© Uluslararası İnsan Bilimleri Dergisi
ISSN: 1303-5134
www.insanbilimleri.com

Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum

GÜVEN ŞEKER[1]

Abstract

We can say that computer evidence is odd. It lurks on computer hard disk drives, zip disks and floppy diskettes at three different levels. Such evidence is fragile and it can easily be destroyed through something as simple as the normal operation of the computer. So that Law enforcements have to use special programs.

In attempting to sketch the future of law practice, it is helpful to focus on some underlying trends. Three such trends are not only influential today, but also signpost the direction in which law practice will move over the next quarter of a century. The three trends in question are dematerialisation, omnipresence and malleability. This trends will change IT ve practice next years in our country .

We aim at describe the technique evidence process. The remainder of this article analyzes the evidence of cyber crime.

Özet

Bilgisayar delillendirme süreci ilginç ve dikkat gerektiren bir süreçtir, 3 farklı seviyede bilgisayar yedeklemesi yapılabilir, hard disk sürücüleri, zip diskleri, disketler ile. Bu iki delillendirme çalışması hassas çalışmayı gerektirir, bilgisayarda yapılan normal çalışmalarda çalışma aygıtında kolaylık ile bozulmalara neden olabilirler.

Yüzyılımızda üç tane süreç bizi hukuk uygulamaların elektronik değişimi ile ilgili zorunluluğu açıklar. Bunlar maddi yapıdan çıkarım (dematerialisation), heryerde her zaman hazır sunum

(omnipresence) ve her düzenlemeye uygunluk (malleability) gerekliliklerdir. Bu şüreçler ülkemizdeki bilgi teknolojisini ve uygulamasını önümüzdeki yıllarda değiştirecektir.

Amacımız delillendirme süreci tekniklerinin ortaya konmasıdır. Bu makalede bilişim suçlarının delillendirilmesi ile ilgili olarak hazırlanmıştır.

ANAHTAR SÖZCÜKLER:

Key Words: Evidience process, Information, Cyber crime, Computer, Law Enforcments.

Anahtar Kelimeler: Delillendirme Süreci, Bilgi, Bilişim Suçu, Bilgisayar, Kanun Adamları.

Giriş

Bilgi teknolojisinin (IT) hızlı ilerleyişi hukuk dalında çalışma yapanları ilerleyen yıllarda nasıl etkileyecektir? Sistemimiz ve onu işletenler bu duruma uyum sağlama için neler yapabilir, sorunsalına uygun yaklaşımların geliştirilmesinin gerekliliği ortadadır.

İnternet elektronik bir dünya olarak, fiziksel dünya ile paralel gitmektedir. İnternet yapısı önceden tasarlanmış bir network (ağ) yapısından çok, hızlı ilerleyen birçok bilgisayarın dahil olduğu network (ağ) yapılarının büyük bir network (ağ) havuzunda birleşiminden oluşmaktadır. Bugün artık entegre bir yapıya sahip olan internet, bilgilerin sunulduğu, tartışıldığı, yenilerinin yaratıldığı, depolandığı, işlem gördüğü ve iletişim için kullanıldığı dünya çapında bir çevreyi oluşturmuşturmaktadır.

İnternet ile bilgi, fiziksel dünyadan elektronik dünyaya doğru bir göç yaşamaktadır (Buna bilişim dünyası, Siber Dünya da denilmektedir). Bu durum ilk olarak 2. Dünya Savaşı sonrası süreçte gelişmiştir. Her ne kadar da kişisel bilgisayarlar 1970' li yıllarda kullanılmaya başladı ise de, bu geçiş çok yavaş ve birbirinden kopuk olmuştur. 1980 ve 90' lı yıllarda artık bir çok bilgi elektronik formatta yada kağıttan, elektronik ortama aktarım süreci yaşamıştır. İnternetin ilk olarak orta ölçekte iletişimde kullanımı ile, bu süreç hızlanmış ve "kağıtsız büro" kavramını ortaya çıkmıştır.

1. Bilgi Teknolojisi Ve Elektronik Uygulama Zorunluluğunun Etkisi

Teknolojideki hızlı değişimi ile ilgili şu ilginç olay bize değişimin hızını göstermektedir. Aya ilk ayak basan insan olan Armstrong' un hocası bir konferansında; "Benim babam uçağı görmedi, görse de çelik yığınının havada uçabileceğine inanmazdı. Bense, uçağın icadına ve sesten hızlı gidenine şahit oldum. Sonunda benim bir öğrencim , bir uzay aracı vasıtası ile aya inmeyi başardı. Bütün bu gelişmelerin mazisi üç nesil yani yetmiş beş yılı kapsar" demiştir. Değişimin bu yüzü tabi ki bilgisayar alanında bu hızdan daha büyük hızla ilerlemektedir. Yüzyılımızdaki üç süreç bize hukuk uygulamaların elektronik değişimi ile ilgili zorunluluğu açıklamaktadır. Bunlar; maddi yapıdan çıkarım (dematerialisation), her yerde her zaman hazır sunum (omnipresence) ve her düzenlemeye uygunluktur (malleability).

