Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik / IWW
Studiengang Digitale Forensik (M.Sc.)

StuPO 24.1
ab dem Wintersemester 24/25
Ersteller: Maureen Schneider
Verantwortlich: Prof. Dr. German Nemirovski

In Kooperation mit

- *Friedrich-Alexander-Universität Erlangen-Nürnberg und*
- *Universität des Saarlandes, Saarbrücken*

Inhaltsverzeichnis

1 Vorwort 3
2 Übersicht der Modulbeschreibungen 4
3 Qualifikationsziel-Modul-Matrix 5
4 Studiengangs-Kompetenzmatrix 6
5 Modulbeschreibungen 7
Modul: Grundlagen Informatik und Programmierung 7
Modul: Grundlagen Betriebssysteme und Shell-Programmierung 8
Modul: Webtechnologien und Internetdienste 10
Modul: Programmieren und Datenanalyse in der Forensik 12
Modul: Methoden digitaler Forensik 14
Modul: Incident Response 15
Modul: Betriebssystemforensik und -artefakte 17
Modul: Netzwerkforensik und -analyse 19
Modul: Informationsrecht 21
Modul: Reverse Engineering und Malware-Analyse 23
Modul: Datenträgerforensik 25
Modul: Cyberstrafrecht 27
Modul: Browser- und Anwendungsforensik 29
Modul: Live Analyse 30
Modul: E-Evidence 32
Modul: Forensik mobiler Geräte 34
Modul: IT-Strafverfolgung 36
Modul: Wirtschaftskriminalität 37
Modul: Digitale Ermittlungen 39
Modul: Master-Thesis 41

1 Vorwort

Der Studiengang ist als Fernstudium mit integriertem Blended Learning-Ansatz modular mit Studienbriefen, Präsenz- und Onlinephasen sowie Betreuung durch Online-Tutoren und Dozenten aufgebaut. Die Regelstudienzeit beträgt nach § 2 Abs. 1 StuPO bis zum Erreichen des Master-Grades sieben Semester.

Das Studium vermittelt theoretische und praktische Kenntnisse in den Bereichen der Datenträgerforensik, Netzwerkforensik, forensische Methodik und die auf Computer-kriminalität bezogenen rechtlichen Grundlagen. Das Ziel des Studiums ist die Befähigung der Absolventen zu praktischen, konzeptionellen, wissenschaftlichen und juristischen Tätigkeiten im Bereich der Digitalen Forensik.

Im 1. Semester werden die für die Digitale Forensik erforderlichen Grundlagen der Informatik und Informationstechnik vermittelt. Studierende mit einem Erststudium aus dem Bereich Informatik- / Informationstechnik müssen das 1. Semester nicht besuchen und erhalten eine Anrechnung von Amts wegen. Im 2. Semester werden Forensik-spezifische Grundlagen zum Programmieren und zu IT-Angriffstechniken behandelt. Aufbauend darauf werden im 3. bis 6. Semester Module angeboten, die jeweils die Themenschwerpunkte Datenträger, Netzwerke, Methodik und rechtlicher Rahmen haben und eine Einführung sowie Vertiefung in die Digitale Forensik darstellen.

Mit der Masterthesis zeigen die Teilnehmer am Ende ihres Studiums, dass sie die Fähigkeit besitzen, Theorien und Techniken mit Reflexion auf die eigene berufliche Qualifizierung an einem anwendungsbezogenen Beispiel wissenschaftlich umzusetzen.

2 Übersicht der Modulbeschreibungen

1. Semester

201 Grundlagen Informatik und Programmierung
202 Grundlagen Betriebssysteme und Shell-Programmierung
203 Webtechnologien und Internetdienste

2. Semester

204 Programmieren und Datenanalyse in der Forensik
205 Methoden Digitaler Forensik
206 Incident Response

3. Semester

207 Betriebssystemforensik und -artefakte
208 Netzwerkforensik und -analyse
209 Informationsrecht

4. Semester

210 Reverse Engineering und Malware-Analyse
211 Datenträger-Forensik
212 Cyberstrafrecht

5. Semester

213 Browser- und Anwendungsforensik
214 Live Analyse
215 E-Evidence

6. Semester

216 Forensik mobiler Geräte
217 Juristisches WPM (Wirtschaftskriminalität oder IT-Strafverfolgung)
218 Digitale Ermittlungen

7. Semester

219 Masterthesis

3 Qualifikationsziel-Modul-Matrix

Die Qualifikationsziele im Studiengang Digitale Forensik 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.

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
Modul M201	Grundlagen Informatik und Programmierung	4	2	1	1	0
Modul M202	Grundlagen Betriebssysteme und Shell-Programmierung	4	2	1	1	0
Modul M203	Webtechnologien und Internetdienste	4	2	1	1	0
Modul M204	Programmieren und Datenanalyse in der Forensik	5	2	1	2	0
Modul M205	Methoden Digitaler Forensik	5	1	2	1	1
Modul M206	Incident Response	6	2	1	2	1
Modul M207	Betriebssystemforensik und -artefakte	7	2	2	2	1
Modul M208	Netzwerkforensik und -analyse	7	2	2	2	1
Modul M209	Informationsrecht	4	0	1	1	2
Modul M210	Reverse Engineering und Malware-Analyse	6	1	2	2	1
Modul M211	Datenträgerforensik	6	1	2	2	1
Modul M212	Cyberstrafrecht	6	0	2	2	2
Modul M213	Browser- und Anwendungsforensik	5	0	2	2	1
Modul M214	Live Analyse	5	0	2	2	1
Modul M215	E-Evidence	6	0	2	2	2
Modul M216	Forensik mobiler Geräte	5	0	2	2	1
Modul M217	Juristisches WPM Wirtschaftskriminalität oder IT-Strafverfolgung	6	0	2	2	2
Modul M218	Digitale Ermittlungen	6	0	2	2	2
Modul M219	Masterthesis	7	1	2	2	2

4 Studiengangs-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
Modul M201 - Grundlagen Informatik und Programmierung		6	6					6			6
Modul M202 - Grundlagen Betriebssysteme und Shell-Programmierung		6	6	6				6			6
Modul M203 - Webtechnologien und Internetdienste	6	6	6	6				6			6
Modul M204 - Programmieren und Datenanalyse in der Forensik	7	7	7	7			7	7		7	7
Modul M205 - Methoden Digitaler Forensik	7	7		7	7	7	7	7		7	7
Modul M206 - Incident Response	7	7	7	7			7	7	7	7	7
Modul M207 - Betriebssystemforensik und -artefakte	7	7	7	7			7	7		7	7
Modul M208 - Netzwerkforensik und -analyse	7	7	7	7	7		7	7	7	7	7
Modul M209 - Informationsrecht		7	7	7			7	7	7	7	7
Modul M210 - Reverse Engineering und Malware-Analyse	7	7	7	7	7		7	7	7	7	7
Modul M211 - Datenträgerforensik	7	7	7	7	7		7	7	7	7	7
Modul M212 - Cyberstrafrecht	7	7	7	7	7	7	7	7	7	7	7
Modul M213 - Browser- und Anwendungsforensik	7	7	7	7	7	7	7	7	7	7	7
Modul M214 - Live Analyse	7	7	7	7	7	7	7	7	7	7	7
Modul M215 - E-Evidence	7	7	7	7	7	7	7	7	7	7	7
Modul M216 - Forensik mobiler Geräte	7	7	7	7	7	7	7	7	7	7	7
Modul M217 - Juristisches WPM Wirtschaftskriminalität oder IT-Strafverfolgung	7	7	7	7	7	7	7	7	7	7	7
Modul M218 - Digitale Ermittlungen	7	7	7	7	7	7	7	7	7	7	7
Modul M219 - Masterthesis	7	7	7	7	7	7	7	7	7	7	7

Niveau des Studiengangs: 7

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

5 Modulbeschreibungen

<table>
<tr><td colspan="7">Modul: Grundlagen Informatik und Programmierung</td></tr>
<tr><td colspan="2">Kennnummer
201</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
LV 10110 – Grundlagen Informatik und Programmierung
LV 10120 - Laborarbeit (unbenotet)</td><td>Sprache
deutsch</td><td>Kontakt-zeit
20 h</td><td>Selbst-studium
130 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Präsenzanteil: 20h
• Vorlesungsteil: 8h
• Virtuelle Lehre: 5h
• Übungsteil: 2h
• Prüfungsvorbereitungsveranstaltung: 4h
• Prüfung: 1h

Fernstudienanteil: 130h
• Selbstgesteuertes Lernen: 80h
• Wahrnehmen der Online Betreuung und Beratung: 20h
• Ausarbeiten von Aufgaben: 10h
• Individuelle Prüfungsvorbereitung der Studierenden: 20h

1 KP=30h, 20% der Summe in Präsenz</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die wesentlichen Merkmale und Komponenten eines Rechnersystems sowie grundlegende Methoden der Informatik. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, Methoden der Informatik zur Konzeptionierung von Programmabläufen umzusetzen. [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels des spezifischen Vokabulars auszudrücken, sich verständlich zu machen und andere zu verstehen. [Kommunikation, 7]

