

## Modul

### ITF - IT-Forensik

Master Medientechnologie 2020

---

Version: undefined | Letzte Änderung: - | Entwurf: undefined | Status: undefined | Verantwortlich: SGL\_MaTIN

#### ^ Allgemeine Informationen

<b>Anerkannte Lehrveranstaltungen</b>	<a href="#">ITF_Bornemann</a>
<b>Dauer</b>	1 Semester
<b>ECTS</b>	5
<b>Zeugnistext (de)</b>	IT-Forensik
<b>Zeugnistext (en)</b>	IT Forensics
<b>Unterrichtssprache</b>	deutsch
<b>abschließende Modulprüfung</b>	Ja

#### Modulprüfung

<b>Benotet</b>	Ja
<b>Frequenz</b>	Einmal im Jahr

#### Prüfungskonzept

Benotet werden die schriftliche Projektdokumentation und die Leistung in einem abschließenden mündlichen Fachgespräch.

#### ^ Allgemeine Informationen

# Inhaltliche Voraussetzungen

keine

## Kompetenzen

Kompetenz	Ausprägung
Medientechnische Systeme und Prozesse analysieren	diese Kompetenz wird vermittelt
Medientechnische Systeme und Prozesse prüfen	diese Kompetenz wird vermittelt
Erkennen und Verstehen technischer Zusammenhänge	diese Kompetenz wird vermittelt
Eigene wissenschaftliche und technische Ergebnisse zielgruppenorientiert präsentieren	diese Kompetenz wird vermittelt
Sich selbst organisieren	diese Kompetenz wird vermittelt

## ^ Vorlesung / Übungen

### Exemplarische inhaltliche Operationalisierung

Vorlesung und Übung zu folgenden Themen:

- Einführung und Übersicht: Cyber Security und digitale Forensik
- Cyber-Attacks: Schwachstellen, Bedrohungen und Risiken
- Gefahren bei mobilen Systemen, Home-Office, WLAN's
- Werkzeuge für präventiven Cyberschutz
- Grundlagen und Arbeitsweisen der IT-Forensik
- Forensische Dokumentationserstellung
- Gängige Werkzeuge für forensische Untersuchungen
- Digitale Beweise erkennen u. sichern
- Open-Source-Forensik
- Dateisystem-Forensik
- Forensische Analyse mobiler Systeme
- Schwachstellen, Bedrohungen, Angriffe auf Netzwerkstrukturen
- KALI Linux – Operating System für Vulnerability und Pentesting

### Separate Prüfung

keine

## Exemplarische inhaltliche Operationalisierung

Bearbeitung fallbezogener Aufgaben und Vorfälle eigenständig oder in Arbeitsgruppen zur Sicherstellung, Analyse und Dokumentation digitaler Beweise. Ausgehend von der vorhandenen forensischen Hard- und Softwareausstattung können Fälle aus folgenden Bereichen behandelt werden:

- a) stationäre Systeme (Arbeitsplatz-PCs, Server, industrielle Steuerungssysteme)
- b) Netzwerkangriffe
- c) Internet und Clouds
- d) Mobile Systeme jeglicher Art.

## Separate Prüfung

<b>Benotet</b>	Nein
<b>Frequenz</b>	Einmal im Jahr
<b>Voraussetzung für Teilnahme an Modulprüfung</b>	Ja

## Prüfungskonzept

Abgabe schriftlicher Projektdokumentation