Open C^{3}S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

(Stand 01.01.2017)

Zertifikatsprogramm

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

FAU FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

RUHR UNIVERSITÄT BOCHUM RUB

Inhalt

1. Einführung

Das Zertifikatsprogramm ist Teil der wissenschaftlichen Fort- und Weiterbildungsinitiative Open C³S und steht für eine gezielte wissenschaftliche Weiterbildung im Bereich der Cyber-Sicherheit. Zwischen Oktober 2011 und März 2015, wurden in der ersten Phase des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts, mehr als 30 in sich abgeschlossene Studienmodule zu den Themenschwerpunkten entwickelt:

- Sicherheit
- Forensik
- Kryptografie
- Recht
- Politik und
- praktische Informatik

Die Hälfte der entwickelten Module wurde nach einer einjährigen Pilotphase in das reguläre Weiterbildungsangebot der Hochschule Albstadt-Sigmaringen aufgenommen. Eine Auswahl der Module finden Sie in unserer Jahresplanung 2016 wieder.

Die Zertifikatsmodule auf wissenschaftlichem Niveau bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung mit hohem Praxisbezug. Nach erfolgreichem Abschluss eines Moduls erhält jeder Absolvent eine Zertifikatsurkunde. Mehrere Zertifikatsmodule können zu einem spezifischen Zertifikatsstudium kumuliert werden. Nach erfolgreichem Abschluss der Module erhalten die Absolventen anschließend das Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ oder „Netzwerkforensiker/-in Open C³S“ mit ausgewiesenen ECTS-Leistungspunkten.

<u>Das Zertifikatsprogramm auf einen Blick:</u>

- Es bestehen keine formellen Zulassungsbeschränkungen.
- Die Studiendauer beträgt 8 Wochen pro Modul und schließt mit einer Prüfung ab.
- Die Module haben ein hohes wissenschaftliches Niveau mit ausgeprägtem Praxisbezug.
- In einem praktischen Teil wird unter anderem der Umgang mit Werkzeugen und Beweisgrundlagen gelernt.
- Pro Modul ist ein Workload von 150 Stunden vorgesehen, davon beträgt das Selbststudium ca. 80%.
- Der Abschluss eines Moduls wird durch Prüfungsleistungen mit ECTS-Leistungspunkten versehen.
- Gesamtzertifikat als fachliche Expertise
- Nach erfolgreichem Abschluss eines Moduls erhalten Sie eine Zertifikatsurkunde.
- Einzelmodule zum Einführungspreis von 1.490,

Das Zertifikatsprogramm wurde von der Hochschule Albstadt-Sigmaringen in Kooperation mit den folgenden Universitäten entwickelt:

Freie Universität Berlin	Goethe-Universität Frankfurt am Main
Friedrich-Alexander-Universität Erlangen	Ruhr-Universität Bochum

Die Kooperation mit den oben genannten Partnern garantiert ein hochqualifiziertes Team mit ausgesprochenen Kompetenzen im Sektor der Cyber-Sicherheit.

Für die Teilnehmer besteht zudem teilweise die Möglichkeit, ihre Prüfungsleistungen auf den Bachelor-Studiengang “IT-Sicherheit“ oder die Masterstudiengänge „IT Governance, Risk and Compliance Management“ sowie "Master Digitale Forensik" anrechnen zu lassen.

Wissenschaftliche Studienangebote wie das Zertifikatsprogramm unterstützen den Übergang von der beruflichen zur hochschulischen Bildung und qualifizieren Fachkräfte in spezifischen Themengebieten. Die Module des Programms bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung mit hohem Praxisbezug.

Das Studienprogramm ist als Fernstudium mit integriertem Blended Learning-Ansatz modular mit Studienbriefen, Präsenz- und Onlinephasen sowie Betreuung durch Online-Tutoren und Dozenten aufgebaut.

2. Modulübersicht

2.1 Curriculum 2017/2018

Ende Februar bis Mitte Mai	Ende Mai bis Ende Juli	Mitte September bis Mitte November	Mitte November bis Anfang Februar 2018
Python 1 (Z-202)* Programmierung und Forensik **HSAS**	Internettechnologien (Z-206) **HSAS**	Python 2 (Z-203)* Penetration Testing **HSAS**	Applied Computer Systems (Z-201) Rechnersysteme **HSAS**
Datenträgerforensik 1 (Z-204)* **HSAS**	Computerstrafrecht (Z-401) **GU**	Computerstrafprozessrecht (Z-402) **GU**	Netzsicherheit 3 (Z-303)* **RUB**
Netzsicherheit 1 (Z-301)* **RUB**	SPAM (Z-304) **RUB**	Netzsicherheit 2 (Z-302)* **RUB**	Reverse Engineering (Z-103)* **FAU**
Mobilfunkforensik (Z-107) **FAU**	Methoden digitaler Forensik (Z-101) **FAU**	Systemnahe Programmierung (Z-102)* **FAU**	
		Datenträgerforensik 2 (Z-205)* **HSAS**	

Alle hier gemachten Angaben verstehen sich vorbehaltlich etwaiger Änderungen.

2.2 Gesamtzertifikate

Datenträgerforensiker /-in	
Modul	**Hochschule**
Z-201 Applied Computer Systems	Hochschule Albstadt-Sigmaringen
Z-202 Python 1 – Programmieren im IT-Security-Umfeld	
Z-203 Python 2 - Programmieren im IT-Security-Umfeld	
Z-204 Datenträgerforensik 1	
Z-205 Datenträgerforensik 2	
Z-101 Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
Z-401 Computerstrafrecht	Goethe-Universität Frankfurt am Main
Netzwerkforensiker /-in	
Modul	**Hochschule**
Z-201 Applied Computer Systems	Hochschule Albstadt-Sigmaringen
Z-203 Python 2 - Programmieren im IT-Security-Umfeld	
Z-206 Internettechnologien	
Z-101 Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
Z-301 Netzsicherheit 1	Ruhr-Universität Bochum
Z-302 Netzsicherheit 2	
Z-401 Computerstrafrecht	Goethe-Universität Frankfurt am Main

Wahlmodule (jeweils ein Modul pro Bündel muss aus den zwei Wahlmodulen belegt werden)

3. Prüfungsübersicht aller angebotenen Module im ZP gemäß Studienprüfungsordnung „ZertO“

* Voraussetzung: Ha bestanden

Modulbezeichnung	Institution	Gesamt-hoch-schul-zertifikat	ECTS-Punkte	Prüfungsart	Prüfungsdauer min	Unbenotet Art
Applied Computer Systems	HSAS	DTF/NTF	5	K60*	60	Ha
Computerstrafrecht	GU	DTF/NTF	5	K60	60	
Computerstrafprozessrecht	GU		5	K60	60	
Cybercrime	FUB		5	K60	20	
Datenträgerforensik 1	HSAS	DTF	5	K60*	60	Ha
Datenträgerforensik 2	HSAS	DTF	5	K60*	60	Ha
Einführung Cyberwar	FUB		5	K60	60	
Internettechnologien	HSAS	NTF	5	K60*	60	Ha
Kryptographie 1	RUB		5	K120	120	
Kryptographie 2	RUB		5	K120	120	
Methoden digitaler Forensik	FAU	DTF/NTF	5	verpflichtende Abgabe von Prüfungsaufgaben		Ü (bestanden/ nicht bestanden)
Mobilfunkforensik	FAU		5	Ha (1,5) M (3,5)		
Netzsicherheit 1	RUB	NTF	5	K120	120	
Netzsicherheit 2	RUB	NTF	5	K120	120	
Python 1 - Programmieren im IT-Security-Umfeld	HSAS	DTF	5	K60*	60	Ha
Python 2 - Programmieren im IT-Security-Umfeld	HSAS	DTF/NTF	5	K60*	60	Ha
Reverse Engineering/Malware-Analyse	FAU		5	Ha (5)		
SPAM	RUB		5	K60	60	Ü
Systemnahe Programmierung	FAU		5	Ha (5)		
Unix-Forensik	HSAS		5	K60*	60	Ha
Windows-Forensik	HSAS		5	K60*	60	Ha

a) Allgemeine Abkürzungen:

ECTS	=	European Credit Transfer System

b) Prüfungsarten:

