

DİJİTAL DELİL ARAŞTIRMA SÜRECİ

Yusuf UZUNAY
Ankara Emniyet Müdürlüğü
Bilgi İşlem Şube Müdürlüğü
Ankara, Türkiye
yuzunay(at)ankara.pol.tr

Özet. Bilgi üretimi ve paylaşımının önemi gittikçe daha iyi anlaşılmakta ve bunun bir sonucu olarak da bir çok bilişim teknolojisi karşımıza çıkmaktadır. Günümüzde mevcut iş ve iş süreçlerinin çoğunun bu teknolojiler üzerine kayması, suçluların da ilgisini çekmiş ve bilişim suçları kavramını ortaya çıkarmıştır. Dijital deliller ise bir bilişim suçunun çözümlenmesi ve yargılanmasındaki en önemli noktadır. Dijital deliller, yapı itibarıyla çok kolay bir şekilde bozulabilmekte veya değiştirilebilmektedir. Dolayısıyla bu delillerin araştırılmasında belirli prosedür ve standartları barındıran süreçlere ihtiyaç vardır. Bu makalede, dijital delillerin nasıl araştırılacağına dair bir süreç modeli incelenecek olup, dijital delillendirme anlamında dikkat edilmesi gereken noktalar vurgulanacaktır.

Anahtar Kelimeler: Bilişim Suçları, dijital delil, dijital delillendirme, dijital delil araştırma süreci

1 GİRİŞ

Bulduğumuz çağ bilgi ve bilişim çağı olarak adlandırılırken, günümüzde bilişim devrimi sanayi devriminden daha sık telaffuz edilen bir kavram olarak karşımıza çıkmaktadır. Teknolojideki son gelişmeleri takip edip, bu bağlamda bilgiyi ön plana çıkararak devletler, diğerlerinden daha ön plana gelmişlerdir.

Teknolojik gelişmelerin en büyüğü olarak görülen internet, bilginin hazırlanması, işleyişi, paylaşımı ve pazarlanmasında çok büyük rol oynamıştır. İnternet üzerinden işleyen bilginin miktarı ve değerinin artması, bütün dünya ile çok kısa bir sürede bağlantı kurulabilmesi, suçluların da ilgisini çekmiş ve internete yönelmelerini sağlamıştır. Bu yeni dünyaya çok hızlı adapte olan suçlular, kendilerini teknoloji alanında da hızlı bir şekilde geliştirmiş, normal yollar ile oldukça zor gerçekleşecek suçları, internet ortamından kolay bir şekilde yapabilmeye başlamışlardır. Bu suçlar günümüzde bilişim suçları, bilgisayar suçları, ileri teknoloji suçları gibi bir çok kavramla ifade edilmektedir. Makale kapsamında daha çok bilişim suçları kavramı kullanılacaktır.

Bilişim suçları şuanda, bütün dünyayı tehdit eden en büyük meselelerden biri olarak görülmektedir. Bu nedenle bir çok ülkenin polis birimleri altında, konu ile ilgili özel birimler oluşturulmuştur.

Bilişim suçları, çok kapsamlı bir konu olduğu için bir çok tanım ve sınıflandırma ile karşılaşmak mümkündür. Tanımlardan bir tanesini ele alırsak; *ceza kanununu*

2. Polis Bilişim Sempozyumu, Nisan 2005, Ankara

ihlal eden, işlenmesinde, veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu olarak tanımlanmaktadır (USDOJ, 2004).

Suçların açığa çıkarılması ve yargılanması için delillendirme şarttır. Bilişim suçları kapsamında ise fiziksel delillerden ziyade, dijital deliller daha büyük bir önem arz etmektedir. Dijital delillerin doğru bir şekilde toplanması, analiz edilmesi ve mahkemeye sevk edilebilmesi için bazı standart prosedürler izlemek şarttır.

Bu makalede öncelikle dijital deliller ve bu bağlamdaki bazı önemli noktalar ve mevcut sıkıntılar kısaca incelendikten sonra, bir bilişim suçu ile ilgili dijital delilleri ortaya çıkarmak için gerekli olan araştırmalar, bir süreç modeli içerisinde incelenecek ve son bölümde sonuç ve önerilere değinilecektir.

