ELEKTRONİK KOPYANIN (ADLİ İMAJ) ALINMASINDA AÇIK KAYNAK UYGULAMALARININ GÜVENİRLİĞİ

Hayrettin CATALKAYA, Muhammer KARAMAN, Erdal KOCA
War Colleges Command, Army War College, Student Officer, İstanbul, Türkiye
hcatalkaya@gmail.com, muammerkaraman29@gmail.com, erdalkoca@yandex.com

ÖZET

Usulüne uygun toplanmış ve analize tabi tutulmuş deliller, suçun aydınlatılmasında soruşturma makamı için temel istihbarat kaynağıdır. Delilin incelenmesi aşamasında kullanılan bilimsel teknikler, doğru yer ve zamanda kullanıldığında doğruluğu yüksek bilgi sağlayan temel kaynaklar arasında yer almaktadır. Elektronik deliller günümüzde kolluk kuvvetlerinin en fazla rastladığı deliller arasında bulunmaktadır. Elektronik delillerin; kolaylıkla değiştirilebileceği, iz bırakmadan silinebileceği ve yoktan var edilebileceği gerçekleri karşısında, sayısal delillere el konulmasının, toplanmasının, analiz ve rapor edilmesinin önemi bugün daha iyi anlaşılmaktadır. Delili toplayan veya muhafaza altına alan birimler delil bütünlüğünün korunarak ceza adalet sistemine hukuki delil olarak girdi yapılmasından sorumludur. Bilgisayar, bilgisayar kütükleri ve programlarında arama ve el koyma işlemi CMK'nın 134. maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde yer alan muğlâk ifadeler, elektronik delillerin tespiti ve toplanması aşamasında art niyetli kullanılmasına fırsat sağlamaktadır. Elektronik delillerin nasıl kopyalandığından(imaj oluşturma) ziyade, bütünlüğünü sağlayacak donanım ve yazılımların kullanılması ön plana çıkmaktadır. Günümüzde adli kopyalama işlemlerinde yüksek maliyetli adli kopyalama donanımlarının yanında açık kaynak adli kopyalama yazılımları da kullanılmaktadır. Bu çalışmada, açık kaynak uygulamalar ile yapılan adli kopyalamanın bütünlüğü ve güvenirliği konusu ele alınmış, mevcut yapılarda iyileştirilmeler önerilmiş, delillere ilk müdahaleden raporun teslimine kadar geçen sürede yapılması gerekenlerin ayrıntılı olarak düzenlenmiştir. Bu makale, ISDFS 2015'de sunulmuş olup seçilerek bu dergide yayımlanmıştır.

Anahtar Kelimeler: Elektronik Delil, Adli Kopya (imaj), CMK 134, Açık Kaynak Uygulamaları, Delilin Toplanması, Bilgisayar Adli İncelemesi, Yazma Koruma

RELIABILITY OF OPEN SOURCE APPLICATIONS IN ACQUIRING THE DIGITAL COPY(FORENSIC IMAGE)

ABSTRACT

The evidence appropriately collected and subjected to analysis is basic intelligence source for the investigating authorities to the elucidation of the crime. Scientific techniques used in examining the evidence, are among the main sources providing high information if they are used accurately, used in the right place and time. Digital evidence today are among the mostly faced evidence by the security forces. In the truth of being easily changed, deleted without a trace and created from the scratch, the digital evidence's importance in the seizure, aqquisition, analysis and reporting is beter understood today. The units collecting and preserving the evidence are responsible for ensuring the integrity of evidence, providing legal inputs to the criminal justice system. Ambigous expressions in CMK's Article 134 and Judicial and Prevention Searches Regulation Article 17, about the search and seizure process in computers, computer folders and programs serve an opportunitiy to malevolent people in detection and collection of evidence. The tools and softwares that provide integrity of the evidence is more important than how the digital evidence is acquired. Today, open source forensic acquisition tools are being used besides highly cost forensic

duplicate hardware tools. In this study, the subject of integrity and security of forensic duplication in open source tools is handled, improvements are recomended and to do's ranging from first respond to evidence to reporting are arranged in detail.

Keywords: Digital Evidence, Forensic Images, CMK 134, Open Source Tools, Evidence Collection, Computer Forensics, Write Protection.

