HOCHSCHULE MITTWEIDA
University of Applied Sciences

Modulhandbuch

IT-Forensik/ Cybercrime (B.Sc.)

Inhaltsverzeichnis

MNR	*MC*	*Modulbezeichnung*	*Seite*
7602	03-FEINF	Grundlagen der IT-Forensik	4
7603	03-FEITS	Einführung in die IT-Sicherheit	5
7604	03-FAFI	Allgemeine Forensik I	6
7605	03-FCYB1	Cybercrime I	7
7606	03-FPRO1	Programmierung I	8
7607	03-FREBS	Betriebssysteme und digitale Spuren I	9
7608	03-FAFII	Allgemeine Forensik II	11
7611	03-FCYB2	Cybercrime II	12
7601	03-FCFM	Computerforensische Methoden	13
7609	03-FPRO2	Programmierung II Skriptsprachen	14
7610	03-FBUDS	Betriebssysteme und digitale Spuren II	15
7612	03-FBDFD	Forensik in DBMS	17
7613	03-FGDMF	Grundlagen der Mobilfunkforensik	18
7615	03-FEDSS	Entwicklung und Design sicherer Systeme	19
7633	03-FDAV	Grundlagen der Datenanalyse und -visualisierung	21
7622	03-FALGO	Algorithmen und Datenstrukturen	22
7625	03-FKPKR	Komplexpraktikum Krisenmanagement	23
7621	03-FGDK	Grundlagen der Kryptologie	24
7619	03-FGML	Grundlagen des maschinellen Lernens	25
7624	03-FFBVA	Forensische Bild- und Videoanalyse	26
7618	03-FDNCF	Datennetze/Cloud Forensik	27
7640	03-TRTM	Text Retrieval und Text Mining	28
7626	03-FKANA	Kryptoanalyse	29
7623	03-FDKMF	Datenkompression/Multimediaformate	30
7639	03-FPPDU	Predictive Policing/Dunkelfeld	32
7637	03-FNWF	Netzwerkforensik/ Abwehr von IT-Angriffen	34
7641	03-FSWPW	Softwareprojekt	35
7635	03-FMA	Malware Analysis	36
7627	03-FESFS	Embedded Systems Forensics und Speichertechnologien	37
7614	03-FSEOS	Social Engineering und OSINT	38
7636	03-FDSVG	Der Sachverständige vor Gericht	39
7638	03-FWOPM	Wissenschaftliches Oberseminar/ Projektmanagement	40
7632	03-FBP	Bachelorprojekt	41

Hinweis zur Bestellung der Prüfer:

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

Formen für Prüfungsvorleistungen und Prüfungssleistungen:

PVL-Formen: Te = Testat, s = schriftlich, m = mündlich, T = Testat, Prüfungsformen: M = Modulprüfung, Pl = Prüfungsleistung, s = schriftlich, m = mündlich, a = alternativ, sn = sonstige, BA = Bachelorarbeit, B = Beleg, K = Kolloquium, PA = Projektarbeit, V = Vortrag

Sonstige Abkürzungen:

V = Vorlesung (SWS), S = Seminar/Übung (SWS), P = Praktikum (SWS), T = Tutorium (SWS), PVL = Prüfungsvorleistung, PL = Prüfungsleistung, CP = Credit Points, SWS = Semesterwochenstunden, MNR = Modulnummer, MC = Modulcode

7602 Grundlagen der IT-Forensik

Modulname:	**Grundlagen der IT-Forensik**	*Unterrichtssprache:*	deutsch
Modulnummer:	7602	*Abschluss:*	B.Sc.
Modulcode:	03-FEINF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, 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 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.		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Grundlagen der IT-Forensik	0	2	0	1		Ms/90	5

7603 Einführung in die IT-Sicherheit

Modulname:	**Einführung in die IT-Sicherheit**	*Unterrichtssprache:*	deutsch
Modulnummer:	7603	*Abschluss:*	B.Sc.
Modulcode:	03-FEITS	*Häufigkeit:*	Wintersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, in denen die 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 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.

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter:

03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):

Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher)
M.Sc. Philipp Engler (Dozent)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Einführung in die IT-Sicherheit	0	2	0	1		Ms/90	5

7604 Allgemeine Forensik I

Modulname:	**Allgemeine Forensik I**	*Unterrichtssprache:*	deutsch
Modulnummer:	7604	*Abschluss:*	B.Sc.
Modulcode:	03-FAFI	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, in denen die 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 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		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Allgemeine Forensik I	0	2	0	1		Ms/90	5

7605 Cybercrime I

Modulname:	**Cybercrime I**	*Unterrichtssprache:*	deutsch
Modulnummer:	7605	*Abschluss:*	B.Sc.
Modulcode:	03-FCYB1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	1

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 und Skripte digital zur Verfügung gestellt, in denen die 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 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

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter:

03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):

Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Cybercrime I	0	2	0	1		Msn/PA	5

7606 Programmierung I

Modulname:	**Programmierung I**	*Unterrichtssprache:*	deutsch
Modulnummer:	7606	*Abschluss:*	B.Sc.
Modulcode:	03-FPRO1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, in denen die 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 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

Arbeitslast:

60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Programmierung I	0	2	1	1		Ms/90	5

