IT Forensik
FH Aachen

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Herzlich
Willkommen!

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-Forensik
an der FH Aachen

Prof. Dr. Marko Schuba, Dipl.-Ing. Hans Höfken
Lehrgebiet Datennetze

IT Forensik
FH Aachen

FH Aachen

FH Aachen

über 10.000 Studierende
ca. 220 Professoren
ca. 250 Lehrbeauftragte
ca. 450 Assistenten und Mitarbeiter
39 Bachelor–, 17 Master-Studiengänge

Standorte Aachen und Jülich

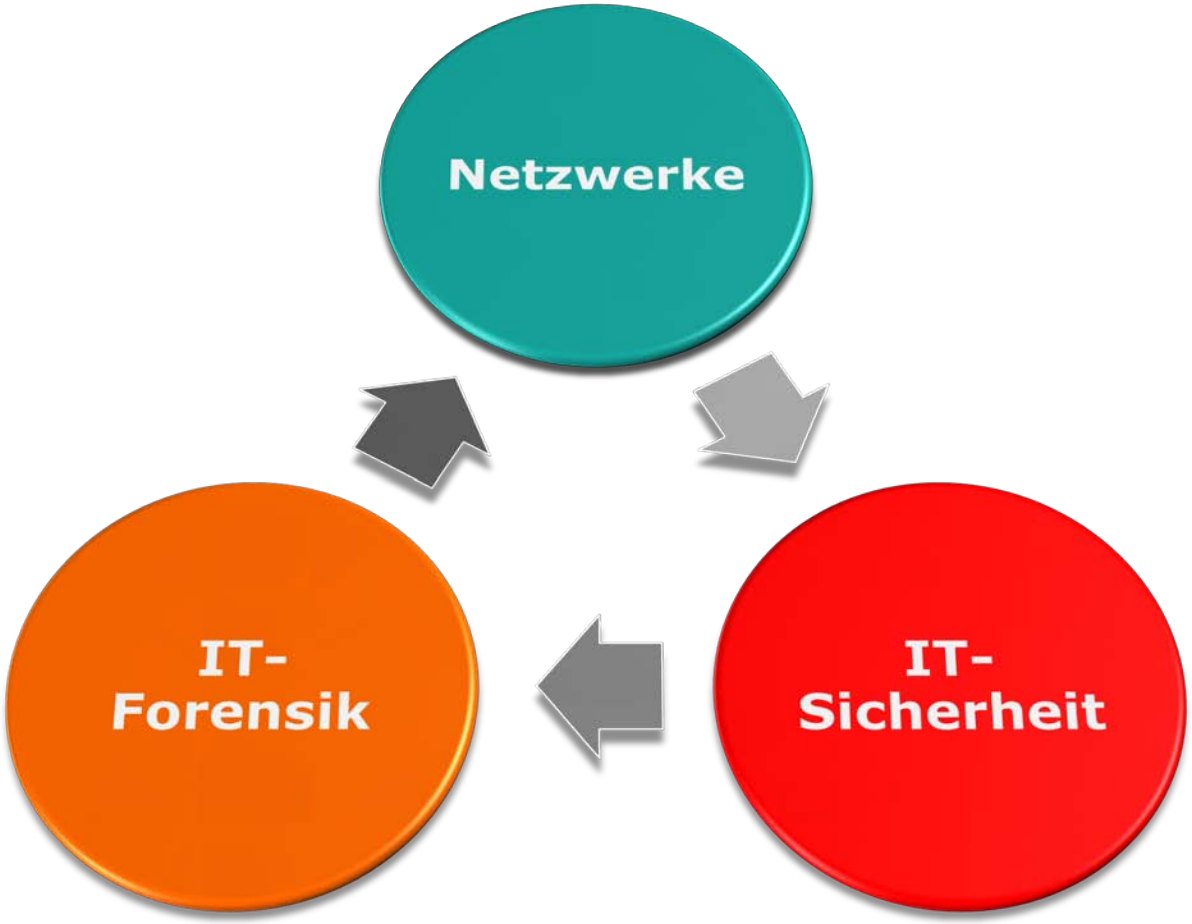
FB Elektrotechnik und Informationstechnik

über 1000 Studierende
28 Professoren und ca. 15 Lehrbeauftragte
ca. 50 Assistenten und Mitarbeiter
7 Bachelor–, 5 Master-Studiengänge

Wirtschaftswoche FH Ranking 2012:
E-Technik: Platz 1
Informatik: Platz 4 (2011: 7)

1	2	3	4	5
Architektur	Bauingenieur-wesen	Chemie und Bio-technologie	Gestaltung	Elektrotechnik und Informations-technik
6	7	8	9	10
Luft- und Raumfahrttechnik	Wirtschafts-wissenschaften	Maschinenbau und Mechatronik	Medizintechnik und Technomathematik	Energietechnik

