Karta przedmiotu

Nazwa i kod przedmiotu	Informatyka sądowa (Ćw.laboratoryjne), PG_00188512						
Kierunek studiów	Analityka kryminalistyczna						
Data rozpoczęcia studiów	październik 2026 r.		Rok akademicki realizacji przedmiotu	2026/2027			
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów			
Forma studiów	stacjonarne		Sposób realizacji	na uczelni			
Rok studiów	1		Język wykładowy	polski Język Polski			
Semestr studiów	2		Liczba punktów ECTS	2.0			
Profil kształcenia	ogólnoakademicki		Forma zaliczenia	zaliczenie			
Jednostka prowadząca							
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr inż. Stanisław Witkowski				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	0.0	0.0	30.0	0.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach	Praca własna studenta		RAZEM
	Liczba godzin pracy studenta	30		5.0	15.0		50
Cel przedmiotu	Głównym celem informatyki sądowej jest dostarczanie cyfrowych dowodów na potrzeby postępowań prawnych. Obejmuje to zbieranie, odzyskiwanie, analizę i prezentację danych cyfrowych z różnych nośników (np. dysków twardych, telefonów komórkowych, chmury) w celu wyjaśnienia przestępstw, nadużyć lub odtworzenia przebiegu zdarzeń.Kluczowe cele informatyki sądowej: 1. Zbieranie i odzyskiwanie danych 2. Analiza danych 3. Dostarczanie dowodów 4. Wsparcie organów prawnych 5. Badanie nadużyć						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[AKRL3_K05] Absolwent jest gotów do popularyzacji nauki i kształtowania świadomości społecznej w zakresie analityki kryminalistycznej.	Student potrafi wykorzystać poznane oprogramowanie do pozyskiwania w sposób legalny informacji z sieci.	[SK1] oral statement/conversation/ discussion [SK2] presentation/project/paper/ report [SK3] text preparation/written work [SK5] implementation of a problem task [SK8] observation of student's independent or team work
	[AKRL3_U06] Absolwent potrafi wykorzystać oprogramowanie specjalistyczne oraz zaawansowane techniki informacyjno-komunikacyjne do opracowania i wizualizacji danych eksperymentalnych.	Jest przygotowany do uzupełniania swojej wiedzy; umie ocenić stopień zrozumienia przez siebie problemu.	[SU1] oral statement/conversation/ discussion [SU3] text preparation/written work [SU5] implementation of a problem task [SU6] demonstration of practical skills [SU8] observation of student's independent or team work
	[AKRL3_W08] Absolwent zna i rozumie zastosowanie technologii informacyjnych w analizie danych, interpretacji wyników i raportowaniu badań kryminalistycznych.	Student zna i rozumie zagadnienia związane z pozyskiwaniem informacji z systemów informatycznych, a także przepisy prawne i normy, które musi spełnić aby pozyskać informację w sposób legalny.	[SW4] test/exam - oral or written [SW1] oral statement/ conversation/discussion [SW5] implementation of a problem task

Treści przedmiotu	**1. Wprowadzenie.** • Informatyka sądowa i dowód elektroniczny definicje, koncepcje, ryzyka. • Incident response na podstawie norm serii 27000. • Procesy i procedury informatyki sądowej. • Najlepsze praktyki informatyki sądowej. **2. Wybrane aspekty prawne** • Podstawowe przepisy i akty prawne. • Prawa i obowiązki biegłych. • Ekspertyzy i opinie prywatne. **3. Warsztat informatyka śledczego** • Blokery. • Urządzenia kopiujące. • Urządzenia mobilne. **4. Zabezpieczenie materiału dowodowego** • Podstawowe zasady i przygotowanie do zabezpieczania nośników / danych. • Zabezpieczanie z użyciem blokerów. • Zabezpieczanie z użyciem urządzeń mobilnych. • Metodyka zabezpieczania danych. **5. Zabezpieczanie systemów Linux. Wykorzystywanie dystrybucji programów informatyki śledczej systemów Linux** • Wprowadzenie. • Omówienie komendy dd. • Podstawowa prezentacja dystrybucji systemu Linux Sumuri Paladin/CAINE. **6. Wprowadzenie do programu FTK Imager** • Przygotowanie do pracy z programem FTK Imager. • Przegląd programu. • Tworzenie kopii binarnej. • Wstępna selekcja danych, TRIAGE. **7. Wprowadzenie do programu Magnet Acquire** • Omówienie programu. • Tworzenie kopii binarnej. • Omówienie różnic w możliwościach konfiguracji plików obrazów wykonywanych z wykorzystaniem FTK Imagera oraz Magnet Acquire. **8. Wprowadzenie do programu Autopsji.** • Przygotowanie i konfiguracja programu. • Tworzenie sprawy. • Analiza obrazu dysku. • Przegląd plików graficznych oraz dokumentów. **9. Alternatywne strumienie danych w systemie NTFS** • Podstawy • Ćwiczenia praktyczne **10. Analiza śledcza przygotowanych materiałów samodzielne ćwiczenia** • Praca na przygotowanym materiale dowodowym. Student prowadzi **podstawową** analizę śledczą na podstawie zdobytej wcześniej wiedzy **11. Zabezpieczanie i analiza obrazów pamięci RAM** • Wprowadzenie do programu Volatility • Ćwiczenia praktyczne **12. Live Forensic** • Przygotowanie wersji mobilnej programu Autopsji • Przydatne bezpłatne oprogramowanie • Ćwiczenia praktyczne **13. Analiza wybranych norm i standardów sądowych w Polsce i w UE.**

14. "Projekt" sprawy sądowej

a) Tworzenie bezpiecznego środowiska pracy.
b) Techniki pozyskiwania informacji (rejestry państwowe, przeglądarki internetowe, serwisy społecznościowe, Deep Web).
c) Zaawansowane techniki analizy danych (analiza metadanych, techniki analizy obrazów, analiza infrastruktury, sposoby na deanonimizację).

