Modulhandbuch

Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik (ohne angestrebte Abschlussprüfung)

Inhaltsverzeichnis

MNR	*MC*	*Modulbezeichnung*	*Seite*
0001	03-WSRGA	Rechtsgrundlagen Allgemein	4
0002	03-WSRGC	Rechtsgrundlagen Cybercrime	5
0003	03-WSDF	Digitale Forensik Grundlagen	6
0004	03-WSBS	Betriebssysteme	7
0005	03-WSNCF	Netzwerke und Cloudforensik	9
0006	03-WSFS	Filesysteme	10
0007	03-WBGE	IT-Forensische Gutachten in der Praxis (fakultativ)	11
0008	03-WSWZ	Werkzeuge	12

Hinweis zur Bestellung der Prüfer:

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

Formen für Prüfungsvorleistungen und Prüfungssleistungen:

PVL-Formen: Te = Testat, s = schriftlich, m = mündlich, Prüfungsformen: M = Modulprüfung, Pl = Prüfungsleistung, s = schriftlich, m = mündlich, a = alternativ, sn = sonstige, PA = Projektarbeit

Sonstige Abkürzungen:

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

0001 Rechtsgrundlagen Allgemein

Modulname:	**Rechtsgrundlagen Allgemein**	*Unterrichtssprache:*	deutsch
Modulnummer:	0001	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSRGA	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	1
Ausbildungsziele:	Die Teilnehmer verfügen über Basiswissen im Bereich Rechtswissenschaften, um die für einen kriminaltechnischen Sachverständigen einer jeweiligen Fachrichtung relevanten rechtlichen Grundbedingungen und Zusammenhänge verstehen und erläutern zu können. Er muss sich insbesondere über seine Rechte und Pflichten im Strafverfahren auskennen. Lernziele in diesem Modul sind demnach Kenntnisse im Ablauf von Hauptverhandlungen (Gericht, Instanzen und Spruchkörper) und die Rolle der Beteiligten, mit dem Schwerpunkt auf den Sachverständigen im Strafprozess.		
Lehrinhalte:	Grundrechte im Grundgesetz Unterscheidung zwischen privatem und öffentlichem Recht Gerichtsaufbau, Instanzenzug, Spruchkörper Hauptverhandlung und Rolle der Beteiligten Rechtsmittel: Berufung und Revision Prozessablauf; Sachverständigen Rolle		
Lernmethoden:			
Literatur:			
Arbeitslast:	**15** Stunden Lehrveranstaltungen **75** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Rechtsgrundlagen Allgemein	1	0	0	0		Ms/60	3

0002 Rechtsgrundlagen Cybercrime

Modulname:	**Rechtsgrundlagen Cybercrime**	*Unterrichtssprache:*	deutsch
Modulnummer:	0002	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSRGC	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	1
Ausbildungsziele:	Die Teilnehmenden sollen in der Lage sein, Sachverhalte unter den einschlägigen materiellrechtlichen und formalrechtlichen Vorschriften subsumieren zu können. Die Teilnehmenden machen sich mit dem Begriff Cybercrime vertraut und sind in der Lage Cybercrime im engeren und weiteren Sinne auf aktuelle Straftatbestände und Straftatbestandsmerkmale anzuwenden.		
Lehrinhalte:	Die strafbare Handlung: Aufbau der Straftat, Tatbestandsmäßigkeit, objektiver und subjektiver Tatbestand, Rechtswidrigkeit und Schuldhaftigkeit Erscheinungsformen strafbarer Handlungen Cybercrime: Definition und Grundbegriffe Strafrecht- verfahrensrecht Ablauf und Grundsätze eines Strafverfahrens Ausgewählte Gesetzestexte Tatmittel Internet Phänomene im Bereich Cybercrime Objektive und subjektive Straftatbestandsmerkmale an aktuellen Phänomenen		
Lernmethoden:			
Literatur:			
Arbeitslast:	**15** Stunden Lehrveranstaltungen **75** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Rechtsgrundlagen Cybercrime	1	0	0	0		Ms/60	3

