

2. Abschnitt Einzelregelungen der Studiengänge

§ 33 Studiengang Digitale Forensik (DF)

Zu § 1 Geltungsbereich

Der Studiengang wird von der Fakultät Informatik der Hochschule Albstadt-Sigmaringen, in Kooperation mit weiteren Hochschulen betrieben. Informationen zu den jeweiligen Kooperationspartnern, sowie deren Rechte und Pflichten ergeben sich aus gesonderten Kooperationsvereinbarungen. § 6 Abs. 3 S. 2 LHG bleibt unberührt.

Ziel des Studiengangs

- (1) Der Master-Studiengang Digitale Forensik ist ein berufsbegleitender, weiterbildender Masterstudiengang. Ziel des Studiums ist eine wissenschaftlich fundierte, grundlagenorientierte Ausbildung, die eine breite und in ausgewählten Teilgebieten vertiefte Basis fachlichen Wissens sowie eine umfassende, auch anwendungsorientierte kriminaltechnische Methodenkompetenz vermittelt. Der Theorieanteil erhält besonderes Gewicht im Curriculum, damit der Promotionsbefähigung Rechnung getragen wird.
- (2) Die Vermittlung analytischer, kreativer und gestalterischer Fähigkeiten sowie anwendungsbezogener Fertigkeiten im Umgang mit modernen Hard- und Softwaresystemen unter der Zielsetzung, innovative Methoden zur Sicherung und Auswertung digitaler Spuren zu entwickeln sind oberstes Ziel des Studiums. Großer Wert wird auf die Vermittlung von allgemeinem Anwendungswissen (ökonomische, arbeitswissenschaftliche, ethische und juristische Zusammenhänge) sowie die Integration von Sozialkompetenz (Teamfähigkeit, Führungs- und Kommunikationsfähigkeit, Verantwortungsbewusstsein, strategisches Denken) gelegt. Die Besonderheit des Studiums besteht darin, die Studierenden zur Forschung auf dem Gebiet der digitalen Forensik in Verzahnung mit mehreren Fachdisziplinen aus den Bereichen der Ingenieur-, Wirtschafts- und Rechtswissenschaften zu befähigen, um so dem wachsenden Bedarf von Industrie, Wirtschaft und Gesellschaft im Bereich der digitalen Forensik und Cyberkriminalität Rechnung zu tragen.
- (3) Durch eine enge Verknüpfung von Forschung, Lehre und Praxis wird das Studium in stofflicher und didaktischer Hinsicht an den aktuellen Erkenntnissen des Fachgebiets orientiert.
- (4) Im Hinblick auf die berufsbegleitende Konzeption des Studiengangs werden bei der Bereitstellung des Lehrangebots die Möglichkeiten des Fernstudiums sowie der Informations- und Kommunikationstechnik (multimediales Lernen) eingesetzt. Der Studiengang basiert auf dem Prinzip des „Blended Learning“.

Zu § 2 Regelstudienzeit, Studienaufbau und Modularisierung

Abs. 3

Das Studium wird eingeleitet mit sechs Grundlagenmodulen mit insgesamt 30 ECTS-Punkten, die dem Aufbau und der Vertiefung von Grundlagentheorien im Bereich der Informatik dienen. Darauf aufbauend umfasst das Studium vier Säulen von Themenfeldern, innerhalb derer jeweils drei Module à 5 ECTS-Punkten angeboten werden. Entsprechend dem Lernfortschritt und der Semesterzuordnung werden Basis- und Vertiefungsmodule unterschieden. Das Studium endet mit der Verteidigung der Master-Thesis (§ 23).

Im sechsten Semester haben die Studierenden Lehrveranstaltungen aus dem juristischen Wahlpflichtbereich im Gesamtumfang von 5 ECTS auszuwählen (Wahlpflichtmodul) und die für die ausgewählten Lehrveranstaltungen angegebenen unbenoteten und benoteten Modulteilprüfungen zu erbringen. Die Lehrveranstaltungen der Wahlpflichtmodule sind aus einer Liste auszuwählen, welche vor Beginn jeden Semesters bekannt gegeben wird. Sie werden in der Regel einmal jährlich angeboten. Für jede im Rahmen des Wahlpflichtmoduls gewählte Veranstaltung sind die vorgesehenen Prüfungsleistungen zu erbringen. Die Anmeldung zu den zugehörigen Modulteilprüfungen erfolgt über die Studiengangskoordination. Für Wahlpflichtfächer kann eine Mindestteilnehmerzahl definiert werden, die bei Unterschreiten zur Absage dieser Wahlpflichtfächer führen kann. Die Anmeldung ist bindend.

