt werden. Auch soll der forensische Nutzen von Event Dateien und anderen von MS Windows verwalteten forensisch wertvollen Informationen vermittelt werden. Für das Betriebssystem OSX werden die Property Lists und deren Aufbau und Verwendung besprochen. Für das Betriebssystem Linux soll das Protokollierungssystem verstanden werden und für die Studierenden auswertbar gemacht werden. Nach Abschluss des Moduls sollen die Studierenden qualifiziert sein selbstständig vom Betriebssystem verwaltete Spuren forensisch auszuwerten und zu interpretieren.
Lehrinhalte:	• Grundlagen von MS Windows, Dateisysteme (FAT und NTFS), Zeitstempel, Aufbau des Betriebssystems, Besonderheiten bei der Dateiverwaltung, Aufbau und Inhalt der Registry, Ereignislogging, besondere Dateien • Grundlagen von OSX, Dateisysteme (HFS+ und APFS), Zeitstempel, Aufbau des Betriebssystems, Besonderheiten bei der Dateiverwaltung, Aufbau und Inhalt der Property Lists, besondere Dateien • Grundlagen von Linux, Dateisysteme (ext und btrfs), Zeitstempel, Aufbau des Betriebssystems, Besonderheiten bei der Dateiverwaltung, Aufbau und Inhalt der Protokolldateien, besondere Dateien • Speichermanagement bei den og. Betriebssystemen, RAM-Analyse • Ausblick auf andere Betriebssysteme
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. Dies beinhaltet die speziellen Eigenheiten der vorgestellten Betriebssysteme und die Auswirkungen auf die digitale Beweissicherung. Es sollen ausgewählte Themen durch die Studierenden selbstständig vertieft werden. Im Praktikum sollen die Studierenden selbstständig Daten auswerten. Dazu sollen Ihnen sogenannte Images zur Verfügung gestellt werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Leitfaden IT-Forensik. Bundesamt für Sicherheit in der Informationstechnik, 2011. • Mark E. Russinovich, David A. Solomon, Alex Ionescu: Windows Internals. Microsoft Press, 2012. • Jonathan Levin: Mac OS X and iOS Internals: To the Apple's Core. Wrox, 2012. • Philip Polstra: Linux Forensics. CreateSpace, 2015. • Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley, 2014. • Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005.
Dozententeam:	
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7610 Betriebssysteme und digitale Spuren	0	2	1	1		S 90	1/36	5

Modulname:	**Cybercrime II**	*Sprache:*	*deutsch*
Modulnummer:	7611	*Abschluss:*	B.Sc.
Modulcode:	03-FCYB2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	3

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime II soll auf die sogenannte IuK-Kriminalität im weiteren Sinne (Tatmittel Internet) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden relevante Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären.
Lehrinhalte:	IuK Kriminalität im weiteren Sinne: ● Verbreitung pornographischer Schriften (Kinderpornographie) über das Internet ● Verbreitung von Gewaltdarstellungen im Internet ● Onlinemarktplätze (Drogenhandel, Waffenhandel, Menschenhandel) ● Urheberrechtsdelikte Cybercrime im Staatsschutz ● Internetdelikte PMK Rechts ● Internetdelikte PMK Links ● Internetdelikte PMK Islamismus Einsatz von IuK in der Organisierten Kriminalität ● Geldwäsche im Internet ● Bedeutung von IuK für grenzüberschreitende Kriminalität ● Fälschungen IuK im Strafverfahren ● IuK als falsche Beweise
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	● Gerrit Manssen, Jörg Fritzsche, Robert Uerpmann-Wittzack: Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz. LIT, 2006 ● Philip Jenkins: Beyond Tolerance: Child Pornography. NYU Press, 2001. ● Jörg Kinzig: Die rechtliche Bewältigung von Erscheinungsformen der Organisierten Kriminalität, Berlin, 2004. ● Sean S. Costigan, Jake Perry: Cyberspaces and Global Affairs. Routledge, 2012. ● Bösche, Andreas: Rechtsextremismus im Internet. Schattenseiten des www. Hall 2001 ● Rüdiger Quedenfeld, Udo Mühlroth, Martin Plischke, Marc Studer: Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität. ESV, 2013.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine

Vorausges. Module:	7605 Cybercrime I
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7611 Cybercrime II	0	2	0	1		S 90	1/36	5

Modulname:	**Big Data / Forensik in DBMS**	*Sprache:*	*deutsch*
Modulnummer:	7612	*Abschluss:*	B.Sc.
Modulcode:	03-FBDFD	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	3

Ausbildungsziele:

Die bloße Menge an gespeicherten Daten nimmt stetig zu, derzeit verdoppelt sie sich alle zwei Jahre. Die stellt ganz besondere Anforderungen an die IT-Forensik. Insbesondere in Wirtschaftsstrafverfahren sind die aufzuwertenden Datenmengen heute schon mit klassischen Verfahren nicht mehr zu bewältigen. Das Modul "Big Data / Forensik in DBMS" soll die Studierenden mit der Auswertung und Analyse von Massendaten vertraut machen. Es soll ein detailliertes Bild, von der Herangehensweise, den Konzepten und Techniken die bei der Lösung von Fällen mit Massendaten hilfreich sind, vermittelt werden. Nach Abschluss des Moduls sollen die Studierenden in der Lage sein, selbstständig effiziente Lösungsansätze für solche Aufgabenstellungen zu entwerfen.

Die Studierenden erlernen den Umgang mit unstrukturierten Datenmengen und Auswerteansätze, wie NoSQL Datenbanken. Auf der anderen Seite wird auch speziell auf Datenbankmanagementsysteme (DBMS) eingegangen und die Besonderheiten bei der Sicherung und Auswertung solcher Systeme.

Lehrinhalte:

- Forensik im Wirtschaftsstrafverfahren
- Handling von Massendaten
- NoSQL Ansätze
- Forensik in DBMS
- Auswertung von ERP-Systemen wie SAP

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.

Literatur:

- Gottfried Vossen: Datenmodelle, Datenbanksprachen und Datenbankmanagementsysteme. Oldenbourg, 2008
- Paul M. Wright, Oracle Forensics In a Nutshell. 2007
- Jonas Freiknecht: Big Data in der Praxis: Lösungen mit Hadoop, HBase und Hive. Daten speichern, aufbereiten, visualisieren. Hanser, 2014.
- Norbert Gronau: Enterprise Resource Planning: Architektur, Funktionen und Management von Erpsystemen: Architektur, Funktionen und Management von ERP-Systemen. Oldenbourg, 2010

Dozententeam:	NN, Informatik (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7612 Big Data / Forensik in DBMS	0	2	0	1		S 90	1/36	5

Modulname:	**Grundlagen der Mobilfunkforensik**	*Sprache:*	*deutsch*
Modulnummer:	7613	*Abschluss:*	B.Sc.
Modulcode:	03-FGDMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	4

Ausbildungsziele:

Weltweit existieren über 6 Mrd. Mobilfunknutzer, dies macht mehr als 90% der Weltbevölkerung aus. Bereits im Jahr 2013 waren in 85% aller Kriminalfälle mobile Endgeräte involviert. Trotz der stetig wachsenden Bedeutung mobiler Endgeräte wie Mobiltelefonen, Smart-Phones, PDAs und Musikgeräten gilt die forensische Untersuchung solcher Geräte als teuer und kompliziert.

