KPMG Türkiye Adli İmaj Alımı & Delil Toplama Süreçleri El Kitapçığı

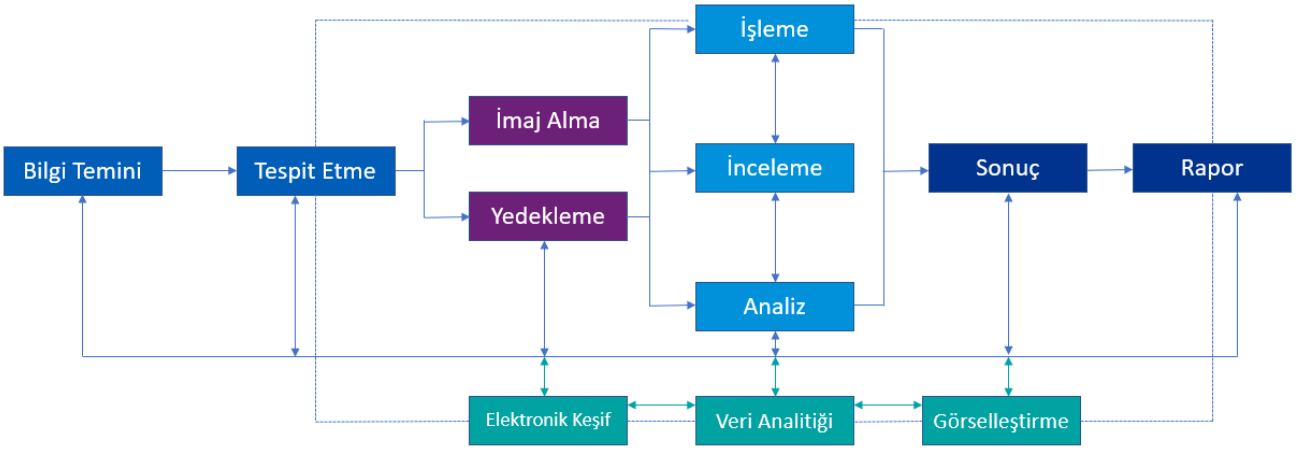
Usulsüzlük Önleme, İnceleme, Ticari Uyuşmazlık ve Uyum Hizmetleri – Adli Bilişim Departmanı

KPMG Türkiye

kpmg.com/tr

Şeffaf Adli Bilişim ve Elektronik Keşif Yaklaşımımız

Adli Bilişim Departmanı olarak şeffaf bir çalışma metodolojisine sahibiz. Cihazın teslim alınmasından itibaren imaj çalışmalarının gerçekleştirilmesi ve verilerin analizine kadar tüm adli bilişim süreçlerine ilişkin hizmet vermekteyiz. Metodolojimizin daha iyi anlaşılabilmesi adına, gerçekleştirdiğimiz çalışma adımlarını kısaca özetleyen şemayı aşağıda yer almakta, çalışma adımlarımız ise ilerleyen kısımlarda açıklanmaktadır.



Adım 1: Bilgi ve Cihaz Temini

Cihazların Tutanak İle Teslim Alınması

Cihazın teslimi esnasında bir teslim tesellüm belgesi düzenlenir. Bu belge içerisinde cihazın üreticisi, cihazın modeli gibi teknik özellikler ile birlikte teslim eden ve teslim alan kişilerce, cihazın teslim esnasındaki durumunu da gösterir şekilde imzalanarak tutanak altında alınır. Cihaz üzerindeki incelemelerin sona ermesi neticesinde yine tutanak altına alınarak karşı tarafa teslim edilir. Bu aşamada düzenlenen ve doldurulan tutanaklar aşağıdaki gibidir:

Delil Zinciri Tutanağı: Cihazın kimin tarafından teslim alındığı bu form içerisinde belirtilir ve taraflarca imzalanır. Böylelikle yapılan işlemler sırasında cihazın sahipliğinin kimde olduğu kayıt altına alınır.

Muvafakatname: Cihazı teslim eden personelin, rızasının yer aldığı imzalı dokümandır. Bu tutanağı doldurarak ilgili kişi, cihazının içerisinde inceleme gerçekleştirilmesine müsaade eder.

