

ELEKTRONİK DELİLİN TOPLANMASI VE MUHAFAZASI*

COLLECTION AND STORAGE OF ELECTRONIC EVIDENCE

Hakemli Makale

Yusuf BAŞLAR**

İÇİNDEKİLER

GİRİŞ	79
I. ELEKTRONİK DELİL TOPLANIRKEN UYULMASI GEREKEN TEMEL İLKELER	82
II. ELEKTRONİK DELİL TOPLANMASI AŞAMASINDA YAPILMASI GEREKLİ İŞLEMLER	86
A. Canlı Analiz	86
B. İmaj Alma (Birebir Kopyalama).....	88
C. Hash (Veri Bütünlük) Değeri.....	92
D. Zaman Damgası (Time Stamping)	95
E. Koruma Zinciri (Chain of Custody)	98
III. ELEKTRONİK DELİLİN PAKETLENMESİ, TAŞINMASI VE MUHAFAZASI	100
SONUÇ	102
KAYNAKÇA	104

DOI: 10.32957/hacettepehdf.690592

Makalenin Geliş Tarihi: 18.02.2020

Makalenin Kabul Tarihi: 23.03.2020

* Bu makale, “Ceza Yargılamasında Elektronik Delil” isimli doktora tezinden üretilmiştir.
Bu çalışmada Araştırma ve Yayın Etiği'ne uyulmuştur.

** Dr., E-posta: yusufbaslar@hotmail.com.

ORCID: 0000-0003-3575-6345

ÖZ

Elektronik delilin ceza yargılamasında kullanılabilmesi veri bütünlüğünün korunmuş olmasına bağlıdır. Zira bir elektronik delilin veri bütünlüğünün bozulmuş olması onun geçerliliğini de olumsuz etkileyecek ve ispat fonksiyonunun ortadan kalkmasına neden olabilecektir. Bir elektronik verinin bozulmasına neden olabilecek durumların başında ise onun uygun koşullarda toplanmamış ve muhafaza edilmemiş olması yer almaktadır. Bu bakımdan elektronik delilin yapısı itibarıyla hassas özellik arz etmesi ve kolay bozulabilen nitelikte olması bu delilin toplanması sırasında bazı temel ilkelere uyulmasını, delil toplama sürecinde canlı analiz, imaj alma, hash değeri alma, zaman damgası ve koruma zinciri gibi bazı işlemlerin yapılmasını ve toplanan elektronik verilerin uygun şartlarda muhafaza edilmesini gerekli kılmaktadır. Biz de bu çalışmamızda elektronik delilin toplanması ve muhafazası sürecinde uyulması gereken prensipleri ve yapılması gereken işlemleri ele aldık.

Anahtar Kelimeler: Elektronik delil, adli imaj, hash değeri, zaman damgası, adli bilişim.

ABSTRACT

The availability of electronic evidence in criminal proceedings depends on the protection of data integrity. Because the deterioration of data integrity of an electronic evidence would negatively affect its validity and may cause its proving function to perish. One of leading the situations that can cause an electronic data to be corrupted is that it has not been collected and preserved under appropriate conditions. In this regard, the fact that the electronic evidence has a sensitive feature in terms of its structure and that it is easily corruptible requires some basic principles should be followed during the collection of such evidence, some analysis must be conducted such as live analysis, image and hash value taking, time stamp and chain of custody during the collection of evidence and the collected electronic data is required to be kept under suitable conditions. In this study, we discussed the principles and the procedures to be followed during the collection and preservation of electronic evidence.

Keywords: Electronic evidence, forensic image, hash value, time stamping, computer forensic.

GİRİŞ

Elektronik delil toplama süreci hukuka uygun bir zeminde başlamalıdır. Bu bağlamda öncelikle, eğer bir adli soruşturma kapsamında elektronik delil toplanacaksa -ülke uygulamasına göre- arama ve elkoyma öncesinde gerekli hukuksal sürecin işletilmesi ve bu hususta yazılı bir savcılık veya hâkim kararının bulunması gerekmektedir¹.

Bu aşamada, adli kolluk görevlilerinin yapacakları arama işlemlerinde ciddi bir plan dâhilinde hareket etmeleri gerekir. Bu plan yalnızca arama işlemlerinin gerçekleştirilmesiyle ilgili değildir. Söz konusu plan, en başta arama kararı alınırken büyük öneme sahiptir. Soruşturma evresinde, işin başında yapılacak arama planı, alınacak arama kararının kapsamını da belirleyecektir. Arama kararı talebinin ciddi bir plan dâhilinde yapılmaması durumunda ise alınan arama kararına dayalı olarak yapılan arama işlemleri sırasında, çoğu zaman arama kararının kapsamı yetersiz gelmekte bu durum da yeni bir arama kararının istenmesi, yetkisiz arama işlemi yapılması ve arama işlemine son verilerek başarısızlığa neden olunması gibi sorunlara neden olabilmektedir. Belirtmek gerekir ki bu durumda, yeni bir arama kararı istenilmesi en uygun çözüm gibi görünse de arada geçecek zaman nedeniyle, bilişim sisteminin kendine özgü yapısı karşısında, başarı elde edilebilmesi zordur².

Diğer taraftan elektronik delile ilk kimin temas edeceği hususu da son derece önemlidir. Bu hususta ülkeden ülkeye farklılık arz eden bir uygulama söz konusudur. ABD gibi bazı ülkelerde bu tür delillere nasıl davranılması gerektiği konusunda eğitim almış özel birimler (ilk müdahale ekipleri) bulunurken bazı ülkelerde ise bu işi söz konusu hususta yeterince eğitim almamış kolluk personeli (polis memuru) yerine getirmektedir³. Bu

¹ COSIC, Jasmin / COSIC, Zoran, “Chain of Custody and Life Cycle of Digital Evidence”, **Computer Technology and Application**, Yıl: 2012, Cilt: 3, Sayı: 2, s. 127.

² KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2. Basım, Seçkin Yayıncılık, Ankara, 2011, s. 98.

³ COSIC / COSIC, **2012**, s. 127.

bağlamda Türkiye’de de bu işlemlerin yeterli eğitime sahip olmayan kolluk personeli ile gerçekleştirildiği görülmektedir.

Günümüzde bilişim sistemleri suç işlemek için kullanılabilen, suça ilişkin delilleri içerebilmekte ve hatta bazen kendileri suçun hedefi olabilmektedirler. Bu bakımdan olaya ilk müdahale eden personelin elektronik delilin tanınmasında, bulunmasında, korunmasında ve taşınmasında temel bilgilere sahip olması hassas bir yapıya sahip olan elektronik delil için oldukça önemlidir⁴.

Elektronik delil yapısı gereği, dış dünyaya ancak görsel veya işitsel olarak yansıtılabilir. Ancak, elektronik delilin elde edilmesi kolay değildir. Çoğunlukla, incelenen bilişim cihazlarından başka bilişim materyali kullanılarak delil elde edilmeye çalışılmaktadır. Bu nedenle kullanılacak ürünlerin kapsamı ve yetenekleri ölçüsünde delil elde edilebilmektedir. Bu döngünün sorgulanabilmesi için bilişim cihazlarında suça ait iz ve emarelerin bulunabileceği yerlerin iyi bilinmesi ve tüm ihtimaller üzerinde titizlikle durulması gerekmektedir. Bilişim cihazlarındaki elektronik delilin tespiti için en önemli husus, bu cihazların iyi tanınması ve delil olabilecek verilerin iyi bilinmesidir⁵.

Elektronik delilde bilgiler manyetik ortamda yazılarak saklanır. Bu bakımdan suçtaki hedef alanın niteliğine göre elektronik delil elde etme yöntem ve donanımı (programı) da farklılık gösterebilir. Bu karmaşık yapı içerisinde, delillerin toplanmasında yapılacak yanlış bir müdahale işi başarısız kılabilir⁶. Başka bir ifadeyle bu süreçte, kasti veya ihmali bir

⁴ ÖZDİLEK, Ali Osman, **Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku**, Vedat Kitapçılık, İstanbul, 2006, s. 202.

⁵ ÖZTÜRK, Mustafa İlker, **Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s. 55-56.

⁶ KARAGÜLMEZ, Ali, “Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular”, **2. Polis Bilişim Sempozyumu (14-15 Nisan 2005)**, Emniyet Genel Müdürlüğü. Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2005, s. 31.

hareket, aslında bir gerçeğin ortaya çıkarılmasına hizmet edebilecek bir delilin kullanılamaz hale gelmesine neden olabilir⁷.

Adli soruşturma kapsamında toplanan bir elektronik delil yine adli makamlar tarafından muhafaza altına alınmalıdır. Muhafaza aşaması aynı zamanda koruma zinciri (chain custody) oluşturulması sürecini ihtiva etmektedir. Nitekim koruma zincirinin herhangi bir şekilde bozulması elektronik delilin geçerliliği konusunda şüpheye neden olacaktır. Diğer taraftan, muhafaza aşaması elektronik delile kasıtlı zarar vermek isteyen kötü niyetli kişilerden veya kazara zarar verebilmesi muhtemel tecrübesiz personelden güvenli bir şekilde korunmasını da içermektedir.