Çalışma alanındaki bilgilerin içeriğinin fiziksel formattan, elektronik formata dönüşümü yani bunların maddi yapıdan çıkarım (dematerialise) sürecinde olması konusuna eğilmek gerekmektedir. Bu süreç tabi ki her yerde bankalarda, okullarda, alışveriş merkezlerinde, kütüphanelerde, mahkemelerde, devlet kurumlarında, kontrollü veya kontrolsüz olarak oluşmaktadır. Çok sağlam bürokratik yapıya giren yeni kavram eskinin yerine kesinlikle olmaz, böyle bir şey mümkün değil, sistemi engeller, gibi bir yaklaşım her zaman var olacaktır. Ayrıca yüz yüze iletişim üzerine kurulu fiziksel ortam yerine, elektronik etkileşim ile ilgili giderek daha çok artan kullanım baskısı bizim bu konudaki girişimlerimizin daha hızlı olmasını gerektirmektedir.

Her yerde her zaman hazır sunum (omnipresence) kavramı; maddi yapıdan çıkarım (dematerialisation), bilgi yaklaşımının bir sonucu olarak ortaya çıkan bir kavramdır. Dokümanlar ile insan ve mekanın durumları arasında bulunan fiziksel mesafe engel oluşturabilecektir. Elektronik mesafe kavramı ise, coğrafik durumunuza bakılmaksızın sanki aynı odadaymışsınız gibi, bilgi ve kurumların içine girilebilir gibi erişilebilir duruma getirmektedir. Ayrıca bilgi ve kurumlar sadece bir yerde olmaz böylelikle her yerde bulunabilirler. Ve sadece her yerde olmak ile kalınmayacak ve her yerde varlığını hissettirecektir. Her yerde her zaman hazır sunum kavramı elektronik dünyanın dikkate değer özelliklerinden biri olan aynı zamanda birçok yerde mevcut olma durumunu ifade etmektedir (Widdison, 1997:143 - 163). Nitekim bu kavram Bilişim Şurasında "e- Devlet yapısına özgü düzenlemelerin gerçekleştirilmesi"(bilisimsurasi.org.tr, 2002: 293) gerekliliği ortaya konarak ulusal yapıdaki vatandaşın her yerden her zaman hazır olarak kurumlara elektronik ulaşımı hedeflenmektedir.

Her düzenlemeye uygunluk (malleability); yukarıdaki iki kavramı birleştiren bir kavramdır. İlk olarak uygunluğa intibak kabiliyetini gösterir. Bilgisayarlar diğer şeylere oranla insan yapısına uyum sağlayabilen dünyadaki çok az şeyden biridir. Daktilo devamlı daktilodur, fotokopi makinesi fotokopi makinesidir, telefon bir telefondur. Bir bilgisayar, her ne kadar da yazı yazsa, fotokopi çekse, telefon, faks aleti olarak kullanılabilse de günlük olarak, dosyalama aracı olarak, grafik çizme aracı olarak, kütüphane olarak, kütüphaneci olarak ve sayılamayacak kadar çok şeyi yapabilmektedir. Böylelikle bilgi teknolojisini (IT) her nerede kullanmak istiyor isek orada kullanabiliriz. Var olan formları yenilikçi uygulamalar adına istediğimiz şekilde bilgi teknolojisi ile sınıflandırıp sunabiliriz. Elektronik formdaki bilgi her bir bireysel kullanıcı tarafından düzenlemeye, sınıflamaya, seçilmeye ve sunulmaya hazır bilgi anlamına gelmektedir.

Her düzenlemeye uygunluk, bilgi teknolojisi tabanlı çalışma araçlarının karakteristik anahtar özelliği olmamakla birlikte, sosyal alanı ilgilendiren özellikle işin nasıl, ne zaman ve nerede yapıldığı ile ilgilidir. 1970' lerde kişisel bilgisayar kullanıcılarının ilk öncüleri devletlerin ve diğer tabu haline getirilmiş değerlerin önünde bilgi teknolojisini özgür bırakmıştır. Bu bireyler arasında bilgisayarın demokratik ortamda, dünyaya yayılan gücünün artık politik bir anahtar ve sosyal bir nesne olması ile ilgilidir. Dünyadaki yapılan iş yeniden şekillenmiştir. Çalışanların iş merkezli çalışmalarından esnek ev temelli ve kişi temelli çalışmaya dönük bir yol ortaya çıkmıştır (Widdison, 1997:143 - 163). Maddi yapıdan çıkarım (dematerialisation), her yerde her zaman hazır sunum (omnipresence) ve her düzenlemeye uygunluk (malleability) kavramları alışkanlıkları ve çalışma yapılarını derinden etkileyebilecek kavramlar olarak sistemleri zorlamaktadır. Bu etki ile yeniden yapılanan bilgi sistemi beraberinde belli sıkıntıları da meydana getirmiştir. Tabi ki bu süreçte bu bilgi ile ilgili art niyetli ve bilginin suç aracı kullanımı gibi bir durum ortaya çıkmıştır.

