Adli Bilişim (Digital Forensic)

Bilişim Suçu Türleri Nelerdir?

Bilgisayar Sistemlerine ve Servislerine yetkisiz erişim
Bilgisayar sabotajı
Bilgisayar yoluyla dolandırıcılık ve sahtecilik
Bir bilgisayar yazılımının izinsiz kullanımı
Kişisel Verilerin Kötüye Kullanılması
Sahte Kimlik Oluşturma ve Kimlik Taklidi
Yasa Dışı Yayınlar
Ticari Sırların Çalınması
Terörist Faaliyetler
Çocuk Pornografisi

Bilişim Suçlarında Suçlu Tipleri Nelerdir?

Hacker, Cracker, Lamer, Script-Kid, Meraklılar

Suçlu Profilleri

Hedefli ve Bilinçli Saldırgan
Hedefsiz ama Bilinçli Saldırgan
Hedefli ama Bilinçsiz Saldırgan
Hedefsiz ve Bilinçsiz Saldırgan

Dijital Deliller Nelerdir?

Hard Disk, CD, DVD, Disket, USB, Hafıza Kartları (SD,MMS,CF), Kamera, Fotoğraf Makinesi, El Bilgisayarı (PDA), Cep Telefonları, Oyun Konsolları, Akıllı TV, Bazı yazıcı ve faks cihazları, Network cihazları (Hafızası mevcut ise), Network Ortamlarda (Akışkan Delil)

Adli Bilişim (Forensic) Nedir?

Bir olayın aydınlatılmasına yönelik olarak, olayla ilgili bilgi içerebilecek bilişim cihazlarının incelenmesi.

Olaya İlk Müdahale, Nelere Dikkat Edilmelidir?

Sistem izole edilmelidir.
Bilgisayar üzerinde bulunan canlı ve geçici verileri nedeniyle kapatılmamalıdır.
Veriler düzgün şekilde kopyalanmalı ve sonunda hash değerleri karşılaştırılmalıdır.

Yapılan işlemler kayıt altına tutulmalıdır. Sorumluluk almamak adına bunlar kanıtlanmalıdır.
Olay yeri koruma altına alınmalıdır. Sadece yetkili kişiler içeri girmelidir.
Olay yerinde değişiklik yapmadan önce video ve fotoğraf alınmalıdır.
Dijital deliller alınmadan önce cihazlarda parmak izi alınması gerekiyorsa öncelik diğer ekiplere atanmalıdır.
Dijital deliller etiketlenmeli ve üzerine detaylı açıklamalar eklenmelidir.
Karmaşık parolalar için olası tüm credential bilgileri alınmalıdır.
Anti forensic sistemlerin cihazlar üzerinde aktif olabileceği unutulmamalıdır.
Dijital delil içeren cihazların konumuna yakın yerler de araştırılmalıdır.

Dijital Delil Nedir?

Delillerin bulgu olabilmesi için;
Akla uygunluk, kabul edilebilirlik, gerçeklik, tam ve eksiksiz olması, güvenilirlik, inanılabilirlik, tekrar edilebilirlik.

Hukukta Adli Bilişim

5237 sayılı TCK göre: (ONUNCU BÖLÜM - Bilişim Alanında Suçlar)
*Madde 243, 244, 245, 246
https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf
5271 sayılı TCK göre: (DÖRDÜNCÜ BÖLÜM - Arama ve Elkoyma)
*Madde 134
https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf

Adli Bilişim Görevlileri Neler Yapar?

Veri kurtarma; yazılım tabanlı kurtarma, dosya kurtarma, klasör ve format kurtarma, bölüm kurtarma (partition), donanım tabanlı kurtarma
Veri imha etme, veri dönüştürme, veri saklama, şifre kırma, ilk müdahale, bilgisayar ağ incelemeleri

Bilgisayarda yapılan adli bilişim işlemleri;

Elektronik delillerin muhafazası
Elektronik delillerin incelenmesi ve raporlanması
İlgili dosyaya erişim, oluşturma ve son yazma sürelerinin belirlenmesi
İnternet gezgininden hangi sitelere hangi zamanlarda bağlanıldığının tespit edilmesi
İnternetten hangi dosyaların indirildiğinin/download edildiğinin tespit edilmesi
Uzantısı değiştirilen dosyaların orijinal halinin belirlenmesi
Silinen dosyaların, klasörlerin ve bölümlerin geri getirilmesi

Forensic Araçları Nelerdir?