Elektronik delilin toplanması ve muhafazası aşamasında, delillerin toplanması, delillerin bütünlüğünün sağlanması ve kontrol edilmesi işlemleri yerine getirilmektedir. Aslında bu aşamadan önce veya bu aşamayla birlikte yürütülen bir başka süreç de elektronik delilin belirlenmesi/tespiti sürecidir. Bu süreçte ise nelerin elektronik delil olduğu belirlenerek buna göre delil toplama ve muhafaza işlemi yürütülmektedir⁸.

Elektronik delilin tespiti ve toplanarak muhafaza altına alınmasının kendine mahsus özellikler arz etmesine karşın elektronik delilin araştırılma yöntemleri ile fiziksel delillerin araştırılma yöntemleri birçok yönüyle de benzerlik göstermektedir. Bilişim sistemleri, suçlular tarafından suçun işlenmesinde araç olarak kullanılmaları veya herhangi bir suçun işlenmesinde doğrudan olmasa bile suçluların kendi aralarındaki iletişimi veya işlemleri kolaylaştırmak ve bilgileri yedeklemek için kullanılmaları durumunda adli bilişime konu olmaktadır. Bilgisayar teknolojileri işlenen suçların araştırılmasında kullanılan aygıtlar olabileceği gibi bu cihazların kullanılması ile de birçok suç işlenebilmektedir⁹.

⁷ ARSLAN, Çetin, “Dijital Delil ve İletişimin Denetlenmesi”, **Ceza Hukuku ve Kriminoloji Dergisi (CHKD)**, Yıl: 2015, Cilt: 3, Sayı: 2, s. 265.

⁸ ŞEN, Osman Nihat, “Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi”, **2. Polis Bilişim Sempozyumu (14-15 Nisan 2005)**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2005, s. 36.

⁹ YETİM, Servet, “Dijital Kanıt Araştırma Yöntemleri”, **İstanbul Barosu Dergisi**, Yıl: 2008, Cilt: 82, Sayı: 3, s. 1209.

Bilgisayar bağlantılı suçların araştırılması sırasında olay yerinde çalışma yapan adli bilişim ekibinin en çok zaman ayırdığı aşama delillerin toplanması ve belgelere kaydedilmesi aşamasıdır. Bu aşamada gösterilen titizlik, elektronik delilin nerelerden elde edilebileceği hakkında önemli ipuçlarının yakalanmasını sağlayabilir¹⁰.

I. ELEKTRONİK DELİL TOPLANIRKEN UYULMASI GEREKEN TEMEL İLKELER

Elektronik delilin toplanması ve muhafaza edilmesi aşaması adli bilişim sürecinin başlangıç aşaması olup delil bütünlüğünün sağlanması bakımından çok önemli bir safhasıdır. Zira bu aşamada elektronik delilin zarar görmesi veya yok olması oldukça muhtemeldir. Nitekim bilgisayarın basit bir şekilde hareket ettirilmesi bile kimi zaman dosya, veri, zaman mührü (damgası) gibi elektronik nitelikteki delilin değişmesine neden olabilmektedir. Bu durum ise elektronik delilin toplanması aşamasında bazı kurallara riayet etme zorunluluğunu doğurmaktadır.

Ülkemizde elektronik delilin ne şekilde elde edileceğine ilişkin kapsamlı bir yasal düzenleme bulunmamaktadır. Oysa -ABD gibi- kimi ülkelerde, soruşturma evresinde elektronik delilin elde edilmesine ilişkin çalışmalarda bulunan teknik ekibin nasıl hareket edeceklerini bağlayıcı kılan, yanlış yapılan işlemlerin bir ihlal olarak değerlendirilerek cezai takibatı gerektireceğini düzenleyen yasal hükümler yer almaktadır. Ülkemizdeki, elektronik delilin elde edilmesine ilişkin yasal boşluğun başlıca nedenleri arasında bilişim teknolojilerinin ülkemize alt yapısı olmaksızın ithal edilmiş olması, işlenen bilişim suçlarının boyutlarının yeterince bilinmemesi ve suç mağdurlarının konunun farkında olmaması gösterilebilir¹¹.

¹⁰ HENKOĞLU, Türkay, **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, Pusula Yayıncılık, İstanbul, 2011, s. 5.

¹¹ KARAGÜLMEZ, **2011**, s. 403.

Adli bilişim süreci günümüzde soruşturma ve kovuşturma işlemlerinin ayrılmaz bir parçası haline gelmiştir. Suç ve suç yeri ile ilk temasa geçen kolluk görevlilerinin aranıp gerektiğinde elkonulacak bilişim sistemlerine ve ekipmanlarına nasıl müdahalede bulunmaları, bunları incelemenin yapılacağı yere ne şekilde götürmeleri gerektiğine ilişkin tavsiye kuralları veya örnek uygulamanın bilinmesi ve yerine getirilmesi, toplanan delillerin hukuka aykırılığı iddialarının önüne geçilmesi açısından büyük önem taşımaktadır¹².

Elektronik delil elde etme aşaması elektronik delile yönelik olay yeri çalışması ile başlar ve elektronik delil elde edilmesi muhtemel bilişim cihazlarına usulüne uygun müdahale edilmesi ile devam eder. Bu bakımdan olay yerinde yapılan işlemlerde yapılan hatalar delillerin gerçekliği ve güvenilirliğine gölge düşürebilir ve tüm süreci sekteye uğratabilir¹³.

Olay yerini inceleyen ilk müdahale ekibi öncelikle delil elde etmede kullanılacak cihazları hazır etmeli, kendi güvenliğinden emin olmalı, olay yerinin güvenliğini sağlamalı, daha sonra da olay yerindeki elektronik nitelikte olan veya olmayan tüm delillerin sağlamlığını ve bütünlüğünü koruma altına almalıdır¹⁴.

İşlemlere başlamadan önce kullanılacak olan kontrol listeleri, donanım birimleri ve ihtiyaç duyulacak yazılımlar hazırlanmalıdır. Kontrol listeleri, olay yerindeki olumsuz havanın etkisine rağmen, herhangi bir adımı atlamadan, sağlıklı ve eksiksiz bir çalışma yapılmasına yardımcı olacaktır¹⁵.

Elektronik delil elde etme işlemleri mümkün olduğunca adli bilişim uzmanları tarafından yapılmalıdır. Gerçekten de elektronik delilin elde edilmesi aşamasında

¹² KESER BERBER, Leyla, **Adli Bilişim**, Yetkin Yayınları, Ankara, 2004, s. 7.

¹³ HENKOĞLU, 2011, s. 17; AYDOĞAN, Hakan, **Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009, s. 13.

¹⁴ YETİM, 2008, s. 1209.

¹⁵ HENKOĞLU, 2011, s. 19.

değişikliğe uğramaması bakımından bu işe liyakatsiz kimselerin karışması, işi baştan sonuçsuz kılabilir. Bu bakımdan elektronik delilin elde edilmesi için işi iyi bilen bir adli bilişim uzmanının delil elde etme işlemini sürdürmesi gerekmektedir. Elektronik delilin fiziksel delillere göre farklı yapısı bu durumu zorunlu kılmaktadır¹⁶. Zira ancak bir adli bilişim uzmanı, delil kaybına neden olmaksızın -ya da mümkün olan en az kayıpla- elektronik delili toplayabilecektir¹⁷.

Olay yerinde bulunan ve delil olarak değerlendirilmesi muhtemel tüm malzemelerin üzerinde yeterli açıklayıcı bilgi bulunan delil etiketleri ile etiketlenmesi oldukça önemlidir. Diğer taraftan bir envanter oluşturularak olay yerinde elkonulan tüm nesnelere seri numaraları ile birlikte kaydedilmelidir. Her türlü nesne için farklı bir envanter listesi oluşturulmalı ve oluşturulan listeler grup içerisinde bulunan farklı kişiler tarafından da kontrol edilmelidir. Envanterlerin kopyalanması ve her kopyanın imzalatılması ihmal edilmemelidir¹⁸. Ayrıca elkonulan bilişim sistemlerinin daha sonra tekrar birleştirilebilmesi için tüm kablolar renk kodu ile kodlanmalıdır¹⁹.

Elektronik delilin elde edilmesi ile ilgili tüm işlemler belgelenmeli (tutanağa bağlanmalı) ve yeni bir inceleme için kullanılabilir halde korunmalıdır. Elektronik delilin elde edilmesine ilişkin araştırmalar fiziki ortama dayalı olmadığı için başından sonuna kadar yapılan işlemlerin tek tek tutanağa bağlanması önem taşımaktadır. Zira bu tutanaklar, elektronik delilin, delil niteliğini kuvvetlendirmekte ve onunla bütünleşmektedir. Diğer taraftan elektronik delilin elde edilmesi işlemleriyle ilgili her aşamada tutulan tutanaklar, kovuşturma aşamasında bu delile ceza muhakemesi kurallarına göre yöneltilen itirazlar

¹⁶ KARAGÜLMEZ, 2011, s. 401; ÇAKIR, Hüseyin / SERT, Ercan, “Bilişim Suçları ve Delillendirme Süreci”, Örgütlü Suçlar ve Yeni Trendler, **Uluslararası Terörizm ve Sınırtaş Suçlar Sempozyumu (UTSAS 2010)**, Polis Akademisi Yayınları, (der. Oğuzhan Ömer Demir ve Murat Sever), Ankara, 2011, s. 156.