2. Elektronik Ortamda Suç ve Suçun Tespiti

Bilişim suçları ile ilgili birçok hukuki boyutta bilişim suçunu hazırlayanlar ve işleyenler ile ilgili makaleler yazılmaktadır[1] örneğin; bilgisayarla veya bilgisayar vasıtası ile işlenen suçlar ile ilgili. Bu makalelerden çoğu bazı sosyal varsayımlara dayanarak yazılmakta ve her şeyi bilişim suçuymuşçasına adlandırılmaktadır. Nitekim bizim ceza kanunumuzda bilişim alanındaki suçlar,TCK' nun 525/a, 525/b, 525/c ve 525/d maddeleri olmak üzere toplam 4 maddeden oluşmaktadır. 525/a ve b ve c maddelerinde beş değişik suç söz konusudur. 525/d maddesinde de yeni bir suç tipi yaratılmamış feri cezalar öngörülmüştür. Tüm bu suçlar TCK' nuna 3756 sayılı yasa ile 1991 yılında eklenerek 11. Babta düzenlenmiştir.

Bilişim suçlarının alanına hangi faaliyetlerin girdiğinin tespiti uygulamanın ve yargılamanın başlıca sorunudur.

Bu soruna genel hatları ile değerlendirildiğinde ortaya şu sonuç çıkmaktadır. Faaliyet bilgisayar sistemi ile mi temellendirilmektedir, yoksa bilgisayar o faaliyetin gerçekleşmesinde yardımcı bir unsur olarak mı kullanılmaktadır. Bankaların A.T.M. uygulaması bilgisayar temelli olduğu için bilişim faaliyetidir. Çünkü bu sistem çöktüğünde bu faaliyet asla icra edilemez. Ancak Radyo ve Televizyon Yayıncılığı bilgisayar sistemlerini faaliyetlerinin çeşitli aşmalarında kullanmakta ise de, bunların faaliyeti bilişim temelli değil, iletişim temellidir. Yararlanma, bu yayınları bilgisayar temelli hale getirmez.

Bu suçların yargılaması da Asliye Ceza Mahkemelerinde yapılır ve takibi şikayete bağlı suçlar olmadığından, kovuşturmaları da re' sen yapılmaktadır. Ayrıca bilişim suçları içinde en önemli alanlardan biri olan internet suçları ile ilgili 4756 sayılı kanun ile[2] yeni bir düzenleme getirilmiş ve artık internet kaynaklı konularda basın kanunu altına alınmıştır. Ayrıca bu alanda bir de, Fikir ve Sanat Eserleri Kanunundan yararlanılarak eser sayılan metalar ile ilgili gerekli hükümler uygulanır.

Bilişim suçları diğer geleneksel suçlardan farklı olarak yeni kanunlar ve yeni araştırma teknikleri gerektiren bir alandır (Brenner: 2001: 3.Prg.). Ayrıca siber alan ileride de ele alınacağı üzere yeni çalışma teknik ve yöntemleri gerektiren bir konudur.

Suçlar sözde geleneksel anlamı ile gerçek yaşam alanı olarak adlandırılan ve fiziksel gerçeklerin paylaşıldığı alan içinde kalmaktadırlar. Bu nedenle bilişim suçları özel hayata müdahale, kamu haklarını ihlal gibi alanlarda değerlendirilmektedir. Modern ceza hukuku hala esas varsayım olarak dış alandan yani fiziksel alandan ilişki kurulabilecek davranışların -konu ile ilgili eylem yada eylemsizliğin hukuk ile ilgili alanın oluşmasını bekleyerek- beklenilmesini iddia etmektedir. Ayrıca bu iddiasın da sorumluluk olarak başkaca bir şey yüklenilmesini istemez (Brenner: 2001: 10.Prg.).

Siber alan; etki alanı ile var olan, fiziksel dünyadan ayrı bir alandır. "Sanal dünya" deyimi ile kavramsal olarak gerçekliği paylaştığı kadar, fiziksel gerçeklik ile paylaşımda bulunmaz. Fiziksel alan olmadığından beri, Ceza Hukukunun şimdiki ilkelerinin tartışılması ve kolaycı yol ile suçlara kolaylıkla siber alemin avantajlarını belki de sömürerek çeşitli yorumlamalarda bulunabiliriz. Bu kabul edilen yetersizlik, siber suçlar ve suç arasındaki maddi farklılıklardan kaynaklanmaz, bu kusurların ve zararın her ikisinin de birlikteliğinden meydana gelir (Brenner: 2001: 11.Prg.). Bu tür suçlar ile adli ve idari mücadelenin zorluğu da bu nedenden kaynaklanmaktadır.

3. Bilgisayar Delillendirme Süreci

Bilgisayar delillendirme süreci ilginç ve dikkat gerektiren bir süreçtir. Beş farklı seviyede hard disk sürücüleri, zip diskleri, disketler, cdler, dvdler ile bilgisayar yedeklemesi yapılabilir. İlk iki yedekleme bilgisayar kullanıcılarına anlamlı gelmeyebilir. Bu iki delillendirme çalışması hassas çalışmayı gerektirir, bilgisayarda yapılan normal çalışmalarda çalışma aygıtında kolaylık ile bozulmalara neden olabilirler. Elektro mıknatıs etki, zarar verici trojan(truva) atı ve virüs, programları ve diğer belirsiz nedenler ile birkaç saniyede bilgisayar delilleri yok olabilir. Bu konu ile ilgili başka benzer delillendirme süreçlerinde bu kadar araştırmacıya potansiyel problem ve zorluk çıkaran başka bir alan bilinmemektedir. Önceleri Amerikan Adli Sisteminde avukatlar ve savcılar delillendirme süreci ile ilgili çok şey bilmiyorlardı. Bu nedenle savunma konuları çok karmaşık bir durumda idi. Zamanla durumlar değişti ve kanun adamları hukuk alanında elektronik dokümanları keşif etmişlerdir. Ve zaman değişti, bir şeyleri kitaba göre yapmadan daha önemli hale geldi.

