Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Open C³S
Open Competence Center for Cyber Security

Zertifikatsprogramm Open C³S

Modulhandbuch

(Stand 01.01.2024)

In Kooperation mit

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

FAU Friedrich-Alexander Universität Erlangen-Nürnberg

Universität Passau

und Dozenten der

Goethe Universität Frankfurt am Main

Universität des Saarlandes

Inhalt

1. Einführung ... 4
1.1 Über das Zertifikatsprogramm ... 4
1.2 Vorwort ... 6
2. Modulübersicht ... 7
2.1 Modulkatalog ... 7
2.2 Qualifikationsziel-Modul-Matrix ... 9
2.3 Weiterbildungsprogramm-Kompetenzmatrix ... 12
2.4 Curriculum Hochschulzertifikate 2024/2025 ... 14
2.5 Gesamtzertifikate ... 15
2.5.1 Certificate of Advanced Studies (CAS ≥ 15 ECTS) ... 15
2.5.2 Diploma of Advanced Studies (DAS ≥ 30 ECTS) ... 16
3. Prüfungsübersicht aller Module im ZP gem. Studienprüfungsordnung „ZertO“ ... 19
4. Modulbeschreibungen ... 22
4.1 Friedrich-Alexander-Universität Erlangen-Nürnberg ... 22
4.1.1 [Z-101] Methoden digitaler Forensik ... 22
4.1.2 [Z-102] Systemnahe Programmierung ... 24
4.1.3 [Z-103] Reverse Engineering ... 27
4.1.4 [Z-104] Live-Analyse - Spurensicherung u. Analyse am laufenden System ... 30
4.1.5 [Z-105] Browser- und Anwendungsforensik ... 32
4.1.6 [Z-106] Web Application Security ... 34
4.1.7 [Z-107] Mobilfunkforensik ... 37
4.2 Hochschule Albstadt-Sigmaringen ... 39
4.2.1 [Z-201] Applied Computer Systems / [M-101] Einführung in die Informatik ... 39
4.2.2 [Z-202] Programmieren im IT-Security-Umfeld mit Python 1 ... 42
4.2.3 [Z-203] Penetration Testing mit Python ... 45
4.2.4 [Z-204] Grundlagen Datenträgerforensik ... 47
4.2.5 [Z-205] Vertiefung Datenträgerforensik ... 50
4.2.6 [Z-206] Internettechnologien ... 54
4.2.7 [Z-208] Forensische Analyse eines Windows-Systems ... 56
4.2.8 [Z-209] Forensische Analyse eines Unix-Systems ... 59
4.2.9 [Z-210] Forensische Analyse eines MacOS-Systems ... 63
4.2.10 [Z-211] Forensische Analyse von Netzwerken ... 67
4.2.11 [Z-212] Vertiefung Netzsicherheit ... 70
4.2.12 [Z-213] Incident Response & Malware Defence ... 72

4.2.13 [Z-214] Forensische Analyse eines Windows-Systems für Sachverständige 75
4.2.14 [Z-215] Forensische Analyse eines Unix-Systems für Sachverständige 75
4.2.15 [Z-216] Forensische Analyse eines MacOS-Systems für Sachverständige 75
4.2.16 [Z-217] Forensische Analyse von Netzwerken für Sachverständige 75
4.2.17 [Z-218] Sachverständigenmodul „Auftreten vor Gericht“ 76
4.2.18 [Z-219] Sachverständigenmodul „Einrichten eines forensischen Labors“ 78
4.2.19 [Z-220] Netzsicherheit I - IT-Sicherheit von Netzwerken 80
4.2.20 [Z-221] Netzsicherheit II – *In Überarbeitung!* 83
4.2.21 [Z-222] Netzsicherheit III – *In Überarbeitung!* 83
4.2.22 [Z-223] Windows-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung* 84
4.2.23 [Z-224] Unix-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung* 84
4.2.24 [Z-225] MacOS-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung* 84
4.2.25 [Z-226] Netzwerkforensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung* 84
4.3 Ruhr-Universität Bochum 85
4.3.1 [Z-304] SPAM 85
4.3.2 [Z-305] Kryptographie 1 87
4.3.3 [Z-306] Kryptographie 2 89
4.3.4 [Z-307] Kryptanalytische Methoden und Werkzeuge 91
4.3.5 [Z-308] Sicherheit mobiler Systeme 93
4.4 Goethe-Universität Frankfurt am Main / Universität des Saarlandes 96
4.4.1 [Z-401] Computerstrafrecht 96
4.4.2 [Z-402] Computerstrafprozessrecht 98
4.5 Universität Passau 100
4.5.1 [Z-801] Cloud-Sicherheit und Cloud-Forensik – Angriffsanalyse 100
4.5.2 [Z-802] Cloud-Sicherheit und Cloud-Forensik – Zugriffskontrolle 102

1. Einführung

1.1 Über das Zertifikatsprogramm

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 40 in sich abgeschlossene Studienmodule zu den Themenschwerpunkten entwickelt:

• Sicherheit

• Forensik

• Kryptografie

• Recht

• Politik und

• praktische Informatik

Mehr als 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 2020 wieder.

Die Zertifikatsmodule sind auf wissenschaftlichem Niveau und bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung, mit hohem Praxisbezug. Nach erfolgreichem Abschluss eines Moduls erhält jeder Absolvent ein Hochschulzertifikat mit ausgewiesenen ECTS-Leistungspunkten (5 ECTS-Punkte/Modul). Die ECTS-Leistungspunkte können auf weiterführende Studiengänge der Hochschule Albstadt-Sigmaringen, wie zum Beispiel auf den Bachelor-Studiengang "IT-Sicherheit" oder die Masterstudiengänge „IT Governance, Risk and Compliance Management" sowie "Master Digitale Forensik" und andere Studienangebote (national, international, Uni oder Hochschule) angerechnet werden.

Mehrere Zertifikatsmodule können zu einem spezifischen Zertifikatsstudium kumuliert werden. Nach erfolgreichem Abschluss der Module erhalten die Absolventen ein Certificate of Advanced Studies (CAS ≥ 15 ECTS) oder das Diploma of Advanced Studies (DAS ≥ 30 ECTS) als Gesamtzertifikat mit ausgewiesenen ECTS-Leistungspunkten.

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

- Es bestehen keine formellen Zulassungsbeschränkungen.
- Die Studiendauer beträgt ca. 8 Wochen pro Modul und schließt mit einer sogenannten Prüfungsleistung 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%.
- Nach erfolgreichem Abschluss eines Moduls erhalten Sie ein Hochschulzertifikat mit ausgewiesenen ECTS-Leistungspunkten.
- Die Teilnahmegebühr für ein Einzelmodul beträgt gemäß der geltenden Gebührensatzung 2.000,- EUR.
- Unsere Gesamtzertifikate (CAS & DAS) gelten als fachliche Expertise.

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
- Universität Passau

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

Wissenschaftliche Studienangebote wie das Zertifikatsprogramm unterstützen den Übergang von der beruflichen zur hochschulischen Bildung und qualifizieren Fachkräfte in spezifischen Themengebieten.

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

1.2 Vorwort

Dieses Dokument enthält die Beschreibungen aller Module des berufsbegleitenden Zertifikatsprogramm Open C³S und soll Ihnen einen Überblick über das aktuelle Modulangebot, sowie deren wichtigsten und charakteristischen Informationen zu Inhalt und Umfang liefern.

Ziel dieses Modulhandbuchs ist es, den Interessenten und angehenden Absolventen eine Übersicht der geforderten Leistungen sowie allen Informationen rund um die Module zu bieten. Die Übersicht auf den nachfolgenden Seiten soll Ihnen bei der Zuordnung und Orientierung helfen und dazu dienen, die Angebotsabläufe zu verstehen. Abkürzungen in diesem Dokument werden erläutert und den Oberbegriffen zugeordnet.

Im Anschluss daran finden Sie die einzelnen Module jeweils nach Universität bzw. Hochschule aufgelistet. Generelle Informationen zum Beispiel zur Veranstaltungssprache, Zeitaufwand und Vorkenntnisse können sie den detaillierten Beschreibungen entnehmen.

Die Module haben einen Umfang von 150 Zeitstunden und beinhalten Prüfungsleistungen. Für jedes erfolgreich absolvierte Einzelmodul werden 5 ECTS-Punkte vergeben.

2. Modulübersicht

2.1 Modulkatalog

	Modulbezeichnung	Hochschule/ Universität	Modulnummer
1	Methoden digitaler Forensik	FAU	Z-101
2	Systemnahe Programmierung	FAU	Z-102
3	Reverse Engineering	FAU	Z-103
4	Live Analyse / Spurensicherung	FAU	Z-104
5	Browser- und Anwendungsforensik	FAU	Z-105
6	Web Application Security	FAU	Z-106
7	Mobilfunkforensik	Extern	Z-107
8	Applied Computer Systems (Rechnersysteme)	HSAS	Z-201
9	Programmieren im IT-Security-Umfeld mit Python	HSAS	Z-202
10	Penetration Testing mit Python	HSAS	Z-203
11	Grundlagen Datenträgerforensik	HSAS	Z-204
12	Vertiefung Datenträgerforensik	HSAS	Z-205
13	Internettechnologien	HSAS	Z-206
14	Forensische Analyse eines Windows-Systems	HSAS	Z-208
15	Forensische Analyse eines Unix-Systems	HSAS	Z-209
16	Forensische Analyse eines MacOS-Systems	HSAS	Z-210
17	Forensische Analyse von Netzwerken	HSAS	Z-211
18	Vertiefung Netzsicherheit	HSAS	Z-212
19	Incid6nt Response & Malware Defence	HSAS	Z-213

	Modulbezeichnung	Hochschule/ Universität	Modulnummer
20	Forensische Analyse eines Windows-Systems für Sachverständige	HSAS	Z-214
21	Forensische Analyse eines Unix-Systems für Sachverständige	HSAS	Z-215
22	Forensische Analyse eines MacOS-Systems für Sachverständige	HSAS	Z-216
23	Forensische Analyse von Netzwerken für Sachverständige	HSAS	Z-217
24	Sachverständigenmodul „Auftreten vor Gericht“ (BKA/LKÄ)	Extern	Z-218
25	Sachverständigenmodul „Einrichten eines forensischen Labors“ (BKA/LKÄ)	Extern	Z-219
26	Netzsicherheit 1 – IT-Sicherheit von Netzwerken	HSAS	Z-220
27	Netzsicherheit 2 *(in Bearbeitung!)*	HSAS	Z-221
28	Netzsicherheit 3 *(in Bearbeitung!)*	HSAS	Z-222
29	Windows-Forensik Gutachter - Vorbereitendes Modul zur Gutachterprüfung	HSAS	Z-223
30	Unix-Forensik Gutachter - Vorbereitendes Modul zur Gutachterprüfung	HSAS	Z-224
31	MacOS-Forensik Gutachter - Vorbereitendes Modul zur Gutachterprüfung	HSAS	Z-225
32	Netzwerkforensik Gutachter - Vorbereitendes Modul zur Gutachterprüfring	HSAS	Z-226
33	SPAM	RUB	Z-301
34	Einführung in die Kryptographie	RUB	Z-302
35	Kryptographie 1	RUB	Z-303
36	Kryptographie 2	RUB	Z-304
37	Kryptanalytische Methoden und Werkzeuge	RUB	Z-305
38	Sicherheit mobiler Systeme	RUB	Z-306
39	Computerstrafrecht	GU/UdS	Z-401
40	Computerstrafprozessrecht	GU/UdS	Z-402
41	Cloud-Sicherheit und Cloud-Forensik – Angriffsanalyse	UPA	Z-801
42	Cloud-Sicherheit und Cloud-Forensik – Zugriffskontrolle	UPA	Z-802

2.2 Qualifikationsziel-Modul-Matrix

Die Qualifikationsziele im Zertifikatsprogramm Open C³S sind:

1. Umfassendes technisches IT-Wissen inklusive detailliertem Know-how über Computer und Netzwerke.
2. Genaue Methodenkenntnis der Digitalen Forensik inklusive spezifischer Vorgehensweisen bei der Identifikation, Sicherung und Analyse aller Arten digitaler Beweismittel.
3. Praxiserfahrung, um nach dem Studium eine schnelle Einarbeitung in die praktische Berufstätigkeit zu ermöglichen.
4. Juristische Grundlagen, um das Bewusstsein für mögliche rechtliche Konsequenzen des Handelns in der späteren Berufspraxis zu schärfen.

Nachfolgend finden Sie die Qualifikationsziel-Modul-Matrix im Einzelnen.

Qualifikationsziel-Modul-Matrix

Unterstützung der Qualifikationsziele in den Modulen (0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

Modul-Nr.	Qualifikationsziel (QuZ)	Summe der Unter-stützungs-punkte	Qualifikations-ziel 1	Qualifikations-ziel 2	Qualifikations-ziel 3	Qualifikations-ziel 4
Z-101	Methoden digitaler Forensik	5	1	2	1	1
Z-102	Systemnahe Programmierung	6	2	1	2	1
Z-103	Reverse Engineering	6	1	2	2	1
Z-104	Live Analyse / Spurensicherung	5	0	2	2	1
Z-105	Browser- und Anwendungsforensik	5	0	2	2	1
Z-106	Web Application Security	6	2	1	2	1
Z-107	Mobilfunkforensik	7	2	2	2	1
Z-201	Applied Computer Systems (Rechnersysteme)	4	2	1	1	0
Z-202	Python 1 – Programmierung und Forensik (Programmieren im IT-Security-Umfeld)	6	1	2	2	1
Z-203	Python 2 – Penetration Testing (Programmieren im IT-Security-Umfeld)	6	2	1	2	1
Z-204	Datenträgerforensik 1	5	1	2	1	1
Z-205	Datenträgerforensik 2	6	1	2	2	1
Z-206	Internettechnologien	4	2	1	1	0
Z-208	Windows-Forensik	7	2	2	2	1
Z-209	Unix-Forensik	7	2	2	2	1
Z-210	Mac-Forensik	7	2	2	2	1
Z-211	Netzwerkforensik	7	2	2	2	1
Z-212	Netzwerkanalyse	6	2	2	1	1
Z-213	Netzwerkhacking	6	2	1	2	1
Z-214	Sachverständigenmodul Windows-Forensik	7	2	2	2	1
Z-215	Sachverständigenmodul Unix-Forensik	7	2	2	2	1
Z-216	Sachverständigenmodul Mac-Forensik	7	2	2	2	1
Z-217	Sachverständigenmodul Netzwerkforensik	7	2	2	2	1
Z-220	Netzsicherheit 1 – IT-Sicherheit von Netzwerken	5	2	1	2	0
Z-401	Computerstrafrecht	6	0	2	2	2
Z-402	Computerstrafprozessrecht	6	0	2	2	2
Z-801	Cloud-Sicherheit und Cloud-Forensik – Angriffsanalyse	5	1	2	2	0
Z-802	Cloud-Sicherheit und Cloud-Forensik – Zugriffskontrolle	5	1	2	2	0

Die nachfolgenden, bereits entwickelten Module können derzeit leider nicht in aktualisierter Form angeboten werden und wurden daher in der Qualifikationsziel-Modul-Matrix nicht bewertet.