Kx	=	Klausur (x = Dauer in Minuten)
Mx	=	Mündliche Prüfung (x = Dauer in Minuten)
R	=	Referat
Ha	=	Hausarbeit
La	=	Laborarbeit
Pa	=	Projektarbeit
Ü	=	Übungsaufgaben

c) Institutionen:

FAU	=	Friedrich-Alexander Universität Erlangen-Nürnberg
FUB	=	Freie Universität Berlin
GU	=	Goethe-Universität Frankfurt am Main
HSAS	=	Hochschule Albstadt-Sigmaringen
RUB	=	Ruhr-Universität Bochum

d) Bezeichnung der Hochschulzertifikatsstudien (Gesamtzertifikate):

DTF	=	Datenträgerforensiker/-in Open C³S
NTF	=	Netzwerkforensiker/-in Open C³S

1 Modulbeschreibungen

1.1 Friedrich-Alexander-Universität Erlangen-Nürnberg

1.1.1 Methoden digitaler Forensik

Modulbezeichnung:	**Methoden digitaler Forensik**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in“ sowie „Netzwerkforensiker/-in“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Prof. Dr. Felix Freiling
Zeitraum:	24. Mai 2017 – 17. Juli 2017; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Sachbearbeiter im Bereich IuK-Kriminalität Mitarbeiter in IT-Beweissicherungsabteilungen der Polizei Mitarbeiter in unternehmensinternen IT-Sicherheitsabteilungen IT-Sicherheitsberater
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Projekt mit Erstellung eines forensischen Berichts (1/3), Präsentation und Ver-teidigung der Projektergebnisse (2/3)
Notwendige Voraussetzungen:	grundlegende Programmierkenntnisse in einer höheren Programmiersprache; Linux-Kenntnisse; Grundverständnis von Rechnerarchitektur
Empfohlene Voraussetzungen:	
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalt und Niveau:	• klassische (analoge) Forensik: Beispiele, Theorie der Entstehung von Spuren • Terminologie: Identifizierung, Klassifizierung, Individualisierung, Assoziation • Quantifizierung der Assoziation: Rechenbeispiele • Digitale Spuren • Kurze Einführung in die Datenträgeranalyse: Partitionssysteme (DOS, GPT) • Regeln für den Aufbau forensischer Gutachten, Qualitätskriterien für forensische Dokumentation • **Übungen:**

	• Einübung der Terminologie an Beispielen
	• Digitale Spuren und digitale Forensik: Abgrenzung und Gemeinsamkeiten
	• Programmierung von mmls (für DOS- und GPT-Partitionen). Untersuchung folgender Fragestellungen:
	  ○ Wie behandeln unterschiedliche Betriebssysteme die nicht-essentiellen Daten in der Partitionstabelle?
	  ○ Wie werden erweiterte Partitionen standardmäßig von verschiedenen Betriebssystemen angelegt?
	  ○ Wie verhalten sich Betriebssysteme bei nicht standardmäßiger Codierung von erweiterten Partitionen (z.B. Zyklen)?
	• **Projekt:** Schreiben eines forensischen Berichts zu einem individuellen Fall. Dieser basiert auf der Frage, ob Manipulationen in einem gegebenen Partitionssystem vorliegen.
	• **Präsenzphase:** Vorstellung und Verteidigung des Berichts in einer mündlichen Prüfung (Rollenspiel)
	
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).

Angestrebte Lernergebnisse:	• Die Teilnehmer beherrschen die terminologischen Grundlagen der digitalen Forensik und können Beziehungen zwischen Konzepten der klassischen Forensik und der digitalen Forensik herstellen • Die Teilnehmer haben ein einfaches Werkzeug zur Analyse von Partitionstabellen erstellt und dadurch ein Verständnis für die Komplexität forensischer Software entwickelt • Die Teilnehmer können forensische Gutachten aufgrund von allgemeinen Qualitätskriterien bewerten
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung, Präsentation und Verteidigung der Projektergebnisse Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	• Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005. • Eoghan Casey: Digital Evidence and Computer Crime: Forensic Sci-ence, Computers, and the Internet. Academic Press, 2. Auflage, 2004. • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2011. • Alexander Geschonneck: Computer Forensik. dpunkt Verlag, 5. Auf-lage, 2011. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.1.2 Systemnahe Programmierung

Modulbezeichnung:	**Systemnahe Programmierung**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Dr. Werner Massonne
Zeitraum:	6. September 2017 – 26. November 2017; Dauer ca. 3 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen, die ein solides Basisverständnis im Bereich der systemnahen Programmierung (Assembler und C) benötigen; Angehende Programm- und Malware-Analysten/-innen, die mit Mitteln des Reverse Engineering Schadsoftware verstehen wollen (Vorbereitungsmodul für das Modul „Reverse Engineering / Malware-Analyse“). Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Cyber-Sicherheit weiterbilden möchten.
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Hausarbeit
Notwendige Voraussetzungen:	Allgemeine Programmierkenntnisse (beliebige Programmiersprache), Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII)
Empfohlene Voraussetzungen:	
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	80	Zeitstunden
davon Aufgaben und Hausarbeit:	50	Zeitstunden
davon Online-Betreuung:	5	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	10	% = Präsenz

Lerninhalt und Niveau:	• Grundlagen Rechnerarchitektur und Assembler-Programmierung
	  ○ Von-Neumann-Architektur
	  ○ Allgemeine Prinzipien der Assemblerprogrammierung
	• Grundlagen Betriebssysteme
	  ○ Grundbegriffe
	  ○ Prozesse, Threads, Datenstrukturen
	  ○ Adressräume
	  ○ Programmierschnittstellen (API)
	• Intel x86-IA-32-Architektur und IA-32-Assembler
	(Starke Vertiefung der allgemeinen Grundlagen)
	  ○ Architekturmerkmale
	  ○ Registersatz
	  ○ Befehlssatz
	  ○ Adressierung
	  ○ Stack und Unterprogramm-Aufrufkonventionen
	  ○ Speicherverwaltung
	  ○ Befehlsformat
	  ○ Begleitende Übungen
	• Die Programmiersprache C
	  ○ Datentypen, Operatoren und Ausdrücke
	  ○ Kontrollstrukturen
	  ○ Funktionen, Gültigkeitsbereiche und Präprozessor
	  ○ Zeiger und Felder
	  ○ Strukturen und Verbunde
	  ○ Standardbibliothek
	  ○ Inline-Assembler
	  ○ Begleitende Übungen
	• Softwaresicherheit
	  ○ Buffer Overflows
	  ○ Gegenmaßnahmen zur Vermeidung von Buffer Overflows
	  ○ Gegen-Gegenmaßnahmen (z.B. Return Oriented Programming)
	• Sortieralgorithmen und Sortierbäume als Programmierprojekt
	  ○ Einführung und Übersicht über Sortierverfahren
	  ○ Einführung Sortier- und Suchbäume
	  ○ Programmierprojekt in Assembler und C als Hausarbeit
	• Präsenzwochenende
	  ○ Vorlesung
	  ○ Programmierübungen
	  ○ Vorbereitung auf die Hausarbeit
	
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)

Angestrebte Lernergebnisse:	Die Studierenden kennen die Einsatzszenarien der systemnahen Programmierung, und ihre Prinzipien und Methoden sind ihnen bekannt. Sie können die Grundprinzipien aktueller Rechnerarchitekturen und Betriebssysteme benennen und einordnen. Die Intel IA-32-Architektur ist ihnen im Detail vertraut. Sie sind in der Lage, Assemblerprogramme für diese Architektur zu schreiben und zu verstehen. Ebenso sind sie in der Lage, Programme in der höheren, systemnahen Programmiersprache C zu verfassen. Den Studierenden sind die Stärken, aber auch die Schwächen - bzgl. Softwaresicherheit - der Programmiersprache C bekannt. Einige der bedeutendsten Sicherheitsprobleme/Sicherheitslücken, die insbesondere durch die Verwendung von C auf heutigen Rechnerarchitekturen entstehen können, können Sie erklären. Des Weiteren können Sie übliche Gegenmaßnahmen beschreiben, die die Ausnutzung von Sicherheitslücken unterbinden sollen. Durch eigenständiges Programmieren sind sie in der Lage, Programmierprojekte in C und Assembler umzusetzen und den Sinn sowie die Notwendigkeit effizienter Algorithmen und Datenstrukturen zu erkennen. Die Absolventen haben fundierte Grundkenntnisse erworben, die erforderlich sind, um Maschinenprogrammanalysen zum Reverse Engineering durchzuführen.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	• Kip R. Irvine: *Assembly Language for Intel-based Computer,* Prentice Hall, 2010. • Brian W. Kernighan and Dennis M. Ritchie: *Programmieren in C*, Hanser Fachbuch, 1990. • Th. H Cormen, C.E. Leiserson, R. Rivest, C. Stein, P. Molitor: *Algorithmen - Eine Einführung*, Oldenbourg Wissenschaftsverlag 2004. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.1.3 Reverse Engineering / Malware-Analyse

