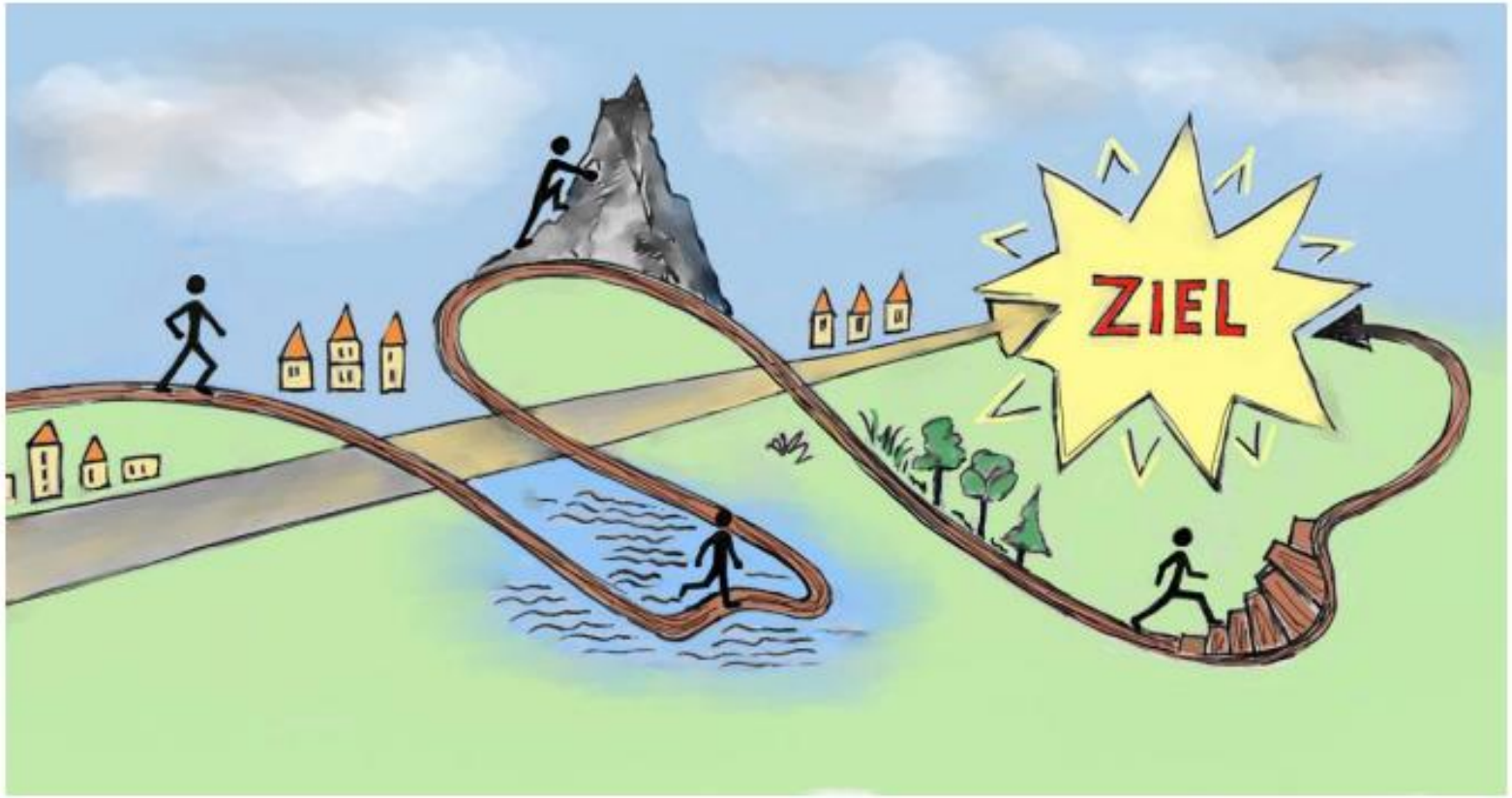
HOCHSCHULE MITTWEIDA
University of Applied Sciences

Grundlagen Digitale Forensik

Einführung

Prof. Dr. Dirk Labudde

Bundeskriminalamt



Ihr Studium in Bildern

Organisatorisches

Fakultät Angewandte Computer- und Biowissenschaften / Sachbearbeiter:in Digitale Forensik

Digitale Forensik Grundlagen SoSe23

Kurs | Einstellungen | Teilnehmer/innen | Bewertungen | Berichte | Mehr

Allgemeines

Alles einklappen

Name	Digitale Forensik Grundlagen
Nummer	0004
Credits	5
Zeiten	Lehrveranstaltungen 35 SWS
Prüfungsvorl.	keine
Prüfung	90 Min schriftlich
Gewichtung	1/8

DATEI
Themenschwerpunkte

FORUM
Ankündigungen

Behandelt werden die Grundzüge und Grundbegriffe der Informationsverarbeitung sowie deren Potenziale. Dabei steht zunächst die Vermittlung eines fundierten Fachwissens bezüglich der Komponenten und Teilsysteme integrierter Anwendungssysteme im Vordergrund (Analysekompetenz; Konzeptionskompetenz). Darauf aufbauend soll der Studierende in die Lage versetzt werden, Zusammenhänge der Gestaltung von Informationssystemen zu erkennen und anwendungsorientiert reflektieren zu können (Verstehen und Anwenden, Reflektieren). Hierzu sollen grundlegende Methodenkompetenzen in der Analyse und Beschreibung von Informationssystemen herausgebildet werden.

