F302 Uçucu Veriler ve RAM Adli Bilişim Eğitimi

Süre 3 gün Başlangıç ve Orta Seviye

Uçucu veriler ve bellek (RAM) incelemeleri adli bilişim içerisinde belki de en ilginç alandır. Bir işletim sistemi veya uygulama tarafından gerçekleştirilen her işlem bilgisayar RAM biriminde belirli değişiklikler oluşturur ve bu durum genellikle işlemden uzun süre sonra da devam eder. Bellek adli incelemeleri sistemin durumu, hangi işlemlerin çalıştığı, açık ağ bağlantıları ve yakın zamanda yürütülen komutlar gibi önemli bilgiler için kapsamlı bir kaynak sağlar. Bu kalıntıları incelenen sistemden tamamen bağımsız bir şekilde araştırabilir, böylece kötü amaçlı yazılımların veya rootkit'lerin elde edilecek sonuçlara müdahale etme olasılığını azaltabiliriz. Disk şifreleme anahtarları, bellekte yerleşik olarak eklenen kod parçaları, kayıt dışı sohbet iletileri, şifrelenmemiş e-posta iletileri ve önbelleğe alınamayan Internet geçmişi kayıtları gibi kritik veriler genellikle yalnızca bellekte bulunur. Bu eğitim ile bilgisayar bellek imajının nasıl alınacağını ve içerik profilini çıkarmayı öğrenerek; ilk müdahale, kötü amaçlı yazılım analizi ve adli bilişim konularında çok yararlı bilgiler edineceksiniz. Sabit sürücülerin ve ağ paketlerinin incelenmesi bizlere birçok önemli kanıt sunabilse de zararlı bir yazılımın bulaşması veya bir saldırı olayının öncesinde, anında ve sonrasında neler olduğunu belirlemek için gerekli birçok bilgi RAM içeriğinde yer almaktadır.

MODÜL 1 Giriş	MODÜL 3 Linux OS RAM İncelemeleri
MODÜL 2 Windows OS RAM İncelemeleri	MODÜL 4 Mac OS RAM İncelemeleri