2 DİJİTAL DELİLLER

Dijital deliller, dünya için oldukça yeni bir kavramdır. Özellikle bilişim suçlarındaki yoğun artıştan sonra, bilimsel alanda da çok yoğun tartışmaların odak noktası olmuş olan dijital deliller hakkında, farklı tanımlamalar mevcuttur.

Shinder'e göre "*bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil*" denilmektedir (Shinder, 2002).

Chisum ise dijital delilleri "*bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler*" olarak tanımlamıştır (Chisum, 1999).

Son olarak Casey'in tanımına bakarsak dijital deliller "*bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler*" olarak karşımıza çıkmaktadır (Casey, 2000).

Dijital delil kaynakları göz önünde bulundurulduğunda, bilişim sistemleri açısından üç farklı grup düşünülebilir (Henseler, 2000):

- 1- *Açık Bilgisayar Sistemleri:* Harddisk, klavye, monitör gibi aygıtlardan oluşan dizüstü, masaüstü, sunucu gibi herkesin bildiği klasik bilgisayar sistemleri, artan kayıt alanlarıyla dijital deliller yönünden oldukça zengin bir kaynak teşkil etmektedir. Bu sistemlerin üzerinde, basit olarak görünen bir dosya, oluşturulma zamanı, değiştirilme zamanı ve kim tarafından oluşturulduğu gibi bazı özellikleriyle suça yönelik önemli bilgiler barındırabilmektedir.
- 2- *İletişim Sistemleri:* Geleneksel telefon sistemleri, kablosuz haberleşme sistemleri, internet ve bilgisayar ağları gibi bir çok iletişim sistemi üzerinde, oldukça fazla dijital delile rastlamak mümkündür. Örneğin internet üzerinden gönderilmiş bir e-posta mesajındaki gönderilme

2. Polis Bilişim Sempozyumu, Nisan 2005, Ankara

zamanı, kimin gönderdiği, mesajın içeriği gibi konular, delillere ulaşma noktasında oldukça büyük önem arz ederken, mesajın geçtiği sunucular, yönlendiriciler gibi aradaki sistemlerin üzerindeki kayıtlar da, ele geçirilen mesaj ile ilgili bazı hususları doğrulama noktasında, pekiştirici bilgi olarak kullanılabilir.

- 3- *Gömülü Bilgisayar Sistemleri*: Mobil telefonlar, PDA cihazları, akıllı kartlar gibi gömülü bilgisayar sistemlerinin bir çoğu, dijital delillere kaynak teşkil edebilmektedir. Örneğin GPRS, GPS gibi sistemler, araçların nerede olduğunun tespiti için kullanıldığı gibi, araçların üzerine yüklenecek gömülü bilgisayar sistemine sahip modüller sayesinde aracın hızı, frenlerin durumu, etkiden önceki 5 saniye içerisindeki işlevler gibi bir kaza esnasında oldukça yararlı ve kazayı aydınlatıcı bilgilere ulaşılabilir. Günümüzde, gömülü bilgisayar sistemlerine sahip mikro dalga fırınlar, internet üzerinden bilgi alışverişi yapabilmekte ve bazı ev aygıtları, kablosuz ağ veya internet kullanılarak uzaktan kumanda edilebilmektedir. Teknolojinin bu seviyede olduğu bir ortamda, mikro dalga üzerinden elde edilecek veriler, bir kundakçılık olayında fırının belirli bir zamanda yangın çıkarmak için programlandığını ortaya çıkarabilmektedir.

Günümüzde bilgisayar sistemlerine kayıt edilmiş veya bilgisayar sistemleri kullanılarak iletilmiş verilerle ilişkisi olmayan çok az suç kalmıştır. Bu yüzden dijital deliller sadece bilişim suçları kapsamında değil adam öldürme, cinsel saldırı, kayıp şahıslar, çocuk tacizi ve uyuşturucu gibi bir çok olayın aydınlatılmasında da kullanılabilir. Bu makale çerçevesinde konuyu çok fazla dağıtmamak için dijital delillerin daha çok bilişim suçları içerisindeki boyutu ele alınacaktır.

