

# Tytuł szkolenia: Kryminalistyka w systemie Linux – poziom ekspercki

Kod szkolenia: Linux-kryminalistyka

## Wprowadzenie

## Adresaci szkolenia

Szkolenie przeznaczone jest dla osób, które chcą zapoznać się z zasadami kryminalistyki w systemie Linux.

## Cel szkolenia

## Czas i forma szkolenia

- 21 godzin (3 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

## Plan szkolenia

1. Biały wywiad na podstawie narzędzi w systemach Linux
2. Linux jako narzędzie wykonywania kopii binarnych - lokalnych i sieciowych
3. SED, GREP, AWK
4. Narzędzia do analizy tablicy MFT
5. Analiza osi czasu systemu Windows
6. Analizy binarnych plików - pagefile.sys, hiberfile, SPL, SHD, RAM
7. Zaawansowana analiza pamięci operacyjnej
8. Odzyskiwanie plików z wykorzystaniem systemu Linux
9. Steganografia w systemie Linux
10. Analiza logów w systemie Linux
11. Analiza strategicznych miejsc w systemie Linux
12. Analiza ruchu sieciowego na podstawie darmowych narzędzi
13. Gotowe platformy analityczne - przedstawienie i omówienie
14. Kali Linux USB z trybem zapisywania zmian