Semih DOKURER
Başkomiser
Kriminal Polis Laboratuarları
semih.dokurer@kpl.gov.tr

ADLİ BİLİŞİM

GİRİŞ

Uzun yıllardan beri adli tıp, adli kimya gibi adli uzmanlık alanları suç soruşturmacılarına yardım ederek, bir çok adli olayın bilimsel yöntemlerle çözülmesine olanak tanımıştır. Uzmanlar olay mahallindeki biyolojik veya fiziksel izlerin kendilerine gösterdiği ipuçları ile olay hakkında ayrıntılı bilgiler elde edebilmiştir. Fakat günümüzde suçların ve suçluların dijital ortamda kendilerini göstermesiyle, olayları aydınlatmaya çalışan uzmanları artık doğadaki iz ve bulgular değil, bilgisayarlardaki manyetik olarak kodlanmış 1 ve 0'lar beklemektedir.

Teknolojinin hızla gelişmesi paralelinde Bilişim Suçları, kullanım ve erişim kolaylığının artmasıyla günümüzde suçluların yeni trendi haline gelmiştir. Suçları soruşturmakla görevli kolluk görevlileri de bilişim suçları ile mücadele edebilmek için dijital ortamı çok iyi tanıyor olmalıdır. Olay yerinde bulunmuş dijital delile yaklaşım tarzı diğer delillere göre farklılıklar arz eder. Delilin toplanması ve laboratuarda incelenmesi ayrı bir uzmanlık dalıdır.

Bu yazıda Adli Bilişim kavramı; bilişim suçları ve dijital delil tanımları ile birlikte anlatılacaktır. Ayrıca Adli Bilimler çerçevesinde Adli Bilişimin süreçleri ve prosedürleri ile incelemeler esnasında dikkat edilmesi gereken hususlara değinilecektir. Bunun yanında, Adli Bilişim hizmetlerinden yararlanmak isteyenler için bu hizmeti veren kurumlarda hangi servislerin yer aldığından da bahsedilecektir.

Yazının amacı; bilişim suçlarının çağımızın korkulu rüyası olmadığını, bu suçlarla mücadele konusunda çalışmaların bulunduğunu göstermektir. Ancak bu servisleri verebilmek için bilgiye ve insana yatırım yapılması gerektiği de yazıda vurgulanacaktır.

BİLİŞİM SUÇLARI

Teknolojinin hızla gelişmesi ile bir zamanlar bir odanın içine ancak sığdırılabilen bilgisayarların şimdilerde daha gelişmiş olanları avuç içinde kumanda edilebilmektedir. Bilgisayarlara erişim ve bilgisayar kullanım kolaylığı arttıkça, suç işlemeye eğilimi olan insanların elinde bilgisayarların suç aleti olma olasılığı da aynı hızda artmaktadır. Böylece insan hayatını her geçen gün biraz daha kolaylaştıran bilgisayar ve iletişim teknolojileri, bir çok alanda klasikleşmiş anlayışları değiştirerek insanlara yeni bir görüş, yeni bir

hayat tarzı kazandırmanın yanında bilişim suçları olgusunu da beraberinde getirmiştir.

Bilişim suçları özellikle dijital ortamdaki değerlere yapılan saldırılardır ve genellikle bankalardaki finans ve hastane kayıtları, askeri bilgiler v.b. saldırılara maruz kalma potansiyelini taşımaktadır. Bilgisayar üzerinden daha ucuz ve kolay suç işleme olanağı ileride bu suç tipleri ile daha çok karşılaşacağımız anlamına gelmektedir. Bu durum ise bilişim suçlarının hırsızlık, soygun, terörizm, sabotaj, kaçakçılık gibi bildiğimiz klasik suç tiplerinin dijital ortamda yerini alacağı anlamına gelmektedir. Bununla birlikte ülkeler arasındaki sanayi, teknoloji ve strateji casusluğu dijital ortamda yapılmakta ve ülkeler bundan dolayı büyük zararlar görmektedir. Ayrıca banka hırsızları artık klasik yöntemler yerine iletişim sistemlerini kullanarak bankalardaki hesap kayıtlarını rahatça değiştirilebilmektedir. Ek olarak internet üzerinde oluşturulan sistemler ile kumar oynatılabilmekte, pornografik ve hatta devlet aleyhine yasadışı yayınlar yapılabilmektedir. Güncel hayatta daha sık karşılaştığımız bu örnekler her geçen gün daha da artmaktadır.