Dozenten

- Prof. Dr. rer. nat. Labudde, Dirk
- B. Sc. Laura Pistorius

Organisatorisches

Vorlesung: Moodle (alternativ bei Ausfällen: Zoom)

Unterlagen: Moodle

Informationen: E-Mail, Stundenplan, Moodle

labudde@hs-mittweida.de

pistori1@hs-mittweida.de

friedewa@hs-mittweida.de

Nur wer analoge und digitale Spuren als Einheit begreift und zu deuten versteht, hat heute eine Chance, Verbrechen aufzuklären.

- Dirk Labudde

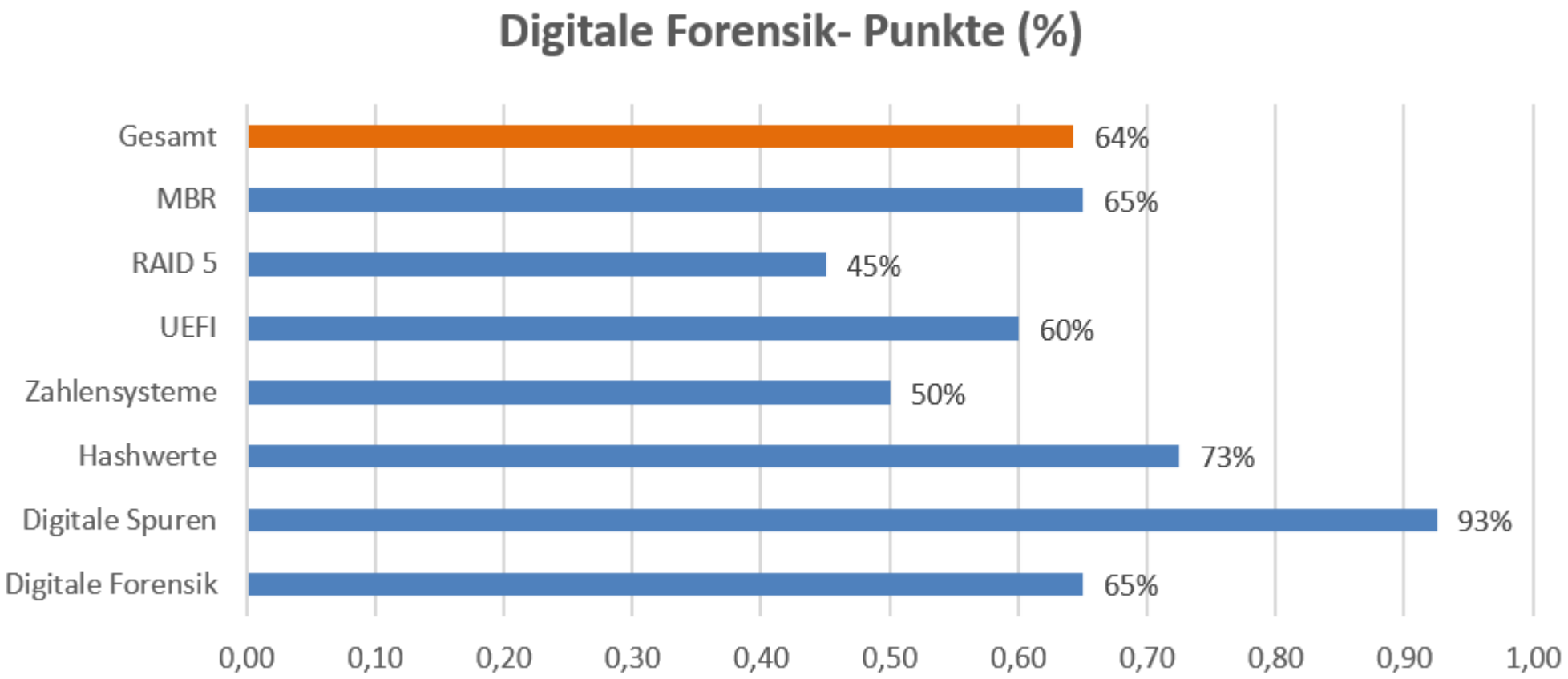
Ablaufplan

Uhrzeit	14.03.	15.03.	21.03.	22.03.	28.03.		04.04.	05.04.	11.04.
08:00 – 09:30 2 SWS	Einführung in das Studium	GDF V4_Zahlensysteme	GDF Praktikum Linux	GDF V5_Computersysteme_und_Datenträgertechnik	GDF V6_Betriebssyteme_2	Karfreitag Vorlesungsfrei	GDF V8_Erster_Angriff_1	GDF V9_dmzAkptCmAAmtCvoADmznipzmv	GDF V11_Zusammenfassug
09:45 – 11:15 2 SWS	GDF V1_Einführung	GDF V7_Einführung_Linux	GDF Praktikum Linux	GDF V6_Betriebssyteme_1			GDF V8_Erster_Angriff_2	GDF V10_Werkzeuge_1	
11:30 – 13:00 2 SWS	GDF V2_Forensische_Prinzipien		GDF Praktikum Bash					V10_Werkzeuge_2	
14:00 – 15:30 2 SWS	GDF V3_Modell_Prozess_Methode		GDF Praktikum Bash						

Prüfungskonsultation: 18.04.2023, 14 Uhr

Modulprüfung: 19.04.2023, 8.00 - 9.30 Uhr

Ergebnisse Vorkurs



Beispiele Aus der Praxis


SIM-Swapping Wie Hacker nur mit der Handynummer Konten plündern

SIM-Swapping:

SIM-Swapping, auch SIM-Karten-Swap, ist ein Betrugsmasche, bei der sich ein Hacker die *Mobiltelefonnummer* eines Benutzers erschleicht, um sich – unter Umständen nur kurzfristig – der OnlineIdentität des angegriffenen Opfers bemächtigen und als die Zielperson ausgeben zu können **(Identitätsdiebstahl)**.