I. GİRİŞ (INTRODUCTION)

Sanayi toplumunda kullanılan insan ve makine gücünün yerini, bilgi toplumunda düşünce ve akıl gücünün alması ile toplumların kullanımında olan vasıtalar dönüşüme uğramıştır. 90'lı yılların başından itibaren ülkemizde kullanılmaya başlayan bilgisayar ve bilişim sistemleri zaman içerisinde hızlı bir artış göstermiştir. Suçluların hızlı değişimin yaşandığı teknoloji dünyasına ayak uydurmakta gösterdiği başarı devlet bünyesinde karşılığını bulamamıştır. Hayatımızın bir parçası olan elektronik cihaz ve veri depolama aygıtlarının, bir suça tanık olması, ipucu veya kanıtlar barındırması günümüzde sıkça rastlanılan bir durumdur. Bu durum suçun aydınlatılmasında elektronik delillerin önemini her geçen gün artırmaktadır [1]. Toplumda bilişim suçları, bilgisayar suçları olarak da bilinmektedir. Bilgisayar teriminden: "Programlara ve verilen komutlara göre işlem yapan, otomatik olarak çalışan, sıralı işlem yapan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan, elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanılabilme özelliklerine sahip elektronik cihazlar" [2] anlaşılmaktadır. Aslında bilgisayar bilişimin bir unsuru olup, bilişim faaliyetinin gerçekleşmesinde önemli bir etken cihazdır.

Günümüzde olay yerinde klasik suç delillerinden farklı olarak elektronik delillere sıkça rastlanmaktadır. Delil ihtiva etmesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin yazma korumalı bir ortamda ve dijital imzalı doğrulaması yapılmış olarak birebir alınmış kopyaları üzerinde gerçekleştirilmelidir [3]. CMK'nın 134. Maddesinde: "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir." ifadesi yer almaktadır. Söz konusu kopyaya "adli kopya" veya "imaj" adı verilmektedir.

Günümüzde bu kopyalama (imaj alma) işlemleri çeşitli donanım veya yazılımlar kullanılarak gerçekleştirilmektedir. Adli kopyaların teknik incelemesi ardından hazırlanan teknik inceleme raporunun sorgulanması Anglo-Sakson ve Kıta Avrupası hukuk sistemlerinde, 30 yıllık bir geçmişe sahiptir. 1980'lerin ortasından başlayıp 1990'lardan itibaren ABD'de "uzman görüşünün" rutin bir süreç dâhilinde delil olarak kabul edilmesi bilim adamları tarafından yüksek sesle tartışılmaya başlanmıştır [4].

Son dönemlerde, klasik sistemde tarafların inisiyatifine bırakılmış olan bilirkişi raporu hazırlanması konusu mahkemelerin yetkisi içine alınması eğilimi gözlenmektedir [5]. Kıta Avrupası'ndaki mahkemeler resmi olarak görevlendirilmiş bilirkişinin ulaştığı sonuçları kabul edebilir ya da etmeyebilirler [6]. ABD Yüksek Mahkemesinin "Daubert v. Merrell Dow İlaç A.Ş." hakkındaki davada bilirkişi ifadesini bilimsellikten uzak olarak ifade etmesi [7] sonucundaki süreçte, bilimsel delil hakkındaki düşünce: "Teknik verilerle ulaşılan sonuçların genel kabul edilebilir olmasından ziyade her koşul altında aynı sonucu vermesi" yönünde değiştiği görülmüştür [8].

II. DİJİTAL DELİLLERİN KOPYALANMASI
(ACQUIRING DIGITAL EVIDENCES)

A. Adli Kopya ve Özet (Hash) Değeri

Olay yerinden elde edilen bir nesnenin delil olarak kabul edilebilmesi için bütünlüğünün korunmuş olması gerekmektedir. CMK Md. 217/2 fıkrasında "yüklenen suç, hukuka uygun elde edilmiş her türlü delille ispat edilir" hükmü ile hukuka uygun elde edilen her türlü delilin suçu aydınlatmada kullanılabileceği vurgulanarak, kabul edilme şartı hukuka uygun elde edilmesine bağlanmıştır. Yine CMK 206. maddesi, kanuna aykırı olarak elde edilen delillerin ret edileceği hükmünü içerir. Elektronik delilin geçerli sayılabilmesi için kanuna uygun elde edilmiş olması gerekmektedir. Elektronik delillerin (E-delil), elde edilmesine yönelik hususlar CMK'nın 134. Maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. Maddesinde "Bilgisayar, bilgisayar kütükleri ve programlarında arama el koyma" başlığı ile düzenlenmiştir.

