AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu zajęć: Wprowadzenie do informatyki śledczej

Rok akademicki: 2019/2020 Kod: HNKT-1-209-s Punkty ECTS: 4

Wydział: Humanistyczny

Kierunek: Nowoczesne technologie w kryminalistyce Specjalność: —

Poziom studiów: Studia I stopnia Forma studiów: Stacjonarne

Język wykładowy: Polski Profil: Ogólnoakademicki (A) Semestr: 2

Strona www: —

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

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

Przedmiot wprowadza w szerokie zagadnienie informatyki śledczej i analizy dowodowej w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.

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
60	30	0	30	0	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	60 godz
Przygotowanie do zajęć	20 godz
Samodzielne studiowanie tematyki zajęć	25 godz
Dodatkowe godziny kontaktowe	5 godz
Sumaryczne obciążenie pracą studenta	110 godz
Punkty ECTS za moduł	4 ECTS

Pozostałe informacje

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

Wykład

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

Ćwiczenia laboratoryjne

1. Metody zbierania danych do analizy
2. Analiza pamięci operacyjnej
3. Analiza systemów plików
4. Analiza ruchu sieciowego
5. Analiza artefaktów użytkownika
6. Analiza systemów mobilnych
7. Przygotowanie własnej analizy dowodowej.

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 laboratoryjne: W trakcie zajęć laboratoryjnych studenci samodzielnie rozwiązują zadany problem praktyczny, dobierając odpowiednie narzędzia. Prowadzący stymuluje grupę do refleksji nad problemem, tak by otrzymane wyniki miały wysoką wartość merytoryczną.

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

Laboratorium: średnia ocen z poszczególnych tematów laboratoriów.

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 laboratoryjne:
– Obecność obowiązkowa: Tak
– Zasady udziału w zajęciach: Studenci wykonują ćwiczenia laboratoryjne zgodnie z materiałami udostępnionymi przez prowadzącego. Student jest zobowiązany do przygotowania się w przedmiocie wykonywanego ćwiczenia, co może zostać zweryfikowane kolokwium w formie ustnej lub pisemnej. Zaliczenie zajęć odbywa się na podstawie zaprezentowania rozwiązania postawionego problemu.

Sposób obliczania oceny końcowej

Średnia ocen z laboratorium i egzaminu.

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:

W przypadku usprawiedliwionej nieobecności na zajęciach laboratoryjnych student może odrobić maksymalnie jedne zajęcia w innym terminie.
Nieusprawiedliwione nieobecności na laboratorium powodują brak zaliczenia przedmiotu.

Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności modułów

Studenci powinni:
- rozumieć budowę pamięci operacyjnej,
- znać budowę prostego systemu plików (np. FAT, albo EXT2),
- znać podstawy sieci.

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