Bilgisayar araştırmacıları sadece bilgisayarın sahibi tarafından oluşturulan yıkıcı süreçler ve aygıtlardan endişelenmek ile kalmaz ayrıca, bilgisayar çalışma sistemi ve aygıtlardan endişelenmelidir. Deliller tipik bellek içinde, tablolama programlarında, veri tabanı ve kelime işlem dosyalarında bulunabilir. Ayrıca potansiyel deliller herhangi bir yerde, silinmiş dosyalarda ve Windows'un geçici dosyalarında bulunabilir. Bu gibi deliller Windows' un bilgi parçalarında ve kolaylıkla üzerilerine bilgisayarın yeniden başlatılması ile ve/veya Microsoft Windows'un çalışması ile yazılabilecek durumda bulunur. Windows başladığı zaman potansiyel olarak yeni dosyalar oluşturur ve normal bir süreç olarak var olan dosyayı açar. Bu durum silinmiş dosyaların üzerine yeniden yazılmayı ve Windows' un geçici dosyalarının değişmesine yada bozulmasına sebep olur. Ayrıca Windows normal işletim sürecinde dizin girişlerini günceller, bu noktada tabi ki dosya zaman ve tarihleri delillendirme sürecinde çok önemlidir.

Bilgisayar araştırmacıları için bir diğer sıkıntı, konu olan bilgisayardaki bir diğer programın çalışmış olmasıdır. Suçlular işletim sisteminde standart sistem komutları ile delilleri yok edebileceklerdir. Nitekim bu konuda uygulamalı yapılan eğitimlerde delil olarak düzenlenmiş düzeneğin "DIR" komutu ile yok edildiği gösterilmiştir. Yüksek teknolojik bilgilere sahip olan suçlularca (Bugün artık bilgisayar okur yazarlığına sahip suçlularca) standart program isimleri ve Windows program ikonlarının fonksiyonları değiştirilip yıkıcı ve ortadan kaldırıcı etkilere sahip olundurulabilir.

Bilişim polislerinin kelime işlemcilerden Microsoft Word ve Word Perfect gibi programlara dahi güvenmesi kendi adlarına bir tehlike yaratabilir. Bu programların çalışma

anlayışı; kelime işlemci dosyalar açıldığı ve göründüğü zaman, geçici dosyalar kelime işlemci tarafından oluşturulmaktadır. Bu dosyalar geçici dosyalar üzerine daha önceden potansiyel delil olarak kullanılabilecek bölümlerin üzerine yazar. Bilgisayar delillendirme süreci potansiyel riskler taşıyan bir iştir. Bilgisayar araştırmacılarının omuzlarında bazı kritik materyallerin kayıp olması yada önem arz eden işin devri gibi bir yük yükler. Birçok içsel problem bilgisayar delillerinin üzerinde çalışma sürecinde kayıp olması gibi bir sonuç vermektedir.

Bilgisayar delillendirme de bilgisayarı güvene aldıktan sonra ilk yapılacak şey, bilgisayarın bütün bilgilerinin bitlerini içeren yedeklemesinin (bit stream back up) üzerinde çalışmadan ve tekrar gözden geçirmeden yapılmasıdır. Bilgisayar çalıştırılmadan önce bu işlem normal olarak yapılmalıdır. Bütün suç ile ilgili işlemlerde delillerin sunulması öncelikli iştir, bundan bilgisayar delillendirme işlemini soyutlayamayız. Delillendirmenin bu temel kuralı değişmez. Bütün acemilerde bilir ki bedeli ne olursa olsun deliller adalete sunulmalıdır. Yukarıda da belirtildiği gibi deliller çok yönlü düzeylerde ve farklı bellek konumları içinde bulunabilir. Bu düzeyler tahsis edilmiş dosyalar, silinebilir yada silinmeye uygun dosyaları ifade eder. Hard diskin standart kopyalanmasında bu yeterli olmayabilir. Eğer böyle standart bir yedekleme yapılır ise bilgilerin dosya alanından silinmesi yada bozulması mümkün olabilecektir. Bir alanda delillerin yedeklenmeden üzerinde çalışmak bunları bozabilecek veya üzerinde değişikliklere neden olabilecektir. Standart yedeklemedense bitlerini içeren yedekleme çok daha fazla özenli yedeklemedir. Bit stream yedeklemesi bilgi saklama aracı üzerindeki her bir biti birebir yedekler ve genelde bu işle uğraşanlar orijinal hard diskin iki kopyasını yapmaktadırlar. Hangi süreç denenmek isteniyor ise yedeklenen kopya üzerinde bu işlem yapılabilir. Daha önceden sıkıntı oluşturabilecek delillendirme süreci artık "kolay bir süreç" haline gelir.

Unutulmamalıdır ki; bilgisayar delillendirme sürecinde kullanılabilecek sadece bir tek hak vardır, bunu iyi kullanabilmek ancak kullanılan araçlar üzerinde tam hakimiyet ile olabilir (Anderson, 2002).