Selbstständigkeit
Die Studierenden sind in der Lage, eigene Lösungsansätze zu prüfen. [Reflexivität, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
• Informationsspeicherung auf einem Computer, Einheiten, Größenordnung, Zahlensysteme, Zeichensätze/ -kodierung, Datentypen
• Computersysteme: Aufbau eines Rechners, Rechnerstruktur, Zentraleinheiten, Prozessorarchitektur, Speicherhierarchie, Peripherie-Komponenten
• Software-Komponenten: Firmware, Betriebssystem, Anwendungsprogramme, verteilte Anwendungen, Erstellungsprozess von Software</td></tr>
</table>

	• Einführung in die Programmiersprachen: Programmentwurf (Pseudocode u. Ablauf-diagramme), Ablaufsteuerung, Entwicklungsumgebungen, Aspekte der theoretischen Informatik • Netzwerkgrundlagen: Klassifizierung, Protokolle und Internetprotokolle, Einführung in T/IP-Netzwerke, Subnetze, IP-Routing, Ports, Domain Name System • IT-Sicherheitsaspekte in Rechnern und Netzwerken, Angriffsmechanismen, Schutzmechanismen, Update-Mechanismen, Verschlüsselung
	Empfohlene Literaturangaben: • Gumm, H.-P.(2016). Einführung in die Informatik. München; Wien: Oldenbourg • Hellmann, R. (2016). Einführung in den Aufbau moderner Computer. München; Wien: Oldenbourg: Oldenbourg Wissenschaftsverlag • Henning, P. A. (2007). Taschenbuch Programmiersprachen. München: Fachbuchverlag Leipzig im Carl-Hanser-Verlag • 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.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Keine; empfohlen: Grundfertigkeiten im Umgang mit IT-Systemen
6	**Prüfungsformen***:* K75 (5 ECTS) Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen der Laborarbeit
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Hower Dozenten: Prof. Dr. Hower
10	***Optionale Informationen:***

Modul: Grundlagen Betriebssysteme und Shell-Programmierung						
Kennnummer 202	**Workload** 150 h	**Modulart** P	**Studiensemester** 1		**Dauer** 1 Semester	**Häufigkeit** SS
1	**Lehrveranstaltung(en)** LV 10210 - Grundlagen Betriebssysteme und Shell-Programmierung LV 10220 - Laborarbeit (unbenotet)		**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:**					

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die wesentlichen Merkmale und Komponenten eines Betriebssystems sowie grundlegende Methoden der Informatik. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, Skripte zur Systemadministration sowie für forensische Zweck zu konzeptionieren und zu erstellen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels des spezifischen Vokabulars auszudrücken, sich verständlich zu machen und andere zu verstehen. *[Kommunikation, 6]* *Selbstständigkeit* Die Studierenden sind in der Lage, eigene Lösungsansätze zu erarbeiten. *[Reflexivität, 7]*
4	**Inhalte*:*** • Benutzung eines Betriebssystems am Beispiel UNIX: Konzepte und Entwicklung von Betriebssystemen, Linux, Benutzerverwaltung, Dateisystem (Dateien, Verzeichnisse), Zugriffskontrolle, Logdateien; Kommandozeileninterpreter (Shell) und Skriptprogrammierung mit der Shell, Zugriff auf Systeminformationen; forensische Auswertung einiger Dateien • Arbeiten mit einer Shell unter Windows: PowerShell, Commandlets, Grundlagen der Shell-Programmierung unter Windows, Objekte, Datentypen, Funktionen, Variablen, Pipeline und Objekte, Arrays, Hash-Tabellen, Ablaufsteuerung, Fehlerbehandlung, Zugriff auf Systeminformationen. Forensische Auswertungen mittels grafischer Benutzeroberfläche oder mittels automatisierbare Skripte *Empfohlene Literaturangaben:* • Glatz, E. (2019). Betriebssysteme: Grundlagen, Konzepte, Systemprogrammierung. Heidelberg: dpunkt • Weltner, T. (2018). Grundlagen & Scripting-Praxis für Einsteiger. Unterschleißheim: O'Reilly

	• Schwichtenberg, Holger (2020): Windows PowerShell 5.0 und 7 - Das Praxisbuch: Einführung und Lösungen für Windows- Administratoren • Günther, (K. (2014) Bash - kurz & gut. O'Reilly Verlag GmbH & Co. KG Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Keine; empfohlen: Grundfertigkeiten im Umgang mit IT-Systemen
6	**Prüfungsformen***:* K75 (5 ECTS) Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen der Laborarbeit
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:***

Modul: Webtechnologien und Internetdienste					
Kennnummer 203	**Workload** 150 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** SS

1	**Lehrveranstaltung(en)** LV 10310 - Webtechnologien und Internetdienste LV 10320 - Laborarbeit (unbenotet)	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	• Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen wesentliche Merkmale Komponenten und Mechanismen der Internettechnologie. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, http-basierte Inhalte zu analysieren und zu erstellen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels des spezifischen Vokabulars auszudrücken, sich verständlich zu machen und andere zu verstehen. *[Kommunikation, 7]* *Selbstständigkeit* Studierende können neue Internet-Anwendungen eigenständig untersuchen und erforschen sowie mit der Fachcommunity diskutieren Die Studierenden sind in der Lage, eigene Lösungsansätze zu prüfen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Client- und Serveranwendungen im Internet: Funktionen und Anwendungen, HTTP-Protokolle • Markup Sprachen: HTML, XHTML, XML, CSS: Syntax und Struktur • JavaScript, Ajax und Integration in Webseiten • Erstellung von Webseiten • Sicherheitsaspekte webbasierter Anwendungen • Forensische Erkenntnisse aus der Internet-Nutzung • Aufzeichnung, Analyse und Decodierung von http(s)-Netzwerkverkehr mit Wireshark *Empfohlene Literaturangaben:* • Seite von „SELFHTML WIKI“; zuletzt abgerufen: 20.06.2023. https://wiki.selfhtml.org/ • Clemens Gull, Stefan Münz (2014): HTML5 Handbuch. 10. Auflage. Herausgeber: Franzis Verlag GmbH • Ackermann, P. (2018) JavaScript: Das umfassende Handbuch für Anfänger, Fortgeschrittene und Profis. Herausgeber: Bonn Rheinwerk Verlag • Chappell, Laura (2017): Wireshark 101: Essential Skills for Network Analysis. 2. Auflage. Herausgeber: Laura Chappell University Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Keine; empfohlen: Grundfertigkeiten im Umgang mit IT-Systemen
6	**Prüfungsformen***:* K75 (5 ECTS)

	Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen der Laborarbeit
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Fein Dozenten: David Schlichtenberger, M. Sc.
10	***Optionale Informationen:***

Modul: Programmieren und Datenanalyse in der Forensik						
Kennnummer 204	**Workload** 150 h	**Modulart** P	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** LV 20110 - Vorlesung Programmieren und Datenanalyse in der Forensik LV 20120 - Laborarbeit	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Summe: 150h Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz						
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden haben aktives Wissen zu modernen Programmierparadigmen in den Sprachen Assembler, C und Python. Die Studierenden kennen grundlegende Methoden der Datenanalyse. *[Wissen, 7]* *Kompetenz Fertigkeiten*					

	Die Studierenden können Problemstellungen in Algorithmen und Datenstrukturen umsetzen und diese programmtechnisch implementieren. Die Studierenden können grundlegende Datenanalysen durchführen. *[Instrumentelle Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden können sich mit dem Fachvokabular der Informatik in der Community über Software-Lösungen informieren und austauschen. *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können eigenständig Lösungsansätze entwickeln und verfolgen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Assemblerprogrammierung Befehle, Register, Schritte der Programmausführung, Debugging • Grundlagen der C-Programmierung: Datentypen, Kontrollfluss, Funktionen, Arrays, Zeiger, Umgang mit Entwicklungswerkzeugen • Einführung in Python: Objekte und Datentypen, Ablaufsteuerung, Funktionen, Dateien, Module, Objektorientiertes Programmieren (Konzepte, Klassen, Vererbung), Forensische Anwendungen • Datenanalyse in Python: Auswertung von Daten (u.a. mit numpy, pandas), insb. mit forensischer Motivation
	Empfohlene Literaturangaben: • Randall Hyde (2021): The Art of 64-Bit Assembly, Volume 1: x86-64 Machine Organization and Programming No Starch Press • Manfred Dausmann, Ulrich Bröckl, Joachim Goll (2014). C als erste Programmier-sprache. Wiesbaden: Teubner Verlag • Klein, T. (2003): Buffer Overflows und Format-String-Schwachstellen: Funktionsweisen, Exploits und Gegenmaßnahmen; Heidelberg: dpunkt-Verlag • Ernesti, J. & Kaiser, P. (2020). Python 3. Bonn: Rheinwerk Computing Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Kenntnisse aus M201, M202, M203
6	**Prüfungsformen***:* K75 (5 ECTS) Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen der Laborarbeit
8	***Verwendbarkeit des Moduls:***

	Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Fein Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:***

Modul: Methoden digitaler Forensik					
Kennnummer 205	**Workload** 150 h	**Modulart** P	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 20210 – Vorlesung Methoden Digitaler Forensik und prakt. Arbeit	**Sprache** deutsch	**Kontakt-zeit** 30 h	**Selbst-studium** 120 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**