ADLİ BİLİŞİM

Bilişim suçlarının sınıflandırılması hakkında bir çok çalışma mevcuttur. Bu çalışmaların bir kısmı suçun amacına, bir kısmı suçun tekniğine, bir kısmı da hukuki yönüne göre sınıflandırılmış durumdadır. Ancak her ne şekilde olursa olsun bu suçlarda yüksek teknoloji kullanılması kaçınılmazdır. Yüksek teknoloji bilgisi ile işlenen suçları yine aynı seviyede bir bilgi birikimi ile inceleyerek çözmek mümkün olabilir. Yüksek teknoloji suçlarının incelenmesini kapsayan Adli Bilişim tanımına diğer tüm adli inceleme tanımlarının bilgisayara uyarlanmış şekli de denebilir. Kısaca adli bilişim, olay yerinden alınan elektronik bir delilin mahkemede sunulmasına kadar geçen süre içerisinde yapılan laboratuar çalışmalarını kapsamaktadır.

DİJİTAL DELİL

Türk hukukunda ispat için kullanılmak istenen bir vasıtanın delil olarak nitelendirilebilmesi için iki temel özelliği taşıması gerekmektedir. Birincisi bu vasıtanın gerçekte olayı temsil ediyor olabilmesi, ikincisi ise olayı temsil eden vasıtanın akla, maddi gerçeğe ve hukuka uygun olması gerekliliğidir. [Uygulamalı Ceza Muhakemesi Hukuku Prof. Dr. Bahri Öztürk, Yrd. Doç. Dr. Mustafa Ruhan Erdem, Yrd. Doç. Dr. Veli Özer Özbek,Seçkin Yayınevi 7. Baskı, Sh:411]

Dijital delil ise temel delil şartlarını sağlamanın yanında suça delil niteliği sağlayan ve mahkemelere sunulabilecek dijital veri saklayabilen ve/veya elektronik devre akımları ile çalışan disk, disket, CD, bilgisayarlar, cep telefonları, PDA cihazları, flash bellekler, SIM kartlar, bir bilgisayara ait dahili veya harici donanımlar gibi çeşitli

elektronik cihazlardır. Elektronik cihaz oldukları için "Elektronik Delil" tanımı ile de bir çok yerde karşılaşılabilmektedir.

Günümüzde insanlar verilerini defter ve kağıttan çok dijital ortamlarda saklamayı tercih etmektedir. Not defterlerinin yerini cep telefonları, PDA cihazlar veya dizüstü bilgisayarlar almaktadır. Klasik mektuplaşma yönteminin yerine ise internet üzerinden e-posta göndermek güncel konumdadır. Bir şirket kendisine ait mali ve idari tüm kayıtlarını raflarda dosyalamak yerine bilgisayarlardaki veri bankalarında saklamaktadır. İşte bu noktada bu veriler suça dahil olduklarında dijital delil niteliğini kazanmaktadır. Ancak bu veriler kağıt ortamı gibi gözle görülebilen veya doğal olaylarla çok kolay açıklanabilen bir yapıda olmadığı için farklılık göstermektedir.

Dijital bilgi elektrik gelince görünen elektriği kesince yok olan sanal bir bilgidir. Bu yüzden hukuki olarak delil niteliği taşımasında da bir çok problemle karşılaşılmaktadır. Fakat bu bilgiler metafizik gibi ispat edilemeyecek de değildir. Aslında veri depolama ortamlrının üzerindeki veriyi oluşturan 1'leri ve 0'ları tanımlamak için değişik yöntemler kullanılmaktadır. Manyetik alanlar bunlardan biridir. Disk yüzeyinde oluşturulmuş olan pozitif veya negatif yönlü manyetik alanlar 1 ve 0'ları, 1 ve 0'lar da verileri oluşturmaktadır. Bu yüzden bilimsel yöntemlerle yapılan Adli Bilişim incelemeleri hukuken sonuç doğurabilmektedir. Bilgisayarların çok hızlı işlem kapasiteleri sayesinde veriler üzerinde bazı görsel işlemleri sanalmış gibi yapıyor olsak da, esasında bu işlemlerin altında her zaman bilimsel olarak ispat edilebilen bir alt yapı mevcuttur.