7607 Betriebssysteme und digitale Spuren I

Modulname:	**Betriebssysteme und digitale Spuren I**	*Unterrichtssprache:*	deutsch
Modulnummer:	7607	*Abschluss:*	B.Sc.
Modulcode:	03-FREBS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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. Im Modul sollen zudem die drei gebräuchlichsten Betriebssysteme MS Windows, macOS und Linux vorgestellt werden. Für alle Betriebssysteme sollen Kenntnisse der Protokollierungs- und Konfigurationsdaten sowie deren forensischer Nutzen vermittelt werden. Nach Abschluss des Moduls sollen die Studierenden qualifiziert sein selbstständig vom Betriebssystem verwaltete Spuren forensisch auszuwerten und zu interpretieren.		
Lehrinhalte:	Betriebssystemarchitektur: - Ebenen eines Rechnersystems - Definition, schematischer Aufbau und Aufgabe von Betriebssystemen - Ressourcenverwaltung durch Betriebssysteme - Betriebssystemarchitekturen - Zugriffsverwaltung Prozesse, Tasks und Threads - Speicherverwaltung und Speicherzugriffe - Datenträgeranbindung Windows: - Einrichtung und Administration aktueller Betriebssysteme - Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, EventLogging, Registrierungsdatenbank, Betriebssystemartefakte, Benutzerkonten und Gruppen) - Verwendung von Netzwerken und Schutzmechanismen - Virtualisierung und Subsysteme in Windows Linux: - Historie und aktuelle Distributionen - Filesystem Hierarchy Standard - Paket- und Dienstmanager - Sicherheitsmechanismen in Linux - Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, Logging, Konfiguration, Betriebssystemartefakte, Benutzerkonten und Gruppen) macOS: - Speicherstrukturen SQLite und Plist verstehen und anwenden - Systeminterne Spuren und forensische Aspekte (zuletzt verwendete Dokumente, Kommunikationsapps, Spotlight und Browser-Artefakte) - Logdateien - Umgang mit Diskimages und Backupmöglichkeiten (iOS und Time-Machine) - Grundlagen und Integration von iCloud		

Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Studienhefte/Lehrmaterialien digital zur Verfügung gestellt, in denen die wichtigsten theoretische und praxisrelevante Grundlagen des Moduls vermittelt werden. Dabei werden ausgewählte Probleme (z.B. Prozess-/Threadverwaltung, Prozess-Synchronisation und - Kommunikation) diskutiert und typische Algorithmen bzw. Strategien von Betriebssystemen 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 durchgeführt bzw. diskutiert. Dies beinhaltet die speziellen Eigenheiten der vorgestellten Betriebssysteme und die Auswirkungen auf die digitale Beweissicherung. Dies dient gleichzeitig der Prüfungsvorbereitung.
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. - Brandt, Marc: Mac OS Hacking: Professionelle Werkzeuge und Methoden zur forensischen Analyse des Apple-Betriebssystems, FRANZIS Verlag GmbH; 1st edition (28 Aug. 2017), ISBN-13: 978-3645605519 - Mandel,P.: Grundkurs Betriebssysteme. Wiesbaden: Vieweg, 4. Aufl. 2014 - Schneider, U. (Hrsg.): Taschenbuch der Informatik. München: Hanser (Leipzig: Fachbuchverlag), 7. Auflage, 2012 - Tanenbaum, A.S.: Moderne Betriebssysteme, 3. Aufl., Pearson Studium, 2009
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. pol. Ronny Bodach (Dozent)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Betriebssysteme und digitale Spuren I	0	2	0	1		Ms/90	5

7608 Allgemeine Forensik II

Modulname:	**Allgemeine Forensik II**	*Unterrichtssprache:*	deutsch
Modulnummer:	7608	*Abschluss:*	B.Sc.
Modulcode:	03-FAFII	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung, 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 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
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)
Vorausgesetzte Module:	7604 Allgemeine Forensik I

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Allgemeine Forensik II	0	2	0	1		Ms/90	5

7611 Cybercrime II

Modulname:	**Cybercrime II**	*Unterrichtssprache:*	deutsch
Modulnummer:	7611	*Abschluss:*	B.Sc.
Modulcode:	03-FCYB2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 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 und Skripte digital zur Verfügung gestellt, in denen die 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 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.

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)

Vorausgesetzte Module: 7605 Cybercrime I

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Cybercrime II	0	2	0	1		Msn/PA	5

7601 Computerforensische Methoden

Modulname:	**Computerforensische Methoden**	*Unterrichtssprache:*	deutsch
Modulnummer:	7601	*Abschluss:*	B.Sc.
Modulcode:	03-FCFM	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	3

Ausbildungsziele:

Im Modul Computerforensische Methoden werden den Studierenden theoretische und praktische Grundlagen der Computerforensik und damit die klassischen Kompetenzen eines IT-Forensikers vermittelt.

Sie lernen das Aufgabenfeld, Probleme und Lösungen an Hand von Datensicherungs- und Untersuchungsmethoden kennen. Dabei werden Sie mit den entsprechenden Methoden und ausgewählten Werkzeugen vertraut gemacht. Die Vorlesung wird durch ein Praktikum ergänzt, um erworbene Kenntnisse praktisch zu erproben und zu vertiefen. Die Studierenden werden in die Lage versetzt, selbstständige computerforensische Untersuchungen durchzuführen, Probleme zu erkennen und zu lösen, und neue Methoden und Werkzeuge auf ihre Eignung einzuschätzen.

Die Grundlagen umfassen Aspekte der strategischen wie auch operativen Vorbereitung von Datensicherungen und Datenuntersuchungen. Hierfür werden verschiedene Anwendungsfälle bezogen auf die möglichen Datensicherungsmethoden vorgestellt, sowie auf Standards der computerforensischen Untersuchungen hingewiesen.

Vertiefend werden die verschiedenen Arten der Datenaufbereitung und Datenauswertung im Rahmen einer computerforensischen Untersuchung besprochen. Dabei wird auf die Datenspeicherung, auf Werkzeuge sowie für die forensische Fallarbeit wichtige Artefakte von unterschiedlichen Betriebssystemen sowohl im privaten wie auch unternehmerischen Umfeld eingegangen.