Präsenzanteil: 30h

- Vorlesungsteil: 10h
- Übungsteil: 5h
- Praktischer Teil: 10h
- Prüfungsvorbereitungsveranstaltung: 4h
- Prüfung: 1h

Fernstudienanteil: 120h

- Durcharbeiten der Studienbriefe: 50h
- Durcharbeiten des Online-Lernmaterials: 10h
- Wahrnehmen der Online Betreuung und Beratung: 10h
- Ausarbeiten von Aufgaben: 30h
- Individuelle Prüfungsvorbereitung der Studierenden: 20h

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

Die Studierenden können die Basisterminologie forensischer Arbeit definieren und wiedergeben. *[Wissen, 7]*

Kompetenz Fertigkeiten

Die Studierenden sind in der Lage, die Qualität forensischer Dokumentation zu definieren und einzuschätzen. Sie können einfache Anwendungen auf forensische Spuren hin untersuchen. *[Instrumentelle Fertigkeiten, 7]*

Sozialkompetenz

Die Studierenden sind in der Lage, die Fachterminologie der Forensik anzuwenden, Sachverhalte darin auszudrücken, und sich mit anderen darüber zu verständigen. *[Kommunikation, 7]*

Selbstständigkeit

Die Studierenden können einfache Anwendungen eigenständig auf forensische Spuren hin untersuchen und die Korrektheit ihrer Funde selbst überprüfen. *[Eigenständigkeit/Verantwortung, 7]*

4 **Inhalte*:***

- Einführung in die forensischen Wissenschaften im Allgemeinen und in die digitale Forensik im Speziellen
- Methodische Fundierung der digitalen Forensik: Einbettung der digitalen Forensik in die klassische kontinuierliche (analoge) Forensik

	• Dokumentation von forensischen Untersuchungen, forensische Prinzipien bei Sammlung, Aufbereitung und Analyse digitaler Spuren • Analyse forensischer Berichte • Anwendung forensischer Prinzipien am Beispiel einer einfachen Anwendungsanalyse
	Empfohlene Literaturangaben: • Dan Farmer, Wietse Venema: Forensic Discovery. Addison-Wesley, 2005. • Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2. Auflage, 2004. • Alexander Geschonneck: Computer Forensik. dpunkt Verlag, 2. Auflage, 2006. • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015.
5	**Teilnahmevoraussetzungen:** Grundlegende Programmierkompetenzen sind empfehlenswert
6	**Prüfungsformen***:* Praktische Arbeit
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der prakt. Arbeit. Hier wird anhand eines Experiments der Aspekt des wissenschaftlichen Hinterfragens in der Digitalen Forensik erarbeitet.
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Dozent: Prof. Dr. Felix Freiling
10	***Optionale Informationen:***

Modul: Incident Response

Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
206	150 h	P	2	1 Semester	WS

1	**Lehrveranstaltung(en)** LV 20310 - Vorlesung Incident Response	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Begrifflichkeiten im Gebiet der IT-Sicherheit. Die Studierenden kennen die Schwachstellen, Bedrohungen, Angreifer und Angriffe, wie sie typischerweise von Malware, Netzwerk-Angriffen und Internetangriffen ausgehen. Die Studierenden kennen die Möglichkeiten des Security-Engineerings und der Sicherheitskonzepte. Die Studierenden kennen die Methoden zu Incident Response. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können IT-Angriffe erkennen und klassifizieren. Die Studierenden sind in der Lage, IT-Sicherheitsmechanismen anzuwenden und auf ihre Wirksamkeit zu prüfen. Die Studierenden können Incident-Response Abläufe und Aktivitäten ausführen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, in einem Team IT-Konzepte zu entwickeln und laufende IT-Angriffe zu entdecken und abzuwehren. *[Team-/Führungsfähigkeit, 7]* *Selbstständigkeit* Die Studierenden können in kritischen Situationen der IT-Sicherheit selbständig Entscheidungen vorbereiten und verantwortlich treffen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Grundlagen der IT-Sicherheit: Begriffe, Konzepte, Mechanismen; Umsetzung von Schutzzielen • Security Engineering: Konzeption, Aufbau und Betrieb von sicheren Rechnersystemen; Analyseverfahren und Sicherheitsmodelle • IT-Bedrohungen: Schadsoftware, Bedrohung aus dem Rechnernetz, Bedrohungen aus dem Internet; Experimente mit Angriffsvektoren; Abwehrmechanismen • Maschinelles Lernen [ML]: ML aus Verteidiger-Sicht; ML aus Angreifer-Sicht • Incident Response: Vorgehensmodell; Phasen des Incident Response Management; Fallbeispiele; Praktisches Training zu Incident Response mit aktiven Angriffen • Penetration Testing: Zielsetzung, Methodik und Durchführung; die wichtigsten Methoden zur Informationsbeschaffung und zum Eindringen in Systeme; Vulnerability Assessment in Theorie und Praxis. *Empfohlene Literaturangaben:* • Claudia Eckert (2023): IT-Sicherheit - Konzepte - Verfahren - Protokolle. Oldenbourg Verlag, München, überarbeitete und erweiterte Auflage

	• BSI (Bundesamt für Sicherheit in der Informationstechnologie) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2020.pdf?__blob=publicationFile&v=1. • BSI (Bundesamt für Sicherheit in der Informationstechnologie). Ein Praxis-Leitfaden für IT-Sicherheit-Pentrationstest. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3 • Jürgen Ebner (2020): Einstieg in Kali Linux: Penetration Testing und Ethical Hacking mit Linux. mitp Verlags GmbH & Co. KG • Lorenz Kuhlee, Victor Völzow (2012): Computerforensik Hacks. O'Reilly Verlag. • National Institute of Standards and Technology. Computer Security Incident Handling Guide, 2012. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist • Johansen, Gerard (2022).: Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response. Packt Publishing; 3. Edition Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** • Obligatorisch: Kenntnisse aus den Modulen M201, M202, M203, M204 • Empfohlen: Nutzersicht von vernetzten Rechnern, Programmierkenntnisse in Python
6	**Prüfungsformen***:* Hausarbeit und Referat (5 ECTS)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Hausarbeit Bestehen des Referats
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:***

Modul: Betriebssystemforensik und -artefakte					
Kennnummer 207	**Workload** 150 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** SS

1	**Lehrveranstaltung(en)** LV 30110 - Vorlesung Betriebssystemforensik und -artefakte	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	LV 30120 - Laborarbeit (unbenotet)				
2	**Lehrform(en) / SWS:** Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden haben vertieftes Wissen zu Betriebssystemmechanismen. Die Studierenden kennen die Bedeutung des Betriebssystems für die IT-Sicherheit und für die Entstehung von forensischen digitalen Spuren. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können aktiv digitale forensische Spuren in den Betriebssystemen Windows und Linux korrekt erheben, analysieren und beschreiben. Die dazu erforderlichen Methoden können sie professionell anwenden. Sie sind in der Lage, erforderlichenfalls Werkzeuge hierfür anzupassen oder zu erstellen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden können die aus der forensischen Analyse von Spuren in Betriebssystemen gewonnenen Ergebnisse fachkundig in der Community darstellen und diskutieren. *[Kommunikation, 7]* *Selbstständigkeit* Sind in der Lage, komplexe Fragestellungen selbständig zu bearbeiten, den eigenen Fortschritt adäquat zu bemessen und die gewonnenen Erkenntnisse zu überdenken. Die Studierenden gehen verantwortlich damit um, dass ihre Berichte für andere entscheidende Auswirkungen haben können. *[Reflexivität, 7]*				
4	**Inhalte*:*** • Eigenschaften von Betriebssystemen: Prinzipien, Ansätze, grundsätzliche Mechanismen, Untersuchung von Betriebssystemen mit Systemprogrammen • Prozesse: Threads, Scheduling, Interprozesskommunikation, Implementierung bei Unix & Windows; Schadsoftware und Prozesse • Speicherverwaltung: Memory Management, Virtueller Speicher, Paging, Implementierung bei Unix & Windows				

	• Ein/- Ausgabe: Geräte, Konzepte und Architekturen für Input / Output, Gerätetreiber • Das MS-Windows-Betriebssystem aus Sicht des Forensikers: Systemarchitektur, Sicherheit, Spuren • Windowsforensik I: Spezifische Formate und deren Analyse; Speicherorte, Analysemethoden, Auswertung von Event-Logs • Windowsforensik II: Registry; Aufbau, Forensische Auswertung; Artefaktanalyse an Fallbeispielen • Windowsforensik III: Spezifische Spuren in Windows 10/11; Methoden der Untersuchung in Betriebssystemen
	Empfohlene Literaturangaben: • Tanenbaum, A. S. (2016). Moderne Betriebssysteme. München; Boston [u.a.]: Pearson Studium • Glatz, E. (2019). Betriebssysteme: Grundlagen, Konzepte, System-Programmierung. Heidelberg: dpunkt • Mark E. Russinovich, Andrea Allievi, Alex Ionescu (2017, 2021). Windows internals Part1 and 2: Microsoft Press • Johansen, Gerard (2022).: Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response. Packt Publishing; 3. Edition. Academic Press • H. Carvey (2016). Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. Syngress • Bruce Nikkel (2021): Practical Linux Forensics: A Guide for Digital Investigators. No Starch Press Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** • Obligatorisch: Kenntnisse aus den Modulen M201, M202, M203, M204, M205 • Empfohlen: Anwenderkenntnisse Windows und Unix, Programmierkenntnisse in Python
6	**Prüfungsformen***:* K75 (5 ECTS) Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen der Laborarbeit
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:***