Dijital delilleri ele almak oldukça meşakkatli bir iştir. Örneğin harddisk içerisinde dağılmış bir e-mail mesajının parçalarını bulup birleştirmek, tercüme etmek ve anlam vermek bir DNA analizi kadar zordur denilebilir (Casey, 2004). Dijital deliller, yapı itibarıyla, fiziksel delillere göre daha hassas ve kolay bozulur nitelikte oldukları için bir çok sıkıntıyı içlerinde barındırmaktadırlar. Dijital delillerin, mahkeme esnasında gerçek delil özelliği gösterebilmesi için delillerin bütünlüğünün, doğrulanmasının, inkar edilememesinin, doğruluğunun ve daha sonradan ele alınabilirliğinin sağlanması gerekir (Hosmer, 2002). Bu noktada çözüm olarak genellikle kriptografik teknikler kullanılmaktadır (Örneğin, MAC, Hash, Dijital İmza, Dijital sertifika v.b). Fakat bu teknikler dijital delillere kesinlik kazandırma yönünde ne yazık ki yeterli gelmemektedir (Uzunay ve Koçak, 2005). Örneğin günümüzde adını çok sık duyduğumuz dijital imza ve doğru bir şekilde uygulanabilmesi için gerekli olan açık anahtar alt yapısı ile ilgili bazı sorunlara göz atalım :

- Güvenilir sertifika otoritesi bulunması gerekmektedir.
- Bilişim suçu küresel bir kavramdır ve bu suçlarda dijital imzanın delillendirmede kullanılabilmesi için dünyadaki bütün sertifika otoritelerinin birbirleriyle iletişim kurabilmesi ve bu iş için ortak protokol ve kanunların düzenlenmesi gerekir.

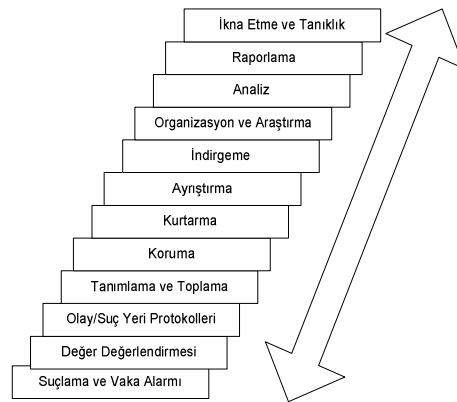
2. Polis Bilişim Sempozyumu, Nisan 2005, Ankara

- Sertifikanın süresinin dolması anında yapılacak işlemlerde bazı problemler bulunmaktadır.
- Sertifikanın nasıl iptal edileceği, önemli konulardan biridir.
- Kapalı anahtarın başka bir kişi tarafından ele geçirilmesi, sistemi tamamen etkisiz kılmaktadır.
- Bir dosya sistemi üzerine kayıt edilmiş anahtar, dosya sisteminin güvenliği ölçüsünde güvenlidir.
- Eğer anahtar şifreli halde saklanıyorsa, anahtar güvenliği şifreleme algoritmasının güvenliğine eşittir.
- Virüsler, Truva Atları, Arka kapılar gibi zararlı kodlar bilgisayar üzerinde, kullanıcının bilgisi dışında işlemler gerçekleştirebilmekte ve hatta kullanıcının kendi ekranından okuyup onayladığı dosyalar ile gerçekte imzalanan dosyalar birbirinden farklı olabilmektedir. Örneğin bir e-sözleşmeyi ele alırsak 100 000\$'lık bir sözleşme virüsler tarafından değiştirilip, kullanıcıya 100\$ şeklinde görüntülenebilir ama asıl imzalanan sözleşme 100 000\$'dır.

Dijital delillerdeki bu sıkıntılar çeşitli ortamlarda tartışılmakta olup, hala kesin bir çözüm bulunamamıştır. Örneğin Maurer dijital delillere ek olarak, **dijital bildirimlerin** de kullanılabilirliğini vurgulamıştır (Maurer, 2004). Bu bir nevi soyut delillere, bir şekilde fiziksel bir yön kazandırarak daha gerçekçi deliller elde etme çabası olarak düşünülebilir.

3 DİJİTAL DELİL ARAŞTIRMA SÜREÇ MODELİ

Dijital delilleri belirli metot ve prosedürlere uygun olarak araştırabilmek için bir takım ortak süreçlere ihtiyaç duyulmaktadır. Bu bölümde Casey'in oluşturduğu, şekil 1'de görünen 12 basamaklı süreç modeli incelenecektir (Casey, 2004).



