Open C3S
Open Competence Center for Cyber Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16OH12021 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor/bei der Autorin.

Open Competence Center for Cyber Security

E R G E B N I S B O G E N
EQF-Bewertung

HSAS, FAU, RUB, GU

>Zertifikatsangebot "Open C3S"<

Darmstadt, den 18.03.2017

Open C³S

Median (MD) / Minimum (Min.) / Maximum (Max.) der EQF-Stufen ...

... über alle Teilprozesse und Kategorien
[S. 1; Größe der Auswertungseinheit: N]

... je Kategorie über alle Teilprozesse
[S. 1; Größe der Auswertungseinheit: N]

... je Kategorie in den Teilprozessen
[S. 2 ff.; Größe der Auswertungseinheit: N]

N = Fallzahl; F = davon fehlend

Die EQF-Bewertungen wurden von zwei unabhängigen externen IT-Experten durchgeführt.
Die berichteten Ergebnisse stellen den Konsens der beiden Experten dar.
Die EQR-Bewertungen basieren ausschließlich auf den Angaben und Formulierungen im Modulhandbuch (Stand 28. Juni 2016).
Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C³S zu entnehmen.

Zusammenfassende Mediane

Median in der Gesamtbetrachtung
der EQF-Stufe über alle Teilprozesse, Kategorien und Fälle

MD	Min.	Max.	N	F
4	**3**	**5**	**114**	**0**

Kategorie "Kenntnisse"
Median der EQF-Stufe über alle Teilprozesse und Fälle

MD	Min.	Max.	N	F
5	3	5	38	0

Kategorie "Fertigkeiten"
Median der EQF-Stufe über alle Teilprozesse und Fälle

MD	Min.	Max.	N	F
4	3	5	38	0

Kategorie "Kompetenz"
Median der EQF-Stufe über alle Teilprozesse und Fälle

MD	Min.	Max.	N	F
4	3	4	38	0

Werte je Kategorie in den Teilprozessen über alle Fälle
und je Teilprozess über alle Kategorien und Fälle

Forschungsgruppe Brinkmann/Seger
seger@ifs.tu-darmstadt.de

	Module des Zertifikatangebots > "Open C3S" < entsprechend den Modulbeschreibungen Stand 28. Juni 2016	Erlernte Kompetenzlevel je EQF-Kategorie in den Teilprozessen über alle Fälle
1	**Methoden digitaler Forensik** (2 Monate / 150 Lernstunden / 5ECTS) * Die Teilnehmer beherrschen die terminologischen Grundlagen der digitalen Forensik und können Beziehungen zwischen Konzepten der klassischen Forensik und der digitalen Forensik herstellen. * Die Teilnehmer haben ein einfaches Werkzeug zur Analyse von Partitionstabellen erstellt und dadurch ein Verständnis für die Komplexität forensischer Software entwickelt. * Die Teilnehmer können forensische Gutachten aufgrund von allgemeinen Qualitätskriterien bewerten. Inhalt - klassische (analoge) Forensik: Beispiele, Theorie der Entstehung von Spuren - Terminologie: Identifizierung, Klassifizierung, Individualisierung, Assoziation - Quantifizierung der Assoziation: Rechenbeispiele - Digitale Spuren - Kurze Einführung in die Datenträgeranalyse: Partitionssysteme (DOS, GPT) - Regeln für den Aufbau forensischer Gutachten, Qualitätskriterien für forensische Dokumentation **Übungen**: - Einübung der Terminologie an Beispielen - Digitale Spuren und digitale Forensik: Abgrenzung und Gemeinsamkeiten - Programmierung von mmls (für DOS- und GPT-Partitionen). Untersuchung folgende Fragestellungen: - Wie behandeln unterschiedliche Betriebssysteme die nicht-essentiellen Daten in der Partitionstabelle? - Wie werden erweiterte Partitionen standardmäßig von verschiedenen Betriebssystemen angelegt? - Wie verhalten sich Betriebssysteme bei nicht standardmäßiger Codierung von erweiterten Partitionen (z.B. Zyklen)? **Projekt:** Schreiben eines forensischen Berichts zu einem individuellen Fall. Dieser basiert auf der Frage, ob Manipulationen in einem gegebenen Partitionssystem vorliegen. **Präsenzphase:** Vorstellung und Verteidigung des Berichts in einer mündlichen Prüfung (Rollenspiel)	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse: 5 / 3 / 5 / 2 / 0 Fertigkeiten: 5 / 3 / 5 / 2 / 0 Kompetenz: 4 / 3 / 4 / 2 / 0 Über alle Kategorien: 5 / 3 / 5 / 6 / 0

