Elektronik Delillerde Arama ve El Koyma

Tuncay Beşikçi

Middlesex University, UK

Abstract

This paper explores the legal, technical, and procedural aspects of searching and seizing electronic evidence in the context of criminal investigations in Turkey. The discussion includes relevant national legislation, international frameworks, and key forensic principles required to ensure the integrity, reliability, and admissibility of digital evidence in criminal trials.

Elektronik delillerde arama ve el koyma

Delil, yargılama konusu olayın açıklığa kavuşturulması, maddi gerçeğin ortaya çıkarılması için ispat amacı ile kullanılan araçlardır. Delilsiz mahkûmiyet olamayacağından, ceza yargılamalarında delil elde etme işlemi ile çok önemli bir ameliye olarak karşılaşılmaktadır.

Bilişim sistemlerinin yaygınlaşmasıyla, delil elde etme bağlamında dijital delillerin (elektronik delil veya sayısal delil olarak da anılır) önemi gittikçe artmaktadır. Bilişim sistemleri ile ilgili olay yeri inceleme, arama ve el koyma işlemlerine dair hususlar asıl olarak, 17 Aralık 2014 tarihinde Resmi Gazete'de yayımlanan Ceza Muhakemesi Kanunu ("CMK") 134. maddesinde ve 24 Mayıs 2003 tarihinde Resmi Gazete'de yayımlanan "Adlî ve Önleme Aramaları Yönetmeliği'nin "Bilgisayarlarda, bilgisayar programlarında ve

kütüklerinde arama, kopyalama ve el koyma" başlıklı 17. maddesinde açıklanmıştır. Maddi gerçeğin ortaya çıkarılması ve adil bir muhakeme yapılabilmesi için olay yerinin layıkıyla korunması ve delillerin dürüst bir şekilde olay yerinden elde edilmesinin sağlanması gerekmektedir.

Yargıtay Ceza Genel Kurulu'nun 19 Nisan 1993 tarihli 1993/108 numaralı kararında, "Gerçek; akla uygun ve realist, olayın bütününü veya bir parçasını temsil eden kanıtlardan veya kanıtların bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa bir takım varsayımlara ulaşılarak sonuca ulaşılması Ceza Muhakemesinin amacına kesinlikle aykırıdır" tespitinde bulunarak delillerin sahip olması gereken özelliklerin çerçevesini çizdiği anlaşılmaktadır.

Bu kapsamda delillerde bulunması gereken özellikler şu şekilde sıralanmıştır.

- Kanuna uygun olarak elde edilmiş olması
- Beş duyu organımızla algılanabilmesi
- Maddi gerçeğin ortaya çıkarılmasına aracılık etmesi
- Doğruluğu ve gerçekliği konusunda şüphe içermemesi
- Delil veya delil ile ilgili raporun herkese açık olması
- Mümkünse farklı deliller ile desteklenebilmesi

Elektronik deliller de tıpkı diğer delillerde olduğu gibi, mahkeme önüne getirilmeden önce, diğer tüm delillerin taşıdığı özelliklere de sahip olmalıdır. Yasal yollardan elde edilmiş olmalı, iddiaları doğrulayan nitelikte gerçek olmalı, tam ve tekrarlanabilir (üçüncü şahıslar tarafından incelendiğinde aynı sonuçlara ulaşılabilir) olmalı, delilin elde edilmesi konusunda herhangi bir şüphe olmamalı ve mahkemeler tarafından anlaşılabilir olmalıdır.

Dijital veri içeren herhangi bir delilin "mutlak delil" özelliği gösterebilmesi için öncelikle herhangi bir suç katoloğunun kanun tarafından öngörülmemiş olması gerekmekte, ele geçirildiğinde mutlaka nerede, kimden ve tam olarak ne zaman ele geçirildiği, ele geçiren kişi ve yapılan işlemin hukuki dayanağı da dâhil olmak üzere kayıtlara geçirilmeli ve tutanak altına alınmalıdır. Yine bu işlemin üzerinde analiz yapılacak nüshasını (adli imaj) oluşturmak amacı ile veya taraflara verilmek üzere ne şekilde kopyalandığı ve hangi yöntemlerin kullanıldığı yazılı hale getirilerek tutanak altına alınmalıdır. Adli kopyalama sırasında orijinal verinin veya dosyanın mutlaka günün teknolojisi ile uygun özet ("HASH"), yani değişmezlik değeri alınmalıdır.