15. Test końcowy

Eksperci z informatyki sądowej potrafią m.in:

- pozyskiwać dane skasowane z komputera;
- pozyskiwać dane ukryte w komputerze;
- analizować dokładnie pracę komputera oraz systemu komputerowego (czyli ustalać wszystkie czynności podejmowane na danym komputerze krok po kroku);
- pozyskiwać dane z zniszczonych nośników (połamane dyski twarde, utopione lub nadpalone komputery, komórki etc.);
- odzyskiwać skasowane e-maila oraz smsy (w tym odtwarzać ich treść);
- ustalać historię korzystania z internetu przez użytkownika komputera (np. w celu ustalenia czy korzystał on z stron z treścią niedozwoloną);
- poddawać analizie programy komputerowe zainstalowane na danym komputerze (np. czy dany program ma ważną licencję, ustalanie czemu dokładnie służy);
- analizować poziom zabezpieczenia komputerowego w celu ustalenia czy do komputera nie włamał się nikt z zewnątrz, a jeśli to zrobił to jakie podjął działania na przejętym komputerze.

Wymagania wstępne i dodatkowe

Umiejętność wyszukiwania informacji w sieci internetowej.

Umiejętność poszukiwania podstawowej logiki zdarzeń na podstawie dostępnych materiałów.

Podstawowa wiedza z zakresu cyberbezpieczeństwa, sieci komputerowych oraz umiejętność pozyskiwania informacji ze wskazanych źródeł.

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
50% - wejsciówka, 20% - aktywność, 30% - sprawozdania	50.0%	100.0%

Zalecana lista lektur

Podstawowa lista lektur	1. William Oettinger Informatyka śledcza. Gromadzenie, analiza i zabezpieczenie dowodów elektronicznych dla początkujących 2022 wyd. Helion S.A. 2. C. Altheide, H. Carvey Informatyka śledcza. Przewodnik po narzędziach open source, Helion 2014 3. Dz. U. 2018 poz. 1560, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa 4. J. Kavrestad, "Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications", Springer, 2nd Edition, 2020 5. W. Oettinger, "Learn Computer Forensics: a beginner's guide to searching, analyzing, and securing digital evidence", Packt Publishing, 2020 6. A. Chojnowski Informatyka sądowa w praktyce. Wydawnictwo:Helion. 2020
Uzupełniająca lista lektur	1.C. Altheide, H. Carvey, Informatyka śledcza. Przewodnik po narzędziach open source, Gliwice 2014 2.A. Kalinowski, Metody inwigilacji i elementy informatyki śledczej, Kwidzyn 2013 3.H. Carvey, Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows, Gliwice 2013 4. M. SZMIT Elementy Informatyki Sądowej, Polskie Towarzystwo Informatyczne 2011

	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	1. Jak stwierdzić, czy nośnik zawiera pliki o nazwach ABC 2. Jak stwierdzić, czy nośnik obejmuje pliki zawierające w swej treści słowa XYZ 3. Jak stwierdzić, czy na nośniku znajdują się pliki np. pakietu Office, multimedialne, bądź graficzne 4. Jak stwierdzić, czy dane z nośnika były usuwane, kasowane, modyfikowane, kopiowane, zapisywane na nośniki zewnętrzne, przenoszone do innej lokalizacji, wysyłane za pośrednictwem elektronicznych kanałów komunikacji 5. Jak stwierdzić, kiedy został zainstalowany system operacyjny w tej chwili zapisany na nośniku 6. Jak stwierdzić, czy dysk twardy był formatowany, a jeśli tak to kiedy i przez jakiego użytkownika 7. Jak stwierdzić, czy za pośrednictwem komputera wysyłana była korespondencja mailowa z konta użytkownika Jan Kowalski 8. Jak stwierdzić, czy skrzynka pocztowa zawiera korespondencję mailową wysyłaną i odbieraną od użytkownika Jan Nowak 9. Jak stwierdzić, czy skrzynka mailowa zawiera załączniki wskazujące na treści XYZ 10. Jak stwierdzić, czy w historii korespondencji mailowej znajdują się treści wskazujące na kradzież danych stanowiących tajemnicę przedsiębiorstwa 11. Jak stwierdzić, czy w korespondencji mailowej znajdują się pliki wskazujące na niedochowanie przez inspektora procedur BHP 12. Jak stwierdzić, czy wśród danych wykasowanych z nośnika znajduje się plik o nazwie baza danych 13. Jak stwierdzić, czy komputer zawiera pliki o charakterze pornograficznym 14. Jak stwierdzić, czy przy użyciu komputera użytkownik odwiedzał strony internetowe o tematyce abc 15. Jak stwierdzić, czy użytkownik logował się przy użyciu komputera do portalu, bądź aplikacji abc 16. Czy zapisy zawarte w logach systemu informatycznego znajdują się informacje świadczące o fałszowaniu kart pacjentów 17. Jak stwierdzić, czy telefon zawiera wiadomości sms przychodzące z numeru 123 18. Jak stwierdzić, czy w historii połączeń (również tej wykasowanej) widnieją połączenia z numerem 123 19. Jak stwierdzić, czy w historii wiadomości sms znajdują się treści o charakterze uporczywego nękania czyli stalkingu 20. Jak wyodrębnić dane o często zadawanych pytaniach	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.