Lehrinhalte:

- strategische wie operative Vorbereitung von computerforensischen Untersuchungen
- Datensicherungsmethoden und deren Anwendung auch in Bezug auf spezielle Anwendungsfälle, wie defekten Datenträgern und RAID Systemen
- Datenuntersuchungsmethoden und deren Techniken, wie etwa das Carving bei der Datenwiederherstellung und der Umgang mit gelöschten Daten, wie etwa den Slackbereichen
- Informationsgewinnung aus Strukturen von Dateisystemen und Betriebssystemen und deren zeitliche Einordnung
- Virtualisierung als Untersuchungsgegenstand und Virtualisierung als Teil der computerforensischen Untersuchungsmethoden
- Probleme und Grenzen der computerforensischen Methoden

Lernmethoden:

Die Vorlesung vermittelt das notwendige Wissen und die Grundlagen über anerkannte Verfahren und Techniken sowie Spezialwissen in ausgewählten Bereichen. Im Praktikum sollen die Studierenden selbstständig Aufgabenstellungen im Bereich der Datensicherungs- und Untersuchungsmethoden erarbeiten.

Literatur:

-Leitfaden IT-Forensik. Bundesamt für Sicherheit in der Informationstechnik, 2011.

- Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005.
- Lorenz Kuhlee, Victor Völzow: Computer-Forensik Hacks. O'Reilly Verlag GmbH & Co. KG, 2012.
- Harlan Carvey: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Syngress, 2016.
- Harlan Carvey: Investigating Windows Systems, Academic Press, 2018
- William Oettinger: Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital, Packt Publishing, 2020
- Bruce Nikkel: Practical Forensic Imaging: Securing Digital Evidence with Linux Tools, No Starch Press, 2016

Arbeitslast:

60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. pol. Ronny Bodach (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Computerforensische Methoden	0	2	1	1		Ms/90	5

7609 Programmierung II Skriptsprachen

Modulname:	**Programmierung II Skriptsprachen**	*Unterrichtssprache:*	deutsch
Modulnummer:	7609	*Abschluss:*	B.Sc.
Modulcode:	03-FPRO2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 sowie Skripte, 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		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Dipl.-Informatiker (FH) Daniel Stockmann (Dozent, Inhaltverantwortlicher)		
Vorausgesetzte Module:	7606 Programmierung I		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Programmierung II Skriptsprachen	0	2	0	1		Ms/90	5

7610 Betriebssysteme und digitale Spuren II

Modulname:	**Betriebssysteme und digitale Spuren II**	*Unterrichtssprache:*	deutsch
Modulnummer:	7610	*Abschluss:*	B.Sc.
Modulcode:	03-FBUDS	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	3
Ausbildungsziele:	Dateisysteme liefern generell umfangreiche forensisch wertvolle Informationen. Dies liegt darin begründet, dass die Grundlage für funktionierende Computersysteme die persistente Speicherung von Daten auf Massenspeichern ist. Automatisierte Werkzeuge sind in der Lage diese Daten aufzubereiten. Inhalt des Moduls, soll es sein die automatisierten Abläufe dieser Werkzeuge zu verstehen und Dateisysteme manuell zu untersuchen. Dabei liegt der Fokus auf der forensischen Untersuchung dieser Dateisysteme, was unter anderem die Wiederherstellung gelöschter Daten beinhaltet. Nach Abschluss des Moduls sollen die Studierenden qualifiziert sein selbstständig von den gängigen Dateisystemen gespeicherte Daten forensisch auszuwerten und gegebenenfalls wiederherzustellen.		
Lehrinhalte:	Einführung: - Grundbegriffe und Bedeutung von Dateisystemen - Festplattenpartitionierung (Master Boot Record und GPT Partitionierung) - Besonderheiten in Dateisystemen (Zeitstempel, Slackspeicher, Disableing Last Access Timestamp) Windows Dateisysteme: - FAT-Dateisysteme (Aufbau FAT-Partition, Strukturen im FAT Dateisystem, Löschung und Wiederherstellung von Daten in FAT) - NTFS-Dateisystem (Historie, Aufbau von NTFS, Strukturen im NTFS, Speichern und Löschen von Daten in NTFS) - ExFAT Dateisystem (Aufbau ExFAT-Partition, Strukturen im ExFAT Dateisystem, Löschung und Wiederherstellung von Daten in ExFAT) - LDM, WSS und ReFS Dateisystem Linux Dateisysteme: - Ext-Dateisystem (Klassifikation von Linux Dateisysteme, Grundlegendes und Komptabilität von Extx, Besonderheiten von Ext3 und Ext4, Journaling in Ext, Sparse, Flex und Meta Blockgroups) - F2FS Dateisystem (Aufbau Log Structured Dateisysteme, Aufbau von F2FS, Strukturen im F2FS, Speichern und Löschen von Daten in F2FS) - Logical Volume Manager / Device Mapping macOS Dateisysteme: - HFS+ (Historie, Aufbau von HFS, Strukturen im HFS,Besonderheiten der B-Tree Strukturen, Speichern und Löschen von Daten in HFS) - APFS (Neuerungen und Features von APFS, Aufbau von APFS Partitionen, Forensische Untersuchung von APFS Container		
Lernmethoden:	Die Vorlesung vermittelt das notwendige Wissen. Dies beinhaltet die speziellen Eigenheiten der vorgestellten Dateisysteme, deren Kenngrößen und die Auswirkungen auf die forensischen Beweisspuren. Im Seminar sollen ausgewählte Themen durch die Studierenden unter Anleitung selbstständig erarbeitet werden. Im Praktikum sollen die Studierenden selbstständig Daten auswerten. Dazu sollen Ihnen sogenannte Images zur Verfügung gestellt werden. Hier soll ihnen vermittelt werden, wie sie ihr gewonnenes Wissen praktisch einsetzen und anwenden können.		
Literatur:	- Leitfaden IT-Forensik. Bundesamt für Sicherheit in der Informationstechnik, 2011. - Mark E. Russinovich, David A. Solomon, Alex Ionescu: Windows Internals. Microsoft Press, 2012. - Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005. - Brandt, Marc: Mac OS Hacking: Professionelle Werkzeuge und Methoden zur forensischen Analyse des Apple-Betriebssystems, FRANZIS Verlag GmbH; 1st edition (28 Aug. 2017), ISBN-13: 978-3645605519		
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		

Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	M.Sc. Stefan Schildbach (Dozent) Prof. Dr. rer. pol. Ronny Bodach (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Betriebssysteme und digitale Spuren II	0	2	1	1		Ms/90	5

7612 Forensik in DBMS

Modulname:	**Forensik in DBMS**	*Unterrichtssprache:*	deutsch
Modulnummer:	7612	*Abschluss:*	B.Sc.
Modulcode:	03-FBDFD	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	3

Ausbildungsziele:

Die Menge an Daten in vielen Bereichen, u.a. in der Forensik, nimmt ständig zu. Die richtige Aufbereitung und Verwaltung dieser Daten entscheidet vielfach über den Erfolg, sei es bei geschäftskritischen Anwendungen oder zur Fahndung nach Tätern. Das Modul zeigt auf, wie Daten sinnvoll strukturiert und mit der aktuellen Datenbanktechnologie verwaltet und verarbeitet werden können. Dabei wird der Bogen vom konzeptionellen Design bis zur Implementierung gespannt. Im Ausblick werden weitere Technologien, NoSQL Systeme, vorgestellt, die insbesondere zur Verwaltung von großen Datenmengen verwendet werden.
Die Studierende erlernen den Umgang mit Daten, ihre Strukturierung sowie ihre Verwaltung unter Nutzung von Datenbanksystemen. Die Datenbanken werden mit besonderen Augenmerk auf die Verwaltung von großen Datenbeständen entwickelt.

Lehrinhalte:

- Strukturierung von Daten
- Design und Implementierung von Datenbanken
- Import, Modifikation und Retrieval von Daten in Datenbanken
- Verwaltung von Forensikdaten
- Überblick über NoSQL Ansätze und Systeme

Lernmethoden:

Im Rahmen des berufsbegleitenden Fernstudiums werden wichtige theoretische Grundlagen und deren praktische Anwendung vermittelt. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden Herangehensweisen konfrontiert und ausgewählte Themen eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Aufgaben können in einem bereitgestellten Datenbanksystem umgesetzt werden. Die Lösungen werden in Tutorien und Konsultationen besprochen.

Literatur:

- M. Emrich (2013): Datenbanken & SQL für Einsteiger: Datenbankdesign und MySQL in der Praxis. CreateSpace Independent Publishing Platform
- H. Garcia-Molina, J. Ullman, J Widom (2009): Database Systems. The Complete Book. Pearson. Prentice Hall
- S. Edlich, A. Friedland, J. Hampe, B. Brauer, M. Brückner (2011): NoSQL - Einstieg in die Welt nichtrelationaler Web 2.0 Datenbanken. Hanser Verlag.

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. nat. Hanna Köpcke (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Forensik in DBMS	0	2	0	1		Ms/90	5

7613 Grundlagen der Mobilfunkforensik

Modulname:	**Grundlagen der Mobilfunkforensik**	*Unterrichtssprache:*	deutsch
Modulnummer:	7613	*Abschluss:*	B.Sc.
Modulcode:	03-FGDMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, 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 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
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. pol. Ronny Bodach (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Grundlagen der Mobilfunkforensik	0	2	1	1		Ms/90	5

7615 Entwicklung und Design sicherer Systeme

Modulname:	**Entwicklung und Design sicherer Systeme**	*Unterrichtssprache:*	deutsch
Modulnummer:	7615	*Abschluss:*	B.Sc.
Modulcode:	03-FEDSS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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/Lehrmaterialiendigital zur Verfügung gestellt, 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		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		

Dozententeam (Rollen):	Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher) M.Sc. Philipp Engler (Dozent)
Vorausgesetzte Module:	7606 Programmierung I, 7609 Programmierung II Skriptsprachen

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Entwicklung und Design sicherer Systeme	0	2	0	1		Ms/90	5

7633 Grundlagen der Datenanalyse und -visualisierung

Modulname:	**Grundlagen der Datenanalyse und -visualisierung**	*Unterrichtssprache:*	deutsch
Modulnummer:	7633	*Abschluss:*	B.Sc.
Modulcode:	03-FDAV	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	4
Ausbildungsziele:	Die Studierenden werden in die Lage versetzt, selbstständig unbekannte Datensätze zu analysieren, statistisch zu beschreiben, sinnvolle Fragestellungen abzuleiten und Zusammenhänge in geeigneter Weise visuell zu präsentieren.		
Lehrinhalte:	Die Studierenden erhalten einen umfassenden Einblick in die explorative Datenanalyse mittels deskriptiver Statistik. Dabei wird ein iterativer Prozess durchlaufen, welcher von den Rohdaten zu sinnvollen Einsichten und neuen Fragestellungen führt. Dieser Prozess umfasst neben der Datenbereinigung,- erweiterung und -transformation auch deskriptive Statistik und die Fähigkeit Zusammenhänge in geeigneter Weise zu visualisieren. Die Studierenden erhalten Sie eine grundlegende Einführung in die Programmiersprache R. Die vermittelten theoretischen Grundlagen werden praktisch anhand von Real-World-Datensätzen mit Hilfe von R untermauert.		
Lernmethoden:			
Literatur:	D. Wollschläger, Grundlagen der Datenanalyse mit R - Eine anwendungsorientierte Einführung, 2. Auflage, Springer Spektrum (Heidelberg) 2012		
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Michael Spranger (Dozent, Inhaltverantwortlicher) M.Sc., M.A. Jenny Felser (Dozent)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Grundlagen der Datenanalyse und -visualisierung	0	2	1	1		Msn/B	5