2	**Systemnahe Programmierung** (2 Monate / 150 Lernstunden / 5ECTS) * 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. Inhalt: **Grundlagen Rechnerarchitektur und Assembler-Programmierung** - Von-Neumann-Architektur - Allgemeine Prinzipien der Assemblerprogrammierung **Grundlagen Betriebssysteme** - Grundbegriffe - Prozesse, Threads, Datenstrukturen **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	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse: 5 / 5 / 5 / 2 / 0 Fertigkeiten: 5 / 5 / 5 / 2 / 0 Kompetenz: 4 / 4 / 4 / 2 / 0 Über alle Kategorien: 5 / 4 / 5 / 6 / 0

3	**Reverse Engineering** (2 Monate/150 Lernstunden / 5 ECTS) * Die Studierenden können den Begriff „Reverse Engineering" einordnen und definieren. Sie können die typischen Einsatzgebiete von Reverse Engineering benennen. Die Strukturen von Microsoft Windows sind ihnen bekannt. Den Aufbau von Programmdateien in Windows können sie beschreiben und analysieren. Sie können die Methoden zur Dekompilierung von Maschinenprogrammen benennen und anwenden. Verschiedene Optimierungsverfahren der Compiler, die eine Dekompilierung erschweren, können sie erkennen und benennen. Die üblichsten Werkzeuge zur Programmanalyse können die Absolventen einsetzen, Vorteile und Nachteile einer statischen und dynamischen Programmanalyse sind ihnen bekannt, und sie können diese bedarfsabhängig einsetzen. Sie haben detaillierte Kenntnisse über Malware sowie verschiedene Methoden und Tricks der Malware-Autoren. Die Absolventen können „einfache" Malware für Windows-Systeme selbstständig analysieren. Sie beherrschen die Grundlagen für eine Vertiefung des weiten Gebietes der Malware-Analyse. Inhalt: **Einführung in Reverse Engineering** - Abgrenzung des Begriffs Reverse Engineering - Einsatzgebiete - Zielsetzung und Grenzen von Reverse Engineering **Microsoft Windows** - Aufbau und Struktur - Anwendungen und Bibliotheken, API-Programmierung - Detaillierte Betrachtung der PE-Struktur zur Programmanalyse: Importe, Exporte, Sections, Windows-Loader, Datenstrukturen - Prozesse, Threads und ihre Datenstrukturen - Exceptions und Exception-Behandlung **Programmanalyse** - Codeerzeugung durch Compiler und Decompilierung - Optimierungsverfahren - Kontroll- und Datenflussanalyse **Werkzeuge zur Programmanalyse: IDA und OllyDbg** - Statische Analyse - Dynamische Analyse - Übungen: Analyse einfacher Binaries, einfaches Debugging/Cracking, Sicherheitsprüfungen aushebeln **Malware und Malware-Analyse** - Obfuscation - Verhinderung von Disassemblierung - Malware-Techniken, Packer, Anti-Reverse-Engineering-Methoden Analyse realer Malware in einer virtuellen Analyseumgebung Übungen: Malware-Analyse mit IDA und OllyDbg **Präsenzwochenende:** Vorlesung, Übungen in Gruppen: Analyse verschleierter Binaries, Analyse von Malware, Vorbereitung auf die Hausarbeit	

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	2	0
Fertigkeiten	5	5	5	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	5	4	5	6	0

4

Mobilfunkforensik

(2 Monate / 150 Lernstunden / 5 ECTS)

* Der Aufbau und die Funktionsweise von Android und Android-Applikationen ist den Studierenden bekannt. Die grundlegenden Methoden zur Vorbereitung einer forensischen Analyse von Android Mobiltelefonen sind Ihnen geläufig. Sie können unterschiedliche Verfahren und Werkzeuge zur Analyse benennen und anwenden. Die Studierenden können einfache Applikationen für Android programmieren. Sie gewinnen Kenntnisse zur Analyse von Android Applikationen. Die sicherheitskritische Betrachtung von Android Applikationen ist Ihnen vertraut. Die Absolventen können eine forensische Analyse von Mobiltelefonen auf der Basis von Android durchführen.