Dijital deliller, gözle görülemeyen, soyut verilerden oluşmaktadır. Bu delillerin varlığının anlaşılabilmesi, diğer delillerden farklı olarak yardımcı cihaz ve yazılımlar ile mümkün olabilmektedir. Örneğin, bir metin belgesinde bulunan veriyi görüntüleyebilmek için ekran veya yazıcı çıktısı gereklidir. Bu yöntemlerde dahi dosyaya ait üstveri bilgilerini görmek mümkün olmayacaktır. Bu nedenle, rapor kapsamında incelenen dava dosyasında da yer almış benzer çıktılar, delilin kendisi değildir, delilin kendisi bizzat dijital ortamdaki halidir. Dijital delillerin yapısal özellikleri şu şekilde sıralanabilir :

- Kolaylıkla kopyalanabilir ve çoğaltılabilirler
- Manyetik alan, sıcaklık, nem gibi sebeplerle bozulabilirler
- Üzerinde işlem yapılarak kolayca değiştirilebilirler
- Tekrar elde edilemeyecek şekilde silinebilirler
- Gizlenmiş veya şifrelenmiş başka verileri üzerlerinde barındırabilirler

Dijital veriler yukarıda sayılan özelliklerinden dolayı kolayca manipüle edilebilmektedir. Bu nedenle, dijital verilerin delil olarak kabul edilebilmesi için aslına uygun olduklarının ve değiştirilmemiş olduklarının ispat edilmesi de zorunludur. Dijital delillerde bulunması gereken bazı özellikleri de şu şekilde sıralamak mümkündür:

- Akla uygun ve kabul edilebilir olmalıdır
- Gerçek olmalıdır
- Hatasız ve doğru olmalıdır
- Eksiksiz ve tam olmalıdır
- Güvenilir ve itimat edilebilir olmalıdır
- İnandırıcı olmalıdır
- Tekrar edilebilir olmalıdır
- Mevcut yasal düzenlemelere uygun olmalıdır

Adlî ve Önleme Aramaları Yönetmeliği'nin "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 17. maddesinde belirtilen hususlara uyulması delil güvenilirliği, delil zincirinin korunması ve delillerin mahkemelerce "hukuki" olarak kabul edilebilmesi açısından oldukça önemlidir.

Bilgisayar, bilgisayar programlarında ve kütüklerinde, arama, kopyalama ve el koyma tedbiri ise CMK'nın 134. maddesinde düzenlenmiştir.

Delil bütünlüğü ve güvenilirliği açısından CMK m. 134'te yer alan hususlara uygun işlem yapılması elzemdir. Zira bu hüküm uyarınca bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi

için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bununla beraber bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. İstenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (CMK m. 134/2, 3, 4, 5).

Bu koşullardan, özellikle, bilgisayarlara el konulması esnasında sistemdeki bütün verilerin yedeklemesinin yapılması ve bu yedekten bir kopyanın şüpheliye veya vekiline verilmesi çok önemlidir. Önceki dönemde bu talep hakkından çoğu avukatın dahi haberdar olmaması nedeniyle atıl olan bir hüküm, madde metninde yapılan değişiklikle zorunlu hale getirilmiştir. Ancak, inceleme yapılacak olan hard diskten yedek alınması yeterli değildir. Delillerin alındığı aşamadaki sıhhatinin korunması amacıyla, işlemi yapan kolluk tarafından, bilgisayarın hard diski alındığı anda öncelikle HASH değeri alınarak tutanak tutulmalı ve bütün bu imaj alma, yedekleme vb. işlemler şüpheli veya vekilinin yanında gerçekleştirilmelidir. Zira, söz konusu yedekleme işlemi yapılmaz ve kişinin bilgisayarına öylece el konulursa, sistemde değiştirilmesi son derece basit olan verilerin, bilgisayarına el konulan kişi aleyhine değiştirilmesi durumunda kişinin hiçbir güvencesi kalmayacak ve bu durum neticesinde kişi en temel hak ve özgürlüklerine halel gelecek biçimde mağdur olabilecektir. Nitekim, CMK'nda yer alan koruma tedbirleri kişilerin temel hak ve özgürlüklerini kısıtlayıcı tedbirler olduğundan, bu tedbirler uygulanırken muhakeme yönünden doğabilecek zararın ağırlığı ve bunun gerçekleşmesi ihtimalinin yoğunluğu ile