Üzerlerine dijital bir veri saklanmıyor olsa bile bir modem, telefon, uzaktan kumanda, kamera vs. gibi çeşitli elektronik cihazlar da dijital delil niteliği taşıyabilmektedir. Çünkü üzerlerindeki değişik mantık kapıları ile karar verebilen elektronik devreler sayesinde başka bir elektronik delili tetikleyebilecek bir mekanizmaya sahip olabilirler.

Dijital işlemler ister yazılımlar sayesinde, isterse de elektronik mantık kapıları ile yapılıyor olsun sonuçta yüksek teknoloji bilgisi ile yapılmaktadır. Bu dijital işlemler eğer bir suçun işlenmesinde rol alıyorsa, incelenmesi de mecburen yine aynı seviyede bir teknoloji bilgisi gerektirmektedir. Bu konuda özel uzmanlarca inceleme yapılması gereken deliller Adli Bilişimin materyallerini oluşturmaktadır. Bu adli materyallere ise elektronik veya dijital delil denilmektedir.

ADLİ BİLİŞİM SÜRECİ

Adli Bilişim süreci hazırlık soruşturması içerisindeki laboratuar incelemelerini kapsamaktadır. Tüm adli bilimlerde olduğu gibi Adli Bilişim de adli bir olayın maddi delillerle ispatlanması için laboratuar ortamında gerçekleştirilen bir çalışmadır. Ancak bu çalışma öncesi olay yerinden delillerin toplanması işlemi ve mahkemede bu delillerin

açıklanabilir bir şekilde ifade edilmesi de özel bir bilgi birikimi istediğinden Adli Bilişimin konusu içerisine girmektedir.

Olay yerinde bulunup incelemeye alınan her hangi bir materyal hiç bir zaman için mahkemede kabul edilmediği sürece delil niteliği taşımayacağı için Adli Bilişim süreci ne kadar prosedürlere uygun olur ise, elde edilen bulguların da mahkemece delil niteliği taşıma olasılığı o kadar artacaktır. Bu süreç içerisinde yapılması gereken üç ana aşama bulunmaktadır. Bunlar delilin Elde Edilmesi ve Muhafazası, İnceleme ve Analiz Edilmesi ile Raporlanarak Mahkemeye Sunması aşamalarıdır.

Delili Elde Etme ve Muhafaza Aşaması:

Olay yerine varıldığında çevre güvenliğinin sağlanmasından, delilerin laboratuara ulaştırılmasına kadar olan süreci kapsar. Her ne kadar olay yerinden delillerin toplanması bir laboratuar çalışması gerektirmiyor gibi görünse de kimi zaman delilin toplanması mümkün olamayan durumlarda olay yerinde laboratuar incelemesi yapılması gerekebilmektedir. Örneğin 7/24 hizmet veren bir internet servis sağlayıcısının sunucu bilgisayarlarını incelemek için laboratuar ortamına getirmek mümkün olamamaktadır. Bu durumda incelemenin olay yerinde gerçekleştirilmesi gerekecektir. Ayrıca olay yerinde bir uzman eşliğinde laboratuar incelemesine gerek duyulmuyor olsa bile delillerin toplanması dahi özel bir uzmanlık gerektirmektedir. Bu yüzden olay yeri incelemesi Adli Bilişimin süreçleri içerisinde girmektedir.