A. Bilişim Suçlarının Delilendirilmesinde Program Kullanımı

Amerika' da Federal kanun koruyucuları eğitim seminerindekiler tarafından 1989' da ilk olarak bilgisayar kriminal bilimi kursunda bitleri içeren yedekleme konusu ihtiyacı belirtilmiştir. Paul Mace diye bir şirkette çalışan Micheal White tarafından geliştirilen ilk yedekleme işlem programı "IMDUMP" olarak isimlendirilmişti. Bu program 1991 yılına kadar şirketin programı başka bir şirkete satılmasına kadar delillendirme sürecinde Amerika' da kullanılmaya devam edilmiştir. Daha sonra Sydex Inc. isimli firma bu faaliyete devam etmiştir. Bu şirkette elektronik suç alanı sunumunda devrim yapan "Safeback" isimli programı yapmıştır. "Safeback" bu süreçte birçok devlet gizli servislerinde, askeri servislerde ve kanun adamlarının tüm dünyada yapılan çalışmalarında kullanılmıştır. Normal yedekleme programlarından farklı

olarak "Safeback" hard disk üzerinde bulunan bütün bilgileri kopya etmekte ve sunmaktadır. Bu işlem kötü sektörlerdeki (bad sectors) gizli bilgileri ve CRC (Computer Recycling Center) bilgisayar geri dönüşüm kutusundaki tüm bilgileri yedekler. "Safeback" isimli programın üreticisi olan Sydex isimli (sydex.com, 2002) Amerikan şirketi kendi internet sitesi üzerinden, yönlendirme yapmakta[3] burada bahse konu New Technologies Inc. NTI (Yeni Teknolojiler Şirketi) isimli şirket sayfalarında Amerika' daki askeri ve hukuk ile alakalı kamu kurum, kuruluşları ile Fortune 500' deki büyük şirketlere bilgisayar delilleri bulma, bilgisayar bilgi sızmalarına karşı hizmet verdiğini bildirmektedir. Bu sitenin içerisinde programlar bölümü altında (forensics-intl.com, 2002) "Safeback" ile ilgili iletişime geçilebilecek adresler verilmekte ayrıca dellilendirme ve polisin bu süreçte kullanacağı diğer programlar başlık altında ortaya konmaktadır[4]. Bu suçun delillendirme sürecindeki yeni yaklaşım olan metotlar ile ilgili ciddi bir eğitim süreci gerektiği ortadadır, zaten konu ile ilgili programın satıcısı şirket eğitimlerin verilmesi ile ilgili yönlendirmeleri yapmaktadır.

Bu gibi konularda kanun adamlarına bu kadar yardım edebilecek başka bir program ise yine kanun adamlarınca kolay kullanımından dolayı tercih edilen "Snapback" isimli programdır. Bu program ne yazık ki "Safeback" isimli programdan daha pahalı ve orijinal programı delillendirme süreci için tasarlanmamıştır (Anderson, 2002). Özellikle Windows NT ve Novell Netware server ile ilgili yedekleme yapan program internet sitesinde (snapback.com, 2002) "Gerçek imaj, bütün sistem dosyalarını, registry, açık dosyalar, bilgi bölgelerini kısa zamanda yedekleme yapmaktadır" şeklinde tanıtımını yapmaktadır.

Delillendirme de her aşamada ortaya çıkan yanlış yedeklemede programın bir diğer olumsuz yönüdür. Gerçekte bu program sistem yöneticilerince network ortamında yapılacak yedeklemeler için tasarlanmıştır.

Hard disklerde yapılacak bit stream yedeklemesi ve disketlerde yapılacak standart Dos Diskcopy işlemi olmadan yapılacak delillendirme işi ateş işe oynamak gibidir. Ayrıca bu delillendirme ile ilgili ileride yapılacak talimatlarda bu konunun kesinlikle göz önüne alınması gereklidir. Disket yedeklemelerinde Dos Diskcopy kullanıldığı zaman, DOS' un 6.22 versiyonu kullanılmalı ve /V (Bilgi Doğrulama - Data Verification) parametresi ana dizinde kullanılmalıdır.

Bilgisayarda bulunan verilerin delillendirmesi işleminde kullanılacak program ve dikkat edilecek konular tabi ki bu kadar değildir. Bu konuda ileri teknik eğitim ve araştırmalara ihtiyaç duyulmaktadır.

B. Delillendirmeye Karşı Yapılan Programlar

Amerika' daki serbest piyasa ortamında devletin yaptığı kanuni çalışmalara karşı özel sektörde özel kişi veya kurumlara yönelik özde delillendirmeyi önleyecek makinenin hard diskindeki verilerin, bulunamayacak şekilde, istenilen zamanda ve/veya her makine açılıp kapandığında ortadan kaldıran programları piyasaya sürmüştürler. Bu yapılan çalışmada programlardan Kanıt Kaldırıcı "Evidence Eliminator" ve Siber Silici "CyberScrub" isimli iki program ortaya konmaya çalışılacaktır.