CMK'nın 134/2'nci fıkrasında; *"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." ifadesi yer almaktadır. 134/3'üncü fıkrasında; "*Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır."* ifadesine yer verilmektedir. 134/5'inci fıkrasında ise "*Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir."* Şeklinde ifade edilmektedir. E-Delillere "Hangi hallerde el konulacağı ve kopyalanmasına" yönelik hususlar bu şekilde açıklanmıştır.

CMK'nın 134. Maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. Maddesinde ayrıntılı olarak tanımlanmamış olsa da e-delillerin toplanmasında, klasik delillerin toplanması sürecinde olduğu gibi "delilin usulüne uygun toplanması" yani "değiştirilmeksizin (bütünlüğü korunarak) ceza adalet sistemine girdi yapılması" gerekir. Öte yandan hukuk sistemine, dolayısıyla da hukuk kurallarına aykırı biçimde elde edilmiş delil olarak tanımlanabilecektir. Gerek mahkeme kararlarında gerekse de öğretide çok doğru biçimde dile getirilen "hukuka aykırılık" kavramı "yasaya aykırılıktan" daha geniş bir anlama sahiptir [9]. "Hukuka aykırılık" en başta milli hukuk sistemimiz içinde yürürlükteki tüm hukuk kurallarına aykırılık anlamına gelir. Bu çerçevede; anayasaya, usulüne uygun olarak kabul edilmiş uluslararası sözleşmelere, kanunlara, kanun hükmünde kararnamelere, tüzüklere, yönetmeliklere, içtihadı birleştirme kararlarına ve teamül hukukuna aykırı uygulamaların tümü "hukuka aykırılık" kavramı içinde yer alır [10]. Hukuka aykırı olarak elde edilmiş delilin akıbeti konusunda da tartışmalar olmakla birlikte, söz konusu e-delil "usulsüz ulaşılan delil" ya da "hukuka aykırı delil" olacağından dolayı kolayca reddedilebilecektir [11].

Söz konusu bilgiler ışığında, elektronik delillerin toplanmasında veya elde edilmesinde önemli olan husus kopyalama yapan yazılım/donanımın çıktısının, kopyası alınan veri depolama aygıtının birebir aynısı olması ve değiştirilmesi durumunda bunun tespit edilebilmesidir.

Günümüzde doğrulama işlemi özeti (sayısal doğrulama değeri) değeri kullanılarak yapılmaktadır. Bu sayısal doğrulama değeri tek yönlü algoritmik bir fonksiyondur. Tek yönlü olma özelliği sayesinde bu değerden geriye dönülerek, doğrulama değeri hesaplanan veri parçasına ulaşılması hesaplama zamanı açısından pratikte mümkün olmamaktadır. Sayısal doğrulama değerinin kullanım alanlarından birisi de orijinal veri ile o verinin adli kopyasının birbirleri ile aynı olup olmadığını karşılaştırmaktır [12]. Günümüzde kullanılmakta olan tek yönlü sayısal doğrulama değerleri: Snefru, N-Hash, MD4, MD5, SHA serisi ve diğerleridir [13].

Elektronik delilin bütünlüğünün korunmasına ilişkin kontrol verisi sayısal doğrulama değeri olup, kopyalamanın yazılım veya donanım kullanılarak gerçekleştirilmesinin hiçbir önemi yoktur. Sadece kopyalama işlemini yapan yazılım veya donanımın veriyi değiştirmeksizin kopyalaması istenmektedir.

B. Adli Kopyalama Yöntemleri

Bilgisayar veya bilgisayarı kütüklerinin kopyalanması işleminde donanımsal ve yazılımsal teknikler kullanılmaktadır. Hangi teknik kullanılırsa kullanılsın, hukuka uygun delil olması için e-delilin bütünlüğünün bozulmamış olması gerekmektedir. E-delilin bütünlüğün korunarak kopyalanmasında, kopyalamayı gerçekleştiren yazılım ya da donanımdan; herhangi bir müdahale olmaksızın (e-delil içerisine veri girişi veya çıkışı, I/O) işlemin gerçekleşmesi veya işlemin ardından sayısal doğrulama değerinin üretmesi gibi ihtiyaçları karşılaması beklenmektedir.