Im Modul "Grundlagen der Mobilfunkforensik" sollen verbreitete Mobilfunkstandards, Betriebssysteme und Grundlagen der Architektur von mobilen Endgeräten strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für mobile Endgeräte vorgestellt und Szenarien erörtert werden.

Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Mobilfunkforensik der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.

Lehrinhalte:

- Mobilfunkstandards: GSM, GPRS, LTE
- Grundlagen und Begriffe der Mobilfunkforensik
- Smartcards: insbesondere SIM
- Mobile Betriebssysteme: insbesondere Android, iOS, WindowsPhone
- Architektur von Mobilfunkendgeräten: insbesondere Speichertechnologien
- Forensische Tools: insbesondere UFED, XRY
- Der IMSICatcher

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Mobilfunkendgeräte sowie mögliche Lösungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.

Literatur:

- Satish Bommisetty, Rohit Tamma, Heather Mahalik: Practical Mobile Forensics. Packt Publishing 2014
- Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart Cards. 5. Auflage, Hanser, 2008.
- Bernhard Walke: Mobilfunknetze und ihre Protokolle 1, Stuttgart 2001, ISBN 3-519-26430-7
- Jonathan Zdziarski : iOS Forensic Investigative Methods, 2012

Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7613 Grundlagen der Mobilfunkforensik	0	2	1	1		S 90	1/36	5

Modulname:	**Social Engineering und OSINT**	*Sprache:*	*deutsch*
Modulnummer:	7614	*Abschluss:*	B.Sc.
Modulcode:	03-FSEOS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	4

Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den Grundlagen von Social Engineering. Sie sind mit gängigen Techniken vertraut und kennen die psychologischen Grundlagen der einzelnen Angriffsmuster. Sie kennen Abwehrstrategien gegen Social Engineering und sind in der Lage Sicherheitsrichtlinien und Schulungen zu entwickeln. Jeder Teilnehmer kennt die Möglichkeiten von OSINT (Open Source Intelligence) zur Datengewinnung. ER kann selbstständig Werkzeuge einsetzen um Daten automatisiert zu sammeln, zusammenzuführen und auszuwerten. Dabei wird er mit den Besonderheiten von Big Data konfrontiert. Alle Kursteilnehmer sind vertraut der Daten Gewinnung aus Sozialen Netzwerken, Webseiten, Medien und anderen offenen Quellen. Sie lernen Personen zu identifizieren und zu lokalisieren.
Lehrinhalte:	Grundlagen des Social Engineering • Reziprozität • Konsistenz • Commitement Andrere Techniken • Phishing • Dumpster Diving Abwehrstrategien gegen Social Engineering Grundlagen von OSINT • Arten von offenen Quellen • Automatisiertes Sammeln von Informationen • Zusammenführen von Informationen • Auswertung offener Quellen • Big Data
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Studienhefte/Lehrmaterialien versandt, in denen die wichtigsten theoretische und praxisrelevante Grundlagen des Moduls vermittelt werden. Dabei werden ausgewählte Themen aus dem Bereich Social Engineering und OSINT vertiefend diskutiert und typisch Strategien und Angriffsmuster an Beispielszenarien aufgezeigt. Das Lehrmaterial enthält zusätzliche didaktische Hinweise und Anregungen zur schrittweisen erfolgreichen Bearbeitung sowie Fragen/Aufgaben zur Selbstkontrolle (mit Lösungshinweisen). Im Rahmen der Präsenzveranstaltungen werden ausgewählte Schwerpunkte sowie ggf. Übungsaufgaben diskutiert, dies dient gleichzeitig der Prüfungsvorbereitung.
Literatur:	• Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006 • Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007. • Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010 • Arthuer S. Hulnick: 'The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?', pages 229-241, The Oxford Handbook of National Security Intelligence, 2010 -Andreas Weyert : Hacking mit Kali. Francis, 2014.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher) M.Sc. Spranger, Michael
Voraussetzungen:	keine

Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7614 Social Engineering und OSINT	0	2	0	1		S 90	1/36	5

Modulname:	**Entwicklung und Design sicherer Systeme**	*Sprache:*	*deutsch*
Modulnummer:	7615	*Abschluss:*	B.Sc.
Modulcode:	03-FEDSS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	4

Ausbildungsziele:	Ziel des Moduls ist es, den Studierenden Kenntnisse über das Gebiet der Planung und Entwicklung sicherer Systeme zu vermitteln. • die Teilnehmer sammeln Wissen über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten. Dabei lernen Sie die Bedeutung von Design-Pattern und deren Anwendung im Rahmen der Planung von Anwendungssoftware kennen. • Die Studierenden kennen typische Schwachstellen beim Entwurf von Softwarelösungen und wissen, wie diese minimiert werden können (Fachkompetenz). • Sie kennen die wichtigsten Bedrohungen und Schwachstellen heutiger IT-Systeme kennen. • Innerhalb der praktischen Übung erlangen die Studierenden Erfahrungen bezogen auf die Nutzung bzw. Wirkung von Sicherheitsmaßnahmen bei der Softwareentwicklung (Methodenkompetenz). • Insbesondere wird jeder Modulteilnehmer für typische Problemstellungen in Zusammenhang mit der Sicherheit von Softwarelösungen im beruflichen Alltag sensibilisiert.
Lehrinhalte:	• Design und Entwicklung sicherer Systeme • Grundlagen Softwaretechnik und Modellierung von Anwendungssystemen • Security by Design, Vorgehensmodelle • Sicherheitspolitiken für komplexe Systeme und Mechanismen zur sicheren Komposition von in sich sicheren Teilsystemen • Software-Pattern für Sichere Systeme (Input-Validator-Pattern, Secure Logger Pattern, Attack-Pattern) • Secure Programming - Richtlinien, Aspektorientierte Programmierung, • Security Pattern engineering, Entwicklung sicherer Webanwendungen, • Generische Module zur Entwicklung sicherer Steuergeräte-Software, • Entwicklung von Sicherheitsmechanismen in verschiedenen, Anwendungsgebieten(Industrie 4.0, Gesundheit, kritische Infrastrukturen) • Absicherung von Enterprise-Software durch existierende Frameworks wie z. B. J2EE. Darüber hinaus werden grundsätzliche Fragen der Zuverlässigkeit von Software behandelt, etwa Safety, sicheres Funktionieren von Software und Usability.
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Studienhefte/Lehrmaterialien versandt, in denen die wichtigsten theoretische und praxisrelevante Grundlagen des Moduls vermittelt werden. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert. Das Lehrmaterial enthält zusätzliche didaktische Hinweise und Anregungen zur schrittweisen erfolgreichen Bearbeitung sowie Fragen/Aufgaben zur Selbstkontrolle (mit Lösungshinweisen). Im Rahmen der Präsenzveranstaltungen werden ausgewählte Schwerpunkte sowie ggf. Übungsaufgaben diskutiert, dies dient gleichzeitig der Prüfungsvorbereitung.
Literatur:	• Roland Schmitz, Walter Kriha: Sichere Systeme - Konzepte, Architekturen und Frameworks. Springer-Verlag 2009. • Entwicklung sicherer Software durch Security by Design, Frauenhofer SIT2013 (SIT-TR-2013-01). • Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley 2008. • Hollunder, B.; Herrmann, M. ; Hülzenbecher, A.: Design by Contract for Web Services: Architecture, Guidelines, and Mappings. In: International Journal On Advances in Software 5 (2012) • Peter Gutmann: Engineering Security. Free E-Book. (2013) http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	7606 Programmierung I 7609 Programmierung II Skriptsprachen
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7615 Entwicklung und Design sicherer Systeme	0	2	0	1		S 90	1/36	5