Unterstützung der Qualifikationsziele in den Modulen (0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

Modul-Nr.	Qualifikationsziel (QuZ)	Summe der Unterstützungspunkte	Qualifikationsziel 1	Qualifikationsziel 2	Qualifikationsziel 3	Qualifikationsziel 4
Z-218	Sachverständigenmodul „Auftreten vor Gericht"	-	-	-	-	-
Z-219	Sachverständigenmodul „Einrichten eines forensischen Labors"	-	-	-	-	-
Z-221	Netzsicherheit 2 – Kabellose Netze *(in Bearbeitung!)*	-	-	-	-	-
Z-222	Netzsicherheit 3 *(in Bearbeitung!)*	-	-	-	-	-
Z-301	SPAM	-	-	-	-	-
Z-302	Einführung in die Kryptographie	-	-	-	-	-
Z-303	Kryptographie 1	-	-	-	-	-
Z-304	Kryptographie 2	-	-	-	-	-
Z-305	Kryptanalytische Methoden und Werkzeuge	-	-	-	-	-
Z-306	Sicherheit mobiler Systeme	-	-	-	-	-

2.3 Weiterbildungsprogramm-Kompetenzmatrix

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestal-tung	Kommuni-kation	Eigenstän-digkeit/ Verant-wortung	Reflexi-vität	Lern-kompetenz
Z-101	Methoden digitaler Forensik	7	7		7	7	7	7	7		7	7
Z-102	Systemnahe Programmierung	7	7	7	7	7		7	7	7	7	7
Z-103	Reverse Engineering	7	7	7	7	7		7	7	7	7	7
Z-104	Live Analyse / Spurensicherung	7	7	7	7	7	7	7	7	7	7	7
Z-105	Browser- und Anwendungsforensik	7	7	7	7	7	7	7	7	7	7	7
Z-106	Web Application Security	7	7	7	7	7	7	7	7	7	7	7
Z-107	Mobilfunkforensik	7	7	7	7	7	7	7	7	7	7	7
Z-201	Applied Computer Systems		7	7					7			7
Z-202	Python 1 – Programmieren im IT-Security-Umfeld	7	7	7	7			7	7	7	7	7
Z-203	Python 2 – Penetration Testing	7	7	7	7	7	7	7	7	7	7	7
Z-204	Datenträgerforensik 1		7	7	7			7	7	7	7	7
Z-205	Datenträgerforensik 2	7	7	7	7	7		7	7	7	7	7
Z-206	Internettechnologien		7	7	7				7			7
Z-208	Windows-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-209	Unix-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-210	Mac-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-211	Netzwerkforensik	7	7	7	7	7	7	7	7	7	7	7
Z-212	Netzwerkanalyse	7	7	7	7	7		7	7	7	7	7
Z-213	Netzwerkhacking	7	7	7	7	7	7	7	7	7	7	7
Z-214	Sachverständigenmodul Windows-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-215	Sachverständigenmodul Unix-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-216	Sachverständigenmodul Mac-Forensik	7	7	7	7	7	7	7	7	7	7	7
Z-217	Sachverständigenmodul Netzwerkforensik	7	7	7	7	7	7	7	7	7	7	7
Z-220	Netzsicherheit 1	7	7	7	7	7		7	7	7	7	7
Z-401	Computerstrafrecht	7	7	7	7	7	7	7	7	7	7	7
Z-402	Computerstrafprozessrecht	7	7	7	7	7	7	7	7	7	7	7
Z-801	Cloud-Sicherheit und Cloud-Forensik – Angriffsanalyse	7	7	7	7	7		7	7	7	7	7
Z-802	Cloud-Sicherheit und Cloud-Forensik – Zugriffskontrolle	7	7	7	7	7		7	7	7	7	7

Die nachfolgenden, bereits entwickelten Module können derzeit leider nicht in aktualisierter Form angeboten werden und wurden daher in der Weiterbildungsprogramm-Kompetenzmatrix nicht bewertet.

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestal-tung	Kommuni-kation	Eigenstän-digkeit/ Verant-wortung	Reflexi-vität	Lern-kompetenz
Z-221	Netzsicherheit 2 – Kabellose Netze *(in Bearbeitung!)*	-	-	-	-	-	-	-	-	-	-	-
Z-222	Netzsicherheit 3 *(in Bearbeitung!)*	-	-	-	-	-	-	-	-	-	-	-
Z-301	SPAM	-	-	-	-	-	-	-	-	-	-	-
Z-302	Einführung in die Kryptographie	-	-	-	-	-	-	-	-	-	-	-
Z-303	Kryptographie 1	-	-	-	-	-	-	-	-	-	-	-
Z-304	Kryptographie 2	-	-	-	-	-	-	-	-	-	-	-
Z-305	Kryptanalytische Methoden und Werkzeuge	-	-	-	-	-	-	-	-	-	-	-
Z-306	Sicherheit mobiler Systeme	-	-	-	-	-	-	-	-	-	-	-

2.4 Curriculum Hochschulzertifikate 2024/2025

BLOCK 1 Zeitraum: Januar bis Mai	BLOCK 2 Zeitraum: Mai bis Juli	BLOCK 3 Zeitraum: September bis November	BLOCK 4 Zeitraum: November bis Februar
[Z-103] Reverse Engineering *Anmeldeschluss: 17.01.2024* FAU	[Z-101] Methoden digitaler Forensik *Anmeldeschluss: 17.04.2024* FAU	[Z-213] Incident Response & Malware Defence *Anmeldeschluss: 31.07.2024* HSAS (LB)	[Z-102] Systemnahe Programmierung *Anmeldeschluss: 09.10.2024* FAU
[Z-106] Web Application Security *Anmeldeschluss: 20.03.2024* FAU	[Z-801] Cloud-Sicherheit- und Forensik „Angriffsanalyse“ *Anmeldeschluss: 27.03.2024* UPA (LB)		[Z-401] Computerstrafrecht *Anmeldeschluss: 09.10.2024* GU
[Z-214] Netzsicherheit 1 IT-Sicherheit von Netzwerken *Anmeldeschluss: 24.01.2024* HSAS (LB)	[Z-214] Forensische Analyse eines Windows-Systems für Sachverständige *Anmeldeschluss: 27.03.2024* HSAS (LB)		[Z-216] Forensische Analyse eines MacOS-Systems für Sachverständige *Anmeldeschluss: 09.10.2024* HSAS (LB)
[Z-215] Forensische Analyse eines Unix-Systems für Sachverständige *Anmeldeschluss: 24.01.2024* HSAS (LB)	[Z-223] Windows-Forensik Gutachter – Vorbereitendes Modul zur Gutachterprüfung *Anmeldung ausschließlich über das BKA* HSAS (LB)		[Z-225] MacOS-Forensik Gutachter – Vorbereitendes Modul zur Gutachterprüfung *Anmeldung ausschließlich über das BKA* HSAS (LB)
[Z-224] Unix-Gutachter – Vorbereitendes Modul zur Gutachterprüfung *Anmeldung ausschließlich über das BKA* HSAS (LB)			

Alle Angaben verstehen sich vorbehaltlich etwaiger Änderungen.

2.5 Gesamtzertifikate

2.5.1 Certificate of Advanced Studies (CAS ≥ 15 ECTS)

Nr.	Bezeichnung	Pflichtmodule
C1	**Netzsicherheit (NSi)**	▪ [Z-220] Netzsicherheit I ▪ [Z-221] Netzsicherheit II *(in Bearbeitung!)* ▪ [Z-222] Netzsicherheit III *(in Bearbeitung!)*
C2	**Pythonanwendungen (PyA)**	▪ [Z-201] Applied Computer Systems ▪ [Z-202] Programmierung und Forensik mit Python ▪ [Z-203] Penetration Testing mit Python
C3	**Betriebssystemforensik (BSF)**	▪ [Z-208] Windows-Forensik* ▪ [Z-209] Unix-Forensik* ▪ [Z-210] Mac-Forensik*
C4	**Reverse Engineering (RE)**	▪ [Z-102] Systemnahe Programmierung ▪ [Z-103] Reverse Engineering ▪ [Z-203] Penetration Testing mit Python
C5	**Kryptographie (Kry)**	▪ [Z-306] Kryptographie 1 ▪ [Z-307] Kryptographie 2 ▪ [Z-308] Kryptanalytische Methoden und Werkzeuge
C6	**Cloud-Forensik (ClF)**	▪ [Z-101] Methoden digitaler Forensik ▪ [Z-212] Netzwerkanalyse ▪ [Z-801] oder [Z-802] Cloud-Sicherheit und Cloud-Forensik
C7	**Computerstrafrecht (CoS)**	▪ [Z-201] Applied Computer Systems ▪ [Z-401] Computerstrafrecht ▪ [Z-402] Computerstrafprozessrecht
C8	**Gerichtliche Sachverständige „Digitale Forensik“ (GSA)**	▪ [Z-218] Sachverständigenmodul „Auftreten vor Gericht“ ▪ [Z-219] Sachverständigenmodul „Einrichten eines forensischen Labors“ ▪ [Z-401] Computerstrafrecht

* Ersatzweise das entsprechende Sachverständigenmodul

2.5.2 Diploma of Advanced Studies (DAS ≥ 30 ECTS)

D1	Netzwerkforensiker/-in Open C³S (NF)	
Pflichtmodule	[Z-201] Applied Computer Systems	Hochschule Albstadt-Sigmaringen
	[Z-203] Python 2 – Penetration Testing	
	[Z-206] Internettechnologien	
	[Z-212] Netzwerkanalyse	
	[Z-213] Netzwerkhacking	
Wahlpflichtmodule**	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-401] Computerstrafrecht	Goethe-Universität Frankfurt a. M. und Uni des Saarlandes
	[Z-402] Computerstrafprozessrecht	
	[Z-801] Cloud-Sicherheit und Cloud-Forensik - Angriffsanalyse	Universität Passau
	[Z-802] Cloud-Sicherheit und Cloud-Forensik - Zugriffskontrolle	

** Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

D2	Datenträgerforensiker /-in Open C³S (DTF)	
Pflichtmodul	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-202] Python 1 – Programmierung und Forensik	Hochschule Albstadt-Sigmaringen
	[Z-203] Python 2 – Penetration Testing	
	[Z-204] Datenträgerforensik 1	
	[Z-205] Datenträgerforensik 2	
Wahlpflichtmodul**	[Z-201] Applied Computer Systems	
	[Z-401] Computerstrafrecht	Goethe-Universität Frankfurt a. M. und Uni des Saarlandes
	[Z-402] Computerstrafprozessrecht	
	[Z-801] Cloud-Sicherheit und Cloud-Forensik - Angriffsanalyse	Universität Passau
	[Z-802] Cloud-Sicherheit und Cloud-Forensik - Zugriffskontrolle	

** Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

2.3.2 Diploma of Advanced Studies (DAS ≥ 30 ECTS)

D3	**Live-Forensiker /-in Open C³S (LiF)**	
Pflichtmodul	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-102] Systemnahe Programmierung	
	[Z-103] Reverse Engineering	
	[Z-104] Live-Analyse	
	[Z-201] Applied Computer Systems	Hochschule Albstadt-Sigmaringen
Wahlpflichtmodul**	[Z-401] Computerstrafrecht	Goethe-Universität Frankfurt a. M. und Uni des Saarlandes
	[Z-402] Computerstrafprozessrecht	
	[Z-801] Cloud-Sicherheit und Cloud-Forensik	Universität Passau
	[Z-802] Cloud-Sicherheit und Cloud-Forensik	

** Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

D4	**Computerforensiker /-in Open C³S (CoF)**	
Pflichtmodul	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-201] Applied Computer Systems	Hochschule Albstadt-Sigmaringen
	[Z-208] Windows-Forensik**	
	[Z-209] Unix-Forensik**	
	[Z-210] Mac-Forensik**	
Wahlpflichtmodul**	[Z-203] Python 2 – Penetration Testing	
	[Z-401] Computerstrafrecht	Goethe-Universität Frankfurt a. M. und Uni des Saarlandes
	[Z-402] Computerstrafprozessrecht	

* Ersatzweise das entsprechende Sachverständigenmodul

** Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

2.3.2 Diploma of Advanced Studies (DAS ≥ 30 ECTS)

D5	**Cloud-Forensiker/-in Open C³S (CIF)**	
Pflichtmodul	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-202] Python 1 – Programmierung und Forensik	Hochschule Albstadt-Sigmaringen
	[Z-203] Python 2 – Penetration Testing	
	[Z-206] Internettechnologien	
	[Z-214] Netzsicherheit I	
Wahlpflichtmodul**	[Z-212] Netzwerkanalyse	
	[Z-213] Netzwerkhacking	
	[Z-801] Cloud-Sicherheit und Cloud-Forensik - Angriffsanalyse	Universität Passau
	[Z-802] Cloud-Sicherheit und Cloud-Forensik - Zugriffskontrolle	

* Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

D6	**Der Gerichtliche Sachverständige „Digitale Forensik“ Open C³S (GSa)**	
Pflichtmodul	[Z-101] Methoden digitaler Forensik	Friedrich-Alexander-Universität Erlangen-Nürnberg
	[Z-218] Sachverständigenmodul „Auftreten vor Gericht“	Extern
	[Z-219] Sachverständigenmodul „Einrichten eines forensischen Labors“	
	[Z-401] Computerstrafrecht	Goethe-Universität Frankfurt a. M. und Uni des Saarlandes
	[Z-402] Computerstrafprozessrecht	
Wahlpflichtmodul**	[Z-208] Windows-Forensik*	Hochschule Albstadt-Sigmaringen
	[Z-209] Unix-Forensik*	
	[Z-210] Mac-Forensik	
	[Z-214] Sachverständigenmodul Windows-Forensik	
	[Z-215] Sachverständigenmodul Unix-Forensik	
	[Z-216] Sachverständigenmodul Mac-Forensik	

* Es muss jeweils ein Wahlpflichtmodul pro Bündel belegt werden.

