

Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları

Murat ÖZBEK

İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Hukuku Enstitüsü, İstanbul/Türkiye, mur.ozbek@gmail.com

Özet—Adli bilişim alanında yapılan inceleme ve değerlendirme çalışmaları elektronik delillerden alınan adli kopyalar üzerinden yapılmaktadır. Hukuki olarak uygulamada adli kopyası alınmış olan orijinal elektronik delil üzerinden tekrar adli kopya alınarak hash değerleri kıyaslanmakta ve kıyaslama sonucu hash değerlerinde uyumsuzluk söz konusu olursa elektronik aygıt üzerinde değişiklik yapıldığı gerekçesiyle delil olarak kabul edilmemektedir. Bu çalışmada, orijinal delillerde bozulmalar olabileceği veya çalışma yapıları itibariyle şahısların müdahalesi olmaksızın kayıtlı olan verilerde değişiklikler olabileceği hakkında bilgiler verilmiştir. Hukuki açıdan yapılan uygulamalarda: delil üzerinde veri bütünlüğünün korunup korunmadığının kontrolü için tekrar orijinal delil üzerinden adli kopya alınması ve hash hesaplatılması gibi bir yol izlenmemesi gerektiği; bu kontrol işleminin, önceden alınmış olan adli kopya üzerinde değişiklik olup olmadığı şeklindeki hash hesaplatma çalışmalarıyla yapılmasının uygun olduğu sonucuna varılmıştır.

Anahtar kelimeler—Adli Bilişim, adli kopya, hash sorunları, ssd disk incelemeleri, optik disk incelemeleri, sabit disk incelemeleri

Abstract—Analysis and investigations in computer forensic are carried out on forensic images. Pertaining to law, when a forensic image is made of the original electronic evidence which already had a forensic image, and the hash values of both images are compared, the electronic device in question is not accepted as evidence when the comparison result are incompatible. In this study, information reveals that there may be deterioration of the original evidence, or there may have been changes in the provided data without the intervention of individuals because of their operating structure. Applications made from a legal point of views: that for the control of data integrity of the evidence, there should not be taken a new forensic image of the original evidence and make a hash calculation; for this control process, we take hash calculation using the first taken forensic image to determine if there have been changes.

Keywords—Computer forensic, forensic image, hash issues, ssd forensic, cd-dvd forensic, hard disk forensic

1. GİRİŞ

Adli Bilişim; bir olay yeri incelemesi veya bir kurban üzerinde yapılan otopsinin eşdeğeridir. [1] Sayısal verileri elde

etme, muhafaza etme ve çözümleme işlemlerinin delilin gereklerine uygun olarak mahkemeye sunulması aşamasına kadar uygulanması[2]; özel inceleme ve analiz teknikleri kullanılarak, bilgisayarlar başta olmak üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi süreci kısaca Adli Bilişim (Computer Forensic)[3] olarak açıklanmaktadır. Bu süreç içerisinde elde edilen elektronik deliller:

- Kabul edilebilir(admissible[4]) olmalıdır.

E-delil, dava sırasında hakim veya başka insanlar tarafından kabul edilebilir olmalıdır.

- Gerçek ve aslına uygun(authentic[5]) olmalıdır.

Soruşturma veya kovuşturma altındaki konu ile ilgili doğrudan bir nedensellik bağı veya destekleyici mantıksal bağlar olması gerekir. Nedensellik bağı (illiyet rabitası) aynı zamanda suçun kanun tanımında yer alan maddi unsurlarındandır ve meydana gelen netice ile fail arasındaki neden-sonuç ilişkisini ifade etmektedir[6]. E-delil mahkemede dava konusu olayla ve faille ilgili ve bağlantılı olmalıdır.

- Eksiksiz ve tam(complete[7]) olmalıdır.

Elde edilebilen tüm deliller toplanmalıdır. Bu deliller yalnızca, failin suçlanmasına ilişkin değil, varsa suçsuzluğuna ilişkin olanları da kapsamalıdır. Nitekim 5271 sayılı Ceza Muhakemesi Kanunu'nun 170. maddesinin (4) ve (5) numaralı fıkralarına göre, iddianamede, yüklenen suç oluşturulan olaylar, mevcut delillerle ilişkilendirilerek açıklanmalı; iddianamenin sonuç kısmında, şüphelinin sadece aleyhine olan hususlar değil, lehine olan hususlarda ileri sürülmelidir.[8] Sadece maddi olmamalıdır. Şüphelinin suçlu olduğunu veya suçsuz olduğunu kanıtlayan bir delil olmalıdır.