Modulübersicht

Master-Thesis (219)				
Säule	Säule 1: Rechnersysteme	Säule 2: Vernetzung	Säule 3: Methodik + Wahlpflicht	Säule 4: Rechtlicher Rahmen
Vertiefung	Reverse Engineering und Malware-Analyse (210, FAU)	Browser- und Anwendungsforensik (213, FAU, Alb.-Sig.)	Forensik mobiler Geräte (216, FAU)	Juristisches Wahlpflichtmodul (217, Uds)
	Datenträger-Forensik (211, Alb.-Sig.)	Live Analyse (214, FAU)	Digitale Ermittlungen (218, FAU, Alb.-Sig.)	E-Evidence (215, Uds)
	Betriebssystemforensik und -artefakte (207, Alb.-Sig.)	Netzwerkforensik und -analyse (208, Alb.-Sig.)	Methoden Digitaler Forensik (205, FAU)	Cyberstrafrecht (212, Uds)
Grundlagen II	Incident Response (206, Alb.-Sig.)	Programmieren und Datenanalyse in der Forensik (204, Alb.-Sig.)		Informationsrecht (209, Tübingen)
Grundlagen I	Grundlagen Informatik und Programmierung (201, Alb.-Sig.)	Grundlagen Betriebssysteme und Shell-Programmierung (202, Alb.-Sig.)	Webtechnologie und Internetdienste (203, Alb.-Sig.)	

Zu § 3 Prüfungsaufbau und –fristen; Verlust des Prüfungsanspruchs

Abs. 1

Die Masterprüfung besteht aus Modulprüfungen (§§ 11 ff.), der Master-Thesis (§ 21) und der Verteidigung der Master-Thesis (§ 23).

Zu § 4 ECTS-Punkte und Lernumfang

Abs. 3

Die Zuordnung der ECTS-Punkte zu den einzelnen Modulen (Lehrveranstaltungen) bzw. Teilmodulen ist in der Tabelle „Studien- und Prüfungsplan“ bestimmt. Das Studium ist erfolgreich abgeschlossen, wenn die festgelegten Module mit einem Lernumfang von 120 ECTS-Punkten bestanden sind.

Zu § 6 Prüfungsausschuss

Erweiterung Abs. 1

Der Prüfungsausschuss besteht aus vier Mitgliedern:

- dem Studiendekan des Studiengangs Digitale Forensik - kraft Amtes - im Verhinderungsfall dessen Stellvertreter;
- ein weiteres Mitglied wird vom Fakultätsrat der Fakultät, welcher der Studiengang zugeordnet ist, bestellt aus dem Kreis der Professoren dieser Fakultät oder Professoren anderer Fakultäten, die in dem Studiengang regelmäßig Lehrveranstaltungen abhalten;
- jeweils einem bestellten hauptamtlichen Professor der im Kooperationsvertrag benannten Partner

Für die nicht kraft Amtes dem Prüfungsausschuss angehörenden Mitglieder werden jeweils Stellvertreter bestimmt.

Zu § 7 Zuständigkeiten

Erweiterung Abs. 1

9. über die Genehmigung einer Studienzeiterkürzung (§ 2 Abs. 1)
10. über die nachträgliche Feststellung einer Täuschung bzw. Benutzung nicht zugelassener Hilfsmittel (§ 29 Abs. 2);
11. über Richtlinien zur Gleichwertigkeitsprüfung (§ 19 Abs. 4 a);
12. über Ausnahmen gem. § 21 Abs. 1;

13. über das Bestehen, das Nichtbestehen, die Rücknahme der ergangenen Prüfungsentscheidung (§§ 25 Abs. 1, 28, 29, 18 Abs. 1).

Zu § 12 Prüfungsarten

Abs. 1

Die für den Nachweis einer Modul- bzw. Modulteilprüfung geforderte Prüfungsart wird in der Tabelle „Studien- und Prüfungsplan“ festgelegt.