Not: Cihazı teslim eden personelin özellikle muvafakatnameye imza atması, cihaz üzerinde gerçekleştirilen incelemelerin hukuka uygunluğunun belgelenebilmesi adına önemlidir. Aksi halde, rızasız şekilde temin edilen cihazlar hukuk sürecinde şirket ve inceleyen taraflar adına zor durumları beraberinde getirebilir.

Cihazların Teslim Esnasındaki Durumu

İnceleme gerçekleştirilecek cihaz, talep edildiği durumda sahibi tarafından şirkete veya KPMG

yetkililerine açık durumda ve uçak moduna alınmış biçimde, mümkün mertebe SIM kartı ile birlikte teslim edilmelidir. Cihazın ekran parolasının ve SIM kart alındı ise SIM kart şifresinin şirket tarafından temin edilmiş olması gerekir. Eğer inceleme gerçekleştirilecek cihaz bir bilgisayar ise, bu bilgisayarın mevcut ise Bitlocker şifresinin ve Windows kullanıcı şifresinin yine kullanıcıdan veya ilgili IT biriminden temin edilmesi gerekmektedir.

Not: Bu bilgiler eğer mevcut değilse, KPMG Adli Bilişim Departmanı tarafından cihazın teslimi esnasında personelin rızası olmak koşulu ile kendisinden talep edilebilir. Bu verilerin mevcudiyeti, cihazdan elde edilecek verilerin niteliğine ilişkin önem arz etmektedir. Ekran kilidi ve SIM kart gibi verilerin mevcut olmaması, cihazdan elde edilecek verileri kısıtlar, hatta temin edilmesi imkansız hale getirebilir.

Adım 2: İmaj Alım ve Keşif Çalışmaları

Kanıt Bütünlüğü

Adli Bilişim Departmanı olarak imaj alım sırasında veri bütünlüğünün korunması her zaman ilk önceliğimiz olmaktadır. Bu sebeple imajı alınan cihazların içerisine herhangi bir yazılım kurulmaz ve cihaz içeriğinde yer alan herhangi bir veri kaybedilmez. Ayrıca imaj çalışmalarımız esnasında cihazları garanti kapsamından çıkaracak ve içerisindeki verinin güvenilirliğini etkileyebilecek metotlar tarafımızca kullanılmaz. Bu sayede imaj alım sonucunda elde edilecek veriler, kanıt olma özelliklerini korur.

Hash Değeri: Çalışmalara başlamadan önce eldeki dosyalar veya tüm disk içerisindeki veriler belirli bir matematiksel fonksiyondan geçirilerek 32 karakterlik bir dizi haline indirgenir. Bu dizi, taklit edilmesi neredeyse olanaksız bir veriyi ifade eder. Bu işleme “Hash Verification” adı verilir.

Not: Özellikle bilgisayarlardan elde edilen verilerde Hash Verification işleminin yapılması ve çıkan hash kodunun bir kopyasının kaydedilmesi önem arz etmektedir. Bu veri, adli makamlarca kanıt bütünlüğünün sağlandığı anlamına gelmektedir.

İmaj Alım Çalışmalarının Kayıt Altına Alınması

Cihaz üzerinde gerçekleştirilen çalışmalar, imaj alım formu içerisine işlenir. Bu form içerisinde başlıca aşağıdaki bilgiler kaydedilmektedir:

- Cihaz sahibi bilgileri,
- Cihaz bilgileri,
- Parola ve diğer çeşitli şifreler,
- İmaj alım yöntemi,
- Hash değeri,
- İmaj alım esnasında kullanılan yazılımlar ve teknolojiler,
- İmajın başarılı şekilde alınıp alınmadığı,
- Çalışmanın gerçekleştiği tarih bilgileri ve diğer pek çok bilgi

İmaj Alım Yöntemleri

İmaj alım süreci, imaj alımında kullanılacak yazılımın ve metotların belirlenmesi ile başlar. Cihazların şifrelenmiş durumda olup olmaması, şirket politika ve prosedürleri, düzenleyici yasalar ve imaj alım talebinde

bulunan iş ortağının çıktılardan beklentisi doğrultusunda kullanılacak yazılım ve metotlar farklılık gösterir.