Bereits 2013, 2014 und 2015 erbeuteten Betrüger auf diese Weise meist fünfstellige Euro-Beträge, der Gesamtschaden belief sich auf über eine Million Euro. Mobilfunkanbieter verstärkten darauf ihre Sicherheitsmaßnahmen, insbesondere bei der Freischaltung von Ersatz-SIM-Karten in den MobilfunkShops über die Hotline.

Beispiele Aus der Praxis

Computerbetrug im Onlinebanking durch Phishing und Änderung der Rufnummer für das mTAN-Verfahren

Modus operandi

Ausspähen der Zugangsdaten zum Konto

• Phishing-Mail oder Schadprogramme

Änderung der Rufnummer für das mTAN-Verfahren

• Durch Brief, Fax oder Anruf (Social Engineering)

Änderungen im Konto

• Auffüllen des Onlinekontos von Unterkonten, Erhöhung des Limits

Reale und Digitale Methoden

In Auswertung der nunmehr bekannten Buchungsvorgänge konnten 4 Geldwäschekonten bei der Fidor Bank AG ermittelt werden.

Konto	DE73 7002 2200 0073 5196 91	DE67 7002 2200 0074 6753 60	DE35 7002 2200 0073 8169 04	DE14 7002 2200 0071 9214 17	gesamt
Kontoinhaber	xxxx, Steffen geb. 03.05.1989	xxxx, Andreas geb. 30-01.1951	xxxx, Martin geb. 30.01.1961	xxxx, Helmut geb. 23.09.1938	
Umsätze	115.704,69 €	268.561,33 €	135.013,12 €	52.064,50 €	**571.343,64 €**

Beispiele Aus der Praxis

Kommerzielles SMS-Gateway

- www.sms77.io
- täterseitig 84 Rufnummern für ca. 14 T BTC angemietet

Beispiele Aus der Praxis

Verfügbar bei Ali Express

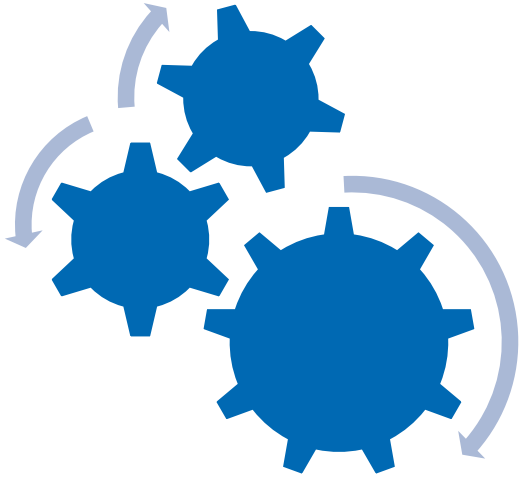
Beispiele Aus der Praxis

Was wollte ich Ihnen sagen?

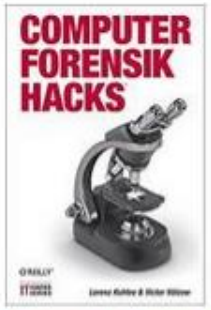
Trennung von Spuren Hinweisen?

Trennung von analogen und digitalen Techniken?

Allumfassend denken und ermitteln!



Literatur



Computer-Forensik Hacks
Lorenz Kuhlee
19
Taschenbuch
EUR 34,90 prime

Computer-Forensik (iX Edition): Computerstraftaten...
› Alexander Geschonneck
1
Taschenbuch
EUR 42,90 prime

Forensische Informatik
Andreas Dewald
Taschenbuch
EUR 39,00 prime

Hacking & Security: Das umfassende Handbuch
› Michael Kofler
13
Gebundene Ausgabe
EUR 49,90 prime

Computer-Forensik: Computerstraftaten erkennen, ermitteln,...
› Alexander Geschonneck
18
Broschiert
EUR 42,90

Viele Links im Netz!


KRISE DER WISSENSCHAFT
Wahrheitssuche zwischen Skepsis und Vertrauen


7 GRÜNDE, WARUM FORENSIK KEINE WISSENSCHAFT IST


7. STARKE BEEINFLUSSBARKEIT
Ein spezieller Punkt bei der subjektiven Arbeit ist die Beeinflussbarkeit der Forensiker. Ein Beispiel: Forscher der University of Southampton legten fünf Experten zwei Fingerabdrücke vor. Die Abdrücke stammten von derselben Person und waren von den befragten Forensikern bereits vor Gericht als identisch klassifiziert worden. Doch den Experten wurde gesagt, dass einer der Abdrücke von Brandon Mayfield sei. Den Forensikern war bekannt, dass dieser fälschlicherweise für die Anschläge in Madrid verhaftet worden war. Das Ergebnis des Tests: Drei der Experten erklärten, dass die Abdrücke nicht übereinstimmten, einer enthielt sich, und der fünfte erkannte als Einziger, dass sie identisch waren. Übersetzt heißt das: 80 Prozent dieser Forensiker ließen sich von ihrem Vorwissen und den zusätzlichen Informationen beeinflussen.