Modulbezeichnung:	**Reverse Engineering / Malware-Analyse**
Zertifikatsabschluss:	
Verwendbarkeit:	
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Dr. Werner Massonne
Zeitraum:	22. November 2017 – 28. Februar 2018; Dauer ca. 4 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten, die bereits tiefgehende Kenntnisse im Bereich systemnaher Programmierung und Assemblerprogrammierung (IA-32) besitzen. Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Cyber-Sicherheit weiterbilden möchten.
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Hausarbeit
Notwendige Voraussetzungen:	Grundverständnis von Betriebssystemen und Rechnerarchitektur, Programmierkenntnisse insbesondere in C, detaillierte Kenntnisse in Intel IA-32-Assembler
Empfohlene Voraussetzungen:	Modul „Systemnahe Programmierung“
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	80	Zeitstunden
davon Aufgaben und Hausarbeit:	50	Zeitstunden
davon Online-Betreuung:	5	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	10	% = Präsenz

Lerninhalt und Niveau:	• Einführung in Reverse Engineering
	  ○ Abgrenzung des Begriffs Reverse Engineering
	  ○ Einsatzgebiete
	  ○ Zielsetzung und Grenzen von Reverse Engineering
	• Microsoft Windows
	  ○ Aufbau und Struktur
	  ○ Anwendungen und Bibliotheken, API-Programmierung
	  ○ Detaillierte Betrachtung der PE-Struktur zur Programmanalyse: Importe, Exporte, Sections, Windows-Loader, Datenstrukturen
	  ○ Prozesse, Threads und ihre Datenstrukturen
	  ○ Exceptions und Exception-Behandlung
	• Programmanalyse
	  ○ Codeerzeugung durch Compiler und Dekompilierung
	  ○ Optimierungsverfahren
	  ○ Kontroll- und Datenflussanalyse
	• Werkzeuge zur Programmanalyse: IDA und OllyDbg
	  ○ Statische Analyse
	  ○ Dynamische Analyse
	  ○ Übungen: Analyse einfacher Binaries, einfaches Debugging/Cracking, Sicherheitsprüfungen aushebeln
	• Malware und Malware-Analyse
	  ○ Obfuscation
	  ○ Verhinderung von Disassemblierung
	  ○ Malware-Techniken, Packer, Anti-Reverse-Engineering-Methoden
	  ○ Analyse realer Malware in einer virtuellen Analyseumgebung
	  ○ Übungen: Malware-Analyse mit IDA und OllyDbg
	• **Präsenzwochenende:** Vorlesung, Übungen in Gruppen: Analyse verschleierter Binaries, Analyse von Malware, Vorbereitung auf die Hausarbeit
	
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master)

Angestrebte Lernergebnisse:	Die Studierenden können den Begriff „Reverse Engineering“ einordnen und definieren. Sie können die typischen Einsatzgebiete von Reverse Engineering benennen. Die Strukturen von Microsoft Windows sind ihnen bekannt. Den Aufbau von Programmdateien in Windows können sie beschreiben und analysieren. Sie können die Methoden zur Dekompilierung von Maschinenprogrammen benennen und anwenden. Verschiedene Optimierungsverfahren der Compiler, die eine Dekompilierung erschweren, können sie erkennen und benennen. Die üblichsten Werkzeuge zur Programmanalyse können die Absolventen einsetzen, Vorteile und Nachteile einer statischen und dynamischen Programmanalyse sind ihnen bekannt, und sie können diese bedarfsabhängig einsetzen. Sie haben detaillierte Kenntnisse über Malware sowie verschiedene Methoden und Tricks der Malware-Autoren. Die Absolventen können „einfache“ Malware für Windows-Systeme selbstständig analysieren. Sie beherrschen die Grundlagen für eine Vertiefung des weiten Gebietes der Malware-Analyse.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	• Eldad Eilam: *Reversing: Secrets of Reverse Engineering*, John Wiley & Sons, 2005 • Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.1.4 Mobilfunkforensik

Modulbezeichnung:	**Mobilfunkforensik**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. Michael Spreitzenbarth
Dozent(in):	Dr. Michael Spreitzenbarth
Zeitraum:	22. Februar 2017 – 24. April 2017; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Projekt mit Erstellung eines forensischen Berichts (1/3), Präsentation und Verteidigung der Projektergebnisse (2/3)
Notwendige Voraussetzungen:	Programmierkenntnisse in Python, gute Linux-Kenntnisse, Englischkenntnisse
Empfohlene Voraussetzungen:	Programmierkenntnisse in Java
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	80	Zeitstunden
davon Aufgaben:	50	Zeitstunden
davon Online-Betreuung:	5	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	10	% = Präsenz

Lerninhalt und Niveau:

1. Einführung in Android
   - Aufbau des Android Systems
   - Unterschiede zwischen der Java VM und der Dalvik VM
   - Das Android SDK

2. Einführung in Mobilfunkforenisk für Android
   - Wie kommt man an die wichtigen Daten
   - Rooting, Recovery und andere Zugriffsstrategien
   - Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie
   - Einführung in SQLite
   - Einführung in Volatility für Android
   - Beispiel: Manuelle Analyse der Datenbanken der Adressbuch Applikation
   - Beispiel: Manuelle Analyse der Speicherinhalte der Facebook Applikation mit Hilfe von Volatility

- Das Mobilfunkforensik-Framework ADEL
- Aufgabe I: Forensische Analyse einer Applikation (RAM und lokaler Speicher)
- Aufgabe II: Entwicklung eines Plugins für ADEL

3. Aufbau von Android Applikationen
   - Bestandteile einer Android Applikation (Manifest, Dalvik-Bytecode, Zertifikate, native Bibliotheken, usw...)

4. Analyse von Android Applikationen
   - Einführung in das Decompilieren und Reversen von Android Applikationen
   - Automatisierte Analysetechniken: Überblick, Einführung und Diskussion statische vs. dynamische Analyse
   - Einführung in die Tools smali, dex2jar und JD-GUI
   - Beispiel: Manuelle Analyse einer einfachen Android Malware mit Hilfe von dex2jar und JD-GUI
   - Einführung in die Tools Androguard, Droidlyzer und DroidBox
   - Beispiel: Analyse einer komplexeren Android Malware mit Hilfe von Droidlyzer und DroidBox
   - Exkurs: Die Mobile-Sandbox
   - Aufgabe I: Analyse einer komplexeren Android Malware mit Hilfe der zuvor vorgestellten Tools und Systemen

5. Schreiben von Android Apps
   - Aufbau und das Android-Manifest
   - Einführung in Rechte und Intents
   - Code-Beispiele und einfache Beispiel-Applikationen

6. Obfuscation
   - Einführung in Obfuscation
   - Verschleierung von Variablen-/Funktionsnamen
   - String-Obfuscation (XOR, Crypt, ...)
   - Junkbytes zum Verwirren der Disassembler
   - XOR von Code nicht so einfach machbar ==> JNI benutzen
   - Collusion mehrerer Apps zum Verschleiern der Schadfunktion
   - Aufgabe I: Schreiben einer einfachen obfuskierten Applikation
   - Aufgabe II: Analyse einer obfuskierten Applikation

Projekt:
- Im Rahmen des Projekts soll eine vollständige forensische Analyse eines Mobiltelefons durchgeführt werden. Dabei sollen sowohl die installierten Applikationen selbst als auch ihre verwendeten Datenstrukturen analysiert werden. Die durchgeführte Untersuchung soll in einem möglichst gerichtsverwertbaren Bericht zusammengefasst werden.