Mobil cihazlar, tabletler, şirket bilgisayarları, yazıcılar, fotoğraf makineleri ve drone kameralar gibi içerisinde herhangi bir depolama aygıtı bulunan pek çok cihazın imajı alınabilir. Adli Bilişim Departmanı olarak birden farklı imaj alım yazılımı ve yardımcı ekipmanları kullanarak cihazların teknik altyapısına ve üretildikleri yılın teknolojisine göre farklı metotlar kullanılarak imaj alım sürecinin yol haritası ve uygun yazılımlar belirlenir.

Masaüstü ve Laptop Bilgisayarlar: Masaüstü ve laptop bilgisayarlardan 2 farklı metot aracılığı ile imaj alımı gerçekleştirilebilir. Bunlar kısaca aşağıdaki şekilde sınıflandırılabilir:

Fiziksel İmaj Alımı: Bu yöntemde bilgisayar sökülerek içerisindeki diskler bilgisayardan bağımsız şekilde, diskin üzerine yazmayı önleyici donanımlar aracılığı ile cihaz dışında imaj alma şeklinde uygulanır. Özellikle personelin bilgisayarından oturum açılmadan imaj alımı çalışmaları gerçekleştirilmesi talep edildiğinde veya şirket prosedürleri gereği USB portları kapalı durumda olduğu zaman bu yöntem tercih edilir.

Canlı İmaj Alımı: Cihazın sökülmesinin tercih edilmediği durumlarda bu yöntem tercih edilebilir. Burada disk üzerine veya RAM'e yazma durumları söz konusu olabilir. Bu durumdan kaçınmak adına mümkün mertebe alternatif Linux işletim sistemleri kullanılması önerilmektedir.

Not: Silinen verilerin geri getirilmesi, sıklıkla merak edilen konulardan biridir. Masaüstü ve laptop bilgisayarlarda silinen verinin geri getirilmesi, diskin türüne ve diskin kullanım şekline göre değişiklik gösterir. Özellikle HDD (Hard Disk Drive) disklerden, SSD (Solid State Drive) disklere göre daha fazla silinmiş veri kurtarılabilmektedir.

Mobil Cihazlar ve Tabletler: Mobil cihazlar ve tabletler üzerinde izlenecek yöntemler, cihazın donanımsal özelliklerine, üreticisine ve işletim sistemine göre değişiklik gösterir. Burada da yine yukarıda belirtilen şekilde 2 ana imaj alım metotu bulunsa da, bunlar kendi içerisinde farklı şekillerde detaylanır ve alt yöntemlere ayrılır. Bu yöntemlere ve detaylarına ilişkin bizlerle iletişime geçebilirsiniz.

Alternatif Yöntem; Cloud Extraction: İhtiyaç duyulması halinde, daha hızlı bir yöntem olarak çeşitli ulut tabanlı yöntemler aracılığı ile Whatsapp yazışmaları da temin edilebilir. Buradan temin edilecek veriler, direkt olarak incelemeye müsait şekilde liste olarak çıkartılabilmektedir.

Not: Mobil cihazlar özelinde de silinen verilerin geri getirilebilirliği çokça merak edilmektedir. Mobil cihazlarda silinen verilerin geri getirilmesi pek mümkün olmamakla birlikte, bir cihazın sıfırlandığına veya tesliminden önce hangi uygulamaların yüklü olduğu gibi veriler elde edilebilmektedir. Ayrıca cihazın root'lu, yani üst düzey erişime açık olması, elde edilecek verinin boyutunun artmasını sağlar.

Elde Edilen Veri Türleri

İmaj alım sürecinin sonucunda cihazlar içerisindeki e-posta yazışmaları, Whatsapp ve diğer chat uygulamaları yazışmaları, kısa mesajlar, fotoğraflar üzerindeki geo-lokasyon, tarih, saat bilgileri, uygulamaların içerikleri, uygulamaların bulut servisler üzerinde yedeklenen kopyalarında yer alan bilgiler, arama yapılan ve cihaza gelen aramaların listesi, bağlanılan bluetooth cihazları ve bağlanılan tarih/saat bilgisi, cihazın bağlandığı wi-fi ağları ve bu ağların geo-lokasyon bilgileri vb. gibi birçok çıktı elde edilebilmektedir.