Şekil 1: Dijital Delil Araştırma Süreç Modeli (Casey, 2004)

3. 1 Vaka Alarmı ve Suçlama

Her sürecin bir başlama noktası vardır. Dijital delil araştırma süreç modelinde ise başlama noktası, saldırı tespit sisteminden gelen bir alarm, sistem yöneticisinin ateş duvarı kayıtlarını gözden geçirmesi ve şüpheli kayıtlara rastlaması, ağ içerisindeki çeşitli güvenlik sistemlerinden gelen uyarılardan bir tanesi olabilir. Hukuksal açıdan değerlendirildiğinde ise, bir kişinin ihbarı üzerine araştırma başlatılabilmektedir.

Bir ihbar veya alarm alındığında bilginin kaynağı ve güvenilirliği önem arz etmektedir. Örneğin ekranındaki nesnelerin hareket ettiğini ihbar eden bir kullanıcının bilgisayarına, virüs bulaşmış olabilir veya saldırı tespit sistemi tarafından "saldırı var" şeklinde üretilen bir alarmın teşebbüs edilmiş ama geçerli olmamış bir saldırı olduğu tespit edilebilir. Dolayısıyla bu aşamada, kaynağın iyi anlaşılması ve aynı zamanda sayısal verilerin yanı sıra, insan faktörünün de göz önünde bulundurulması gerekir.

Bir suçlama veya alarmı değerlendirirken, geniş çaplı bir inceleme başlatılmadan önce bazı ön bilgilerin toplanması faydalı olacaktır. Bilgisayar alanında çalışan teknik insanlar bile bazen normal bir sistem davranışını, saldırı olarak algılayabilmektedir. Olay ile ilgili kişilerle görüşme ve olayı yerinde kontrol etme, bu tip yanlış anlamaları engelleyecek, vakaya karşı gerekli ve doğru tepki vermeye yönlendirecektir. Bu basamak, üzerinde hassasiyetle durulması gereken bir basamaktır. Çünkü olay mahallindeki en ufak bir yanlış hareket, delillerin yok olmasına veya bozulmasına neden olabilmektedir. Dolayısıyla herhangi bir yetkilendirme, hazırlık ve bir takım prosedürler yerine getirilmeden bu tip girişimlerde bulunulmamalıdır.

3.2 Değer Değerlendirmesi

Bilişim suçları ile ilgili yapılmış olan en ufak bir ihbar bile, göz ardı edilemez. Bütün ihbarlar değerlendirilmek zorundadır. Değer değerlendirme safhasında, genel olarak problemin önemi belirlenmeye çalışılır. Örneğin mevcut konunun fiziksel zararlara, önemli kayıplara, daha büyük sistem ihlallerine veya bozukluklarına neden olabilecek riskleri taşıyıp taşımadığı gibi noktalar üzerinde durulur. Eğer problem çok hızlı bir şekilde oluşmuş, çok az derecede veya hiç zarara neden olmamış ve geleceğe yönelik de durumu daha kötüye götürecek riskler oluşturmadan sona ermişse, araştırmaya daha fazla devam etmeye gerek duyulmadığı kanaatine varılabilir.

3.3 Olay/Suç Yeri Protokolleri

Geniş çaplı bir araştırma başlatılmadan önce, ilk olarak olay yerindeki mevcut dosyaların (dijital veya değil) bütünlüğü ve durumu belgelendirilmelidir. Herhangi bir hataya sebebiyet verilmemesi için ilgili protokoller ve prosedürler belirlenerek

2. Polis Bilişim Sempozyumu, Nisan 2005, Ankara

gerekli pratik ve hazırlıklar yapılmalıdır. Olay yerinin güvenliğinden kimin sorumlu olduğu, ilgili protokolleri izleyecek olan ilk müdahale ekibinin ve adli bilişim analizcilerinin eğitimine gerek olup olmadığı gibi hususlar belirlenmelidir. Protokoller sağlık ve güvenlik konularını, yetkilileri bilgilendirmeyi ve olay yerinin güvenli hale getirilmesi için neler yapılması gerektiğini kapsar.

Bu aşamanın asıl amacı olay yerindeki ilgili nesnelerin kayıt edilmesi, değişik açılardan fotoğraflarının çekilmesi ve çeşitli diyagramlar çizilmek suretiyle suç sahnesinin durumu ile ilgili araştırmacılara suçtaki potansiyel elemanları tanıtmak, potansiyel elemanları belirlemek ve yol gösterici bilgiler vermektir.

