Bilişim Etiği ve Hukuku

Prof. Dr. Eşref ADALI

Bilişim Hukuku

12

Bilişim Suçları-I

Avrupa Ekonomik Topluluğu bilişim suçlarını 5'e ayırmıştır:

1. Bilgisayarda bulunan bir kaynağa veya herhangi bir değere yasal olmayan biçimde ulaşarak aktarımını sağlamak için bilerek bilgisayardaki verilere ulaşmak, bunları bozmak, silmek veya yok etmek,
2. Bir sahtekârlık yapmak için bilerek bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,
3. Bilgisayar sistemlerinin çalışmasını engellemek için bilerek bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,
4. Ticari anlamda yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,
5. Bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme bilerek girip müdahalede bulunmaktır.

Bilişim Suçları-II

Bir Bilgisayar ile Gerçekleştirilen Suçlar: Bir bilgisayar ya da bir bilgi sistemini kullanarak işlenen suçlar kapsamında, Genelağ bankacılığındaki soygunlar, bilgi sistemlerini çalışamaz duruma sokan saldırılar, zararlı yazılımlar ile bilgi sistemlerine zarar verme eylemleri düşünülebilir. Geçmiş dönemlerde havacılık sistemlerine, petrol boru hatlarının sistemlerine, trafik sistemlerine yapılmış saldırılara tanık olunmuştur.

Bilgisayar veya Bir Bilgi Sistemi Üzerinde İşlenen Suçlar: Bilgi sistemine sızarak veri tabanındaki verileri çalma, değiştirme veya silme işlemi bu konuya en uygun örnektir. Bilgi sistemine yerleştirilen bomba ve mevcut yazılımlara yapılan eklemeler bu tür için diğer örneklerdir.

Bilişim Ortamında Yapılan Yayımlar ve Hizmetler ile İşlenen Suçlar: Genelağ ortamı insanlara geniş ve olabildiğince rahat bir yayım olanağı sunmaktadır. Bu özgür ortamı kullanarak yararlı yayımlar yapılabileceği gibi çok zararlı işler de yapılabilmektedir. Bu tür zararlı çalışmaların kapsamında:

- Genel ahlaka aykırı yayımlar,
- Ulusal güvenliği bozucu yayımlar,
- Yanıltıcı haberler,
- Çocuk pornografisi,
- Kumar

sayılabilir.

Bilişim Suçları ile İlgili Yasalar

- Yeni Türk Ceza Kanunu (TCK-5237):
  - Madde 243 – Bilişim Sistemine girme Suçu
  - Madde 244 – Sistemi Engelleme, Bozma, Verileri Yok Etmek veya Engellemek
  - Madde 245 – Banka veya Kredi Kartlarının Kötüye Kullanılması
  - Madde 246 – Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması
- Yeni Ceza Muhakemeleri Kanunu (CMK-5271):
  - Madde 134 – Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma
- Elektronik İmza Kanunu (5070):
  - Madde 15 – Denetim
  - Madde 16 – İzinsiz Kullanım
  - Madde 15 – Sahtecilik
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651)
- Kişisel Verilerin Korunması Kanunu (6698):

Avrupa Sanal Suçlar Sözleşmesi

- **Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanımına açık bulunmasına yönelik suçlar**
  - Yasa dışı erişim
  - Yasa dışı müdahale
  - Verilere müdahale
  - Sisteme müdahale
  - Cihazların kötüye kullanımı
- **Bilgisayarlarla ilişkili suçlar**
  - Bilgisayarlarla ilişkili sahtecilik fiilleri
  - Bilgisayarlarla ilişkili sahtekârlık fiilleri
  - İçerikle ilişkili suçlar
  - Çocuk pornografisiyle ilişkili suçlar
  - Telif haklarının ve benzer hakların ihlaline ilişkin suçlar
  - Saklanan bilgisayar verilerinin korunmasının kolaylaştırılması
  - Trafik bilgilerinin korunmasının kolaylaştırılması ve kısmen açıklanması
  - Saklanan bilgisayar verilerinin aranması ve bunlara el konulması
  - Trafik bilgilerinin gerçek zamanlı olarak toplanması
  - İçerikle ilgili bilgilere müdahale edilmesi