¹⁷ ÖZBEY, Özcan, “Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK’nın 134. Maddesi)”, **Yargıtay Dergisi**, Yıl: 2010, Cilt: 36, Sayı: 3, s. 121; ÜNVER, Yener / HAKERİ, Hakan, **Ceza Muhakemesi Hukuku**, 1. Cilt, 8. Basım, Adalet Yayınevi, Ankara, 2013, 73.

¹⁸ HENKOĞLU, 2011, s. 19.

¹⁹ DEĞİRMENCİ, Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Seçkin Yayıncılık, Ankara, 2014, s. 214.

karşısında, tarafsız uzman bilirkişi raporu alınmasında, bu delilin gerçekten söz konusu bilişim sisteminden elde edilip edilmediğinin kontrolü bakımından da kolaylık sağlayacaktır²⁰.

Olay yerinde bulunan bilişim sistemlerinden kapalı olanlarının açılmaması gerekmektedir. Zira bilişim sistemlerinde elektronik delilin bulunması muhtemel durumlarda sistemin açılması mevcut delillerin zarar görmesine sebep olabilir. Örneğin, bilişim sistemlerinin işletim sistemleri açılırken birçok konfigürasyon dosyasına erişim sağlanmakta ve delil niteliğindeki verilerin zarar görmesine yol açılabilmektedir. Dosyaların erişim tarihlerinin dahi bazı durumlarda delil niteliği taşıyabileceği düşünüldüğünde böyle bir uygulama sakınca doğurabilir. Aynı zamanda, işletim sistemlerinin açılırken oluşturabilecekleri geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş verilerin delil niteliğinde kurtarılabilme ihtimalini ortadan kaldırmış olacak ve bu durum da delil bütünlüğünün bozulmasına neden olacaktır²¹.

Diğer taraftan, olay yerinde bulunan bilişim sistemlerinden açık durumdaki bilişim sistemlerine ise dokunulmamalı, ekranda açık olan herhangi bir pencere ya da yapılan bir işlem varsa bu durum tutanağa bağlanmalı, sonrasında ise cihazın türüne göre kontrol edilerek gücü kesilmek suretiyle kapatılmalıdır. Ayrıca, bilişim teknolojileri ile ilgili bir olay yeri müdahalesi öncesinde muhtemel olay yerine uzaktan erişim ile delillerin karartılması ihtimaline karşı elektromanyetik koruma sağlayacak donanım ve yazılımlar bulundurulmalıdır²².

²⁰ KARAGÜLMEZ, 2011, s. 401.

²¹ EKİZER, A. Hakan, **Adli Bilişim (Computer Forensics)**, <https://www.ekizer.net/adli-bilisim-computer-forensics/> (erişim tarihi: 02.02.2020).

²² ÖZTÜRK, 2007, s. 68; ÇAKIR / SERT, 2011, s. 157.

II. ELEKTRONİK DELİL TOPLANMASI AŞAMASINDA YAPILMASI GEREKLİ İŞLEMLER

Elektronik delilin ceza yargılamasında kullanılabilmesi veri bütünlüğünün korunmuş olmasına bağlıdır. Zira bir elektronik delilin veri bütünlüğünün bozulmuş olması onun geçerliliğini de olumsuz etkileyecek ve ispat fonksiyonunun ortadan kalkmasına neden olabilecektir. Bir elektronik verinin bozulmasına neden olabilecek durumların başında ise onun uygun koşullarda toplanmamış olması yer almaktadır. Bu bakımdan elektronik delilin yapısı itibariyle hassas özellik arz etmesi ve kolay bozulabilen nitelikte olması bu delilin toplanması sırasında bazı temel ilkelere uyulmasının yanı sıra aşağıda açıklayacağımız kimi işlemlerin de yerine getirilmesini gerekli kılmaktadır.

A. Canlı Analiz

Elektronik delil toplamak amacıyla olay yerine gelen ekipler, öncelikle üzerinde inceleme yapılacak olan bilgisayarların düzgün bir şekilde kapatılması ve muhafazasından sorumludurlar. Bundan sonra ise söz konusu bilgisayarlar üzerinde bulunan ve diğer veri depolama ünitelerinin imaj alma işlemlerine başlanır. Bununla birlikte üzerinde inceleme yapılacak bilgisayarların kapatılması veya yeniden başlatılması, sistem üzerinde bulunan uçucu verilerin kaybedilmesine neden olmaktadır²³.

Birkaç yıl öncesine kadar adli bilişim sürecinde incelenen bilgisayarın çalışır vaziyetteyken elkonulmasına karar verildiğinde bilgisayarı kapatarak değil geleneksel metot olan doğrudan kablo çekilmek (pull the plug) suretiyle elektriğin birden kesilmesi sonucunda bilgisayar kapatılmakta ve böylece elkoyma işlemi gerçekleştirilmekteydi. Bu yöntemle elektrik kesilmesi sonrasında kapanan bilgisayardaki bilgilerin bilgisayar içerisinde bir yerlere kaydedilmesi ve sonrasında bilgilerin soruşturmada kullanılması hedeflenmekteydi²⁴.

²³ HENKOĞLU, 2011, s. 26.

²⁴ ŞEN, Bilal, “Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller”, **Ankara Barosu Uluslararası Hukuk Kurultayı (11 Ocak-15 Ocak 2010)**, Cilt. 3, Ankara Barosu Yayınları, Ankara, 2010, s. 69.

Bununla birlikte zaman içerisinde gelişen teknolojiyle birlikte açık biçimde elkonulan bilgisayarlar da bulunan uçucu verilerin olayların aydınlatılmasındaki önemi nedeniyle bilgisayar kapatıldığında kaybolacak uçucu verilerin kaybolmaya maruz kalmaksızın elde edilmesine yönelik araçlar üretilmiş, aynı amaçla da canlı analiz yöntemi uygulanmaya başlanmıştır.

Günümüzde çalışır vaziyette bulunan bilgisayar sistemlerindeki uçucu verilerin toplanması amacıyla canlı analiz yapma özelliğine sahip birçok yazılım bulunmaktadır. Bu yazılımların en önemli özelliği sisteme kurulmadan çalışabilmeleridir. Bu sayede incelenen sistemin diski üzerinde herhangi bir ekleme yapılmaksızın ve elektronik delilin orijinalliği bozulmaksızın gerekli işlemler yapılabilmektedir²⁵.

Canlı analiz yöntemi, sıradan elektronik delil elde etme işleminin ötesinde teknik uzmanlık gerektiren bir yöntemdir. Bazen, suç işlemekte çokça kullanılan bilgisayarlar üzerinde, elektronik delilleri yok edecek veya bir virüsü etkin hale getirebilecek tuzakların bulunduğu görülmektedir. Özellikle, zararlı kodların dağıtımı, siber saldırılar, kredi kartları ve internet aracılığıyla işlenen dolandırıcılık suçlarının işlenmesinde kullanılan bilgisayarlar üzerinde yapılacak incelemelerde söz konusu bilgisayarlar kapatılmadan uçucu verilerin elde edilmesi ve kayda alınması gerekmektedir. Elektronik delillerin toplanması sırasında uçucu verilerin elde edilmesi amacıyla kullanılan bu yöntem, herhangi bir siber saldırıya maruz kalınması halinde, sistem yöneticileri tarafından verileri kurtarmak amacıyla da kullanılmaktadır²⁶.

Bu bağlamda, olay yerine varıldığında açık olan bir bilgisayarla karşılaşılması ve bilgisayar üzerinde bazı şifreleme programlarının tespit edilmesi durumunda bilgisayar kapatılmadan önce canlı analiz işleminin yapılması gerekmektedir. Canlı analiz işlemini gerekli kılan diğer bir husus ise olay yerinde açık halde bulunan bilgisayarın üzerinde hâlihazırda şüpheli programların çalışıyor olması ve ekranda delil niteliğine sahip

²⁵ HENKOĞLU, 2011, s. 29.

²⁶ HENKOĞLU, 2011, s. 27.

dosyaların açık bulunmasıdır. Zira uçuculuğu yüksek olan bu tür verilere de sistemin kapatılması halinde tekrar ulaşılması imkânsızdır²⁷.

Ağ trafiği bilgilerinin elde edilmesine yönelik işlemler de canlı analiz işlemi gerekliliği kılın başka bir durumdur. Ağ trafiği bilgileri toplanırken, sistem canlı halde bulundurulduğundan sistemin anlık resminin çekilmesi suretiyle o anda sistemde bulunan veriler ele geçirilerek analize tabi tutulmaktadır²⁸.

B. İmaj Alma (Birebir Kopyalama)

Elektronik verinin elde edilmesi sürecine ilişkin olarak soruşturma veya kovuşturmaya konu suçun aydınlatılmasına fayda sağlayacak elektronik verinin orijinalinin elde edilemeyerek sadece normal kopyasının elde edildiği bir durumda, bu kopya üzerinden yeni bir kopya çıkartılarak bilirkişi incelemesi yapılması usule uygun kabul edilmeyecektir. Bilindiği üzere genel hukuk kuralları uyarınca belgeler üzerinde yapılacak olan sahtecilik incelemesinin, ancak orijinal metin üzerinden yapılması gerekmekte olup fotokopi üzerinden sahtecilik incelemesi yapılamamaktadır. Aynı şekilde normal (basit) kopyası elde edilen bir elektronik verinin de orijinali ile eş değer tutulması söz konusu olmayıp gerçek ve geçerli bir elektronik delil olarak kabul edilmesi mümkün değildir. Aksi durum olayın ispatı konusunda soru işaretlerine neden olacaktır.

