IT-Forensik – Projekt | Organisatorisches

WS 2021/22

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

Wer steht vor Ihnen?

Bastian Grube

- bastian.grube@polizei.niedersachsen.de
- 04131 – 8306 3524
- Diplom Wirtschaftsinformatik
- Polizeidirektion Lüneburg / Zentrale Kriminalinspektion Lüneburg
  - IT-Spezialist Mobilfunkforensik
    - IT-Forensik, Schulungen, Softwareentwicklung
  - Ansprechpartner Informationssicherheit
- Masterstudiengang IT-Sicherheit und IT-Forensik

- 2/2004 - 3/2018
  - Message Mobile GmbH, Lüneburg
    - Softwareentwickler (bis 2011)
    - Ausbilder - Fachinformatiker Systemintegration (ab 2010)
    - Aufbau/Leitung Abteilung Operations

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Wer sind Sie? Was erwarten Sie?

- Bitte stellen Sie sich kurz vor!
  - Wer sind Sie?
  - Haben Sie Vorkenntnisse?
- Warum haben Sie das IT-Forensik Projekt gewählt?
  - Was erhoffen erwarten Sie von diesem Seminar?
- Haben Sie schon spezielle Fragen?

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

Was bekommen Sie?

- Theoretische und praktische Einführung in die IT-Forensik
- Vertiefung Digitale Spuren auf Mobiltelefonen
- Datensicherung
- Datenanalyse / Datenauswertung
  - Freie und kommerzielle Software
- Erstellung eines forensischen Gutachtens
- Ergebnispräsentation

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

Organisatorisches

- Grundsätzlich in Präsenz
  - Fragen zur vorherigen Woche
  - Theorie
  - Praktische Übungen / Demonstrationen

- Mindestens zwei Termine Online in Zoom
  - 26.10.2021
  - 09.11.2021

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

Prüfungsleistung

- Projektarbeit (2-3 Personen pro Gruppe)
  - Erstellung eines fiktiven Tatherganges unter Verwendung zweier gestellter Mobiltelefone
  - Erzeugen der dazugehörigen digitalen Spuren auf den Mobiltelefonen
    - Hinweis: Dokumentieren Sie das Vorgehen bzw. die Aktionen
  - Sicherung beider Mobiltelefone
  - Auswertung der digitalen Spuren mittels gestellter Software
  - Implementierung einer geeigneten Darstellung gleichartiger digitaler Artefakte beider Mobiltelefone
  - Erstellung einer Projektdokumentation
    - Beschreibung der Ausgangslage
    - Formulierung der Fragestellungen an die IT-Forensik
    - Auswertung im Gutachten-Stil

- Prüfungsmodalitäten
  - 30% Ergebnispräsentation der Eigenimplementierung (30min Präsentation + 15min Fachfragen) – 01.02.2021
  - 70% Abgabe Projektdokumentation – 28.02.2021

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

IT-Forensik – Projekt | Einführung

WS 2021/22

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

Forensik

- Wortherkunft: Forensik, von lat. forum (Marktplatz)
  - Marktplatz war Schauplatz der Gerichte
- Wissenschaftliches und technisches Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden (Wikipedia)
- Eine Spur (engl. evidence) ist ein **Indiz** (Hinweis/Zeugnis), das eine Theorie über einen Tathergang **stützen oder widerlegen** kann
- Mit forensisch wird die Eigenschaft von Spuren bezeichnet, als **Beweismittel vor Gericht verwendbar** zu sein
- Forensik (oder forensische Wissenschaft) ist die Anwendung **wissenschaftlicher Methoden** zur Untersuchung und Verfolgung von Straftaten
- „Jeder oder alles am Tatort nimmt etwas mit und lässt etwas zurück!“ (Edmund Locard, 1877 – 1966)