Bunlardan ilk olarak Kanıt Kaldırıcı isimli Siber Silici'den biraz daha profesyonel olan programdan bahsedeceğiz. "Biliyor musunuz devlet ve polis ISP' ler(İnternet servis sağlayıcılar) aracılığı ile sizin internetten indirdiğiniz kanunsuz dosyaları kayıt ediyor ve sizin internette yaptığınız gezinti ve dosya indirimleri kanıt için toplanıyor" başlığı ile programını sunan şirket[5] devamında internet geçici belleği ve tarihi silmenin sizi koruyamayacağı bilgisayarınızın hala bir delillendirme aracı olabileceğine dikkat çekilerek, bilgisayarınıza format bile çekseniz yıllar sonra bile istenilen bütün bilgilere ulaşılabileceği belirtilerek, tüm bu tehlikelere karşı internet erişiminizi yeni bir bilgisayarmışçasına güvenli ve hızlı yapın sloganı ile Kanıt Kaldırıcı isimli programının sunumunu yapmaktadır. Ayrıca ilerleyen sunumda Amerika' da bütün şirketlerin % 73.5' inin personelin tüm kayıtlarını tuttuğu ortaya konmakta, bu nedenle internetteki dolaşılan yerler ile ilgili kanıt bırakmama için programın kullanımı tavsiye edilmektedir[6]. Ayrıca programı "The Washington Times" dan "RocketDownload.com" a kadar birçok kurum ve kişi önerileri internet sayfasında ortaya konmaktadır. Fiyatı oldukça pahalı olan program özellikle üst gelir seviyesindeki kullanıcılara yönelik hizmet verdiği düşünülmektedir.

Bir diğer program olan Siber Silici isimli program Kanıt Kaldırıcı programına göre kullanımı biraz daha ev kullanıcısına uygun bulunan amatör bir programdır. "Hassas bilgileri bilgisayarınızdan bir tuşa basarak uzaklaştırabilirsiniz" sloganı ile reklamını yapan program, internete bağlandığınızda bilgisayarda bulunan bütün hareketlerin kaldırıldığı ve arkanızda hiçbir delil bırakmadığınızı belirterek, özellikle rakibi olan Kanıt Kaldırıcı isimli programdan farklı olarak yarı fiyatına aynı hizmetleri verdiğini vurgulamaktadır (cyberscrub.info, 2002).

4. FBI Bilişim Suçlarını Nasıl Soruşturur?

Bu bölümde bilişim suçlarını soruştururken FBI' ın kullandığı izlenen yöntem, politika ve kaynaklar ortaya konmaya çalışılacaktır. Bilgisayar suçları ile ilgili olarak FBI birçok karmaşık teknik programın yanında gittikçe büyüyen bu alanda yeni metotlar ile mücadele etmektedir. FBI' ın resmi merkezi Amerika' nın 41 Eyaletinde karmaşık yöntemler kullanarak bilişim olaylarını tüm dünyada araştırmaya çalışmaktadır. Amerika' da Ulusal Altyapı Koruma Merkezinde (NIPC) özel bir birim ile Amerika' daki meydana gelen bilişim suçları koordine edilmektedir.

FBI bilgisayar kriminal uzmanları yetiştirmeye yönelik, yaptığı çalışma ile Amerika'nın 51 FBI alanındaki memurlarına dijital kanıt elde etme ve sunabilme sertifika programı düzenlemektedir.

Amerika'da FBI dan herhangi bir olay olduğunda istenilecek yardım ile ilgili olarak çeşitli yerlerde bilgilendirme yapılmaktadır. Ayrıca bu konu ile ilgili olarak akıla takılan olası sorularda FBI' ın yerel bürolarına başvurma gibi yönlendirme yapılmaktadır.

A. Bilişim Suçları Araştırmaları

Bilişim suçları kendi içinde iki kategoriye ayrılır; 1- Bilgisayar yardımı ile suç, 2- Hedefi Bilgisayar olan suç.

Bilgisayar yardımı ile suç, bir suç işlerken kullanılan bir alet edevat gibi bilgisayarın bir araç olarak kullanıldığı suçlardır. Bu dolandırıcılık ile bilgileri kayıt etme, hatalı kimlik tanımlama, telif haklarını ihlal ederek kopya yapmak ve dağıtmak, çocuk pornografisi ile ilgili şeyleri toplamak ve dağıtmak, ve diğer suçları yapmayı ifade eder.

Bilgisayar ile işlenen suçlarda hedef diğer geleneksel suçlardaki hedeflere benzemez. Teknoloji kim, ne, nerede, ne zaman ve nasıl sorularının sorulabilmesini zor bir duruma sokmuştur. Böylece geçmişten farklı olarak teknoloji, elektronik ve dijital kanıtların toplanmasını ve yürütülmesini farklı bir şekilde ortaya koymuştur.

FBI bilgisayar suçları ile ilgili birkaç federal kanunu kullanmaktadır. FBI kurbanların her türlü öneri ve isteklerine açık, olarak FBI ve Birleşik Devletler avukatları beklemekte, gerekirse kurbanları önemseyerek çalışmaktadırlar. Amerika' da bilgisayar suçlarında sık sık kullanılan federal yasalar;

18 U.S.C. 875 Devletler arası iletişimler: Tehdidi , adam kaçırmayı, fidye istemeyi, zorla almayı kapsayan.

18 U.S.C. 1029 Erişim Aygıtlarına Sahip Olma
18 U.S.C. 1030 Bilgisayara Hile Ve Bununla İlgili Aktivitelerle Sahip Olma
18 U.S.C. 1343 Kablo, Radyo veya Televizyon ile hile yapma

18 U.S.C. 1361 Devlet Mülkiyetine Zarar
18 U.S.C. 1362 Devlet İletişim Sistemleri
18 U.S.C. 1831 Ekonomik Casusluk Kanunu
18 U.S.C. 1832 Ticari Sırlar Kanunu

Ayrıca her bir federe devlet bilgisayar suçları ile ilgili değişik kanun ve prosedürlere sahiptir (CERT Coordination Center, 2002).