1. ZU VIEL MATERIAL
Allein in Großbritannien und den USA, den Staaten mit den größten forensischen Sammlungen, umfassen die Datenbanken derzeit DNA von mehr als elf Millionen Menschen. 1998 waren es in den USA gerade mal 250 000 Proben. Damals waren große Übereinstimmungen selten und galten damit als sichere Indizien in Kriminalfällen. Bei der aktuellen Menge an genetischem Material kommt es dagegen immer mehr auf kleinste Abweichungen an – doch die Auswertung ist dafür nicht präzise genug.
2. ZU VIEL SPIELRAUM
Zwölf oder mehr identische Merkmale eines Fingerabdrucks bedeuten in der Kriminalistik eine Übereinstimmung. Im Mayfield-Fall gab es 15 passende Merkmale – und dennoch war der Verdächtigte nicht der Täter. Ouhnane, der wahre Terrorist, wies 21 Übereinstimmungen mit den Fingerabdrücken auf. Das zeigt vor allem: Die Parameter der Forensik sind extrem vage und funktionieren nach dem Prinzip der Wahrscheinlichkeit. Und genau dieses Prinzip schließt Fehler automatisch mit ein.
3. KAUM KONTROLLE
Viele Kritiker bemängeln außerdem, dass die forensischen Labore und die Arbeit der Ermittler keiner echten Kontrolle unterliegen. Besonders in den USA sind diese flexibel und unabhängig. So können Unternehmen private Labore eröffnen und der Kriminalpolizei ihre Dienste anbieten. Da es kaum festgelegte Normen gibt, können die Methoden oft frei gewählt werden. Ein Beispiel: Es gibt fünf verschiedene Methoden der DNA-Analyse, die bei der Personenidentifizierung genutzt werden.
4. FEHLERHAFTE TECHNIK
Der Mayfield-Fall zeigt auch, dass den Forensikern technische Grenzen gesetzt sind: Die sichergestellten Fingerabdrücke befanden sich auf einer Plastiktüte. Plastik ist ein sehr glattes Material und schlecht als Träger für forensische Informationen geeignet. Um überhaupt den Fingerabdruck zu erhalten, mussten die Ermittler die Tüte mit Cyanoacrylat bedampfen. Das konserviert die Spuren, indem es Schweiß und Talg mit einer klebrigen Schicht überdeckt. Allerdings kann die Chemikalie auch Linien verändern oder Details des einzigartigen Musters verdecken.
5. VIEL ERFAHRUNG, WENIGE STUDIEN
Grundsätzlich beruhen fast alle forensischen Methoden hauptsächlich auf Erfahrung (Trial and Error) und nicht auf jahrelangen wissenschaftlichen Studien. Das bedeutet vor allem, dass die Kriminologie nicht nach festgelegten wissenschaftlichen Standards arbeitet, sondern wie bereits erwähnt mit der Wahrscheinlichkeit. So können Techniken zum Einsatz und werden Schlüsse gezogen, die in 100 vorhergehenden Fällen zum Erfolg geführt haben. Im 101. Fall können sie dennoch versagen.
6. SUBJEKTIVE ANALYSE
Die vagen Methoden bieten aber auch viel Platz für menschliche Irrtümer. Wann erachtet ein Kriminologe ein Indiz als unumstößlichen Beweis? Wie viel Zeit nimmt sich der Gerichtsmediziner für eine Obduktion? Wie sauber arbeitet das Laborpersonal? Wie interpretiert ein forensischer Archäologe eine Knochenverletzung? Die Antworten sind von Fall zu Fall sehr unterschiedlich und zeigen, wie subjektiv die Ermittlungen sind.

Richterin

WIE VIELE ÜBEREINSTIMMUNGEN SIND NOTWENDIG ...

Jeder Abdruck besteht aus Bogen, Schleifen oder Wirbeln

Übereinstimmungen hängen stark von der Interpretation des Experten ab

Nicht jede Person hat einen Fingerabdruck. Menschen mit der genetischen Störung Albinismus könnten also das perfekte Verbrechen begehen

KANN EIN BEWUSSTLOSER MANN EINEN MORD BEGEHEN?

„Die Fingerabdruck-Analyse ist eine subjektive, ungetestete, nicht nachweisbare Methode der Identifizierung, die vorgibt, unfehlbar zu sein."

Susan M. Souder, Richterin am Baltimore County Circuit

Brandon Mayfield

UNSCHULDIG ANGEKLAGT

?

Daktyloskopie

Ist all das im Cyberraum noch akuter?

Was ist Digitale Forensik?

Definition

Einordnung

Spezialgebiete

Forensik

Forensik ist die Anwendung von Wissenschaft auf das Rechtssystem.