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Forensik

- Forensische …
  - …. Balistik
    - Auswertung von Geschossen, Waffemn, etc.
  - … Serelogie
    - Auswertung von Blut oder anderen Sekreten
  - … Daktyloskopie
    - Auswertung von Fingerabdrücken
  - … Toxikoligie
    - Nachweis von Giften und/oder Drogen
  - … DNA-Analyse
  - …

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG

IT-Forensik

„**IT-Forensik** ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung…“ (BSI)

- Insbesondere im Hinblick auf eventuelle Gerichtsverfahren sind folgende Anforderungen zu erfüllen:
  - Akzeptanz
  - Glaubwürdigkeit
  - Wiederholbarkeit
  - Integrität
  - Ursache und Auswirkungen
  - Dokumentation
  - Authentizität der Daten

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Zentrale Fragestellungen der IT-Forensik

- **Was** ist geschehen?
- **Wo** ist es passiert?
- **Wann** ist es passiert?
- **Wie** ist es passiert?
- **Wer** hat es getan?
- **Was** kann gegen eine Wiederholung getan werden?

Technische Herausforderungen

- Identifikation relevanter Daten, Datenbestände

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Gerichtsfestigkeit

Damit gesammelte Daten vor Gericht verwertbar sind, umfasst der gesamte Forensikprozess hinsichtlich der Beweismittel und Analyseschritte folgende Merkmale:

- Dokumentation
  - Lückenlos
  - Umfassend
  - nachvollziehbar Darstellung für Menschen mit nicht technischem Hintergrund
- Sicherstellung der Datenintegrität
  - 4-Augen-Prinzip
  - Hashwerte
- [Praxisbezug]
  - Objektivität
  - keine Wahrscheinlichkeiten
  - Nur nachweisbare Schlussfolgerungen

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Digitale Spuren

- Digitale Spuren
  - „Digitale Spuren sind alle, die auf Daten basieren, die in Computersystemen gespeichert oder übertragen worden sind.“ (Casey)

- Spurenträger
  - externe Festplatten / Wechseldatenträger
  - Computer
  - NAS, Server, etc.
  - Spielekonsolen (Play Station, X-Box, etc.)
  - Mobiltelefone / Smartphones
  - Navigationsgeräte
  - Smart Devices (IoT)
  - uvm.

ZENTRALE KRIMINALINSPEKTION LÜNEBURG

Digitale Spuren

- … können leicht manipuliert werden
  - absichtlich - durch Straftäter oder auch Ermittler
  - unabsichtlich - durch Ermittler
  - Manipulation hinterlässt keine unmittelbaren sichtbare Zeichen
  - Manipulation kann durch Vergleich mit Originalkopie nachgewiesen werden
- … sind nicht personenbezogen
  - Zuordnung von Handlungen einer Person zu digitalen Spuren nur durch einen starken Authentifizierungsmechanismus möglich
  - eine ausschließliche Beweisführung auf Basis von digitalen Spuren ist nicht durchführbar
  - Man benötigt immer zusätzliche (nicht-digitale) Spuren
- … können exakt dupliziert werden
- … sind schwer zu vernichten

Live- und Post-Mortem-Forensik

- Live-Forensik
  - Forensikprozess beginnt bereits während der Laufzeit des Vorfalls
  - Im Vordergrund steht insbesondere die Sicherung von flüchtiger Inhalten
    - Hauptspeicherinhalt
    - Cacheinhalte
    - Netzwerkverbindungen
    - Laufende Prozesse

- Post-Mortem-Forensik
  - Forensikprozess findet anhand (gerichtsverwertbar) gesicherter Beweismittel und Daten im Nachhinein des Vorfalls statt
  - verwendet hauptsächlich Images (1:1 Abbild des physikalischen Speichers)
  - Flüchtige Daten sind in der Regel bereits verloren

Sicherungsarten

- Physikalisches Abbild
- Logische Sicherung
- Dateisystem
- Backup

Fragen? Fragen!

ZENTRALE
KRIMINALINSPEKTION
LÜNEBURG