Olay yerinden delillerin toplanması en temel aşamadır. Çünkü deliller ne kadar sağlıklı toplanırsa bundan sonraki aşamalar da o kadar başarılı bir şekilde sonuçlanacaktır. Olay yeri ekipleri bilişim sistemleri konusunda yeterli bilgiye sahip olmalı ve delilleri yok edebilecek dijital bubi tuzaklarına karşı dikkatli davranmalıdır. Bilgisayarlardaki verilerin çok kolay yok olabileceği göz önüne alınarak, herhangi bir dijital bubi tuzağı olmasa bile delilleri toplama esnasında hatayla yok edilmemesi için özenle çalışılmalıdır. Örneğin; olay yerindeki bilgisayarın içinde ne var diye açılması, hatta açık olarak bulunmuş bir bilgisayarın kapatılması bile o anda içerisindeki kritik düzeydeki bir çok bilgiyi yok edebilecektir.

Olay yerinde elde edilen delillerin laboratuara getirilmesine kadar olan zaman diliminde delillerin bozulmadan saklanması ve laboratuara sevk edilmesi de bu süreç içerisindedir. Manyetik olarak saklanan verilerin bozulmaması için delillerin özel anti-manyetik torbalara ve fiziksel darbelere karşı koruyabilecek özel kutulara konulması gerekmektedir. Her ne kadar dijital verilerin biyolojik deliller gibi belli bir zamandan sonra bozulma riski olmasa da manyetik alanlardan çok rahat etkilendiklerinden delillerin korunması için özel anti-manyetik odalarda ve/veya dolaplarda muhafaza edilmesi de şarttır.

İnceleme ve Analiz Aşaması:

Sağlıklı bir inceleme ve bu inceleme sonucunda maddi gerçeğe uygun bir delil elde edilebilmesi için, olay yerinden toplanan materyallerin incelemesini yapacak her türlü cihaz ve konusunda uzman personelin bulunduğu bir laboratuar ortamına gerek duyulmaktadır. Her türlü ihtimale karşı, inceleme yazılımları, bir çok dönüştürücü cihaz ve tamir bakım setleri gibi araç gereçlerin her an hazır tutulması gerekmektedir.

Tüm adli incelemeler esnasında delil bütünlüğünün sağlanması ve kanıtların laboratuar ortamında birbirine karışmayacak ve değişmeyecek durumda olması gerekmektedir. Adli Bilişimde de bu tür konulara dikkat edilmelidir. Bir delil üzerinde bulunan bir bilgisayar virüsünün başka bir delile bulaşması, inceleme esnasında hata ile verilerin silinmesi veya değiştirilmesi gibi durumlar delilin niteliğini yok edecektir. Bu gibi durumlarla karşılaşmamak için delilin imaj dosyası üzerinde çalışmak her zaman daha sağlıklı bir yaklaşım olacaktır. Hatta olay yerinden mahkemeye kadar geçen süre içerisinde delilin değişmediğinin ispat edilebilmesi için delilin toplanması aşamasında özetleme işlemi (ing. hashing) diye bilinen ve verinin kısa bir özetini alan bir işlemden geçirilmelidir. Özetleme işlemi soruşturmanın herhangi bir süresinde tekrar alındığında yine aynı özet bilgiyi veriyorsa delilin inceleme esnasında değişmediği ispatlanabilmektedir. Veri üzerinde tek bir byte'ın bile değişiyor olması özetleme işleminin aldığı özet bilgiyi değiştirecektir.

İnceleme aşaması teknik konuları kapsamaktadır. Ancak bu teknik bilgilerin elde edilmesi sırasında soruşturma başka aşamalara da kayabilir. Bu yüzden soruşturmacının bu teknik inceleme sonuçlarını analiz etmesi ve buna göre soruşturmaya yön vermesi de Adli Bilişimin safhaları içerisindedir. Böylece delilerin incelenmesi sırasında elde edilen bilgiler devamı başka bir dijital delilin içerisinde yer alıyor olabilir ve ancak bütün delillerin incelemesi sonucunda anlamlı bir yargıya varılıyor olabilir.

Raporlama ve Mahkemeye Sunma Aşaması:

Adli bilimler ışığında yapılan tüm çalışmalar özel bir uzmanlık gerektirmektedir. Ancak uzmanlık incelemeleri teknik konuları kapsadığı için, sonuçların hem mahkemenin hem de tarafların anlayacağı ve ikna olabileceği şekilde izah edilmesi şarttır. Bunun için gerekli raporun hazırlanması da Adli Bilişim süreci içerisinde yer almaktadır. Çünkü rapordaki açıklamaları incelemeyi yürüten uzman dışında birisinin yapması mümkün değildir.

