Kryminalistyka cyfrowa

Głównym celem zajęć powinno być zapoznanie studenta z metodami pozyskiwania, zabezpieczania i analizy danych cyfrowych.

W tym celu student powinien zostać zaznajomiony z:

- podstawowymi pojęciami związanymi z kryminalistyką cyfrową:
  - dowód cyfrowy,
  - autentyczności i wiarygodności dowodu cyfrowego,
  - biegły sądowy.
- metodami pozyskiwania oraz zabezpieczania danych, aby miały wartość dowodową z
  - różnych nośników danych,
  - z systemów operacyjnych oraz mobilnych systemów operacyjnych,
  - pamięci operacyjnej,
  - chmury.
- metodami analizy danych
  - dostępnych w różnych systemów operacyjnych Linux, macOS, Android i iOS,
  - systemów plików,
  - artefaktów z systemów operacyjnych,
  - artefaktów uzyskanych z przeglądarek, wyszukiwarek, maili, dokumentów,
  - metadanych plików graficznych i multimedialnych,
  - logów i rejestrów systemowych,
  - ruchu sieciowego.
- Raportowaniem wykonanej analizy

Student powinien poznać:

- narzędzia open source jak i komercyjnymi, wspierającymi pracę informatyka śledczego, np. Autopsy, EnCase Forensic, FTK Imager ,
- systemami operacyjnymi wspierającymi pracę informatyka śledczego i posiadającymi już zainstalowane narzędzia śledcze, np. Kali Linux.

Sugerowana literatura:

1. Dr Darren R. Hayes, Informatyka w kryminalistyce. Praktyczny przewodnik, Helion, 2021

2. Cory Altheide, Harlan Carvey, Informatyka śledcza. Przewodnik po narzędziach open source. Helion, 2014

3. Jason T. Luttgens, Matthew Pepe. Incident Response; Computer Forensics, Third Edition. McGraw-Hill Education 2014.

4. Gerard Johansen. Digital Forensics and Incident Response. Packt Publishing 2017.

5. Aleksandra Boniewicz, Analiza śledcza urządzeń mobilnych. Teoria i paktyka. Helion, 2022

6. Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, The Art of Memory Forensics. John Wiley and Sons, 2014