**Table of Contents**

[1. AMAÇ 1](#__RefHeading___Toc118_1789639072)

[2. KAPSAM 1](#__RefHeading___Toc120_1789639072)

[3. TANIMLAR 1](#__RefHeading___Toc122_1789639072)

[4. ROL VE SORUMLULUKLAR 2](#__RefHeading___Toc124_1789639072)

[5. BİLİŞİM İNCELEME SÜRECİ 2](#__RefHeading___Toc126_1789639072)

[5.1. Talep ve Yetkilendirme 2](#__RefHeading___Toc128_1789639072)

[5.2. Cihazların Tanımlanması 2](#__RefHeading___Toc130_1789639072)

[5.3. Güvenli Veri Toplama ve Çıkarma 3](#__RefHeading___Toc132_1789639072)

[5.4. İnceleme ve Analiz 4](#__RefHeading___Toc134_1789639072)

[5.5. Raporlama 5](#__RefHeading___Toc136_1789639072)

[5.6. Cihaz ve Verilerin Saklanması 5](#__RefHeading___Toc138_1789639072)

## AMAÇ

Bu prosedürün amacı, Teftiş Kurulu Başkanlığı bünyesinde yürütülecek dijital kanıtların toplanması, korunması, analiz edilmesi ve belgelenmesine yönelik bilişim incelemelerinin eksiksiz, güvenli ve yasal ve düzenleyici gerekliliklere uygun şekilde yürütülmesini sağlamaktır.

## KAPSAM

İnceleme kapsamında dijital kanıtların toplanacağı dijital varlıklar dizüstü ya da masaüstü kişisel bilgisayarla sınırlandırılmıştır.

## TANIMLAR

**Obje/Artefakt:** Belirli bir olay, faaliyet veya davranış hakkında kanıt veya içgörü sağlayabilecek herhangi bir dijital bilgi veya veri parçasıdır. Dijital kanıtların kaynakları olup disk sistemleri, ağlar ve yazılım uygulamalarında çeşitli şekillerde bulunabilirler.

**Dijital kanıt:** Dijital biçimde depolanan veya iletilen her türlü bilgi veya veridir. Elektronik belgeler, e-postalar ve anlık mesajlar, dijital görüntüler ve videolar, internet geçmişi ve web günlükleri, dosya meta verileri, sistem günlükleri ve olay kayıtları, ağ trafiği ve paket yakalamaları, mobil cihaz verileri, veritabanı kayıtları, sosyal medya içeriği gibi çeşitli şekillerde olabilir.

## ROL VE SORUMLULUKLAR

**Bİ Müfettişi:** Dijital kanıtların toplanması, korunması, analiz edilmesi ve belgelenmesine yönelik bilişim incelemelerinin yürütülmesinden sorumludur.

## BİLİŞİM İNCELEME SÜRECİ

Dijital kanıtların toplanması, korunması, analiz edilmesi ve belgelenmesine yönelik bilişim incelemeleri aşağıda altı adımda yürütülür:

1. Talep ve Yetkilendirme
2. Cihazların Tanımlanması
3. Güvenli Veri Toplama ve Çıkarma
4. İnceleme ve Analiz
5. Raporlama
6. Cihaz ve Verilerin Saklanması

### Talep ve Yetkilendirme

Bilişim incelemeleri devam eden bir olay incelemesini desteklemek amacıyla yürütülür. Olayın örgü ve bağlamı bilişim incelemelerinin de ana yönünü belirleyeceğinden, talep edilen bilişim incelemesinin kapsamını, hedeflerini ve özel gerekliliklerini netleştirmek için talep sahibi ile ön görüşme düzenlenir.

### Cihazların Tanımlanması

Kullanıcılara Bankamızca tahsis edilmiş olan cihazların tanımlanabilmesi için potansiyel kanıt kaynakları ve şüphelenilen durumlara ilişkin bilgi toplanır. Gerekirse olayın niteliği, spesifik endişeler ve incelemenin istenen sonuçları ile ilgili açıklama istenebilir.