Lehrgebiet Datennetze



IT-Forensik an der FH - Rückblick

- 2009
  - Auf Initiative von Hans Höfken entsteht IT-Forensik-Arbeitsgruppe

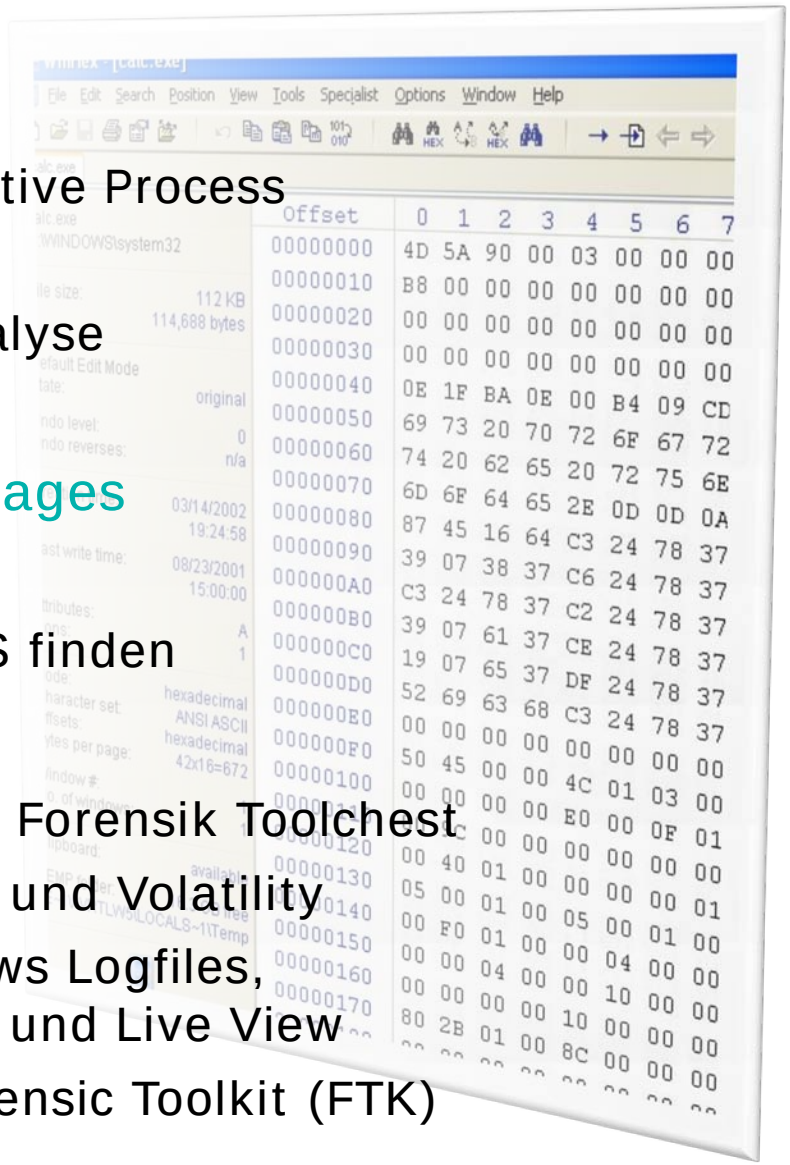
- 2010
  - Berufung Marko Schuba (Lehrgebiet Datennetze)
  - 1. Vorlesung „IT-Forensik“ als Wahlpflichtfach März 2010
- 2011
  - zusätzlich Angebot für Studenten: Zertifizierungskurse
    - CHFI (Computer Hacking Forensik Expert)
    - CEH (Certified Ethical Hacker)
  - 1. IT-Forensik Workshop (50 Teilnehmer)
- 2012
  - Vorlesung im dritten Jahr, Workshop im zweiten…
  - WLAN-Hacking Bootcamp

Interesse an IT-Forensik groß

- Beliebtes Fach der Studenten
  - > 30 Teilnehmer an Vorlesung
  - 15 Studierende im CHFI-Kurs
- Besonders beliebt: Gastvorträge
  - Polizei, BSI, Firmen, Anwälte, Sachverständige… vielen Dank!!!
- Abschlussarbeiten im Bereich IT-Forensik
  - 2011
    - 9 abgeschlossene Arbeiten
  - 2012
    - 2 abgeschlossene Arbeiten
    - 6 laufende Arbeiten
    - 8 weitere Kandidaten