Modul: Netzwerkforensik und -analyse					
Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

208	150 h	P	3	1 Semester	SS

1	**Lehrveranstaltung(en)** LV 30210 - Vorlesung Netzwerkforensik und -analyse	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**

Präsenzanteil: 20h

- Vorlesungsteil: 8h
- Virtuelle Lehre: 5h
- Übungsteil: 2h
- Prüfungsvorbereitungsveranstaltung: 4h
- Prüfung: 1h

Fernstudienanteil: 130h

- Selbstgesteuertes Lernen: 80h
- Wahrnehmen der Online Betreuung und Beratung: 20h
- Ausarbeiten von Aufgaben: 10h
- Individuelle Prüfungsvorbereitung der Studierenden: 20h

1 KP=30h, 20% der Summe in Präsenz

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

Die Studierenden haben vertiefte Kenntnisse zu Netzwerkstrukturen, zu Protokollen und zu Netzwerkdiensten. Die Studierenden kennen die zu erwartenden digitalen Spuren, die bei der Netzwerkbenutzung entstehen können. *[Wissen, 7]*

Kompetenz Fertigkeiten

Die Studierenden können Netzwerkverkehr aufzeichnen, analysieren und interpretieren. Die Studierenden können aus dem Netzwerkverkehr, aus Clients und Servern sowie aus aktiven Netzwerkkomponenten digitale Spuren fachkundig erheben, analysieren und darstellen. *[Instrumentelle Fertigkeiten, 7]*

Sozialkompetenz

Die Studierenden können die aus der forensischen Analyse von Spuren im Rechnernetz gewonnenen Ergebnisse fachkundig in der Community darstellen und diskutieren. *[Kommunikation, 7]*

Selbstständigkeit

Die Studierenden sind in der Lage, komplexe Fragestellungen selbständig zu bearbeiten, den eigenen Fortschritt adäquat zu bemessen und die gewonnenen Erkenntnisse zu überdenken. Die Studierenden gehen verantwortlich damit um, dass ihre Berichte für andere entscheidende Auswirkungen haben können. *[Reflexivität, 7]*

4 **Inhalte*:***

- Rechnernetze: Begriffe und Leistungsmerkmale
- Netzwerk-Codierung und –Zugriff: Codierung von Informationen, Frame-Bildung, Fehlererkennung, zuverlässige Übertragung

	• ISO/OSI-Schichtenmodell, Grundlagen von LAN, WAN, WLAN, Ethernet-Protokoll • Konzeption und Analyse von Rechnernetzen Netzwerk-Komponenten, Routing, Vermittlung und Weiterleitung Analyse mit PowerShell, Bordwerkzeugen, Wireshark und anderen Werkzeugen • TCP/IP: IP-Adressierung, Subnetting, CIDR; IPv6-Spezifica und Erweiterungen; TCP/IP-Frames: Aufbau und Auswertung • Sicherheitsmechanismen in Rechnernetzen: Verschlüsselung, VLAN, Firewall, Intrusion Detection • Forensische Untersuchungen im Rechnernetz log-Dateien, Router-Logs, Netzwerkverkehrsanalyse; Forensische Analyse von Router, Proxa, IDS und Firewall im Detail • Network Security Monitoring: Datenaufzeichnungsphase, Detektionsphase, Analysephase; Forensische Gesichtspunkte und Nutzungsmöglichkeiten
	Empfohlene Literaturangaben: • Peterson, L./ Davie, B. (2021): Computer Networks. Morgan Kaufmann-Verlag • Tanenbaum, A. S. (2021). Computer Networks. Pearson Studium • Laura Chappell (2014): Wireshark Network Analysis. Verlag: Laura Chappell University • Johansen, Gerard (2022).: Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response. Packt Publishing; 3. Edition. Academic Press • Eckert, C. (2023). IT-Sicherheit Konzepte - Verfahren - Protokolle. München Wien: Oldenbourg Verlag • Davidoff, S., Ham, J. (2012). Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall • Chris Sanders, Jason Smith (2016): Applied Network Security Monitoring; Collection, Detection, and Analysis. Syngress Publishing, Inc. Elsevier, Inc. • Nipun Jaswal (2019: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Packt Publishing Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** • Obligatorisch: Kenntnisse aus den Modulen M201, M202, M203, M204, M205, M206 • Empfohlen: Erfahrungen in der Nutzersicht von vernetzten Rechnern, Erfahrungen im Umgang mit virtuellen Maschinen, Programmierkenntnisse in Python
6	**Prüfungsformen***:* Hausarbeit (Ha) + Referat (Rf)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Hausarbeit Bestehen des Referats
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):***

	Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:***

Modul: Informationsrecht					
Kennnummer 209	**Workload** 150 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** SS

1	**Lehrveranstaltung(en)** LV 30310 – Vorlesung Informationsrecht	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2	**Lehrform(en) / SWS:** Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 20h • Übungsteil: 5h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 50h • Durcharbeiten des Online-Lernmaterials: 10h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 20h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden besitzen nach erfolgreichem Abschluss des Moduls grundlegende Kenntnisse über Konzepte, Funktionen und Erscheinungsformen des Rechts, Rechtsanwendung und -durchsetzung sowie Arbeitsmethoden. Sie besitzen einen Überblick über die zentralen Rechtsprobleme der digitalen Forensik. Sie kennen internationale, insbesondere europäische juristische Rahmenbedingungen. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können juristische Fachbegriffe identifizieren und einordnen und Rechtsfragen gutachterlich bearbeiten. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Sie können die gewonnenen Erkenntnisse reflektieren und juristische Fragestellungen in der Gruppe erläutern und diskutieren. *[Kommunikation, 7]*

	Selbstständigkeit Die Teilnehmer/innen sind in der Lage, juristische Fragestellungen einzuordnen, Problempunkte zu erkennen, diese selbständig gutachterlich zu bearbeiten bzw. durch entsprechende vertragliche Gestaltung Vorsorge zu treffen. *[Reflexivität, 7]*
4	**Inhalte*:*** Im Informationsrecht werden, aufbauend auf einer kurzen Übersicht über die Rechtssystematik und einer kurzen Einführung in zentrale Grundlagen der Rechtsordnung, folgende Bereiche behandelt: • Übersicht über das Zivilrecht: u.a. Probleme beim Vertragsschluss, der Vertragsgestaltung und der Vertragsbeendigung; Gewährleistungsrechte beim Hard-und Softwarekauf und –miete; Verfahrensrecht: Durchsetzung zivilrechtlicher Ansprüche • Grundlagen des Strafrechts • Kauf im Internet • Urheberrecht und Recht am eigenen Bilde • Rechtsfragen der Open Source Software, Unterschiede einzelne Lizenztypen • Urheber-und Patentschutz bei Software; u.a. Lizenzrechte, Rechtsschutz und Verwertung von Computerprogrammen, Rechtsschutz für Datenbanken • Markenrecht • Wettbewerbsrecht und Abmahnung • Datenschutzrecht inkl. EU-DSGVO • Neuere Rechtsentwicklungen: EU-Richtlinien und EU-Verordnungen, TKG, TMG, IT-SicherheitsG, VertrauensdiensteG, EU-Richtlinie Urheberrecht • Internetrecht: Domainrecht, Rechtsfragen Homepage und Impressum
	Empfohlene Literaturangaben: • Thomas Hoeren: Internetrecht; Online-Version; März 2023; Verfügbar unter: https://www.itm.nrw/lehre/materialien/ • Jochen Schneider: Handbuch des EDV-Rechts: IT-Vertragsrecht, Datenschutz, Rechtsschutz; 5., Aufl. Köln: O. Schmidt 2017
5	**Teilnahmevoraussetzungen:** Juristische Grundkenntnisse und Zusammenhänge, grundlegende IT-Kenntnisse
6	**Prüfungsformen***:* Klausur K100
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Gerblinger Dozenten: Prof. Gerblinger
10	***Optionale Informationen:***

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

Modul: Reverse Engineering und Malware-Analyse					
Kennnummer 210	**Workload** 150 h	**Modulart** P	**Studiensemester** 4	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 40110 - Vorlesung Reverse Engineering und Malware-Analyse und Prakt. Arbeit	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**

Summe: 150h

Präsenzanteil: 25h

- Vorlesungsteil: 10h
- Übungsteil: 5h
- Praktischer Teil: 10h

Fernstudienanteil: 120h

- Durcharbeiten der Studienbriefe: 50h
- Durcharbeiten des Online-Lernmaterials: 10h
- Wahrnehmen der Online Betreuung und Beratung: 10h
- Prüfungsleistung, Praktische Arbeit: 55h

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

Die Studierenden können den Begriff „Reverse Engineering“ einordnen und definieren. Sie können die typischen Einsatzgebiete von Reverse Engineering benennen. Die Studierenden haben fundierte Kenntnisse in der Programmierung von IA-32 auf Maschinenebene. 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 vertiefte 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. *[Wissen, 7]*