3. Prüfungsübersicht aller Module im ZP gem. Studienprüfungsordnung „ZertO“

Modul-Nr.	Modulbezeichnung	Institution	Modulprüfung / Modulteilprüfung: Benotete Art (Gewicht)	Modulprüfung / Modulteilprüfung: Unbenotet Art	ECTS-Punkte	Gesamtzertifikat (vgl. Anlage 1): CAS-Nr.	Gesamtzertifikat (vgl. Anlage 1): DAS-Nr.
Z-101	Methoden digitaler Forensik	FAU	HA (5)		5	C6	D1/D2/D3/D4/D5/D6
Z-102	Systemnahe Programmierung	FAU	HA (5)		5	C4	D3
Z-103	Reverse Engineering	FAU	HA (5)		5	C4	D3
Z-104	Live Analyse / Spurensicherung	FAU	Ha (1,5) + M (3,5)		5	-	D3
Z-105	Browser- und Anwendungsforensik	FAU	Ha (1,5) + R (3,5)		5	-	-
Z-106	Web Application Security	FAU	M30* (5)	Ü	5	-	-
Z-107	Mobilfunkforensik	Extern	Ha (1,5) + M (3,5)		5	-	-
Z-201	Applied Computer Systems	HSAS	K60* (5)	HA	5	C2	D1/D2/D3/D4
Z-202	Python 1 – Programmierung und Forensik	HSAS	K60* (5)	HA	5	C2	D2/D5
Z-203	Python 2 – Penetration Testing	HSAS	K60* (5)	HA	5	C2/C4	D1/D2/D4/D5
Z-204	Datenträgerforensik 1	HSAS	K60* (5)	HA	5	-	D2
Z-205	Datenträgerforensik 2	HSAS	K60* (5)	HA	5	-	D2
Z-206	Internettechnologien	HSAS	K60* (5)	HA	5	-	1/5
Z-208	Windows-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-209	Unix-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-210	Mac-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-211	Netzwerkforensik	HSAS	K60* (5)	HA	5	-	-
Z-212	Netzwerkanalyse	HSAS	K60* (5)	HA	5	C6	D1/D5
Z-213	Netzwerkhacking	HSAS	K60* (5)	HA	5	-	D1/D5

* Voraussetzung: Ha bestanden

Änderungen vorbehalten!

Modul-Nr.	Modulbezeichnung	Institution	Modulprüfung / Modulteilprüfung: Benotete Art (Gewicht)	Modulprüfung / Modulteilprüfung: Unbenotet Art	ECTS-Punkte	Gesamtzertifikat (vgl. Anlage 1): CAS-Nr.	Gesamtzertifikat (vgl. Anlage 1): DAS-Nr.
Z-214	Sachverständigenmodul Windows-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-215	Sachverständigenmodul Unix-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-216	Sachverständigenmodul Mac-Forensik	HSAS	K60* (5)	HA	5	C3	D4/D6
Z-217	Sachverständigenmodul Netzwerkforensik	HSAS	K60* (5)	HA	5	-	-
Z-218	Sachverständigenmodul „Auftreten vor Gericht“	Extern	n.n.	n.n.	5	C8	D6
Z-219	Sachverständigenmodul „Einrichten eines forensischen Labors“	Extern	n.n.	n.n.	5	C8	D6
Z-220	Netzsicherheit I	HSAS	HA* (1,5) + R (3,5)	Ü	5	C1	D5
Z-221	Netzsicherheit II *(in Bearbeitung)*	HSAS	n.n.	n.n.	5	C1	-
Z-222	Netzsicherheit III (in Bearbeitung)	HSAS	n.n.	n.n.	5	C1	-
Z-305	SPAM	Extern	K120 (5)		5	-	-
Z-306	Kryptographie 1	Extern	K120 (5)		5	C5	-
Z-307	Kryptographie 2	Extern	K120 (5)		5	C5	-
Z-308	Kryptanalytische Methoden und Werkzeuge	Extern	n.n.		5	C5	-
Z-309	Sicherheit mobiler Systeme	Extern	K120 (5)		5	-	-
Z-401	Computerstrafrecht	GU/UdS	K60 (5)		5	C7/C8	D1/D2/D3/D4/D6
Z-402	Computerstrafprozessrecht	GU/UdS	K60 (5)		5	C7	D1/D2/D3/D4/D6
Z-801	Cloud-Sicherheit und Cloud-Forensik – Angriffsana-	UPA	K60* (5)	HA	5	C6	D1/D2/D3/D5
Z-802	Cloud-Sicherheit und Cloud-Forensik – Zugriffskon-	UPA	K60* (5)	HA	5	C6	D1/D2/D3/D5

* Voraussetzung: Ha bestanden

Änderungen vorbehalten!

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
Pa	=	Projektarbeit
Ü	=	Übungsaufgaben
p.P.	=	praktische Prüfung

c) Dozenten folgender Institutionen:

FAU	=	Friedrich-Alexander-Universität Erlangen-Nürnberg
GU	=	Goethe-Universität Frankfurt am Main
HSAS	=	Hochschule Albstadt-Sigmaringen
RUB	=	Ruhr-Universität Bochum
UdS	=	Universität des Saarlandes
UPA	=	Universität Passau
Extern	=	Andere Institutionen oder institutionsunabhängige Dozenten

4. Modulbeschreibungen

4.1 Friedrich-Alexander-Universität Erlangen-Nürnberg

4.1.1 [Z-101] Methoden digitaler Forensik

Modulbezeichnung:	[Z-101] Methoden digitaler Forensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C6/D1/D2/D3/D4/D5/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Prof. Dr. Felix Freiling
Zeitraum:	17.05.2023 – 24.07.2023; Anmeldeschluss: 05.04.2023
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:	10 bis 30
Studien- und Prüfungsleistungen:	praktische Arbeit zur Analyse von Spuren einer Anwendung (Berechnung der charakteristischen Spurenmenge)
Notwendige Voraussetzungen:	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:	125	Zeitstunden
davon Selbststudium:	70	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 ➢ Charakteristische Spuren: Wie man sie berechnet und was sie bedeuten ➢ Analyse und Qualitätsbetrachtungen echter forensischer Berichte • **Praktische Arbeit:** Berechnung charakteristischer Spuren von einer Reihe künstlicher Anwendungen **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 charakteristische Spuren einer Reihe von Anwendungen berechnet 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 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 Science, 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. Auflage, 2011. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.1.2 [Z-102] Systemnahe Programmierung

Modulbezeichnung:	[Z-102] Systemnahe Programmierung
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C4/D3 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. rer. nat. Werner Massonne
Dozent(in):	Dr. rer. nat. Werner Massonne
Zeitraum:	22.11.2032 – 09.02.2024; Anmeldeschluss: 11.10.2023
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:	10 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:	<u>Präsenzveranstaltung:</u> Vorlesung, Übung <u>Onlineveranstaltung:</u> 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.

4.1.3 [Z-103] Reverse Engineering

Modulbezeichnung:	[Z-103] Reverse Engineering
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C4/D3 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. rer. nat. Werner Massonne
Dozent(in):	Dr. rer. nat. Werner Massonne
Zeitraum:	01.02.2023 – 28.04.2023; Anmeldeschluss: 21.12.2022
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten, die bereits Grundkenntnisse im Bereich Rechnerarchitektur und Betriebssysteme sowie Kenntnisse in der Programmierung mit C 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:	10 bis 30
Studien- und Prüfungsleistungen:	Hausarbeit
Notwendige Voraussetzungen:	Grundkenntnisse im Bereich Betriebssysteme sowie im Bereich Rechnerarchitektur und Assemblerprogrammierung (plattformunabhängig), Programmierkenntnisse insbesondere in der Programmiersprache C.
Empfohlene Voraussetzungen:	Kenntnisse aus dem Modul „Systemnahe Programmierung (Z-102)“, sofern die genannten notwendigen Voraussetzungen nicht gegeben sind.
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
	  o Abgrenzung des Begriffs Reverse Engineering
	  o Einsatzgebiete
	  o Zielsetzung und Grenzen von Reverse Engineering
	
	• Intel x86-IA-32-Architektur und IA-32-Assembler
	  o Architekturmerkmale
	  o Registersatz
	  o Befehlssatz
	  o Adressierung
	  o Stack und Unterprogramm-Aufrufkonventionen
	  o Speicherverwaltung
	  o Befehlsformat
	  o Begleitende Übungen
	
	• Microsoft Windows
	  o Aufbau und Struktur
	  o Anwendungen und Bibliotheken, API-Programmierung
	  o Detaillierte Betrachtung der PE-Struktur zur Programmanalyse: Importe, Exporte, Sections, Windows-Loader, Datenstrukturen
	  o Prozesse, Threads und ihre Datenstrukturen
	  o Exceptions und Exception-Behandlung
	
	• Programmanalyse
	  o Codeerzeugung durch Compiler und Dekompilierung
	  o Optimierungsverfahren
	
	• Werkzeuge zur Programmanalyse: IDA und OllyDbg
	  o Statische Analyse
	  o Dynamische Analyse
	  o Übungen: Analyse einfacher Binaries, einfaches Debugging/Cracking, Sicherheitsprüfungen aushebeln
	
	• Malware und Malware-Analyse
	  o Obfuscation
	  o Verhinderung von Disassemblierung
	  o Malware-Techniken, Packer, Anti-Reverse-Engineering-Methoden
	  o Analyse realer Malware in einer virtuellen Analyseumgebung
	  o Übungen: Malware-Analyse mit IDA
	
	• **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 Intel IA-32-Architektur ist ihnen im Detail vertraut. Sie sind in der Lage, Assemblerprogramme für diese Architektur zu schreiben und zu verstehen. 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.

4.1.4 [Z-104] Live-Analyse - Spurensicherung u. Analyse am laufenden System

Modulbezeichnung:	[Z-104] Live-Analyse - Spurensicherung u. Analyse am laufenden System
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate D3 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Prof. Dr. Felix Freiling
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten
min.-max. Teilnehmerzahl:	10 bis 20
Studien- und Prüfungsleistungen:	Projekt mit Erstellung eines forensischen Berichts (1/3), Präsentation und Verteidigung der Projektergebnisse (2/3)
Notwendige Voraussetzungen:	Linux-Kenntnisse, Grundverständnis von Rechnerarchitektur, Grundverständnis von Betriebssystemen, Grundlagen digitaler Forensik
Empfohlene Voraussetzungen:	Modul „Methoden digitaler Forensik“
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 Leistungspunkt nach ECTS

Lerninhalt und Niveau:

- kurze Einführung in die digitale Forensik
- Theorie: Flüchtigkeitshierarchie
- Vor- und Nachteile von Live-Analyse (vs. Tot-Analyse)
- Anwendungsszenarien von Live-Analyse
- Funktionsweise von Rootkits und deren Gefahren bei der Live Analyse
- Techniken und Qualitätskriterien für Hauptspeicherimages
- Einführung in Volatility und/oder Rekall
- **Übungen:**
  - Hauptspeicheraquise (cold boot, Windows Tools, Live-CD Tools) einüben
  - Qualität der gemachten Images untereinander vergleichen
  - erste Schritte mit Volatility und/oder Rekall
- **Projekt:** Durchführung einer Live Analyse inklusive Analyse eines Hauptspeicherimages u.a. mit Volatility

	○ individuelle Images verteilen und spezifische Fragestellungen untersuchen lassen ○ Fragestellungen beziehen sich auf bereits existierende Volatility-Module ○ Teilnehmer sollen die Module anwenden und die Ergebnisse interpretieren • **Präsenzphase:** Vorstellung und Verteidigung eines Berichts in einer mündlichen Prüfung --- **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	• Die Fähigkeit, die Relevanz von flüchtigen Spuren einzuschätzen, eine Sicherungsstrategie zu entwickeln und die Sicherung durchzuführen. • Die Fähigkeit, die Vertrauenswürdigkeit von Systemen mit Werkzeugen zu prüfen. • Die Fähigkeit, die Qualität von forensischen Berichten zu 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:	• Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2. Auflage, 2004. • Stefan Vömel, Felix Freiling: A Survey of Main Memory Aquisition and Anaysis Techniques for the Windows Operating System. Digital Investigation, 8 (1), 2011. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.1.5 [Z-105] Browser- und Anwendungsforensik