Modulname:	**Softwareprojekt Massendaten**	*Sprache:*	*deutsch*
Modulnummer:	7616	*Abschluss:*	B.Sc.
Modulcode:	03-FSWPM	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	4

Ausbildungsziele:	Die Studierenden sind in der Lage, als Mitglied eines Softwareentwicklungsteams an einem realistischen Softwareprojekt aus dem Umfeld der Digitalen Forensik von der Aufgabenstellung bis zur Inbetriebnahme des Softwaresystems zu arbeiten. Das Projekt soll den Umgang mit Massendaten realisieren, dazu werden realistische Daten oder tatsächliche Falldaten verwendet. Im Projekt werden alle Fach- und Methodenkompetenzen, die in den Grundlagenmodulen der Informatik erworben worden sind, von den Studierenden erprobt, geübt und gefestigt. Die Studierenden können gemeinsam an einer Aufgabenstellung arbeiten und übernehmen Rollenverantwortung innerhalb des Teams. Sie beherrschen ihre Kommunikationsfähigkeiten in der jeweiligen festgelegten Rolle als Verantwortlicher, Fach- oder Methodenspezialist. Sie beherrschen die grundlegenden Anforderungen des Projektmanagements. Sie sind in der Lage, auf schwierige Projektsituationen so zu reagieren, dass das Gesamtziel der Erstellung eines Softwareprototypen nicht gefährdet wird. Die Studierenden sind in der Lage, professionelle und fachlich korrekte begleitende Dokumentationen zu den einzelnen Projektphasen unter Zuhilfenahme spezieller Tools zu erstellen. Die Studierenden sind für den beruflichen Einsatz trainiert, softwaretechnische Prinzipien, Methoden und Werkzeuge auf praxisrelevante Fallbeispiele im Umfeld der Digitalen Forensik anzuwenden und bis zu einem Demonstrationsprototypen als Teil eines Teams zu entwickeln. Dabei können sie die ersten eigenen praktischen Erfahrungen vorweisen.
Lehrinhalte:	Bearbeitung einer praxisrelevanten Aufgabenstellung in der Auswertung und dem Umgang mit Massendaten im Projektteam unter Beachtung forensischer Strategien und Regeln
Lernmethoden:	Die Studierenden bilden selbstständig Projektgruppen, denen Projekte von den Modulverantwortlichen übertragen werden. Es soll den Gruppen auch möglich sein ihre eigenen Projekte vorzuschlagen, ein Anspruch auf ein Thema besteht aber nicht. Die Studierenden müssen in Ihren Projekten zusammenarbeiten auch wenn sie durch den Charakter eines berufsbegleitenden Fernstudiums örtlich voneinander getrennt sind. Dazu müssen sie sowohl mit Systemen zur verteilten Versionsverwaltung arbeiten als auch Kommunikationsstrategien entwickeln. Die Projektfortschritte sind zu dokumentieren und an die Betreuer einzusenden. Das erstellte Projekt wird als Beleg bewertet, zusätzlich legen die Studierenden eine mündliche Prüfung zu den oben genannten Ausbildungszielen ab.
Literatur:	Fachspezifische Literatur (projektbezogen)
Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher) Prof. Dr. rer. nat. Hummert, Christian Prof. Dr. rer. nat. Labudde, Dirk M.Sc. Spranger, Michael
Voraussetzungen:	keine
Vorausges. Module:	7606 Programmierung I 7609 Programmierung II Skriptsprachen
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7616 Softwareprojekt Massendaten	0	0	2	1			1/36	5
7616(T1) Beleg						B		
7616(T2) Mündlich						M 30		

Modulname:	**Internet und Internetartefakte Hacking, Angriffsanalyse**	*Sprache:*	*deutsch*
Modulnummer:	7617	*Abschluss:*	B.Sc.
Modulcode:	03-FIIHA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	5

Ausbildungsziele:	Im Phänomenbereich Cybercrime nimmt die sogenannte "IuK Kriminalität im engeren Sinne" eine herausgehobene Stellung ein. Die Studierenden sollen Kompetenzen bei der Verfolgung und Aufklärung von Verbrechen in diesem Phänomenbereich gewinnen. Hierzu sollen Angriffsszenarien in Computernetzen strukturiert dargestellt werden und sowohl Verteidigungsszenarien erörtert werden, wie auch die Möglichkeiten der Beweissicherung nach einem solchen ITAngriff. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich IT-Forensik / Cybercrime in der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Fälle aufzuklären.
Lehrinhalte:	• Cybercrime im Strafrecht, Verfolgung von Cybercrime Delikten in Deutschland • IT-Angriffe und deren Abwehr strukturiert und gestaffelt nach dem OSI-Schichten Modell. • Intrusion Detection Systeme • Auswertung von Log Dateien, Aufklärung von IP-Adressen • Darkweb und Deepweb
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. Dies beinhaltet die zugrundeliegenden Protokolle der einzelnen Services ebenso wie die die IT-Sicherheit im Speziellen Fall. Es sollen ausgewählte Themen vertieft werden. Im Praktikum sollen die Studierenden selbstständig IT-Angriffe erproben und die Beweissicherung üben. Hier soll ihnen vermittelt werden, wie sie ihr gewonnenes Wissen praktisch einsetzen und anwenden können. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Michael Gregg: Hack the Stack. Syngress, 2006. • Ryan Trost: Practical Intrusion Analysis. Addison-Wesley, 2009 • Michael S Collins: Network Security Through Data Analysis: Building Situational Awareness. O'Reilly, 2014. • Michael Messner: Metasploit. dpunkt, 2012.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7617 Internet und Internetartefakte Hacking, Angriffsanalyse	0	2	0	1		M 30	1/36	5

Modulname:	**Datennetze / Cloud Forensik**	*Sprache:*	*deutsch*
Modulnummer:	7618	*Abschluss:*	B.Sc.
Modulcode:	03-FDNCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	5

Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den technischen Grundlagen von Cloudanwendungen. Sie sind vertraut mit den gängigen Verfahren zur Datensicherheit lokal und innerhalb der Cloud. Jeder Teilnehmer kennt die Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten. Alle Kursteilnehmer sind vertraut mit der Handhabung forensischer Werkzeuge, die für die Sicherstellung und Untersuchung von digitalen Spuren innerhalb der Cloud verwendet werden können und wenden diese praktisch an.
Lehrinhalte:	Cloud Computing Stack, Cloud Security and Privacy, Internet-fähige Endgeräte, Smartphones und Cloud Computing, Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte, konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten, forenische Analyse aktueller Cloud-Anwendungen (Dropbox, Micosoft Aszure, Cloudflare, Amazon Cloud Front, Amazone S3, Google Drive etc.)
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Studienhefte/Lehrmaterialien versandt, in denen die wichtigsten theoretische und praxisrelevante Grundlagen des Moduls vermittelt werden. Dabei werden ausgewählte Probleme aus dem Bereich Datennetze / Cloud Forensik vertiefend diskutiert und typische Szenarien an Beispielaufgaben aufgezeigt. Das Lehrmaterial enthält zusätzliche didaktische Hinweise und Anregungen zur schrittweisen erfolgreichen Bearbeitung sowie Fragen/Aufgaben zur Selbstkontrolle (mit Lösungshinweisen). Im Rahmen der Präsenzveranstaltungen werden ausgewählte Schwerpunkte sowie ggf. Übungsaufgaben diskutiert, dies dient gleichzeitig der Prüfungsvorbereitung.
Literatur:	• Raymond Choo, Darren Quick, Ben Martini : Cloud Storage Forensics. 1. Edition. Elsevier LTD, Oxford (2014) • Keyun Ruan: Cybercrime and Cloud Forensics Applications for Investigation Processes (2013) • Wilie E. May: NIST Cloud Computing 2 Forensic Science Challenges. Draft NISTIR 8006 (2014) • Josiah A. Dykstra: Digital Forensics for Infrastructure-as-a-Service Cloud Computing. Dissertation. (2013) http://www.cisa.umbc.edu/papers/dissertations/dykstra-dissertation-2013.pdf • Cloud Computing Security, Roland L. Krutz and Russel Dean Vines, 2010, Wiley.
Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7618 Datennetze / Cloud Forensik	0	2	0	1		S 90	1/36	5

Modulname:	**Ontologie und Semantik / Textmining**	*Sprache:*	*deutsch*
Modulnummer:	7619	*Abschluss:*	B.Sc.
Modulcode:	03-FOSTM	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	5

Ausbildungsziele:	Ausgehend vom Phänomen Massendaten, welches sich in der Forensik gezeigt hat, erlernen die Studierenden Strategien zur Analyse dieser Daten kennen. Als grundlegendes Werkzeug lernen Sie die Begriffe Ontologie und Semantik als Modellierungswerkzeuge kennen.
Lehrinhalte:	• Phänomen Massendaten • Ableitung der Eigenschaften aus Big Data (Geschwindigkeit, Volumen und Heterogenität) • Modellierung von Ontologien in vorgegebenen forensischen Domänen Analyse großer Datenmengen mit Hilfe der Konstruktion eigener Ontologien • Techniken des Textmining als besondere Form des Data Mining • Grundprinzipien des Datenmanagements • Rolle von Datenbanken und Ontologien
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgaben blättern und Übungen kontrolliert.
Literatur:	• Dengel: Semantische Technologien - Grundlagen, Konzepte, Anwendungen. Spektrum Akademischer Verlag, 2012. • Jansen; Smith: Biomedizinische Ontologie - Wissen strukturieren für den Informatik-Einsatz. 2011 • Heyer; Quasthoff: Text Mining - Wissensrohstoff Text - Konzepte Algorithmen, Ergebnisse. 2006
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7619 Ontologie und Semantik / Textmining	0	2	0	1		S 60	1/36	5

Modulname:	**Softwareprojekt Werkzeuge**	*Sprache:*	*deutsch*
Modulnummer:	7620	*Abschluss:*	B.Sc.
Modulcode:	03-FSWPW	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	5

Ausbildungsziele:	Die Studierenden sind in der Lage selbstständig ein realistisches Softwareprojekt aus dem Umfeld der Aufklärung von Delikten aus dem Phänomenbereich Cybercrime von der Aufgabenstellung bis zur Inbetriebnahme des Softwaresystems zu arbeiten. Das Projekt soll ein konkretes Werkzeug zu Ermittlungsunterstützung realisieren, dazu werden realistische Daten oder tatsächliche Falldaten verwendet. Im Projekt werden alle Fach- und Methodenkompetenzen, die in den Grundlagenmodulen der Informatik erworben worden sind, von den Studierenden erprobt, geübt und gefestigt. Die Studierenden sollen selbstständig an einer Aufgabenstellung arbeiten, sie sind in der Lage, auf schwierige Projektsituationen so zu reagieren, dass das Gesamtziel der Erstellung eines Softwareprototypen nicht gefährdet wird. Die Studierenden sind in der Lage, professionelle und fachlich korrekte begleitende Dokumentationen zu den einzelnen Projektphasen unter Zuhilfenahme spezieller Tools zu erstellen. Die Studierenden sind für den beruflichen Einsatz trainiert, softwaretechnische Prinzipien, Methoden und Werkzeuge auf praxisrelevante Fallbeispiele im Umfeld der Ermittlung anzuwenden.
Lehrinhalte:	Bearbeitung einer praxisrelevanten Aufgabenstellung in der ein Werkzeug zur Ermittlungsunterstützung aus dem Phänomenbereich Cybercrime unter Beachtung forensischer Strategien und Regeln erstellt wird. Dabei kann es sich um ein Plugin oder eine eigenständige Software handeln.
Lernmethoden:	Den Studierenden wird ein Projekt von den Modulverantwortlichen übertragen werden. Es soll aber auch möglich sein ihre Projekte vorzuschlagen, ein Anspruch auf ein Thema besteht aber nicht. Die Studierenden müssen in Ihre Projektthemen eigenverantwortlich bearbeiten. Die Projektfortschritte sind zu dokumentieren und an die Betreuer einzusenden. Das erstellte Projekt wird als Beleg bewertet, zusätzlich legen die Studierenden eine mündliche Prüfung zu den oben genannten Ausbildungszielen ab.
Literatur:	Fachspezifische Literatur (projektbezogen)
Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher) Prof. Dr. rer. nat. Hummert, Christian Prof. Dr. rer. nat. Labudde, Dirk
Voraussetzungen:	keine
Vorausges. Module:	7606 Programmierung I 7609 Programmierung II Skriptsprachen
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7620 Softwareprojekt Werkzeuge	0	0	2	1			1/36	5
7620(T1) Beleg						B		
7620(T2) Mündlich						M 30		

Modulname:	**Grundlagen der Kryptologie**	*Sprache:*	*deutsch*
Modulnummer:	7621	*Abschluss:*	B.Sc.
Modulcode:	03-FGDK	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	5

