AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu zajęć: Pozyskiwanie, zabezpieczanie i analiza danych cyfrowych

Rok akademicki: 2019/2020 Kod: HNKT-1-507-s Punkty ECTS: 2

Wydział: Humanistyczny

Kierunek: Nowoczesne technologie w kryminalistyce Specjalność: —

Poziom studiów: Studia I stopnia Forma studiów: Stacjonarne

Język wykładowy: Polski Profil: Ogólnoakademicki (A) Semestr: 5

Strona www: —

Prowadzący moduł: dr inż. Faber Łukasz (faber@agh.edu.pl)

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

Przedmiot uszczegóławia zagadnienia informatyki śledczej i analizy dowodowej w zakresie pozyskiwania, zabezpieczania i analizy danych cyfrowych.

Opis efektów uczenia się dla modułu zajęć

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Powiązania z KEU	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć
Wiedza: zna i rozumie			
M_W001	Zna konstrukcję systemów plików, pamięci i ruchu sieciowego w stopniu pozwalającym na ich analizę.	NKT1A_W04	Wykonanie ćwiczeń laboratoryjnych
M_W002	Zna podstawowe artefakty w systemach Windows, Linux, macOS, Android i iOS.	NKT1A_W04	Wykonanie ćwiczeń laboratoryjnych
Umiejętności: potrafi			
M_U001	Potrafi przeprowadzić analizę dowodową w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.	NKT1A_U04	Wykonanie ćwiczeń laboratoryjnych
Kompetencje społeczne: jest gotów do			
M_K001	Rozumie, jakie konsekwencje mogą mieć dane pozyskane w ramach analizy dowodowej.	NKT1A_K02	Egzamin

Liczba godzin zajęć w ramach poszczególnych form zajęć

	Forma zajęć dydaktycznych										
Suma	Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
40	20	0	0	20	0	0	0	0	0	0	0

Matryca kierunkowych efektów uczenia się w odniesieniu do form zajęć i sposobu zaliczenia, które pozwalają na ich uzyskanie

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Forma zajęć dydaktycznych									
		Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
Wiedza: zna i rozumie												
M_W001	Zna konstrukcję systemów plików, pamięci i ruchu sieciowego w stopniu pozwalającym na ich analizę.	+	-	-	+	-	-	-	-	-	-	-
M_W002	Zna podstawowe artefakty w systemach Windows, Linux, macOS, Android i iOS.	+	-	-	+	-	-	-	-	-	-	-
Umiejętności: potrafi												
M_U001	Potrafi przeprowadzić analizę dowodową w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.	+	-	-	+	-	-	-	-	-	-	-
Kompetencje społeczne: jest gotów do												
M_K001	Rozumie, jakie konsekwencje mogą mieć dane pozyskane w ramach analizy dowodowej.	+	-	-	+	-	-	-	-	-	-	-

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w zajęciach dydaktycznych/praktyka	40 godz
Przygotowanie do zajęć	10 godz
Samodzielne studiowanie tematyki zajęć	10 godz
Dodatkowe godziny kontaktowe	5 godz
Sumaryczne obciążenie pracą studenta	65 godz
Punkty ECTS za moduł	2 ECTS

Pozostałe informacje

Szczegółowe treści kształcenia w ramach poszczególnych form zajęć (szczegółowy program wykładów i pozostałych zajęć)

Wykład

1. Zbieranie cyfrowych danych dowodowych.
2. Zaawansowane artefakty w systemach Windows, Linux Windows, Linux, macOS.
3. Zaawansowane artefakty w systemach mobilnych Android i iOS.
4. Zaawansowana analiza pamięci operacyjnej.
5. Zaawansowana analiza systemów plików.
6. Zaawansowana analiza ruchu sieciowego.

Ćwiczenia projektowe

Projekt obejmować będzie przeprowadzenie własnej analizy dowodowej lub przygotowanie demonstracyjnego zestawu danych.

Metody i techniki kształcenia:

Wykład: Treści prezentowane na wykładzie są przekazywane w formie prezentacji multimedialnej w połączeniu z klasycznym wykładem tablicowym wzbogaconymi o pokazy odnoszące się do prezentowanych zagadnień.
Ćwiczenia projektowe: Nie określono

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

Projekt: średnia ważona ocen za realizację etapów projektu.

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:

Wykład:
– Obecność obowiązkowa: Nie
– Zasady udziału w zajęciach: Studenci uczestniczą w zajęciach poznając kolejne treści nauczania zgodnie z syllabusem przedmiotu. Studenci winni na bieżąco zadawać pytania i wyjaśniać wątpliwości. Rejestracja audiowizualna wykładu wymaga zgody prowadzącego.
Ćwiczenia projektowe:
– Obecność obowiązkowa: Tak

– Zasady udziału w zajęciach: Nie określono

Sposób obliczania oceny końcowej
Ocena końcowa to ocena z projektu.

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:
Dopuszczalny będzie jeden dodatkowy termin oddawania projektu.

Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności modułów
Wymagane jest ukończenie przedmiotu “Wprowadzenie do informatyki śledczej”.

Zalecana literatura i pomoce naukowe

- Jason T. Luttgens, Matthew Pepe. "Incident Response & Computer Forensics, Third Edition." 2014, McGraw-Hill Education.
- Gerard Johansen. "Digital Forensics and Incident Response." 2017, Packt Publishing.
- Michael Hale Ligh & Andrew Case & Jamie Levy & Aaron Walters. "The Art of Memory Forensics". 2014, John Wiley and Sons.
- Bruce Nikkel. "Practical Forensic Imaging." 2016, No Starch Press.

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu
Nie podano dodatkowych publikacji

Informacje dodatkowe
Brak