3.4 Tanımlama ve Toplama

Olay yeri güvenli hale getirildikten sonra, söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak büyük önem arz etmektedir. Deneyimli ve tecrübeli araştırmacılar için bu safhadaki amaç sanal veya fiziksel bütün delilleri toplamak değil, nelerin toplanıp nelerin toplanmayacağı konusunda mantıklı kararlar vermek, doküman oluşturmak ve ondan sonra eylemi gerçekleştirmektir.

Dökümantasyon bütün basamaklarda yapılması gereken bir iştir ancak delillerin toplanması esnasında ayrı bir öneme sahiptir. Toplanan her bir delille ilgili ayrıntılı rapor tutmak, bunların doğrulanabilirliğini kolaylaştırıp, koruma zincirini (chain of custody) başlatacaktır.

Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazılarının kaybedilmesi, bozulması ile karşılaşılabilir. Özellikle uçucu veriler (Ör: Bellek, CPU Kaydedicileri, Çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delilleri barındıran bilgisayarlarda bazı ek işlemlerin gerçekleştirilmesi gerekmektedir.

İngiltere Polis Başkanları Birliği tarafından yayınlanan "Bilgisayar Tabanlı Elektronik Deliller için İyi Pratikler Rehber"inde 4 prensipten bahsedilmiştir (NHCTU,2003):

Prensip 1 : Kanun uygulayıcılar ve görevlileri tarafından, mahkemede kullanılma ihtimali olan bilgisayar veya farklı bir medya üzerinde bulunan verileri değiştirecek herhangi bir eylemde bulunulmayacaktır.

Prensip 2 : Bir kişinin hedef sistem üzerinde bulunan orijinal verilere erişmesi gerektiği istisnai durumlarda, ilgili kişinin mutlaka o konuda tecrübeli ve uzman olması ve aynı zamanda yaptığı bütün işlemleri ve gerekçelerini daha sonradan ispatlayacak bir durumda olması gerekir.

2. Polis Bilişim Sempozyumu, Nisan 2005, Ankara

Prensip 3 : Bilgisayar tabanlı delillere uygulanmış olan bütün süreçlerin bir izleme kaydı oluşturulmalı ve koruma altına alınmalıdır. Üçüncü bir şahıs tarafından bu süreçler incelenebilmeli ve aynı sonuçlara varılmalıdır.

Prensip 4 : Olaydan sorumlu memur, yapılan işlemlerin hukuka ve prensiplere uygun olup olmadığını denetlemekten de sorumludur.

3.5 Koruma

Deliller üzerinde çalışan araştırmacıların dikkat edeceği en önemli husus, olay yerinden alınan delillerin bozulmadan mahkeme esnasına kadar korunmasıdır. Bu safha iki farklı alanda düşünülebilir. Bunlar dijital olarak koruma ve fiziksel olarak korumadır (Uzunay ve Koçak, 2005). Dijital olarak koruma, delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak çeşitli mekanizmaları kapsar. Bu işlem genellikle kriptografik teknikler kullanılarak gerçekleştirilir. Fiziksel olarak koruma ise delillerin incelenecek yere bozulmadan taşınması, mahkeme esnasına kadar uygun ortamlarda saklanması ve yine mahkemeye gidiş esnasında her hangi bir bozukluğa uğramamasını içerir. Deliller mümkün olduğunca toplandığı ortam koşullarına benzer ortamlarda taşınmalı veya saklanmalıdır. Unutulmaması gereken başka bir nokta toplanan bütün delillerin etiketlenerek, uygun şekilde paketlenildikten sonra mühürlenmesidir (Shinder, 2002).

3.6 Kurtarma

Korunmuş dijital deliller üzerinde tam bir analize başlamadan önce, silinmiş, gizlenmiş, şekli değiştirilmiş veya mevcut işletim sistemi veya dosya sistemi ile görüntülenemeyen verilerin ortaya çıkarılması gerekmektedir. Buna *verilerin kurtarılması (Data Recovery)* denir. Bu işlem mümkünse orijinal deliller üzerinde değil, bire bir kopyaları üzerinde gerçekleştirilmelidir. Amaç normalde görünmeyen fakat bir olayın aydınlatılmasında dijital delil özelliği gösterebilecek, soruşturmaya yön teşkil edebilecek önemli verilere ulaşmaktır.

