Co-funded by the
Erasmus+ Programme
of the European Union

Syllabus Modułu 5: Podstawy informatyki śledczej (Digital Forensics Fundamentals)

Obciążenie pracą i ECTS

Zajęcia wideo: 8 godzin
Praca samodzielna: 67
godzin ECTS: 3

Efekty uczenia się (wiedza, umiejętności i kompetencje)

Moduł Comprehensive Digital Forensics Fundamentals zapewnia teoretyczne i praktyczne wykorzystanie tej wiedzy w gromadzeniu, analizie i zabezpieczaniu dowodów, co prowadzi do uznania ich za dowody w sądzie. Treści zawarte w programie tego modułu pozwalają na utrwalenie jego celu. Umiejętności, które należy rozwinąć, są następujące

1. Student zna modele cyfrowej analizy kryminalistycznej;

2. Uczeń zna zależności między wskazówkami, dowodami i przestępstwem;

3. Student wykonuje raporty kryminalistyczne;

4. Uczeń w miejscu zdarzenia identyfikuje, gromadzi, pozyskuje i zachowuje wskazówki cyfrowe, stosując różne techniki, chroniąc integralność dowodów;

5. Uczeń stosuje najlepsze praktyki i procedury w zakresie pozyskiwania i przetwarzania dowodów cyfrowych;

6. Student zna różne techniki informatyki śledczej w zakresie gromadzenia i analizy różnego rodzaju dowodów cyfrowych z wykorzystaniem określonych technik i narzędzi.

Spis treści

1. Pojęcia, definicje i modele
2. Zabezpieczanie i gromadzenie dowodów cyfrowych na miejscu przestępstwa
3. Procedury pozyskiwania dowodów cyfrowych
3.1. Procedury sterylizacji
3.2. Techniki pozyskiwania
4. Pozyskiwanie i analiza informacji lotnych
5. Identyfikacja i analiza punktów zainteresowania informacji w systemach operacyjnych
6. Wykorzystanie narzędzi analitycznych typu OpenSource
7. Studia przypadków z zakresu informatyki śledczej
7.1 Studium przypadku 1: Hakowanie przy użyciu narzędzi SO systemu Windows

Wykazanie spójności treści z efektami kształcenia jednostki kursowej

Celem modułu jest teoretyczne zapoznanie się z koncepcjami informatyki śledczej oraz wykorzystanie tej wiedzy do gromadzenia, analizowania i zabezpieczania materiału dowodowego, co prowadzi do uznania go za dowód w sądzie. Treści zawarte w programie tego modułu pozwalają na utrwalenie tego celu.

Metodyka nauczania

Teoretyczne i praktyczne filmy wideo, które obejmują prezentację tematów popartą demonstracjami nauczyciela, a następnie quizy oceniające postępy uczniów i analizę rzeczywistych przypadków. W zależności od wyników uczniów w quizach, należy im udostępnić różne filmy wideo, aby wzmocnić te przedmioty, w przypadku których ocena nie osiągnęła minimalnego poziomu wymaganego do przejścia do następnego przedmiotu. W ten sposób każdy uczeń mógłby mieć własną ścieżkę na filmach przygotowanych dla danego modułu, w zależności od swoich wyników.

Wykazanie spójności metodologii nauczania z efektami kształcenia jednostki kursowej

Umiejętności, które należy osiągnąć w ramach tego modułu, dzielą się na dwa obszary: obszar teoretyczny dotyczący procedur gromadzenia, analizy i zabezpieczania dowodów. Przyjęta metodyka nauczania dzieli się na dwa rodzaje filmów: teoretyczne i praktyczne filmy wykładowe ukierunkowane na osiągnięcie celu związanego z wiedzą teoretyczną z zakresu technik informatyki śledczej oraz zajęcia laboratoryjne ukierunkowane na naukę posługiwania się narzędziami; filmy demonstracyjne ukierunkowane na osiągnięcie celu związanego z efektywnym posługiwaniem się narzędziami do analizy śladów kryminalistycznych.

Metody oceny

Ocena opiera się na zestawie quizów, które koncentrują się na ważnych aspektach każdej z treści. Każdy uczeń musi uzyskać określony procent poprawnych odpowiedzi, aby przejść do następnego tematu.

Bibliografia główna

[1] BUNTING, Steve, The Official EnCE: EnCase Certified Examiner Study Guide, 2012.
[2] GRUNDY, Barry J., The Law Enforcement and Forensic Examiner's Introduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.
[3] CASEY, Eoghan, Digital Evidence and Computer Crime, Academic Press, 2011.
[4] BROWN, Christopher L. T., Dowody komputerowe: Gromadzenie i zabezpieczanie, wyd. 2, 2009.
[5] CARVEY, Harlan, Badanie systemów Windows, wydanie 1, 2018.
[6] HALE LIGH, Michael, Sztuka kryminalistyki pamięci: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition, 2014.
[7] ENISA, Identyfikacja i postępowanie z dowodami elektronicznymi Toolset, wrzesień 2013 r.

[8] ENISA, Identyfikacja i postępowanie z dowodami elektronicznymi Podręcznik, wrzesień 2013 r.
[9] NIST, Computer Security Incident Handling Guide, Special Publication 800-61r2.