Präsenzphase:
- Präsentation und Verteidigung der Projektergebnisse

Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7

(Master)

Angestrebte Lernergebnisse:	Der Aufbau und die Funktionsweise von Android und Android-Applikationen ist den Studierenden bekannt. Die grundlegenden Methoden zur Vorbereitung einer forensischen Analyse von Android Mobiltelefonen sind Ihnen geläufig. Sie können unterschiedliche Verfahren und Werkzeuge zur Analyse benennen und anwenden. Die Studierenden können einfache Applikationen für Android programmieren. Sie gewinnen Kenntnisse zur Analyse von Android Applikationen. Die sicherheitskritische Betrachtung von Android Applikationen ist Ihnen vertraut. Die Absolventen können eine forensische Analyse von Mobiltelefonen auf der Basis von Android durchführen.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung, Präsentation und Verteidigung der Projektergebnisse Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Die Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2 Hochschule Albstadt-Sigmaringen

1.2.1 Applied Computer Systems

Modulbezeichnung:	**Applied Computer Systems**
Zertifikatsabschluss:	Hochschulzertifikat mit 5 ECTS-Punkten
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in“ sowie „Netzwerkforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	22. November 2017 – 3. Februar 2018; Dauer ca. 3 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit geringen IT-Kenntnissen
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	keine
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS		

Lerninhalt und Niveau:	In diesem Modul werden die technischen Kenntnisse vermittelt, die ein IT-Sicherheitsexperte braucht, um ein Rechnersystem und Angriffsmöglichkeiten darauf verstehen zu können. Schwerpunkt des Moduls ist die IT-Sicherheit, wobei die vorangeführten Studienbriefe zu der Thematik hinführen und das Grundwissen hierfür vermitteln. Die atomare Betrachtung eines digitalen Rechnersystems wird durch Algorithmen und Software weiter abstrahiert und findet schließlich in den Internettechnologien ihre Anwendung. Diese drei Themenfelder legen den Grundstein für das Verständnis der IT-Sicherheit. 1. Digitale Rechnersysteme EVA-Prinzip, Von Neumann-Architektur, Bits und Bytes, Zahlensysteme, Byte-Reihenfolge, Zeichenkodierung, Digitale Logik, Hardware-Komponenten 2. Algorithmen und Software Rechenmaschinen, Digitalrechner, Programmiersprachen, Compiler vs. Interpreter, Algorithmen, UML, Variablen, Kontrollstrukturen, Komplexität von Software, Bubblesort, Zusammenspiel von Hard- und Software, Softwarearten, Betriebssysteme 3. Internettechnologien ISO/OSI-7-Schichtenmodell, TCP/IP-Referenzmodell 4. IT-Sicherheit Hackerparagraph, Schutzziele, Angriffstypen, spezielle Bedrohungen, Angriffsszenario im WWW, Sniffer, Klartext vs. Verschlüsselung Die Inhalte des Moduls werden in einer Linux-Umgebung angewendet und somit auch der Umgang mit unixoiden Betriebssystemen vermittelt. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Die Studierenden haben Kenntnisse über Instrumente und Methoden der Informatik. Sie haben insbesondere grundlegende Kenntnisse in der praktischen, technischen und theoretischen Informatik. Sie können Darstellungsformen und -formaten von Informationen in Rechnern interpretieren und umwandeln. Die Grundzüge von Rechnern und die Aufgaben unterschiedlicher Software können erläutert werden. Grundlegende Kennt-nisse der IT-Sicherheit wurden erworben. Die möglichen Angriffsarten auf ein IT-System können durch die Studierenden erläutert werden und damit eine fundamentale Bewertung der IT-Infrastruktur getroffen werden. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine

Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und -Korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen
Literatur:	• Gumm, H.-P.(2011): Einführung in die Informatik. München; Wien: Oldenbourg. • Herold, H; Lurz, B; Wohlrab, J. (2007): Grundlagen der Informatik. München ; Boston {[u.a.] : Pearson Studium. • Tanenbaum, A. S. (2006): Computerarchitektur : Strukturen - Konzepte – Grundlagen. München ; [Boston {u.a.] : Pearson Studium • Schiffmann , W., Bähring H., Hönig, U. : Technische Informatik 3 (2011): Grundlagen der PC-Technologie; Berlin: Springer-Lehrbuch. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.2 Python 1 – Programmieren im IT-Security-Umfeld

Modulbezeichnung:	**Python 1 – Programmieren im IT-Security-Umfeld**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	22. Februar 2017 – 13. Mai 2017; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit grundlegenden IT-Kenntnissen, keine bis geringe Programmierkenntnisse
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Programmierkenntnisse
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	In diesem Modul werden die Kenntnisse in Informatik und Programmieren vermittelt, die ein IT-Sicherheitsexperte braucht, um für ein Rechnersystem spezifische Programme zur Analyse des IT-Sicherheitsstands vornehmen zu können sowie um sicherheitsrelevante Vorgängen überprüfen zu können. Damit ist auch die Grundlage für einen guten Einstieg zum Erlernen weiterer Programmiersprachen gelegt. 1. Einführung in Python Syntax und Semantik, Programmierparadigmen, Installation, Interaktiver Modus, Objektorientiertes Programmieren , Funktionen, Methoden, Standard-

	Datentypen, Erstellen von Skriptdateien, Kontrollstrukturen, Definition eigener Klassen, guter Programmierstil **Praktische Übung:** Erstellen eines Programms, welches Dateien sucht und diese anhand des Dateityps kategorisch sortiert. In einer Textdatei werden die Informationen über die Dateien festgehalten. 2. Forensische Analyse mit Python: Datenbanken und Anwendungen, Grundlagen Datenbanken, SQL-Syntax, sqlite3-Modul in Python, Untersuchen von Anwendungs-Artefakten an den Beispielen Skype, Firefox und Chrome **Praktische Übung:** Ergänzung und Optimierung der praktischen Übung aus SB1, Textdateien durch Datenbankeinträge ersetzen, Suchanfragen über sqlite3 realisieren; Extraktion von Anwendungsdaten aus Skype und Firefox 3. Forensische Analyse mit Python: Windows Auslesen der Windows-Registry bei einem Live-System, Analyse der Hive-Dateien (Post Mortem), Entschlüsselung von WLAN-Kennwörtern, Wiederherstellung von gelöschten Daten, Analyse von Metadaten **Praktische Übung:** String-Suche in Hive-Dateien, Wiederherstellung von WLAN-Passwörtern, Metadaten von Bildern auswerten **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Die Studierenden können aus einer abstrakten Aufgabenstellung ein ablauffähiges Programm entwickeln. Wenn die Programmierung konkret wird, so findet die Programmiersprache Python Verwendung. Python ist eine leistungsfähige Skriptsprache, die im Forensikumfeld häufig verwendet wird. Die Grundkonstrukte von Programmen und deren Umsetzung in Python wurde erlernt. Die Studierenden haben erste Erfahrungen mit programmbasierten Sicherheitsschwachstellen und verstehen einfache Angriffsmechanismen. Die Studierenden können mit den selbst erstellten Programmen häufig in der Praxis vorkommende Aufgabenstellungen bewältigen wie z. B. das Durchsuchen eines Rechners nach auffälligen Bildern (Zuwachs an Methodenkompetenz). Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen

Literatur:	• Ernesti, Johannes ; Kaiser, Peter (2012): Python 3 : Das umfassende Handbuch. 3. Aufl.. Bonn: Galileo Press GmbH. • Weigend, Michael (2009): OOP mit Python 3; PR. 4. Aufl. München: Hüthig Jehle Rehm. • O'Connor, TJ (2012): Violent Python. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. London (Newnes). Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.3 Python 2 – Programmieren im IT-Securtiy-Umfeld

Modulbezeichnung:	**Python 2 – Programmieren im IT-Security-Umfeld**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	6. September 2017 – 4. November 2017; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit grundlegenden IT-Kenntnissen, keine bis geringe Programmierkenntnisse
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Python 1 – Programmierung im IT-Security-Umfeld oder fortgeschrittene Programmierkenntnisse
Empfohlene Voraussetzungen:	Kenntnisse über Netzwerkprotokolle und Internettechnologien
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:

In diesem Modul werden die Kenntnisse vertieft, die ein IT-Sicherheitsexperte benötigt, um den Datenverkehr im Netzwerk zu analysieren oder Schwachstellen durch gezielte Manipulationen aufzudecken. Durch das Aufzeigen von antiforensischen Maßnahmen und das Realisieren von Angriffsszenarien tritt zudem eine Sensibilisierung für das Thema IT-Sicherheit ein.