7622 Algorithmen und Datenstrukturen

Modulname:	**Algorithmen und Datenstrukturen**	*Unterrichtssprache:*	deutsch
Modulnummer:	7622	*Abschluss:*	B.Sc.
Modulcode:	03-FALGO	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	4
Ausbildungsziele:	Die Studierenden erhalten einen Einblick in ausgewählte Kapitel der Algorithmen und Datenstrukturen. Sie lernen neben grundlegenden algorithmischen Design-Prinzipien, insbesondere die asymptotische Abschätzung als Werkzeug der Beurteilung von Algorithmen und Datenstrukturen hinsichtlich ihrer Komplexität kennen. Nach Abschluss des Moduls sind die Teilnehmer in der Lage geeignete Algorithmen und Datenstrukturen für die Lösung eigener Problemstellungen auszuwählen und zu implementieren.		
Lehrinhalte:	-Ausgehend von der grundlegenden Erörterung der Begriffe Algorithmen und Datenstrukturen werden Fragen der Effizienz diskutiert und die asymptotische Komplexitätsabschätzung eingeführt. Anschließend wird eine Auswahl algorithmischer Design-Prinzipien vorgestellt, wie: • Rekursion • Greedy-Strategie • Divide and Conquer • Dynamische Programmierung Anschließend werden ausgewählte Algorithmen und Datenstrukturen vorgestellt und praktisch in der Programmiersprache R implementiert, z.B.: • Such- und Sortieralgorithmen • String Matching • Graph-Algorithmen • Stack, Arrays, Listen, Hashtabellen		
Lernmethoden:			
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		
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Michael Spranger (Dozent, Inhaltverantwortlicher) M.Sc., M.A. Jenny Felser (Dozent)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Algorithmen und Datenstrukturen	0	2	1	1		Ms/90	5

7625 Komplexpraktikum Krisenmanagement

Modulname:	**Komplexpraktikum Krisenmanagement**	*Unterrichtssprache:*	deutsch
Modulnummer:	7625	*Abschluss:*	B.Sc.
Modulcode:	03-FKPKR	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	4

Ausbildungsziele:

Die Bedrohungslage für Unternehmen und Behörden steigt immer weiter an: laut Bitkom waren von 2015 bis 2016 53% der Unternehmen in Deutschland direkt von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen - Tendenz steigend. Durch die zunehmende Vernetzung von Geräten und Diensten Vergrößert sich die virtuelle Angriffsfläche in Organisationen. Damit wachsen auch die unmittelbaren Auswirkungen eines Cyber-Angriffs und die damit verbundenen Schäden innerhalb einer Organisation. Um bei Angriffen oder Notfällen eine strukturierte und zielführende Vorgehensweise zu wahren, ist ein wirkungsvolles Krisenmanagement erforderlich. Dies stellt eine komplexe Aufgabe dar, da viele verschiedene Akteure berücksichtigt werden müssen. Hinzu kommt ein geringes Risiko- und Gefahrenbewusstsein innerhalb von Organisationen.

-Das eigene Bewusstsein für die Gefahren von Cyberangriffen bezogen auf den Einzelnen und ganze Unternehmen schärfen

- Souverän in Krisensituationen reagieren zu können
- Die Verbesserung der Kommunikation sowie die gemeinsame Lösungsfindung im Krisenfall
- die eigenen Abläufe und interne sowie externe Prozesse in Krisensituationen besser nachvollziehen können

Lehrinhalte:

- Kommunikationstheorie
- Entscheidungsmodell und Problemlösungsprozess
- Krisensimulation
- Review der Simulation

Lernmethoden:

Simulation von realitätsnahen Krisensituationen

Handlungsorientierte Empfehlungen zur Lösung von Krisensituationen

Business Impact Analyse und Entwicklung eines Risikomodells

Literatur:

Arbeitslast:

120 Stunden Lehrveranstaltungen
30 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter:

03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):

Prof. Dr. rer. nat. Dirk Labudde
(Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Komplexpraktikum Krisenmanagement	0	2	4	2		Msn/PA	5

7621 Grundlagen der Kryptologie

Modulname:	**Grundlagen der Kryptologie**	*Unterrichtssprache:*	deutsch
Modulnummer:	7621	*Abschluss:*	B.Sc.
Modulcode:	03-FGDK	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 • Algebraische und zahlentheoretische Grundlagen • Asymmetrische Verfahren • Kryptographische Hashfunktionen • Digitale Signaturen		
Lernmethoden:	Im Rahmen des berufsbegleitenden Fernstudiums werden Lehrbriefe und Skripte digital zur Verfügung gestellt, 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.		
Literatur:	• B. Esslinger: Das CrypTool-Skript, Draft-Version, 2013. • A. McAndrew: Introduction to Cryptography with Open-Source Software. CRC Press, 2011		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Christian Hummert (Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Grundlagen der Kryptologie	0	2	0	1		Mm/15	5