orantılı olması gerekliliğinin yanı sıra, tedbir uygulanırken aleyhine uygulanan kişinin temel hak ve özgürlüklerinin hukuki sınırları aşar biçimde sınırlandırılmamasına ve kişisel verilerinin zarar görmemesine dikkat edilmesi gerekmektedir. Zira, özellikle CMK m. 134'teki koruma tedbirinin uygulanmasında, ceza muhakemesinin amacına uygun bir şekilde kişisel verilerin korunması, tedbiri uygulayan makamların birincil görevi olmalıdır .

Bir adli inceleme sırasında elde edilen deliller mahkeme huzuruna sunulduğunda, her türlü şüpheden uzak olarak ilk bulundukları şekilde olduğu, üzerinde herhangi bir değişiklik, ekleme veya çıkarma yapılmadığı, depolama birimine sonradan kaydedilmediği, kısaca her türlü şüpheden uzak olarak isnat edilen suçu ispatlaması beklenir. Ancak bu durumda dijital delillerin geçerliliğinden bahsedilebilecektir. Elde edilen dijital delilin orijinaline uygunluğunun kanıtlanabilmesi için bazı mekanizmalar geliştirilmiştir. Bu mekanizmalardan en önemlisi veri bütünlüğünü kontrol etmek için kullanılan, tek yönlü özetleme algoritması olarak da tanımlanabilecek HASH bilgisidir. HASH veya Özet değeri, Adli Bilişim incelemelerinde uygulanan yöntemlerin, delili değiştirmediğini ispat etmek için kullanılmaktadır. HASH değer verilerde yapılacak en küçük değişikliği ortaya çıkarma açısından oldukça kullanışlıdır.

Elde edilen dijital deliller hukuka uygun olarak elde edilseler bile, tarafların bilgisine sunulmadan ve mahkemede tartışılmadan hükme esas alınamayacaktır. CMK 217. Madde uyarınca hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir.

Sonuç olarak, elektronik delillerin hukuki geçerliliğinin denetlenmesinde öncelikle hukukun temel gerekleri olan ve diğer delillerde bulunması gereken özellikler olan gerçeklik, akılcılık, erişilebilirlik, olayı temsil edicilik, müştereklik ve hukuka uygunluk özelliklerine sahip bulunması zorunludur. Delilin müştereklik özelliğinin gereği olarak, bir ceza yargılamasında öne sürülen elektronik delilin, davanın bütün taraflarınca bilinir ve tartışılabilir olması zorunludur.

Türk Hukukunda elektronik delilin ceza yargılamasında bir delil türü olarak kabul edilip edilmeyeceği, kabul edildiği takdirde ise elektronik delilin tek başına mahkûmiyet kararı vermek için yeterli olup olmayacağı hususlarında farklı görüşler yer almaktadır.

Bir görüşe göre, soruşturma sırasında delil olarak elde edilen elektronik verilerin bilgisayar ortamında tutulmalarından dolayı, silinebilir, değiştirilebilir veya yenilenebilir nitelikte olmaları nedeniyle hukuki anlamda çok sağlam delil kategorisinde değerlendirilmemektir. Elektronik delillerin ceza yargılamasında tek başına mahkûmiyete yetecek kuvvette olmadığı yönündeki diğer bir görüşe göre, elektronik verilerin içeriğinin değiştirilebilir nitelikte olması, bu verilerin tek başlarına delil olma gücünü zayıflatmakta ve hatta ortadan kaldırmaktadır. Bir başka görüşe göre, elektronik verilerin delil olarak kullanılması, çoğu zaman ek delillerle desteklenmesini veya başka araştırmalar yapılmasını gerekli kılmaktadır. Bununla birlikte, elektronik delilin sağlamlığının ortaya konulması bilirkişi incelemesini gerekli kılmalıdır. Bu bakımdan, elektronik verilerin ceza yargılamalarında delil olarak kullanılabilmesi, üzerinde çok kolay oynama yapılabilen ve fakat bu tür oynamaların da teknik olarak belirlenmesi mümkün olan verilerin sağlamlığı CMK madde 66 uyarınca bilirkişi tarafından inceleme yapılarak kontrol edildikten sonra hiçbir değişikliğe uğramadan mahkeme huzuruna getirilmesine bağlıdır.