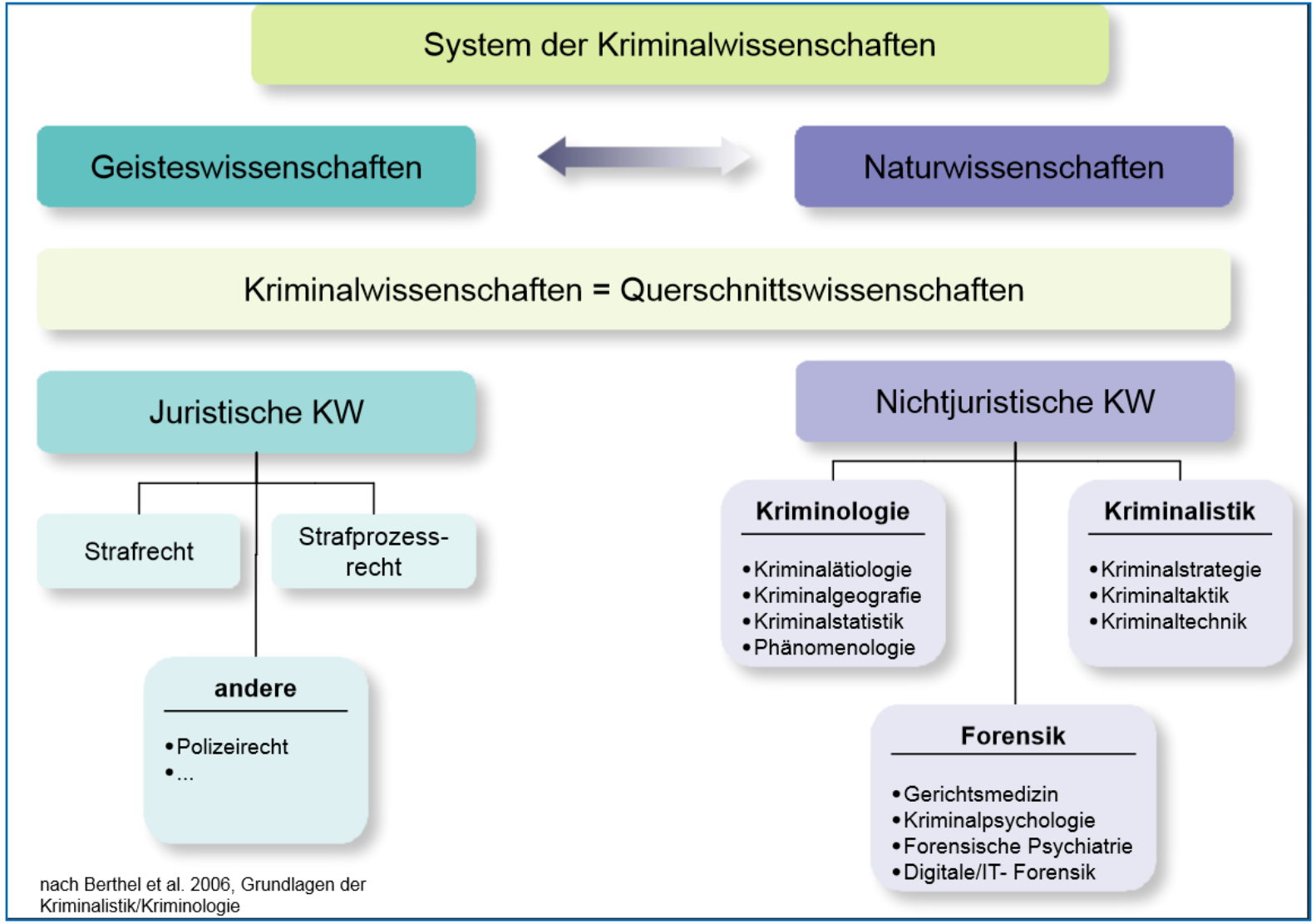
- American Academy of Forensic Sciences, AAFS

Und jetzt digital?

Digitale Forensik

- Digitale Forensik beschäftigt sich mit der **gerichtsfesten Sicherung** und **Verwertung** digitaler Spuren
- Als forensische Wissenschaft muss die digitale Forensik **wissenschaftliche Methoden** anwenden
  - Beweisführung kann dazu führen, dass Menschen ihrer Freiheit beraubt werden
  - Nur eine verlässliche und objektive Methodik wird dieser Verantwortung gerecht
  - Methodik muss immer wieder neu überdacht werden

Informatik als forensische Wissenschaft



Informatik als forensische Wissenschaft

Forensische Informatik: *ist die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems.*[Dewald 2011]
- i.e.S. - Untersuchung technisch unvermeidbarer Beweismittel
- i.w.S. - Untersuchung technisch vermeidbarer Beweismittel

IT-Forensik/Digitale Forensik: ist die streng methodisch vorgenommene Datenanalyse auf Datentragern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems. [BSI 2011]

Post-mortem-Analyse (Offline-Forensik)
- Untersuchung von Datentragerabbildern (so genannten Images)
- Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien

[BSI 2011]

Live-Analyse (Online-Forensik)
- Untersuchung beginnt bereits während der Laufzeit des Vorfalls
- Gewinnung und Untersuchung flüchtiger Daten

[BSI 2011]

Data-Forensik
forensische Datenanalyse - Analyse von (meist großen) Datenbeständen aus Anwendungen und den zugrunde liegenden Datenbanken

Disk-/Computerforensik
Analyse von Computer- oder Mobilgeräten und der darin enthaltenen Daten

Informatik als forensische Wissenschaft

Digitale Forensik

"...ein pragmatisches technisches Sachverständigenwesen...unter dem Oberbegriff 'Computerforensik' oder 'digitale Forensik'...."[Geschonneck:2006; Casey:2004]

"...[es] besteht der wesentliche Unterschied zwischen der klassischen Forensik und der digitalen Forensik in der Natur der Spuren, die in beiden Bereichen untersucht werden."[Dewald:2011]

"Fast alle Prinzipien, die man in der klassischen Forensik für physische Spuren entwickelt hat, lassen sich auch auf digitale Spuren anwenden."[Dewald:2011]