7619 Grundlagen des maschinellen Lernens

Modulname:	**Grundlagen des maschinellen Lernens**	*Unterrichtssprache:*	deutsch
Modulnummer:	7619	*Abschluss:*	B.Sc.
Modulcode:	03-FGML	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	5
Ausbildungsziele:	Die Studierenden werden mit den grundlegenden Fragestellungen des maschinellen Lernens als Teilgebiet der künstlichen Intelligenz vertraut gemacht. Sie werden in die Lage versetzt, selbstständig Probleme zu identifizieren, die mittels maschinellen Lernens gelöst werden können und geeignete Lernverfahren auszuwählen. Weiterhin sollen die Teilnehmer befähigt werden die Performanz verschiedener Verfahren für ein konkretes Problem zu beurteilen.		
Lehrinhalte:	Inhalt: Neben grundlegenden Begriffsdefinitionen und - abgrenzungen werden ausgewählte Algorithmen und Strategien aus den folgenden Bereichen vermittelt: • Regression • Klassifikation • Clusteranalyse • Evaluation • Text Mining Die vermittelten theoretischen Grundlagen werden praktisch anhand von Real-World-Datensätzen mit Hilfe der Programmiersprache R untermauert.		
Lernmethoden:			
Literatur:	M. Kubat, An Introduction to Machine Learning, 2. Edition, Springer Int., 2017		
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Michael Spranger (Dozent, Inhaltverantwortlicher) M.Sc., M.A. Jenny Felser (Dozent)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Grundlagen des maschinellen Lernens	0	2	1	1		Ms/90	5

7624 Forensische Bild- und Videoanalyse

Modulname:	**Forensische Bild- und Videoanalyse**	*Unterrichtssprache:*	deutsch
Modulnummer:	7624	*Abschluss:*	B.Sc.
Modulcode:	03-FFBVA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	5
Ausbildungsziele:	Den Teilnehmern werden Grundlagen der Bildverarbeitung vermittelt, die sowohl in der industriellen Anwendung, wie auch für die digitale Forensik, benötigt werden. Studierende sollen in die Lage versetzt werden Fachpublikationen zu spezielleren Verfahren zu verstehen, oder eigene Lösungen aus einem Repertoire von Algorithmen zu entwickeln. An einigen Stellen wird speziell auf die Anforderungen der Bild- und Video-Forensik eingegangen.		
Lehrinhalte:	• Vorstellung bildgebender Geräte wie CCD- und Zeilensensoren • Farbpattern, Interpolationsverfahren • Digitale Kurven • Houghtransformation und Curvature Scale Space • Der Gradient und einige praktische Anwendungen • Neuronale Netze in der Mustererkennung inkl. Backpropagation • Die Fouriertransformation • Die Diskrete Cosinustransformation • Filter und Faltungen • Histogramme, Histogrammverbesserungen • Texturmaße		
Lernmethoden:	Die Vermittlung des Grundwissens findet über kurze Videos statt, die nach Themen geschnitten sind und im Vorfeld jeder Veranstaltung gehört werden. Über das Semester finden zu vereinbarten Zeiten einige Onlineveranstaltung statt. In diesen greifen wir die Inhalte aus den Videos auf, vertiefen Sie und arbeiten Beispiele aus, die gemeinsam bearbeitet und anschließend aufgelöst werden. Einige Verfahren werden in den Videos an konkreten Codebeispielen veranschaulicht und sofort demonstriert. Diese Beispiele werden in den Onlineveranstaltungen i.d.R. aufgegriffen und ergänzt.		
Literatur:	Zur Veranstaltung werden umfangreiche Materialien wie Folien, Videos und Codebeispiele zur Verfügung gestellt. Der Erwerb weiterer Literatur ist nicht zwingend nötig. Einige Inhalte wurden den folgenden Veröffentlichungen entnommen. • Tönnies, K.D.: Grundlagen der Bildverarbeitung, Pearson Studium, 2005 • Zamperoni, P.: Methoden der digitalen Bildsignalverarbeitung, Braunschweig, Vieweg, 1991 • Gonzales, R.C.; Wintz, P.: Digital Image Processing, Addison-Wesley, 1987 • Steinbrecher, R.: Bildverarbeitung in der Praxis, Oldenbourg, 1993 • Pavlidis, T.:Algorithms for Graphics and Image Processing, Springer, 1982 • 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		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. habil. Thomas Haenselmann (Dozent, Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Forensische Bild- und Videoanalyse	0	2	0	1		Ms/90	5

7618 Datennetze/Cloud Forensik

Modulname:	**Datennetze/Cloud Forensik**	*Unterrichtssprache:*	deutsch
Modulnummer:	7618	*Abschluss:*	B.Sc.
Modulcode:	03-FDNCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 digital zur Verfügung gestellt, 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.
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher) M.Sc. Philipp Engler (Dozent)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Datennetze/Cloud Forensik	0	2	0	1		Ms/90	5