Ausbildungsziele:	Nach Abschluss des Moduls verfügen die Studierenden über mathematisch fundiertes Verständnis für die Funktionsweise moderner kryptographischer Verfahren. Jeder Teilnehmer ist dann in der Lage, die in der Lehrveranstaltung behandelten Verfahren, anzuwenden, anzupassen und ihre Sicherheit kritisch zu beurteilen. Das Modul fördert das Abstraktionsvermögen und die algorithmische Denkweise sowie die Berufsbefähigung der Absolventen auf dem Gebiet der IT-Forensik / Cybercrime.
Lehrinhalte:	• Klassische Chiffriermethoden • Moderne symmetrische Verfahren • Differentielle und lineare Kryptoanalyse • Shannons Theorie der Kryptosysteme • Algebraische und zahlentheoretische Grundlagen • Asymmetrische Verfahren • Komplexitätsklassen • Kryptographische Hashfunktionen • Digitale Signaturen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen die Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Zusammenhänge offengelegt. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert. Jeder Studierende bereitet einen Seminarvortrag vor, den er vor der Gruppe präsentiert.
Literatur:	J. Hromkovic et al.: Einführung in die Kryptologie, Springer Vieweg, 2014. B. Esslinger: Das CrypTool-Skript, Draft-Version, 2013. A. McAndrew: Introduction to Cryptography with Open-Source Software. CRC Press, 2011
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7621 Grundlagen der Kryptologie	0	2	0	1	LT	M 30	1/36	5

Modulname:	**Algorithmen**	*Sprache:*	*deutsch*
Modulnummer:	7622	*Abschluss:*	B.Sc.
Modulcode:	03-FALGO	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	6

Ausbildungsziele:	Das Modul Algorithmen soll die Studierenden mit einer Reihe von konkreten Algorithmen aus den verschiedensten Bereichen, sowie Prinzipien für das Design von Algorithmen, deren Komplexitätsanalyse und dem Einsatz von Zufall in verschiedenen Ausprägungen in der Algorithmik vertraut machen. Es soll ein detailliertes Bild, von der Herangehensweise, den Konzepten und Techniken die bei der Lösung von insbesondere schlecht-gestellten Problemen hilfreich sind, vermittelt werden. Nach Abschluss des Moduls sollen die Studierenden in der Lage sein, selbstständig effiziente Lösungsansätze für solche Aufgabenstellungen zu entwerfen.
Lehrinhalte:	• Grundlegende Konzepte der Algorithmik • Dynamisches Programmieren • Greedy Algorithmen • String Matching • Heuristische Algorithmen • Algorithmen für das Erfüllbarkeitsproblem • Ausgewählte interessante Algorithmen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Algorithmen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Uwe Schöning: Algorithmik, Spektrum 2001 • Donald E. Knuth: The Art of Computer Programming, Addison Wesley • Thomas A. Cormen: Introduction to Algorithms, MIT Press • Michael R. Garey, David S. Johnson: Computers and Intractability. Twenty-third Printing
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7622 Algorithmen	0	2	0	1		S 90	1/36	5

Modulname:	**Datenkompression / Multimediaformate**	*Sprache:*	*deutsch*
Modulnummer:	7623	*Abschluss:*	B.Sc.
Modulcode:	03-FDKMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	6

Ausbildungsziele:	Das Modul "Datenkompression / Multimediaformate" soll die Studierenden zunächst mit den Grundlagen der Informationstheorie und der Nachrichtenübertragung sowie der verlustfreien und verlustbehafteten Datenkompression bekannt machen. Die Studierenden beherrschen nach Abschluss des Moduls die Methodik verschiedener Kompressionsverfahren und können die Grenzen der Datenkompression erfassen. Es wird Reihe von konkreten Verfahrenstechniken aus den verschiedensten Bereichen der Daten- und Multimediakompression sowie die Prinzipien für das Design von Algorithmen und deren Komplexität dargestellt. Es soll ein detailliertes Bild von der Herangehensweise, den Konzepten und Techniken der Datenkompression vermittelt werden, was klassische und moderne Bild-, Video- und Audioformate einschließt. Nach Abschluss des Moduls sollen die Studierenden nicht nur in der Lage sein selbstständig unterschiedliche Multimediadateien für die weitere Verarbeitung im Bereich der Medieninformatik einzusetzen, sondern die angewandten Verfahren im Bedarfsfall im Rahmen der IT-Forensik zu entwickeln.
Lehrinhalte:	Grundlagen der Informationstheorie: • Informationsgehalt und Entropie • Optimaler und redundanter Code • Digitalisierungsstrategien und Datenreduktion • Qualität und Datenrate Kompressionstechniken: • Systematisierung von Codierungstechniken • Lempel-Ziv Kompression • Präfix Codes, Huffman-Kodierung, Shannon-Fano-Kodierung • Andere verlustfreie Verfahren wie Burrows-Wheeler-Transformation Bildkodierung: • Pixelgraphiken und Farbräume • JPEG und Diskrete Cosinus Transformation • Vektorgraphiken Videokodierung und Multimediaformate: • Prinzipien der Bewegtbildkodierung in H.261 • Von H.261 bis H.265 • Grenzen moderner Verfahren Weitere Kodierungsformen: • Audiokodierung: Von PCM zu MPEG Audio Layer-3 • Hexagonale Kodierung
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und verbreitete Kompressionsverfahren eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Effelsberger, Wolfgang; Steinmetz, Ralf (1998). Video Compression Techniqus. dpunkt.verlag, Heidelberg • Küsters, Heiner (1995). Bilddatenkomprimierung mit JPEG und MPEG. Franzis, Poing. • Lipp, Thomas W. (1997). Grafikformate. Microsoft Press, Unterschleißheim.

- Meyer, Yves (1992). Wavelets and Operators. Cambridge: Cambridge University Press.
- Miano, John (2000). Compressed Image File Formats. Addison-Wesley, Reading.
- Sayood, Khalid (2005). Introduction to Data Compression. 3rd Ed., San Francisco, CA: Morgan-Kaufmann.
- Salomon, David (2006). Data Compression, The Complete Reference. Springer; 4th ed.
- Strutz, Tilo (2002). Datenkompression. Grundlagen, Verfahren und deren Anwendung in der Verarbeitung von Graustufen und Farbbildern. Rostock
- Taubman, David S. & Marcellin, Michael (2001). JPEG2000: Image Compression Fundamentals, Standards and Practice, Kluwer International Series in Engineering & Computer

Dozententeam:	NN, Informatik (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7623 Datenkompression / Multimediaformate	0	2	0	1		S 90	1/36	5

Modulname:	**Forensische Bild und Videoanalyse**	*Sprache:*	*deutsch*
Modulnummer:	7624	*Abschluss:*	B.Sc.
Modulcode:	03-FFBVA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	6