1. Donanımsal Kopya Alma

Şekil 1. Adli Kopyalama Cihazları

Adli kopya alma işlemi için özel olarak geliştirilmiş cihazlar kullanılarak kopya alma işlemidir. Söz konusu cihazların bir girişine delil diski diğer girişine de kopyanın içine alınacağı disk bağlanarak işlem gerçekleştirilir. Burada delil diskinin bağlı olduğu girişin yazma korumalı olması sebebi ile delil bütünlüğünün bozulması ihtimali söz konusu değildir. İşlem sonucunda sayısal doğrulama değeri üretilir (Bkz. Şekil 1.).

2. Yazılımsal Kopya Alma

Donanımsal imaj almada kullanılan cihazların maliyetlerinin yüksek olması kolluk kuvvetlerini ücretsiz ve güvenilir alternatifler aramaya itmiş olup bu kapsamda kullanılan yazılımsal imaj alma tekniklerini iki başlık altında toplayabiliriz.

a. Çalıştırılabilir CD'ler Vasıtasıyla;
İnternet üzerinden ücretsiz olarak temin edilebilen ve delil bilgisayarına takılarak, CD üzerinde yüklü olan işletim sisteminin çalıştırılması ve delil disklerinin yerlerinden sökülmeksizin adli kopyalarının alınması işlemidir. Donanımsal kopya almaya oranla daha fazla eğitim gerektirmektedir. İşlem sonucunda Sayısal Doğrulama Değeri üretilir. En çok kullanılan adli inceleme amaçlı hazırlanmış çalıştırılabilir CD'ler; FCCU Gnu/Linux Boot CD, Helix Boot CD, Caine Boot CD, Backtrack Boot CD vb.

b. Adli İnceleme Yazılımları Kullanılarak;
Adli incelemede kullanılan programların hemen hemen hepsinin adli kopya alma bölümü bulunmakta olup delil diski programın çalıştığı bilgisayara yazılımsal veya donanımsal yazma korumalı olarak bağlanması suretiyle kopyanın alınması işlemidir. Bu işlem sonucunda da sayısal doğrulama değeri üretilir.

TABLO I. ADLI KOPYALAMA YÖNTEMİ KARŞILAŞTIRILMASI

Adli Kopyalama Teknikleri		İlave Yazma Koruma İhtiyacı	Bağlantı Tipi	Sayısal Doğrulama Değeri
Donanımsal Kopyalama Cihazları		Yoktur.	IDE/EIDE/ ATA/SATA/ATAPI /SCSI I/SCSI II/SCSI III/USB/ Kart Okuyucu/ Disket/Firewire	Var.
Yazılımsal Kopyalama	Çalıştırılabilir CD'ler Kullanılarak Kopyalama	Kısmen Vardır.	Çalıştığı Bilgisayarın Veri Girişi Bağlantılarına Göre Değişiklik Gösterir.	Var.
	Adli Bilişim Yazılımları Üzerinden Kopyalama	Kısmen Vardır.		Var.

Söz konusu teknikler karşılaştırıldığında, yazılımsal tekniklerin bir kısmında yazma koruma özelliği bulunmasına rağmen bir bölümünde bu özelliğin mevcut olmadığı görülmektedir. Her iki yöntem sonucunda da sayısal doğrulama değeri üretildiği görülmüştür (Bkz. Tablo I.).

Delilin bozulmasını engellemek için depolama birimlerinin kopya alacak donanım veya yazılımın çalıştığı bilgisayara yazma korumalı olarak bağlanması gerekir. Yazma koruma donanımları, adli kopyalama cihazı veya işletim sisteminden herhangi bir komutun diske gitmesini engellemek üzere tasarlanmıştır [14].

Söz konusu cihaz veya yazılımlar sayesinde, kopyalama yapan donanım veya yazılımdan, delil depolama birimine veri transferi önlenmiş olur. Yazılımsal yöntemlerle kopyalamanın, ilave yazma koruma ihtiyacı eksikliğini gidermek için ilave yazma koruma cihazları kullanılmaktadır (Şekil 2.).