Elektronik verilerin yazıcı çıktılarının veya içerik fotokopilerinin ceza yargılamalarında delil niteliğine haiz olması, yazıcı çıktılarının mutlak şekilde doğrulanması ve kabul edilebilirliğinin ispatlanmasına bağlıdır. Bu bağlamda dijital ortamda saklanan verinin çıktısı alınan nüsha ile aynı olması durumunda, çıktısı olarak alınan elektronik veri de delil niteliğine sahip olacaktır. Bununla birlikte çıktı olarak alınan elektronik verinin gerçekliğini yitirmesi, temsil ediciliğini kaybetmesi durumunda ise delil olarak değerlendirilmesi mümkün olmayacaktır.

Türkiye Cumhuriyeti'nin Avrupa Birliği müktesebatına daha fazla uyum sağlamak amacı ile, gerekli tüm uluslararası sözleşmelere taraf olacağını taahhüt etmiş ve bunların etkin şekilde uygulanmasını sağlayacak tedbirleri alacağını beyan etmiştir . Dijital ve İnternet suçlarını gözeten ilk uluslararası sözleşme olma özelliğini taşıyan Siber Suçlar Sözleşmesi, "6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" adıyla 2 Mayıs 2014 tarihinde Resmi Gazete'de yayımlanarak yasalaşmış, Türkiye Cumhuriyeti'nin taraf olduğu (ve Sözleşme'nin Türkiye açısından bağlayıcılık durumu bulunduğu) Siber Suç Sözleşmesi'nin 15. Maddesinin 1. fıkrasında, sözleşmeyi kabul eden ülkelere, bilişim sistemlerinde delil elde etme ve kullanma sırasında sahip olunan temel hakların korunmasına ve orantılılık ilkesine uygun kullanılmasını zorunlu kılar .

Avrupa Konseyi'nin liderlik ettiği ve Türkiye'nin de yer aldığı bir AB projesinde, yürütülen çalışmaların bir çıktısı olarak; "Elektronik Delil Rehberi; Kolluk, Hakimler ve Savcılar İçin Temel Rehber" isimli bir belge hazırlanmıştır ("AK Elektronik Rehber Taslağı" olarak adlandırılacaktır). Rehbere göre, bilişim sistemlerinde arama ve el koymada elde edilen dijital delillerin; özgün olması, soruşturulan olayla objektif bir

bağlantısının bulunması ve bu bağlantının değişmemiş olması, güvenli olması, elde edilen delillerin ne şekilde toplandığı ve ne şekilde işleme tabi tutulduğu konularında bir şüphe bulunamaması, inandırıcı ve anlaşılabilir olması gerekmektedir. AK Elektronik Delil Rehber Taslağı, elektronik delillerin taşınması için gerekli olan genel ilke ve prensipleri de belirleyerek, soruşturmaya konu bilişim sistemlerinde değişikliğe neden olabilecek hiçbir harekette bulunulmayacak ve delillerin ilk elde edilmesinden itibaren delil zinciri oluşturulacaktır. İkinci ilke, elektronik delil elde edilirken yapılan her işlemin, üçüncü bir şahıs tarafından tekrarlanarak izlenebilir olmasıdır. Bu ilke gereği, yapılan her işlem kayıt altına alınmalı ve alınan bu kayıtlar sayesinde aynı işlem, başka bir uzman tarafından tekrarlanması halinde aynı sonuçlara ulaşacaktır. AK Elektronik Delil Rehberi'nde yer alan 3. temel ilke, uzman veya harici bilirkişi yardımından zamanında yararlanılmasıdır. Rehberin 5. ve son teme ilkesinde ise hukuka uygunluk ilkesidir. Rehbere göre her üye ülke kendi iç hukuk kurallarını uygularken, hükümleri yorumlamada yukarıda sayılan temel ilkeleri göz önünde bulundurmalıdır.