7640 Text Retrieval und Text Mining

Modulname:	**Text Retrieval und Text Mining**	*Unterrichtssprache:*	deutsch
Modulnummer:	7640	*Abschluss:*	B.Sc.
Modulcode:	03-TRTM	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	6
Ausbildungsziele:	Die Studierenden erhalten einen umfassenden Einblick in grundlegende Modelle und Methoden des Text Retrieval und Text Mining.		
Lehrinhalte:	• Retrieval-Modelle (Vektorraummodelle, probabilistische Sprachmodelle) • Implementierung und Evaluation von Suchmaschinen • Feedback in Text-Retrieval-Systemen • Suche im Web (Indexing, Linkanalyse) • Recommender Systems (Content-based Filtering, Collaborative Filtering) • Word Association Mining (syntagmatische und paradigmatische Relationen) • Text Clustering/Categorization • Topic Analysis (PLSA, LDA) • Opinion Mining/Sentiment Analysis • Joint Analysis (Text und strukturierte Daten)		
Lernmethoden:	• Vorlesungen mit Folien, Beamer-Präsentationen, Tafel; • Übungen, Präsentationen und Animationen, Gruppengespräche		
Literatur:	• Zhai; Massung: Text Data Management and Analysis. 2016 • Manning and Schütze: Foundations of Statistical Natural Language Processing. MIT Press. Cambridge, MA: May 1999. • Heyer; Quasthoff: Text Mining - Wissensrohstoff Text - Konzepte Algorithmen, Ergebnisse. 2006		
Arbeitslast:	**60** Stunden Lehrveranstaltungen **90** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Michael Spranger (Dozent, Inhaltverantwortlicher) M.Sc., M.A. Jenny Felser (Dozent)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Text Retrieval und Text Mining	2	1	1	0		Ms/90	5

7626 Kryptoanalyse

Modulname:	**Kryptoanalyse**	*Unterrichtssprache:*	deutsch
Modulnummer:	7626	*Abschluss:*	B.Sc.
Modulcode:	03-FKANA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	6
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 und Skripte digital zur Verfügung gestellt, in denen die 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 Aufgabenblättern und Übungen kontrolliert.		
Literatur:	Wird in der Vorlesung bekanntgegeben.		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Christian Hummert (Inhaltverantwortlicher)		
Vorausgesetzte Module:	7621 Grundlagen der Kryptologie		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Kryptoanalyse	0	2	0	1		Mm/15	5

7623 Datenkompression/Multimediaformate

Modulname:	**Datenkompression/Multimediaformate**	*Unterrichtssprache:*	deutsch
Modulnummer:	7623	*Abschluss:*	B.Sc.
Modulcode:	03-FDKMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, in denen die 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 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
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):	Prof. Dr. rer. nat. Marc Ritter (Dozent, Inhaltverantwortlicher) M.Sc. Manuel Heinzig (Dozent)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Datenkompression/Multimediaformate	0	2	0	1		Ms/90	5

7639 Predictive Policing/Dunkelfeld

Modulname:	**Predictive Policing/Dunkelfeld**	*Unterrichtssprache:*	deutsch
Modulnummer:	7639	*Abschluss:*	B.Sc.
Modulcode:	03-FPPDU	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	6
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 und Skripte digital zur Verfügung gestellt, in denen die 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 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.		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Predictive Policing/Dunkelfeld	0	2	0	1		Mm/30	5

7637 Netzwerkforensik/ Abwehr von IT-Angriffen

Modulname:	**Netzwerkforensik/ Abwehr von IT-Angriffen**	*Unterrichtssprache:*	deutsch
Modulnummer:	7637	*Abschluss:*	B.Sc.
Modulcode:	03-FNWF	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	6

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 IT-Angriff.

Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich ITForensik / 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:

Die Vorlesung vermittelt das notwendige Wissen. Dies beinhaltet die zugrunde liegenden Protokolle der einzelnen Services ebenso wie die die IT-Sicherheit im Speziellen Fall. Im Seminar sollen ausgewählte Themen seminaristisch 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.

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.

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. pol. Ronny Bodach (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Netzwerkforensik/ Abwehr von IT-Angriffen	0	2	1	0		Ms/90	5

7641 Softwareprojekt

Modulname:	**Softwareprojekt**	*Unterrichtssprache:*	deutsch
Modulnummer:	7641	*Abschluss:*	B.Sc.
Modulcode:	03-FSWPW	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	7
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)		
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher) Prof. Dr. rer. nat. Michael Spranger (Dozent, Inhaltverantwortlicher)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Softwareprojekt	0	0	2	1		Msn/PA	5

7635 Malware Analysis

Modulname:	**Malware Analysis**	*Unterrichtssprache:*	deutsch
Modulnummer:	7635	*Abschluss:*	B.Sc.
Modulcode:	03-FMA	*Häufigkeit:*	Wintersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	7

Ausbildungsziele:	Die Teilnehmer kennen Aufbau und Arbeitsweise von Computerviren, Würmern, Trojanern, Rootkits und anderen Malware-Programmen (Grundlagenwissen und Fachkompetenz). Sie verfügen über vertiefte Kenntnisse über grundlegende Viren-Erkennungsverfahren. Sie besitzen praktische Erfahrungen bei der Implementierung eigener signatur- und lernbasierter Erkennungsverfahren für Computerviren (Methodenkompetenz).
Lehrinhalte:	• Aufbau und Funktionsweise von Viren, Würmern und Trojanern. • Schutztechniken von Computerviren (Verschlüsselung, Stealth, Retro, Polymorph, Metamorph) • Formen von Viren (Boot-, Makro-, Skript-, Email-, Datei- und Linkviren), • Infektorverfahren (SLOW und FAST) • Tarntechniken (Rootkits) • ClamAV-Engine • Signaturbasierte Erkennung versus maschinelle Lernansätze • Grundlagen des maschinellen Lernens auf strukturierten Daten • Klassifikationsalgorithmen zur Identifizierung von Malware/Viren • Theoretische Grenzen der Erkennungsleistung von Schadprogramm-Scannern.
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten Programmieraufgaben, u.a. im Umfeld der Antiviren-Software ClamAV. Am Beispiel dieses Open-Source-Frameworks werden Verfahren der Virensuche und Erkennung praktisch gezeigt, bis hin zur Implementierung eigener Such-Heuristiken. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	• Vorlesungsmanuskript (Folienkopien) • Skoudis, E; Zeltser, L.: Malware: Fighting Malicious Code., Prentice Hall International 2003. • Ligh, M. et al: Malware Analiyst's Cookbook: Tools and Techniques for Fighting Malicious Code. John Wiley and Sons 2010. • Malin C.H. et al: Malware Forensics: Investigating and Analyzing Malicious Code. Syngress Media 2008. • Szor, P. : The Art of Computer Virus Research and Defense. Addison Wesley, 3. Auflage 2005.
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher) M.Sc. Philipp Engler (Dozent)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Malware Analysis	0	2	0	1		Ms/90	5