- Güvenilebilir(reliable[9]) olmalıdır.

E-delil güvenilir olmalıdır. Analiz için kabul edilmiş prosedürlere uygunluğundan ve doğruluğundan şüphe edilmemelidir.

- İnanılabilir(believable[10]) olmalıdır.

E-delil, kanıtlama değerine sahip olmalıdır. Sanal yapıda olsa da[11], hakim veya taraflar tarafından açıkça anlaşılabilir ve inanılabilir olmalıdır.

- Yasaya uygun olmalıdır.

E-delil, yukarıdaki özelliklere sahip olsa da, yasaya uygun bir şekilde elde edilmemiş veya her ne kadar yukarıdaki özellikleri taşıyor olsa da yasaya uygun elde edilmediği için delil olarak değerlendirilemeyecektir. Örneğin 5271 sayılı CMK'nın 134. maddesine aykırı olarak bilgisayarlarda arama, kopyalama veya elkoyma işlemi yapılmışsa[12], elde edilenler mahkeme tarafından delil olarak değerlendirilmeyecektir.

Adli bilişimde elektronik deliller üzerinde yapılacak incelemeler elektronik delilin adli kopyası(forensic image) üzerinden yapılmaktadır. Orijinal delil üzerindeki verilerin değişmemesi için, istisnai durumlar hariç, orijinal delil üzerinde inceleme yapılmamaktadır. Adli bilişimde İngilizce kullanımı “forensic image” olan işlem, Türkçe kaynaklarda “birebir” kopyalama, yabancı kaynaklarda ise “sektör-by-sektör” veya “bit-by-bit” kopyalama işlemi olarak ifade edilmektedir[13]. Veri depolama aygıtlarından yapılan birebir kopyalama işlemine imaj da(forensic image) denilmektedir. Kopyalama işlemi sektör-sektör veya bit-bit denilen şekilde hiçbir veri değişmeden, eksilmeden ve artmadan her veri aynı olacak şekilde, dosya halinde bir başka diske yapılmaktadır. İşletim sistemlerinde günlük hayatta yapılan normal kopyalama işleminde kullanıcılar tarafından görülen dosya veya klasörler bir başka bilişim aygıtına aktarılırken bu işlemde bazı bilgilerin(oluşturma tarihi gibi) değişebilmesinin yanı sıra yapılan işlemde sadece görülmekte olan bilgiler kopyalanır. Hatta 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 üstveriler de kopyalanamamaktadır. Dolayısıyla adli kopya elektronik delil üzerindeki verinin tamamını kapsadığı için incelemeler de adli kopyalar üzerinden yapılmaktadır.

Elektronik delillerden adli kopya alınması sırasında aynı zamanda adli kopyanın hash değeri de hesaplanabilmektedir. Hash tek yönlü bir algoritmik fonksiyondur. Tek yönlü olma özelliği sayesinde hash değerinden geriye dönülerek hash değeri hesaplanan veri parçasına ulaşılması hesaplama zamanı açısından pratikte mümkün olmamaktadır. Hash değerinin kullanım alanlarından birisi de orijinal data ile o datanın adli kopyasının birbirleri ile aynı olup olmadığını karşılaştırmaktır. Hash değerleri eşleştiği zaman, bu verilerin tam bir kopyasının olduğunun kanıtı olarak kabul edilmektedir[14]. Bir veri veya veri depolama biriminin ilk sektörden başlanıp son sektöre kadar tamamının, belirli bir algoritmik fonksiyondan geçirilmesiyle bir hash değeri hesaplanır. Son sektörün de aynı işleme tabi tutulmasıyla ortaya çıkan değere o veriye ait hash değeri denilmektedir. Bu hash değeri verinin değişikliğe uğrayıp uğramadığını kontrolde kullanılmaktadır. Adli bilişimde genellikle kullanılan standart hash algoritmaları şunlardır:

- **MD2, MD4 ve MD5:** bu metotların hash değeri(Message Digest) 128 bit uzunluğundadır. Bu metotlar Ron Rivest tarafından oluşturulmuştur ve çoğunlukla dijital imzalar için kullanılmaktadır. Günümüzde MD2, MD4 ve MD5 metotlarında MD5 metodunun kullanımı daha fazla tercih edilmektedir.