Inhalt:

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

2. Einführung in Mobilfunkforenisk für Android
- Wie kommt man an die wichtigen Daten
- Rooting, Recovery und andere Zugriffsstrategien
- Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie
- Einführung in SQLite
- Einführung in Volatility für Android
- Beispiel: Manuelle Analyse der Datenbanken der Adressbuch Applikation
- Beispiel: Manuelle Analyse der Speicherinhalte der Facebook Applikation mit Hilfe von Volatility
- Das Mobilfunkforensik-Framework ADEL
- Aufgabe I: Forensische Analyse einer Applikation (RAM und lokaler Speicher)
- Aufgabe II: Entwicklung eines Plugins für ADEL

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

4. Analyse von Android Applikationen
- Einführung in das Decompilieren und Reversen von Android Applikationen
- Automatisierte Analysetechniken: Überblick, Einführung und Diskussion statische vs. dynamische Analyse
- Einführung in die Tools smali, dex2jar und JD-GUI
- Beispiel: Manuelle Analyse einer einfachen Android Malware mit Hilfe von d ex2jar und JD-GUI
- Einführung in die Tools Androguard, Droidlyzer und DroidBox
- Beispiel: Analyse einer komplexeren Android Malware mit Hilfe von Droidlyzer und DroidBox
- Exkurs: Die Mobile-Sandbox
- Aufgabe I: Analyse einer komplexeren Android Malware mit Hilfe der zuvor vorgestellten Tools und Systemen

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

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

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

Präsenzphase
- Präsentation und Verteidigung der Projektergebnisse

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	2	0
Fertigkeiten	5	5	5	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	5	4	5	6	0

5	**Applied Computer Systems** (2 Monate / 150 Lernstunden / 5 ECTS) * 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. * Die Studierenden haben Kenntnisse über Instrumente und Methoden der Informatik. Sie haben insbesondere grundlegende Kenntnisse in der praktischen, technischen und theoretischen Informatik. * Sie können Darstellungsformen und -formaten von Informationen in Rechnern interpretieren und umwandeln. Die Grundzüge von Rechnern und die Aufgaben unterschiedlicher Software können erläutert werden. Grundlegende 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). Inhalt: **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.	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse: 5 / 4 / 5 / 2 / 0 Fertigkeiten: 4 / 3 / 4 / 2 / 0 Kompetenz: 4 / 4 / 4 / 2 / 0 Über alle Kategorien: 4 / 3 / 5 / 6 / 0

6

Python 1 – Programmieren im IT-Security-Umfeld

(2 Monate/150 Lernstunden / 5 ECTS)

* 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.
* 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).

Inhalt:

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

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	4	6	0

7	**Python 2 – Programmieren im IT-Security-Umfeld** (2 Monate/150 Lernstunden / 5 ECTS) * 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. * 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). Inhalt: **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.	EQF-Kategorien Kenntnisse Fertigkeiten Kompetenz Über alle Kategorien MD 5 5 4 5 Min. 4 4 4 4 Max. 5 5 4 5 N 2 2 2 6 F 0 0 0 0

8	**Datenträgerforensik 1** (2 Monate/150 Lernstunden / 5 ECTS) * 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. * 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. Inhalt: **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	

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	4	6	0

9	**Datenträgerforensik 2** (2 Monate/ 150 Lernstunden / 5 ECTS) * 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. * 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. Inhalt: **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 in Zusammenhang 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 Mountpointsund 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. **3. Linux/Unix Extended Dateisysteme (Ext3)** - Linux-Bootprozess unter der Verwendung der Bootloader LiLo und GRUB: Virtuelles Dateisystem bei Linux-Betriebssystemen allgemeiner Überblick 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-Tabelle Aufbau und Funktion von Inodes bzw. der 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-Dateisystemen 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	

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	2	0
Fertigkeiten	5	4	5	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	5	4	5	6	0

10

Windows-Forensik

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die Möglichkeiten, die forensische Analyse eines Windows-Rechners bietet. Er kennt für die Forensik relevante Dateien und Verzeichnisse des Windows-Betriebssystems und kann diese auswerten und über gefundene Ergebnisse berichten. Dabei erstreckt sich die Analyse auf Post-Mortem-Analyse, Live-Systeme und Arbeitsspeicherabbilder.
* Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße.