Mahkemece bilirkişilik istenmemiş olsa da bazı durumlarda konunun uzmanın da şahitlik yapması istenebilir. Bu gibi hallerde uzmanlar yazılı bir metin yerine sorulan olayın nasıl olduğunu sözlü olarak da izah edebilir.

ADLİ BİLİŞİM SERVİSLERİ

Suç öncesi ve suç sonrası olmak üzere iki tür polislik bulunmaktadır. Suç işlenmeden evvel suçun önlenmesi için yapılan her türlü istihbari takipler, devriyeler veya eğitim seminerleri gibi suçu önleyici faaliyetler suç öncesi polislik kavramına girmektedir. Ancak Adli Bilişim servisleri suçun işlenmesinden sonra olay yerindeki dijital iz ve bulguların incelemesini ele alır.

Bu aşamada Adli Bilişim servislerine gelebilecek bulgular genelde veri saklama medyalarıdır. Ancak bu medyalar değişik şekillerde zarar görmüş olabilir. Bu noktada Adli Bilişim Servisleri iki amaç için çalışır. Birincisi zarar görmemiş bir medya üzerinden suçun aydınlatılması için yapılan Veri inceleme Servisi diğeri ise zarar görmüş bir veri saklama medyasından daha sonra incelenmek üzere içindeki verileri kurtarma servisidir. Buları inceleyecek olursak:

Veri İnceleme Servisi:

Bir bilişim suçunu işleyen kişi bilgisayar sistemleri üzerinde geçtiği tüm yollarda iz bırakmaktadır. İster bilgisayar ağları, ister tek bir bilgisayar üzerinden bilişim suçu işleniyor olsun üzerinde veri saklayabilen tüm cihazlar incelemeye alınmalıdır. Şüphelinin kendi bilgisayarında, internet servisini almış olduğu servis sağlayıcısında, mağdur tarafın bilgisayarında ve buraya ulaşmak için kullanmış olduğu tüm geçit noktalarında (Proxyler, sunucu makineler, router'lar vs.) tutulan kayıtlar o kişinin suçu işlediğine dair bir çok delil taşır. Bu yüzden sadece olay yerinde bulunan bir cihazı değil, suçun işlenmesinde geçiş noktası olarak kullanılabilecek tüm cihazlar inceleme altına alınmalıdır. Çünkü bu cihazların tutmuş oldukları gigabyte'larca kayıt içerisinden belki bir yada iki tanesi suçu aydınlatabilecek kanıt olabilir.

Bu tür incelemelerde genelde mağdurun bilgisayarından geriye doğru yapılacak olan takipler olayı çözmek için doğru bir yaklaşımdır. Bu bilgisayara nereden bağlanılmış? Bağlanıldığı yere de nereden bağlanılmış?... gibi sorulara yanıt bulabiliyorsak suçu işleyen kişinin bilgisayarına kadar ulaşmak mümkün olacaktır. Bu sorulara cevap alabilmek için tüm geçiş noktalarındaki kayıtların tutuluyor olması gerekmektedir. Bir noktada alınamayan kayıt bilgi izin takibinin kesilmesi ile sonuçlanabilir. Bu kayıt bilgileri suçu işleyen veya yardımcısı tarafından da silinmiş olabilir. O yüzden silindi bilgisinin tutulmasının bile soruşturmacılara büyük yardımı olacaktır. Bir çok insanın internete bağlanmak için servis aldığı internet servis sağlayıcılarının kendi sistemlerinde detaylı kayıt tutmaları gerekir.

Soruşturma esnasında bazı bilgisayarlara el koyup incelemek her zaman mümkün olamayabilir. Servis sağlayıcılarındaki kesintisiz 7/24 hizmet veren sunucu bilgisayarların incelenmesi için hizmetin

kapatılıp tüm sistemin laboratuar ortamına getirilmesi her zaman mümkün olmayacaktır. Bu yüzden bu tür bilgisayar ve cihazlardaki bilgilerin olay yerinden alınması için gerekli teçhizatların veya olay yerinde inceleme yapabilecek uzman ekiplerin bulunması gerekecektir.