3.7 Ayırıştırma

Bu safhanın başlangıcında, bir vaka ile ilgili potansiyel bütün dijital deliller araştırılmaya hazır durumdadır. Soruşturma ile ilgili veriler bir araya toplanır. Bu safha asıl detaylı incelemenin başladığı safhadır. Araştırma takımı tarafından öne sürülen hipotezler doğrulanır veya çürütülür. Böylelikle artık soruşturma bir şekil almaya başlar. Amaç daha sonraki araştırmalara kolaylık sağlaması için verileri belirli özelliklerine göre bir araya toplamaktır. Örneğin çocuk pornografisi vakaları genellikle görsel dijital verilere dayandığı için bu kategoride bir suç araştırılırken genellikle uzantısı gif, jpeg ve benzeri olan dosyalar bir araya getirilir.

3.8 İndirgeme

Toplanan veriler arasında konu ile doğrudan ilgili olanlara yönelip, ilgisiz olanları elimine etmeye indirgeme diyebiliriz. Bu aşamada nesnenin geneli değerlendirilir, içeriği ve kapsamı çok fazla düşünülmez. Dikkat edilmesi gereken husus elemelerin hangi kriterlere göre yapıldığıdır. Bu kriterlerin mahkeme esnasında sorgulanabileceği düşünülerek, büyük bir titizlikle içerisinde çalışmalar sürdürülmelidir.

3.9 Organizasyon ve Araştırma

Doğru bir analiz gerçekleştirmek için bir önceki basamakta indirgenmiş verileri organize etmek, gruplamak, etiketlemek ve anlamsal birimlere yerleştirmek gerekir. Bu aşamanın ana amacı araştırmacıların analiz aşamasında verileri bulup tanımlamasını, tanıklık esnasında bu verilere anlamlı bir biçimde referans vermesini sağlamaktır. Ayrıca yine bu safhada materyallere verimli bir şekilde ulaşılmasını, ilgili, ilgisiz ve ayrıcalıklı materyalleri tanımlamaya yardımcı olması amacıyla, araştırılabilir bir veri indeksi oluşturulur.

3.10 Analiz

Bu safha, önceki aşamalarda elde edilen verilerin ayrıntılı bir şekilde incelenmesini içerir. En çok teknik bilgi gerektiren safhadır ve bilgisayar adli tıbbi uzmanları tarafından gerçekleştirilir. Analiz safhasını dört aşamada ele alabiliriz; Öncelikle insan tarafından okunabilir dijital veri nesnelere içerdiği incelenerek bazı anlamsal verilere ulaşılabilir. Bu aşamaya *Değerlendirme* aşaması denir. Daha sonra *Deney* aşaması gelmektedir. Araştırma esnasında bazı metotların uygulanmasını kapsar. Tabii bu metotların bazı standart ve prosedürlere uyması ve ayrıntılı bir şekilde dökümente edilmesi şarttır. Araştırma esnasında dijital ve dijital olmayan birçok kaynaktan veri toplanmaktadır. Sadece dijital deliller bütün hikayeyi aydınlatmaya yetmeyecektir. Tersine de yani sadece dijital olmayan delilleri de kullanmak yeterli gelmemektedir. Anlamlı sonuçlara ulaşabilmek için verilerin bir araya getirilmesi önem arz eder. Buna *Birleştirme* denir. Örneğin olayların oluş sırasına göre kronolojik bir sıraya sokulması konu ile ilgili aydınlatıcı ip uçları verebilmektedir. Birleştirme esnasında verilerin içerik olarak da birbirleriyle ilişkili olup olmadığının incelenmesi ise *Korelasyon* olarak adlandırılır. Son aşama olarak *Onaylama* gelir. Kısaca analiz safhasının çıktısı ve sonucudur denilebilir. Bulgular pozitif delil olarak ilgili birimlere gönderilir.

3.11 Raporlama

Araştırma sürecine şeffaf bir görünüm kazandırmak için, buraya kadar saydığımız safhalarda kullanılan bütün metot ve prosedürlerin önem arz edecek detayları en son hazırlanacak olan final raporlarında mutlaka anlatılmalıdır. Raporun büyük bir kısmı sonuca götürücü analiz ve bunları destekleyen delillerin

tanımlamalarıyla ilgilidir. Destekleyici deliller ve analizler tam olarak ve doğru bir şekilde tanımlanmadan sonuç yazılamaz.