Bilişim Suçlarını Soruşturma ve Kovuşturma

Bilişim alanında işlenen suçların niteliği bilinen suçlardan farklı olduğu için soruşturmalarının ve kovuşturmalarının buna göre yapılması gerekir. Bilişim ile ilgili suçları diğer suçlardan farklı kılan bazı önemli hususlar:

- **Suçun işlendiği yer ile suçu işleyen aynı yerde olmayabilir**: Bilinen suç türlerinde, suçu işleyen genellikle suçun işlendiği yerde olur. Bilişim suçlarında suçlu hemen hemen hiçbir zaman suçun işlendiği yerde olmaz, hatta yakınında bile olmaz. Suçlu bir başka kentte bir başka ülkede bile olabilir.

  Bilişim suçları uluslararası nitelikte olabilmektedir. Bu nedenle uluslararası iş birliklerini gerekli kılar.
- **Soruşturmanın hızlı olması gerekir**: Bilişim suçunu işleyenler her zaman aynı yerde oturmazlar. Hatta sabit bir yerden Genelağ'a bağlanmazlar. Böylece yerlerinin bilinmemesini sağlamaya çalışırlar. Ancak belli bir süre aynı yerden, aynı IP adresini kullanarak bağlandıkları da görülmektedir. Bu nedenle bir suçluyu yakalamak için şikâyet alınır alınmaz konum bilgisinin öğrenilmesine çalışmak gerekir. Bu aşamada bilişim teknolojilerinden yararlanmak yerinde olur.
- **Kanıtlarının toplanması için özel bilgi gerektirir**: Bilişim suçunun kanıtları bilişim ortamında bulunabilecek, adına sayısal kanıt dediğimiz belge, çizelge, ses kaydı, fotoğraf, film ve değişik ortamlardaki verilerdir. Bu veriler kurallarına göre toplanmazlar ise kanıt olma niteliklerini yitirirler. Böyle bir yanlıştan en çok gerçek suçlular kazançlı çıkar.
- **Olayı ancak bilişim uzmanları değerlendirebilir**: Bilişim suçunun oluş biçimi, bıraktığı izler ve kanıtlar ancak bu konuda uzman olan bilişim uzmanları tarafından değerlendirilebilir.

Bilişim ortamındaki veriler kurallarına göre toplanmazlar ise kanıt olma niteliklerini yitirirler. Böyle bir yanlıştan en çok gerçek suçlular kazançlı çıkar.

Uluslararası Sözleşmeler-I

Türkiye'nin taraf olduğu Avrupa Sanal Suçlar Sözleşmesi'nin 19. maddesi, bilişim ortamındaki verilerin aranması ve bunlara el konulması hakkındadır . TBMM tarafından onaylanan biçim aşağıda aynen verilmiştir.

Madde 19 - Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması

1. Taraflardan her biri, kendi ülkesindeki yetkili makamların,

   a. Bir bilgisayar sisteminin tamamı veya bir kısmını ve içerisindeki depolanmış bilgisayar verilerini; ve

   b. Bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtını

   arama ve benzer şekilde bunlara erişme yetkisine sahip olmaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

2. Tarafların her biri, paragraf 1.a uyarınca makamlarının özel bir bilgisayar sisteminin tamamı veya bir kısmını araması veya benzer şekilde bunlara erişim sağlaması söz konusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğuna inanmak için gerekçeleri bulunduğunda ve söz konusu veriler yasalara uygun biçimde ilk sistemden erişilebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Uluslararası Sözleşmeler-II

3. Taraflardan her biri, yetkili makamlarına, paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koymaya veya benzer şekilde güvence altına alma yetki tanımak için gerekli olabilecek yasama tedbirlerini veya diğer tedbirleri kabul edecektir. Bu tedbirler:

a. bir bilgisayar sisteminin tamamına veya bir kısmına veya bilgisayar verileri depolama aygıtına el koymaya veya bunları benzer şekilde güvence altına almaya;

b. söz konusu bilgisayar verilerinin bir kopyasını oluşturmaya ve bunu muhafaza etmeye;

c. ilgili depolanan verilerin bütünlüğünü korumaya;

d. erişim sağlanan bilgisayar sistemindeki bilgisayar verilerini erişilemez hâle getirmeye ve kaldırmaya yönelik yetkileri içerecektir.