Modulbezeichnung:	[Z-105] Browser- und Anwendungsforensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Dozent(in):	Prof. Dr. Felix Freiling
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Projekt mit Erstellung eines forensischen Berichts (1/3), Präsentation und Verteidigung der Projektergebnisse (2/3)
Notwendige Voraussetzungen:	Linux-Kenntnisse, Programmierkenntnisse, Kenntnisse in Dateisystemen, Grundverständnis von Betriebssystemen
Empfohlene Voraussetzungen:	Modul „Methoden digitaler Forensik“
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	1	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:	▪ Kurze Einführung in die digitale Forensik ▪ Theorie: Black-Box-Analyse von Anwendungen: o Modellbildung auf Basis von Spuren im Dateisystem, Beispiele mit Zeitstempeln o Modellbildung durch dynamische Analyse, Beispiel pyBox/ CWSandbox ▪ Theorie der Inferenz mit Beispielen, grundsätzliche Resultate ▪ Beispiele basierend auf Zeitstempeln ▪ Übungen: o Umgang mit dem Tool fiwalk o Analyse einer bekannten Anwendung: Browser, Instant Messenger, etc. im Labor ▪ **Projekt: Analyse einer unbekannten Anwendung** Jeder Teilnehmer bekommt eine eigene Anwendung in einer speziellen Version mit einer Liste von Operationen, die bezüglich ihrer Spuren im Dateisystem untersucht werden sollen. ▪ Erstellen eines detaillierten Analyseberichts ▪ **Präsenzphase:** Vorstellung der Erkenntnisse in der Gruppe (Referat) ---------- **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	• Die Fähigkeit, die charakteristischen Spuren eines beliebigen Softwaresystems zu ermitteln. • Die Fähigkeit, Standardmethoden der Multimediaforensik anzuwenden.
Lehrveranstaltungen und Lehrformen:	<u>Präsenzveranstaltung:</u> Vorlesung, Übung, Präsentation und Verteidigung der Projektergebnisse <u>Onlineveranstaltung:</u> 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:	• Carsten Willems, Thorsten Holz, Felix Freiling: Toward Automated Dynamic Malware Analysis Using CWSandbox. IEEE Security and Privacy, Band 5, Nr. 2, S. 32-39, 2008. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.1.6 [Z-106] Web Application Security

Modulbezeichnung:	[Z-106] Web Application Security
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Dr.-Ing. Ben Stock
Dozent(in):	Dr.-Ing. Ben Stock
Zeitraum:	30.04.2024 – 19.06.2024; Anmeldeschluss: 20.03.2024
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen, die ein solides Grundverständnis der Sicherheit von Web-Applikationen benötigen; insbesondere angehende Web-Entwickler, die ihre Applikationen von Grund auf sicher gestalten wollen, sowie Betreiber von bestehenden Web-Applikationen, die nachträglich Sicherheitsmechanismen ausrollen wollen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, zur Teilnahme vorher 50% der erreichbaren Punkte in den Übungen
Notwendige Voraussetzungen:	Grundlegendes Verständnis von IT-Sicherheit und bekannten Schutzzielen (z.B. Integrität, Vertraulichkeit)
Empfohlene Voraussetzungen:	Python-Grundkenntnisse sind hilfreich, da Übungsaufgaben primär in Python gestaltet sind.
Sprache:	**Deutsch-Englisch**
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	5	Zeitstunden
Fernstudienanteil:	130	Zeitstunden
davon Selbststudium:	75	Zeitstunden
davon Aufgaben:	50	Zeitstunden
davon Online-Betreuung:	5	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalt und Niveau:

- Angreifermodelle und historische Grundlagen
  - Web-, Netzwerk-, Remote-, Social-Engineering-Angreifer
  - Historie HTTP/HTML
- Grundlegende Technologie/Sicherheit im Web
  - Session-Management: Cookies
  - JavaScript: Syntax, Scoping, DOM
  - Same-Origin Policy
  - Domain Relaxation

- Cross-Origin Kommunikation
  - JSONP: Konzept und Probleme
  - Cross-Origin Resource Sharing (CORS)
  - PostMessages
  - DNS Rebinding
- Cross-Site Scripting
  - Server-side reflected XSS
  - Server-side persistent XSS
  - Client-side reflected XSS
  - Client-side persistent XSS
  - Prävention aller Arten von XSS
  - Content Security Policy
- Cross-Site Attacks
  - Cross-Site Request Forgery (CSRF)
  - Cross-Site Script Inclusion (XSSI)
  - Präventation von CSRF und XSSI
  - Subresource Integrity
  - iFrame Sandboxing
  - Clickjacking und Gegenmaßnahmen
- Sicherheit von Datenbankabfragen
  - SQL Grundlagen
  - SQL Injections (inkl. Blind und Timing-based)
  - NoSQL Injections
  - Prävention von SQL und NoSQL Injection
  - Programmierprojekt in Assembler und C als Hausarbeit
- Code Injection & Friends
  - Command Injection
  - Path Traversal
  - Arbitrary File Upload
  - Deserialization Attacks
  - Template Injections
  - Vorbereitung auf die Hausarbeit
- HTTP Parameter Pollution, XML Insecurity, Server-side Request Forgery
- Infrastruktur-Sicherheit
  - Grundlagen zu TLS/HTTPS
  - Perfect Forward Secrecy
  - Certificate Authorities
  - OCSP & Stapling
  - Certificate Transparency

Die Lerninhalte werden neben der Aufbereitung in Form eines Studienbriefes sowie der Online-Vorlesungen durch passende praktische Übungen unterstützt. Dabei lernen die Studierenden, Schwachstellen zu erkennen, auszunutzen und insbesondere auch zu beheben.

	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).
Angestrebte Lernergebnisse:	Die Studierenden kennen alle relevanten Angriffsklassen gegen client- und server-seitige Web Applikationen. Sie können anhand von Code-Stücken Verwundbarkeiten erkennen und beschreiben und kennen zudem die notwendigen Gegenmaßnahmen. Sie können bestehende Verwundbarkeiten beheben sowie in der Entwicklung neuer Applikationen von vornherein diese unterbinden. Sie kennen zudem für Sicherheitsmechanismen wie CSP solche Funktionalität, die einem Deployment im Wege steht. Durch eigenständiges Bearbeiten der Übungen sind sie außerdem in der Lage, kurze Proof-of-Concept-Exploits zu entwickeln sowie die notwendigen Patches an bestehenden Applikationen durchzuführen.
Lehrveranstaltungen und Lehrformen:	Onlineveranstaltung: Vorlesung, flexible Vertiefung relevanter Themen, Fragen/Antworten Präsenzveranstaltung: Übung Übungsbetrieb: Zusätzlich zum Studienbrief gibt es praktische Übungen, die die Studierenden selbst-ständig (ggf. in Kleingruppen) bearbeiten, um die theoretischen Inhalte zu vertiefen
Anerkannte Module:	
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplatt-form, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Relevante Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.1.7 [Z-107] Mobilfunkforensik

Modulbezeichnung:	[Z-107] / [M-116] Mobilfunkforensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Dr.-Ing. Michael Spreitzenbarth
Dozent(in):	Dr.-Ing. Michael Spreitzenbarth
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur
Notwendige Voraussetzungen:	Programmierkenntnisse in Python und Java, gute Linux-/UNIX-Kenntnisse, gute Englischkenntnisse
Empfohlene Voraussetzungen:	Kenntnisse der forensischen Grundsätze
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	75	Zeitstunden
davon Aufgaben:	50	Zeitstunden
davon Online-Betreuung:	10	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 iOS
   - Aufbau des iOS-Systems
   - Sicherheitskonzept und Secure-Boot
   - Verschlüsselung und Datenschutz

3. Einführung in Mobilfunkforensik für iOS
   - Wie kommt man an die wichtigen Daten?
   - Jailbreaking und andere Zugriffsstrategien
   - Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie?

	4. Aufbau von Android Applikationen • Bestandteile einer Android Applikation (Manifest, Dalvik-Bytecode, Zertifikate, native Bibliotheken, usw.) • Einführung in das Dekompilieren und Reversen von Android-Applikationen • Automatisierte Analysetechniken: Überblick, Einführung und Diskussion statische vs. dynamische Analyse • Einführung in die Tools: Android Studio, JadX, Hashcat 5. Obfuskierung • Einführung in Obfuskierung • String-Obfuscation (XOR, Crypt, etc.) • Junkbytes zum Verwirren der Disassembler • Kollision mehrerer Apps zum Verschleiern der Schadfunktion **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	**Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse über den Aufbau des Android und iOS Betriebssystems. Sie sind in der Lage Android und iOS Mobiltelefone zu analysieren und Spuren auf diesen Geräten zu sichern. Ebenso sind sie in der Lage Android-Applikationen zu analysieren und verdächtiges Verhalten zu identifizieren. **Methodenkompetenz:** Die Studierenden beherrschen die Arbeitstechnik, mit bekannten Tools und Werkzeugen im Bereich Forensik und Android-Applikations-Analyse umzugehen. Weiter beherrschen sie die Problemlösefähigkeit, ein Android-Programm auf sein Verhalten zu untersuchen. **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung, Präsentation 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 und kann dem Studienbrief entnommen werden.

4.2 Hochschule Albstadt-Sigmaringen

4.2.1 [Z-201] Applied Computer Systems / [M-101] Einführung in die Informatik

Modulbezeichnung:	[Z-201] Applied Computer Systems / [M-101] Einführung in die Informatik
Zertifikatsabschluss:	Hochschulzertifikat mit 5 ECTS-Punkten
Verwendbarkeit:	Gesamtzertifikate C2/D1/D2/D3/D4 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit geringen IT-Kenntnissen
min.-max. Teilnehmerzahl:	10 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 Rechnem interpretieren und umwandeln. Die Grundzüge von Rechnern und die Aufgaben unterschiedlicher Software können erläutert werden. Grundlegende Kenntnisse 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.

4.2.2 [Z-202] Programmieren im IT-Security-Umfeld mit Python 1

Modulbezeichnung:	[Z-202] Programmieren im IT-Security-Umfeld mit Python 1
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C2/D2/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 10 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit grundlegenden IT-Kenntnissen, keine bis geringe Programmierkenntnisse
min.-max. Teilnehmerzahl:	10 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:	<u>Präsenzveranstaltung:</u> Vorlesung, Übung <u>Onlineveranstaltung:</u> 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.

4.2.3 [Z-203] Penetration Testing mit Python

Modulbezeichnung:	[Z-203] Penetration Testing mit Python
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C2/C4/D1/D2/D4/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 10 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit grundlegenden IT-Kenntnissen, keine bis geringe Programmierkenntnisse
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Kenntnisse aus dem Modul „Python 1 – Programmierung und Forensik (Z-203)“ 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 7 (Master).**
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 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.

4.2.4 [Z-204] Grundlagen Datenträgerforensik

Modulbezeichnung	[Z-204] Grundlagen Datenträgerforensik
Zertifikatabschluss	Hochschulzertifikat
Verwendbarkeit	Gesamtzertifikate D2 und in ausgewählten Studiengängen
Modulverantwortliche(r)	Prof. Dr. Martin Rieger
Dozent(in)	Prof. Dr. Martin Rieger
Zeitraum	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 10 Wochen
Leistungspunkte	5 ECTS-Punkte
Zielgruppe	Personen mit fortgeschrittenen IT-Kenntnissen
Min.-max. Teilnehmerzahl	10 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	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.

4.2.5 [Z-205] Vertiefung Datenträgerforensik

Modulbezeichnung:	[Z-205] Vertiefung Datenträgerforensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate D2 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit fortgeschrittenen IT-Kenntnissen
Min.-max. Teilnehmerzahl	10 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:	<u>Präsenzveranstaltung:</u> Vorlesung, Übung <u>Onlineveranstaltung:</u> 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.

4.2.6 [Z-206] Internettechnologien

Modulbezeichnung:	[Z-206] Internettechnologien
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate D1/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne Informatik-Ausbildung
min.-max. Teilnehmerzahl:	10 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.

4.2.7 [Z-208] Forensische Analyse eines Windows-Systems

Modulbezeichnung:	[Z-208] Forensische Analyse eines Windows-Systems
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C3/D4/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	voraussichtlich zwischen Mai und November; Dauer: ca. 14 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne Informatik-Ausbildung, Personen mit geringen IT-Kenntnissen
min.-max. Teilnehmerzahl:	10 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:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 Leistungspunk nach ECTS	22	% = Präsenz

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 und Rechtesystem, Reguläre Ausdrücke, Grundlagen der (Windows-) Netzwerktechnik, Ermitteln der Netzwerkeigenschaften des Rechners ▪ **Spezifische Strukturen und Analysemethoden zu Windows-Systemen** forensisch relevante Verzeichnisse und Dateien, Schattenkopien, Speicherabbilder gewinnen und auswerten, Protokolldateien gewinnen, Windows-Zugriffsrechte analysieren und verändern, Schlüsselwortsuche, Filecarving, Schlupfspeicher extrahieren, indizieren von Metadaten, Forensische Arbeitsweise im Windows-System ▪ **Forensische Erkenntnisse aus der Registry** Aufbau, SIDs, SAMs, GUID Forensisch relevante Registry-Einträge, Werkzeuge zur Registry-Analyse Antiforensische Maßnahmen ▪ **Logfile-Analyse** NTFS-Journal-Protokollierung, Struktur der Logging-Einträge, Auswertung, Windows-Event-Log, Anwendungs- und Dienstprotokolle, Security-Log, Setup-Log, Überwachungsrichtlinien Antiforensische Maßnahmen ▪ **Forensische Untersuchung von Internetdiensten** Peer-to-Peer-Aktivitäten aufdecken, Skype-Accounts untersuchen Client-Datenbanksystem, SQLite-Anwendungs-Artefakte auswerten (Skype, Firefox, Chrome), Microsoft-Anwendungs-Artefakte auswerten (Internet Explorer, Edge, Outlook) ▪ **Forensische Analyse von Arbeitsspeicher und Windows-Live-Artefakten** Flüchtige Informationen ermitteln, Systemzeit auslesen, eingeloggte Benutzer, offene Dateien, Netzwerkverbindungen, Prozessinformationen, Zwischenablage, Dienste/Treiber-Informationen, Erstellung eines Arbeitsspeicherabbilds, Arbeitsspeicheranalyse mit dem Volatility-Framework und mit Rekall, Artefakt-analyse ▪ **Forensische Fallbeispiele** o <u>Analyse eines Rechners mit Malware-Befall:</u> Indicators of Compromise, Schrittweise Analyse mit automatischen und händischen Methoden, Bereinigung des Rechnersystems o <u>Der Fall Evil Knievel:</u> Forensische Untersuchung auf Illegalen Handel, Auswertung vieler Windowsspezifischer Artefakte, Umgehen mit antiforensischen Maßnahmen **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**

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 der Registry, der Logdateien 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.