A.B.D. müktesebatında, dijital delillerin ne şekilde aramaya tabi tutulup, bunlara el konulacağı hususlarını, Federal Adalet Bakanlığı tarafından yayınlanan bir rehberde düzenlenmiştir. A.B.D. anayasının bir parçası olan Dördüncü Değişiklik'e göre (İng. "The 4th Amendment") soruşturmalarda icra edilecek arama ve el koymalarda aranacak şüphe derecesi makul şüphe olacaktır. A.B.D.'nin elektronik delillerin toplanması, işlenmesi ve saklanmasına ilişkin hususların, Depolanmış İletişim Bilgileri Kanunu'nda (İng. Stored Communication Act) yer alır.

Bilişim sistemlerinde adli arama ve el koyma işlemleri ayrıca; İngiltere (Computer Misuse Act), İrlanda (Criminal Damage Act madde 2/1 ve 2/a), Fransa (Ceza Kanunun

323-2), Almanya (Ceza Kanunu 303a) ve Norveç (Ceza Kanunu madde 156) gibi ülkelerde de, A.B.D. mevzuatındakine benzer şekilde delillerin kabul edilebilirliği aşamasında usul hukuku açısından katı kurallara tabi tutulmuştur. [30].

Sonuç

Ceza soruşturmalarında dijital delillerin incelenmesi, modern adli ve hukuki süreçlerin temel bileşenlerinden biridir. Bu çalışmada da ortaya konduğu üzere, elektronik deliller doğası gereği uçucu, kolayca değiştirilebilir ve özel araçlar olmadan doğrudan gözlemlenemeyen niteliktedir. Bu durum, hukuki, teknik ve usuli güvenlik önlemlerine sıkı sıkıya uyulmasını zorunlu kılmaktadır. Türkiye'de Ceza Muhakemesi Kanunu'nun 134. maddesi ve Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesi gibi düzenlemeler, dijital verilerin aranması, kopyalanması ve el konulması süreçlerini tanımlamaktadır. Ancak, bu düzenlemelerin pratikte uygulanmasında yaşanan tutarsızlıklar, delil zincirinin korunması, veri bütünlüğü ve temel hakların ihlali gibi endişeleri beraberinde getirmektedir.

Dijital delillerin kabul edilebilirliği için gereken özgünlük, güvenilirlik, tekrarlanabilirlik ve yasal yollarla elde edilme kriterlerinin titizlikle karşılanması gereklidir. HASH değerleri, adli imaj alma süreçleri ve zamanında belgelendirme gibi mekanizmalar, delilin bütünlüğünün sağlanmasında kritik öneme sahiptir. Buna ek olarak, Avrupa Konseyi'nin Elektronik Delil Rehberi ve Budapeşte Siber Suçlar Sözleşmesi gibi uluslararası standartlar da, orantılılık, yasallık ve şeffaflık ilkelerine vurgu yapmaktadır.

Ancak Türk yargı uygulamalarında dijital delillerin tek başına mahkûmiyet için yeterli görülmediği yönünde bir tereddüt mevcuttur. Bu durum, dijital verilerin fiziksel ya da

tanıksal delillerle desteklenmesi ve uzman incelemeleriyle doğrulanması ihtiyacını doğurmaktadır. Kolluk, adli bilişim uzmanları ve yargı mercileri arasında disiplinler arası iş birliği, delilin güvenilirliğini artıracaktır.