Ausbildungsziele:	Die Veranstaltung hat das Ziel die Teilnehmer mit einem Repertoire an Bildverarbeitungsverfahren vertraut zu machen, die ihre Anwendung z.B. in der industriellen, medizinischen oder forensischen Praxis finden. Diese Verfahren werden teilweise isoliert, teilweise anhand von konkreten Anwendungsbeispielen erläutert. Ein konkretes Beispiel hierfür ist die Erkennung von handgeschriebenen Schriftzeichen. Diese Anwendung motiviert u.A. den Einsatz von digitalen Kurven und Methoden zu deren vergleich. Anhand von fertigen oder teilfertigen Programmen als Quelltext sollen Teilnehmer auch an die programmtechnische Implementierung einiger Verfahren herangeführt werden.
Lehrinhalte:	(in nicht chronologischer Reihenfolge) • Grundlagen: Bildgebende Geräte, neueste Forschungsrichtungen im groben Überblick, Farbräume • Digitale Kurven: Kodierung, Eigenschaften, Kurvenvergleiche, Merkmale, Hough-Transformation und Curvature Scale Space. Anwendung auf Erkennung von Fingerabdrücken. • Regionen: Merkmale, (Zentral-)Momente (translations-, skalierungs-, rotationsinvariant) • Bildsegmentierung u. Alpha-Matting: Pixel-, silhouetten und regionenbasierte Verfahren, dynamische Programmierung, Watershed-Verfahren, Einführung des Gradienten • Basistransformationen: Diskrete Fourier-Transformation, DCT, Einführung in die Idee und Wavelet-Transformation • Filter: Hoch-, Tief-, Bandpass, Definition und Implementierung von Faltungen • Histogramme: Entropie von Grauwertverteilungen, Histogrammmanipulationen • Textumaße
Lernmethoden:	Die mathematischen oder informatischen Inhalte der Bildverarbeitung eignen sich nur selten für dialektische Erörterungen und erfolgen größtenteils als klassischer Frontalunterricht. Wenn möglich werden die Teilnehmer allerdings durch gezielte Fragen motiviert aus ihrem bekannten Wissen die Inhalte der Vorlesungseinheit abzuleiten. Die meisten Themenfelder werden durch einen vollständigen Foliensatz unterstützt. Er dient mit seinen teilweise ausführlichen textuellen Erläuterungen eher als Skript für die Nachbereitung bzw. kann im Vorhinein ausgedruckt und während der Veranstaltungen um Kommentare ergänzt werden. Ab dem Sommersemester 2016 werden auch Videoaufzeichnungen der Veranstaltungen verfügbar sein. In den Übungen werden die vorgestellten Verfahren an konkreten Rechenbeispielen vergegenständlicht oder in Beispielprogrammen implementiert. Dabei stehen den Studierenden Templates zur Verfügung, die um einfache Programmkonstrukte oder Formeln ergänzt werden

	müssen. Dabei liegt der Fokus nicht auf der Programmierung, sondern der Anwendung der Inhalte aus der Vorlesung. Rudimentäre Kenntnisse einer prozeduralen Programmiersprache reichen für die Lösung der Aufgaben aus. Nach der Übersetzung des Quelltexts kann das Ergebnis an Beispielbildern getestet werden.
Literatur:	Tönnies, K.D.: Grundlagen der Bildverarbeitung, Pearson Studium, 2005 Jähne, B.: Digitale Bildverarbeitung, Springer, 1991 Wahl, F.M.:Digitale Bildverarbeitung, Springer, 1984 Pratt, W.K.: Digital Image Processing, John Wiley &Sons, 1978 Handels, H.: Medizinische Bildverarbeitung, B.G. Teubner, 2000
Dozententeam:	Prof. Dr. rer. nat. habil. Haenselmann, Thomas (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7624 Forensische Bild und Videoanalyse	0	2	0	1		S 90	1/36	5

Modulname:	**Komplexpraktikum Forensische Methoden**	*Sprache:*	*deutsch*
Modulnummer:	7625	*Abschluss:*	B.Sc.
Modulcode:	03-FKPLX	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	2
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	6 - 7

Ausbildungsziele:

Die Studierenden lernen in selbstgewählten Modulen praktische Verfahrensweisen aus dem Bereich IT-Forensik / Cybercrime kennen. In den einzelenen Praktika sollen die Studierenden erlernen Ihre im Studium erworbenen Fähigkeiten einzusetzen und selbst gewählte Spezialgebiete vertiefen.

Lehrinhalte:

Auswahl von bis zu 2 Praktika aus:

- Forensische Digitalfotographie
- Sicherheitsmerkmale bei Wertzeichen und Urkunden
- Open Source Intelligence
- Malware Forensics
- Digitale Audioanalyse
- Methoden der Digitalen Tatortrekonstruktion
- Car Forensics
- Digitale Fallanalyse
- Digital Video Analysis
- Mobilfunkforensik

(Die Module werden entsprechend der Fortschritte der IT-Forensik aktualisiert.)

Lernmethoden:

Die Komplexpraktika finden als zweiwöchige Präsenzpraktika an der Hochschule Mittweida statt. Hier sollen die theoretische Grundlagen der Studierenden zu Anwendung kommen. In diesem Zusammenhang werden ausgewählte Probleme vertiefend in Vorlesungen und Seminaren diskutiert und Strategien zur Problemlösung vorgestellt. Dann sollen die Studierenden konkrete Problemen in Kleingruppen praktisch lösen.

Literatur:

Die Literaturempfehlungen richten sich nach den gewählten Einzelpraktika im Rahmen des Komplexpraktikums.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)

Voraussetzungen:

keine

Vorausges. Module:

keine

Arbeitslast: *- workload*

300 Stunden, davon
120 Stunden Lehrveranstaltungen
180 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7625 Komplexpraktikum Forensische Methoden	2	4	2	0	LT	A	2/36	10

Modulname:	**Kryptoanalyse**	*Sprache:*	*deutsch*
Modulnummer:	7626	*Abschluss:*	B.Sc.
Modulcode:	03-FKANA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	7

Ausbildungsziele:	Vermittlung aktueller Kenntnisse und fortgeschrittener Methoden auf dem Gebiet der Kryptoanalyse; Befähigung zur selbstständigen Aneignung neuen Wissens.
Lehrinhalte:	• Angriffsszenarien • Modelle und Aussagen zur Sicherheit kryptographischer Verfahren • Statistische Methoden der Kryptoanalyse • Lineare Kryptoanalyse • Differenzielle Kryptoanalyse • Algebraische und zahlentheoretische Analysemethoden • Anwendungen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	Wird in der Vorlesung bekanntgegeben.
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	7621 Grundlagen der Kryptologie
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7626 Kryptoanalyse	0	2	0	1	U	M 30	1/36	5

Modulname:	**Embedded Systems Forensics und Speichertechnologien**	*Sprache:*	*deutsch*
Modulnummer:	7627	*Abschluss:*	B.Sc.
Modulcode:	03-FESFS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	7