Mevcut kaynaklar, sahip olunan uzmanlıklar ve kurumsal önceliklerle uyum gibi faktörler dikkate alınarak bir süre kestirimi yapılır. Personel, ekipman ve bütçe dahil olmak üzere kaynakların mevcudiyeti belirlenir. Talebin iç kaynakların yetkinleriyle zamanında karşılanamamasının öngörülmesi durumunda dış kaynak kullanımı yoluna gidilebilir.

Cihazlar, sistemler, uygulamalar ve veri havuzları dahil olmak üzere incelemeyle ilgili potansiyel dijital kanıt kaynakları belirlenir. Veri hassasiyeti, yasal sonuçlar ve potansiyel iş etkisi gibi faktörler göz önünde bulundurarak olayın potansiyel etkisi değerlendirilir. Örneğin, incelemeye konu edilecek olan kullanıcının mevcut bir çalışan, ayrılmış bir çalışan ya da dış hizmet alınan kuruluş çalışanı olması durumu göz önünde bulundurulur. Bilgi paylaşımını ve koordinasyonu kolaylaştırmak için olaya müdahale edenler, hukuk müşavirleri, yönetim ve dış taraflar dahil olmak üzere ilgili paydaşlarla iletişim kanalları kurulur.

İncelemenin başlangıcına ilişkin kayıt oluşturmak üzere inceleme detayları, kilit paydaşlar, görevlendirilen müfettiş ve ilk değerlendirme bulguları kayıt altına alınır.

Kapsam dahilindeki tüm varlıkların tanımlanması, konumlarının, konfigürasyonlarının ve bağlantılarının belirlenebilmesi için Bankanın varlık envanter veritabanlarını kullanılır. Ayrıca diğer araç, teknik ve manuel incelemeden yararlanarak inceleme kapsamındaki dijital varlıkların listesi oluşturulur. İnceleme kapsamındaki Kullanıcılara ilgili dönemde tahsis edilmiş olan tüm cihazlar dikkate alınır.

### Güvenli Veri Toplama ve Çıkarma

Tanımlanan kapsam dahilinde dijital delilleri elde etmek için aşağıdaki adımlar izlenir:

**Bilgisayara El Koyulması**

İncelenecek varlıkların konumları Altyapı Teknoloji Bölümü’nden (ATB) öğrenilir. İncelemenin aciliyetine göre ilgili yere intikal edilmesi ya da cihazın ABM’ye kargolanması seçeneklerinden biri tercih edilir.

**Bilgisayarın Sabit Diskinin Sökülmesi ve Dijital İmajının Alınması**

Söküm işlemi bir ATB çalışanı ya da ATB tarafından dış hizmet alınan bir firma çalışanı tarafından ve en az iki müfettişin nezaret ve gözetiminde yapılır. İşlem sonucunda sevk irsaliyesinin haricinde işlemi gerçekleştiren kişinin ve işleme nezaret eden müfettişlerin imzaladığı bir tutanak düzenlenir.

Sökülen diskin imajı, söküm işleminin yapıldığı yerde, sökümün bitmesinin hemen akabinde alınır. Bunun için sökülen disk bir harici harddisk kutusuna bağlanır. Harici harddisk kutusu ise analiz bilgisayarına USB ile bağlanır. Analiz bilgisayarında kurulu olan **AccessData FTK Imager** yazılımı kullanılarak disk kutusundaki fiziksel sürücünün analiz bilgisayarının diski üzerine **RAW imajı (**dd** formatında) alınır. İşlem sonucunda fiziksel sürücü kaynağının ve alınan imajın MD5/SHA1 hash değerlerinin eşleştiği doğrulanır. İmaj alma işlemi sonucunda işlemi gerçekleştiren ve işleme nezaret eden müfettişlerin imzaladığı bir tutanak düzenlenir. Tutanağa, MD5/SHA1 hash değerleri ve söz konusu değerlerin eşleştiği hususu da eklenir.**

**İşlemin ardından fiziksel sürücü disk kutusundan ayrılır, etiketlenir, elektrostatik deşarj (ESD) riskini minimize eden antistatik bir çantaya koyulur. Doğrudan güneş ışığı almayan sıcaklığı 15-24ºC arasında değişen düşük nemli (%30-50) bir ortamda, tercihen bir kasada saklanmak üzere su geçirmez bir taşıma çantası ile taşınır.**

### İnceleme ve Analiz

İncelemeye başlamadan önce **dd** formatında alınmış olan imajın hash değeri hesaplanır ve imajın alınmasına ilişkin tutanakla karşılaştırılır.