Şekil 2. Yazma Koruma Cihazları

Uygun yazma koruma cihazları ile koruma altına alınmış delillerin kopyalanması için kullanılacak donanım veya yazılım işlevsel olarak aynıdır. Aralarındaki fark; hız, raporlama, kopya format gibi adli mercilerin, şüpheli ya da sanığın ihtiyacı olmayan ayrıntılardan ibarettir. Kaldı ki söz konusu verilerden hız durumsal farklılıklar gösterebilmektedir. Yani her seferinde aynı hız olmama ihtimali mevcuttur. Intel Core i5 işlemci, 1.80GHz hız ve 4.00 GB RAM sahip bilgisayar kullanılarak, 2 GB (1.928Mb) kapasiteli çubuk (flash) diskin, farklı kopyalama teknikleri ve donanımlar kullanılarak adli kopyalama işlemi gerçekleştirilmiştir. Kopyalama işlemi sırasında özel bir yazma koruma donanımı kullanılmamıştır. Kopyalama işleminde;

- Açık kaynak kodlu Caine GNU/Linux işletim sisteminde çalışan GuyMaker ve Linux DD açık kaynak kodlu kopyalama yazılımları,
- TD-3 donanımsal kopyalama cihazı,
- Adli bilişim yazılımları (X-Ways, EnCase, FTK) üzerinden kopyalama işlemleri gerçekleştirilmiştir.

Yapılan kopyalama neticesinde ulaşılan sonuçlar "TABLO II" de sunulmuştur.

Üç farklı adli kopyalama tekniği kullanılarak alınan birebir kopyaların MD5 sayısal doğrulama değerinin aynı olduğu görülmüştür. Yapılan uygulama ile sayısal doğrulama değerinin, kullanılan yazılım veya donanıma göre değişiklik göstermeyeceği görülmüştür.

III. SONUÇLAR (CONCLUSIONS)

Ceza adalet sisteminin sağlıklı işlemesinde ihtiyaç duyulan güvenilir veya kabul edilebilir delil, değiştirilmemiş ve el koyulduğundaki hali ile birebir aynı olmalıdır. E-delillerin kopyalanmasında, uygulamayı gerçekleştirenin (kolluk, bilirkişi, vb.) delilin "ayna görüntüsünü" [16] aktarabilmesi gerekmektedir. Elektronik delillere ilk müdahale kritik önemde olup, elektronik delillerin yok olmasına veya değişmesine neden olabilecek riskler ile doludur. Çalışan sistemin kapatılmaması, kapalı sistemin açılmaması şeklinde basite indirgenemeyeceği düşünülen ilk müdahale uzman personel tarafından gerçekleştirilmelidir. Yazma koruma donanımlarının ilk amacı, sabit disk üzerindeki tüm veriye erişim imkânı verirken, kullanıcının alanında her hangi bir değişikliği engellemektir [17]. Tüm verinin okunmasına imkân verirken, disk üzerine yazmaya engel olmaktır.

TABLO II. ÖRNEK DİSKİN KOPYALANMASI SONUÇLARI

Yazılım/ Donanım	Süre (sn)	Ortalama Hız (MB)	Kopya Boyutu (GB)	MD5 Özet
TD-3	86	31,75	1,87	Değişmedi
GuyMaker	106	14,37	1,97	Değişmedi
Linux DD	87	2,10	2,00	Değişmedi
FTK İmager	90	21,87	1.96	Değişmedi
EnCase	115	16,54	1,90	Değişmedi
X-Ways	87	22,63	1,96	Değişmedi

Adli kopyalama cihazları ile kopyalama yapılırken, ayrı bir yazma koruma ünitesine ihtiyaç duyulmamaktadır. Söz konusu cihazlara bağlanan delil diskleri bu cihazlar içerisinde yer alan özellikler sayesinde yazma korumalı olarak bağlanmaktadır. Kopyalamanın yazılımsal olarak gerçekleştirilmesi durumunda, farklı bir yazma koruma yazılım ya da donanımının kullanılması gerekmektedir. Adli kopya alma yazılımlarının bir kısmı beraberinde yazma koruma özelliği bulundurmaktadır. Fakat bu özelliğin aktife edilerek, delil diskinin bütünlüğünü korunması bilişim uzmanının yeterliliğine bağlıdır. Delillerin kopyalanması işleminin yazma korumalı olarak gerçekleştirilmiş ve işlem sonucunda özet (hash) değerinin üretilmiş olması taraflar veya adli makamlar için en sağlıklı dayanaklardır.

