Szkolenie

Informatyka śledcza Pozyskiwanie i analiza elektronicznych dowodów przestępstw

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Fascynuje Cię świat przestępstw komputerowych? Chcesz poznać najnowsze technologie stosowane w kryminalistyce IT? Musisz wiedzieć jak postępować w sytuacji, gdy kluczowym jest zabezpieczenie dowodów na urządzeniach mobilnych? Nie zwlekaj i już dziś zapisz się na szkolenie informatyki śledczej w Autoryzowanym Centrum Szkoleniowym Dagma!

Dlaczego właśnie my?

Nasze szkolenia prowadzą uznani w Polsce i na świecie eksperci w informatyce śledczej. Ich wiedzę potwierdzają liczne certyfikaty i dyplomy. O wysokich kwalifikacjach i niezwykłym doświadczeniu naszych trenerów świadczyć może fakt, że polskie sądy i policja regularnie proszą ich o pomoc przy zdobywaniu dowodów do toczących się śledztw.

1 dzień szkolenia

Podczas pierwszego dnia szkolenia przyswoisz podstawy konieczne do rozpoczęcia przygody z kryminalistyką IT. Dowiesz się, co to jest dowód elektroniczny i jak należy się z nim obchodzić. Poznasz cyfrowe metody śledcze. Nauczysz się, jak zabezpieczyć dane zawarte na nośniku cyfrowym i jak nadać im wartość dowodową. Zapoznasz się także z urządzeniami i oprogramowaniem niezbędnym w świecie informatyki śledczej. Ponadto będziesz miał niepowtarzalną okazję, aby przećwiczyć metody zabezpieczania nośników z wykorzystaniem najlepszych światowych urządzeń Falcon firmy Logicube, a także urządzeń mobilnych za pomocą UFED firmy Cellabrite – potentata na rynku informatyki śledczej, specjalizującego

się w urządzeniach mobilnych. Do Twojej dyspozycji oddamy również narzędzie do zabezpieczania zaszyfrowanych kopii dysków twardych z komputerów Mac Recon - firmy Sumuri.

2 dzień szkolenia

Drugiego dnia szkolenia nauczymy Cię jak stworzyć własne środowisko analityczne, które może Ci służyć przez wiele lat Twojej kariery. Zdradzimy, jak w sposób całkowicie „bezprogramowy" przeprowadzić pełne badania nośników cyfrowych, jak zabezpieczać dane mając do dyspozycji jedynie CDLive z systemem Linux. Odkryjemy przed Tobą tajniki analiz systemów VSS, tablicy MFT, sposoby ukrywania i wyszukiwania informacji w alternatywnych strumieniach danych, sposoby ukrywania tekstu w grafice - steganografia oraz przedstawimy „setkę" innych zagadnień z zakresu zaawansowanych technik wykorzystywanych w kryminalistyce komputerowej.

3 dzień szkolenia

Trzeciego dnia skupiamy się na urządzeniach mobilnych – poznasz programy i narzędzia, pomagające wyodrębniać informacje zapisane w pamięci urządzeń mobilnych, z wykorzystaniem uznanych na świecie urządzeń UFED firmy Cellebrite. Nauczysz się obsługi specjalistycznego oprogramowania, ekstrakcji logicznej urządzeń oraz kart SIM, poznasz metody ekstrakcji systemu plików i dowiesz się jak wyszukać konkretną informację w gąszczu wszystkich posiadanych danych.

Całość szkolenia opiera się na praktycznych zadaniach, realizowanych na przygotowanych obrazach urządzeń mobilnych, a także na fizycznych smartfonach i tabletach. Ten etap szkolenia wprowadzi Cię w świat analizy istniejących i usuniętych danych, budowania wyrażeń regularnych, umożliwiających wyszukiwanie danych w kodach Hexadecymalnych oraz wyszukiwania artefaktów pomijania zabezpieczeń i blokad użytkowników.