Kompetenz Fertigkeiten

Die Studierenden haben die Fähigkeit, systemnahe Programme zu erstellen und zu verstehen. Diese Kenntnisse können die Studierenden bei der Analyse unbekannter Malware Binaries einsetzen. *[Systemische Fertigkeiten, 7]*

Sozialkompetenz

Aufgrund der Teamarbeit, unter anderem am Präsenzwochenende, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *[Kommunikation, 7]*

Selbstständigkeit

	Durch das eigenverantwortliche Entwickeln von Programmen und die Programmanalyse erweitern die Studierenden ihr selbstständiges Handeln. Durch das Verfassen eines Berichts wird die Selbstsicherheit der Studierenden gestärkt. *[Reflexivität, 7]*
4	**Inhalte*:*** • Reverse Engineering, Zielsetzung und Grenzen • Aufbau und Assemblerprogrammierung von Intel IA-32 • Grundlagen von Microsoft Windows, Aufbau und Datenstrukturen von Windows-Software • Decompilierung, Erkennung von Optimierungen und Obfuscation • Benutzung des Disassemblers/Debuggers IDA Pro
	Empfohlene Literaturangaben: • Eldad Eilam: Reversing: Secrets of Reverse Engineering, John Wiley & Sons, 2005 • Chris Eagle. The IDA Pro Book. No Starch Press, 2008. • Michael Sikorski and Andrew Honig. Practical Malware Analysis, No Starch Press, 2012
5	**Teilnahmevoraussetzungen:** • Grundlagenmodule • Programmierkenntnisse in C
6	**Prüfungsformen***:* Praktische Arbeit
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der praktischen Arbeit
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Dr. Werner Massonne Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Dozent: Dr. Werner Massonne Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
10	***Optionale Informationen:***

Modul: Datenträgerforensik					
Kennnummer 211	**Workload** 150 h	**Modulart** P	**Studiensemester** 4	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 40210 - Vorlesung Datenträgerforensik	**Sprache** deutsch/ englisch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Präsenzanteil: 20h • Vorlesungsteil: 8h • Virtuelle Lehre: 5h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 4h				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	• Prüfung: 1h Fernstudienanteil: 130h • Selbstgesteuertes Lernen: 80h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 10h • Individuelle Prüfungsvorbereitung der Studierenden: 20h 1 KP=30h, 20% der Summe in Präsenz
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen Aufbau, Strukturen und Wirkungsweisen der Dateisysteme FAT, NTFS und EXT. Die Studierenden kennen verschiedene Konzepte zum Partitionieren, zum Zusammenfassen und Aufteilen von physischen und logischen Datenträgern. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, auch komplex angelegte Datenträger forensisch korrekt zu duplizieren und zu sichern. Die Studierenden können nach dem Stand der Technik auch komplex angelegte digitale Spuren in verschiedenen Dateisystemen analysieren und die resultierenden Erkenntnisse aufbereiten. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, die Ergebnisse ihrer Analysen einem fachkundigen Kreis zu erläutern und mit Experten dazu eine Diskussion zu führen. Die Studierenden gehen verantwortlich damit um, dass ihre Berichte für andere entscheidende Auswirkungen haben können. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden sind in der Lage, komplexe Aufgabenstellungen selbständig zu bearbeiten, den eigenen Fortschritt adäquat zu bemessen und die gewonnenen Erkenntnisse zu überdenken. *[Reflexivität, 7]*
4	**Inhalte*:*** • Übersicht der Speichermedien: Festplatten, Flashspeicher, SSD; Speicher-Server und Cloud; prinzipielle Analysemöglichkeiten; Forensische Software kommerziell und Open Source • Festplattentechnik: Aufbau, Arten, Standards, Schnittstellen, Partitionssysteme, Formatierung • Forensische Sicherung von Datenträgern und Informationen: Lesen des Originals, Schreiben und Integritätsprüfung der Kopie; Duplikation und logische Sicherung • Datenträgeranalyse: Auswerten von Partitionsinformationen und von versteckten/gelöschten Bereichen; Formate, Methoden, Werkzeuge • Besondere Problemstellungen: verschlüsselte Datenträger, SSD-Korrosion • Methodik der Datenträgeranalyse in Kategorien nach Brian Carrier: Dateisystem-, Inhalt-, Metadaten-, Dateinamen-, Anwendungs-Kategorie; bilden von Timelines • FAT-Dateisystem: Analyse in Kategorien an praktischen Beispielen; Besonderheiten von Zeitstempeln und Allokationsalgorithmen • Ext-Dateisystem: Analyse in Kategorien an praktischen Beispielen; Besonderheiten der Blockstruktur und der Versionen; forensische Auswertung des Journals und gelöschter Metadaten • NTFS-Dateisystem: Analyse in Kategorien an praktischen Beispielen; Besonderheiten der MFT und deren forensische Auswertung; verschlüsselte Datenträger; forensische Auswertung von Zeitstempeln

	Empfohlene Literaturangaben: • Brian Carrier (2005): File System Forensic Analysis. Addison-Wesley Professional • Alexander Geschonneck(2014). Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären. Heidelberg: dpunkt Verlag • BSI: M 6.126 Einführung in die Computer-Forensik. 2009 • Eoghan Casey (2011). Handbook of Digital Forensics and Investigation. Amsterdam: Academic Press Inc. • Dan Farmer (2009). Forensic Discovery. Pearson Addision Wesley • Dewald, Andreas ; Freiling, Felix C. (2013): Forensische Informatik. BoD – Books on Demand. • André Årnes (2017): Digital Forensics. Wiley. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** • Obligatorisch: Kenntnisse aus den Modulen M201, M202, M203, M204, M205, M206, M207 • Empfohlen: Grundlegende Erfahrungen mit dem forensischen Sichern und Auswerten von digitalen Spuren
6	**Prüfungsformen***:* Hausarbeit Ha Referat Rf
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Hausarbeit Bestehen des Referats
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Fein Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:***

Modul: Cyberstrafrecht

Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
212	150 h	P	4	1 Semester	WS

1	**Lehrveranstaltung(en)** LV 40310 – Klausur	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Summe: 150h Synchrone Lehre: 20h • Übungsteil: 14h • Vorlesungsteil: 4h • Prüfung: 2h				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Asynchrone Lehre (Fernstudienanteil): 130h • Durcharbeiten der Studienbriefe: 55h • Durcharbeiten des Online-Lernmaterials: 15h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 30h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen nach erfolgreichem Abschluss des Moduls die Grundprinzipien des Strafrechts und die Voraussetzungen strafrechtlicher Verantwortlichkeit in Bezug auf typische Straftatbestände, zu deren Begehung Informationstechnologie eingesetzt wird oder bei denen Informationstechnologie Angriffsobjekt ist. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können nach erfolgreichem Abschluss des Moduls die Grundprinzipien des Strafrechts und die Voraussetzungen strafrechtlicher Verantwortlichkeit auf Sachverhalte anwenden, bei denen zur Tatbegehung Informationstechnologie eingesetzt wird oder Informationstechnologie Angriffsobjekt von Straftaten ist und so strafbares von straflosem Verhalten unterscheiden. Sie haben ein Verständnis für die Relevanz der Grundrechte und das Prinzip der Verhältnismäßigkeit für das Strafrecht entwickeln können. Zudem können sie das Strafrecht in die Gesamtrechtsordnung einordnen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden können nach erfolgreichem Abschluss des Moduls strafrechtliche Sachverhalte und deren Beurteilung präsentieren und über die hierbei relevanten Rechts- und Sachfragen in einen interdisziplinären Diskurs eintreten. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden können nach erfolgreichem Abschluss des Moduls die Voraussetzungen typischer IT-Straftaten erkennen und hierdurch digital-forensische Auswertungen rechtssicher und zielgenauer gestalten. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Das Strafrechtssystem vor den Herausforderungen der Informationsgesellschaft • Anwendungs- und Wirkbereich deutscher Normen; Extraterritoriale Ermittlungen • Die strafrechtliche Deliktsprüfung am Beispiel des § 303a StGB (strafrechtliche Fallbearbeitung; Tatbestand; Rechtswidrigkeit; Schuld) • Täterschaft und Teilnahme, Versuchs- und Fahrlässigkeitsdelikte im Computerstrafrecht • Strafrechtlicher Schutz informationstechnischer Systeme (Vertraulichkeit, Integrität und Verfügbarkeit) • Computerstrafrechtlicher Eigentums- und Vermögensschutz • Pornografie- und Äußerungsdelikte *Empfohlene Literaturangaben:* • Brodowski, Dominik / Freiling, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft; Forschungsforum Sicherheit, Berlin 2011

	• Eisele, Jörg: Computer- und Medienstrafrecht; C. H. Beck, München 2013 • Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht; Springer, 3. Auflage; Berlin 2023 • Malek, Klaus / Popp, Andreas / Diana Nadeborn: Strafsachen im Internet; C.F. Müller, 3. Auflage, Heidelberg 2015
5	**Teilnahmevoraussetzungen:** Grundlegende Kenntnisse über Konzepte, Funktionen und Erscheinungsformen des Rechts, über die Rechtsanwendung und -durchsetzung sowie über juristische Arbeitsmethoden. Studierende sollen einen Überblick über die zentralen Rechtsprobleme der digitalen Forensik besitzen sowie juristische Fachbegriffe identifizieren und einordnen können.
6	**Prüfungsformen***:* Klausur K120
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Dominik Brodowski, LL.M. (UPenn), Universität des Saarlandes, Saarbrücken (UdS) Dozent: Prof. Dr. Dominik Brodowski, LL.M. (UPenn)
10	***Optionale Informationen:***