4.2.8 [Z-209] Forensische Analyse eines Unix-Systems

Modulbezeichnung:	[Z-209] Forensische Analyse eines Unix-Systems
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C3/D4/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	voraussichtlich zwischen März und Juni; Dauer: ca. 14 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit geringen IT-Kenntnissen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Vertraut mit Unix-Benutzersicht, Kenntnisse des forensischen Arbeitens
Empfohlene Voraussetzungen:	Kenntnisse im Umgang mit Rechnern, dem Internet und dem Unix-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:	125	Zeitstunden
davon Selbststudium:	70	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 Leistungspunk nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:	In diesem Modul werden Ihnen verschiedene Aspekte des Betriebssystems Unix bzw. Linux vermittelt, die es Ihnen ermöglichen Untersuchungen forensischer Art oder zur IT-Sicherheit an den genannten Betriebssystemen durchzuführen. Grundlage hierfür ist das Verständnis über wichtige Konzepte und Eigenschaften von Unix bzw. Linux. In den einzelnen Studienbriefen werden verschiedene Bereiche unixoide Betriebssysteme betrachtet und analysiert. ▪ Das Unix-Rechnersystem Grundlegende Begrifflichkeiten, Unix-Varianten, Umgang mit der grafischen Oberfläche und dem Terminal, Dateisysteme, Verzeichnisstruktur, Passwort- und Schattendatei, Zugriffsrechte und Zugriffskontrolle Erstellung von und Arbeiten mit Bash-Skripten Erstellung von und Arbeiten mit Python-Skripten ▪ Struktur und Analyse von unixoiden Systemen Hardwareinformationen, Systemprozesse und Leistungsüberwachung, Untersuchungen an Prozessen und Threads, Systeminformationen, Dienste, reguläre Ausdrücke, Suchprogramme, Untersuchung zu Rootkits, Nachweis von Rootkits ▪ Logfile-Analyse: Rsyslog-Daemon-Analyse und Konfiguration, Logfile-Analyse mit Bordmitteln, mit petit und logwatch, Auswertung von Benutzeranmeldungen und Anmeldeversuchen, von USB-Benutzung, von WLAN-Anmeldung, von SW-Installation ▪ Live-Analyse Flüchtige Informationen ermitteln, Systemzeit auslesen, eingeloggte Benutzer, offene Dateien, Netzwerkverbindungen, Prozessinformationen, Dienste/Treiber-Informationen ▪ Forensische Analyse von Arbeitsspeichern: Erstellen eines Arbeitsspeicherabbilds, Möglichkeiten der Erfassung, Erstellen von Profilen für das Volatility Framework, Analyse mit dem Volatility Framework, Analyse mit Rekall ▪ Linux Serverdienste: Installation von Apache2 Webserver und Wordpress, Cyber-Angriffe auf Wordpress und dessen Nachweis, Datengewinnung aus MySQL-Datenbanken, Auswertung von E-Mails, Mailservern, Auswertung von Routern, Firewalls und Netzwerkkomponenten ▪ Fallbeispiele: o Bau, Suche und Nachweis eine Rootkits o Analyse eines Linux-Livesystems mittels eigener Skripte o Möglichkeiten von Zeitgeist/Zeitgeist-Explorer an beispielen o Forensische Arbeitsspeicheranalyse eines kompromittierten Servers o Fallbeispiel (NAS) QNAP Asservat o Übung Fallbeispiel Datenträger

	Die Hackergruppe "Who Are You" steht im Verdacht illegales Bildmaterial zu besitzen und zu vermarkten. Es wird vermutet, dass der Kern der Gruppe aus drei Tätern besteht. Da es sich um eine Hackergruppe handelt, wird angenommen, dass die Täter sich bei der Kommunikation und dem Datentransfer für unterschiedlichste Wege entschieden haben. (SSH, MySQL, Email, Webserver, USB-Sticks). Es wird angenommen, dass die Täter auch das Bildmaterial auf mehreren Wegen vertreiben. (Webserver und USB-Sticks). Um möglichst wenig individuelle Spuren zu hinterlassen, haben sich die drei Täter universelle Benutzer und Passwörter ausgedacht. ---------- **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Die Studierenden sind in der Lage die Unix-Bordmittel sowie weitere Werkzeuge souverän mit Terminal oder über eine GUI anzuwenden. Es ist Ihnen möglich zwischen den Inhalten der einzelnen Verzeichnisse zu differenzieren. Zudem können Sie die Aufgabe spezieller Dateien beschreiben und analysieren. Sie können allgemeine Informationen zum Betriebssystem ermitteln. Auf der Grundlage von Regulären Ausdrücken und anderer Möglichkeiten können sie das Suchen optimieren. Zudem können Sie weitere Vertreter der Desktopsuche anwenden und die Qualität der Suchergebnisse durch einen direkten Vergleich beurteilen. Sie wissen, wie das Logging unter Linux von statten geht und können die wichtigsten Logdateien benennen und forensisch korrekt auswerten. Sie können flüchtigen Informationen definieren und diese an einem laufenden System unter forensischen Gesichtspunkten auslesen. Sie sind in der Lage, ein Speicherabbild zu erstellen und dieses zu analysieren. Sie kennen einige Aspekte von Linux Server-Umgebungen sowie verschiedenen unter Linux betriebenen Serverdienste. Sie können die damit verbundenen Spuren erheben und auswerten. Sie sind in der Lage ein komplexes unixoides Asservat mit flüchtigen und nichtflüchtigen Spuren forensisch korrekt zu analysieren und die Ergebnisse in einem Bericht darzustellen. 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:	<u>Präsenzveranstaltung:</u> Vorlesung, Übungen <u>Onlineveranstaltung:</u> 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:	• Herold, H; Lurz, B; Wohlrab, J.: Grundlagen der Informatik. München; Boston [u.a.]: Pearson Studium. • Tanenbaum, A. S. (2006): Computerarchitektur : Strukturen - Konzepte – Grundlagen. München; [Boston {u.a.]: Pearson Studium • Brian Ward: How Linux Works: What Every Superuser Should Know No Starch Press; Auflage: 2 (11. November 2014) • Michael Kofler: Linux: Das umfassende Handbuch. Rheinwerk Computing; Auflage: 14 (30. November 2015) • Nemeth, Evi, Snyder, Garth, Hein, Trent R., Whaley, Ben: UNIX and Linux System Administration Handbook Prentice Hall 4th Edition (2011) • Dr. Philip Polstra: Linux Forensics CreateSpace Independent Publishing Platform; Auflage: 1 (13. Juli 2015). Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.9 [Z-210] Forensische Analyse eines MacOS-Systems

Modulbezeichnung:	[Z-210] Forensische Analyse eines MacOS-Systems
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C3/D4/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	voraussichtlich zwischen November 2024 und Februar 2025; Dauer: ca. 14 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit geringen IT-Kenntnissen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Kenntnisse im Umgang mit Rechnern, dem Internet und dem macOS-Betriebssystem (mit der Nutzersicht vertraut)
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 Leistungspunk nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:

In diesem Modul werden Ihnen verschiedene Aspekte des Betriebssystems MacOS vermittelt, die es Ihnen ermöglichen Untersuchungen forensischer Art oder zur IT-Sicherheit an den genannten Betriebssystemen durchzuführen. Eine Grundlage hierfür ist das Verständnis über wichtige Konzepte und Eigenschaften von Linux, FreeBSD und vor allem den MacOS-spezifischen Komponenten. In den einzelnen Studienbriefen werden verschiedene Bereiche des MacOS-Betriebssystems betrachtet und analysiert.

- **Apple-Hardware**
  Apple Inc. Firmengeschichte, Desktop und mobile Computer, Set Top Boxen, Server, tragbare Geräte, Software, Hardwarearchitekturen (Litte/Big Endian), Datenübertragungsschnittstellen

- **MacOS-Betriebssystem**
  Klassisches Mac OS/System 7, OPENSTEP, macOS Versionen (Client), macOS Versionen (Server), MacOSX,
  Betriebssystemarchitektur (Kernel, Userland),
  Property Lists, AppleScript,
  Sicherheitsfunktionen (Sandboxing, XPC, Gatekeeper, Xprotect, Fileattributes)
  Dateisysteme HFS+, APFS
  Forensisch bedeutsame Artefakte, die durch MacOS und das Dateissystem erzeugt werden.

- **Persistente Spuren:**
  Die MacOS Verzeichnisstruktur (Benutzer, Library, Spotlight, Netzwerkkonfiguration, Drucker, Repositoryverwaltungen),
  Nutzerdomäne (Benutzerverwaltung, Applikationsstruktur, Zeitstempel, Apple Applikationen, Papierkorb, Backups, Virtualisierung, Zuletzt verwendete Objekte)
  Spezifische Formate und deren Auswertung
  Forensische Analyse der persistenten Spuren an Beispielen

- **Netzwerkbasierte Dienste:**
  iCloud Services, Mobile Device Management, Synchronisation iCloud und lokale Verzeichnisse
  Netzwerkdienste in der lokalen Domäne (AFP, SMB, VNC, FTP, SSH, ARD, Webserver)

- **Methoden digitaler Forensik im MacOS-Umfeld:**
  Investigativer Prozess nach Casey
  MacOS Sicherungsvorgehen,
  Liveanalyse,
  Post Mortem Analyse (Disk Arbitration, Verschlüsselung, Livesystem)

- **Nichtpersistente Spuren und Forensische Analyse von Arbeitsspeichern:**
  Einführung in die RAM-Analyse, Struktur des Arbeitsspeichers,
  Erstellen eines Arbeitsspeicherabbilds,
  Möglichkeiten der Erfassung, Erstellen von Profilen für das Volatility Framework,
  Analyse mit dem Volatility Framework, Analyse mit Rekall

- **Fallbeispiele:**
  Analyse eines MacOS-Livesystems mittels eigener Skripte
  Forensische Arbeitsspeicheranalyse eines kompromittierten Clients

  Übung Fallbeispiel Datenträger:
  Forensische Untersuchung auf Illegalen Handel, Auswertung vieler MacOS-spezifischer Artefakte, Umgehen mit antiforensischen Maßnahmen

---

Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).

Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls kennt der Student die verschiedenen Produkte der Apple Inc. Hierbei werden die Kategorien Hard- bzw. Software genauer erläutert. Abschließend wurden dem Studenten die Unterschiede zwischen verschiedenen Hardwarearchitekturen und Schnittstellen vermittelt. Nach erfolgreichem Abschluss des Moduls erlernte der Student die einzelnen macOS Betriebssystemversionen. Neben der Versionshistorie der Client/ Serverbetriebssysteme, wird ein Einblick in die Entstehungsgeschichte und die verschiedenen Einflüsse vom heutigen MacOS gegeben. Nach erfolgreichem Abschluss des Moduls wurden dem Student die einzelnen macOS Architekturschichten vermittelt. Weiter wurde der Umgang mit betriebssystemspezifischen Dateiformaten und Skriptsprachen gelehrt. Zum zentralen Bestandteil dieses Moduls gehört das Sicherheitskonzept, welches anhand von Beispielen und Kontrollaufgaben vermittelt wird. Abschließend wird ein Einblick in das Dateisystem HFS+ gegeben. Nach erfolgreichem Abschluss des Moduls erlernte der Student die System- bzw. Nutzerdomäne von macOS kennen. Dabei beschäftigt sich der Student detailliert mit den Verzeichnisstrukturen und Datenformaten und den Loggingmechanismen. Somit ist er in der Lage die MacOS-spezifischen persistenten Spuren zu bergen und zu analysieren. Nach erfolgreichem Abschluss des Moduls wurden dem Studenten die verschiedenen netzwerkbasierten Dienste im Betriebssystem MacOS vermittelt. Dabei wird zwischen proprietären Cloudlösungen und lokalen Services unterschieden. Weiter ist die zentrale Verwaltung mobiler Geräte vertraut. Damit ist der Student in der Lage, die mit der Cloud in Verbindung stehenden Spuren forensisch auszuwerten. Nach erfolgreichem Abschluss des Moduls lernte der Student den klassischen investigativen Prozess nach Casey kennen. Praktische Anwendung findet das erlernte Wissen in verschiedenen Macintosh Sicherungsvorgehen und Liveanalysen. Abschließend werden Möglichkeiten der Post Mortem Analyse angewendet. Nach erfolgreichem Abschluss des Moduls lernte der Student die Sicherungsvorgehen eines Macintosh Computers von nicht persistenten Spuren kennen. Im Anschluss wird die Analyse mittels dem Volatility Framework angewendet
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:	• Jonathan Levin. Mac OS X and IOS Internals: To the Apple's Core. John Wiley & Sons • Topher Kessler. EFI firmware protection locks down newer Macs. Website,. https://www.cnet.com/news/efi- firmware- protection- locks- down- newer- macs/.

- Maximillian Dornseif. Vorlesung Computerforensik. Friedrich-Alexander Universität Erlangen-Nürnberg,
- Brian Ward: How Linux Works: What Every Superuser Should Know No Starch Press; Auflage: 2 (11. November 2014)
- Marc Brandt. Forensische Analyse von Mac OS X. Hochschule Albstadt-Sigmaringen, 2016.
- Brian Carrier. File system forensic analysis. Addison-Wesley Pro-fessional, 2005.
- Eoghan Casey. Handbook of digital forensics and investigation. Academic Press, 2009.
- A. Singh. Mac OS X Internals: A Systems Approach. Pearson Edu-cation, 2006. ISBN 9780132702263. URL https://books.google.co.il/books?id=K8vUkpOXhN4C.
- Jesse Varsalone. Mac OS X, iPod, and iPhone forensic analysis DVD toolkit. Syngress, 2008.

Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.10 [Z-211] Forensische Analyse von Netzwerken

Modulbezeichnung:	[Z-211] Forensische Analyse von Netzwerken
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 14 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit Kenntnissen in TCP/IP-Rechnernetzen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Kenntnisse in TCP/IP-Rechnernetzen
Empfohlene Voraussetzungen:	Kenntnisse in TCP/IP-Rechnernetzen
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 Leistungspunk nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:

Grundlagen der Netzwerkforensik

- Forensische Untersuchungen an Rechnern in Netzwerken
- Datengewinnung aus aktiven Netzkomponenten
- Datengewinnung aus dem Netzwerkdatenstrom mittels Netzwerk-Sniffer
- IT-Strukturen
- Network Security Monitoring (NSM) Vorgehensmodell

Post Mortem-Analyse von Server-Diensten und -Komponenten

- Analyse von Logdateien
- Sicherung und Analyse von Serverdiensten
- Analyse Microsoft Serverdiensten
- Forensische Auswertung von Routern und anderen Netzwerkkomponenten

	Live-Analyse von Server-Diensten und -Komponenten ▪ Aufbereitung von Server-Sicherungen zur Virtualisierung ▪ Live-Analyse laufender Systeme am Beispiel ▪ Erstellung und Analyse eines Arbeitsspeicherabbildes ▪ Analyse von IoT-Systemen ▪ Analyse von Schadsoftware **Internet- und Cloudforensik** ▪ Internet- und Cloudspuren im Client ▪ Geräte im Netzwerk erkennen ▪ Sichern von Clouddaten am Beispiel Facebook ▪ Kryptowährungen **Forensische Fallbeispiele** ▪ DoS-Angriff auf virtuelle Netzwerkumgebung: Auswertung der Spuren ergibt das Schadensbild Spuren zum Tathergang und zu den Tätern ▪ ARP-Spoofing- Angriff in virtueller Netzwerkumgebung analysieren: Auswertung der Spuren ergibt das Schadensbild Spuren zum Tathergang und zu den Tätern ▪ Browser-Analyse und Facebook-Analyse: Nachweis von illegalem Handel einer Bande ▪ Die Milka-Bande: Nachweis von illegalem Handel einer Bande in einer ausgedehnten virtuellen Netzwerkumgebung; als Methoden werden u.a. Netzwerkmitschnitte, Analyse der mitschnitte, sowie Eindringen und Zugriff auf Server angewendet. **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Mit diesem Modul soll der Teilnehmer in die Lage versetzt werden, die vielfältigen Quellen rund um das Rechnernetz forensischen ausnutzen zu können. Teilnehmer lernen, das Netzwerk mit seinen Teilnehmern zu erfassen, zu beobachten und zu analysieren. Wesentlich ist, Netzwerkdaten aufzeichnen und hinsichtlich der Metadaten und ggf., hinsichtlich der Inhaltsdaten analysieren zu können. Hinzu kommt die Auswertung aktiver Netzgeräte, wie z. B. Router und Switches, die Aussagen über das "Wann“ und "Woher" von Daten ermöglichen können. Essentielle Dienste, die von Servern angeboten werden, wie z. B. Webserver und Proxyserver müssen analysiert werden mit dem Ziel, Aussagen machen zu können z. B. über die beteiligten Kommunikationspartner und die transportieren Daten. Die Teilnehmer wenden eine forensische Arbeitsweise an, die darin besteht, Informationen aus laufenden Systemen zu gewinnen, wie z. B. der laufenden Prozesse, der bestehenden Netzwerkverbindungen oder der verschlüsselten Container. Dazu können einerseits die Systeme im laufenden Betrieb analysiert werden. Andererseits ist es häufig günstiger, die laufenden Systeme einzufrieren", d. h. einen Arbeitsspeicherdump oder sogar ein virtualisiertes Abbild des Systems zu gewinnen und spätere Analysen an diesem Abbild vorzunehmen.

	Die Teilnehmer lernen die Nutzung von netzwerkzentrierten Anwendungen, wie z. B. Messengerdienste, Browser, Clouddienste oder soziale Netzwerke aus den Spuren sowohl in der Cloud als auch auf den Clients zu bergen geborgen und zu analysieren. 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, 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:	• Andrew Tanenbaum (2012): Compternetzwerke. Verlag Pearson Studium; 5. Auflage: • Claudia Eckert (2016): IT-Sicherheit Strukturen - Konzepte – Grundlagen. Verlag De Gruyter Oldenbourg, 9. Auflage.) • Jörg Schwenk (2014): Sicherheit und Kryptographie im Internet. Verlag: Springer Vieweg, 4. Auflage: • S. Davidoff, J. Ham (2012): Network Forensics. Verlag Prentice Hall Interna-tional. • Chris Sanders, Jason Smith (2013): Applied Network Security Monitoring: Collection, Detection, and Analysis. Verlag: Syngress. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.11 [Z-212] Vertiefung Netzsicherheit

Modulbezeichnung:	[Z-212] Vertiefung Netzsicherheit
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C6/D1/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 10 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit Kenntnissen in TCP/IP-Rechnernetzen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Netzwerkgrundlagen, Kenntnisse in TCP/IP-Rechnernetzen
Empfohlene Voraussetzungen:	Netzwerkgrundlagen, Kenntnisse in TCP/IP-Rechnernetzen
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 Leistungspunk nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:

Netzwerkprotokolle
- Modelle
- Schichten und Veranschaulichung von Protokollen
- Mitschnitt von Netzwerkverkehr

Datengewinnung und Analyse aus dem Netzwerkdatenstrom
- Analyse der Netzwerkinfrastruktur
- Aufzeichnungsgeräte
- Aufzeichnungsarten
- Analyse von Mitschnitten

IT-Netzwerkstrukturen und IT-Netzwerkkomponenten
- Netzwerk-Strukturen
- Netzwerkadapter

	▪ Datengewinnung aus aktiven Netzkomponenten ▪ Analyse von Log-Dateien ▪ Firewalls ▪ Beispiel IPFire **Post Mortem-Analyse von Server-Diensten und -Komponenten** ▪ Sicherung und Analyse von Serverdiensten (Firewall, Web-Proxy, IDS, DHCP) am Beispiel IPFire **Live-Analyse von Server-Diensten und Komponenten** ▪ Virtualisierung von Rechnersystemen ▪ Analyse des laufenden Systems ▪ Live-Sicherung ▪ Arbeitsspeicheranalyse ▪ Analyse von Schadsoftware **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Mit diesem Modul soll der Teilnehmer in die Lage versetzt werden, die vielfältigen Quellen rund um das Rechnernetz forensischen ausnutzen zu können. Das beginnt damit, das Netzwerk mit seinen Teilnehmern erfassen, beobachten und analysieren zu können. Wesentlich ist, Netzwerkdaten aufzeichnen und hinsichtlich der Metadaten und ggf. hinsichtlich der Inhaltsdaten analysieren zu können. Hinzu kommt die Auswertung aktiver Netzgeräte, wie z. B. Router und Switches, die Aussagen über das Wann und Woher von Daten ermöglichen können. Essentielle Dienste, die von Servern angeboten werden, wie z. B. Webserver und Proxyserver müssen analysiert werden mit dem Ziel, Aussagen machen zu können z. B. über die beteiligten Kommunikationspartner und die transportieren Daten. Häufig besteht eine forensische Arbeitsweise darin, Informationen aus laufenden Systeme zu gewinnen, wie z. B. der laufenden Prozesse, der bestehenden Netzwerkverbindungen oder der verschlüsselten Container. Dazu können einerseits die Systeme im laufenden Betrieb analysiert werden. Andererseits ist es häufig günstiger, die laufenden Systeme „einzufrieren“, d. h. einen Arbeitsspeicherdump oder sogar ein virtualisiertes Abbild des Systems zu gewinnen und spätere Analysen an diesem Abbild vorzunehmen. Die Nutzung von netzwerkzentrierten Anwendungen, wie z. B. Messengerdienste, Browser, Clouddienste oder soziale Netzwerke, hinterlässt sowohl in der Cloud als auch auf den Clients forensische Spuren, die geborgen und analysiert werden müssen.
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.

4.2.12 [Z-213] Incident Response & Malware Defence

Modulbezeichnung:	[Z-213] Incident Response & Malware Defence
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate D1/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Martin Rieger
Dozent(in):	Prof. Dr. Martin Rieger
Zeitraum:	18.09.2024 – 29.11.2024; Anmeldeschluss: 31.07.2024
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Personen mit Kenntnissen in TCP/IP-Rechnernetzen
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Netzwerkgrundlagen, Kenntnisse in TCP/IP-Rechnernetzen
Empfohlene Voraussetzungen:	Netzwerkgrundlagen, Kenntnisse in TCP/IP-Rechnernetzen
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 Leistungspunk nach ECTS	22	% = Präsenz

Lerninhalt und Niveau:

Bedrohungen der IT-Sicherheit:
- Modelle
- Schichten und Veranschaulichung von Angriffen

Grundlagen von Hacking-Techniken:
- Schadsoftware
- Bedrohungen im Rechnernetz und Internet
- Social Engineering
- Hardware-Tools
- Router-Konfiguration

IT-Verteidigungsmaßnahmen:
- BSI-Sicherheitsprozess
- Bausteine zur IT-Sicherheit
- Incident Response

	▪ Network Security Monitoring **Penetration Testing:** ▪ Methodik von Penetrationstests ▪ Nmap ▪ Passwort-Cracking ▪ ARP-Spoofing ▪ DNS-Spoofing und Phishing **Fallbeispiele zur Behandlung netzwerkzentrierter Angriffe:** ▪ Ransomware: Implementierung und Incident Response ▪ Keylogger: Implementierung und Incident Response ▪ Prozessermittlung **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Dieses Modul soll zeigen, wie einfach es in vielen Fällen ist, einen Angriff durchzuführen. Wir wollen vermitteln, worauf ein erfolgreicher Angriff basiert: ▪ Ansatz des Angriffs ▪ Mechanismen von Schadsoftware ▪ Stufenweises Vorgehen ▪ Schadsoftware tarnt sich ▪ Schadsoftware verankert sich im System ▪ Schadsoftware ist „fernsteuerbar“ Es soll auch gezeigt werden, wie vorgegangen werden kann, wenn ein Angriff bereits eingetreten ist oder eventuell sogar noch aktiv ist. ▪ Incident Response, „Feuerwehr“ ▪ Forensische Ermittlungen Die bekannten Prinzipien zum Aufbau sicherer digitaler Infrastruktur werden erlernt: ▪ Bausteine sicherer digitaler Netze: Zutrittskontrolle, Zugriffskontrolle, Verschlüsselung, Firewalls ▪ Analyse und Design der erforderlichen Sicherheitsmaßnahmen ▪ Schutzmaßnahmen für Clients ▪ Konzepte zur Netzwerksicherheit Wir lernen den Nutzen einer ständigen Überwachung der Netzwerksicherheit kennen: ▪ Network Security Monitoring ▪ Vorgänge erfassen ▪ Vorgänge detektieren ▪ Vorgänge analysieren Es ist sinnvoll, Systeme selbst zu testen (Penetrationstests) und somit bereits möglichst früh einen Großteil der Schadsoftware auszusperren. ▪ Schließen der Sicherheitslücken ▪ Schulung der Mitarbeiter

Lehrveranstaltungen und Lehrformen:	<u>Präsenzveranstaltung:</u> Vorlesung, Übungen <u>Onlineveranstaltung:</u> 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.

4.2.13 [Z-214] Forensische Analyse eines Windows-Systems für Sachverständige

Aktuelle Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-208] Forensische Analyse eines Windows-Systems“.

4.2.14 [Z-215] Forensische Analyse eines Unix-Systems für Sachverständige

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-209] Forensische Analyse eines Unix-Systems“.

4.2.15 [Z-216] Forensische Analyse eines MacOS-Systems für Sachverständige

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-210] Forensische Analyse eines MacOS-Systems“.

4.2.16 [Z-217] Forensische Analyse von Netzwerken für Sachverständige

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-211] Forensische Analyse von Netzwerken“.

4.2.17 [Z-218] Sachverständigenmodul „Auftreten vor Gericht“

Modulbezeichnung:	[Z-218] Sachverständigenmodul „Auftreten vor Gericht“
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C8/ D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	N.N.
Dozent(in):	N.N.
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 14 Wochen
Leistungspunkte	5 ECTS
Zielgruppe:	Aspiranten der IT-Forensik-Sachverständigentätigkeit aus Behörden, Unternehmen oder als Selbständige
min.-max. Teilnehmerzahl:	10 bis 20
Studien- und Prüfungsleistungen:	Seminararbeit, Referat, ggf. nachgeschaltete Prüfung zum Sachverständigen
Notwendige Voraussetzungen:	Langjährige Erfahrung im Umfeld der IT-Forensik
Empfohlene Voraussetzungen:	Langjährige Erfahrung im Umfeld der IT-Forensik
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	

Präsenzstudium:	ca. 25	Zeitstunden
Fernstudienanteil:	125	Zeitstunden
davon Selbststudium:	45	Zeitstunden
davon Aufgaben:	60	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
davon individuelle Prüfungs-vorbereitung	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS		

Lerninhalt und Niveau:

Formale Inhalte

- Aufgabe eines Sachverständigen
- Selbstverständnis und Rolle eines Sachverständigen
- Vorbereitung zur Sachverständigenprüfung
- Rollen der Beteiligten vor Gericht
- Typisches Verhalten Beteiligter vor Gericht (Fachanwalt, Staatsanwalt, Richter, Zeugen)

Fachliche Inhalte

- Normenwerk „ISO/IEC 27037:2012" Leitlinien für die Identifizierung, Sammlung, Erfassung und Archivierung elektronischer Beweise