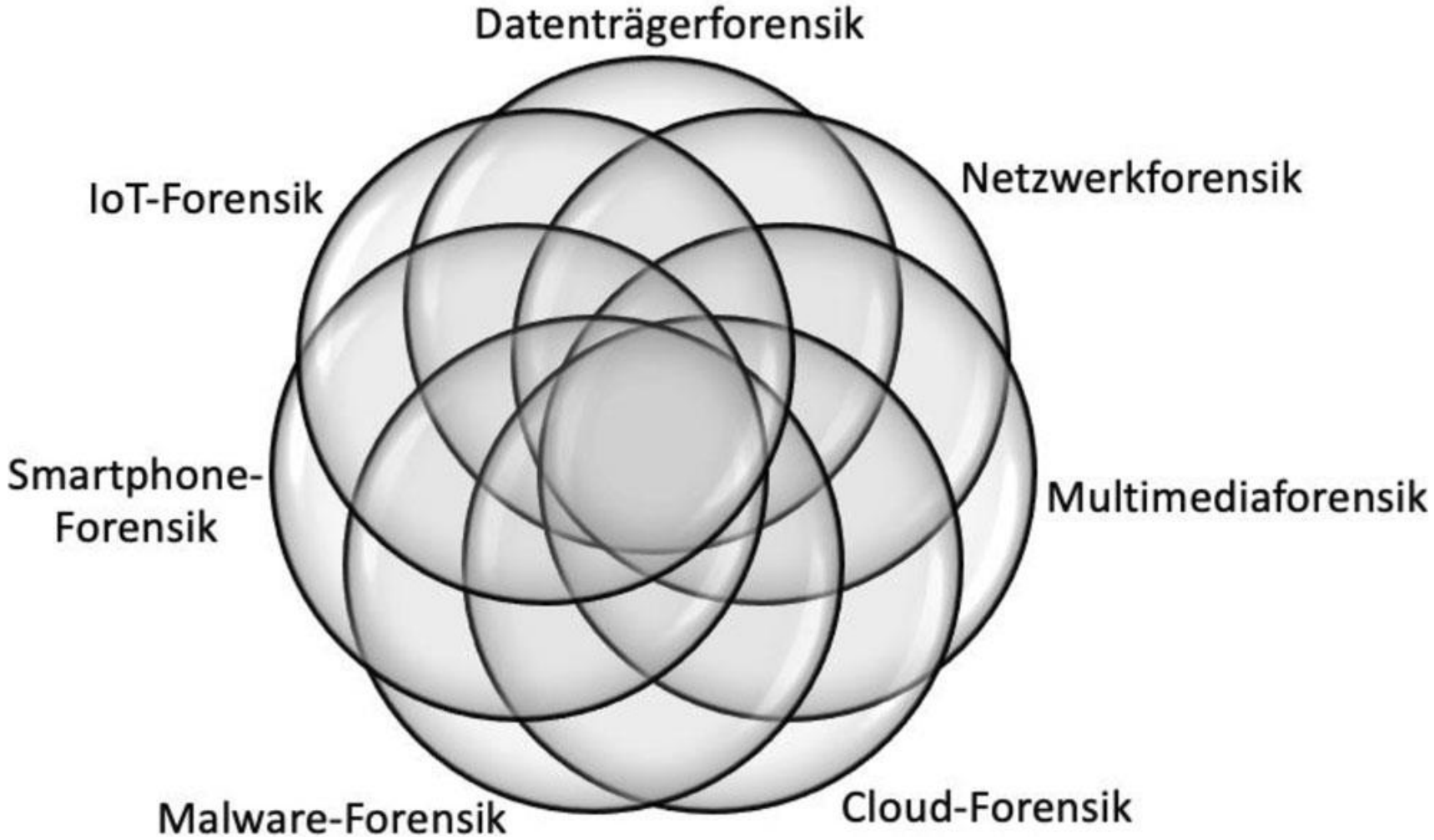
"...die Untersuchung digitaler Spuren [verlangt] manchmal neue Methoden."[Dewald:2011]

Informatik als forensische Wissenschaft

Die Computerforensik (Geschonneck, 2006) umfasst in ihrer aktuellen Form eine Vielzahl unterschiedlicher Aufgaben, wie beispielsweise:

- die möglichst schnelle Bewertung eines Sicherheitsvorfalls anhand erster, durch Techniken der Live-Analyse (Carrier, 2005, S. 13 ff.) erhobener, Daten zur Planung der weiteren Untersuchung des Vorfalls.
- die Anfertigung einer forensischen Kopie physischer Speichermedien unter Einsatz spezieller Hardware und Software.
- die Umgehung von Schutzmechanismen digitaler Systeme, um eine Erhebung von Daten zu ermöglichen.
- die Extraktion kryptographischer Schlüssel aus Hauptspeicherabbildern, zur Erhebung verschlüsselter Daten.
- die Rekonstruktion gelöschter Daten anhand von Dateisystem Metadaten oder durch *Filecarving*.
- die Erstellung von Timelines untersuchter Systeme, also die Erfassung einer zeitlichen Abfolge vergangener Ereignisse auf dem untersuchten System.

