



iSMMMOAkademi



ADLİ BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

ADLI BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

EĞİTİMİN AMACI

- İnceleme ve Soruşturmalarda görev yapacak olanların adli bilişim konseptini anlayarak, uygulanan iş akışlarını konseptte uygun hale getirmelerini sağlamak,
- Yapılabilecek hatalardan veya çeşitli sebeplerden doğabilecek veri kayıplarını önlemek,
- Hukuki yükümlülükleri dikkate alarak ve en uygun iş süreçlerini takip ederek soruşturma sürecinin en kısa sürede tamamlanmasını sağlamak,
- Soruşturmacıların, teknik işleri ve bu işleri yapan ekibin kabiliyetlerini anlayarak talep edebilecekleri verileri daha doğru ve uygun şekilde sağlamak, ayrıca teknik limitleri öğrenerek kendilerine sunulan raporları daha iyi yorumlamak,
- Uygulamalı olarak verilecek eğitimle, katılımcıların adli bilişim süreci hakkında bilgi edinmelerini sağlamak ve teknik bilgilerini geliştirmek,
- Bilgisayar incelemesinde kullanılacak yazılım programlarının kullanımını öğrenmek.

ADLI BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

EĞİTİM SÜRESİ VE EĞİTİM GÜNLERİ

- Toplam 84 Saat
- Cumartesi / Pazar (10.00-17.00)

EĞİTİM PROGRAMI BEDELİ

1.500 + KDV (%18)

EĞİTİM PROGRAMINA KATILIM ŞARTLARI

Minimum orta düzey Bilgisayar Bilgisi ve Kullanımı

ADLİ BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

EĞİTİM PROGRAMINA KİMLER KATILABİLİR?

- Denetim ve Riskten Sorumlu Yönetim Kurulu Üyeleri ve Üst Yönetim
- Denetim Komitesi
- Teftiş Kurulu
- İç Denetim
- Risk Yönetimi
- İç Kontrol
- IT Denetim
- IT Güvenlik
- Fraud Yönetimi
- Mali İşler ve Hukuk
- Sahtecilik ve Suistimal Önleme Personelleri
- Sistem Yöneticileri, Ağ Yöneticileri ve Operatörleri
- Bilgi Güvenliği Uzmanları
- Adli Bilişim Uzmanları
- Bilişim Hukuku Alanında Çalışanlar (Avukatlar vb.)
- Risk Yönetimi personelleri
- Akademisyenler
- Kariyerine Bu Alanda Devam Etmek İsteyen Lisansını Tamamlamış Kişiler ve/veya Son Sınıf Öğrencileri
- YMM ve SMMM ler.

ADLI BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

PROGRAMDA YER ALAN EĞİTİM KONULARI

- Digital Forensic Nedir? (Teorik)
- Computer Forensic Nedir? (Teorik)
 - o Genel Terminoloji
- Bilgisayar incelemesi ile hedeflenenler (Teorik)
 - o Soruşturmacı için veri kaynakları
- Kullanıcı bilgisayarı
- Çevresel donanımlar
- Bilgisayar ağı uç noktaları
- Network trafiği ve logları
- Uygulama erişim logları
- İnternet trafiği ve logları
- Uygulanan iş akışları (Teorik)
 - o Forensic Konsepti
- İş emiri
- Analiz
- Rapor
- Bilgisayar nasıl çalışır (Teorik)
 - o Hardisk yapısı ve terminolojisi
 - o Binary ve hexadecimal data
 - o Temel text encoding
 - o Cmosi, Bios ve Boot volume
 - o Binary ve Hexadecimal verilerin yorumlanması
 - o Bilgisayar bootup
- Computer Forensic Laboratuvar Şartları
- İmaj alma ve İmaj yapıları (Teorik)
 - o Yazma koruma yazılım-donanımları
 - o Yazılım ile İmaj alma
 - o Donanımlar ile İmaj alma
 - o Tutanak
- İnceleme yazılımları (Teorik)
 - o FTK
 - o Encase
 - o Helix
 - o X-ways
 - o Registry Analiz Uygulamaları
 - o Sifre Kurtarma yazılım-Donanımları
 - o Veri kurtama yazılım-Donanımları
- Dosya Sistemleri (Teorik)
- Dosya Sistemi Nedir?
 - o FAT
 - o NTFS
 - o EXT
 - o HSF
- İleri Dosya Sistemleri (Teorik + Uygulamalı)
 - o FAT Dosya Sistemi
- FAT Dosya Sistemi Versiyonları