Inhalt:

- **Das Windows-Rechnersystem:**
  Grundlegende Konzepte und Begriffe, Windows-„Bordwerkzeuge" (Untersuchung von Prozessen und Threads, Leistungsüberwachung), System-Architektur (Gerätetreiber, Systemprozesse, Kernel, HAL), Sicherheitskomponenten, Reguläre Ausdrücke, Ermitteln der eigenen IP-/MAC-Adresse, Grundlagen Netzwerktechnik
- **Struktur und Analyse von Windows-Systemen:**
  Schlüsselwortsuche, Filecarving, Schlupfspeicher extrahieren, indizieren von Metadaten, Speicherabbilder, Protokolldateien, Hashing, Zugriffsrechte, forensisch relevante Verzeichnisse und Dateien, Schattenkopien
- Erkenntnisse aus der Registry:
  Aufbau, SIDs, SAMs, GUIDs, forensisch relevante Registry-Einträge, Werkzeuge zur Registry-Analyse
- **Logfile-Analyse:**
  NTFS-Journal-Protokollierung, Struktur der Logging-Einträge, Auswertung, Windows-Event-Log, Anwendungs- und Dienstprotokolle, Security-Log, Setup-Log, Überwachungsrichtlinien
- **Forensische Untersuchung von Internetdiensten:**
  Peer-to-Peer-Aktivitäten aufdecken, IP-Adresse von Skype-Accounts ermitteln, Datenbanksystem, SQLite-Andwendungs-Artefakte auswerten (Skype, Firefox, Chrome), Microsoft-Anwendungs-Artefakte auswerten (Internet Explorer, Outlook)
- **Forensische Analyse von Arbeitsspeicher und Windows-Artefakten:**
  Flüchtige Informationen, Systemzeit auslesen, eingeloggte Benutzer, offene Dateien, Netzwerkverbindungen, Prozessinformationen, Zwischenablage, Dienste/Treiber-Informationen, Erstellung eines Arbeitsspeicherabbilds, Arbeitsspeicheranalyse mit dem Volatility-Framework, Artefakt-analyse

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	2	0
Fertigkeiten	5	4	5	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	5	4	5	6	0

11

Internettechnologien

(2 Monate / 150 Lernstunden / 5 ECTS)

* 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.

Inhalt:
- **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.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	4	5	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	5	6	0

12

Netzsicherheit 1

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls erkennen die Studierenden/Teilnehmer die wichtigen Strukturen von Sicherheits-mechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln.
* Sie können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern.
* Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, die sie auf neue Protokolle und Verfahren übertragen werden können.
* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
* Sie haben die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten haben ein „gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten entwickelt.

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

- Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	3	4	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	4	6	0

13	**Netzsicherheit 2** (2 Monate / 150 Lernstunden / 5 ECTS) * Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der dritten und vierten Ebene des OSI-Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. * Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. * Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. * Sie haben die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten haben ein „gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten entwickelt. Inhalt: - **SSL** **Praktische Übung:** Erzeugung eines eigenen (Digitalen) SSL-Zertifikats. - **SSH** **OpenPGP** **Praktische Übung:** Erzeugung eines eigenen PGP-Schlüssels zum Ver- und Entschlüsseln von Dateien. - **S/MIME** **Praktische Übung:** Manipulation S/MIME signierter Mails ohne Gültigkeit der Signatur zu beeinflussen. - **DNSSEC** - Neben den Systemen werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Als Grundlage werden kurz die Transportprotokolle TCP und UDP behandelt.	