Kendisi görüntü kopyası alabilen ve almış olduğu kopyalar üzerinde adli inceleme yapabilen çeşitli yazılımlar soruşturmacılara yardımcı olmaktadır. Yine de sadece bu programların yanı sıra işletim sistemlerinin kendi kayıtlarının incelenmesi, elektronik postalar ve şifreli dosyaların açılması için kullanılan özel bazı programlara da ihtiyaç duyulabilecektir.

Veri Kurtarma Servisi :

Veri saklama medyaları, özellikle sabit diskler, hareketli parçalara sahip olduğu için daha çabuk bozulma eğilimi gösterirler. Diskin mantıksal veya fiziki zarar görmesi çok doğal bir olaydır. Güvenlik uzmanı Steve Gibson bu durumu kısaca şöyle ifade etmektedir: "Sabit diskler ikiye ayrılır: bozulmuş olanlar ve bozulacak olanlar". (http://www.pcnet-online.com/content/utilities/199902.htm)

Ancak laboratuara gelen bazı deliller kasten zarara uğratılmış da olabilir. Her ne şekilde olursa olsun veri saklama medyaları içerisindeki bilgiler çoğu zaman tamamen yok olmamaktadır. Adli Bilişim servisleri açısından böyle bir medya içindeki bilgiler incelemeye alınmadan evvel kurtarma işlemine tabi tutulmalıdır.

Mantıksal Zarar Görmüş Veri Depolama Medyaları : Veri depolama medyaları üzerindeki silinmiş bilgilerin kurtarılması, bozulmuş veya formatlanmış bölümleme yapısı bilgilerinin tekrar oluşturulması gibi mantıksal olarak zarar görmüş medyalardaki bilgilerin tekrardan yerine getirilmesi işlemidir.

Teknik olarak medyalar üzerinde manyetik olarak kodlanmış 1 ve 0'larla ifade edilen bilgilerin silinmesi tekrar oluşturulması kadar zor bir işlemdir. Mesela bir verinin silinmesi için veri boyutu kadar medyaya 1'lerin veya 0'ların konulması yerine, verinin silindi işaretinin konulması veya diskin formatlanması için Gigabyte'larca verinin silinmeye çalışılması yerine sadece boot (diskin başlangıç bölümü) bilgilerinin silinmesi daha pratik bir işlemdir. Esasında bu yüzden veriler hala disk üzerinde durmakta, ancak ulaşılması için işletim sistemi üzerinde bir bilgi bulunmamaktadır. Adli inceleme için kullanılan özel yazılımlar bu bilgileri -bir yere kadar- elde etmemizi sağlayabilmektedirler. Gigabyte'larca bilgi üzerinden yapılan bit bit yapılan veri inceleme işlemleri her ne kadar çok zahmetli olsa da bir suçun araştırılmasında bize çok önemli sonuçlar doğuracağı için, yapılması gerekli bir işlemdir.

Fiziksel Zarar Görmüş Veri Depolama Medyaları: Veri depolama medyaları, özellikle sabit diskler bir veriye ulaşabilmek için çok fazla işlem yapmaktadırlar. Özel bir ara birimle bilgisayar üzerinden hangi dosyaya erişileceği sinyali diskin elektronik devresine gönderilir. Elektronik devre ona göre diskin dönüşünü ve kafanın bilginin manyetik olarak kodlandığı bölüme (sektör/iz) ulaşması için gerekli hareketleri gerçekleştirir ve aynı yolla veriler bilgisayara aktarılır. Bu aşamalar içerisindeki herhangi bir elektronik, mekanik veya manyetik bozukluk veriye ulaşmayı engeller.

