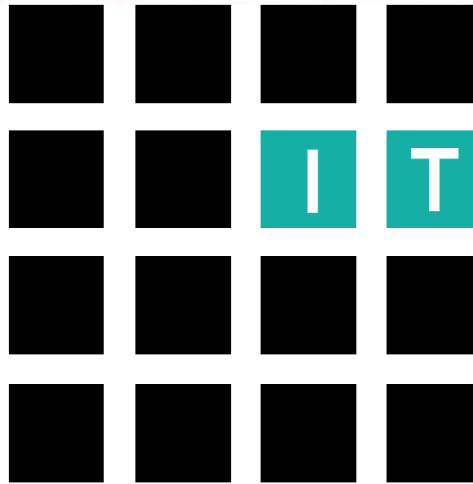


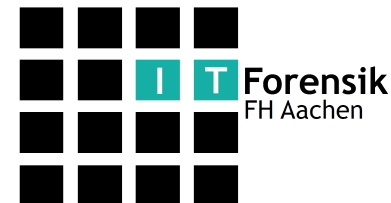
Herzlich
Willkommen

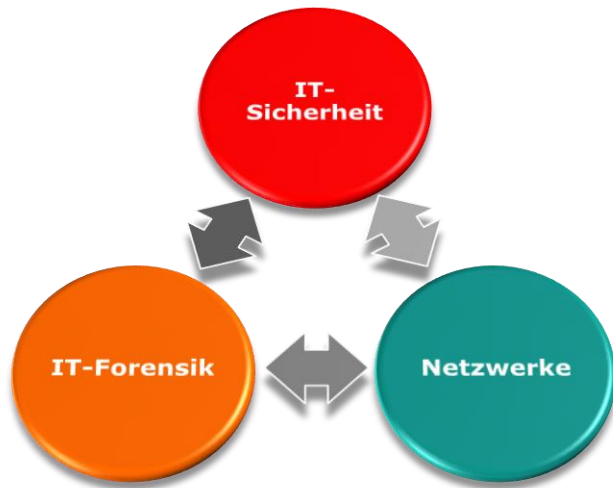


4. IT-Forensik Workshop

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

Lehrgebiet Datennetze,
IT-Sicherheit und IT-Forensik





- Heute der Fokus auf **IT-Forensik**
 - Andere Bereiche deshalb weniger interessant?
 - Mitnichten

- **IT-Sicherheit** fordert Forensiker
 - Anstieg Cyberkriminalität
 - Verschlüsselung
- **Vernetzung** ebenso
 - Fördert Cyberkriminalität
 - Neue vernetzte Geräte
- Was bedeutet das für **IT-Forensik**?
 - Spannende Aufgaben
 - ... und viel Arbeit

Zusammenhang IoT und IT-Forensik?

▪ Zunehmende Digitalisierung und Vernetzung

Neuartige Angriffe auf neue Geräte

- Neue Formen von Schadcode
- Alles eine Frage des Geschäftsmodells

Neue, relevante Beweismittel

- Vielzahl von Geräten speichern (personenbezogene) Daten
- Immer schwieriger, keine Spuren zu hinterlassen

- ### ▪ Wir stellen heute 2 Beispiele für diesen Trend vor
- Vernetzte Automobile bzw. Industrieanlagen
 - Fokus heute: IT-Sicherheit; längerfristig auch: IT-Forensik

Bsp.: IT-Forensik Industrieanlagen (ICS, SCADA)

- Was muss beispielsweise beachtet werden?

Hohe Verfügbarkeit

- Geräte können nicht abgeschaltet werden
- Das gesamte System ist zeitkritisch

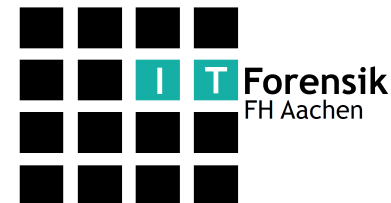
Neue Gerätetypen,
Software, Protokolle

- Klassische Forensik-Tools funktionieren nicht mehr



- Neuentwicklungen / Forschung notwendig

4. IT-Forensik Workshop Programm



- 12:30 – 12:40 **Begrüßung**, Prof. Dr. Marko Schuba, FH Aachen
- 12:40 – 13:20 **Möglichkeiten der Fortbildung auf dem Gebiet der Digitalen Forensik**, Victor Völzow, Polizeiakademie Hessen
- 13:20 – 13:40 **Android-App für First Responder nach ISO/IEC 27037**, P. Heischkamp, FH Aachen
- 13:25 – 14:15 **Dynamische Korrelation von Daten forensischer Berichte**, C. Beckmeyer, FH Aachen
- 14:20 – 14:50 Kaffeepause
- 14:50 – 15:30 **IT-Forensik im Unternehmen - Herausforderungen durch Big Data und Beispiele aus der Beratungspraxis**, Helmut Brechtken, it.sec GmbH & Co. KG
- 15:30 – 15:50 **Angriffe auf SCADA/ICS**, Benedikt Paffen u. Gregor Bonney, FH Aachen
- 15:50 – 16:10 **IT-Sicherheit im Automobil**, Fabian Adolphs, FH Aachen
- 16:10 – 16:30 **Herausford. der Android NAND-Image Analyse**, Michel Erbach, FH Aachen/LKA NRW
- 16:30 – 17:00 Kaffeepause
- 17:00 – 17:1 **Vergleich von XRY, UFED und anderen Analysetools**, Adam Pospiech, FH Aachen
- 17:10 – 17:20 **Sicheres Löschen von Mobiltelefonen**, Eugen Müller, FH Aachen
- 17:20 – 17:30 **Cold Boot Attacks auf RAM Bausteine**, Simon Lindenlauf, FH Aachen
- 17:30 – 17:40 **IT-Forensik virtueller Maschinen**, Remigius Kaminski, FH Aachen
- 17:40 – 17:50 **Forensische Untersuchung von DSL-Routern**, Konrad Albrecht, FH Aachen/LKA NRW
- 17:50 – 18:00 **Analyse von Triplog-Dateien bei TomTom Navis** – S. Braun, FH Aachen/LKA NRW
- ab 18:00 Uhr **Ausklang mit kalten Getränken und Zeit für weitere Diskussionen**
- ab 20:00 Uhr **gemütliches Zusammensein in der Pontstraße (Details siehe Rückseite Programm)**