Bununla birlikte adli bilişim sürecinde elektronik verinin imajının (birebir kopyasının) alındığı durumlarda elektronik verilerden hangisinin asıl olduğunun bir önemi bulunmayacağından belge fotokopilerinin, aslı gibi oldukları tevsik edilmediği sürece hukuksal sonuçlar doğurmayacağına ilişkin genel kuralın imajı alınan elektronik delil bakımından geçerli olmadığı söylenebilir²⁹.

Bilişim sistemlerinde kopyalama işlemi genellikle üç seviyede gerçekleştirilir. Bunlar, dosya seviyesi, bölüm seviyesi ve disk seviyesi kopyalamalarıdır. Dosya seviyesinde ve

²⁷ HENKOĞLU, 2011, s. 27.

²⁸ DEĞİRMENCİ, 2014, s. 223.

²⁹ DEĞİRMENCİ, 2014, s. 140.

bölüm seviyesinde yapılan kopyalamalar, herhangi bir dosyayı normal bir kullanıcı olarak kopyalamaktadır. Bu durumda, diskte bulunan silinmiş veya kısmen silinmiş dosyalar kurtarılamayacaktır. Ancak disk seviyesinde yapılan kopyalama ile orijinal diskin birebir kopyası alınabilmektedir. Adli bilişimde kullanılan kopyalama yöntemi de disk seviyesinde yapılan birebir kopyalamadır. Bu kopyalama türünde orijinal disk ile kopya disk her anlamda birbirine denktir³⁰.

Adli bilişimde yapılan birebir kopyalama işlemine adli imaj (forensic image) denilmektedir. Birebir kopyalama, veri depolama birimi üzerindeki tüm verilerin kopyasının alınmasını ihtiva etmektedir. Alınan birebir kopya, mevcut verileri, silinmiş verileri, gizli bölümleri, veri depolama birimindeki diğer verileri de kapsamaktadır³¹. Ancak birebir kopyalama işlemi sırasında uygun adımlar atılmak suretiyle orijinal veride meydana gelebilecek değişikliklerin önüne geçilmelidir. Bu husus elektronik delil toplama aşamasının en önemli unsurlarından birisidir³².

Bilişim sistemlerinde yer alan verilerin imajının alınmasının amacı verilerin bütünlüğünü ve güvenilirliğini sağlamaktır. Verilerin imajının alınması iki açıdan verilerin bütünlüğünün ve güvenilirliğinin sağlanmasına hizmet etmektedir. Öncelikle şüphelinin kullanmış olduğu bilişim sisteminde elkonulan verilerin daha sonra değiştirilmemiş, verilere herhangi bir ekleme veya çıkarma yapılmamış olduğu güvence altına alınmış olacaktır. Bu sayede savunma tarafından ileri sürülecek “delillerin değiştirildiği veya sonradan eklendiği” yönündeki iddiaların önüne geçilmiş olacaktır. İkinci olarak ise bilişim sistemindeki verilerin toplanması aşamasında verilerin zarar görmesinin önlenmesi sağlanacaktır. Nitekim bilişim sisteminde veri toplanması zor ve riskli bir faaliyet

³⁰ SAY, Kubilay, **Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 71.

³¹ ŞİRİKÇİ, Ahmet Serhat / CANTÜRK, Nergis, “Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi”, **Bilişim Teknolojileri Dergisi**, Yıl: 2012, Cilt: 5, Sayı: 3, s. 30.

³² MASON, Stephen, **International Electronic Evidence**, BIICL, London, 2008, s. xlvi.

olduğundan bazı durumlarda sistemde yer alan veriler toplama faaliyeti sırasında zarar görebilmektedir³³.

Disk imajının oluşturulması, elektronik delilin adli analiz sürecinin başlangıç noktasıdır. Disk imajının doğru bir şekilde alınması, tüm adli süreci etkileyebilecek kadar önemli bir konudur. Alınan imajın doğruluğunun, elektronik delilin adli analizinin yapılması ve mahkeme süreci esnasında sorgulanması bunun bir göstergesidir. Elektronik delilin analizinin söz konusu delil üzerinde doğrudan gerçekleştirilmesi, üzerinde suç şüphesi bulunan veri depolama biriminin zarar görmesine veya inceleme yapan kişi tarafından verilerin değişmesine neden olabilmektedir³⁴.

İnceleme ve analiz işlemleri sırasında yapılacak küçük nitelikteki bir hata bile kimi zaman delil olabilecek bir verinin yok olmasına neden olabilir. Ancak, imaj üzerinde yapılacak çalışmada hata yapılırsa bile orijinal veriler yeni bir imajın üretilmesinde kullanılabilir. Bu nedenle elektronik delil üzerinde analiz işleminin yapılması adli inceleme kuralları açısından doğru değildir ve bu açıdan da orijinal diskin imajının (birebir kopya) alınması bir zorunluluktur³⁵. İmaj alma işlemi sonucunda elde edilen birebir kopya, adli kopya (forensic duplicate) olarak da adlandırılmaktadır³⁶.

Birebir kopyalama işlemi, günlük kullanımda uygulanan normal kopyalamadan farklıdır. Normal kopyalama işlemi, kullanıcı tarafından oluşturulan dosyaların bir kaynaktan başka bir kaynağa aktarılması işlemini ifade etmekte olup sistem dosyaları ve gizli dosyaların kopyalanmasını içermemektedir. Normal kopyalama işleminde dosyaların veri ya da sistem dosyası olduğu ve tarih/zaman bilgileri gibi detaylar yanıtıcı

³³ DEĞİRMENCİ, 2014, s. 76.

³⁴ HENKOĞLU, 2011, s. 47.

³⁵ AKTEPE, Basri, “Emniyet Personelinin Bilgisayar ve Bilgisayarla İlintili Suçlarla Mücadelede Dikkat Etmesi Gereken Hususlar (Adli Tıp Esaslarına Uygun Olarak Delillendirme)”, **1. Polis Bilişim Sempozyumu (21-22 Ekim 2003)**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2004, s. 69; SAY, 2006, s. 86.

³⁶ AYDOĞAN, 2009, s. 35.

olabilmektedir³⁷. Ayrıca, normal kopyalama sırasında dosya alanındaki bilgilerin silinmesi veya bozulması da mümkündür³⁸.

Diğer taraftan işletim sistemlerinde günlük yaşamda yapılan normal kopyalama işleminde kullanıcılar tarafından görülen dosya veya klasörler başka bir bilişim sistemine aktarılması sırasında bazı yeni dosya yapılarında (NTFS) daha detaylı bilgiler tutulabilmekte iken burada bulunan dosya veya klasör eski dosya yapısıyla (FAT) formatlanmış bir veri depolama birimine kopyalandığında bazı üst verilerin kopyalanamadığı görülmektedir. Bu bakımdan adli bilişim uygulamalarında normal kopyalama tercih edilmemekte, birebir kopya elektronik delil üzerindeki verilerin tümünü kapsadığından incelemeler de birebir kopyalar üzerinden yapılmaktadır³⁹.

Disk imajının adli bilişim standartlarına uygun olarak alınması, elektronik delilin elde edilmesi ve analizi sürecinin doğru bir şekilde başlayıp sonuçlandırılması açısından önemlidir. Bu sürecin doğru işlemesi, mahkemede elektronik delilin niteliklerine gölge düşmeyecek şekilde sunulması ve doğru kararların verilmesinde etkili olacaktır⁴⁰.

Adli bilişim sürecinin en önemli işlemlerinden birisi olan imaj alma işlemini standartlara uygun şekilde gerçekleştirmek üzere çeşitli özel yöntemlerin kullanılması gerekmektedir. Günümüzde kullanılan başlıca yöntemler ise donanımsal araçlarla imaj alma ve bilgisayar yazılımları ile imaj alma yöntemleridir.

³⁷ HENKOĞLU, 2011, s. 48.

³⁸ ŞEKER, Güven, “Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum”, **Uluslararası İnsan Bilimleri Dergisi**, Yıl: 2004, Cilt: 1, Sayı: 1, s. 7.

³⁹ ÖZBEK, Murat, “Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları”, **1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (20-21 Mayıs 2013)**, Elazığ, 2013, s. 2, https://www.academia.edu/31927878/Adli_Bilisim_Uzmani_Murat_OZBEK_isdfs_bildiri2013_04_11 (erişim tarihi: 24.02.2020).

⁴⁰ HENKOĞLU, 2011, s. 59.

C. Hash (Veri Bütünlük) Değeri

Teknolojinin kaydettiği hızlı gelişme ve internetin küresel nitelikte kullanımı, çeşitli teknolojilere açık bir yaklaşım biçimini ve elektronik yoldan aktarılan verilerin tasdikini sağlayacak hizmetlerin sunulmasını gerekli kılmıştır. Bu gereğin bir anlam ifade edebilmesi ise buna bağlanacak hüküm ve sonuçların ispat edilebilirliğinin de sağlanmasını zorunlu kılmaktadır. Aksi takdirde bilişim teknolojilerinden tam anlamıyla yararlanmak mümkün olmayacaktır⁴¹.