Not: Kullanılacak imaj alım türüne göre elde edilecek veri türleri ve veri boyutları değişkenlik göstermektedir. Örneğin Cloud Extraction yöntemi kullanıldığı takdirde, elde edilen veriler Cloud içerisinde depolanabilen veriler sınırlı kalmaktadır.

Sızan Verilerin Tespiti

İmaj alım neticesinde cihaza göre değişkenlik göstermekle birlikte veri sızıntısına ilişkin bilgiler elde edilebilir. Özellikle Windows işletim sistemine sahip cihazlar, en son bağlanan donanım bileşenlerini ve erişilen dokümanları tespit etmeye yarayacak farklı sistem dosyaları içerir. Bu verilerin analizi ile sızan verilere ve verinin aktarıldığı cihazlara ilişkin analiz gerçekleştirmek mümkün hale gelmektedir.

Not: Bazı analizlerin gerçekleştirilebilmesi için çeşitli loglama tercihlerinin IT birimleri tarafından açılmış olması gerekmektedir. Örneğin olay günlükleri ekranında yer alan “Enable Logging” seçeneği işaretlenmediği zaman cihaza takılan harici diskler gibi veri depolama aygıtlarına yönelik bilgiler sınırlı hale gelmektedir.

Adım 3: Analiz, Raporlama ve Verilerin Muhafaza Edilmesi

Çevrimdışı Sunucular

Cihazların imaj alım süreçleri tamamlandıktan sonra elde edilen bulguların incelenmesi sürecine geçilir. Ekibimiz, bulguları istenilen anahtar kelimeler ve belirlenen dosya türleri üzerinden sınıflandırmalar yaparak inceleme gerçekleştirir. Ayrıca veriler üzerinde kullandığımız yapay zekâ algoritmaları, birbirinden bağımsız türlerdeki bulguları bir araya getirerek zaman örgüsü içerisinde birleştirebilir ve aralarında var ise anlamlı bağlantıları gösterebilir. Tüm bu çalışmalar çevrimdışı sunucular üzerinde gerçekleştirilir, veri güvenliği en üst düzeyde sağlanmış olur.

Verilerin Muhafaza Edilmesi

Elde edilen veriler, şifrelenmiş depolama aygıtları içerisinde yedeklenerek saklanır ve erişimin özel tanımlı kartlar ile kısıtlı olduğu laboratuvarımızda yedeklenerek muhafaza edilir. Verilerin ve cihazların süreç içerisinde itina ile korunması adına laboratuvarın kendine ait iklimlendirmesi bulunur ve içerideki sıcaklık, nem oranı gibi değerler belirli aralıklarda tutularak kontrol edilir. Bu sayede veriler herhangi bir hasara uğramadan muhafaza edilir.

Not: Verilerin saklanma süresi yasalar çerçevesinde değişkenlik göstermektedir. Müşterinin talebi doğrultusunda elde edilen veriler imha edilebilir. Ancak, hukuki süreçlerin devam ettiği ve bu verilere tekrar ihtiyaç duyulabileceği unutulmamalıdır.

Sonuç ve Raporlama

İş ortağının talep ettiği durumlarda kendi iç birimlerinin incelemesi için PDF, Excel, Html, Loadfile ve daha birçok formatta istenilen bulgular özelinde raporlar üretilebilir. Müşterinin talebine veya ihtiyaca yönelik raporlar veya memorandum olarak da bilinen kısa bilgilendirme notları hazırlanır.

İletişim

Oytun Önder

Danışmanlık Hizmetleri
Usulsüzlük Önleme, İnceleme,
Ticari Uyuşmazlık ve Uyum Danışmanlığı
Şirket Ortağı
oonder@kpmg.com

Batuhan Tellioğlu

Danışmanlık Hizmetleri
Usulsüzlük Önleme, İnceleme,
Ticari Uyuşmazlık ve Uyum Danışmanlığı
Direktör
btellioglu@kpmg.com

İlter Lofçalı

Danışmanlık Hizmetleri
Usulsüzlük Önleme, İnceleme,
Ticari Uyuşmazlık ve Uyum Danışmanlığı
Müdür
ilofcali@kpmg.com