7627 Embedded Systems Forensics und Speichertechnologien

Modulname:	**Embedded Systems Forensics und Speichertechnologien**	*Unterrichtssprache:*	deutsch
Modulnummer:	7627	*Abschluss:*	B.Sc.
Modulcode:	03-FESFS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 digital zur Verfügung gestellt, 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 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

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): M.Sc. Felix Fischer (Dozent, Inhaltverantwortlicher)

Vorausgesetzte Module: 7601 Computerforensische Methoden, 7610 Betriebssysteme und digitale Spuren II

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Embedded Systems Forensics und Speichertechnologien	0	2	0	1		Ms/90	5

7614 Social Engineering und OSINT

Modulname:	**Social Engineering und OSINT**	*Unterrichtssprache:*	deutsch
Modulnummer:	7614	*Abschluss:*	B.Sc.
Modulcode:	03-FSEOS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	7

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 digital zur Verfügung gestellt, 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.

Arbeitslast:

45 Stunden Lehrveranstaltungen
105 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Social Engineering und OSINT	0	2	0	1		Ms/90	5

7636 Der Sachverständige vor Gericht

Modulname:	**Der Sachverständige vor Gericht**	*Unterrichtssprache:*	deutsch
Modulnummer:	7636	*Abschluss:*	B.Sc.
Modulcode:	03-FDSVG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	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 und Skripte digital zur Verfügung gestellt, 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.
Arbeitslast:	**45** Stunden Lehrveranstaltungen **105** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Der Sachverständige vor Gericht	0	2	0	1		Msn/V20	5

7638 Wissenschaftliches Oberseminar/ Projektmanagement

Modulname:	**Wissenschaftliches Oberseminar/ Projektmanagement**	*Unterrichtssprache:*	deutsch
Modulnummer:	7638	*Abschluss:*	B.Sc.
Modulcode:	03-FWOPM	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	IT-Forensik/ Cybercrime	*Regelsemester:*	8

Ausbildungsziele:

Das Modul führt in die Grundlagen der schriftlichen und wissenschaftlichen Dokumentation von Forschungsergebnissen ein. Es befähigt die Studierenden mit relevanten Quellen umzugehen und im Kontext mit den eigenen Daten darzustellen. Dazu zählen auch die graphische Aufarbeitung und die Vorbereitung und Durchführung wissenschaftlicher Vorträge.

Dazu erlernen die Studierenden dem Umgang mit Literaturrecherche auf der Grundlage von Papermonitoring und Präsentationen. Gerade in der forensischen Fallarbeit und Computerforensik ist die Beschaffung von Information von grundlegender Bedeutung. Die Studierenden werden zur selbstständigen wissenschaftlichen Arbeit anhand einer umfangreichen Aufgabenstellung aus den Bereichen Forensik und IT-Sicherheit befähigt.

Lehrinhalte:

- Erarbeitung von Grundlagen in einem neuen Fachgebiet
- Veröffentlichungstypen und deren Aufbau
- wissenschaftliche Redewendungen
- Zitierweisen
- Umgang mit Dokumenten
- Software zur Textverarbeitung und Literaturverwaltung
- LaTeX
- Erstellung von Graphiken
- Grundlagen des wiss. Vortrags
- Fähigkeiten zum Wissenschaftlichen Arbeiten

Lernmethoden:

Literatur:

Arbeitslast:

75 Stunden Lehrveranstaltungen
225 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter:

03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):

Prof. Dr. rer. oec. Alexander Knauer (Dozent)
Prof. Dr. rer. pol. Ronny Bodach (Dozent, Inhaltverantwortlicher)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Wissenschaftliches Oberseminar/ Projektmanagement	2	2	0	1	T	Msn/PA	10

7632 Bachelorprojekt

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

Ausbildungsziele:

Die Bachelorarbeit kann in einem Unternehmen, einer Behörde, einer anderen Einrichtung oder auch an der Hochschule angefertigt werden.

Die Studierenden werden mit dieser abschließenden, selbständigen wissenschaftlichen Arbeit seine Berufsbefähigung für den Bereich der Allgemeinen und Digitalen Forensik nachweisen.

Dabei werden sie 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 Forschungsge-biete anzuwenden.
- Sie erkennen und formulieren Problemstellungen und können 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.

Das Bachelorprojekt schließt mit einer Bachelorarbeit im Umfang von 12

Credits und einem Kolloquium im Umfang von 3 Credits ab.

Lehrinhalte:

Interdisziplinäre und fachspezifische Mitarbeit an Industrie-, Forschungs- und 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.

Arbeitslast:

30 Stunden Lehrveranstaltungen
420 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung

Anbieter:

03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen):

Teilnahmevoraussetzungen:

155 Credits

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Bachelorprojekt	0	0	0	1			15
Bachelorarbeit						BA	
Tutorium für Examenskandidaten	0	0	0	1			
Bachelorkolloquium						Pl4sn/K30	