Neticede, elektronik verilerin hukuki geçerliliği yalnızca teknik doğrulukla değil, aynı zamanda yasal usullere uygunluk ve bireysel hakların korunmasıyla mümkündür. Dijital suçların ve delil teknolojilerinin gelişimi, hukuk sistemlerinin de eş zamanlı olarak gelişmesini, adaletin sağlanmasını ve temel hakların korunmasını zorunlu kılmaktadır. Türkiye'nin uluslararası sözleşmelere uyum sağlama sürecinde, dijital delillerin kullanımı sadece yasal doğrulukla değil, aynı zamanda insan haklarına saygıyla da yürütülmelidir.

Kaynaklar:

Hakeri, H (2005) "Yeni Ceza Muhakemesi Kanununa Göre El Koyma Koruma Tedbiri", TBB Dergisi, S.60, Y.2005, s97-104

Koca, M. (2006). Ceza Muhakemesi Hukukunda Deliller. CHD 1(2), Aralık Türkiye: Seçkin Yayınevi Sayfa 207

Bıçak,V. (2011) Suç Muhakemesi Hukuku (2. Baskı) Türkiye: Seçkin Yayınevi, sayfa 461

Kaygısız, M (2007) Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği, Adalet Yayınevi, 1. Baskı,Ankara, Sayfa 39

Kaygısız, M (2007) Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği, Adalet Yayınevi, 1. Baskı, Ankara, Sayfa 39

Casey, E. (2004) Digital evidence and computer crime (2nd Edition) ABD: Academic Press, Sayfa: 218

Değirmenci, O. (2014) Ceza Muhakemesinde Sayısal (Dijital) delil. Türkiye: Seçkin Yayınevi, Sayfa: 363

Değirmenci, O. (2008) "Ceza ve Ceza Muhakemesi Hukukunda Mağdur Hakları", Türkiye Barolar Birliği Dergisi, Sayı:77, ss. 33-86

Toplaoğlu. N, Çakır H. (2014) Adli Bilişim ve Elektronik Deliller, 1. Baskı, Seçkin Yayıncılık, Ankara

Peter Sommer, Digital Footprints: Emerging Issues in Computer Forensics, http://pmsommer.com/digifootprint07.pdf (15.5.2016)

Ankara Barosu Dergisi, 2005/1, Kaynak:

Toroslu, Nevzat / Feyzioğlu, Metin; Ceza Muhakemesi Hukuku, Ankara, 2006.

Küzeci, Elif; Kişisel Verilerin Korunması, Ankara, 2010, s. 291 vd

Toplaoğlu. N, Çakır H. (2014) Adli Bilişim ve Elektronik Deliller, 1. Baskı, Seçkin Yayıncılık, Ankara

Doğan, Koray (2018), Ceza Muhakemesinde Belirsizlik Kuşkudan Sanık Yararlanır İlkesi, 2. Baskı, Seçkin Yayıncılık, Ankara, s:297

Başlar, Yusur, Ceza Yargılamasında Elektronik Delil, Yenkin Yayınları, 1. Baskı, Ankara 2016, s:92

İsmail Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara: Adalet Yayınevi, 2008, s:44

Veli Özer Özbek, Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi, s:185-186

Murat Kızılyar, Ceza Yargılamasında Dijital Verilerin Delil Değeri", Adalet Dergisi, Sayı 50, Eylül 2014, s:72-89

Kunter Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s:1109

Halid Özkan, Ceza Muhakemesinde Ekran Görüntüsü Çıktıların Delil Niteliği, Yener Ünver(ed) Ceza Muhakemesi Hukukunda Delil ve İspat içinde. Ankara: Seçkin Yayıncılık, 2014, s:282

Olgun Değirmenci, Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği, Terazi Hukuk Dergisi, Cilt:9, Sayı:97, Eylül 2014, s:14-28

http://ab.gov.tr/index.php?p195&1=1

[Görüntülenme tarihi: 8 Mart 2013]

Electronic Evidence Guide; A Basic Guide for Police Officers, Prosecutors And Judges, [Erişim tarihi: 8 Mart 2013]

AK Elektronik Delil Rehberi, s:14

AK Elektronik Delil Rehberi, s:14

AK Elektronik Delil Rehberi, s:15

Department of Justice (USA), [Erişim tarihi: 8 Mart 2013]

Henkoğlu, Türkay, Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, 2. Baskı (2014), s:196

Tuncay Beşikçi
Middlesex University, UK