3.12 İkna Etme ve Tanıklık

Bazı durumlarda karar vericiler, bir vakanın sonucuna ulaşmadan önce rapordaki bulguların sunulmasını ve ilgili sorulara yanıt verilmesini isteyebilirler. Üst seviye mühendislik ve teknoloji bilgisi gerektiren konulara, açık ve anlaşılır bir biçimde cevaplar vermek, oldukça büyük bir efor gerektirir. Bu yüzden iyi bir şekilde hazırlanılması gerekir.

4 SONUÇ ve ÖNERİLER

Bilişim suçları oldukça hassas bir konudur ve geleceğe yönelik büyük tehditler oluşturmaktadır. Bu suçlarla mücadele bağlamında bir çok sıkıntı bulunmaktadır. Bu sıkıntıların üstesinden gelebilmek için öncelikle bilişim suçları alanında teknik çalışmalar yapabilecek uzmanların yetiştirilmesi şarttır.

Suçların aydınlatılmasındaki en önemli husus delillendirmedir. Bilişim suçları kapsamında ise dijital deliller söz konusudur. Dijital deliller, yapı itibarıyla çok hassas ve kolay değiştirilebilir veya bozulur nitelikte oldukları için toplanmasında, korunmasında, analizinde belirli prosedür ve metotların izlenmesi şarttır. Olay yerinde yapılabilecek en ufak bir hata delillerin kaybolmasına yol açabilmektedir.

Bu makalede ise bir bilişim suçu ile ilgili dijital delil araştırma süreci, çeşitli basamaklardan oluşan bir model üzerinde incelenmiştir. Bu modeldeki basamaklar her ne kadar birbirini takip eder bir sırada görünse de, birbirleriyle devamlı etkileşim içerisindedir. Daha önceki bir basamaktan kaynaklanan bir sıkıntı sezilirse, ilgili basamağa dönüş yapılarak, işlemler tekrar değerlendirmeye alınır.

Dijital delil araştırma sürecinde kullanılan bütün prosedür ve metotların doğrulanabilir nitelikte olması ve yapılan bütün işlemlerin ayrıntılı bir şekilde belgelendirilmesi, topladığımız dijital delillerin mahkeme esnasında daha fazla ve daha kolay kabul edilebilirliği anlamına gelmektedir.

Geleceğe yönelik olarak bilişim suçları ile uğraşan birimlerin ortak uygulayabilecekleri süreç modellerinin standart hale getirilmesi, özellikle emniyet içerisinde alanında uzman ve konuya hakim kişilerin yetiştirilmesi ve dijital delillerin teknik olarak doğrulanması konusundaki eksikliklerin giderilebilmesi için üniversiteler ile ortak çalışmalar yapıp çeşitli projelerin başlatılması düşünülebilir.

5 REFERANSLAR

- [Casey, 2000] Casey E., Digital Evidence and Computer Crime, 1st Ed., London: Academic Press. 2000
- [Casey, 2004] Casey E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 2nd Ed., Academic Press. 2004
- [Chisum, 1999] Chisum J. W., "Crime Reconstruction and Evidence Dynamics", Presented at the Academy of Behavioral Profiling Annual Meeting, Monterey, CA. 1999
- [Henseler, 2000] Henseler J., "Computer Crime and Computer Forensics" in the *Encyclopedia of Forensic Science*, London: Academic Press. 2000
- [Hosmer, 2002] Chet Hosmer, "Proving the Integrity of Digital Evidence with Time", International Journal of Digital Evidence, Spring 2002 Volume 1
- [Maurer, 2004] Ueli Maurer, "New Approaches to Digital Evidence", Proceedings of the IEEE Vol. 92, No.6 June 2004
- [NHCTU, 2003] United Kingdom Association of Chief Police Officers, "The Good Practices Guide for Computer Based Electronic Evidence", National High-tech Crime Unit, 2003, Sf:6
- [Shinder, 2002] Shinder, D. L., "Scene of Cybercrime – Computer Forensics Handbook", Syngress Publishing, USA, 2002
- [USDOJ, 2004] U.S Department of Justice, FBI Law Enforcement Bulletin, August 2004
- [Uzunay ve Koçak, 2005] Uzunay Y., Koçak M., "Bilişim Suçları Kapsamında Dijital Deliller", AB'05 Akademik Bilişim Konferansı, Gaziantep, Şubat 2005