Modul: Browser- und Anwendungsforensik					
Kennnummer 213	**Workload** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** SS

1	**Lehrveranstaltung(en)** LV 50110 – Prakt. Arbeit LV 50120 – Referat	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**

Summe: 150h

Präsenzanteil: 20h

- Vorlesungsteil: 3h
- Präsentationsvorbereitung: 2h
- Kolloquiumsteil: 15h

Fernstudienanteil: 130h

- Durcharbeiten der Studienbriefe: 10h
- Ausarbeiten einer Anwendungsanalyse: 100h
- Individuelle Prüfungsvorbereitung der Studierenden: 20h

1 KP=30h, 20% der Summe in Präsenz

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

Die Studierenden verfügen über grundlegende Methoden und spezialisierte Techniken zur forensischen Analyse von digitalen Anwendungsspuren. *[Wissen, 7]*

Kompetenz Fertigkeiten

Die Studierenden sind in der Lage, neue Verfahren zur Analyse neuer Applikationen zu entwickeln. *[Systemische Fertigkeiten, 7]*

Analyseergebnisse können unter verschiedenen Maßstäben beurteilt werden. *[Beurteilungsfähigkeit, 7]*

Sozialkompetenz

Die Ergebnisse einer komplexeren forensischen Anwendungsanalyse können einem Fachpublikum vorgestellt und mit ihm diskutiert werden. *[Kommunikation, 7]*

Selbstständigkeit

Analysemethoden und Techniken zur Untersuchung unbekannter Applikationen kann selbstständig erschlossen werden. *[Lernkompetenz, 7]*

4 **Inhalte*:***

Ein Großteil der Systeminteraktion erfolgt heute durch Anwendungsprogramme wie Browser, E-Mail-Clients, oder Office-Software. Die Spuren, die dadurch auf der Festplatte oder im Speicher entstehen, sind für eine Ermittlung in der Regel hochgradig relevant.
Zusätzlich zur Identifikation von interessanten Dateien, die beim Verwenden von Anwendungen angelegt, modifiziert oder gelöscht werden (vgl. M105), ist auch die Interpretation sowohl solcher Spuren als auch von konkreten Dateiinhalten essentiell, um forensische Fragestellungen zu beantworten. Hierzu zählen

	beispielsweise der Zeitpunkt des letzten Programmstarts, ob eine bestimmte Anwendungsaktion durch einen Benutzer ausgeführt wurde, oder ob eine zurückliegende Installation trotz Deinstallation nachgewiesen werden kann. Solche Sachverhalte lassen sich etwa mit der Ermittlung charakteristischer Spuren belegen. In dieser Lehrveranstaltung untersucht jede/r Teilnehmer/in eigenständig eine existierende, forensisch relevante Anwendung, verfasst einen forensischen Bericht über das Untersuchungsvorgehen und die ermittelten Spuren und vertritt diese Analyse im Rahmen eines wissenschaftlichen Fachvortrages vor einem kritischen Publikum.
	Empfohlene Literaturangaben: • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Kompetenz in forensischer Methodik (wie sie etwa in Modul M205 und M211 vermittelt werden), sowie Programmierkompetenzen und Grundkompetenzen in Betriebssystem- und Netzwerkforensik (wie sie etwa in den Modulen M207 und M208 vermittelt werden)
6	**Prüfungsformen***:* Praktische Arbeit Referat
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die Hausarbeit dokumentiert die Ergebnisse der praktischen Arbeit. Die Ergebnisse der praktischen Arbeit werden am Präsenzwochenende vorgestellt. Die ECTS errechnen sich aus den Ergebnissen der praktischen Arbeit und des Referats.
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Prof. Holger Morgenstern, Hochschule Albstadt-Sigmaringen Dozent: Prof. Holger Morgenstern, Hochschule Albstadt-Sigmaringen
10	***Optionale Informationen:***

Modul: Live Analyse

Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
214	150 h	P	5	1 Semester	SS

	Lehrveranstaltung(en)	**Sprache**	**Kontakt-zeit**	**Selbst-studium**	**Credits (ECTS)**
1	LV 50210 – Vorlesung Live Analyse und mündliche Prüfung LV 50220 – Prakt. Arbeit	deutsch	30 h	120 h	5

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

2	**Lehrform(en) / SWS:** Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 10h • Übungsteil: 5h • Praktischer Teil: 10h • Prüfungsvorbereitungsveranstaltung: 4h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 50h • Durcharbeiten des Online-Lernmaterials: 10h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 30h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden können die Basisterminologie der Live Analyse definieren und wiedergeben. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, forensische Untersuchungen an einem laufenden Rechner fachgerecht zu planen und durchzuführen. Sie können eine entsprechende Dokumentation ihres Vorgehens anfertigen und ihr Vorgehen begründen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, die Dokumentation ihrer Live Analyse unter Anwendung der Fachterminologie zu erläutern und sich mit anderen darüber zu verständigen. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden sind in der Lage, forensische Untersuchungen an einem laufenden Rechner eigenständig zu planen und durchzuführen, sowie die Qualität der Untersuchungsergebnisse selbständig einzuschätzen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Einführung in die Techniken zur Sicherung und Analyse nicht-persistenter Beweismittel wie Hauptspeicherinhalte und Netzwerkverkehr • Themen wie die Extraktion kryptographischer Schlüssel, Behandlung von Netzwerkfestplatten sowie der Umgang mit Netzwerkdiensten wie Google oder DNS im Rahmen forensischer Untersuchungen • Überblick über Methoden und Werkzeuge der Live-Analyse • Überblick über die Informationsarten, die durch eine Live Analyse erhoben werden können • Vorgehensmodelle zur Durchführung von Live Response • Einübung einer Live-Analyse im Rahmen einer praktischen Arbeit mit forensischer Dokumentation *Empfohlene Literaturangaben:* • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015 • Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2. Auflage, 2004 • Alexander Geschonneck: Computer Forensik. dpunkt Verlag, 2. Auflage, 2006

	• Stefan Vömel, Felix C. Freiling: A survey of main memory acquisition and analysis techniques for the windows operating system. Digit. Investig. 8(1): 3-22 (2011)
5	**Teilnahmevoraussetzungen:** Obligatorisch: Kompetenz in forensischer Methodik (wie sie etwa in Modul M205 vermittelt werden), sowie Programmierkompetenzen
6	**Prüfungsformen***:* Mündliche Prüfung (20) (2 ECTS) Praktische Arbeit (3 ECTS)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die mündliche Präsentation der prakt. Arbeit ist obligatorischer Bestandteil der Modulteilprüfung „Remote-Prüfung“. Die Gewichtung der Prüfungsleistungen erfolgt gem. § 32 StuPO: Danach sind praktische Arbeit und mündliche Prüfung zwei Teilleistungen, die zu zwei Noten führen. Das Modul ist bestanden, wenn jede der beiden Teilleistungen einzeln erbracht ist. Eine gegenseitige Verrechnung ist hierbei nicht möglich. Es handelt sich hierbei um zwei Modulteilprüfungen.
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Dozent: Prof. Dr. Konstantin Bayreuther, Duale Hochschule Mannheim
10	***Optionale Informationen:***

Modul: E-Evidence					
Kennnummer 215	**Workload** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** SS

1	**Lehrveranstaltung(en)** LV 50310 – Klausur	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Summe: 150h Synchrone Lehre: 20h • Übungsteil: 14h • Vorlesungsteil: 4h • Prüfung: 2h Asynchrone Lehre (Fernstudienanteil): 130h • Durcharbeiten der Studienbriefe: 55h • Durcharbeiten des Online-Lernmaterials: 15h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 30h • Individuelle Prüfungsvorbereitung der Studierenden: 20h				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen nach erfolgreichem Abschluss des Moduls den grundsätzlichen strafprozessualen Rahmen für die Erhebung von Beweismitteln und verfügen über die notwendigen Kenntnisse In den Bereichen Datenschutz und Datenschutzstrafrecht. *[Wissen, 7]* *Kompetenz Fertigkeiten* Aufbauend auf den Grundprinzipien und Grundlagen des Strafprozessrechts haben die Studierenden nach erfolgreichem Abschluss des Moduls die Fertigkeit entwickelt, strafprozessual zulässiges Vorgehen von rechtswidrigem Vorgehen der Ermittlungsbehörden zu unterscheiden. Sie wissen, wann der Anwendungsbereich des Datenschutzrechts eröffnet ist und vermeiden Datenschutzverstöße. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden können nach erfolgreichem Abschluss des Moduls strafprozessuale und datenschutzstrafrechtliche Sachverhalte und deren Beurteilung präsentieren und über die hierbei relevanten Rechts- und Sachfragen in einen interdisziplinären Diskurs eintreten. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden können nach erfolgreichem Abschluss des Moduls die strafprozessualen Voraussetzungen zur Erhebung von Beweismitteln bestimmen und hierdurch digital-forensische Auswertungen rechtssicher und zielgenauer gestalten sowie Datenschutzverstöße vermeiden. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Grundlagen des Strafverfahrens • Grundlagen digitaler Erkenntnisquellen im Strafverfahren • Offene Ermittlungsmethoden • Grundlagen verdeckter bzw. geheimer Ermittlungsmethoden • Schutz von Geschäftsgeheimnissen • Datenschutz und Datenschutzstrafrecht *Empfohlene Literaturangaben:* • Bär, Wolfgang: Handbuch zur EDV-Beweissicherung; Boorberg, Stuttgart 2007 • Brodowski, Dominik / Freiling, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft; Forschungsforum Sicherheit, Berlin 2011 • Eisele, Jörg: Computer- und Medienstrafrecht; C. H. Beck, München 2013 • Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht; Springer, 3. Auflage, Berlin, 2023
5	**Teilnahmevoraussetzungen:** Grundlegende Kenntnisse über Konzepte, Funktionen und Erscheinungsformen des Strafrechts, über die Strafrechtsanwendung und -durchsetzung sowie über juristische Arbeitsmethoden. Studierende sollen einen Überblick über die zentralen materiell-strafrechtlichen Rechtsprobleme der digitalen Forensik besitzen sowie juristische Fachbegriffe insbesondere des materiellen Strafrechts identifizieren und einordnen können.
6	**Prüfungsformen***:* Klausur K120