Spezialgebiete der Forensik

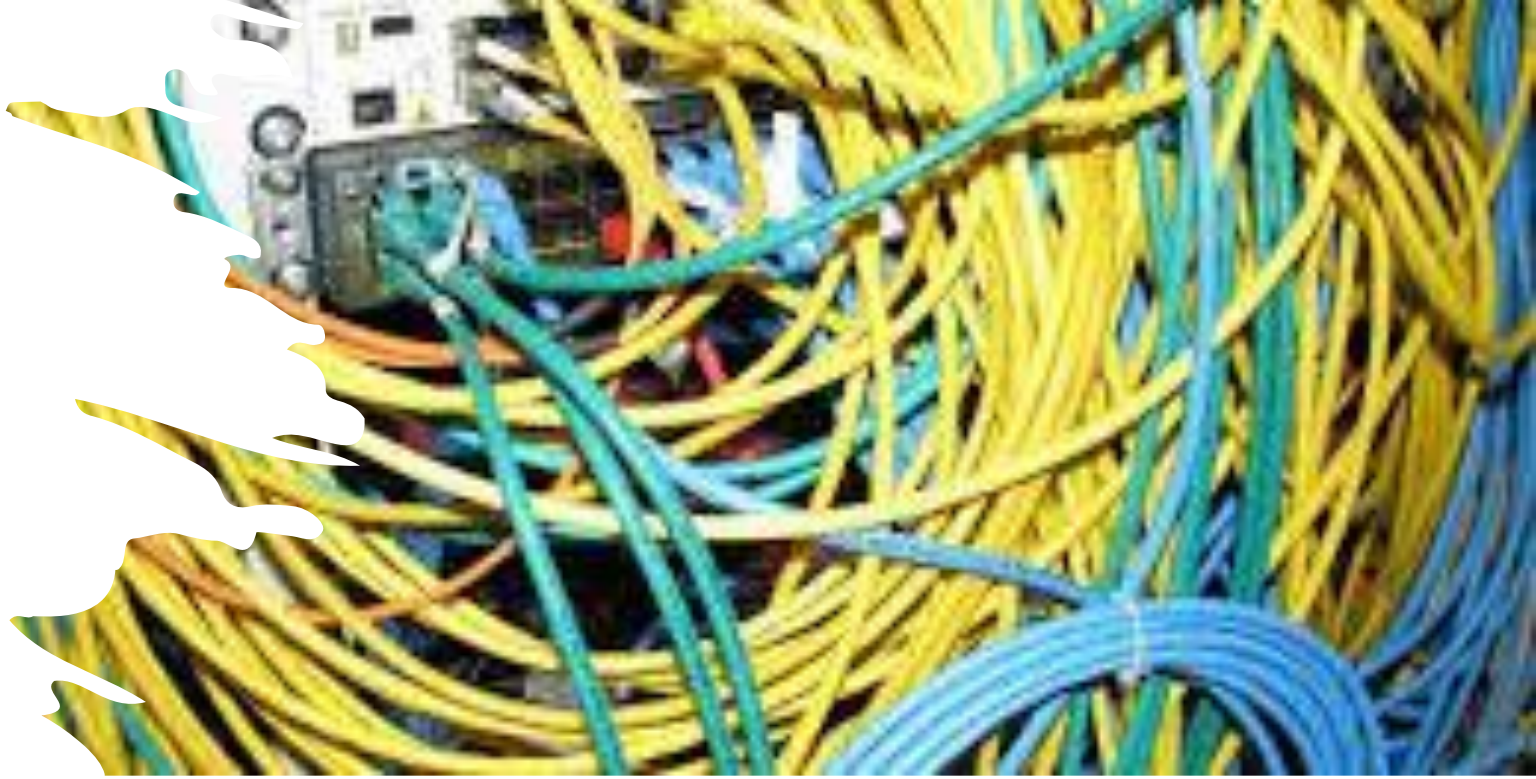


Datenträgerforensik

Alles rund um physische Datenträger, SSD Festplatten, Datenträgerabbilder, Beweissicherung

Netzwerkforensik

- Mitschneiden und analysieren der Netzwerkkommunikation
- Netzwerkmitschnitte von IT-Systemen als Quelle für Informationen



Multimedia-Forensik

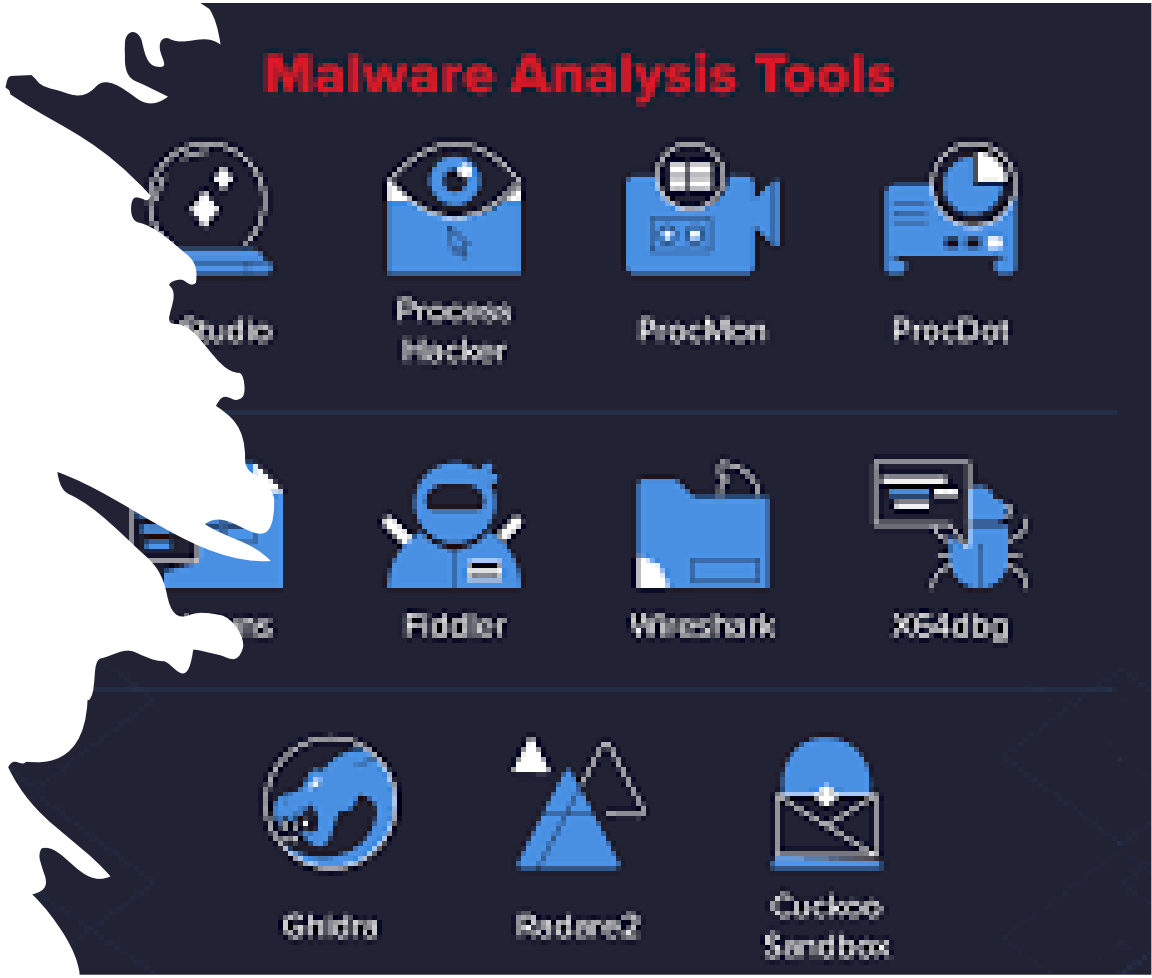
- Bild- und Videoforensik
- Audioanalysen
- Metadatenanalyse