Ausbildungsziele:	Klassische PCs verschwinden zunehmend als Gerät und werden durch "intelligente Gegenstände" ersetzt. Immer kleinere embedded Systems übernehmen Aufgaben, ohne dass ihre Existenz in jedem Fall überhaupt bekannt wird. So werden miniaturisierte Computer, zum Beispiel als sogenannte Wearables, mit unterschiedlichen Sensoren direkt in Kleidungsstücke eingearbeitet. Auch der klassische Magnetspeicher verschwindet zunehmend und wird durch elektronische Flash Speicher ersetzt. Diese Entwicklung stellt ganz neue Herausforderungen an die IT-Forensik und wird zu bedeutenden Umwälzungen führen. Im Teil "Embedded Systems Forensics" sollen verbreitete Technologien und Standards, Betriebssysteme und Grundlagen der Architektur von eingebetteten Systemen strukturiert dargestellt werden. Im Praktikum sollen Embeddeds eigenständig programmiert und ausgewertet werden. Im zweiten Teil "Speichertechnologien" sollen die Grundlagen moderner Speichertechnologien vermittelt werden. Es werden forensischen Tools für die Auswertung von eingebetteten Systemen vorgestellt und Szenarien erörtert. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Embbeded Systems der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.
Lehrinhalte:	• Grundlagen und Begriffe von embedded Systems • Der mbed Standard • RFID • Flash Technologien: NAND-Flash, NOR-Flash, EMMCs • JTAG und Boundary Scans • FPGAs • AT Befehle bei Speichertechnologien
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Embeddeds sowie mögliche Lösungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Jedem Studierendem soll für die praktische Arbeit zu Hause ein mbed-Board zu Verfügung gestellt werden. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• John Catsoulis: Designing Embedded Hardware. O'Reilly, 2005. • Paolo Pavan, Roberto Bez, Piero Olivo, Enrico Zanoni: Flash Memory Cells - An Overview. IEEE 1997 • Klaus Finkenzeller: RFID Handbuch.Hanser 2008 • Niklaus Wirth: Digital Circuit Design An Introduction Textbook. Springer, 1995 • IEEE STd 1149.1 (JTAG) Testability Primer, Texas Instruments, 1997
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	7601 Datenvirtualisierung und Wiederherstellen von Daten 7610 Betriebssysteme und digitale Spuren
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7627 Embedded Systems Forensics und Speichertechnologien	0	2	0	1		S 90	1/36	5

Modulname:	**Der Sachverständige vor Gericht**	*Sprache:*	*deutsch*
Modulnummer:	7628	*Abschluss:*	B.Sc.
Modulcode:	03-FDSVG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	7

Ausbildungsziele:	IT-Forensiker wie Ermittler müssen die Ergebnisse Ihrer Arbeit in Gutachten darlegen. An solche Gutachten werden definierte formale Ansprüche gestellt. Auch müssen diese Gutachten vor Gericht vertreten werden, auch hier gibt es einen formalen Rahmen der einzuhalten ist. Neben den formalen Kriterien gibt es eine Menge ungeschriebene Gesetze einzuhalten und der Sachverständige soll auch rhetorisch überzeugen. Das Modul "Der Sachverständige vor Gericht" soll die Anforderungen an ein Gutachten beziehungsweise an einen Sachverständigenvortrag vermitteln. Daneben sollen sprachliche und rhetorische Besonderheiten im Strafprozess dargelegt werden.
Lehrinhalte:	• Das Sachverständigengutachten • Der Sachverständigenvortrag • Der Sachverständige in der StPO • Juristische Rhetorik • Sprache und Duktus des Sachverständigenvortrags
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand eines konkreten Falls soll eigenständig ein Gutachten geschrieben und ein Sachverständigenvortrag vorbereitet werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Das Erstellte Gutachten soll in einem Sachverständigenvortrag dargestellt werden. In einem Rollenspiel wird eine Gerichtsverhandlung nachgestellt.
Literatur:	• Walter Byerlein: Praxishandbuch Sachverständigenrecht. CH.. Beck, 2000. • Harald Krammer, Jürgen Schille, Alexeander Schmidt, Alfred Tanczos: Sachverständige und ihre Gutachten. Manz 2015 • Fritjof Haft: Juristische Rhetorik. Alber Studienbuch, 2009.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7628 Der Sachverständige vor Gericht	0	2	0	1		V 20	1/36	5

Modulname:	**Predicted Policing / Dunkelfeld**	*Sprache:*	*deutsch*
Modulnummer:	7629	*Abschluss:*	B.Sc.
Modulcode:	03-FPPDU	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	7

Ausbildungsziele:	In der Kriminalforschung bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten, dem Hellfeld, und der vermutlich begangenen Kriminalität. Allein durch die Kriminalstatistiken kann vom Hellfeld nicht auf die tatsächliche Kriminalität geschlossen werden. Daher bedarf es der Dunkelfeldforschung, um das Dunkelfeld aufzuhellen und einen systematischen Überblick über die Kriminalitätsentwicklung zu erreichen. Predictive Policing hingegen bezeichnet die Analyse von Falldaten zur Berechnung der Wahrscheinlichkeit zukünftiger Straftaten zur Steuerung des Einsatzes von Polizeikräften Nach Abschluss des Moduls können die Studierenden die amtlichen Kriminalstatistiken lesen und verstehen. Sie kennen die aktuellen Verfahren um Aussagen über das Dunkelfeld und damit über die tatsächliche Kriminalität zu treffen. Die Studierenden erhalten ein differenziertes Bild von der Möglichkeit des Predictive Policing und Aussagekraft von Aussagen über die Vorhersage von Straftaten. Sie können mit einfachen Methoden selbstständig Modelle entwickeln. Nach Abschluss des Moduls verfügen die Studierenden über einen abgerundeten Überblick über das Fachgebiet. Sie können selbstständig Modellansätze entwerfen und eigenständig berechnen.
Lehrinhalte:	• Die Polizeiliche Kriminalstatisik • Hellfeld und Dunkelfeld • Kriminalitätsmessung • Kriminalitätsanalyse und kriminalstatistische Forschung • "Ethnic Profiling" • Re-Victimisierung • Ethische Implikationen von Predicted Policing • Rational-Choice-Theorie • Boost-Hypothese • Flag-Hypothese • Near-Repeat-Victimisation • Methoden zur Vorhersage • Modellierung von Kriminalität • Extrapolationsalgorithmen • Validierung von Kriminalitätsmodellen
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels einzuschickenden Aufgabenblättern und Übungen kontrolliert.
Literatur:	• Uwe Dörmann, Wolfgang Heinz: Zahlen sprechen nicht für sich. Aufsätze zu Kriminalstatistik, Dunkelfeld und Sicherheitsgefühl aus drei Jahrzehnten. Luchterhand, 2004. • Thomas Feltes, Benjamin Schmidt: Policing Diversity: Über den Umgang mit gesellschaftlicher Vielfalt innerhalb und außerhalb der Polizei. Verlag für Polizeiwissenschaft, 2015. • John S. Dempsey, Linda S. Forst: An Introduction to Policing, Delmar Cengage Learning, 2015. • Runtker Rienks: Predictive Policing: Taking a Chance for a Safer Future. Korpsmedia, 2015.

	• Graham Farrell, Ken Pease: Once Bitten, Twice Bitten: Repeat Victimisation and its Implications for Crime Prevention. Crime Prevention Unit Series Paper No. 46, London, 1993.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7629 Predicted Policing / Dunkelfeld	0	2	0	1		S 90	1/36	5

Modulname:	**Digitale Werte und Güter**	*Sprache:*	*deutsch*
Modulnummer:	7630	*Abschluss:*	B.Sc.
Modulcode:	03-FDWUG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	7