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Dominik Brodowski, LL.M. (UPenn), Universität des Saarlandes, Saarbrücken (UdS) Dozent: Prof. Dr. Dominik Brodowski, LL.M. (UPenn)
10	***Optionale Informationen:***

Modul: Forensik mobiler Geräte

Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
216	150 h	P	6	1 Semester	WS

1	**Lehrveranstaltung(en)** LV 60100 – Vorlesung Forensik mobiler Geräte	**Sprache** deutsch/ englisch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**

• Präsenzzeit: 15 h
– Vorlesungsteil: 5 h
– Übungsteil: 10 h

• Eigenstudium: 135 h
– Durcharbeiten der Studienbriefe: 75 h
– Online Betreuung und Beratung: 10 h
– Ausarbeiten von Aufgaben: 50 h

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

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. *[Wissen, 7]*

Kompetenz Fertigkeiten

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. *[Systemische Fertigkeiten, 7]*

Sozialkompetenz

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Die Studierenden sind in der Lage, die Ergebnisse ihrer Analysen einem fachkundigen Kreis zu erläutern und mit Experten dazu eine Diskussion zu führen. Die Studierenden gehen verantwortlich damit um, dass ihre Berichte für andere entscheidende Auswirkungen haben können. *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden erlangen die Fähigkeit in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden. *[Reflexivität, 7]*
4	**Inhalte*:*** • Einführung in Android – Aufbau des Android-Systems – Unterschiede zwischen der Java-VM und der Dalvik-VM – Das Android SDK • Einführung in iOS – Aufbau des iOS-Systems – Sicherheitskonzept und Secure-Boot – Verschlüsselung und Datenschutz • 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 Mobilfunkforenisk 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? • Aufbau und Analyse 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 • Obfuskierung – Einführung in Obfuskierung – String-Obfuskierung (XOR, Crypt, ...) – Junkbytes zum Verwirren der Disassembler – Kollision mehrerer Apps zum Verschleiern der Schadfunktion
	Empfohlene Literaturangaben: Siehe Verweise innerhalb der einzelnen Studienbriefe
5	**Teilnahmevoraussetzungen:** Empfohlen:

	• Programmierkenntnisse in Python und Java • gute Linux-/UNIX-Kenntnisse • gute Englischkenntnisse • Kenntnisse der forensischen Grundsätze
6	**Prüfungsformen***:* Klausur K75
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Dozent: Dr.-Ing. Michael Spreitzenbarth
10	***Optionale Informationen:***

Modul: IT-Strafverfolgung					
Kennnummer 217	**Workload** 150 h	**Modulart** WP	**Studiensemester** 6	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 60300 – Seminararbeit + Referat	**Sprache** deutsch/ englisch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Summe: 150h Synchrone Lehre: 20h • Übungsteil: 15h • Vorlesungsteil: 5h Asynchrone Lehre (Fernstudienanteil): 130h • Durcharbeiten der Studienbriefe: 55h • Durcharbeiten des Online-Lernmaterials: 15h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeitung der Seminararbeit: 50h				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen*				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Die Studierenden kennen nach erfolgreichem Abschluss des Moduls die wesentlichen Rechtsgrundlagen der IT-Strafverfolgung einschließlich der Verwertbarkeit im gerichtlichen Verfahren. *[Wissen, 7]*
	Kompetenz Fertigkeiten Die Studierenden sind – auch aufgrund fallgestützter Analysen namhafter verdeckter Strafverfolgungsmaßnahmen – nach erfolgreichem Abschluss des Moduls in der Lage, die investigativen und prozessualen Besonderheiten der IT-Strafverfolgung herauszuarbeiten und sich im dynamisch entwickelnden Strafprozessrecht digitaler Ermittlungen zurechtzufinden. *[Instrumentelle Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden können nach erfolgreichem Abschluss des Moduls strafprozessuale IT-Maßnahmen und deren Beurteilung präsentieren und über die hierbei relevanten Rechts- und Sachfragen in einen interdisziplinären Diskurs eintreten.*[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können nach erfolgreichem Abschluss des Moduls die Spezifika der IT-Strafverfolgung erkennen und hierdurch digital-forensische Auswertungen rechtssicher und zielgenauer gestalten. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Umgang mit digitalen Erkenntnisquellen • Verdeckte bzw. geheime Ermittlungsmaßnahmen • Beachtung strafprozessualer Prinzipien • Zweckänderung und Verwertbarkeit • Grundzüge der Polizeigesetze
	Empfohlene Literaturangaben: • Brodowski, Dominik / Freiling, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft; Forschungsforum Sicherheit, Berlin 2011 • Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht; Springer, 3. Auflage, Berlin 2023 • Matthias Bäcker/Erhard Denninger/Kurt Graulich (Hrsg.): Lisken/Denninger, Handbuch des Polizeirechts. Gefahrenabwehr, Strafverfolgung, Rechtsschutz; C.H. Beck, 7. Auflage, München 2021 • Dennis Heinson: IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen; Mohr Siebeck, Tübingen 2015
5	**Teilnahmevoraussetzungen:** Grundlegende Kenntnisse über Konzepte, Funktionen und Erscheinungsformen des Strafrechts, über die Strafrechtsanwendung und -durchsetzung sowie über juristische Arbeitsmethoden. Studierende sollen einen Überblick über die zentralen materiell-strafrechtlichen Rechtsprobleme der digitalen Forensik besitzen sowie juristische Fachbegriffe insbesondere des materiellen Strafrechts identifizieren und einordnen können.
6	**Prüfungsformen***:* Seminararbeit: Hausarbeit + Referat (5 ECTS)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Seminarabeit. Die mündliche Präsentation des Seminarthemas ist obligatorischer Bestandteil der Modulprüfung "Seminararbeit".
8	***Verwendbarkeit des Moduls:*** Kontaktstudium

9	***Modulverantwortliche(r):*** Prof. Dr. Dominik Brodowski, LL.M. (UPenn), Universität des Saarlandes, Saarbrücken (UdS) Dozent: Prof. Dr. Dominik Brodowski, LL.M. (UPenn)
10	***Optionale Informationen:***

Modul: Wirtschaftskriminalität					
Kennnummer 217	**Workload** 150 h	**Modulart** WP	**Studiensemester** 6	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 60300 – Seminararbeit + Referat	**Sprache** deutsch/ englisch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5

2	**Lehrform(en) / SWS:** Summe: 150h Synchrone Lehre: 20h • Übungsteil: 15h • Vorlesungsteil: 5h Asynchrone Lehre (Fernstudienanteil): 130h • Durcharbeiten der Studienbriefe: 55h • Durcharbeiten des Online-Lernmaterials: 15h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeitung der Seminararbeit: 50h
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen nach erfolgreichem Abschluss des Moduls die Grundlagen des Wirtschafts-strafrechts einschließlich prozessrechtlicher Grundlagen. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden sind – auch aufgrund fallgestützter Analysen namhafter Wirtschaftsstraftaten – nach erfolgreichem Abschluss des Moduls in der Lage, die investigativen und prozessualen Besonderheiten von Wirtschaftsstraftaten herauszuarbeiten und dabei die zur digital-forensischen Auswertung relevanten Schwerpunkte von informationstechnischen Systemen zu erkennen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden können nach erfolgreichem Abschluss des Moduls wirtschaftsstrafrechtliche Sachverhalte und deren Beurteilung präsentieren und über die hierbei relevanten Rechts- und Sachfragen in einen interdisziplinären Diskurs eintreten.*[Kommunikation, 7]* *Selbstständigkeit*