	• Typische Zusammenstellung von IT-Beweismitteln - Spuren in Datenträgern und Dateien (reguläre Inhalte, gelöschte Inhalte, verschlüsselte Inhalte) - Spuren im System (Registry, Log-Files, ...) - Spuren aus dem Internet (Browser-Cache, History, Mail) - Spuren mobiler Geräte (Smartphones, Tabletts) • Typische Arbeitsweise von IT-Ermittlern - Beweismittel-Erfassung nach Sparten - Beweismittel-Analyse nach Sparten - Bewertung der Beweismittel - Typische Stärken / Schwächen der Ermittlung • Bewertung der Beweismittel - Zusammenführung der Beweismittel an Fallbeispielen - Wertung der Beweismittel an Fallbeispielen • Bewertung der Ermittlung - Überprüfung der Einhaltung der Norm - Überprüfung auf Einhaltung der „Regeln der Kunst“ - Fallbeispiele --- **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls kennt der Studierende die Aufgaben des Sachverständigen für IT-Forensik und er ist mit den Rollen der Prozessbeteiligten vertraut. Der Studierende wird auf die Sachverständigenprüfung vorbereitet. Er ist in der Lage, die Qualität forensischer Beweismittel und deren Aufbereitung durch Ermittler zu beurteilen.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung Onlineveranstaltung: Vorlesung
Anerkannte Module:	
Medienformen:	Vorlesung mit Beamer, Studienbriefe, Onlinematerial in Lernplattform, Übungen und Tests über Lernplattform, Onlinekonferenzen, Chat und Forum in Lernplattform
Literatur:	Normenwerk „ISO/IEC 27037:2012" Leitlinien für die Identifizierung, Sammlung, Erfassung und Archivierung elektronischer Beweise; Patrick Engebretson (2013): The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress Media; Thomas Wilhelm (2013): Professional Penetration Testing: Creating and Learning in a Hacking Lab: 1 Verlag: Syngress; Manuel Christensen (2012): Certified Professional Penetration Tester (eCPPT) Secrets To Acing The Exam and Successful Finding And Landing Your Next Certified Professional Penetration Tester (eCPPT) Certified Job Verlag: tebbo Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.18 [Z-219] Sachverständigenmodul „Einrichten eines forensischen Labors“

Modulbezeichnung:	[Z-219] Sachverständigenmodul „Einrichten eines forensischen Labors“
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C8/ D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	N.N.
Dozent(in):	N.N.
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 14 Wochen
Leistungspunkte	5 ECTS
Zielgruppe:	Aspiranten der IT-Forensik-Sachverständigentätigkeit aus Behörden, Unternehmen oder als Selbständige
min.-max. Teilnehmerzahl:	10 bis 20
Studien- und Prüfungsleistungen:	Klausur, Seminararbeit mit Referat; ggf. nachgeschaltete Prüfung zum Sachverständigen
Notwendige Voraussetzungen:	Langjährige Erfahrung im Umfeld der IT-Forensik
Empfohlene Voraussetzungen:	Langjährige Erfahrung im Umfeld der IT-Forensik
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	

Präsenzstudium:	33	Zeitstunden
Fernstudienanteil:	117	Zeitstunden
davon Selbststudium:	62	Zeitstunden
davon Aufgaben:	40	Zeitstunden
davon Online-Betreuung:	5	Zeitstunden
davon individuelle Prüfungs-vorbereitung	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS		

Lerninhalt und Niveau:

Formale Inhalte

- Aufgabe eines Sachverständigen
- Selbstverständnis und Rolle eines Sachverständigen
- Vorbereitung zur Sachverständigenprüfung

Fachliche Inhalte

- Normenwerk „ISO/IEC 27037:2012" Leitlinien für die Identifizierung, Sammlung, Erfassung und Archivierung elektronischer Beweise
- Typische Zusammenstellung von IT-Beweismitteln
  - Spuren in Datenträgern und Dateien (reguläre Inhalte, gelöschte Inhalte, verschlüsselte Inhalte)
  - Spuren im System (Registry, Log-Files, …)

	- Spuren aus dem Internet (Browser-Cache, History, Mail) - Spuren mobiler Geräte (Smartphones, Tabletts) • Einrichtung eines normgemäßen Labors für Digitale Forensik - Hardware - Software • Arbeiten im normgemäßen Labor - Abwicklung eines umfassenden Falls (Projektplan) - Fachgemäßes Vorgehensmodell - Fachgemäßes Reporting - Praktische Fallbeispiele **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Nach erfolgreichem Abschluss des Moduls kennt der Studierende die Aufgaben des Sachverständigen für IT-Forensik. Der Studierende wird auf die Sachverständigenprüfung vorbereitet. Er ist in der Lage, ein forensisches Labor einzurichten. In und mit dem Labor kann er forensische Fälle nach fachgemäßen Vorgehensmodellen bearbeiten.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung Onlineveranstaltung: Vorlesung
Anerkannte Module:	
Medienformen:	Vorlesung mit Beamer, Studienbriefe, Onlinematerial in Lernplattform, Übungen und Tests über Lernplattform, Onlinekonferenzen, Chat und Forum in Lernplattform
Literatur:	Normenwerk „ISO/IEC 27037:2012 "Leitlinien für die Identifizierung, Sammlung, Erfassung und Archivierung elektronischer Beweise; Patrick Engebretson (2013): The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress Media; Thomas Wilhelm (2013): Professional Penetration Testing: Creating and Learning in a Hacking Lab: 1 Verlag: Syngress; Manuel Christensen (2012): Certified Professional Penetration Tester (eCPPT) Secrets To Acing The Exam and Successful Finding And Landing Your Next Certified Professional Penetration Tester (eCPPT) Certified Job Verlag: tebbo Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.19 [Z-220] Netzsicherheit I - IT-Sicherheit von Netzwerken

Modulbezeichnung:	Netzsicherheit I: IT-Sicherheit von Netzwerken (Z-220)
Zertifikatsabschluss:	Hochschulzertifikat mit 5 ECTS-Punkten
Verwendbarkeit:	Gesamtzertifikat „Netzwerkforensiker/-in Open C³S“ sowie in ausgewählten Studiengängen
Modulverantwortliche(r):	Tobias Scheible, M.Sc.
Dozent(in):	Tobias Scheible, M.Sc.
Zeitraum:	05.02.2023 – 30.04.2023; Anmeldeschluss: 10.01.2023
Leistungspunkte	5 ECTS
Zielgruppe:	Fachinformatiker*innen (aus den Bereichen Systemintegration oder Anwendungsentwicklung) mit min. 3-jähriger Berufserfahrung, Personen mit Studium der Informatik oder vergleichbarer Studiengänge, andernfalls sollte vorher besprochen werden, ob die Teilnehmer*innen die Eingangsvoraussetzungen erfüllen. ▪ IT-Mitarbeitende ▪ EDV-Systembetreuer ▪ IT-Administratoren
min.-max. Teilnehmerzahl:	10 bis 20
Studien- und Prüfungsleistungen:	Hausarbeit + Referat (15 + 5 Min.) mit obligatorischer Leistungserbringung im Lernmanagementsystem (Lernsequenzen + Übungsaufgaben)
Notwendige Voraussetzungen:	▪ Grundlegendes Verständnis von Betriebssystemen (Prozesse, Speicher, Geräte, ...) ▪ Grundlegende Kenntnisse der Netzwerktechnik (Techniken, Protokolle, …) ▪ Umgang mit der Linux Shell (Bash und Zsh) ▪ gutes analytisches Denken und methodisches Vorgehen ▪ Englischkenntnisse auf B1 Niveau ▪ intrinsische Motivation für ein berufsbegleitendes Zertifikatsmodul in Fernlehre Sollten diese Voraussetzungen partiell nicht erfüllt werden, sollte dies im Einzelfall geklärt werden.
Empfohlene Voraussetzungen:	
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
Prüfung:	2	Zeitstunden
Prüfungsvorbereitung:	15	Zeitstunden
Fernstudienanteil:	118	Zeitstunden
davon Selbststudium:	58	Zeitstunden
davon Aufgaben:	40	Zeitstunden
davon Online-Betreuung:	20	Zeitstunden
Summe:	**150**	**Zeitstunden**

Lerninhalt und Niveau:	**Teil I: Sniffing & Scanning** Protokolle Media Access Control (MAC), Address Resolution Protocol (ARP), Internet Protocol (IP) Cyber Security Bedrohungen, Angreifertypen, Angriffsarten, Schutzziele Angriffsvektoren Eavesdropping, Hacking-Hardware, Arten von Scans Gegenmaßnahmen Physischer Schutz, Honeypots und Honeynets, Seperation von Netzen **Teil II: Denial-of-Service** Protokolle Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Transport Layer Security (TLS) Cyber Security Hashfunktionen, Verschlüsselungsmethoden Angriffsvektoren ARP-Cache-Flooding, IP-Fragment-Flag, ICMP Flood, TCP-SYN-Flooding, DNS Amplification Gegenmaßnahmen Firewalls, IDS & IPS, TCP-SYN-Cookie, Timings **Teil III: Spoofing & Man-in-the-Middle** Protokolle Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) Cyber Security Informationssicherheit vs. Datenschutz Angriffsvektoren ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Rogue-DHCP-Server, Hacking-Hardwar Gegenmaßnahmen MAC-Filter, ARP-Proxy, DNSSEC, Dot, DoH, DHCP-Snooping, TLS **Teil IV: Virtuelle Netze & Verschleierung** Protokolle Virtual Private Network (VPN), Peer-to-Peer (P2P), Tor-Protokoll, Routing Cyber Security Incident Response und IT-Forensik Angriffsvektoren Verschleierung Gegenmaßnahmen Virtual Local Area Network (VLAN) Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).
Angestrebte Lernergebnisse:	In der Lehrveranstaltung „Netzwerksicherheit I: IT-Sicherheit in Netzwerken“ erhalten Sie einen Überblick über die Bedrohungen und Angriffe gegen und über Netzwerke. Darüber hinaus lernen Sie die in Rechnernetzen eingesetzten Technologien und die wichtigsten Merkmale und Eigenschaften von Datennetzen kennen. Die wichtigsten Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Abwehrmaßnahmen werden erläutert. In Übungen im virtuellen Labor führen Sie selbst Angriffe durch, um anschließend Bedrohungsszenarien nachvollziehen und einordnen zu können. Nach erfolgreichem Abschluss des Moduls kennen Sie die wichtigsten Merkmale und Eigenschaften und können die verwendeten Sicherheitskonzepte einordnen. Darüber hinaus haben Sie Kenntnisse über Bedrohungen und den Einsatz von Werkzeugen erworben, um die Möglichkeiten und Grenzen selbst einschätzen zu können.
Lehrveranstaltungen und Lehrformen:	<u>E-Learning Lernplattform:</u> Aufzeichnungen, Interaktive Kontrollaufgaben, Hausaufgaben/Projektaufgaben <u>Online-Vorlesungen:</u> Vorlesung, Fragen und Antworten, Übungen, flexible Vertiefung wichtiger Themen <u>Präsenz-/Remoteveranstaltung:</u> Vorlesung, Übungen mit theoretischem und praktischem Schwerpunkt
Anerkannte Module:	
Medienformen:	Elektronisches Skript, Videos, Lab Environments (VMs), Online-Lernplattform

Literatur:	• IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung | Steffen Wendzel | Springer Vieweg, Wiesbaden | ISBN 9783864914898 • Netzsicherheit: Grundlagen & Protokolle; mobile & drahtlose Kommunikation; Schutz von Kommunikationsinfrastrukturen | Günter Schäfer; Michael Roßberg | dpunkt.verlag, Heidelberg | ISBN 9783864901157 • IT-Sicherheit: Konzepte - Verfahren - Protokolle | Claudia Eckert | De Gruyter, Oldenbourg | ISBN 9783110551587 • Kryptographie und IT-Sicherheit | Stephan Spitz; Michael Pramateftakis; Joachim Swoboda | Springer Vieweg, Wiesbaden | ISBN 9783834881205 • Computernetzwerke | Andrew S. Tanenbaum; David J. Wetherall | Pearson, München | ISBN 9783868941371 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.2.20 [Z-221] Netzsicherheit II – *In Überarbeitung!*

4.2.21 [Z-222] Netzsicherheit III – *In Überarbeitung!*

4.2.22 [Z-223] Windows-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung*

Aktuelle Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-208] Forensische Analyse eines Windows-Systems“.

4.2.23 [Z-224] Unix-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung*

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-209] Forensische Analyse eines Unix-Systems“.

4.2.24 [Z-225] MacOS-Forensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung*

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-210] Forensische Analyse eines MacOS-Systems“.

4.2.25 [Z-226] Netzwerkforensik Gutachter - *Vorbereitendes Modul zur Gutachterprüfung*

Modulbeschreibung folgt in Kürze!
Modulinhalte siehe auch „[Z-211] Forensische Analyse von Netzwerken“.

4.3 Ruhr-Universität Bochum

4.3.1 [Z-304] SPAM

Modulbezeichnung:	[Z-304] SPAM
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Dr. Christoph Wolf
Dozent(in):	
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	
Min.-max. Teilnehmerzahl:	10 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.

4.3.2 [Z-305] Kryptographie 1

Modulbezeichnung:	[Z-305] Einführung in die Kryptographie 1
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr.-Ing. Christof Paar
Dozent(in):	Prof. Dr.-Ing. Christof Paar
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende im Bachelor
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Schriftliche Prüfung (Dauer: 120min)
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Fähigkeit zum abstrakten und logischen Denken
Sprache:	Deutsch (Englisch optional)
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	3	Zeitstunden
davon Prüfung:	3	Zeitstunden
Fernstudienanteil:	147	Zeitstunden
davon Selbststudium:	62	Zeitstunden
Davon Prüfungsvorbereitung:	30	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalt und Niveau:	Es werden zunächst grundlegende Begriffe der Kryptographie und Datensicherheit eingeführt. Nach der Vorstellung einiger historischer Verschlüsselungsverfahren werden Stromchiffren behandelt. Den Hauptteil der Vorlesung bilden Blockchiffren und deren Anwendung. Als bedeutender Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt. Betriebsmodi und Sicherheitseinschätzungen werden ebenfalls behandelt. Gegen Ende der Vorlesung wird das Prinzip der asymmetrische Kryptographie sowie das in der Praxis wichtigste asymmetrischer Verfahren, der RSA-Algorithmus, vorgestellt. Neben den kryptographischen Algorithmen werden die notwendigen mathematischen Grundlagen (u.a. Ringe ganzer Zahlen, euklidischer Algorithmus, endliche Körper) eingeführt.