0003 Digitale Forensik Grundlagen

Modulname:	**Digitale Forensik Grundlagen**	*Unterrichtssprache:*	deutsch
Modulnummer:	0003	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSDF	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	1
Ausbildungsziele:	Gewinnung eines Überblicks über Aufgaben und Anforderungen der digitalen Forensik. Kennenlernen der wichtigsten Methoden und Vorgehensweisen zur Sicherung und Untersuchung digitaler Spuren sowie Vermittlung von Grundlegendem Wissen über Hard- und Software im Zusammenhang mit dem Arbeitsumfeld der digitalen Forensik. Weiterhin sollen Grundlagen im Bereich der Informationstechnik vermittelt werden, die für den gesamten Bereich der Digitalen Forensik notwendig sind. Dabei wird auf grundlegende mathematische Kenntnisse eingegangen, die für die Informatik von Bedeutung sind. Zusätzlich wird grundlegendes Wissen aus dem Bereich der technischen Informatik vermittelt. Dazu gehören Aufbau von Rechnersystemen, Datenträger und Grundlagen der Betriebssysteme.		
Lehrinhalte:	Einordnung der Digitalen Forensik; Informationstechnik und Forensische Sicherung Anwendungsfälle und typische Szenarien Digitale Spuren und deren Eigenschaften Vorgehensmodelle in der Digitalen Forensik Sicherung digitaler Spuren und Anforderungen Ausgewählte Gebiete der Digitalen Forensik		
Lernmethoden:			
Literatur:			
Arbeitslast:	**30** Stunden Lehrveranstaltungen **120** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Digitale Forensik Grundlagen	2	0	0	0		Ms/90	5

0004 Betriebssysteme

Modulname:	**Betriebssysteme**	*Unterrichtssprache:*	deutsch
Modulnummer:	0004	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSBS	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	1
Ausbildungsziele:	Nach diesem Modul verstehen die Studierenden den klassischen Aufbau der von Neumann Architektur mit den wichtigsten Ebenen für die Funktion eines Betriebssystems. Die Teilnehmenden kennen die verschiedenen Klassifikationen von Betriebssystemen und können gängige aktuelle Windows-, Linux und macOS-Systeme installieren, administrieren und verstehen Hintergrundprozesse, welche bedeutsam für die forensische Auswertung sind.		
Lehrinhalte:	Betriebssystemarchitektur: • Ebenen eines Rechnersystems • Definition, schematischer Aufbau und Aufgabe von Betriebssystemen • Ressourcenverwaltung durch Betriebssysteme • Betriebssystemarchitekturen • Zugriffsverwaltung • Prozesse, Tasks und Threads • Speicherverwaltung und Speicherzugriffe • Datenträgeranbindung Windows: • Einrichtung und Administration aktueller Betriebssysteme • Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, Event-Logging, Registrierungsdatenbank, Betriebssystemartefakte, Benutzerkonten und Gruppen) • Verwendung von Netzwerken und Schutzmechanismen • Virtualisierung und Subsysteme in Windows Linux: • Historie und aktuelle Distributionen • Filesystem Hierarchy Standard • Paket- und Dienstmanager • Sicherheitsmechanismen in Linux • Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, Logging, Konfiguration, Betriebssystemartefakte, Benutzerkonten und Gruppen) macOS: • Speicherstrukturen • SQLite und Plist verstehen und anwenden • Systeminterne Spuren und forensische Aspekte (zuletzt verwendete Dokumente, Kommunikationsapps, Spotlight und Browser-Artefakte) • Logdateien • Umgang mit Diskimages und Backupmöglichkeiten (iOS und Time-Machine) • Grundlagen und Integration von iCloud		
Lernmethoden:	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase praktischen Aufgaben Hochschule Mittweida / BKA Wiesbaden		
Literatur:	Mandel,P.: Grundkurs Betriebssysteme. Wiesbaden: Vieweg, 4. Aufl. 2014 Schneider, U. (Hrsg.): Taschenbuch der Informatik. München: Hanser (Leipzig: Fachbuchverlag), 7. Auflage, 2012 Tanenbaum, A.S.: Moderne Betriebssysteme, 3. Aufl., Pearson Studium, 2009		
Arbeitslast:	**90** Stunden Lehrveranstaltungen **120** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Heiko Rittelmeier (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:	*Modulstruktur*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
	Betriebssysteme	4	0	2	0			7
	Teilprüfung (TP) Windows						Pl4s/60	
	Teilprüfung (TP) Linux						Pl4s/60	
	Teilprüfung (TP) macOS						Pl4s/60	