**dd** formatında alınmış olan imaj dosyası, analiz bilgisayarında kurulu olan **Autopsy** uygulamasında başlatılan yeni vakaya veri kaynağı olarak eklenir. Eklenen imaj dosyası üzerinde, incelemenin kapsamı, hedefleri ve bilinen veya şüphelenilen göstergelerine dayalı olarak belirlenen anahtar kelimeler, kelime öbekleri ve terimlere yönelik arama yapılır. Bu kapsamda aşağıdaki objeler araştırılır.

* **Dosya objeleri:** Belgeler (Word, Excel, PowerPoint, PDF), resimler (JPEG, PNG, TIFF), arşivler (ZIP, RAR)
* **Sistem objeleri:** Olay günlükleri (Windows Olay Görüntüleyicisi, syslog), kayıt defteri girdileri (Windows Kayıt Defteri), prefetch dosyaları, sistem yapılandırma dosyaları (INI, XML).
* **Uygulama objeleri:** Tarayıcı geçmişi (Internet Explorer, Chrome), sohbet günlükleri (Jabber), e-posta mesajları (Outlook)
* **Ağ objeleri:** Güvenlik duvarı günlükleri, proxy günlükleri, DNS günlükleri, oturum günlükleri.
* **Silinmiş objeler:** Ayrılmamış disk alanında veya boş alanda, silinmiş dosyaların kalıntıları

Dosya objeleri incelenirken dosya meta verileri (zaman damgaları, dosya boyutu, dosya öznitelikleri) dikkate alınır. Spesifik bir dosyanın arandığı durumlarda aranan dosyanın hash değeri, belirli bir grup dosyanın arandığı incelemelerde ise dosyanın değiştirilme zaman aralığı, MIME tipi ya da boyutu gibi özellikleri doğrultusunda aramalar yapılır.

### Raporlama

Toplanan verilerin incelenmesi ve analizinden elde edilen tüm bulgu, gözlem ve sonuçlar raporlanır. Düzenlenecek raporda ayrıca, bilişim incelemesi kapsamında analiz edilen cihazlara yer verilir.

### Cihaz ve Verilerin Saklanması

Objelerin temin edildiği ve imajı alınarak güvenli bir ortamda saklanan diskler, inceleme raporunda kullanılan somut bir dijital kanıt barındırıp barındırmamasından bağımsız olarak asgari olarak **5 yıl** süreyle saklanır.

Soruşturma veya sonraki yasal işlemler için artık gerekli olmadığı yönünde hukuk görüşü de alınan cihaz ve verilerin imhası için Banka bünyesinde belirlenmiş imha prosedürleri izlenir.

|  |
| --- |
| ***Bilgi Riski Yönetimi Başkanlığı ile Altyapı Teknolojileri Bölümü’ne kim, ne zaman, hangi kanaldan bilgi verir?*** |

|  |
| --- |
| ***Asgari olarak ihtilaflı bir biçimde ayrılan çalışanlara tahsis edilen bilgisayarlar nasıl değiştirilmeden, bir başka çalışana tahsis edilmeden muhafaza edilecektir?***  ***Bunun için ihtilaflı olarak ayrılan çalışanın bilgisayarının teslim alınması sırasında 5.3 bölümündeki aşamaların uygulanması ve diske, imajının alınarak el koyulması yoluna gidilmelidir.*** |

|  |
| --- |
| Donanım İhtiyaçları  Analiz Bilgisayarı - Dizüstü bilgisayar 32 GB RAM, 1 TB hard disk, Windows 10 domaine tanımlanmamış, local admin yetkisi olan bir cihaz  Harici disk kutusu, 2,5 inch 3,5 inch destekleyen, USB 3.0 ve üzeri destekleyen  Antistatik çantalar  Taşıma çantası  Kasa  Tableau imaj alma donanımları yüksek maliyetleri nedeniyle (> 2.000 USD) kapsam dışında tutulmuştur.  Yazılım İhtiyaçları  **AccessData FTK Imager – ücretsiz**  **Autopsy - ücretsiz** |