- **Secure Hash Algorithm (SHA):** bu algoritmanın SHA-1, SHA-256, SHA-384 ve SHA-512 olarak birçok çeşidi bulunmaktadır. Bu çeşitlerin aralarındaki fark hash değerinin bit uzunluklarıdır. SHA hash algoritmaları A.B.D’de kurulmuş olan ve çalışmalarına devam eden NIST ve NSA isimli iki birim tarafından hazırlanmıştır[16].

MD5 ve SHA1 hash değerlerine birer örnek aşağıdadır.

MD5: b8e20611dcc4105286bcf56de754f7a3

SHA1: 9f34ac74f28e6ee9f0ad76d7b39d615722822b4f

Hash değeri, hash’i hesaplanan veriye özel ve parmak izi gibi benzersiz bir değerdir. Hash değeri üzerinden tersine mühendislik yapılarak veriye ulaşamaz[15]. Veri depolama birimi üzerindeki bir karakterin bile değişmesi durumunda hash değişmektedir. Dolayısıyla elektronik delil üzerinde veya o delilden alınan adli kopya üzerinde herhangi bir değişiklik olup olmadığını kontrol etmek için hash hesaplatılır. Hash hesaplaması sonucu çıkan hash değeri ile ilk hesaplanan hash değeri birbiri ile aynı ise elektronik delilin veya elektronik delilden alınan adli kopyanın değişikliğe uğramadığı anlamına gelmektedir. Hash değeri elektronik verinin mührü olarak kullanılmaktadır. Uygulamada: açık olan sistemler, RAM’ler ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alındıktan sonra orijinal elektronik delil üzerinde değişiklik olup olmadığını kontrolü amacıyla orijinal delil üzerinden tekrar hash hesaplaması yapılmamaktadır. Çünkü çalışmaya devam eden bu sistemler üzerinde, halen sistem tarafından zararsız ufak değişiklikler olduğundan hash değerleri de değişmektedir.

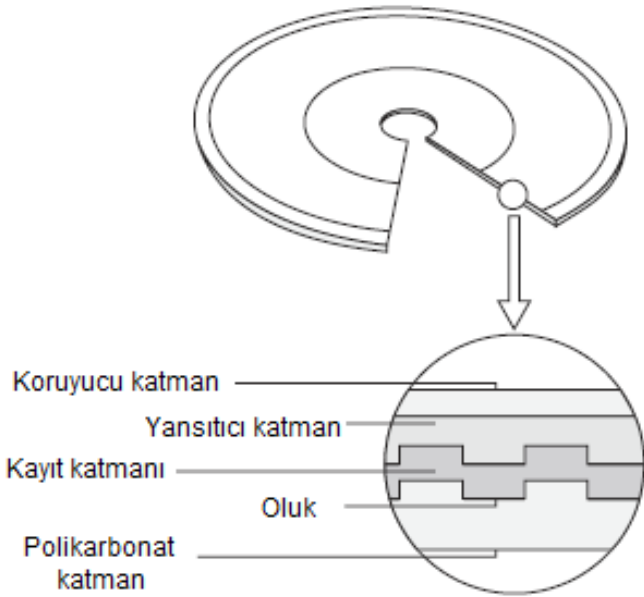
Adli kopya alma işlemi sırasında yapılan uygulamada, adli kopyanın kaydedileceği veri depolama birimine yazılmak için elektronik delil üzerinden okunan verilerin, okundukları esnada hash değeri hesaplanır. Elektronik delil üzerindeki veriler okunduğu esnada hesaplanan hash değeri genellikle adli kopya almakta kullanılan yazılım veya donanım tarafından bir log dosyasına kaydedilir. Adli kopya alma işlemi sona erdikten sonra adli kopya, kayıt edildiği ortamdan baştan sona kadar okunarak okuma sırasında verilerin hash değeri hesaplanır. Bu okuma işlemi sona erdikten sonra hesaplanmış olan hash değeri ile elektronik delil okunduğunda hesaplanmış olan hash değeri kıyaslanır ve kıyaslama sonucunda hash değerleri birebir olarak aynı ise adli kopyanın doğru ve hatasız olarak, okunduğu şekliyle veri depolama birimine kaydedildiği anlamına gelmektedir.