5. Ülkemizde Bilişim Suçlarının Delillendirilmesi

Ülkemizde bilgisayar ve bilgisayar ile işlenen suçlarda yaklaşım Bilişim Şurası raporundaki "Kamu kurum ve kuruluşlarında bilgi işlem birimlerinin kurulmasının ya da eğer mevcutsa bu (veya benzer) birimlerin kamuda Bilişim Teknolojisi kullanımı konusundaki çalışmalara katılım açısından yetkili ve sorumlu oldukları yönünde yasal düzenleme yapılmalıdır" (bilisimsurasi.org.tr, 2002: 300) şeklinde iyi niyetli isteklerden öteye geçememekte ve yasal düzenlemenin yanında yapının yeniden ele alımının yapılmaması, delillendirme de klasik yöntemler ile suç ve suçlu araştırılmaktadır. Bu noktada da ileri teknoloji bilgi ve aracına sahip olan suç ve suçlu ile mücadelede delillendirilme ne yazık ki iyi yapılamamaktadır.

Örnek olaylarda yapılan tahkikatlarda polis elde edilen suç vasıtası olan bilgisayar üzerinde görünen, silinmemiş, verileri tespit edip bunların yazılı olarak kağıttan çıktılarını adalete sunmakta ise de delillendirme de esas olacak yer, zaman, kullanıcı vb. gibi tespitlerin ileri teknoloji ürünü olan programların kullanılmaması dolayısı ile tespiti tam yapılamamakta böylelikle suç ile mücadelede suçu işleyenler duruma göre adalet karşısında güçlü duruma düşülebilmektedirler.

Özellikle silinmiş veya üzerinde işlem yapılmış verilere ulaşma ile ilgili polisin yasal ve teknik anlamda yetkisi ve bilgisi tam olarak bulunmamaktadır.

Sonuç

Çalışmamıza ortaya koyduğumuz delillendirme sistemi Amerikan uygulamasında gördüğümüz yeni bir alan olmasına rağmen 1980' li yılların sonunda başlayan bilgisayar suçlarının delillendirilmesi yol ve yöntemi ile ilgili çalışmalar, ne yazık ki bizde daha yeni gelişmekte olan bir alandır. Özellikle hukuk sistemimiz içerisindeki aktörlerin kaynak ve eğitim sıkıntıları bu süreçte karşılaşılan en önemli problemlerdir.

Yapılacak çalışmalarda yeni gelişen sistem ve tekniklere uygun esnek yapıda örgüt ve çalışma sistemlerine ihtiyaç vardır. Amerika uygulamasından da gördüğümüz kadarı ile artık bilişim sektöründe teknik ve bilgi üretenler her alandaki hakimiyeti sağlayacaklardır. Bu neden ile oluşturulacak sistemlerde eğitim, proje üretme ve uygulama iç içe olmalı Amerikan yapısına göre daha çok devletçi olan yapımızda tüm kamu kuruluşlarının ve gerekli ise bu konuda esnek olarak özel sektörün katılımının da sağlandığı birliktelikler oluşturulmalıdır. Bu konuda Amerika' da var olan ve Federal birimler ile birlikte çalışan Bilgisayar Güvenlik Enstitüsü (CSI)[7] gibi birimlerin yapıları ile ilgili çalışmaların bu konudaki düzenlemelere ışık tutabileceği görüşündeyiz.

Bu gün artık teknolojinin sınır tanımamazlığı ile globalleşen dünyada süper teknolojilere bir tıklama ile erişilmekte, gerektiğinde istenilmeyen delil olabilecek suç unsurları bir program yardımı ile hemen ortadan kaldırılmaktadır. Böyle bir ortamda yapılacak çalışmalarında paradigmaları oluşturarak temeli sağlam bir yapı geliştirmek gerekmektedir.

Hukuk sistemimizin aktörlerinden en önemlisi olan polisin, çağın gerektirdiği her türlü teknik bilgiye erişmek zorunluluğunda, suç ve suçlunun delil yolu ile tespiti için gerekli tüm teknik hazırlığı yapması beklenir. Polisin yapacağı çalışmalardaki becerisi önümüzdeki yıllarda muhtemelen artması beklenen bilgisayar ile ilgili suç türlerindeki olayların çözümünde önemli rol oynayacaktır. Çalışmamızın bu alandaki boşluğa ışık tutmasını diliyoruz.

Kaynakça

WIDDISON, Robin (1997), "Electronic Law Practice: An Exercise in Legal Futurology", Modern Law Review, N: 60, ss.143-163.

Türkiye Bilişim Şurası (2002), "Türkiye Bilişim Şurası Raporu 10-12 Mayıs 2002-Ankara, http://www.bilisimsurasi.org.tr/home.php?golink=rapor, (18.08.2002), s.293-300.

BRENNER, Susan W.(2001), "Is There Such a Thing as "Virtual Crime"?", California Criminal Law Journal, S.1.