1. Netzwerkforensik mit Python
   Physikalischer Standort von IP-Adressen ermitteln und visualisieren, Datenpakete und pcap-Dateien parsen, Sniffing
   Praktische Übung:
   String-Suche in Datenpaketen und pcap-Dateien

	2. Penetrationstest mit Python Internet Wide Scans, Port Scanning, FTP Scanner, SSH-Angriff, DDoS-Angriff, Paket-Injection, Session Hijacking **Praktische Übung:** Angreifen eines SSH Honey Pots, Shellshock 3. Python-Hacks Erstellen eines Proxys, Proxy-Test-Bot, Python-gestützte E-Mail-Kommunikation, Python-gestütztes Webbrowsing, Implementierung von Ransomware **Praktische Übung:** SMTP-Server angreifen und für das Versenden von Spam-Mail missbrauchen. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Die Studierenden können aus einer abstrakten Aufgabenstellung ein ablauffähiges Programm entwickeln. Wenn die Programmierung konkret wird, so findet die Programmiersprache Python Verwendung. Python ist eine leistungsfähige Skriptsprache, die im Forensik- und Pentest-Umfeld häufig verwendet wird. Vertiefte Kenntnisse in dem Umgang mit Python wurden erlernt, wobei die Anwendung von Python-Modulen den Umgang mit externen Bibliotheken gefestigt und die Programmierfähigkeiten verbessert wurden. Die Studierenden können Netzwerkprotokolle analysieren und deren Inhalt aufschlüsseln. Das Implementieren von Penetrationstests hat das Verständnis über Angriffe auf IT-Strukturen erweitert und ermöglicht das Aufdecken von Schwachstellen. Die Implementierung und Anwendung von Proxy-Diensten sowie die Fertigkeit des Python-gestützten Mailens und Browsens runden das Wissensspektrum der IT-Sicherheitsexperten ab. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen
Literatur:	• Ernesti, Johannes ; Kaiser, Peter (2012): Python 3 : Das um-fassende Handbuch. 3. Aufl.. Bonn: Galileo Press GmbH. • Weigend, Michael (2009): OOP mit Python 3; PR. 4. Aufl. München: Hüthig Jehle Rehm. • O'Connor, TJ (2012): Violent Python. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. London (Newnes). Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.4 Datenträgerforensik 1

Modulbezeichnung	**Datenträgerforensik 1**
Zertifikatabschluss	Hochschulzertifikat
Verwendbarkeit	Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r)	Prof. Dr. Martin Rieger
Dozent(in)	Prof. Dr. Martin Rieger
Zeitraum	22. Februar 2017 – 13. Mai 2017; Dauer ca. 8 Wochen
Leistungspunkte	5 ECTS-Punkte
Zielgruppe	Personen mit fortgeschrittenen IT-Kenntnissen
Min.-max. Teilnehmerzahl	12 bis 30
Studien- und Prüfungsleistungen	Klausur, Hausarbeit
Notwendige Voraussetzungen	Keine
Empfohlene Voraussetzungen	Keine
Sprache	Deutsch
Arbeitsaufwand bzw. Gesamtworkload	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau	In diesem Modul gehen wir auf die forensische Untersuchung von sogenannten Massenspeichern (engl. mass storages) ein. Massenspeicher sind Peripheriegeräte, die zur Speicherung großer Datenmengen dienen, wobei als Speichermedium meist magnetische oder optische Träger sowie neuerdings Flash-Speicherbausteine eingesetzt werden. Massenspeicher sind für forensische Untersuchungen von großer Bedeutung, da sie oft einschlägige Informationen enthalten und zudem Rückschlüsse auf Benutzer, Besitzer und Zugriffe ermöglichen. In dem ersten Modul von Datenträgerforensik werden grundlegende Konzepte vermittelt und erste praktische Übungen ohne Fokus auf ein Dateisystem durchgeführt. **1. Einführung, Festplattentechnik, Festplatten kopieren** • Technik klassischer Festplatten (Aufbau, Adressierung) • Technik von Halbleiterspeichern (USB-Medien, Speicherkarten, geräteinterne Speicher mit USB Zugriff) • Wear-Leveling • Systematik zum Sichern von Speichermedien, Datensicherung einer Festplatte, Computerforensik-Programme • **Praktische Übung:** Kopieren von Festplatten mit HPA, Datenträgerkopieren **2. Datenträgeranalyse** • Master Boot Record • Partitionstabellen • Adressierung von Sektoren • Globally Unique Identifier • The Sleuth Kit und Autopsy • Praktische Übung: Arbeiten mit The Sleuth Kit und Autopsy **3. Analyse von Dateisystemen** • Grundlagen • Ansatz der Kategorisierung der Daten, Kategorien • Praktische Übung: Arbeiten mit X-Ways und EnCase **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls hat der Studierende grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann verschiedene Werkzeuge zur Analyse und Wiederherstellung von Dateien auf Datenträgern einsetzen und verfügt über grundlegende Kenntnisse, die in dem zweiten Modul „Datenträgerforensik“ weiter ausgebaut werden können. Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz.

Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	Keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Onlinevorlesung über Web-Konferenzen
Literatur:	• Carrier, Brian: File system forensic analysis. Amsterdam: Addison-Wesley, 2005. • Geschonneck, Alexander: Computer-Forensik. 5. aktualis. A. Köln: Dpunkt-Verlag, 2011. • Bunting, Steve: EnCase Computer Forensics – The Official EnCE: EnCase Certified Examiner Study Guide. Johny Wiley & Sons, 2012. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.5 Datenträgerforensik 2

Modulbezeichnung:	**Datenträgerforensik 2**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	6. September 2017 – 4. November 2017; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit fortgeschrittenen IT-Kenntnissen
Min.-max. Teilnehmerzahl	12 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Keine
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	In diesem Modul werden die Dateisysteme FAT, ExtX und NTFS näher betrachtet. Dieses Modul stellt somit die ideale Ergänzung zu Datenträgerforensik 1 dar und vertieft die Grundlagen, die in dem vorangeführten Modul behandelt wurden. Die einzelnen Studienbriefe sind in sich geschlossen und auch die praktischen Übungen sind auf die einzelnen Dateisysteme speziell abgestimmt. **1. FAT-Dateisysteme:** • Überblick und Vergleich der unterschiedlichen FAT-Dateisysteme (FAT12/16/32) • Bedeutung, Verbreitung und Kompatibilität des FAT-Dateisystems • Allgemeines Partitionsschema des FAT-Dateisystems (MBR, VBR, FAT, Root-Verzeichnis und Datenbereich) • Funktionsweise der File Allocation Table • Aufbau und Organisation von Datei- und Verzeichniseinträgen • VFAT, Dienstprogramme im Zusammenhand mit dem FAT-Dateisystem (z. B. format.exe, attrib.exe und die Windows Datenträgerverwaltung) • **Praktische Übung:** Beispielhafte Einrichtung eines FAT-Dateisystems; Analyse mit Autopsy: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen. **2. NTFS-Dateisystem:** • Allgemeine Informationen über das NTFS-Dateisystem (Einführung eines Berechtigungskonzeptes und die Möglichkeit von Mountpoints und Quotas) • Allgemeiner Aufbau von NTFS-Basisdatenträgern (MBR, VBR, MFT) • Aufbau und Funktionsweise der Master File Table sowie deren Record-Einträge (residente und nicht-residente Dateien und Data Runs) • Weitere wichtige Metadaten (Logfile für das Transaction Logging usw.) • Verzeichnisse • Weitere Features des NTFS-Dateisystems (z. B. Kompression, Verschlüsselung und Alternative Datenströme) • Dienstprogramme in Zusammenhang mit dem NTFS-Dateisystem (DiskPart.exe, fsutil.exe und die Windows Datenträgerverwaltung) • **Praktische Übung:** Beispielhafte Einrichtung eines NTFS-Dateisystems; Analyse mit X-Ways, EnCase: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen.