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Die Studierenden können nach erfolgreichem Abschluss des Moduls die Spezifika von Wirtschafts-kriminalität erkennen und hierdurch digitalforensische Auswertungen rechtssicher und zielgenauer gestalten. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** • Zivilrechtliche Bezüge des Wirtschaftsstrafrechts – Rechtsfähigkeit von Unternehmen • Individuelle strafrechtliche Verantwortlichkeit im unternehmerischen Kontext • Strafbarkeit von Unternehmen? • Internal Investigations und Criminal Compliance • Untreue, Korruption, Geldwäsche und Wettbewerbsstrafrecht
	Empfohlene Literaturangaben: • Müller-Gugenberger, Christian (Hrsg.): Wirtschaftsstrafrecht. Handbuch des Wirtschaftsstraf- und -ordnungswidrigkeitenrechts; Schmidt, 8. Auflage, Köln 2024 • Tiedemann, Klaus: Wirtschaftsstrafrecht; Heymanns, 5. Auflage, Köln 2017 • Wittig, Petra: Wirtschaftsstrafrecht; C.H. Beck, 6. Auflage, München 2023
5	**Teilnahmevoraussetzungen:** Grundlegende Kenntnisse über Konzepte, Funktionen und Erscheinungsformen des Strafrechts, über die Strafrechtsanwendung und -durchsetzung sowie über juristische Arbeitsmethoden. Studierende sollen einen Überblick über die zentralen materiell-strafrechtlichen und strafverfahrensrechtlichen Rechtsprobleme der digitalen Forensik besitzen sowie juristische Fachbegriffe identifizieren und einordnen können.
6	**Prüfungsformen***:* Seminararbeit: Hausarbeit + Referat (5 ECTS)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Seminarabeit. Die mündliche Präsentation des Seminarthemas ist obligatorischer Bestandteil der Modulprüfung "Seminararbeit".
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Dominik Brodowski, LL.M. (UPenn), Universität des Saarlandes, Saarbrücken (UdS) Dozent: Prof. Dr. Dominik Brodowski, LL.M. (UPenn)
10	***Optionale Informationen:***

Modul: Digitale Ermittlungen					
Kennnummer 218	**Workload** 150 h	**Modulart** P	**Studiensemester** 6	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** LV 60310 – Prakt. Arbeit LV 60320 – Referat LV 60330 – Hausarbeit (unbenotet)	**Sprache** deutsch	**Kontakt-zeit** 20 h	**Selbst-studium** 130 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:**				

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	Summe: 150h Präsenzanteil: 20h • Vorlesungsteil: 3h • Vortragsvorbereitungsteil: 1h • Kolloquiumsteil: 16h Fernstudienanteil: 130h • Durcharbeiten der Studienbriefe: 10h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 90h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen praktische Abläufe einer digitalen Ermittlung, das Vorgehen beim Erstellen eines Gerichtsgutachtens und dessen Verteidigung vor Gericht *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können komplexere digitale Ermittlungen strategisch planen und für die Untersuchung spezielle, geeignete Techniken der digitalen Forensik auswählen. *[Instrumentelle Fertigkeiten, 7]* Die Studierenden können neue Ermittlungsideen und Verfahren entwickeln. *[Systemische Fertigkeiten, 7]* Die Studierenden können komplexere Ermittlungsergebnisse hinsichtlich ihres Beweis- und Überzeugungswertes vor Gericht einschätzen. *[Beurteilungsfähigkeit, 7]* *Sozialkompetenz* Die Studierenden können einen komplexen Ermittlungsauftrag selbstorganisiert im Team bearbeiten und steuern. *[Team-/Führungsfähigkeit, 7]* Die Studierenden können komplexe Ermittlungsergebnisse sowohl einem fachfremden Publikum („Gericht“), als auch gegenüber Fachexperten („gegnerische Gutachter“) kommunizieren und diskutieren. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden können neue forensische Methoden und Techniken im Rahmen einer komplexen Ermittlung eigenständig erarbeiten und erproben. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Die Methoden der digitalen Forensik werden typischerweise nach Spurenarten getrennt gelehrt und eingeübt (Datenträgeranalyse, Live Analyse etc.). In der Praxis müssen jedoch je nach Fall die richtigen Methoden aus dem zur Verfügung stehenden Spektrum ausgewählt und im Zusammenhang angewendet werden. Hierbei stehen konkrete Ermittlungsfragestellungen im Vordergrund, die zunächst auf technische Fragestellungen reduziert werden müssen. Anschließend erfolgt die Auswahl und Anwendung der Methoden. In dieser Lehrveranstaltung bearbeiten die Teilnehmer in Kleingruppen über das Semester hinweg einen komplexeren Fall und müssen dort die jeweils richtigen Methoden auswählen und anwenden. Die Erkenntnisse sollen in Form eines forensischen Berichts fixiert und im Rahmen des Präsenzwochenendes verteidigt und diskutiert werden. *Empfohlene Literaturangaben:* • Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015

	• Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2. Auflage, 2004 • Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht, 2. Auflage; Berlin: Springer 2012 (Neuauflage angekündigt für August 2020) Weitere Literatur wird im Rahmen des Moduls bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Obligatorisch: Kompetenzen in forensischer Methodik und Datenträgerforensik Empfohlen sind grundlegende Kenntnisse in Computerstrafprozessrecht
6	**Prüfungsformen***:* Praktische Arbeit (4 ECTS) Referat (1 ECTS) Hausarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Das Modul gilt als bestanden, wenn jede Teilprüfung einzeln bestanden wurde. Eine Verrechnung der Teilprüfungsleistungen untereinander ist nicht möglich.
8	***Verwendbarkeit des Moduls:*** Kontaktstudium
9	***Modulverantwortliche(r):*** Prof. Dr. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) Prof. Holger Morgenstern, Hochschule Albstadt-Sigmaringen Dozent: Prof. Holger Morgenstern, Hochschule Albstadt-Sigmaringen
10	***Optionale Informationen:***

Modul: Master-Thesis

Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
219	900 h	P	7	1 Semester	WS und SS

	Lehrveranstaltung(en)	**Sprache**	**Kontakt-zeit**	**Selbst-studium**	**Credits (ECTS)**
1	LV 70110 - Masterthesis LV 70210 - Verteidigung	deutsch/ englisch	20 h	880 h	30

2 **Lehrform(en) / SWS:**

Summe: 900

Präsenzanteil: 20h

- Vorlesungsteil (Kolloquien- Vortragsteilnahme): 10h
- Virtuelle Lehre: 5h
- Prüfungsvorbereitungsveranstaltung: 4h
- Prüfung (Verteidigung): 1h

Fernstudienanteil: 880h

- Literaturstudium und Anleitung zum wissenschaftlichen Arbeiten: 80h
- Praktische Arbeiten für Entwurf, Umsetzung, Test: 500h
- Wahrnehmen der Online Betreuung und Beratung: 100h

Version	Erstellt/geändert von/am	Dokument	Freigabe am/von	Gültig ab
24.1	19.09.2024	Modulhandbuch Digitale Forensik (M.Sc.)Modulhandbuch_Digitale_Forensik_neu	Prof. Dr. Nemirovski	WiSe 24/25

	• Ausarbeiten der Dokumentation, Verteidigung: 150h • Prüfungsvorbereitung Verteidigung: 50h 1 KP=30h
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden sind in der Lage, eine anspruchsvolle wissenschaftliche Problemstellung aus dem Themenfeld des Masterstudiengangs zu definieren bzw. ein Problem in bestehende Theorien einzuordnen, aus den im Studium erlernten Methoden geeignete zu identifizieren, zu diskutieren und anzuwenden. *[Wissen, 7]* *Kompetenz Fertigkeiten* Mit der Master-Thesis zeigen die Studierenden, dass sie unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten können. Sie werden praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master–Thesis dokumentiert die Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. *[Systemische Fertigkeiten, 7]* *Sozialkompetenz* Die Studierenden sind in der Lage, die Erkenntnisse ihrer Master-Thesis im Kolloquium mündlich darzustellen, zu begründen, im Gespräch zu verteidigen und auf neue Fragestellungen einzugehen. *[Kommunikation, 7]* *Selbstständigkeit* Master-Thesis ist das größte Projekt im gesamten Master-Studium, das die Studierenden nachweislich selbstständig und verantwortlich ausführen. *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Inhalte sind abhängig vom Thema der Master-Thesis *Empfohlene Literaturangaben:* • Anleitung zur wissenschaftlichen Arbeit • Projektmanagement und Dokumentation • Vom Kandidaten selber vorzuschlagende vertiefende Literatur
5	**Teilnahmevoraussetzungen:** Das Thema der Master-Thesis wird frühestens nach Abschluss des vierten Studiensemesters ausgegeben. In Ausnahmefällen kann der Prüfungsausschuss auch bei Fehlen einer Prüfungsleistung [aus den ersten vier Semestern] der Zulassung zur Master-Thesis zustimmen. (gem. § 21 Abs. 1 StuPO)
6	**Prüfungsformen***:* Thesis 25 ECTS Verteidigung 5 ECTS
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen die Masterthesis (schriftliche Ausarbeitung). Bestehen der mündlichen Prüfung/Verteidigung.
8	***Verwendbarkeit des Moduls:***

	Master Digitale Forensik
9	***Modulverantwortliche(r):*** 1. Prüfer: Dozenten der Hochschule AS, UdS Saarbrücken oder FAU Erlangen 2. Prüfer: Dozenten der Hochschule AS, UdS Saarbrücken oder FAU Erlangen oder externer Betreuer
10	***Optionale Informationen:***