

AGENDA

Kurs będzie odbywać się w godzinach 9-17, w cenie przewidziane są dwie przerwy kawowe oraz obiad.

Dzień 1

Temat	Szczegóły	Prowadzący
Wprowadzenie	Podstawowe pojęcia Polskie regulacje prawne Standardy i procedury Obsługa incydentów a norma ISO i specyfikacje NIST oraz SANS Institute	20
Wprowadzenie do informatyki śledczej	Linux jako platforma do wykonywania analiz Zabezpieczanie danych Wyszukiwanie informacji Rekonstrukcja informacji Ograniczanie zakresu wyszukiwania	20
Ćwiczenia	Prawidłowe tworzenie dokumentacji Identyfikacja danych Zabezpieczanie danych	60

Dzień 2

Temat	Szczegóły	%
Budowa systemów plików	EXT2/EXT3 FAT NTFS	10
Ćwiczenia	Analiza dysków - podstawy	10
Wprowadzenie do informatyki śledczej (ciąg dalszy)	Windows jako platforma do wykonywania analiz Wyszukiwanie informacji Rekonstrukcja informacji Ograniczanie zakresu wyszukiwania Super Timeline – odtworzenie zdarzeń w czasie	20
Ćwiczenia	Wyszukiwanie danych Analiza dysków Analiza dzienników zdarzeń Odtworzenie zdarzeń w czasie – system Windows Historia przeglądarki Identyfikacja nielegalnego oprogramowania Analiza nagłówków email	60

Dzień 3

Temat	Szczegóły	%
Ćwiczenia	Analiza systemu plików pochodzącego z komputera na który dokonano włamania	20
Analiza urządzeń mobilnych	Wprowadzenie do analizy telefonów komórkowych i urządzeń „smart”	10
Ćwiczenia	Pobieranie danych z urządzeń mobilnych	10
Ćwiczenia - analiza pamięci RAM systemów Windows	Kopiowanie zawartości pamięci Analiza pamięci	20
Ćwiczenia - Ukrywanie i wykrywanie danych	ADS Ukrywanie w obiektach (pliki graficzne, wykonywalne, muzyczne) Ukrywanie w metadanych	30
Egzamin		10