4. Taraflardan her biri, paragraf 1 ve 2'de belirtilen tedbirlerin tatbik edilmesine olanak sağlanması amacıyla kendi yetkili makamlarına bilgisayar sisteminin işleyişi veya içerindeki bilgisayar verisinin korunması için uygulanan tedbirler hakkında bilgisi olan herhangi bir kişiden, makul ölçüde gerekli bilgileri temin etme konusunda yetki tanınması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Adli Bilişim

- Bilgisayar, bilgi sistemi ve bilişim ortamı ilişkili davalarda kanıt toplama özel bilgi gerektirmektedir. Ayrıca bu incelemelerin yapılabileceği ortamlara gereksinim vardır. Bu nedenle ülkeler Adli Bilişim adını verdiğimiz kurumları oluşturmaya başlamışlardır. Adli bilişim şöyle tanımlanmaktadır:
- Bilişim ortamlarından elde edilen bulguların çeşitli teknik donanım ve yazılımlar kullanılarak hukuki kanıtlara dönüştürülmesi sürecidir.
- Bu yönüyle adli bilişimin hukuktan çok, teknik ağırlıklı bir konu olduğu söylenebilir. Çünkü bilişim sistemlerindeki bulguların, bunlardan ayrıştırılarak birer hukuki kanıta dönüştürülme süreci oldukça yoğun, son derece teknik bilgi gerektiren ve uzmanlık isteyen bir iştir.
  - Disk ile ilgili çalışmalar,
  - Bellek üzerindeki çalışmalar,
  - Bilgisayar ağı ile ilgili olanlar,
  - Gezgin sistemler ile ilgili çalışmalar,

  Çalışma alanına bakılmaksızın adli bilişimin çalışmaları üç aşamada sürdürülür:

  1. Kanıt (delil) elde etme ve saklama,
  2. İnceleme ve çözümleme
  3. Raporlama ve mahkemeye sunma

Bilişim ortamındaki veriler kurallarına göre toplanmazlar ise kanıt olma niteliklerini yitirirler. Böyle bir yanlıştan en çok gerçek suçlular kazançlı çıkar.

Adli Kanıt

Dava konusu olan olayların hepsinde sayısal kanıt karşımıza çıkmakta ve şu sorular sorulmaktadır:

- Bilgisayarın belleğinde bulunan bilgiler adli kanıt sayılabilir mi?
- Bilgisayarın diskinde bulunan bilgiler adli kanıt sayılabilir mi?
- CD veya DVD üzerinde bulunan bilgiler adli kanıt sayılabilir mi?
- Taşınabilir disk ve çubuk bellek üzerinde bulunan bilgiler adli kanıt sayılabilir mi?
- Bulutta bulunan bilgiler kanıt sayılabilir mi?
- E-postalar adli kanıt sayılabilir mi?

Bu soruların ayrıntılı biçimde yanıtlarını vermeden önce adli kanıtı tanımlamak yararlı olur ve şöyle tanımlanır:

Bir olayı kanıtlayabilecek nesnelere kanıt denilmektedir ve kanıt maddi gerçeklere, hukuka ve akla uygun olmalıdır.

Bilgisayarın da konu olduğu olaylarda kanıt toplama, bir cinayet olayından kanıt toplama işleminden çok farklıdır. Bu farklılığı görerek yasalar hazırlanmalı ve yöntemler üretilmelidir.