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	3	4	2	0
Fertigkeiten	5	4	5	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	4	3	5	6	0

14

Netzsicherheit 3

(2 Monate / 150 Lernstunden / 5 ECTS)

* Den teilnehmenden Studierenden soll ein weit gefächertes Wissen über die häufigsten Schwachstellen in Webapplikationen vermittelt werden. Außerdem sollen sie lernen, wie sie derartige Schwachstellen manuell finden können, ohne die Hilfe von automatisierten Webapplikations-Scannern in Anspruch zu nehmen. Darüber hinaus lernen die Studierenden entsprechende Schutzmaßnahmen sowie deren Wirksamkeit kennen.

- Im Laufe der Lehrveranstaltung sollen die Studierenden eine fiktive Online-Banking-Applikation angreifen und dabei die im Laufe der Veranstaltung erlernten Methoden und Techniken einsetzen. Dieses beinhaltet folgende Themengebiete:
  - Cross Site Scripting (XSS)
  - Cross Site Request Forgery (CSRF)
  - Session Hijacking
  - Session Fixation
  - SQL Injection (SQLi)
  - Local/Remote File Inclusion (LFI/RFI)
  - Path Traversal
  - Remote Code Execution (RCE)
  - Logical Flaws
  - Information Leakage
  - Insufficient Authorization

- Das Wissen der Studierenden wird zudem durch externe Experten aus der Industrie und IT-Sicherheits-Szene, die in Vorträgen über verschiedene Thematiken der Webapplikations-Sicherheit referieren werden, angereichert.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	4	5	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	4	4	2	0
Über alle Kategorien	4	4	5	6	0

15

SPAM

(2 Monate / 150 Lernstunden / 5 ECTS)

* 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.

Inhalte:

- 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-Etymologie, 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.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	3	5	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	5	6	0

16

Sicherheit mobiler Systeme

(2 Monate / 150 Lernstunden / 5 ECTS)

* 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.

Inhalt:
- 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**: Analyse von Mobilfunksignalen
  - Auswertung von Signalen
  - Dekodierung
- **Praktische Übung:** Analyse einer Android-App
  - Statische Analyse
  - Dynamische Analyse

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	5	6	0

17

Computerstrafrecht

(2 Monate / 150 Lernstunden / 5 ECTS)

* 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.

Inhalt:
- 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

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	2	0
Fertigkeiten	4	4	4	2	0
Kompetenz	4	3	4	2	0
Über alle Kategorien	4	3	4	6	0

18	**Computerstrafprozessrecht** (2 Monate / 150 Lernstunden / 5 ECTS) * 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. Inhalt: - 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 Übung:** Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse: 4 / 4 / 4 / 2 / 0 Fertigkeiten: 4 / 4 / 4 / 2 / 0 Kompetenz: 4 / 3 / 4 / 2 / 0 Über alle Kategorien: 4 / 3 / 4 / 6 / 0
19	**Europäisierung & Internationalisierung des Strafrechts** (2 Monate / 150 Lernstunden / 5 ECTS) * Nach erfolgreichem Abschluss des Moduls haben die Studierenden Kenntnisse über die Grundzüge internationalen Rechts und supranationaler Regelungsmodelle. In den Modulen Computerstrafrecht oder Computerstrafprozessrecht erworbene Kenntnisse werden vor diesem Hintergrund neu betrachtet. Die Studierenden sind in der Lage, grundsätzliche Aussagen über die Probleme der internationalen strafrechtlichen Zusammenarbeit zu treffen und die aktuelle Entwicklung kritisch zu hinterfragen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompentenz. Inhalte: - Das Modul widmet sich in mehreren Studienbriefen dem Prozess der Europäisierung und Internationalisierung des Strafrechts. Die in den Modulen Computerstrafrecht und Computerstrafprozessrecht nur gestreiften Aspekte der zunehmenden Internationalisierung des Strafrechts werden an dieser Stelle vertieft. Die zunehmende Europäisierung des Rechts macht es besonders im Strafrecht notwendig, bisherige nationalstaatliche Regelungsansätze zu überdenken. Dazu ist es unerlässlich, sich auch mit den durch das Europarecht definierten Vorgaben auseinanderzusetzen. - **Praktische Übung:** Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse: 4 / 4 / 4 / 2 / 0 Fertigkeiten: 4 / 3 / 4 / 2 / 0 Kompetenz: 4 / 3 / 4 / 2 / 0 Über alle Kategorien: 4 / 3 / 4 / 6 / 0