	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor).
Angestrebte Lernergebnisse:	Verständnis der Funktionsweise der wichtigsten symmetrischen Verschlüsselungsverfahren für die Praxis und Grundlagen der asymmetrischen Kryptographie. Darüber hinaus Kenntnis der Denkweisen der modernen Kryptographie.
Lehrveranstaltungen und Lehrformen:	Vorlesung und Übungen
Anerkannte Module:	
Medienformen:	Video, Moodle
Literatur:	*[1] Christof Paar und Jan Pelzl, „Understanding Cryptography: A Textbook for Students and Practitioners", Springer, 2009.* *[2] Christof Paar und Jan Pelzl, „Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender", Springer Vieweg, 2016*

4.3.3 [Z-306] Kryptographie 2

Modulbezeichnung:	[Z-306] Kryptographie 2
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr.-Ing. Christof Paar
Dozent(in):	Prof. Dr.-Ing. Christof Paar
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende im Bachelor
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Schriftliche Prüfung (Dauer: 120min)
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Inhalte des Moduls "Einführung in die Kryptographie 1"
Sprache:	Deutsch (Englisch optional)
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	3	Zeitstunden
davon Prüfung:	3	Zeitstunden
Fernstudienanteil:	147	Zeitstunden
davon Selbststudium:	62	Zeitstunden
Davon Prüfungsvorbereitung:	30	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalt und Niveau:

Einen wichtigen Teil der Vorlesung bilden asymmetrische kryptographische Verfahren basierend auf dem diskreten Logarithmusproblem. Es werden hier der Schlüsselaustausch nach Diffie-Hellman, die Elgamal-Verschlüsselung und Verfahren mit elliptischen Kurven behandelt. Nachfolgend werden Schemata und Protokolle basierend auf symmetrischen und asymmetrischen Primitiven entwickelt. Behandelt werden: Digitale Signaturen, Message Authentication Codes (MACs), Hash-Funktionen, Zertifikate, Protokolle zum Schlüsselaustausch sowie Sicherheitsdienste.

Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).

Angestrebte Lernergebnisse:	Verständnis der wichtigsten asymmetrischen Verschlüsselungsverfahren für die Praxis sowie den Einsatz von Krypto-Primitiven für die Realisierung von Sicherheitsdiensten.
Lehrveranstaltungen und Lehrformen:	Vorlesung und Übungen
Anerkannte Module:	
Medienformen:	Video, Moodle
Literatur:	*Christof Paar und Jan Pelzl, „Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender", Springer Vieweg, 2016*

4.3.4 [Z-307] Kryptanalytische Methoden und Werkzeuge

Modulbezeichnung:	[Z-307] Kryptanalytische Methoden und Werkzeuge
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Tim Güneysu
Dozent(in):	Prof. Dr. Tim Güneysu
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur
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 Methoden und Werkzeuge zur Analyse von Sicherheitsmechanismen und kryptographischen Systemen behandelt. Der praktische Bezug der Methoden steht hierbei im Vordergrund, sodass die Ansätze insbesondere bezüglich verschiedener Rechnerplattformen verglichen werden. Hauptbestandteile der Veranstaltung sind dabei Möglichkeiten der effizienten Passwort- und Schlüsselsuche für kryptographische Systeme, jedoch auch Implementierungsangriffe mittels Seitenkanal- und Fehlerinjektionsangriffen. 1. Sicherheit vs. Rechenleistung Einführung, Plattformen (CPU, GPU, Spezialhardware), Metriken **Praktische Übung:** Vergleich von Sicherheitsanalysen und Angriffswerk-zeugen auf verschiedenen Rechnerplattformen.

	2. Sicherheitsaspekte kryptographischer Geheimnisse mit besonderem Fokus auf die Wahl von Passwörtern als Geheimnis sowie zufällig gewählter Sicherheitsparameter **Praktische Übung:** Durchführen eines parametrisierten Wörterbuchangriffs mittels personalisierter Passwortlisten. 3. Einführung in die Kryptanalyse von Sicherheitssystemen, Standardangriffe auf symmetrische und asymmetrische Kryptosysteme **Praktische Übung:** Implementierung und Optimierung eines kryptanalytischen Angriffs bezüglich Laufzeit/Speicherbedarf. 4. Analyse kryptographischer Implementierungen, Reverse-Engineering-Angriffe, Seitenkanalangriffe, Fehlerinjektionsan-griffe **Praktische Übung:** Implementierungsangriffe auf ein gegebenes Kryptosystem. --- **Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).**
Angestrebte Lernergebnisse:	Die Studierenden werden mit den wichtigsten Komponenten und Werkzeugen der Kryptanalyse vertraut gemacht. Sie haben einen umfangreichen Überblick über Algorithmen und Techniken, die heutzutage zur Analyse bestehender Systeme eingesetzt werden. Des Weiteren haben sie nicht nur Kenntnisse über die neuesten Analyseverfahren, sondern auch die Grenzen bezüglich Rechen,- Speicher- und finanzieller Aufwand. Mit dem vermittelten Wissen, ist es den Teilnehmern zum Ende des Kurses möglich, unterschiedliche Methoden auf die Analyse von bestehenden Systemen erfolgreich anzuwenden sowie die Limitierungen von Sicherheitsana-lysen einschätzen zu können.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, Übung
Anerkannte Module:	Module aus Studiengängen der Informatik oder von stark Informatik-affinen Studiengängen, die ähnliche Lerninhalte und angestrebte Lernergebnisse verfolgen (Überdeckungsgrad > 75 %) und deren Workload vergleichbar ist.
Medienformen:	Elektronischer Studienbrief, Übungs-Einreichung und –Korrektur in elektronischer Form, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.3.5 [Z-308] Sicherheit mobiler Systeme

Modulbezeichnung:	[Z-308] Sicherheit Mobiler Systeme
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	In ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Thorsten Holz
Dozent(in):	Prof. Dr. Thorsten Holz
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Master
Min.-max. Teilnehmerzahl:	10 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.

4.4 Goethe-Universität Frankfurt am Main / Universität des Saarlandes

4.4.1 [Z-401] Computerstrafrecht

Modulbezeichnung:	[Z-401] Computerstrafrecht
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C7/C8/ D1/D2/D3/D4/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Christoph Burchard / Jun.-Prof. Dr. Dominik Brodowski
Dozent(in):	Prof. Dr. Christoph Burchard / Jun.-Prof. Dr. Dominik Brodowski
Zeitraum:	voraussichtlich 27.11.2024 – 07.02.2025; Anmeldeschluss: 09.10.2024
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne juristische Ausbildung
min.-max. Teilnehmerzahl:	10 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 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.

4.4.2 [Z-402] Computerstrafprozessrecht

Modulbezeichnung:	[Z-402] Computerstrafprozessrecht
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C7/ D1/D2/D3/D4/D6 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Christoph Burchard / Jun.-Prof. Dr. Dominik Brodowski
Dozent(in):	Prof. Dr. Christoph Burchard / Jun.-Prof. Dr. Dominik Brodowski
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Studierende ohne juristische Ausbildung
min.-max. Teilnehmerzahl:	10 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.

4.5 Universität Passau

4.5.1 [Z-801] Cloud-Sicherheit und Cloud-Forensik – Angriffsanalyse

Modulbezeichnung:	[Z-801] Cloud-Sicherheit und Cloud-Forensik mit Schwerpunkt Angriffsanalyse
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C6/D1/D2/D3/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Hans P. Reiser
Dozent(in):	Prof. Dr. Hans P. Reiser
Zeitraum:	Voraussichtlich 08.05.2024 – 12.07.2024; Anmeldeschluss: 27.03.2024
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten, Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Cloud-Sicherheit weiterbilden möchten
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Grundlegende Programmierkenntnisse in Python
Empfohlene Voraussetzungen:	Grundverständnis von Betriebssystemen, Linux-Kenntnisse
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	1	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	80	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	10	% = Präsenz

Lerninhalt und Niveau:

- Virtualisierungstechnik und Cloud-Computing
  - Geschichtliche Hintergründe von Virtualisierungstechnik
  - Virtualisierungsarten
  - Details von Rechnervirtualisierung (Intel/ARM)
  - Service- und Verarbeitungsmodelle von Cloud Computing (NIST)
- Cloud-Sicherheit und Bedrohungsmodelle
  - Bedrohungsmodellierung und Risikomanagement
  - Sicherheitsherausforderungen in der Cloud
  - Sichere Datenspeicherung und –verarbeitung in der Cloud
  - Koresidenz und Seitenkanalangriffe

	• Grundlagen von Cloud-Forensik
	  ○ Historische Entwicklung von IT-Forensik
	  ○ Aktuelle Modelle der IT-Forensik
	  ○ Datenträger-Forensik in der Cloud
	  ○ Live-Forensik in der Cloud
	  ○ Forensik-Dienste und Forensik-Readiness-Modelle in der Cloud
	• Virtual Machine Introspection (VMI)
	  ○ Grundlagen, Herausforderungen und Anwendungen von VMI
	  ○ Funktionsweise der Analysebibliothek LibVMI
	  ○ Untersuchung von Linux-Kernel-Datenstrukturen mit Volatility
	  ○ Untersuchung aktiver virtueller Maschinen mit Volatility/LibVMI
	• Cloud-Einbruchserkennungssysteme und Honey Pots
	  ○ Grundlagen von Einbruchserkennungssystemen
	  ○ Grundlagen von Honeypots
	  ○ Einbruchserkennungssysteme in der Cloud
	  ○ Honeypots in der Cloud
	
	(Voraussichtliche Ergänzungen: Service und Verarbeitungsmodell, Identidy and Access Management, weitere Cloud Deployment Modelle)
	
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).

Angestrebte Lernergebnisse:	Nach Abschluss dieses Moduls verfügen Sie über fundierte Kenntnisse im Bereich von Cloud-Sicherheit und Cloud-Forensik. Neben den Konzepten und Architekturen von Virtualisierung umfassen diese Kenntnisse das Wissen über Sicherheitsherausforderungen und Bedrohungsmodellen in Cloud-Infrastrukturen sowie einen Überblick über aktuelle Forensikmethoden und entsprechende Werkzeuge. Darüber hinaus haben Sie weiterführende Kompetenzen in der Verwendung von Virtual Machine Introspection, Honeypots und Einbruchserkennungssystemen als Werkzeuge zur Angriffsanalyse erworben.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Online-Vorlesung über Web-Konferenzen, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

4.5.2 [Z-802] Cloud-Sicherheit und Cloud-Forensik – Zugriffskontrolle

Modulbezeichnung:	[Z-802] Cloud-Sicherheit und Cloud-Forensik mit Schwerpunkt Zugriffskontrolle
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Gesamtzertifikate C6/D1/D2/D3/D5 und in ausgewählten Studiengängen
Modulverantwortliche(r):	Prof. Dr. Hans P. Reiser
Dozent(in):	Prof. Dr. Hans P. Reiser
Zeitraum:	Auf Anfrage und bei Erreichen der Mindestteilnehmerzahl; Dauer: ca. 8 Wochen
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Cloud-Sicherheit weiterbilden möchten
min.-max. Teilnehmerzahl:	10 bis 30
Studien- und Prüfungsleistungen:	Klausur, Hausarbeit
Notwendige Voraussetzungen:	Grundlegende Programmierkenntnisse in Python
Empfohlene Voraussetzungen:	Grundverständnis von Betriebssystemen, Linux-Kenntnisse
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium:	15	Zeitstunden
davon Prüfung und Prüfungsvorbereitung:	1	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	80	Zeitstunden
davon Aufgaben:	45	Zeitstunden
davon Online-Betreuung:	10	Zeitstunden
Summe:	**150**	**Zeitstunden**
30 h = 1 CP nach ECTS	10	% = Präsenz

Lerninhalt und Niveau:

- Virtualisierungstechnik und Cloud-Computing
  - Geschichtliche Hintergründe von Virtualisierungstechnik
  - Virtualisierungsarten
  - Details von Rechnervirtualisierung (Intel/ARM)
  - Service- und Verarbeitungsmodelle von Cloud Computing (NIST)
- Cloud-Sicherheit und Bedrohungsmodelle
  - Bedrohungsmodellierung und Risikomanagement
  - Sicherheitsherausforderungen in der Cloud
  - Sichere Datenspeicherung und -verarbeitung in der Cloud
  - Koresidenz und Seitenkanalangriffe

	• Grundlagen von Cloud-Forensik
	  ○ Historische Entwicklung von IT-Forensik
	  ○ Aktuelle Modelle der IT-Forensik
	  ○ Datenträger-Forensik in der Cloud
	  ○ Live-Forensik in der Cloud
	  ○ Forensik-Dienste und Forensik-Readiness-Modelle in der Cloud
	• Cloud-Einbruchserkennungssysteme und Honey Pots
	  ○ Grundlagen von Einbruchserkennungssystemen
	  ○ Grundlagen von Honeypots
	  ○ Einbruchserkennungssysteme in der Cloud
	  ○ Honeypots in der Cloud
	• Identitätsmanagement und Single Sign-on
	  ○ Grundlagen zu Authentisierung und Autorisierung
	  ○ Identitätsmanagement und Single-Sign-On-Systeme
	  ○ Einrichtung und Verwendung von OAuth/OpenID Connect
	  ○ Aktuelle Herausforderungen in Authentisierung und Autorisierung
	
	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 7 (Master).

Angestrebte Lernergebnisse:	Nach Abschluss dieses Moduls verfügen Sie über fundierte Kenntnisse im Bereich von Cloud-Sicherheit und Cloud-Forensik. Neben den Konzepten und Architekturen von Virtualisierung umfassen diese Kenntnisse das Wissen über Sicherheitsherausforderungen und Bedrohungsmodellen in Cloud-Infrastrukturen sowie einen Überblick über aktuelle Forensikmethoden und entsprechende Werkzeuge. Darüber hinaus haben Sie weiterführende Kompetenzen in der Einrichtung von Identitätsmanagementsystemen erworben, um Zugriffe zu beschränken, und in der Verwendung von Einbruchserkennungssystemen, um unerlaubte Zugriffe nachzuvollziehen.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übung Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung
Anerkannte Module:	keine
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Online-Vorlesung über Web-Konferenzen, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.