Bilgisayarın Belleğinde Bulunan Bilgiler

- Bilgisayarın belleğinde bulunan bilgiler delil olabilir. Ancak delil toplama aşamasında bilgisayarın çalışır durumda olması gerekir. Ayrıca suç ile ilişkili olan programın da çalışır durumda olması gerekir. Bilgisayar kapatıldığında belleğindeki bilgiler yok olmaktadır. Ayrıca bir program ile ilgili bilgiler belleğe bu program çalışırken yüklenir.
- Bilgisayarın belleğindeki bilgilere erişmek her zaman olanaklı değildir. Ayrıca veriler genellikle belgelerde, çizelgelerde veya veri tabanlarında tutulurlar. Bellekte yer kaplayan programlardır.

Bilgisayarın Diskinde Bulunan Bilgiler

- Bilgisayarın diskinde işletim sistemi, değişik amaçlara yönelik programlar, belgeler, veriler, ses kayıtları, fotoğraflar ve filmler bulunabilir. İşletim sisteminin dışındakileri bilgisayarın sahibi ya da başkası üretmiş olabilir.
- Uygulama programları lisanslı ve üreticisi biliniyor ise kanıt açısından bir sıkıntı yoktur. Programın üreticisi belli değil ise kanıt özelliği kesin değildir. Özellikle saldırı ve soygun amaçlı programlar bu niteliklerde olabilir.
- Davalarda en çok gündeme gelen konu bilgisayarda bulunan belgelerdir. Bilindiği gibi belge hazırlamak için kullanılan değişik yazım programları bulunmaktadır. Bu programların çoğunda belgenin yazarının adı, yazıldığı tarih, başkaları tarafından da eklemeler yapıldıysa onların adları ve değişiklik tarihi, basım tarihi gibi bilgiler belgeye başlık bilgisi olarak eklenmektedir. Davalarda bu başlık bilgileri kanıt olarak kullanılmak istenmektedir. Söz konusu bilgiler her zaman değiştirilebilecek bilgilerdir. Daha önce programın kaydettiği geçmişe ilişkin tüm bilgiler daha sonra değiştirilebilir. Dolayısıyla adli kanıt olarak değer taşımazlar.
- Çizelge programları da yazım programlarına benzer şekilde çizelgeyi hazırlayan ve değiştirenlere ilişkin bilgileri tutarlar. Bu bilgiler de daha sonra değiştirilebilir bilgi olduklarından adli kanıt olamazlar.
- Benzer biçimde fotoğraf ve filmlerin eklerinde, kullanılan fotoğraf makinesi, teknik bilgiler, zaman bilgisi ve fotoğrafı veya filmi çekenin adı yazılır. Bu bilgiler de değiştirilebilir bilgiler olduğu için adli kanıt sayılamazlar.
- Bir belge, çizelge, fotoğraf veya bir filmin üzerindeki yapımcı adı, değiştiren adı, yapım ya da çekim tarihi gibi bilgiler, bu nesnenin kanıt olmasına yetmez üstelik kanıt olmadığını gösterir. Benzer durum fotoğraf ve filmler için de geçerlidir

CD/DVD Üzerinde Bulunan Bilgiler

1. Bir CD veya DVD'nin yazıldığı tarihe bakarak o CD veya DVD'nin üzerinde yazılan tarihte yazıldığı söylenemez. CD veya DVD'nin üzerinde görülen yazılma zaman bilgisi yazan bilgisayarın zaman bilgisidir. Bir bilgisayarın zaman ayarı her zaman değiştirilebileceğine göre CD veya DVD üzerindeki zaman bilgisi adli kanıt olamaz.
    - Bir CD veya DVD'ye bilgi yazmak için kullanılan programın üretim tarihi kesin delil olamaz. Eğer CD veya DVD'ye bilgi yazmak için kullanılmış olan program incelemenin yapıldığı tarihten önce kullanımda ise kesinlikle adli delil olamaz. Daha açık bir ifade ile CD veya DVD üzerindeki belgelerin yazılış zamanları yazma programının kullanımda olma zaman aralığı ile uyumlu diye bu bilgilerin söz konusu aralıkta hazırlanmış olduğu sonucuna varılamaz.
    - Daha açık bir ifade ile CD veya DVD üzerindeki belgelerin yazılış zamanları yazma programının kullanıma sürüldüğü tarihten önceyi gösteriyor ise söz konusu CD veya DVD'nin yanıltma amacıyla hazırlandığı açıktır.
2. Bir CD veya DVD üzerindeki belge, tablo, fotoğraf ve filmleri üretenin adı, üretim tarihi, değiştirme tarihi ve benzeri başlık bilgiler daha sonra değiştirilebilen bilgilerdir. Bu nedenle adli kanıt sayılamazlar.