Zu § 19 Anerkennung und Anrechnung auf Studium und Prüfung

Abs. 1

Studienzeiten, Studienleistungen und Prüfungsleistungen von Studierenden mit einem Erststudium aus dem Bereich Informatik-/ Informationstechnik werden für die Module im ersten Semester (Einführung in die Informatik, Einführung in Betriebssysteme und Methoden der Informatik sowie Internet Grundlagen) von Amts wegen anerkannt. Die Bewertung bei unklarer Zuordnung des Studiums trifft der Prüfungsausschuss.

Zu § 21 Master-Thesis

Abs.1

Das Thema der Master-Thesis wird frühestens nach Abschluss des vierten Studienseesters ausgegeben. In Ausnahmefällen kann der Prüfungsausschuss auch bei Fehlen einer Prüfungsleistung der Zulassung zur Master- Thesis zustimmen.

Abs. 2

Das Thema der Master-Thesis wird über den Prüfungsausschuss (§ 6) von einem Dozenten (Professor oder Lehrbeauftragter) des Studiengangs Digitale Forensik ausgegeben und betreut (= 1. Prüfer).

Abs. 5

Für die Master-Thesis werden 25 ECTS-Punkte vergeben. Wird die Masterthesis im Kontext der beruflichen Tätigkeit erbracht, beträgt die Bearbeitungszeit für die Master- Thesis sechs Monate.

Zu § 22 Mündliche Masterprüfung

Im Studiengang Digitale Forensik findet keine mündliche Masterprüfung statt.

Zu § 23 Verteidigung der Master-Thesis

Abs. 1

Die Bearbeitung der Master-Thesis wird mit einer Verteidigung (Disputation) abgeschlossen. Die Verteidigung der Master-Thesis besteht aus 20 Minuten Vortrag und 20 Minuten Fachdiskussion.

Zu § 26 Mastergrad und Urkunde

Abs. 1

Die Hochschule Albstadt-Sigmaringen verleiht nach bestandener Master-Prüfung im Studiengang Digitale Forensik den Abschlussgrad Master of Science (M.Sc.). Dem Titel wird die Bezeichnung „Digitale Forensik“ hinzugefügt.

Module	Semester	Modulnummer	Vorausgesetzte Modulteilprüfung		Modulprüfung/Modulteilprüfung			
			Unbenotet Art	Prüfungsnummer	Benotet Art (Gewicht)	Unbenotet Art	Prüfungsnummer	ECTS-Punkte
Grundlagen Informatik und Programmierung	1	201	La		K75 (5)			5
Grundlagen Betriebssysteme und Shell-Programmierung	1	202	La		K75 (5)			5
Webtechnologie und Internetdienste	1	203	La		K75 (5)			5
Programmieren und Datenanalyse in der Forensik	2	204	La		K75 (5)			5
Methoden Digitaler Forensik	2	205			Pr (5)			5
Incident Response	2	206			Ha + R (5)			5
Betriebssystemforensik und -artefakte	3	207	La		K75 (5)			5
Netzwerkforensik und -analyse	3	208			Ha + R (5)			5
Informationsrecht	3	209			K100 (5)			5
Reverse Engineering und Malware-Analyse	4	210			Pr (5)			5
Datenträgerforensik	4	211			Ha + R (5)			5
Cyberstrafrecht	4	212			K100 (5)			5
Browser- und Anwendungsforensik	5	213			Pr (3), R (2)			5
Live Analyse	5	214			M20 (2), Pr (3)			5
E-Evidence	5	215			K100 (5)			5
Forensik mobiler Geräte	6	216			Pr (5)			5
Juristisches WPM Wirtschaftskriminalität oder IT-Strafverfolgung	6	217			Ha + R (5)			5
Digitale Ermittlungen	6	218			Pr (4), R (1)	Ha (0) 60330		5
Masterthesis	7	219			Ma (25)			25
Verteidigung	7				M40 (5)			5
Σ								120

Inkrafttreten

Dieser spezielle Teil der Studien- und Prüfungsordnung für den berufsbegleitenden Masterstudiengang Digitale Forensik der Hochschule Albstadt-Sigmaringen tritt am Tag nach seiner Bekanntmachung in Kraft und gilt für Studienanfänger ab dem 15.06.2023.

Sigmaringen, 29.06.2023

gez. Dr. Ingeborg Mühldorfer
Rektorin der Hochschule