Ausbildungsziele:	Digitale Werte und Güter sind hochaktuelle Themen und haben weitreichende gesellschaftliche Einflüsse. Dank digitaler Technologien können heutzutage Transaktionen grenzenlos und ohne Einfluss von Regierungen durchgeführt werden. Dies eröffnet nicht nur große gesellschaftliche Chancen wie länderübergreifende Kommunikation oder weltweiten Geldtransfer, sondern auch Gefahren und Risiken. Unternehmen und Forschungseinrichtungen setzen in zunehmendem Maße auf Technologien wie der Blockchain, um Dienste zu dezentralisieren. Auch Regierungen haben das Thema erkannt und bemühen sich, sinnvolle Regulierungs- und Überwachungsmethoden zu implementieren. Dank des erworbenen Fach- und Methodenwissens sind die Teilnehmer in der Lage ● Dienste, die auf der Blockchaintechnologie beruhen, zu entwerfen, implementieren, administrieren und zu testen ● Unternehmen, die auf die Blockchaintechnologie setzen, zu beraten. ● Systeme, die auf der Blockchaintechnologie aufbauen, zu bewerten. Die Teilnehmer lernen und nutzen während des Studiums moderne Methoden und Werkzeuge und wenden diese für ihre eigenen Lösungen an.
Lehrinhalte:	Grundlagen ● Grundlagen Kryptografie und Kryptowährungen ● Dezentralisierung durch die Blockchain, Konsensfindung ● Erzeugen einer eigenen BTC-Adresse, Umgang mit Wallets, Erzeugen von Transaktionen, Verfolgen von Transaktionen im Netzwerk, Anonymität im Netzwerk, Alternative Mining Puzzles Erzeugen einer Altcoin ● Aufsetzen eines eigenen Altcoin-Clients ● Umsetzung einer Miningsoftware für die Altcoin ● Durchführung von Angriffsszenarien innerhalb der Altcoin Gesellschaftliche Einordnung von Bitcoin ● Regulierung ● Geschichte ● Community
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe verschickt, in denen wichtige theoretische Grundlagen vermittelt werden. Die Ausbildung setzt sich aus der Vermittlung von theoretischen Grundlagen und der praktischen Anwendung und Erprobung zusammen. Damit werden die Teilnehmer befähigt, sich selbständig in dem Thema weiterzubilden und dieses praktisch umzusetzen. Mit Literaturhinweisen und Links wird den Studierenden die Möglichkeit gegeben, sich je nach Interesse in weitere Spezialgebiete einzuarbeiten.
Literatur:	● Andreas M. Antonopoulos: Mastering Bitcoin. O''Reilly Media, 2013. ● Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly and Associates, 2015. ● Christof Paar, Jan Pelzl: Understaning Cryptography: A Textbook for Students and Practitioners. Springer, 2011.
Dozententeam:	Prof. Dr.-Ing. Ittner, Andreas (Hauptverantwortlicher) Dipl.-Ing. (FH) Meisel, Michael Dipl.-Volkswirt Oettler, Mario
Voraussetzungen:	keine
Vorausges. Module:	7621 Grundlagen der Kryptologie

Arbeitslast: *- workload*	150 Stunden, davon 45 Stunden Lehrveranstaltungen 105 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7630 Digitale Werte und Güter	0	2	0	1		S 90	1/36	5

Modulname:	**Praxisprojekt**	*Sprache:*	*deutsch*
Modulnummer:	7631	*Abschluss:*	B.Sc.
Modulcode:	03-FPRAX	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	8

Ausbildungsziele:	Die Studierenden sollen im Praktikum ihre bisher erworbenen theoretischen und praktischen Kenntnisse durch die Arbeit im Team anwenden. Dadurch vertiefen die Studierenden ihr im bisherigen Studium erworbenes Wissen und trainieren praktische Abläufe in einem beruflichen oder akademischen Umfeld. Die Studierenden erwerben weiterhin Kenntnisse von Unternehmens- und Institutsabläufen sowie die Kompetenz die Ergebnisse ihrer Tätigkeit nach innen und außen in einer angemessenen Art und Weise zu kommunizieren.
Lehrinhalte:	Interdisziplinäre und fachspezifische Mitarbeit an Forschungs- und Entwicklungsprojekten sowie Machbarkeitsstudien in Sicherheitsbehörden oder mit IT-Forensik / Cybercrime betrauten Unternehmen, Behörden oder Forschungseinrichtungen.
Lernmethoden:	Die wesentliche Methode ist hier "Lernen durch Tun". Anhand des raktikumsberichtes üben die Studierenden die systematische Darstellung der durchgeführten Arbeiten.
Literatur:	Selbst recherchierte Literaturhinweise der Studierenden.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr. rer. nat. Labudde, Dirk Prof. Dr. rer. pol. Pawlaszczyk, Dirk
Voraussetzungen:	130 Credits
Vorausges. Module:	keine
Arbeitslast: *- workload*	300 Stunden, davon 0 Stunden Lehrveranstaltungen 300 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7631 Praxisprojekt						B	2/36	10

Modulname:	**Bachelorprojekt**	*Sprache:*	*deutsch*
Modulnummer:	7632	*Abschluss:*	B.Sc.
Modulcode:	03-FBP	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CC-B 2016 IT-Forensik/Cybercrime	*Semester:*	8

Ausbildungsziele:

Die Bachelorarbeit kann in einem Unternehmen, einer Behörde, einer anderen Einrichtung oder auch an der Hochschule angefertigt werden. Der Studierende wird mit dieser abschließenden, selbständigen wissenschaftlichen Arbeit seine Berufsbefähigung für den Bereich IT-Forensik / Cybercrime nachweisen. Dabei wird er die bisher erworbenen theoretischen und praktischen Kenntnisse und Fertigkeiten ebenso wie übergreifende (soziale) Fähigkeiten anwenden bzw. einsetzen.

Ziele/Angestrebte Lernergebnisse:

- Die Studierenden sind in der Lage, fachbezogene Inhalte und Konzepte darzustellen sowie Kenntnisse einschlägiger Forschungsgebiete anzuwenden.
- Sie erkennen und formuliert Problemstellungen und kann diese innerhalb eines vorgegebenen Zeitrahmens konzeptionell unter Verwendung entsprechender Methoden lösen.
- Sie erfüllen die Anforderungen zur Aufnahme eines Masterstudiums.
- Sie besitzen Schlüsselqualifikationen wie Teamfähigkeit, Selbständigkeit, Durchhaltevermögen, Beharrlichkeit und Interdisziplinarität.

Durch das abschließende Kolloquium wird auch die Fähigkeit zur Präsentation erreichter Ergebnisse und zum fachlichen Streitgespräch gefordert.

Lehrinhalte:

Interdisziplinäre und fachspezifische Mitarbeit an Industrie-, Forschungsund Entwicklungsprojekten sowie Machbarkeitsstudien

Lernmethoden:

Selbständiges wissenschaftliches Arbeiten, ggf. auch im Rahmen eines Teams, unter wissenschaftlicher Anleitung/Betreuung, abschließendes Kolloquium (Präsentation und Diskussion)

Literatur:

Selbst recherchierte Literaturhinweise der Studierenden.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Prof. Dr. rer. nat. Labudde, Dirk
Prof. Dr. rer. pol. Pawlaszczyk, Dirk

Voraussetzungen:

140 Credits

Vorausges. Module:

keine

Arbeitslast: *- workload*

450 Stunden, davon
30 Stunden Lehrveranstaltungen
420 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7632 Bachelorprojekt	0	0	0	1	T		3/36	15
76321 Bachelorarbeit						BA		
76322 Tutorium für Examenskandidaten	0	0	0	1	T			
76323 Bachelorkolloquium						K 30		