Mevzuatlarımızda e-delillere ilk müdahaleden raporlama aşamasına kadar geçen sürede yapılması gerekenlere yönelik düzenlemelere ihtiyaç olup e-delillerin elde edilmesi aşamasında uyulması gerekli hususların bu düzenlemelerin başında geldiği değerlendirilmektedir. İlk planda ele alınması gerektiği düşünülen hususlara ilgili değerlendirmeler aşağıda verilmiştir. Bunlar;

- E-delillerin elde edilmesi aşamasında kullanılacak yazılım ve donanım uygulayıcıların inisiyatifine bırakılmayacak kadar hayati öneme sahip olup kullanılacak donanım ya da yazılımın güvenirliğinin ve kabul edilebilirliğinin test edilmesi gereklidir. Buna yönelik test ve denemelerin ülkemizde de tek elden yapılmasına ihtiyaç vardır. ABD'de söz konusu testler Standartlar Enstitüsü'nde (NIST) e-deliller bölümü tarafından yapılmakta olup ülkemizde de buna benzer yapılanmalar kurulmalıdır.
- Ülkemizde, adalet sisteminin aktörleri tarafından kabul edilecek ve uygulayıcıların kullanabileceği kabul edilebilirlik testinden geçirilmiş adli kopyalama yazılım veya donanımlarının üretilmesine ihtiyaç vardır. Söz konusu yazılım veya donanım ülkemiz kolluk kuvvetlerinin bu konudaki dışarıya bağımlılığı azaltacak, ülkemizde bu alandaki bilgi birikimini arttıracaktır.
- Delillere ilk müdahaleden raporun teslimine kadar geçen sürede yapılması gerekenlerin ayrıntılı olarak düzenlendiği delil elde etme ve raporlama süreci (delil zinciri) oluşturularak ülkemiz mevzuatlarına eklenmeli, e-delillerin kabul edilebilirliği söz konusu sürecin doğru ve eksiksiz işletilmesine bağlanmalıdır.
- E-delillerin olduğu bir davada, şüpheli veya sanık kopyalamada değişim olmadığına emin olmak isterken, hâkim veya savcı da delilin usulüne uygun toplandığına emin olmak ister. Delil toplama sürecinin oluşturularak, bu süreç içerisinde kullanılacak yazılım ve donanımın test edilmiş olması söz konusu kuşkuları en aza indirecektir.
- Ülkemizde dijital delil zinciri oluşturma aşamalarının iyileştirilmesine ihtiyaç olduğundan, uluslararası deneyimlerden ve standartlardan mutlaka faydalanılmalıdır.

VI. KAYNAKLAR (REFERENCES)

[1] M. Brunker (2011, Kasım), "Digital evidence becoming central in criminal cases, Avaiable: http://insidedateline.nbcnews.com

[2] L. Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayıncılık, Ankara, 2005
[3] H. Ekizer, (2014, Şubat), "Adli Bilişim", Avaible: http://www.ekizer.net/adli-bilisim-computer-forensics
[4] Henry F. Fradella, Lauren O'Neill, and Adam Fogarty The Impact of Daubert on Forensic Science, 31 Pepp. L. Rev. 2 (2004)
[5] E. Demirkapı, "Anglo Amerikan Hukukunda Bilirkişilik Kurumunda Yeni Eğilimler", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2003, Cilt 5, Sayı 2, Sf. 72.
[6] "Yargılamada Bilirkişilik Müessesesi Hakkında Mukayeseli Çalışma Görüşme Taslağı", Dünya Bankası, 30 Haziran 2010, Sf. 57
[7] "Daubert v. Merrell Dow Pharmaceuticals" (92-102), 509 U.S. 579 (1993).
[8] P. Huber, "Junk Science in the Courtroom." Val. UL Rev. 26 (1991): 723.
[9] G. Akyürek, Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu, Union of Turkish Bar Associations Review, 61
[10] Anayasa Mahkemesinin E: 1999/2 (Siyasi Parti Kapatma), K: 2001/2 sayılı Kararı, www.resmigazete.gov.tr (Erişim Tarihi:23.01.2015)
[11] V. Bıçak, "Suç Muhakemesi Hukuk" Seçkin, Ankara, 2011, Sf. 519-538.
[12] D. Kleiman, "The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators", Syngress, Burlington, s.10.
[13] Angelo, M. F. (1999). U.S. Patent No. 5,887,131. Washington, DC: U.S. Patent and Trademark Office.
[14] National Institute of Standards and Technology, "Hardware Write Blocker (HWB) Assertions and Test Plan", 21 Mart 2005, s.9.
[15] M. Özbek, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", 1st International Symposium on Digital Forensics and Security (ISDFS'13), May 2013.
[16] L. K. Berber, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma", Ankara Barosu Bilişim Kurulu, 9 Temmuz 2008.
[17] J. R. Lyle, "A strategy for testing hardware write block devices." Digital Investigation 3 (2006): 3-9.