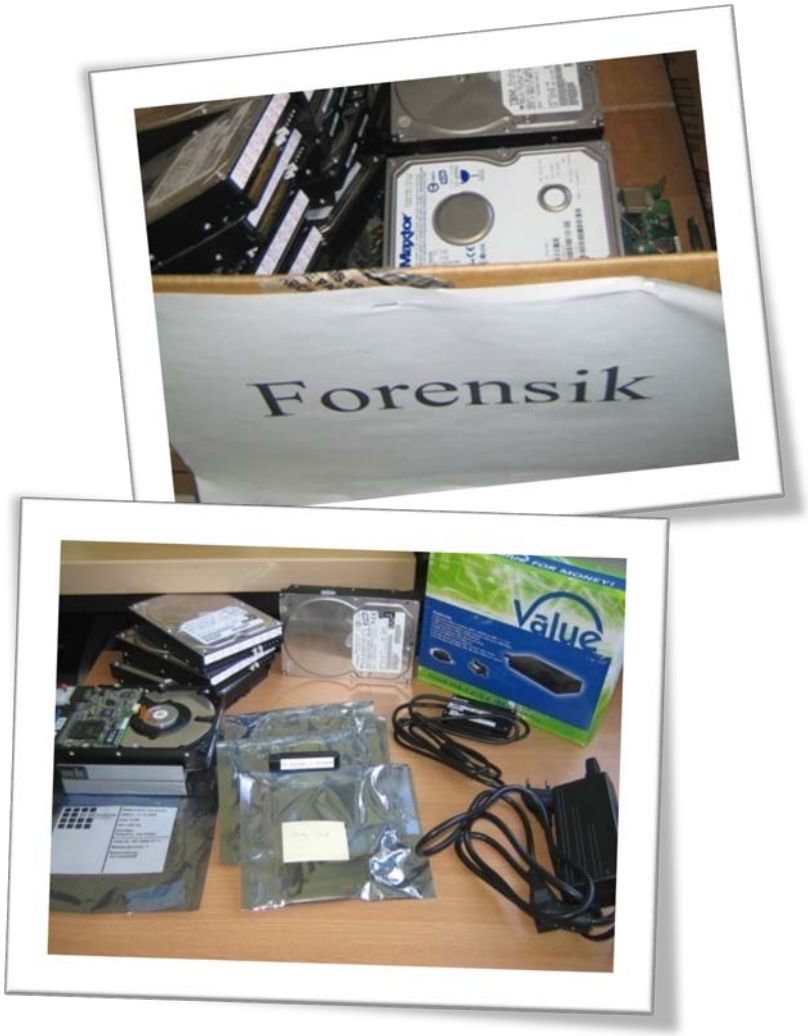
Was lernen die Studenten?

- Theoretischer Hintergrund
  - Incident Response und Investigative Process
  - Live Response
  - Festplatten- und Dateisystemanalyse
  - Mobile Forensik
- Übungen z.B. mit Festplattenimages
  - Partitionstabellen analysieren
  - gelöschte Daten in FAT und NTFS finden
- Praktikumsversuche
  - Live Response mit dem Windows Forensik Toolchest
  - Analyse von RAM Images mit dd und Volatility
  - Post Mortem Analyse von Windows Logfiles, Registry und ADS mit RegRipper und Live View
  - Datenträgeranalyse mit dem Forensic Toolkit (FTK)



„Echter Fall“ parallel zur Vorlesung

- Kriminelle Handlungen in Firma
- 4 Festplatten und 4 USB-Sticks werden beschlagnahmt und landen in der FH-Asservatenkammer
- Studenten ermitteln in Teams
  - erhalten Beweismittel aus Asservatenkammer
  - duplizieren Original-Beweismittel
  - analysieren die Images und ermitteln so Straftaten
  - dokumentieren den Fall vollständig (Chain of Custody, Abschlussbericht)



2. IT-Forensik Workshop

Programm

IT Forensik
FH Aachen

Workshop-Programm

12:30 – 12:45	**Begrüßung**, Prof. Dr. Marko Schuba, FH Aachen
12:45 – 13:30	**Trends in der Forensik von Mobiltelefonen**, Peter Warnke, Cellebrite
13:30 – 13:55	**Analyse der Kommunikation von Android-Apps**, Michael Stahl & Andreas Galauner, FH Aachen
13:55 – 14:15	**Analyse von App-Daten auf Android-Smartphones**, Jens Weidhase, Uni Bochum
14:15 – 14:45	Kaffeepause
14:45 – 15:10	**Forensische Untersuchung von Social Media Apps**, Carsten Crampen, FH Aachen
15:10 – 15:35	**Image Generator für Mobiltelefone,** Benedikt Bauer, FH Aachen
15:35 – 16:00	**Forensik in der Cloud**, Tobias Esser, FH Aachen
16:00 – 16:45	**Mac OS X - Forensik**, Alexander Geschonneck, KPMG
16:45 – 17:10	Kaffeepause
17:10 – 18:00	Kurzvorträge zu neuen Projekten an der FH Aachen
	GUI für Volatility, Steffen Logen, FH Aachen
	Netzwerk Forensik, Jens Berger, FH Aachen
	Korrelationstool für forensische Reports, Martin Pfeiffer, FH Aachen
	Windows 8 Forensik , Alpaslan Aktas, FH Aachen
ab 18:00 Uhr	Ausklang mit kalten Getränken und Zeit für weitere Diskussionen