

KARTA OPISU PRZEDMIOTU

STUDIA PODYPLOMOWE	INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDTCZEJ
--------------------	---

NAZWA PRZEDMIOTU	INFORMATYKA ŚLEDZCA		
SUBJECT TITLE	COMPUTER FORENSICS		
SEMESTR STUDIÓW	ECTS (pkt.)	TRYB ZALICZENIA PRZEDMIOTU	KOD PRZEDMIOTU
1	5	EGZAMIN	
Wymagania wstępne w zakresie przedmiotu	Nazwy przedmiotów	-	
	Wiedza	1. Podstawowa wiedza z zakresu technologii informacyjnej	
	Umiejętności	1. Potrafi obsługiwać komputer i system operacyjny 2. Potrafi samodzielnie dokonywać zmian konfiguracji sprzętowej zestawu komputerowego 3. Potrafi myśleć analitycznie i przewidywać z dużym wyprzedzeniem konsekwencje podejmowanych działań	
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie	

PROGRAM PRZEDMIOTU		
FORMA ZAJĘĆ	LICZBA GODZIN ZAJĘĆ W SEMESTRZE	PROWADZĄCY ZAJĘCIA (tytuł/stopień naukowy, imię i nazwisko)
WYKŁAD	15	MGR INŻ. ARTUR KALINOWSKI
ĆWICZENIA		
LABORATORIUM	15	MGR INŻ. ARTUR KALINOWSKI
PROJEKT		
SEMINARIUM		

TREŚCI KSZTAŁCENIA (PROGRAM NAUCZANIA)			
WYKŁAD	SPOSÓB REALIZACJI:	WYKŁAD Z WYKORZYSTANIEM RZUTNIKA	
Lp.	Tematyka zajęć		Liczba godzin
1.	Cele, podstawowe zasady i obszar działań informatyki śledczej		1
2.	Tworzenie zaplecza technicznego		1
3.	Klasyfikacja typów danych i miejsca ich występowania		1
4.	Metody pozyskiwania i zabezpieczania materiału do analizy		1
5.	Budowa popularnych systemów plików		1
6.	Miejsca przechowywania istotnych danych w popularnych systemach operacyjnych		1
7.	Wstępna analiza danych z utworzonych obrazów nośników i zrzutów pamięci		1
8.	Lokalizacja i odzyskiwanie usuniętych plików		1
9.	Analiza obszarów slack space oraz RAM slack		1
10.	Wyodrębnianie ciągów tekstowych z plików binarnych oraz danych binarnych z plików nieokreślonego typu oraz nośników		1
11.	Określanie lokalizacji poszukiwanych danych na nośniku		1
12.	Przeprowadzanie analizy czasowej		1
13.	Ukrywanie danych na nośnikach poza widoczną strukturą systemu plików		1
14.	Ukrywanie danych w systemie plików		1

15.	Analiza pliku binarnego w celu określenia struktury zawartych w nim danych Zaliczenie przedmiotu.	1
RAZEM GODZIN W SEMESTRZE		15
Sposoby sprawdzenia zamierzonych efektów kształcenia		Kolokwium pisemne

LABORATORIUM		SPOSÓB REALIZACJI:	ZAJĘCIA PRAKTYCZNE Z KOMPUTEREM
Lp.	Tematyka zajęć		Liczba godzin
1.	Tworzenie obrazów nośników z wykorzystaniem blokerów sprzętowych i programowych		1
2.	Porównanie metod tworzenia obrazów nośników oraz ich wad i zalet		1
3.	Zabezpieczanie danych ulotnych		1
4.	Zabezpieczanie plików z danymi		1
5.	Zabezpieczanie danych z wykorzystaniem sieci komputerowej		1
6.	Pozyskiwanie oraz analiza danych z przeglądarek internetowych, programów pocztowych i komunikatorów		1
7.	Podłączanie obrazu nośnika i przeglądanie zgromadzonych na nim danych		1
8.	Odzyskiwanie usuniętych plików z dysków i kart pamięci		1
9.	Pozyskiwanie danych z obszaru slack space		1
10.	Wyodrębnianie ciągów tekstowych oraz znanych typów danych binarnych z obrazu nośnika lub z pliku		1
11.	Określanie fizycznej lokalizacji poszukiwanych danych na dysku (lub w obrazie nośnika) oraz powiązanego z tymi danymi pliku i sąsiadującego obszaru danych		1
12.	Wykorzystanie terminala dyskowego		1
13.	Przeprowadzanie analizy czasowej		1
14.	Tworzenie bazy sygnatur i wyszukiwanie danych w oparciu o bazę sygnatur		1
15.	Analiza pliku nieznanego typu w edytorze szesnastkowym		1
RAZEM GODZIN W SEMESTRZE			15
Sposoby sprawdzenia zamierzonych efektów kształcenia:		Wykonanie zadań wyznaczonych w trakcie zajęć	

Efekty kształcenia dla przedmiotu – po zakończonym cyklu kształcenia	Wiedza	1. Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy zabezpieczaniu elektronicznego materiału dowodowego. 2. Ma podstawową wiedzę o trendach rozwojowych w informatyce i ich wpływie na przetwarzanie i magazynowanie danych w komputerach PC.
	Umiejętności	1. Ma umiejętność samokształcenia się i wyszukiwania potrzebnych informacji 2. Potrafi pozyskiwać i analizować dane, a także umiejętnie interpretować otrzymane wyniki
	Kompetencje społeczne	1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role. 2. Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.

ZAŁOŻENIA I CELE PRZEDMIOTU:

Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie zabezpieczania nośników danych oraz analizy danych pozyskanych z zabezpieczonych nośników pod kątem wykorzystania ich jako materiał dowodowy.

METODY DYDAKTYCZNE:

Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (środki: rzutnik, komputer, prezentacje).

Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego, blokery).

FORMA I WARUNKI ZALICZENIA PRZEDMIOTU:

Wykład – zaliczenie pisemne na ocenę. Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

LITERATURA PODSTAWOWA:

- [1] Kalinowski A., *Metody Inwigilacji i Elementy Informatyki Śledczej.*, ISBN: 978-83-923745-4-1, CSH, 2011
[2] Mueller S., *Rozbudowa i naprawa komputerów PC. Wydanie XVIII.*, ISBN: 978-83-246-1511-7, Helion, 2009

LITERATURA UZUPEŁNIAJĄCA:

- [1] Metzger P., *GIMP. Anatomia PC. Wydanie XI.*, ISBN: 83-246-1119-3, Helion, 2007
[2] Danowski B., Chabiński A., *Montaż komputera PC. Ilustrowany przewodnik.*, ISBN: 83-246-0693-9, Helion, 2007
[3] Lal K., Rak T., *Linux. Komendy i polecenia. Praktyczne przykłady.*, ISBN: 83-7361-994-1, Helion, 2005
[4] Ward B., *Jak działa Linux.*, ISBN: 83-7361-753-1, Helion, 2005

*) niewłaściwe przekreślić

.....
/Kierownik studiów podyplomowych/

.....
/autor – osoba prowadząca wykład/

.....
/Kierownik jednostki organizacyjnej:
pieczęć i podpis/

.....
/Dziekan Wydziału WEAI:
pieczęć i podpis/