Taşınabilir Disk ve Çubuk Bellek Üzerinde Bulunan Bilgiler

Günümüzde taşınabilir disk ve çubuk bellekler yaygın biçimde kullanılmaktadır. Bu tür bilgi saklama aygıtlarında bulunan program, belge, fotoğraf ve filmler bilgisayardan yüklenen bilgilerdir. Yüklendikleri gibi okunup bilgisayara aktarılabilirler. Bilgisayara aktarıldıktan sonra hazırlayan ve değiştiren bilgilerinin tümü değiştirilebilir. Bu değişiklikler yapıldıktan sonra tekrar taşınabilir disk ve çubuk belleğe yüklendiklerinde yapımcı ve değiştiricilere ilişkin bilgiler değişmiş olur. Dolayısıyla taşınabilir disk ve çubuk belleklerde bulunan belge, çizelge, fotoğraf ve filmlerin yapım zamanı, yapımcı adı, değiştirenin adı ve zamanı bilgileri adli kanıt sayılamazlar.

Uzak Ortam ve Bulutta Bulunan Bilgiler

- Günümüzde belge, çizelge, ses kaydı ve görüntü kayıtlarını bilgisayar dışında saklama olanağı bulunmaktadır. Bulut ortamında bedava disk alanı sağlanabildiği gibi büyük boyutlu disk gereksinimleri ücreti karşılığında sağlanabilmektedir. Bulut bilişim bu özelliğe program kullanma hizmeti de eklemektedir. Dolayısıyla bugün bir kişi kendi bilgisayarında hiçbir iz bırakmadan tüm işini bulutta yapabilir ve verilerini bulutta tutabilir.
- Uzak ortam ve bulutta saklanan verilerin adli delil olarak değerlendirilebilmesi için öncelikle bu ortamı sağlayan kuruluşa güvenmek gerekir.

E-postalar

- Bazı davalarda e-postalar kanıt olarak sunulmaktadır. E-postaları gönderen kişi kimlik ve adresini saklayabilmekte, sahte bir kimlikle gönderebilmektedir. Bu nedenle e-postaların adli kanıt sayılması zordur. Ayrıca e-postanın içeriği ve postanın künye bilgisi sonradan da düzenlenebilirler. Ancak e-posta hizmeti sağlayıcılarındaki eylem tutanakları ve trafik bilgileri kanıt olarak kullanılabilir. Adli kanıt sayılabilecek sayısal verilerin nasıl toplanması gerektiği bir sonraki kısımda anlatılacaktır.

Adli Kanıt Toplama-I

- Bilgi sisteminde bulunan her türlü bilginin adli kanıt sayılabilmesi için belli kurallara göre toplanması gerekmektedir. Olay yerinde yapılması gereken bu işlem sırasında sanık ve avukatıyla birlikte savcı, kolluk kuvveti ve varsa adli bilişim uzmanının hazır bulunması gerekir. Bilgi sistemleri çalışır durumda iseler durdurulmaları gerekir. Bunun ardından kanıtlar aşağıdaki yöntemler ile toplanır. Konuya yasal dayanak oluşturan hususlar Ceza Muhakemesi Kanunu (5271) Md.134'te yer almaktadır:
- Ortamda bulunan bilgisayarların belleğinin veya disklerinin birebir kopyalarının, ilgili tarafların gözetiminde alınması gerekir. Alınan kopyanın daha sonra değiştirilmesi olasılığını gidermek için Hash algoritması kullanılarak özeti çıkarılmalıdır. Alınan kopya ve özetinin birer kopyası sanık tarafına verilmelidir.
- Ortamda taşınabilir disk, çubuk bellek ve CD/DVD var ise bunların da birebir kopyaları alınmalı ve her kopyanın özeti çıkarılmalıdır. Her kopya ve özetten birer kopya sanık tarafına verilmelidir.
- Bir bilgi depolama biriminde kayıtlı olanların bire bir kopyasını alabilmek üzere üretilmiş aygıtlar bulunmaktadır. Bu aygıtlar bir donanım ve üzerinde çalışan bir yazılımdan oluşur. Piyasadaki ürünlerin çoğu bireysel bilgisayarların belleğinin birebir kopyasını alabilecek yetenektedir. Bu ürünlerde çalışan programlar için kapalı ve açık kaynak kodlu olanlar bulunmaktadır.