Bu bağlamda elektronik delille ilgili üzerinde durulması gereken en önemli hususlardan birisi de elektronik delilin bütünlüğüdür. Zira elektronik delillerin bütünlüğü, elde edilen, üzerinde çalışılan ve çalışma sonrasında hakkında kanaat bildirilen elektronik verinin herhangi bir şekilde değişikliğe uğrayıp uğramadığı hususuyla ilgilidir. Olay yerinden elde edilen bir verinin orijinal hali ile üzerinde çalışılan verinin birebir aynı olması gerekmektedir⁴².

Bu bakımdan adli bilişim uygulamasında elektronik delilin bütünlüğünün sağlanması yani ilk olay verisinin orijinal hali ile kullanıldığına ilişkin teknik ispatın yapılabilmesi, elektronik delilin korunması ve kontrolünün yapılması için -aşağıda incelenecek olan zaman damgasının (time stamping) yanı sıra- imaj alma işlemi sırasında hash değerinin tespit edilmesi gerekmektedir⁴³.

Veri depolama ünitelerine ait alınan imajların hash değerinin tespiti işleminden hemen sonra bu değerın tutanakla kayıt altına alınarak hazır bulunan taraflara imzalatılması

⁴¹ DELİDUMAN, Seyithan, “Elektronik Verilerin Delil Değeri”, **Bilişim Hukuku**, (der. Mete Tevetoğlu), Kadir Has Üniversitesi Yayınları, İstanbul, 2006, s. 47.

⁴² HENKOĞLU, 2011, s. 80.

⁴³ ÖZTÜRK, 2007, s. 78; “Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tespit edilmemiş bulunması..” Yargıtay 8. CD. 24.10.2013, E. 2012/21817, K. 2013/25428, <https://www.kararara.com/forum/viewtopic.php?t=17165> (erişim tarihi: 24.02.2020).

daha sonra yapılacak itirazları önleyecektir⁴⁴. Bununla beraber uygulamada hash değeri alma işlemi -diğer adli bilişim işlemlerinde olduğu gibi- çoğu zaman tarafların huzurunda gerçekleştirilmediği için bu hassasiyete de riayet edilmediği görülmektedir.

Bir veri veya veri depolama biriminin ilk sektörden başlayarak son sektöre kadar tümünün belirli bir algoritmik fonksiyondan geçmesi sonucunda bir hash değeri oluşmaktadır. Son sektörün de aynı işleme tabi tutulması sonucunda ortaya çıkan değere ise o veriye ait hash değeri denilmektedir. Bu değer benzersiz (unique) nitelikte olduğu için veri depolama birimi üzerindeki bir karakterin değişmesi hash değerinin de değişmesine neden olur. Bu bakımdan elektronik delil veya elektronik delilden alınan imaj üzerinde herhangi bir değişiklik yapıp yapılmadığını kontrol etmek amacıyla hash değeri hesaplatılır ve böylece üzerinde çalışılan verilerin orijinali ile aynı olup olmadığının doğruluğu kontrol edilmiş olur⁴⁵.

Hash algoritmaları imaj alma işlemi sırasında uygulanabileceği gibi imaj alma işlemi sonrasında da her dosya için ayrı ayrı uygulanabilir. Çeşitli hash algoritmaları bulunmakla birlikte, bu algoritmaların hangisi uygulanırsa uygulansın belli boyuttaki bir veri için bulunan hash değeri hep aynı olacaktır⁴⁶. Günümüzde en sık kullanılan hash algoritmaları MD5 ve SHA'dır. Bu algoritmalar sonucu ortaya çıkan değerler imaj ile birlikte aynı dosya içerisinde saklanabilir veya ayrı bir dosya içerisinde toplanabilir⁴⁷.

Hash hesaplaması sonucu çıkan hash değeri ile ilk hesaplanan hash değerinin birbirleri ile aynı olmaları durumunda elektronik delilin veya elektronik delilden alınan

⁴⁴ ORTA, Mesut, **Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)**, Yetkin Yayıncılık, Ankara, 2015, s. 265; HENKOĞLU, **2011**, s. 25.

⁴⁵ AKARSLAN, Hüseyin, **Bilişim Suçları**, Seçkin Yayıncılık, Ankara, 2012, s. 124; ÖZBEK, **2013**, s. 2.

⁴⁶ SARIAKÇALI, Turgay, **İnternet Üzerinden Akdedilen Sözleşmeler**, Seçkin Yayıncılık, Ankara, 2008, s. 69.

⁴⁷ SAY, **2006**, s. 78.

kopyanın herhangi bir değişikliğe uğramadığı sonucuna varılır. Bu bağlamda, hash değeri, elektronik verinin bir nevi mührü konumundadır⁴⁸.

Adli bilişim uzmanının bilirkişi raporunda vermiş olduğu hash değeri ile inceleme yapılan şüpheli sabit diskin imajının alındığı sırada oluşturulan ve imajı alınan diskin kullanıcıya verilen kopya üzerindeki hash değerinin aynı olmaması durumunda yapılan analiz sonucunda elde edilen bulgulara itiraz edilebilecek ve söz konusu bulguların geçerliliği ve doğruluğu hakkında şüphelere neden olacaktır. Nitekim uygulamada karşılaşılan en büyük ihmallerden biri de hash değerinin takibinin ve kontrolünün yapılmamasıdır. Bazen delillerin elde edilmesi ve imaj alma işlemleri sırasında kolluk birimleri tarafından elde edilen ve rapora işlenen hash değerinin, bilirkişi raporunda yer alan hash değerinden farklı olduğu durumlarla karşılaşılmaktadır. Bu durum, bilirkişinin incelemiş olduğu imajın gerçeğinden farklı olduğu ve imaj üzerinden elde edilen bulguların adli bilişim açısından delil değeri taşımadığı tartışmalarına yol açmaktadır⁴⁹.

Belirtmek gerekir ki hash değeri üzerindeki hassasiyet nedeniyle bilirkişilerin kendilerine verilen disk imajlarını öncelikle üzerinde çalışacakları başka bir diske kopyalamaları ve kendilerine verilen imaj üzerinde çalışma yapmamaları gerekmektedir. Zira herhangi bir nedenle imaj üzerinde meydana gelebilecek değişiklik hash değerinin değişmesine ve o zamana kadar yapılan tüm inceleme işlemlerinin geçersiz kabul edilmesine neden olabilecektir⁵⁰.

Diğer taraftan hash değeri, bilişim sistemlerinde bulunan elektronik verinin arama sonucunda elde edildiği hali ile onun üzerinde çalışılan ve mahkemeye sunulan hali veya adli imajı arasındaki güvenilirliği sağlamakta kullanılabilir. Buna karşın, bilişim sisteminde

⁴⁸ ÖZBEK, 2013, s. 2.

⁴⁹ KILIÇ, Mehmet Serkan, “Elektronik Deliller ve Yapısal Özellikleri”, **Adli Bilişim ve Elektronik Deliller**, (ed. Hüseyin Çakır / Mehmet Serkan Kılıç), Seçkin Yayıncılık, Ankara, 2014, s. 149-150; BUCAK, Yeşim, **Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, Üsküdar Üniversitesi Bağlılık ve Adli Bilimler Enstitüsü, 2019, s. 25-26; HENKOĞLU, 2011, s. 54-55.

⁵⁰ HENKOĞLU, 2011, s. 55.

bulunan elektronik veriye ilk temas edildiği arama sırasındaki hash değerinin alınmasından önce bu elektronik verilerde değişiklik yapıldığına ilişkin iddiaların doğruluğunu veya yanlışlığını hash değeri aracılığı ile tespit etmek mümkün değildir. Bu bakımdan hash değerlerinde herhangi bir problemin yaşanmamış olması tek başına elde edilen elektronik delilin güvenilir olduğu sonucunu ortaya koymaz. Bu nedenle elektronik delilin bütünlüğünün tespitinde diğer değişkenlerin de denetlenmesi gerekmektedir.

D. Zaman Damgası (Time Stamping)

Yukarıda da değinildiği üzere elektronik delilin bütünlüğünün korunması için birebir kopyalama işlemi sırasında elektronik verilerin hash değerinin alınmasının yanı sıra bu durumun zaman damgası kullanılarak muhafaza altına alınması da büyük önem arz etmektedir.

Mahkeme sürecinde elektronik delile ne zaman erişildiği, görevli personelin ne kadar süreyle delille temas halinde bulunduğu, elektronik delilin bütünlüğünün ne kadar süreyle sağlanabileceği hususlarına ilişkin soruların cevaplanabilmesi gerekmektedir. Zira elektronik delilin bütünlüğünün ispatlanması ve ayrıca elektronik delile ulaşılma zamanının tam olarak bilinmesi son derece önemlidir. Bu husus ise zaman damgası ile sağlanabilmektedir⁵¹.