Dağıtımlar:

- Bitscout - LiveCD/LiveUSB olarak kullanılan adli bilişim analizi
- Deft - Adli Bilişim Analizi için kullanılan Linux Dağıtımı
- SANS Investigative Forensics Toolkit (sift) - Adli Bilişim Analizi için kullanılan Linux Dağıtımı

Paketler:

- Dff - Adli Bilişim Paketi
- IntelMQ - Güvenlik özetlerini toplayan ve işleyen bir paket
- Laika BOSS - Nesne tarayıcı ve saldırı tespit sistemi
- PowerForensics - Canlı disk analizi için kullanılan bir paket
- The Sleuth Kit - Düşük seviyeli adli analiz aracı
- Turbinia - Bulut platformlarında dli iş yüklerinin dağıtımı, yönetimi ve çalıştırılması için açık kaynaklı bir paket

Canlı Adli Analiz:

- Grr - Google Rapid Response: Sunucu/İstemci mimarisinde çalışan uzaktan canlı adli analiz aracı
- Linux Expl0rer - Python & Flask'ta yazılan Linux uç birimi için kullanımı kolay canlı adli araç
- Mig - Bulut hızında dağıtılmış ve gerçek zamanlı dijital adli analiz aracı
- Osquery - Facebook tarafından geliştirilen SQL destekli işletim sistemi analizi

İmaj Alma/Görüntüleme:

- Dd - I/O aygıtlarının veya diskin bir bölümünün veya dosyanın imajını almak için kullanılan adli analiz aracı
- Dc3dd - Geliştirilmiş dd sürümü
- Dcfldd - dd'nin farklı geliştirilmiş sürümü
- FTK Imager - Windows için ücretsiz imaj alma aracı
- Guymager - Linux sistemlerde açık kaynak kodlu imaj alma aracı

Bellek Adli analiz:

- InVtero.net - .NET'te geliştirilen yüksek hızlı bellek analizi paketi, tüm Windows x64'ü destekler, kod bütünlüğünü ve yazma desteğini içerir.
- KeeFarce - Hafızadan KeePass şifrelerini ayıklar.

- Rekall - 2013 yılında Volatilite'den ayrılan bellek analiz paketi
- Volatility - İleri bellek adli analiz paketi
- VolUtility - Volatilite paketi için web uygulaması
- BlackLight - Hiberfil, pagefile, raw bellek analizini destekleyen Windows / MacOS sistemler için adli analiz aracı
- DAMM - Volatilite üzerine kurulu Bellekte Kötü Amaçlı Yazılımların Diferansiyel Analizi
- Evolve - Volatilite uygulaması için Web arayüzü
- FindAES - Bellekte AES şifreleme anahtarlarını bulma
- Muninn - Volatilite kullanılarak analiz bölümlerini otomatikleştirmek ve okunabilir bir rapor oluşturmak için bir komut dosyası (https://github.com/ytisf/muninn)
- TotalRecall - Çeşitli kötü amaçlı yazılım analiz görevlerini otomatikleştirmek için Volatiliteye dayalı script
- VolDiff - Kötü amaçlı yazılım çalıştırmadan önce ve sonra bellek görüntülerinde Volatilite çalıştırın ve değişiklikleri inceleyin
- WDBGARK - WinDBG Anti-RootKit Uzantısı
- WinDbg - Windows sistemleri için canlı bellek denetimi ve çekirdek hata ayıklama

Volatility

Volatility -> imageinfo (işletim sistemi bilgisini edinmek için)
-> pslist (process list)
-> dllist (dll list)
-> cmdscan (cmd commands all)
-> notepad
-> iehistory
-> psscan (kapatılmış veya kendini gizleyebilen işlemleri listeler)
-> --profile (işletim sistemini de vermek) (daha hızlı)
-> connections (bağlı olduğu ipler)
-> connscan (daha önce bağlantı kurulmuş ipler)
-> hashdump

Haftalık Forensic Gelişmeleri için;

Thisweekin4n6.com
Forensicfocus.com