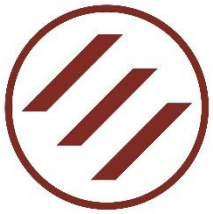
ADEO BİLİŞİM DANIŞMANLIK HİZMETLERİ SAN. VE TİC. A.Ş.

Adli Bilişim Temelleri ve Mobile Forensics

www.adeo.com.tr



Adli Bilişim Temelleri Eğitimi ve Mobile Forensics Eğitimi

Eğitim Süresi: 3 Gün

Eğitim İçeriği

- **Adli Bilişim Nedir ?**
  - *Dijital Delil Nedir?*
  - *Dijital Delilin Taşıması Gereken Nitelikler*
  - *Delil Toplama Süreci*
  - *Dijital Analiz ve Yaşam Döngüsü*
  - *Dijital Delil Tanımlama*
  - *Dijital Delil Koruma*
  - *Uçucu Veriler Tanımlama*
  - *Kritik Uçucu Veri Çeşitleri*
  - *Disk İmaj Formatları*
  - *Uçucu Veri Kurtarma Yöntemleri*
  - *Donanımsal Yöntemler ile Disk İmajı Alma*
  - *Yazılımsal Yöntemler ile Disk İmajı Alma*
  - *İmaj Analizi Yapmak için Kullanılabilecek Yazılımlar ve Yöntemler*
  - *HASH algoritması ve Adli Bilişim İncelemelerinde Olan Önemi*
  - *Delillerin Bulunabileceği Ortamlar*
  - *Olay Müdahalesi*
  - *Olay Müdahalesi Süreçleri*

- **Dosya Sistemi Analizi (NTFS)**
  - *NTFS Dosya Sistemi Çalışma Konsepti*
  - *FAT Dosya Sistemi Çalışma Konsepti*
  - *MFT Çalışma Yapısı*
  - *MFT Analizi*

- **Bellek Analizi**
  - *Bellek Imajının Alınması*
  - *Volatility aracı ile Bellek analizi*

- **Web Browsers Analizi**
  - *Cache İnceleme*
  - *Cookies İnceleme*
  - *Bookmarks İnceleme*
  - *Auto Complete Verileri*
  - *Web Browser Geçmiş Bilgileri*
  - *Download Analizi*
  - *Chrome, Explorer ve Firefox Arasındaki Farklar ve Kritik Dosyalar/Dizinler*
  - *Web Browser Database İncelemesi*

- **Email Analizi**
  - Email Trafik Temelleri
  - Email Yapısı ve Analizi
  - Ekler Analizi
  - Analiz için Kullanılabilecek Araçlar

- **Ek**
  - *ADS*
  - *File Signature*
  - *File Carving*
  - *Windows Sistem Processleri*

- **Adli Bilişim İncelemelerinde Raporlama**
  - Zaman Çizelgesi Oluşturmanın Önemi
  - Olay Müdahalesi Sürecinde Kullanılabilecek Araçlar

- **Demo: Öğrenciler tarafından canlı bir sistem üzerinde ilk Adli müdahale yapılıp deliller toplanacak ve olay müdahalesi süreçleri gerçekleştirilecek.**

- **Mobil Cihaz İnceleme Yöntemleri**
  - *Android Forensics*
  - *Android Mimarisi*
  - *Donanımsal Bileşenler*
  - *Santoku Distro Kullanımı*
  - *Android Cihazlarda Dosya Sistemi*
  - *APK Dosyaları*
  - *Android Cihazlarda Fiziksel İmaj Alma*
  - *Ekran Kilidi Bypass Teknikleri*
  - *Uygulama*

www.adeo.com.tr