Operating System (OS) Forensics

Duration : 5 Day

Course Content

Setelah mengikuti training ini, peserta akan bisa melakukan proses mengumpulkan barang bukti (evidences) dan menganalisa secara live di komputer victim dengan menggunakan beberapa fitur atau utilitas bawaan dari OS tersebut.

Who Should Attend

Training ini ditujukan untuk:

- Security Operation Center Staff
- System Administrators
- Incident Response Team Staff
- Profesi lain terkait IT

Prerequisites

- Pengetahuan umum IT
- Pengetahuan dasar Cyber Security
- Operasi dasar Windows dan Linux

Course objectives

Setelah mengikuti pelatihan ini, peserta akan dapat:

- Mengumpulkan barang bukti (evidences)
- Menganalisa barang bukti secara langsung di komputer victim
- Melakukan Windows forensic
- Melakukan Linux forensicPengurangan frekuensi dan besarnya dampak dari berbagai insiden

Course Outline

- Konsep Dasar Computer Forensic
- Proses dalam Computer Forensic
- Role of First Responder
- Forensic Readiness
- Prinsip Barang Bukti Digital
- Apa itu volatile dan non-volatile information
- Pengumpulan Barang Bukti Digital
- Live forensic
- Windows memory analysis
- Windows registry analysis
- Audit policy
- Event logs analysis
- Shell command
- Linux log files