Cloud-Forensik

- Informationen aus Cloud-Speichern
- Auswertung von Spuren aus Cloudumgebungen (Logfiles, Zugriffsdokumentationen, IP-Adressen, ...)

Malware-Forensik

- Analyse von Schadsoftware (Viren, Würmer, Trojaner, Ransomware…)
- Analyse der Software aber auch Einfallstore und Verbreitungswege

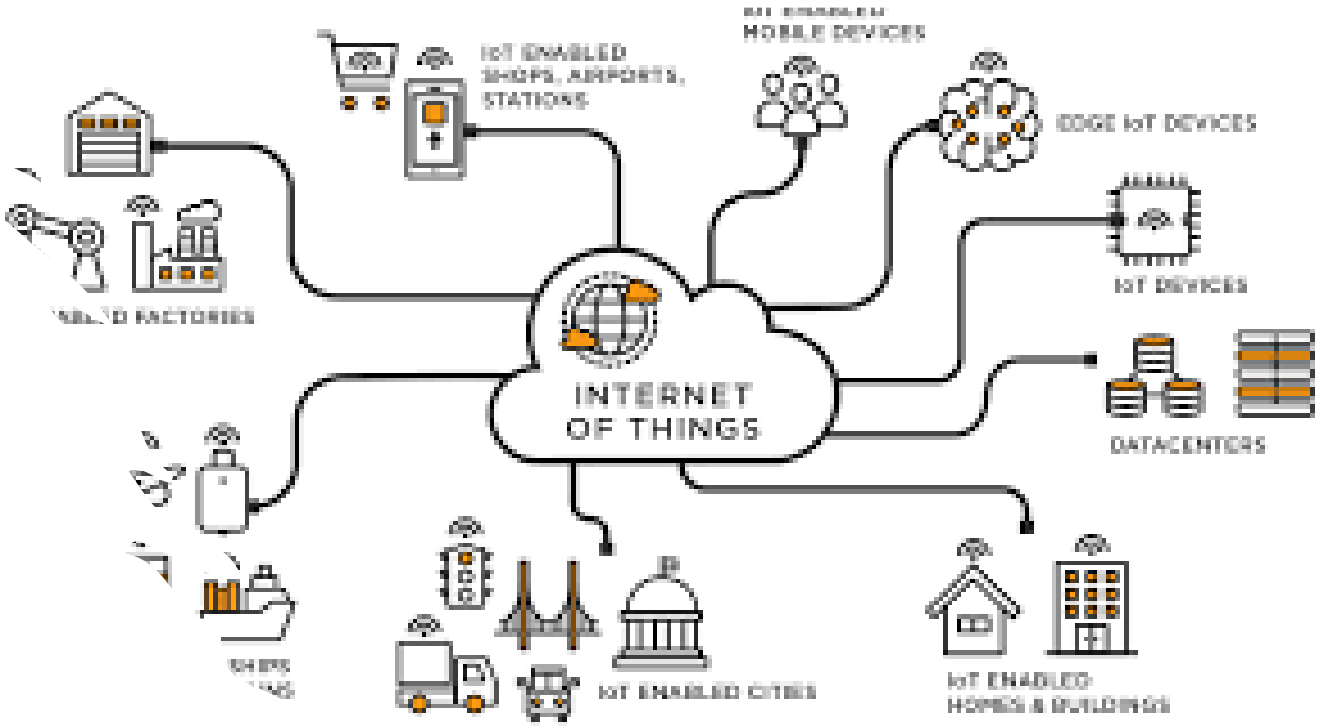


Smartphone-Forensik

- Sicherung, Datenaufbereitung, Entsperrung, Wiederherstellung, Auswertung von Smartphones und entsprechenden Daten

IoT-Forensik

- Analyse von IoT-Geräten, Identifikation von Spurenträgern
- Auswertung der Daten



Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

dirk.labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de