ADLİ BİLGİSAYAR İNCELEME UZMANLIĞI PROGRAMI

- Dosya Kayıt Yapısı
- Dosya Oluşturma
- Dosya Silme
 - o NTFS Dosya Sistemi
- Sistem Dosyaları
- MFT Kayıtları
- Dosya Silme ve kayıt yapısı
- İmaj Alma (Uygulamalı)
 - o İmaj Dosyası nedir
 - o Yazma koruma kullanımı
 - o İmaj alma yazılımları
 - o İmaj alma donanımları
 - o FTK imager (İmaj alma yazılımı) kullanımı ve özellikleri
- Veri Bütünlüğünün Korunması (Teorik-Uygulamalı)
 - o Hash algoritmaları
 - o İmaj dosyası için hash hesabı
 - o Diğer dosya türleri için hash hesabı
 - o Raw İmaj dosya yapısı
 - o Encase İmaj dosya yapısı
- USB bellek Analizi (Uygulamalı)
- Hard Disk analizi -1 (Uygulamalı)
 - o Dosya Türleri
 - o Signiture Analizi
 - o Hash Analizi
 - o Anahtar Sözcük arama
- Windows sistemlerde incele -1 (Uygulamalı)
 - o Registry yapısı
 - o Registry analiz uygulamaları
 - o Registry Dosyaları ve Analizi
- Hard Disk analizi -2 (Uygulamalı)
 - o Veri Kurtarma
 - o Regular Expressions
 - o Filtre oluşturma ve filtre kullanımı
- Windows sistemlerde incele -2 (Uygulamalı)
 - o Kullanıcı Bilgileri
 - o Sistem klasörleri
 - o Compound dosyalar
 - o Thumb.db dosyaları
 - o Windows Restore dosyaları
 - o Link Dosyaları
 - o Email ve İnternet geçmişi
- Windows sistemlerde incele -3 (Uygulamalı)
 - o Windows tabanlı işletim sistemleri
- Windows 95-98,2000,NT, XP, Vista,7
- Windows sistemlerde incele -4 (Uygulamalı)
 - o Metadata Analizi
- Şifre Kurtarma Uygulamaları
- Rapor hazırlama



Emre SEZER

Forensic People

Forensic Servis ve Teknik Departman Sorumlusu

Emre Sezer, bilgisayar inceleme ve telefon inceleme konularında Türkiye'deki en deneyimli analizci ve eğitmenlerden biridir. Şu anda Forensic People firmasının Teknik departman ve Forensic Servis departman sorumlusudur. Son üç yılda bir çok ülkede eğitim, teknik destek ve laboratuvar kurulum projesini tamamlamıştır.

Kosova, Pakistan, Birleşik Arap Emirlikleri, Suudi Arabistan; eğitim ve teknik destek vermek için ziyaret ettiği ülkelerden bazılarıdır. Türkiye'de birçok devlet kurumu ve finansal sektör çalışanına bilgisayar inceleme eğitimi vermiştir. Türkiye'de çok saygın kurumların yanısıra, son olarak EULEX (Avrupa Birliği Polisi) ve Pakistan İçişleri Bakanlığı'na bağlı kurumların teknik uzmanlarına eğitimler vermiştir.

Emre Sezer; bilgisayar inceleme, telefon inceleme, network analizi, kablosuz ağ analizi, steganografi, video analizi, şifre kurtarma ve veri kurtarma konularında tecrübe sahibidir. ACE (Access Data Certified Examiner) sertifikasına sahiptir ve Türkiye'deki tek Access Data ve Encase sertifikalı eğitmenidir.

2002 yılında İstanbul Teknik Üniversitesi'nde, Bilgisayar Mühendisliği eğitimine başlamış; 2007 yılında bankalara kredi kartı ödeme sistemlerinde çözüm sağlayan bir yazılım şirketinde görev almıştır. 2008 yılında Forensic People firmasına katılmış ve üç yıllık dönemde Türkiye ve çevre ülkelerde birçok kamu kurumu ve özel sektör projesini tamamlamıştır.



Eğitimiyle
FARK YARATIR

www.ismmmoakademi.com.tr

info@ismmmoakademi.com.tr

Gayrettepe Mah. Yıldızposta Cad. No:48 Dedeman İş Hanı Kat:3 Beşiktaş Telefon: (212) 274 42 22, (212) 274 35 39