Zaman damgasına ilişkin birçok tanım bulunmaktadır. Gerçek hayatta zaman damgası herhangi bir anı temsil edebilmekteyken dijital dünyada zaman damgası dijital formatta belirli (spesifik) bir anı ifade etmektedir. Bu bağlamda zaman damgası adli bilişim açısından çok önemli bir role sahiptir. Zira soruşturma sürecinde belirli anların tam zamanını bilme gerekliliği bulunmaktadır⁵².

⁵¹ COSIC, Jasmin / BACA, Miroslov, **(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp**, https://www.academia.edu/15316896/_Im_proving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp (erişim tarihi: 02.02.2020).

⁵² COSIC / BACA, https://www.academia.edu/15316896/_Im_proving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp (erişim tarihi: 02.02.2020).

Zaman damgası, bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği zamanın tespit edilmesini sağlayan elektronik bir veridir⁵³. Zaman damgasının bu niteliği sayesinde elde edilen elektronik delilin üretim, erişim veya değiştirilme zamanları üzerinde oynama yapılması veya değiştirilmesi engellenmiş ve delillerin doğruluğu ispatlanmış olmaktadır⁵⁴.

Nitekim 30.11.2007 tarihli ve 26719 sayılı Resmi Gazete'de yayınlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in yer sağlayıcının⁵⁵ yükümlülüklerini düzenleyen 7/1-c maddesinde yer sağlayıcının trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlü oldukları hükme bağlamıştır. Aynı Yönetmelik'in erişim sağlayıcının⁵⁶ yükümlülüklerini düzenleyen 8/1-b maddesinde ise bu yükümlülük 1 yıl süre ile erişim sağlayıcılara da yüklenmiştir.

Bununla birlikte gerçek ve dijital dünya zamanı daima saat ayarına bağlı olduğundan zamanın kaynağının da güvenilir olması gerekir. Bu bakımdan zaman damgasının her hal ve şartta güvenilir bir sonuç doğuracağı söylenemez. Örneğin, başkasına ait ve saat ayarı yanlış olan bir bilgisayar kullanıldığında yanlış bir zaman damgası elde edilecek demektir. Böyle bir durumda zamanın tamamen güvenilir olduğundan bahsedilemez ve bu şartlar

⁵³ TÜRKTRUST, **Zaman Damgası Nedir ?**, <https://www.turktrust.com.tr/tr/urunler/zaman-damgası/> (erişim tarihi: 02.02. 2020).

⁵⁴ AYDOĞAN, **2009**, s. 37.

⁵⁵ Yer sağlayıcı; hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri ifade eder (5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 1-m).

⁵⁶ Erişim sağlayıcı; kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri ifade eder (5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 1-e).

altında elde edilen zaman damgası, elektronik delile ilişkin bir soruşturmada olayların değerlendirilmesine dair hayati öneme sahip bir faktör olarak kullanılamaz⁵⁷.

Zaman damgasına ilişkin olarak zamansal hatanın en yaygın kaynağı sistem saatindeki kaymalardır. Eğer bir yönlendiricinin saati birkaç saat öndeyse, bu uyumsuzluk diğer sistemlerdeki kayıtlarla olayları ilişkilendirmekte sıkıntıya neden olabilir ve sonraki süreçte yapılacak analizlere zarar verebilir. Ayrıca, elektronik delilin toplandığı sistem saatindeki hatalar analiz ve raporlama aşamalarında oluşması muhtemel tutarsızlıklara sebebiyet verebilir. Örneğin, çoğu sistem günlüğü sunucuları⁵⁸ ağ üzerindeki uzak sistemlerden alınan günlük kayıtları için bir zaman damgası oluşturmaktadır. Bu nedenle, sistem günlüğü mesajını gönderen bilgisayar saati doğru olsa bile sunucudaki saat kayması hataya neden olabilecektir⁵⁹.

Ağ günlüklerindeki bir diğer yaygın zamansal hata kaynağı ise saat dilimi farklılıklarıdır. Microsoft gibi bazı web sunucuları GMT (Greenwich Mean Time) zaman damgasına göre günlük kayıtlarını oluşturmaktadır. Bununla birlikte dünya genelindeki bilgisayar sistemleri ise genellikle kendi günlük kayıtlarında yerel saat dilimini kullanırlar. Bu bakımdan zaman dilimi farklılıklarını düzeltmede yaşanacak bir başarısızlık karışıklığın daha da büyümesine sebebiyet verebilir. Örneğin bir internet servis sağlayıcısından bilgi istendiğinde, saat dilimi uyumsuzluğu internet servis sağlayıcısının yanlış abone bilgilerini vermesine ve dolayısıyla masum bir kimsenin töhmet altında kalmasına neden olabilir⁶⁰.

⁵⁷ COSIC / BACA, https://www.academia.edu/15316896/_Im_proving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp (erişim tarihi: 02.02.2020).

⁵⁸ Sunucu (server); dijital bilgileri kapasiteleri oranında depo ederek diğer bilgisayarlara hizmet sağlayan bilgisayarlar ya da programları ifade etmektedir. Bkz. SOYSAL, Tamer, "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu", **Türkiye Barolar Birliği Dergisi**, Yıl: 2005, Sayı: 61, 2005, s. 309.

⁵⁹ CASEY, Eoghan, "Error, Uncertainty, and Loss in Digital Evidence", **International Journal of Digital Evidence**, Yıl: 2002, Cilt: 1, Sayı: 2, https://www.academia.edu/2983793/Error_Uncertainty_and_Loss_in_Digital_Evidence, (erişim tarihi: 02.02.2020).

⁶⁰ CASEY, https://www.academia.edu/2983793/Error_Uncertainty_and_Loss_in_Digital_Evidence, (erişim tarihi: 02.02.2020).

E. Koruma Zinciri (Chain of Custody)

Koruma zinciri, bir delilin fiziki veya elektronik olarak toplanması, muhafaza edilmesi, başka bir yere aktarılması ve analiz edilmesini gösteren kronolojik belgelendirme sürecini ifade etmektedir. Koruma zinciri sayesinde delillerin doğrulanması sağlanmaktadır⁶¹. Bu bakımdan elektronik verilerin ceza yargılamasında kullanılacak nitelikte “sağlam delil” olarak kabul edilebilmesi, bu verilerin ele geçirildiği ilk andan itibaren koruma zinciri (chain of custody) kıstaslarına uygun olarak temiz bir şekilde el değmeden korunarak incelemeyi yapacak uzmanın önüne götürülmesinin sağlanmasına bağlıdır⁶².

Delillendirme sürecinin en önemli unsurlarından birisi delillerin koruma zinciri ile toplanması ve belgelendirilmesidir. Bu bakımdan soruşturma aşamasında elektronik delili elde eden her kişi, bu delilin ilk elde edildiği hali ile mahkemede ileri sürüldüğü halinin aynı olup olmadığı hususunda ifadeye çağırılabilir. Her ne kadar delillere temas eden (delilleri toplayan) her kişinin her durumda mahkemede hazır edilmesi gerekli olmasa bile, bu durumun asgari seviyede tutularak elektronik delilin ilk toplandığı andan mahkemeye sunulduğu ana kadar değiştirilmediği hususunun açıklığa kavuşturulması yerinde olacaktır⁶³.

Koruma zinciri adli bilişim süreci bakımından elektronik delilin geçerliliği hususunda çok önemli bir rol oynamaktadır. Zira adli bilişimin her aşamasında elektronik delilin nerede, ne zaman, nasıl keşfedildiği, ne şekilde toplandığı ve incelemeye tabi tutulduğu, yine delile ne zaman ve kim tarafından ilk olarak temas edildiğinin bilinmesi gerekmektedir. Uygun bir koruma zinciri bu gibi tüm soruların cevaplarını belgeleriyle

⁶¹ GÖZÜŞİRİN, Mesih, **5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2011, s. 93.

⁶² KUNTER, Nurullah / YENİSEY, Feridun / NUHOĞLU, Ayşe, **Açıklamalı Ceza Muhakemesi Kanunu**, Cilt I, Beta Yayınevi, İstanbul, 2013, s. 1320.

⁶³ CASEY, Eoghan, **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**, Third Edition, Academic Press, California, 2011, s. 21.

ortaya koyabilmelidir. Eğer bu sorulardan yalnızca biri bile cevapsız kalırsa koruma zinciri bozulmuş sayılır. Elektronik delil mahkemeye sunulduğunda, eğer koruma zincirindeki herhangi bir halka eksikse, mahkeme delilin suçla ilişkisini kabul etmeyebilir ve bu nedenle de tüm bir soruşturma sonuçsuz kalabilir⁶⁴.

Sağlam bir koruma zincirinin olmaması elektronik delilin usulüne uygun biçimde elde edilmediği, değiştiği, bozulduğu, başka suçlara ait verilerle karıştığı veya sair nedenlerle kirletildiği iddialarına neden olabilir. Koruma zincirinin bozulmasının muhtemel sonuçları arasında delilin yanlış belirlenmesi, delilin kirlenmesi, delilin veya ilgili unsurlarının geçerliliğini kaybedilmesi tehlikesi de bulunmaktadır⁶⁵.

Koruma zinciri meselesi dijital veri ile ilişkili olduğu kadar bu dijital verinin içerisinde bulunduğu elektronik cihazla da ilişkili olduğu için koruma zinciri hem elektronik cihazı hem de bu cihazda bulunan dijital veriyi kapsamaktadır. Bu nedenle soruşturma kapsamında ele geçirilen elektronik cihazın da koruma zinciri güvencesiyle korunması gerekir.