Lerninhalte und Niveau	**3. Linux/Unix Extended Dateisysteme (Ext3)** • Linux-Bootprozess unter der Verwendung der Bootloader LiLo und GRUB: Virtuelles Dateisystem bei Linux-Betriebssystemen • Allgemeiner Überblich über die Linux-Dateistruktur und das Ext3-Dateisystem • Struktur einer Ext3-Partition (Blöcke und Blockgruppen) • Aufbau und Bedeutung des Superblocks und der Gruppendeskriptoren sowie der Bitmap-Tabellen • Aufbau und Funktion von Inodes bzw. Inode-Tabelle (z. B. Pointer und Zugriffsrechte) • Verwaltung von Verzeichnissen beim Ext3-Dateisystem • Linux-Befehle und Dateien in Zusammenhang mit dem Ext2-Dateisystem (z. B. fdisk, mkfs, dump2fs, fsck und /etc/fstab) • Allgemeine Beschreibung der Funktionsweise von Journaling-Dateisystem sowie deren Vorteile, Beschreibung des Journaling • **Praktische Übung:** Beispielhafte Einrichtung eines Ext4-Dateisystems; Analyse mit The Sleuth Kit, X-Ways: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls hat der Studierende einen Überblick über die verbreitetsten Datei- und Betriebssysteme sowie deren Funktionsweisen. Er hat grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern sowie gängiger Dateisysteme der Windows-Betriebssystemfamilie und bei den Unix-Derivaten. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann mit verschiedenen Werkzeugen zur Analyse und Wiederherstellung von Dateien auf Datenträgern umgehen und verfügt sowohl über analytische als auch methodische Fähigkeiten im Umgang mit diesen. Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	Keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und -korrektur in elektronischer Form, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen

Literatur:	• Carrier, Brian: File system forensic analysis. Amsterdam: Addison-Wesley, 2005. • Geschonneck, Alexander: Computer-Forensik. 5. aktualis. A. Köln: Dpunkt-Verlag, 2011. • Bunting, Steve: EnCase Computer Forensics - The Official EnCE : EnCase Certified Examiner Study Guide: John Wiley & Sons, 2012. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.6 Betriebssystemforensik (Windows-Forensik)

Modulbezeichnung:	**Windows-Forensik**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Nächster Angebotszeitraum: geplant ab Anfang 2016
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne Informatik-Ausbildung
min.-max. Teilnehmerzahl:	20 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Kenntnisse im Umgang mit Rechnern, dem Internet und dem Windows-Betriebssystem
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 Leistungspunk nach ECTS		

Lerninhalt und Niveau:	• Das Windows-Rechnersystem: Grundlegende Konzepte und Begriffe, Windows-„Bordwerkzeuge“ (Untersuchung von Prozessen und Threads, Leistungsüberwachung), System-Architektur (Gerätetreiber, Systemprozesse, Kernel, HAL), Sicherheitskomponenten, Reguläre Ausdrücke, Ermitteln der eigenen IP-/MAC-Adresse, Grundlagen Netzwerktechnik • Struktur und Analyse von Windows-Systemen: Schlüsselwortsuche, Filecarving, Schlupfspeicher extrahieren, indizieren von Metadaten, Speicherabbilder, Protokolldateien, Hashing, Zugriffsrechte, forensisch relevante Verzeichnisse und Dateien, Schattenkopien • Erkenntnisse aus der Registry: Aufbau, SIDs, SAMs, GUIDs, forensisch relevante Registry-Einträge, Werkzeuge zur Registry-Analyse • Logfile-Analyse: NTFS-Journal-Protokollierung, Struktur der Logging-Einträge, Auswertung, Windows-Event-Log, Anwendungs- und Dienstprotokolle, Security-Log, Setup-Log, Überwachungsrichtlinien • Forensische Untersuchung von Internetdiensten: Peer-to-Peer-Aktivitäten aufdecken, IP-Adresse von Skype-Accounts ermitteln, Datenbanksystem, SQLite-Andwendungs-Artefakte auswerten (Skype, Firefox, Chrome), Microsoft-Anwendungs-Artefakte auswerten (Internet Explorer, Outlook) • Forensische Analyse von Arbeitsspeicher und Windows-Artefakten: Flüchtige Informationen, Systemzeit auslesen, eingeloggte Benutzer, offene Dateien, Netzwerkverbindungen, Prozessinformationen, Zwischenablage, Dienste/Treiber-Informationen, Erstellung eines Arbeitsspeicherabbilds, Arbeitsspeicheranalyse mit dem Volatility-Framework, Artefakt-analyse **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die Möglichkeiten, die forensische Analyse eines Windows-Rechners bietet. Er kennt für die Forensik relevante Dateien und Verzeichnisse des Windows-Betriebssystems und kann diese auswerten und über gefundene Ergebnisse berichten. Dabei erstreckt sich die Analyse auf Post-Mortem-Analyse, Live-Systeme und Arbeitsspeicherabbilder. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übungen Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Onlinevorlesung über Web-Konferenzen
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.2.7 Internettechnologien

Modulbezeichnung:	Internettechnologien
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in“ sowie „Netzwerkforensiker/-in“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	24. Mai 2017 – 22. Juli 2017, Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne Informatik-Ausbildung
min.-max. Teilnehmerzahl:	20 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Grundkenntnisse im Umgang mit Rechnern und dem Internet
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	• Netzwerktechnik: Topologien und Kommunikationsarten; Überblick zu TCP-/IP-Schichten (Ethernet, WLAN, IPv4, IPv6); Routing (DNS, Ports, VPN, Proxy, Firewall); Infrastruktur (Netze, Dienstleister, Komponenten, Geräte). • Das Internet: Entstehung und Überblick, Organisationen und Verwaltung, Entwicklungen. • Internetdienste: Datenaustauschdienste (FTP, Peer-to-Peer), Zugriffsdienste (Telnet, SSH), E-Mail (Struktur, Clients, SMTP, POP, Signatur, Verschlüsselung, Sicherheit), Kommunikationsdienste (Chat, Internettelefonie, Skype). • World Wide Web: Technik für die Kommunikation (HTTP, Cookie, Verschlüsselung); Technik für den Betrieb einer Website (HTML5, CSS, JavaScript). • Web Applications Security: Sicherheitslücken, Angriffe, aktuelle Vorfälle, Analysemethoden, Demo-Plattform. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die grundlegenden Strukturen und möglichen Transportwege der Informationen im weltweiten Netz. Der Teilnehmer/die Teilnehmerin kann die für den Betrieb des Internets erforderliche Hard- und Software benennen und deren Bedeutung für die IT-Sicherheit beurteilen. Er/Sie kann Eigenschaften verbreiteter Internetdienste erklären. Darüber hinaus können die Teilnehmenden Technologien einsetzen, mit denen Web Applications erstellt werden und die zugehörigen Sicherheitskriterien einordnen. Techniken und Tools zur Analyse der Sicherheit können die Studierenden sowohl bewerten als auch aktiv einsetzen. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übungen Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Onlinevorlesung über Web-Konferenzen
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.3 Ruhr-Universität Bochum

1.3.1 Netzsicherheit 1

Modulbezeichnung:	**Netzsicherheit 1**
Zertifikatsabschluss:	Hochschulzertifikat mit 5 ECTS-Punkten
Verwendbarkeit:	Gesamtzertifikat Netzwerkforensiker/-in Open C³S
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Dozent(in):	Prof. Dr. Jörg Schwenk
Zeitraum:	22. Februar 2017 – 13. Mai 2017; Dauer ca. 2 Monate
Leistungspunkte	5 ECTS
Zielgruppe:	
min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistungen:	Klausur
Notwendige Voraussetzungen:	Grundlegende bis weiterreichende Mathematikkenntnisse; Grundlagen der Mathematik für Informatiker
Empfohlene Voraussetzungen:	keine
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	2	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	2	Zeitstunden
Fernstudienanteil:	148	Zeitstunden
davon Selbststudium:	108	Zeitstunden
davon Aufgaben:	30	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	1	% = Präsenz

Lerninhalt und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der ersten und zweiten Ebene des OSI- Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Einführung in lokale Netze und IP • WLAN (IEEE 802.11) • VPN (IPSec, PPTP, IP Multicast) • Mobilfunk (GSM, UMTS)

	Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls erkennen die Studierenden/Teilnehmer die wichtigen Strukturen von Sicherheits-mechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Sie können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, die sie auf neue Protokolle und Verfahren übertragen werden können. Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Sie haben die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten haben ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten entwickelt.
Lehrveranstaltungen und Lehrformen:	Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und -korrektur in elektronischer Form,
Literatur:	• Jörg Schwenk (2005), Sicherheit und Kryptographie im Internet. • Christof Paar, Jan Pelzl (2010), Understanding Cryptography. • Andrew S. Tanenbaum (2002), Computer Networks. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.3.2 Netzsicherheit 2

Modulbezeichnung:	**Netzsicherheit 2**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Netzwerkforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Dozent(in):	
Zeitraum:	6. September 2017 – 4. November 2017; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	
Min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistung:	Klausur
Notwendige Voraussetzungen:	Grundlegende bis weiterreichende Mathematikkenntnisse; Grundlagen der Mathematik für Informatiker
Empfohlene Voraussetzungen:	Keine
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalte und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der dritten und vierten Ebene des OSI-Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • SSL **Praktische Übung: Erzeugung eines eigenen (Digitalen)SSL-Zertifikats.** • SSH • Open PGP **Praktische Übung: Erzeugen eines eigenen PGP-Schlüssels zum Ver- und Entschlüsseln von Dateien.** • S/MIME **Praktische Übung: Manipulation S/MIME signierter Mails ohne Gültigkeit der Signatur zu beeinflussen.** • DNSSEC Neben den Systemen werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden werden auf gefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an zu stellen. Als Grundlage werden kurz die Transportprotokolle TCP und UDP behandelt. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)**
Angestrebte Lernergebnisse:	Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Sie haben die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten haben ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten entwickelt.
Lehrveranstaltungen und Lehrformen:	Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Übung
Anerkannte Module:	Keine

Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und –Korrektur in elektronischer Form.
Literatur:	• Jörg Schwenk: Sicherheit und Kryptographie im Internet, 2005. • Christof Paar, Jan Pelzl: Understanding Cryptography, 2010. • Andrew S. Tanenbaum: Computer Networks, 2002. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.3.3 Netzsicherheit 3

Modulbezeichnung:	**Netzsicherheit 3**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Dozent(in):	
Zeitraum:	Voraussichtlich ab Mitte 2017; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	
Min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistung:	Klausur
Notwendige Voraussetzungen:	Grundlegende bis weiterreichende Mathematikkenntnisse; Grundlagen der Mathematik für Informatiker
Empfohlene Voraussetzungen:	• Ausgeprägtes Interesse an IT-Sicherheit, speziell am Thema "Websicherheit" • Grundlegende Kenntnisse über TCP/IP und HTTP(S) • Grundlegende Kenntnisse über HTML / JavaScript • Grundkenntnisse in PHP oder einer ähnlichen Scriptsprache • Netzsicherheit 1 + 2 • Web-Engineering
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalte und Niveau:	Im Laufe der Lehrveranstaltung sollen die Studierenden eine fiktive Online-Banking-Applikation angreifen und dabei die im Laufe der Veranstaltung erlernten Methoden und Techniken einsetzen. Dieses beinhaltet folgende Themengebiete: • Cross Site Sripting (XSS) • Cross Site Request Forgery (CSRF) • Session Hijacking • Session Fixation • SQL Injection (SQLi) • Local/Remote File Inclusion (LFI/RFI) • Path Traversal • Remote Code Execution (RCE) • Logical Flaws • Information Leakage • Insufficient Authorization Das Wissen der Studierenden wird zudem durch externe Experten aus der Industrie und IT-Sicherheits-Szene, die in Vorträgen über verschiedene Thematiken der Webapplikations-Sicherheit referieren werden, angereichert.
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).
Angestrebte Lernergebnisse:	Den teilnehmenden Studierenden soll ein weit gefächertes Wissen über die häufigsten Schwachstellen in Webapplikationen vermittelt werden. Außerdem sollen sie lernen, wie sie derartige Schwachstellen manuell finden können, ohne die Hilfe von automatisierten Webapplikations-Scannern in Anspruch zu nehmen. Darüber hinaus lernen die Studierenden entsprechende Schutzmaßnahmen sowie deren Wirksamkeit kennen.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, Übung
Anerkannte Module:	Keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und –Korrektur in elektronischer Form.
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.3.4 Spam

Modulbezeichnung:	**Spam**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. Christoph Wolf
Dozent(in):	
Zeitraum:	24. Mai 2017 – 22. Juli 2017; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	
Min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistung:	Klausur (120 Minuten), Übungsaufgaben (30%)
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Grundkenntnisse des TCP/IP-Protokolls, Grundlagen der Mathematik für Informatiker
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalte und Niveau:	E-Mails bilden heutzutage einen wichtigen Kommunikationskanal. Vor diesem Hintergrund stellt das immer stärker werdende Aufkommen von Spam nicht nur ein Ärgernis dar, sondern verursacht auch einen enormen wirtschaftlichen Schaden. Um zu verstehen, wie Spam entsteht, werden zum einen Grundlagen vermittelt, wie die Wort-Ethymologie, die verschiedenen Formen von Spam in unterschiedlichen Medien, die oft verwendeten Definitionen sowie die in der Vorlesung verwendete Definition. Zum anderen werden in einer Fall-Studie das Wirtschaftsmodell sowie die Enttarnungsmöglichkeiten von Spammern besprochen. Ein tieferer Einblick in das SMTP-Protokoll stellt den Protokollfluss zwischen Sender und Empfänger dar und beschreibt die Verlässlichkeit der verschiedenen im E-Mail-Quellcode enthaltenen Daten und deren Manipulationsmöglichkeiten in Form einer Analyse der Header-Felder. Es werden verschiedene Formen der Anti-Spam-Maßnahmen präsentiert. Darunter fallen einfache Methoden wie Black- und Whitelists sowie die daraus resultierenden und leicht abgewandelten Graylists. Ebenfalls werden fortgeschrittene Methoden von Grund auf besprochen, wie bspw. Bayessche Filter. Weiterhin wird Spam vom juristischen Standpunkt aus betrachtet, wobei das Opt-In bzw. Opt-Out-Verfahren im Fokus liegt. Ebenso werden die Strafbarkeit sowie die zivilrechtlichen Ansprüche und deren Durchsetzbarkeit angesprochen. Hier wird auch das Spam-Verständnis in den USA mit dem der EU verglichen. Weiterhin werden die juristischen Möglichkeiten für Whitelists diskutiert. Im wirtschaftlichen Bereich werden die Preise für E-Mail, die Wirtschaftlichkeit von Spam sowie der Verfolgungsdruck von Spammern behandelt. Als weitere Anti-Spam Techniken werden noch alternative Protokolle angesprochen, die Zeit- und Speicherbeweise als Funktionen einsetzen, ebenso wie SPK und DKIM. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Die Studierenden erhalten grundlegende und vertiefende Kenntnisse der E-Mail-Struktur sowie des verwendeten SMTP-Protokolls. Sie sollen die Fähigkeit erhalten, technische Protokolle unter Sicherheitsaspekten zu betrachten. Dem gegenüber sollen die Studierenden aber auch die Grenzen der technischen Sicherheit erkennen und Grundkenntnisse in organisatorischen, juristischen und wirtschaftlichen Alternativen erwerben. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße.
Lehrveranstaltungen und Lehrformen:	
Anerkannte Module:	Keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungs-Einreichung und -korrektur in elektronischer Form.