ANDERSON, Michael R.(19.05.2002), "Computer Evidence Processing The Third Step - Preserve the Electronic Crime Scene", **http://www.forensics-intl.com/art7.html**., (02.06.2002).

(http://www.forensics-intl.com/suite6.html, 24.08.2002)

(http://www.evidence-eliminator.com/product.shtml, 24.08.2002)

CERT Coordination Center(2002), "How the FBI Investigates Computer Crime", http://www.cert.org/tech_tips/FBI_investigates_crime.html., (19.05.2002).

(http://www.cyberscrub.info, 24.08.2002)

(http://www.snapback.com, 24.08.2002)

(http://www.sydex.com, 24.08.2002)

[1] Özellikle bu konu daha popüler olarak Amerika ve Avrupa'da ele alınmakta ise de ülkemizde bu tip çalışmalar yeni başlamıştır.

[2] Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun, Basın Kanunu, Gelir Vergisi Kanunu ile Kurumlar Vergisi Kanununda Değişiklik Yapılmasına Dair Kanun, K.N. 4756, T. 21.05.2002. Bkz., RG. 15.05.2002, S. 24761, Md. 26(Ek Md.9). "EK MADDE 9. – Bu Kanunun yalan haber, hakaret ve benzeri

fiillerden doğacak maddî ve manevî zararlarla ilgili hükümleri, bilişim teknolojileri ve internet ortamında sayfa açılması veya elektronik gazete, elektronik bülten vb. suretiyle yayınlanan her türlü yazı, resim, işaret, sesli veya sessiz görüntü ve benzerleri hakkında da uygulanır."

[3] http://www.forensics-intl.com/ isimli internet sitesine yönlendirme yapılmaktadır.

[4] CRCMD5 isimli program bir yada iki dosyanın içeriğini göstermekte, DiskScrub isimli program harddiskten aranılan konular ile ilgili bilgileri bulmakta, DiskSig isimli program harddisk imaj yedeklemesi yapmakta, FileList isimli program bilgisayar kullanım zamanları cetveli hazırlayan program, Filter_I isimli program aranılan bilgi ile ilgili mantıksal filitre kullanarak çalışan program, GetFree isimli program ayrılan bilgileri toplamaya yarayan program, GetSlack isimli program gelişi güzel dağılan dosyaları toplamaya yarayan program, GetTime isimli program bilgisayar sistem zamanını tespit etmeye yarayan program, Graphics Image File Extractor isimli program çocuk pornografisi ile ilgili resimleri kontrol eden program, Net Threat Analyzer isimli program internet analiz programı, internet hesabi ile yapılan kötü kullanımları tespite yarayan program, NTI-Doc isimli program kayıt edilen dosyaların tarih, zamanı, uzantılarını kayıt etmeye yarayan program, Seized isimli program delil olarak kullanılan bilgisayarın güvenliğe alımı ve kilitlenmesi ile ilgili kullanılan program, Text Search Plus verilen anahtar kelimeyi diğer ürünlerden daha hızlı bulan program gibi bilgisayar delillendirme sürecinde kullanılabilecek programlar ortaya konmuş olsada burda konumuz dağılacağı endişesi ile bahse konu programların detayına girilmediği gibi zaten bu programlar ile ilgili detay bilgiler için bu programları satan şirket ile iletişime geçip belli bir süreci tamamladıktan sonra bilgilere erişilebilmektedir.

[5] http://www.evidence-eliminator.com.

[6] Konu ile ilgili Bkz. http://www.evidence-eliminator.com/product.shtml, 24.08.2002. Çalışmanın yapıldığı tarihlerde programın Amerika şatış fiyatı 149.95 Dolardır.

[7] 1974 yılında Bilişim güvenliği Profesyonelleri tarafından San Fransisko 'da kurulmuş bulunan danışma birimidir. Dünya çapında binlerce üyesi olan ve değişik geniş çaplı bilgi veren ve uygulamadakilere eğitim veren, kamu ve özel örgütlere bilginin korunması ile ilgili olarak yardım eden bir örgüttür. FBI'da suç olarak ekonomik altyapı sistemlerine ve büyük bilgi sistemlerine zarar verebilecek şahıs veya gruplara yönelik olarak FBI' ın merkezinde Milli Altyapı Koruma Merkezi(NIPC), Bölgesel Bilgisayar Sistemlerine Yönelik Saldırı Timi adında Amerika'nın baştan sona bölgelerinde seçilmiş memurlardan yapılanmış teşkilat oluşturmuştur. NIPC Federal Devlet Daireleri ve özel Endüstri ile birlikte Milli altyapıya yönelik saldırılar ile mücadele etmek ve devletin yönetim mekanizmasının bu alanda etkinliğini sağlama amaçlı olarak düzenlenmiştir. (Bu altyapı Telekominikasyon, Enerji, Ulaşım, Bankacılık ve Finans, İlkyardım Servisleri ve İşletimsel Devlet Kuruluşları). Bölgesel Bilgisayar sistemlerine saldırı timi Bilgisayar Dolandırıcılığı ve Kötüye Kullanma Kanununa göre Korsan bilgisayar yazılımı ve diğer suç vasıtaları ile halka açık network sistemlerine izinsiz girenlere, özel alana müdahale edenlere, büyük bilgisayar networklerine izinsiz girenlere, endistüriyel casusluk yapanlara yönelik soruşturmalarını yapar.