Koruma zinciri konusunda dile getirilen en büyük eleştiri bu kapsamda yapılan kayıtların otomatik bilgisayar işlemi olmayıp doğrudan insan eli ile gerçekleştirilmesidir⁶⁶. Gerek genel gerekse elektronik delille ilgili koruma zincirine ilişkin -eğer varsa- akreditasyon standartlarının, laboratuvar politikalarının, prosedürlerin ve diğer kuralların bilinmesi ayrıca bunların takip edilip edilmediği veya bunlardan sapma olup olmadığının belirlenmesi gerekir. Söz konusu standart, politika ve prosedürlerde sapma olması, dava sürecini etkileyeceğinden bu tür sapmaların yaşanması durumunda mahkemeyi ikna edecek

⁶⁴ COSIC / BACA, https://www.academia.edu/15316896/_Im_proving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp (erişim tarihi: 02.02.2020).

⁶⁵ CASEY, 2011, s. 22.

⁶⁶ KILIÇ, 2014, s. 150.

açıklamalar yapılmalıdır. Diğer taraftan politikalar, prosedürler ve diğer kurallar da dinamik tutulmalıdır⁶⁷.

III. ELEKTRONİK DELİLİN PAKETLENMESİ, TAŞINMASI VE MUHAFAZASI

Bilişim sistemlerinden elde edilen elektronik delillerle ilgili en önemli husus bu delillerin güvenilirliğinin korunması noktasında kendini göstermektedir. Nitekim inceleme ve analiz işlemlerinin yerine getirilmesine yönelik birçok teknolojik cihaz üretilmesine karşın adli bilişim sürecinde bilişim sistemlerinden çıkartılan elektronik delilin bütünlüğünün korunması konusu soruşturma makamları ve taraflarını en çok endişelendiren mesele haline almıştır⁶⁸.

Gerçekten de elektronik delil, hassas yapısından dolayı, yanlış paketlenme, taşıma veya yanlış muhafaza edilme işlemleri sonucunda kolaylıkla değişikliğe uğrayabilir, bozulabilir ya da yok olabilir niteliğe sahiptir. Bu nedenle, elektronik delili paketlemek, taşımak ve muhafaza etmek için özel önlemler alınması gerekir. Aksi halde, elektronik delil kullanılamaz veya sonuca götüremez duruma gelebilir.

Nitekim uygulamada CD, DVD vb. elektronik medyalar aşırı basınç uygulayarak yazı yazılması, zımba teli ile üzerlerinde delik açılması, sıcak mührün elektronik medyalar üzerine uygulanması, çeşitli yapışkanlar kullanılması sonucunda medyalar üzerinde kâğıt ve yapışkan madde bakiyelerinin kalması gibi yanlış uygulamalar nedeniyle elektronik medyalar zarar verildiği görülmektedir⁶⁹.

⁶⁷ HAGY, David W., "Integrity, Discovery, and Disclosure of Digital Evidence", **Digital Evidence in the Courtroom**, (ed. J. D. Nilsson), Nova Science Publishers, Inc., New York, 2010, s. 22.

⁶⁸ HOSMER, Chet, "Providing the Integrity of Digital Evidence with Time", **International Journal of Digital Evidence**, Yıl: 2002, Cilt: 1, Sayı: 1, s. 1.

⁶⁹ BAYRAM, Levent, **Adli Bilimlerde Ses ve Konuşma İncelemeleri**, Seçkin Yayıncılık, Ankara, 2008, s. 155.

Bu bakımdan toplanan elektronik delillin paketlenmesi işlemine başlamadan önce delillerin doğru bir şekilde dokümanının yapılması ve etiketlenmesi gerekir. Gizli ve görülmeyen delillere özel olarak dikkat edilmeli ve bunların muhafazası için gerekli işlemler yapılmalıdır. Manyetik araçlar, kâğıt veya plastik torbalar gibi anti statik ambalajlara sarılmalı, normal plastik torbalar gibi statik elektrik üreten materyaller kullanılmamalıdır. Disket, CD-ROM veya bantlar gibi bilgisayar araçlarının katlanmaması, bükülmemesi ve çizilmemesi gerekmektedir. Delilleri taşımak amacıyla kullanılan konteynerlerin ise doğru bir şekilde etiketlenmiş olması gerekir⁷⁰.

İmaj alma işlemi mümkünse olay mahallinde bağımsız fiziksel kopyalama cihazları ile gerçekleştirilmeli ve bu imajlar muhafaza edilerek orijinal medyalar adli emanete teslim edilmelidir. Olay yerinde imaj alma mümkün değil ise veri depolama üniteleri mühürlü torbalara konularak şüpheli avukatı huzurunda açılmalı, imaj alınmalı ve akabinde adli emanete teslim edilmelidir⁷¹.

Elektronik delilin taşınması sırasında manyetik alanlardan uzak tutulması gerekir⁷². Radyo vericileri, ısıtmalı koltuklar bu delillere zarar verebilirler. Elektronik delilin araç içerisinde uzun süre bulundurulmaması gerekir. Zira aşırı sıcak, nem veya soğuk elektronik delile zarar verebilir. Diğer taraftan konteynerlere yerleştirilmeyen bilgisayar ve diğer bileşenlerin araç içerisinde şoklardan veya aşırı titreşimlerden etkilenmeyecek şekilde güvenli olarak taşınması gerekir⁷³.

Tüm elektronik delillerde olduğu gibi cep telefonlarında bulunan veriler de adli bilişim sürecinde değişikliğe veya bozulmaya karşı korunmalıdır. Cep telefonlarının diğer cep telefonlarıyla veya hücresel ağlarla bağlantı kurmasına izin verilmesi bu cihazlarda bulunan elektronik verilerin zarar görmesine neden olabilir. Bu yüzden, cep telefonları tüm

⁷⁰ KESER BERBER, 2004, s. 72.

⁷¹ ÇAKIR / SERT, 2011, s. 159.

⁷² MUKASEY, Michael B. / SEDGWICH, Jeffrey L. / HAGY, David W., **Electronic Crime Scene Investigation: A Guide for First Responders**, Second Edition, PhotoDisc, Inc, Washington, 2001, s. 21.

⁷³ KESER BERBER, 2004, s. 72.

ağlardan izole edilmelidir. Bunun için ise radyo sinyallerini veya diğer telefonlarla bağlantıyı engelleme özelliği olan faraday poşetleri (faraday bags) kullanılmalıdır⁷⁴.

Nitekim cep telefonlarının faraday poşetlerinde taşınması, taşınma sırasında telefona gelebilecek aramalar ve kısa mesajların engellenmesini ve ayrıca telefonun hizmet aldığı son konum bilgisinin değişmemesini sağlamaktadır. Aksi halde telefona gelebilecek arama ve kısa mesajlar sonucunda kişilerin son arama listesi ve mesaj kutusu değişebilir ve hatta silinen mesajlar üzerine veri yazıldığı için tekrar elde edilmeleri engellenebilir. Ayrıca, şüphelinin en son hizmet aldığı konum bilgisi de taşıma esnasında değişerek delillerin orijinalliği bozulabilir⁷⁵.

Son olarak belirtmek gerekir ki; elektronik medyanın muhafazasında yeterince özen gösterilmemesi halinde bu elektronik medya bozulabilmekte, kaybolabilmekte veya özelliğini kaybedebilmektedir. Bu bakımdan adli emanete teslim edilecek olan orijinal medya, mühürlü torbada muhafaza edilmelidir⁷⁶. Diğer taraftan adli emanete ya da incelenmek üzere laboratuvara götürülen her bilişim sisteminin, toz, nem, rutubet, aşırı ısı ve manyetik alanlar gibi zararlı olabilecek etkilerden uzak tutulması sağlanmalıdır⁷⁷.

SONUÇ

Son dönemde bilişim alanında gerçekleşen baş döndürücü ilerleme sonucunda bilişim sistemleri gerek suçların işlenmesi gerekse işlenmiş olan suçların ispatında önemli bir unsur haline almıştır. Gerçekten de geçmişi çok eskilere dayanmayan elektronik delil kavramı esas olarak bilişim suçlarının soruşturulmasında gündeme gelmekte ise de kimi zaman klasik suçların soruşturulmasında da önemli bir ispat aracı olarak kendinden söz ettirmektedir.

⁷⁴ DANIEL, Larry / DANIEL, Lars, **Digital Forensics For Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom**, Syngress Publishing, Waltham, 2012, s. 265; MUKASEY / SEDGWICH / HAGY, 2001, s. 21.

⁷⁵ AYDOĞAN, 2009, s. 14.

⁷⁶ ÇAKIR / SERT, 2011, s. 160.

⁷⁷ HENKOĞLU, 2011, s. 26.

Elektronik delilin ceza yargılamasında ispat aracı olup olmayacağı, olacaksa da ne ölçüde bunu sağlayacağı tartışmaları halen devam etmekte ise de bu delil türü ile ilgili tartışma konusu olmayan en önemli husus ise elektronik delilin kolay bozulmaya elverişli olması ve bu nedenle de bu delile ilk temas edildiği andan mahkemeye getirilinceye kadar geçen süreçte azami dikkat ve özenin gösterilmesi gerekliliğidir.