Adli Kanıt Toplama-II

- Bire bir kopya alan sistemin güvenilir olması gerekir. Her şeyden önce kopyasını alacağı depolama birimine ekleme yapmayacağından emin olunmalıdır. Dolayısıyla hem kopyalama sisteminin hem de kullanıcısının tarafsız ve güvenilir olması çok önemlidir. Kopya alma işleminde güvenilirlik belgesi olan donanım ve yazılımların kullanılması doğru olur.
- Söz konusu sistemlerin bazıları silinmiş verileri de belli ölçüde getirebilmektedir.
- Olay yerindeki çalışmalar tamamlandıktan sonra donanımların alınıp götürülmesine gerek kalmaz. Böylece bir yanlış uygulama sona erdirilmiş olur. Ancak bir çatışma durumunda elde edilen bilgisayar ve çevre birimler gerekli önlemler alınmak kaydıyla adli bilişim incelemesi için alınıp götürülebilir.
- Yukarıda anlatılanlara ek olarak şu hatırlatmanın yapılmasında yarar vardır. Nereden ve nasıl elde edildiği belirsiz disk, CD/DVD veya çubuk bellekler mahkemeye kanıt olarak sunulduğunda ilk olarak bunların kim tarafından, nasıl, nereden ve ne zaman elde edildiğinin iyice araştırılması gerekir. Sunulan bu ortamlardaki bilgiler doğru olabileceği gibi mahkemeyi yanıltmak amacıyla hazırlanmış düzmece bilgiler de olabilir. Bu ön değerlendirmeden geçtikten sonra teknik değerlendirmesinin yapılması daha doğru olur.
- Günümüzde belge, veri, ses ve görüntüler bulut ortamında da saklanabilmektedir. Bir bilgi sisteminin bulut ortamını kullanıp kullanmadığı bilgisayarda yapılacak araştırmalar sonucunda öğrenilebilir. Bulutta tutulan kayıtların de bire bir kopyalarının alınması yoluna gidilmelidir.

İnceleme ve Çözümleme

- Olay yerinde toplanan kanıtların bir laboratuvar ortamında incelenmesi ve değerlendirilmesi gerekir. Bir benzetme yaparsak bir cinayeti incelemek ve değerlendirmek ile ilgili teknik çalışmaları adli tıp kurumu yapar. Adli tıp kurumunda çalışanlar konunun uzmanı doktorlardır. Dolayısıyla adli bilişim kurumunda da sayısal verileri inceleyecek, çözümleyecek ve değerlendirecek kişilerin de konularında uzman bilişim uzmanları olması beklenir.
- Sayısal verilerin incelenmesi sırasında özel donanım ve yazılımlara gereksinim olacağı açıktır. Bu tür donanım ve yazılımlar piyasadan hazır olarak elde edilebilmektedir. Dolayısıyla gerekli olan bunları kullanabilecek uzmanlardır. Uzmanlar mevcut kayıtların içinde aradıklarını nasıl bulabileceklerini bilen insanlar olmalıdır.
- Toplanan sayısal veriler şifrelenmiş olabilir. Bu durumda, öncelikle sanıklardan çözme parolasının öğrenilmesi yoluna gidilir. Parolanın öğrenilemediği durumlarda çözülmesi yoluna gidilir.