Literatur:	• Brunton, F. (2013) Spam: Shadow History of the Internet (Infrastructures): MIT Press. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.3.5 Sicherheit mobiler Systeme

Modulbezeichnung:	**Sicherheit Mobiler Systeme**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Thorsten Holz
Dozent(in):	Prof. Dr. Thorsten Holz
Zeitraum:	Voraussichtlich ab 2. Quartal 2016; Dauer ca. 2 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Master
Min.-max. Teilnehmerzahl:	12 bis 30
Studien- und Prüfungsleistung:	Klausur
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitsprobleme von Computernetzen
Sprache:	Skript in Englisch, Übungen und Prüfung auf Deutsch oder Englisch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	33	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalte und Niveau:	In der Vorlesung werden verschiedene Sicherheitsaspekte von mobilen Systemen vorgestellt. Anhand von konkreten Beispielen wird erläutert, wie verschiedene Arten von mobilen Systemen aufgebaut sind und welche Sicherheitsrisiken diese besitzen. Dies umfasst unter anderem die folgenden Themen: • Design von GSM und UMTS (Sicherheitsaspekte, Lokalisierungsverfahren, Verbindungsmanagement) • Sicherheit von Satellitentelefonen (GMR) • Sicherheitsaspekte von DECT • Design mobiler Betriebssysteme (Android und iOS) • Analyse von (mobilen) Apps **Praktische Übung(en):** **Analyse von Mobilfunksignalen** • Auswertung von Signalen • Dekodierung **Analyse einer Android-App** • Statische Analyse • Dynamische Analyse **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Sicherheitsaspekten von mobilen Endgeräten vertraut, welche auf andere Arten von Systemen übertragen werden können. Sie verfügen über detaillierte Kenntnisse der Sicherheit von mobilen Endgeräten. Die Studierenden haben die Fähigkeit, sich eine Meinung über die Sicherheit von mobilen Endgeräten zu bilden. Darüber hinaus besitzen sie die Kompetenz, eigenständig neue Angriffe und Bedrohungen aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studierenden tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
Lehrveranstaltungen und Lehrformen:	Onlineveranstaltung: flexible Vertiefung wichtiger Themen; Studienbrief, Übung, Forum in Lernplattform
Anerkannte Module:	Module aus Studiengängen der Informatik oder von stark Informatikaffinen Studiengängen, die ähnliche Lerninhalte und angestrebte Lernergebnisse verfolgen (Überdeckungsgrad > 75%) und deren Workload vergleichbar ist.
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und Korrektur in elektronischer Form, Präsenzveranstaltung mit Rechner und Beamer

Literatur:	• Hannes Federrath: Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehrseitige Sicherheit, Vieweg, 1999 • Noureddine Boudrige: Security of Mobile Communications, Auerbach Publications, 2009 • Miller et al.: iOS Hacker´s Handbook, Wiley. 2012 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.4 Goethe-Universität Frankfurt am Main

1.4.1 Computerstrafrecht

Modulbezeichnung:	**Computerstrafrecht**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikat „Datenträgerforensiker/-in Open C³S“ sowie „Netzwerkforensiker/-in Open C³S“ und in ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. Christoph Burchard
Dozent(in):	Dr. Christoph Burchard
Zeitraum:	24. Mai 2017 – 22. Juli 2017; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne juristische Ausbildung
min.-max. Teilnehmerzahl:	20 bis 30
Studien- und Prüfungsleistungen:	Klausur, Seminararbeit, Präsentation
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	keine
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	Das Modul befasst sich in mehreren Studienbriefen mit dem Phänomen der Computerkriminalität. Um die damit auftretenden Probleme richtig einordnen zu können, wird in Studienbrief 1 zunächst ein Mindestmaß an Grundwissen vermittelt. Diese Einführung in das materielle Strafrecht stellt die Basis für die in den weiteren Studienbriefen vertiefte Auseinandersetzung mit den Tatbeständen dar, die üblicherweise unter den Begriff der Computer- und Internetkriminalität subsumiert werden. Die Studienbriefe fassen die damit zusammenhängenden und dahinterstehenden rechtlichen Probleme in Themenkomplexen zusammen. Beispielfälle und Bezugnahmen auf einschlägige Rechtsprechung sollen helfen, die oft abstrakte Materie greifbar und nachvollziehbar zu machen. Die Darstellung erfolgt dabei anhand der

	einschlägigen Delikte des Strafgesetzbuches sowie einzelner Tatbestände des Nebenstrafrechts, die im Einzelnen näher erklärt und dargestellt werden. Darüber hinaus werden aber auch Grundzüge der mit dem Medium Internet verbundenen verfassungsrechtlichen Fragen sowie rechtliche Rahmenbedingungen für die Anbieter von Inhalten behandelt. **Praktische Übung:** Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls haben die Studierenden Kenntnisse über die Grundzüge des Computerstrafrechts und die verschiedenen Facetten der Computer- und Internetkriminalität. Sie sind in der Lage, grundsätzliche Aussagen über das Phänomen Computerkriminalität zu treffen und Einschätzungen hinsichtlich der Strafbarkeit einzelner, damit verbundener Verhaltensweisen abzugeben. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompetenz.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung Onlineveranstaltung: Vorlesung, gegebenenfalls flexible Vertiefung wichtiger Themen
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.4.2 Computerstrafprozessrecht

Modulbezeichnung:	**Computerstrafprozessrecht**
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	
Modulverantwortliche(r):	Dr. Christoph Burchard
Dozent(in):	Dr. Christoph Burchard
Zeitraum:	6. September 2017 – 4. November 2017; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne juristische Ausbildung
min.-max. Teilnehmerzahl:	20 bis 30
Studien- und Prüfungsleistungen:	Klausur, Seminararbeit, Präsentation
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Abgeschlossenes Modul Computerstrafrecht
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	Das Modul befasst sich in mehreren Studienbriefen mit den Auswirkungen der Informationstechnologie auf das Strafprozessrecht. Unter Bezugnahme auf die im Modul Computerstrafrecht erworbenen materiellrechtlichen Grundkenntnisse werden im Modul grundlegende Kenntnisse im Bereich des Verfahrensrechts und des formellen Strafrechts vermittelt. Auch in diesem Modul wird regelmäßig Bezug auf einschlägige Rechtsprechung genommen und Wert auf eine fallbezogene Wissensvermittlung gelegt. Angesichts der besonderen Bedeutung des Strafverfahrensrechts werden aber auch Grundzüge verfassungsrechtlicher Fragestellungen behandelt. **Praktische Übungen**: Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Die Studierenden erwerben Grundkenntnisse des Strafprozessrechts. Sie können die Grundzüge des Computerstrafprozessrechts in Bezug zur Informationstechnologie und zum Verfassungsrecht setzen. Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage, verfahrensrechtliche Maßnahmen auf ihre Zulässigkeit zu überprüfen und hierzu kritisch Stellung zu nehmen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompentenz.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung Onlineveranstaltung: Vorlesung, gegebenenfalls flexible Vertiefung wichtiger Themen
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und –korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

1.4.3 Europäisierung & Internationalisierung des Strafrechts

Modulbezeichnung:	Europäisierung & Internationalisierung des Strafrechts
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	
Modulverantwortliche(r):	Dr. Christoph Burchard
Dozent(in):	Dr. Christoph Burchard
Zeitraum:	Voraussichtlich ab Ende 2016; Dauer ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne juristische Ausbildung
min.-max. Teilnehmerzahl:	20 bis 30
Studien- und Prüfungsleistungen:	Klausur, Seminararbeit, Präsentation
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Abgeschlossene Module Computerstrafrecht oder Computerstrafprozessrecht
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	25	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	3	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	Das Modul widmet sich in mehreren Studienbriefen dem Prozess der Europäisierung und Internationalisierung des Strafrechts. Die in den Modulen Computerstrafrecht und Computerstrafprozessrecht nur gestreiften Aspekte der zunehmenden Internationalisierung des Strafrechts werden an dieser Stelle vertieft. Die zunehmende Europäisierung des Rechts macht es besonders im Strafrecht notwendig, bisherige nationalstaatliche Regelungsansätze zu überdenken. Dazu ist es unerlässlich, sich auch mit den durch das Europarecht definierten Vorgaben auseinanderzusetzen. **Praktische Übung:** Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls haben die Studierenden Kenntnisse über die Grundzüge internationalen Rechts und supranationaler Regelungsmodelle. In den Modulen Computerstrafrecht oder Computerstrafprozessrecht erworbene Kenntnisse werden vor diesem Hintergrund neu betrachtet. Die Studierenden sind in der Lage, grundsätzliche Aussagen über die Probleme der internationalen strafrechtlichen Zusammenarbeit zu treffen und die aktuelle Entwicklung kritisch zu hinterfragen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompetenz.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung Onlineveranstaltung: Vorlesung, gegebenenfalls flexible Vertiefung wichtiger Themen
Anerkannte Module:	keine
Medienformen:	Schriftlicher und elektronischer Studienbrief, Übungseinreichung und -korrektur in elektronischer Form, Onlinematerial in Lernplattform, Präsenzveranstaltung mit Rechner und Beamer, Online-Vorlesung über Web-Konferenzen
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.