0005 Netzwerke und Cloudforensik

Modulname:	**Netzwerke und Cloudforensik**	*Unterrichtssprache:*	deutsch
Modulnummer:	0005	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSNCF	*Häufigkeit:*	Sommersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	1
Ausbildungsziele:	Die Teilnehmenden soll den Aufbau und die möglichen Funktionen des Internets verstehen, um daraus resultierende digitale Spuren bewerten und Ermittlungsansätze aufzeigen zu können. Das Modul Netzwerke bietet eine Einführung in das Themengebiet Netzwerktechnik und Cloudforensik. Ziel ist es, Grundlagenwissen aus diesem Gebiet zu vermitteln. Nach Besuch des Moduls sind die Studierenden mit der Funktionsweise unterschiedlicher Netzwerkdienste vertraut und kennen Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten.		
Lehrinhalte:	Entwicklung und Struktur weltweiter Netzwerke Cloud-Computing Architekturen Virtualisierung (Speicher- und Netzwerkvirtualisierung) OSI Schichtenmodell Protokolle (IP, ICMP, TCP, TPC, UDP, Mac, ARP) IPv4 vs. IPv6 DNS und URL Möglichkeiten der Verbindungshardware Technische Grundlagen (Hardware und Software) Funktionsweise E-Mail, FTP, Peer to Peer Anonymisierungsdienste TOR-Netzwerk Herausforderungen Cloudforensik im Bereich SaaS und PaaS		
Lernmethoden:	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase		
Literatur:	Michael Gregg: Hack the Stack. Syngress, 2006. Ryan Trost: Practical Intrusion Analysis. Addison-Wesley, 2009 Michael S Collins: Network Security Through Data Analysis: Building Situational Awareness. O'Reilly, 2014. Michael Messner: Metasploit. dpunkt, 2012 Eric Amberg: Linux-Server mit Debian 8 GNU/Linux. Mitp, 2015. Limoncelli, T.A., Hogan, C.J. et al: The Practice of System and Network Administration. Addison-Wesley Longman 2007. Klaus M. Rodewig: Webserver einrichten und administrieren. Galileo Computing, 2011. Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005.		
Arbeitslast:	**30** Stunden Lehrveranstaltungen **120** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. pol. Dirk Pawlaszczyk (Dozent, Inhaltverantwortlicher, Prüfer) M.Sc. Philipp Engler (Dozent, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Netzwerke und Cloudforensik	2	0	0	0		Ms/90	5

0006 Filesysteme

Modulname:	**Filesysteme**	*Unterrichtssprache:*	deutsch
Modulnummer:	0006	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSFS	*Häufigkeit:*	semesterweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	2

Ausbildungsziele:

Das Module Filesysteme erläutert, was ein Dateisystem ist und wozu diese entwickelt wurden. Gleichzeitig werden Grundlegende Begriffe wie Sektoren und Cluster und deren Bedeutung erklärt. Nach erfolgreicher Teilnahme am Modul sind die Studierenden befähigt, gängige Dateisysteme zu verstehen und forensische Analysen manuell durchzuführen.

Lehrinhalte:

Einführung:

- Grundbegriffe und Bedeutung von Dateisystemen
- Festplattenpartitionierung (Master Boot Record und GPT Partitionierung)
- Besonderheiten in Dateisystemen (Zeitstempel, Slackspeicher, Disableing Last Access

Timestamp)

Windows Dateisysteme:

- FAT-Dateisysteme (Aufbau FAT-Partition, Strukturen im FAT Dateisystem, Löschung und Wiederherstellung von Daten in FAT)
- NTFS-Dateisystem (Historie, Aufbau von NTFS, Strukturen im NTFS, Speichern und Löschen von Daten in NTFS)
- ExFAT Dateisystem (Aufbau ExFAT-Partition, Strukturen im ExFAT Dateisystem, Löschung und Wiederherstellung von Daten in ExFAT)
- LDM, WSS und ReFS Dateisystem