Raporlama

- İnceleme ve çözümleme çalışmalarının ardından hâkimin anlayacağı dille ve kanıtlara dayalı olarak bir rapor hazırlanır. Bu raporda:
- Konu aşamaları ile birlikte tanıtılmalı,
- Bulgular teknik bilgiler ile desteklenerek sunulmalı,
- Sonuç kesin biçimde açıklanmalıdır.

Adli Bilişim Çalışmaları-I

Disk İncelemesi

- Disk üzerindeki kayıtların incelenmesi aşamasında aşağıdaki durumlar ile karşılaşılmaktadır:
- Dava ile ilgili belge, ses kaydı, fotoğraf ve filmlerin incelenmesi,
- Şifreli kayıtların açılması,
- Silinmiş kayıtların geri getirilmesi
- Disk üzerinde değişik özellikte kayıtların olacağı bilinmektedir. Bu kayıtlar içinde dava ile ilgili olanlar ayıklanmalıdır. Davaya konu olanlar genellikle bilgisayarın sahibi tarafından oluşturulan dosyalardır. Bilgisayardaki işletim sistemi ve üreticisi bilinen uygulama yazılımları ayrı tutulmalıdır. Dava ile ilişkisi olacağı düşünülen dosyaların içerikleri teker teker incelenmelidir. Dosyaların boyutları çok büyük olabileceğinden içlerindeki taramalar sözcük temelli yapılabilir.
- Şifrelenmiş dosyaların anahtarları sahibinden istenebilir. Alınamadığı durumlarda parola çözümüne gidilebilir.
- Silinmiş kayıtların getirilmesi her durumda olanaklı değildir. Silinmiş ancak üzerine yeni bir şey yazılmamış dosyaların geri getirilmesi olasıdır. Ancak üzerine yeni bilgilerin yazıldığı veya özellikle geri getirilmelerini engellemek üzere kazınmış dosyaları geri getirme olanağı yoktur.
- Bilgisayarın diski için anlatılanlar taşınabilir diskler ve çubuk bellekler için de geçerlidir

Adli Bilişim Çalışmaları-II

Bellek İncelemesi

- Bellek incelemesi bilgisayar çalışır durumda iken yapılabilecek bir çalışmadır. Bilgisayar kapatıldıktan sonra ancak eylem tutanağındaki bilgilere erişilebilir.

Bilgisayar Ağı İncelemesi

- Bilgisayar ağları üzerindeki trafik bilgileri, sızmaları algılama sistemi bulunduran kuruluşlardan ve Genelağ hizmet sağlayıcılarından sağlanabilmektedir. Bu bilgilerden kimin ne zaman kimin ile iletişime geçtiği, ne tür bir iletişim gerçekleştirdiği ve iletişimin ne kadar sürdüğü bilgisi elde edilebilir.

Gezgin Sistemlerin İncelemesi

- Özellikle akıllı cep telefonlarının yaygınlaşması, adli bilişimi bu konuda çalışmaya yöneltmiştir. Telefonların SIM kartları ve bellekleri üzerinde çalışılması gerekmektedir. Bu araştırmalar kişinin konuşma kayıtları, mesaj kayıtları ve aktardığı bilgiler hakkında bilgi vermektedir.
- Cep telefonu işletmeninden alınacak bilgiler ile telefon sahibinin şu an bulunduğu yer ve geçmişte dolaştığı yerler zaman bilgisi ile birlikte öğrenilebilmektedir. Bu bilgilerin elde edilebilmesi için mahkemeden özel izin alınması gerekmektedir.

Adli Bilişimin Önemi

- Adli bilişim, bilişim ortamında var olan bulguların teknik açıdan değerlendirilmesini ve davalara geçerli kanıt olarak sunulması sağlar. Böyle bir hizmet sadece suçluları ortaya çıkarmak açısından değil, suçsuzların da saptanması açısından önemlidir. Bu nedenle günümüzde en az adli tıp kadar gerekli bir kurumdur.
- Adli bilişim kurumunun kurulabilmesi ve yaşayabilmesi için gerekli donanım ve yazılımları barındıran merkezlerin kurulması ve bunları kullanabilecek uzmanların yetiştirilmesi gerekmektedir.