Program szkolenia

Dzień 1

- Informatyka śledcza - definicja, znaczenie
- Cele informatyki śledczej
- Dowód elektroniczny
- Co nam wolno, a na co powinniśmy uważać
- Założenia informatyki śledczej
- Polskie i światowe praktyki wykorzystywane w informatyce śledczej
- Procesy analizy śledczej
- Sposób zabezpieczania i gromadzenia danych
- Reguły i zasady przeprowadzania analizy śledczej
- Opis i przedstawienie narzędzi wykorzystywanych przez śledczych
- Opis i przedstawienie programów wykorzystywanych przez śledczych
- Co to jest kopia binarna i po co jest nam w ogóle potrzebna
- Proces zabezpieczenia materiału jako dowodu
- Kopie binarne komputerów pple
- Proces zabezpieczenia materiału dowodowego zaszyfrowanych nośników
- Proces zabezpieczenia materiału dowodowego – Live Forensics
- Logiczna ekstrakcja urządzeń mobilnych
- Logiczna ekstrakcja – system plików urządzeń mobilnych
- Fizyczna ekstrakcja urządzeń mobilnych
- Różnice między logiczną a fizyczną ekstrakcja urządzeń mobilnych
- Przedstawienie materiału dowodowego z wykorzystaniem interaktywnych raportów
- Cloud Forensics - mechanizmy zabezpieczania danych z chmury
- Suma kontrolna - czy warto ją robić
- Jak przechowywać dowód elektroniczny
- Zabezpieczanie dysków, poczty elektronicznej, strony internetowej, innych nośników
- Zabezpieczanie informacji ulotnych
- Przekazanie materiału dowodowego

Dzień 2

- Wykonywane kopii binarnych w środowisku lokalnym
- Wykonywane kopii binarnych w środowisku sieciowym
- Analiza i zabezpieczanie danych z Volume Shadow Copy
- Różnice w analizie koszta systemowego w systemach operacyjnych
- Analiza zawartości pagefile.sys oraz hiberfile
- Analiza zawartości bufora wydruku
- Ukrywanie danych w Alternatywnych strumieniach danych
- Wyszukiwanie plików w Alternatywnych strumieniach danych
- Informacje zawarte w listach szybkiego dostępu
- Zabezpieczanie informacji ulotnych - TRIGE
- Analiza Prefetch
- Zabezpieczanie obrazu pamięci RAM
- Analiza zawartości pamięci RAM
- Wyszukiwanie plików po sygnaturach czasowych

- Automatyzacja pracy - budowa własnego narzędzia

Dzień 3

- Na czym polega logiczna i fizyczna ekstrakcja
- Klonowanie kart SIM
- Dlaczego karta SIM po klonowaniu zawiera niekompletne dane
- Logiczna ekstrakcja kart SIM
- Zakładanie nowej sprawy
- Analiza danych
- Tagowanie i zaawansowanie wyszukiwanie informacji
- Listy kontrolne
- Filtrowanie danych
- Analiza osi czasu
- Praktyczne analizy urządzeń mobilnych
- Jakie dane można wyodrębnić podczas fizycznej ekstrakcji
- Fizyczna ekstrakcja urządzeń mobilnych
- Praca w programie Physical Phone Analyzer
- Zakładanie nowej sprawy
- Analiza danych
- Analiza systemu plików
- Analiza systemu w kodzie HEX
- Analiza danych z wykorzystaniem wyrażeń regularnych
- Data Carving
- Tagowanie i zaawansowane wyszukiwanie informacji
- Listy kontrolne
- Filtrowanie danych
- Analiza osi czasu
- Wyszukiwanie i analiza złośliwego oprogramowania
- Wyszukiwanie artefaktów JailBreak w iPhone
- Pomijanie zabezpieczeń KOD PIN lub „wężyk” w urządzeniach mobilnych
- UFED Reader

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852