Linux Dateisysteme:

- Ext-Dateisystem (Klassifikation von Linux Dateisysteme, Grundlegendes und Komptabilität von Extx, Besonderheiten von Ext3 und Ext4, Journaling in Ext, Sparse, Flex und Meta Blockgroups)
- F2FS Dateisystem (Aufbau Log Structured Dateisysteme, Aufbau von F2FS, Strukturen im F2FS, Speichern und Löschen von Daten in F2FS)
- Logical Volume Manager / Device Mapping

macOS Dateisysteme:

- HFS+ (Historie, Aufbau von HFS, Strukturen im HFS,Besonderheiten der B-Tree Strukturen, Speichern und Löschen von Daten in HFS)
- APFS (Neuerungen und Features von APFS, Aufbau von APFS Partitionen, Forensische Untersuchung von APFS Container

Lernmethoden:

Vorlesung online

Einzel- und Gruppenübungen während der Online-Phase

praktischen Aufgaben

Literatur:

Arbeitslast:

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

Anbieter: 03 Fakultät Angewandte Computer- und Biowissenschaften

Dozententeam (Rollen): Prof. Heiko Rittelmeier (Dozent, Inhaltverantwortlicher, Prüfer)

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Filesysteme	3	0	2	1		Ms/90	7

0007 IT-Forensische Gutachten in der Praxis (fakultativ)

Modulname:	**IT-Forensische Gutachten in der Praxis (fakultativ)**	*Unterrichtssprache:*	deutsch
Modulnummer:	0007	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WBGE	*Häufigkeit:*	Wintersemester
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	2
Ausbildungsziele:			
Lehrinhalte:			
Lernmethoden:			
Literatur:			
Arbeitslast:	**30** Stunden Lehrveranstaltungen **60** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher, Prüfer) Prof. Heiko Rittelmeier (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
IT-Forensische Gutachten in der Praxis (fakultativ)	0	0	2	0		Msn/PA	3

0008 Werkzeuge

Modulname:	**Werkzeuge**	*Unterrichtssprache:*	deutsch
Modulnummer:	0008	*Abschluss:*	ohne angestrebte Abschlussprüfung
Modulcode:	03-WSWZ	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	*Regelsemester:*	2
Ausbildungsziele:	In diesem Modul werden Teilnehmende dazu befähigt, Werkzeuge zur forensischen Auswertung digitaler Systeme zu verwenden und eigenständig forensische Analysen an Datenträgern und IT-Systemen durchzuführen. Die Teilnehmenden können unter anderem X-Ways, Autopsy, DumpIt, LiME und Volatility anwenden und kennen weitere Werkzeuge zur forensischen Analyse von Datenträgern.		
Lehrinhalte:	spezielle Werkzeuge • Tools zur Datensicherung (GUI, CLI, Datensicherungsformate, etc.) • Tools zur Analyse und Aufbereitung (xmount, scalpel, etc.) spezielle Methoden der digitalen Forensik • Sicherung defekter Datenträger • RAID Sicherung • RAM Sicherung • Carving • GdPDU/GoBD Datenuntersuchung mit Forensik Frameworks • X-Ways • Sleuthkit/Autopsy Virtualisierung • Grundlagen der Virtualisierung • Datensicherung innerhalb Virtualisierungsumgebungwen (Docker, QEMU, ESxi, Hyper V, OpenVZ, etc.) • Virtualisierung von Beweismitteln (Grundlagen, Einrichtung, Rücksetzen von Benutzerkennungen, etc.)		
Lernmethoden:	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase praktischen Aufgaben		
Literatur:			
Arbeitslast:	**90** Stunden Lehrveranstaltungen **120** Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften		
Dozententeam (Rollen):	Prof. Heiko Rittelmeier (Dozent, Inhaltverantwortlicher, Prüfer)		

Lerneinheitsformen und Prüfungen:

Modulstruktur	*V*	*S*	*P*	*T*	*PVL*	*PL*	*CP*
Werkzeuge	3	0	2	1		Ms/90	7