Disklerin fiziksel olarak bozulma olasılıkları ne kadar kolay olsalar da, bu arızanın tespiti ve içerisinden bilginin kurtarılması çok zor bir işlemdir. Çünkü bu veri kurtarma işlemi için uzmanın elinde sabit disk ile alakalı teknik bilgilerin olması gerekmektedir. Ancak bu tür bilgiler diskin üretici firmasında bulunduğu için uzmanların incelemesi bir noktadan sonra bilgi yetersizliğinden dolayı kesilmektedir.

Fiziksel arızalı bir disk üzerindeki verileri okunabilir hale getirebilmek için diskin bu işlemi yaparken kullandığı mekanizmaları üretici firma standartları dışında başka bir ortamda yapılabilir hale getirilebilmesi ve bilgilerin manyetik olarak yazıldığı plağının sökülerek bu ortama taşınması gerekmektedir. Ancak sabit diskin kutusunun içerisine vakumlanarak yerleştirilmiş disk plaklarının incelenebilmesi için yine benzer bir ortam olan ve tozsuz laboratuar diye adlandırılan, içerisine havadaki bir toz zerresinin dahi karışmadığı laboratuar ortamlarında inceleme yapılması gerekir. Aksi bir durumda, kirli bir ortamda açılan disklerin yüzeyine dokunacak en ufak bir toz zerresi dahi diskin dönmesi ve üzerindeki kafanın hareket etmesi esnasında disk yüzeyine zarar verecek ve okunabilir seviyede olan diğer bilgileri de okunamaz hale getirecektir.

Böyle bir laboratuarın hem kurulması, bakımı ve işletilmesi oldukça masraflı olduğundan hem de bunların hepsi finanse edilebilecek olsa da teknolojisi kolayca transfer edilebilir olmadığından tüm dünyada Amerika, İsrail, Finlandiya gibi gelişmiş birkaç ülkede bulunmaktadır.

SONUÇ

Daha düne kadar Bilişim Suçları konusunda kafamızda bir çok soru işaretleri varken, şu an bir çok insan bu tür suçlardan bir şekilde mağdur olmuş durumdadır. Teknolojinin hayatımızın bir çok safhasına girmesiyle de her geçen gün bu suçların sayısının ve şiddetinin daha da artacağı belirgin bir şekilde görülmektedir. Bu yüzden artık insanlar bu suçlardan kaynaklanan mağduriyetlerinin giderilmesi için haklı olarak beklenti içine gireceklerdir. Ülkemizde bilişim güvenliği konusunda çalışmalar yapan bir çok şirket ve bilim adamı mevcuttur. Ancak bilişim güvenliği suçun işlenmesinden önceyi kapsamaktadır.

Bilişim sistemlerinde %100 bir güvenlik sağlanamadığı için bu suçların işlenmesi de kaçınılmaz olacaktır. Bu noktada suç sonrası yapılacak bilimsel incelemeler suçluya giden ipuçlarının bulunmasını sağlayacaktır. Ülkemizde Adli Bilişim konusunda yeterli uzman personel bulunmamaktadır. Özellikle suçla doğrudan ilgili olan ve hazırlık soruşturmasını takip eden kolluk görevlilerinin bu konuya eğilmesi, olay yeri ekiplerinin ve Kriminal Laboratuarlarının geliştirilmesi gerekmektedir. Bu amaçla ülkemizde Kriminal Polis Laboratuarlarında Adli Bilişim hizmetleri vermek üzere Data İncelemeleri Bölümü kurulmuştur. Ancak sadece kolluk görevlileri değil, diğer kamu kurum ve kuruluşları ile özel şirketlerin bilgi işlem departmanları da olay sonrası Adli Bilişim hizmeti verebilecek ekiplerini kurmalıdır. Çünkü kendi sistemlerini en iyi kendileri bileceğinden suç sonrası delillerin toplanması için kolluk görevlilerine büyük yardımları dokunacaktır.

Bilişim Suçlarının yaygınlaşması ile Adli Bilişim hizmeti gündeme gelmiştir. Ancak yetişmiş eleman ve teknoloji eksikliği bu hizmetin sağlıklı verilmesine büyük engel teşkil etmektedir. Bu yüzden Adli Bilişim konusunda ülkemizde hem özel hem de kamu sektörü tarafından gerekli yatırımların yapılması şarttır.