F401 Triyaj ve Analiz

Süre 5 gün Başlangıç, Orta ve İleri Seviye

Herhangi bir soruşturmanın ilk adımı adli bilişimde de olduğu gibi delillerin toplanmasıdır. Adli bilişimde kullanılan deliller ise verilerden oluşmaktadır, veriler çok farklı biçimlerde ve yerlerde karşımıza çıkabilir. Öncelikle gereksinim duyabileceğimiz verileri tanımlayabilmemiz, bu verilerin nerede bulunduğunu belirleyebilmemiz ve toplamak için bir plan ve prosedür oluşturmamız gereklidir. Adli bilişimde genellikle delilleri toplamak için sadece bir tek şansımız vardır. Delillerin uygun biçimde toplanmaması yalnızca soruşturmaya zarar vermekle kalmaz, delil olarak kullanılabilecek verilerin yok olmasına da neden olabilir. Günümüzdeki farklı depolama teknolojilerinin hepsi için standartlaştırılmış tek bir delil toplama yöntemi ne yazık ki mevcut değildir, incelemeciler sadece tek bir sabit sürücünün imajı üzerinden inceleme yaparak sonuca ulaşamamaktadır. Şüpheliler gün içerisinde masaüstü ve dizüstü bilgisayarları, tabletleri ve cep telefonlarını kullanmaktadır. Ek olarak, bulut depolama ve çeşitli servis sağlayıcılara ait uygulamaların artan kullanımı ile tüm bu alanlardan verilerin uygun şekilde toplanması oldukça zorlaşmaktadır. Bu eğitim ilk müdahale ekiplerine ve adli incelemecilere çok çeşitli veri depolama cihazları içerisindeki delilleri tanımlamak, toplamak ve korumak için gerekli becerileri geliştirmek üzere oluşturulmuştur. Eğitim içerisindeki pratik uygulamalarla sabit sürücülerden taşınabilir sürücülere, cep telefonlarından ağ depolama birimlerine kadar birçok farklı senaryo içerisinde verileri elde etme ve analiz süreçleri üzerinde çalışılacaktır.

MODÜL 1 Veriler, dosya sistemleri, delil dosyaları, hızlı veri toplama, olay yeri yönetimi	MODÜL 6 Geleneksel Olmayan İmaj Alma Yöntemleri, Bulut Verileri, Uzaktan İmaj Alma, Çoklu Sürücülü Depolama Aygıtları ve Ağ Üzerinden İmaj Alma
MODÜL 2 İmaj Alma ve Delil Toplama	MODÜL 7 IoT, Apple Cihaz İmajı, Çevrimiçi Tanımlama
MODÜL 3 Delilleri Ekleme, Triyaj, RAM ve Canlı Veri Toplama	MODÜL 8 Veri Kazıma ve Tekrar Oluşturma, Veri Kurtarma