Elektronik delilin ilk elde edildiği andan raporlama işlemi yapılarak mahkemeye sunulduğu ana kadar devam eden sürecin bütünü ihtiva eden adli bilişim sürecinin ilk safhası elektronik delilin toplanması ve muhafazası aşamasıdır. Bu aşama işlenen bir suçta kullanılması ve olayın çözümünde önemli bir unsur teşkil eden bir elektronik delilin bozulma ihtimalinin en yüksek olduğu zaman dilimini ihtiva eder. Zira ilk elde edildiği anda yanlış kişiler ve yanlış işlemlere muhatap olan bir elektronik delilin bütünlüğünün ve geçerliliğinin korunması büyük risk taşımakta olup bu da muhakemenin ilerleyen aşamalarında soru işaretlerine neden olmaktadır.

Bu bakımdan elektronik delilin toplanması aşamasında uyulması gereken temel ilkelere riayet edilmesi, bu aşamada elektronik verinin bütünlüğünün ve geçerliliğinin korunması için gerekli canlı analiz, imaj alma, hash değerinin tespiti, zaman damgasının alınması, koruma zincirinin sağlanması işlemlerinin yerine getirilmesi ve elde edilen elektronik verinin paketlenmesi, taşınması ve muhafazası işlemlerinde azami hassasiyetin gösterilmesi yürütülen soruşturma ve kovuşturma sürecinin selameti bakımından büyük önem taşımaktadır.

KAYNAKÇA

- AKARSLAN, Hüseyin, **Bilişim Suçları**, Seçkin Yayıncılık, Ankara, 2012.
- AKTEPE, Basri, “Emniyet Personelinin Bilgisayar ve Bilgisayarla İlişkili Suçlarla Mücadelede Dikkat Etmesi Gereken Hususlar (Adli Tıp Esaslarına Uygun Olarak Delillendirme)”, **1. Polis Bilişim Sempozyumu (21-22 Ekim 2003)**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2004, (s. 66-69).
- ARSLAN, Çetin, “Dijital Delil ve İletişimin Denetlenmesi”, **Ceza Hukuku ve Kriminoloji Dergisi (CHKD)**, Yıl: 2015, Cilt: 3, Sayı: 2, (s. 253-266).
- AYDOĞAN, Hakan, **Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.
- BAYRAM, Levent, **Adli Bilimlerde Ses ve Konuşma İncelemeleri**, Seçkin Yayıncılık, Ankara, 2008.
- BUCAK, Yeşim, **Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü, 2019.
- CASEY, Eoghan, “Error, Uncertainty, and Loss in Digital Evidence”, **International Journal of Digital Evidence**, Yıl: 2002, Cilt: 1, Sayı: 2, https://www.academia.edu/2983793/Error_Uncertainty_and_Loss_in_Digital_Evidence, (erişim tarihi: 02.02.2020).
- CASEY, Eoghan, **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**, Third Edition, Academic Press, California, 2011.
- COSIC, Jasmin / COSIC, Zoran, “Chain of Custody and Life Cycle of Digital Evidence”, **Computer Technology and Application**, Yıl: 2012, Cilt: 3, Sayı: 2, (s. 126-129).
- COSIC, Jasmin / BACA, Miroslav, **(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp**, https://www.academia.edu/15316896/Im_proving_chain_of_custody_and_digital_evidence_integrity_with_time_stamp (erişim tarihi: 02.02.2020).

- ÇAKIR, Hüseyin / SERT, Ercan, “Bilişim Suçları ve Delillendirme Süreci”, Örgütlü Suçlar ve Yeni Trendler, **Uluslararası Terörizm ve Sınırşan Suçlar Sempozyumu (UTSAS 2010)**, (der. Oğuzhan Ömer Demir ve Murat Sever), Ankara, 2011, (s. 143-170).
- DANIEL, Larry / DANIEL, Lars, **Digital Forensics For Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom**, Syngress Publishing, Waltham, 2012.
- DEĞİRMENCİ, Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Seçkin Yayıncılık, Ankara, 2014.
- DELİDUMAN, Seyithan, “Elektronik Verilerin Delil Değeri”, **Bilişim Hukuku**, (der. Mete Tevetoğlu), Kadir Has Üniversitesi Yayınları, İstanbul, 2006.
- EKİZER, A. Hakan. **Adli Bilişim (Computer Forensics)**, <https://www.ekizer.net/adli-bilisim-computer-forensics/>, (erişim tarihi: 02.02.2020).
- GÖZÜŞİRİN, Mesih, 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2011.
- GÜNDÜZ, M. Zekeriya, Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yayınlanmamış Yüksek Lisans Tezi, Elazığ, Fırat Üniversitesi Fen Bilimleri Enstitüsü, 2012.
- HAGY, David W., “Integrity, Discovery, and Disclosure of Digital Evidence”, **Digital Evidence in the Courtroom**, (ed. J. D. Nilsson), Nova Science Publishers, Inc., New York, 2010.
- HENKOĞLU, Türkey, **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, Pusula Yayıncılık, İstanbul, 2011.
- HOSMER, Chet, “Providing the Integrity of Digital Evidence with Time”, **International Journal of Digital Evidence**, Yıl: 2002, Cilt: 1, Sayı: 1, (s. 1-7).
- KESER BERBER, Leyla, **Adli Bilişim**, Yetkin Yayınları, Ankara, 2004.
- KARAGÜLMEZ, Ali, “Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular”, **2. Polis Bilişim Sempozyumu (14-15 Nisan 2005)**, Emniyet Genel Müdürlüğü. Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2005, (s. 30-34).

- KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2. Basım, Seçkin Yayıncılık, Ankara, 2011.
- KILIÇ, Mehmet Serkan, “Elektronik Deliller ve Yapısal Özellikleri”, **Adli Bilişim ve Elektronik Deliller**, (ed. Hüseyin Çakır / Mehmet Serkan Kılıç), Seçkin Yayıncılık, Ankara, 2014, (s. 137-158).
- KUNTER, Nurullah / YENİSEY, Feridun / NUHOĞLU, Ayşe, **Açıklamalı Ceza Muhakemesi Kanunu**, Cilt I, Beta Yayınevi, İstanbul, 2013.
- MASON, Stephen, **International Electronic Evidence**, BIICL, London, 2008.
- MUKASEY, Michael B. / SEDGWICH, Jeffrey L. / HAGY, David W., **Electronic Crime Scene Investigation: A Guide for First Responders**, Second Edition, PhotoDisc, Inc, Washington, 2001.
- ORTA, Mesut, **Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)**, Yetkin Yayıncılık, Ankara, 2015.
- ÖZBEK, Murat, “Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları”, **1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (20-21 Mayıs 2013)**, Elazığ, 2013, (s.1-7),
https://www.academia.edu/31927878/Adli_Bilisim_Uzmani_Murat_OZBEK_isdfs_bildiri2013_04_11 (erişim tarihi: 24.02.2020).
- ÖZBEY, Özcan, “Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK’nın 134. Maddesi)”, **Yargıtay Dergisi**, Yıl: 2010, Cilt: 36, Sayı: 3, (s. 61-126).
- ÖZDİLEK, Ali Osman, **Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku**, Vedat Kitapçılık, İstanbul, 2006.
- ÖZTÜRK, Mustafa İlker, **Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri**, Yayımlanmamış Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2007.
- SARIAKÇALI, Turgay, **İnternet Üzerinden Akdedilen Sözleşmeler**, Seçkin Yayıncılık, Ankara, 2008.

- SOYSAL, Tamer, “İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu”, **Türkiye Barolar Birliği Dergisi**, Yıl: 2005, Sayı: 61, 2005, (s. 304-339).
- SAY, Kubilay, **Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarında İncelenmesi**, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.
- ŞEN, Bilal, “Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller”, **Ankara Barosu Uluslararası Hukuk Kurultayı (11 Ocak-15 Ocak 2010)**, Cilt. 3, Ankara Barosu Yayınları, Ankara, 2010, (s. 69-70).
- ŞEN, Osman Nihat, “Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi”, **2. Polis Bilişim Sempozyumu (14-15 Nisan 2005)**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2005, (s. 35-41).
- ŞEKER, Güven, “Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum”, **Uluslararası İnsan Bilimleri Dergisi**, Yıl: 2004, Cilt: 1, Sayı: 1, (s. 1-13).
- ŞİRİKÇİ, Ahmet Serhat / Cantürk, Nergis, “Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi”, **Bilişim Teknolojileri Dergisi**, Yıl: 2012, Cilt: 5, Sayı: 3, (s. 29-34).
- TÜRKTRUST, Zaman Damgası Nedir?, <https://www.turktrust.com.tr/tr/urunler/zaman-damgasi/> (erişim tarihi: 02.02.2020).
- ÜNVER, Yener / HAKERİ, Hakan, **Ceza Muhakemesi Hukuku**, 1. Cilt, 8. Basım, Adalet Yayınevi, Ankara, 2013.
- YETİM, Servet, “Dijital Kanıt Araştırma Yöntemleri”, **İstanbul Barosu Dergisi**, Yıl: 2008, Cilt: 82, Sayı: 3, (s. 1201-1222).