II. HASH PROBLEMLERİ

Elektronik delillerin depolandığı aygıtlar kısıtlı bir kullanım ömrüne ve karmaşık veri depolama yapılarına sahiptirler. CD-DVD gibi optik veri depolama aygıtları, Sabit diskler gibi manyetik veri depolama aygıtları, SSD diskler gibi flash yongalar üzerinde veri depolama teknolojisine sahip aygıtlar; her birinin kendine ait olan teknolojisine ve maruz kaldığı dış etkenlere göre değişen bir kullanım ömrü vardır. Bu veri depolama birimleri arasında veri okuma/yazma ömrü en uzun olan ve en yaygın kullanıma sahip olanı sabit disklerdir ancak mekanik diskler de bir noktada bozulacaktır. Kevin O’Shea’ye göre; belki günler, aylar veya daha uzun sürecek ancak bir noktada bozulacaklardır[18].

A. Optik Diskler

Yaklaşık 30 yıldır kullanımda olan optik diskler(CD-DVD) bu 30 yıl içerisinde büyük bir gelişme gösterdiler. Günümüzde optik diskler için 200 yıla kadar ömür biçilse de onların ne zaman bozulacağını tahmin etmek oldukça güç. Tüm optik diskler, ortak olarak şu dört katmana sahiptirler: koruyucu katman, lazeri yansıtan parlak katman, verileri depolayan alaşımın bulunduğu katman ve polikarbonat katman[19].



Şekil 1. CD-ROM katmanları[20]



Şekil 2. DVD'den kesit[21]

Şekil 1 ve Şekil 2'de görüldüğü gibi farklı optik diskler, farklı katmanlara sahiptirler. Bu katmanlardan özellikle yansıtıcı katman, daha çok hasar görebilmektedir. Standart kompakt diskler, alüminyumdan oluşan bir yansıtıcı katmana sahiptir. Alüminyum, havaya maruz kaldığında oksitlenir. Bu, genellikle diskin kenarlarında gerçekleşir. Ancak diskin bozulmasına tek neden olan, yansıtıcı katmanın bozulması değildir. Kullanım ve muhafaza şartlarına bağlı olarak birçok sebep sayılabilir. Elektronik deliller doğru olmayan şekillerde taşınmaları ve muhafaza edilmeleri sonucunda da bozulabilmektedir.

Adli kopyası alınarak hash bilgisi kaydedilen elektronik delil niteliğindeki bir optik diskten bir süre sonra tekrar adli kopya alma işlemi yapıldığında hesaplanan hash değerleri birbirini tutmayabilmektedir. Bunun sebebi tamamen veya kısmen bozulduğu için okunamayan bir sektör olabildiği gibi daha önceden adli kopya alma işlemi sırasında okunamamış veya yanlış okunmuş ancak sonraki adli kopya alma işleminde doğru şekilde okunabilmiş bir sektörden de kaynaklanabilmektedir. Okunama veya eksik okuma sonucu hash değerlerinin uyuşmaması sorunu sadece optik diskten de kaynaklanmıyor olabilir. Bir optik sürücünün okuyabildiği optik disk üzerindeki veriyi, bir başka optik sürücü okuyamayabilmektedir. Ayrıca bazı adli kopya alma yazılımları arasında optik disk üzerinden okudukları sektör sayılarında fark olabilmektedir. Bu fark aynı programın farklı sürümlerinde de görülebilmektedir.

Bir yazılımın x sayıda sektör okuyarak almış olduğu adli kopyanın hash değeri, diğer yazılımın veya aynı yazılımın diğer sürümünün okumuş olduğu x-1 sayıda veya x+1 sayıda sektör okuyarak almış olduğu adli kopyanın hash değeri ile aynı olmayacaktır.

| Uygulama | Hash değerleri | Sektör sayısı |
|---------------|---|---------------|
| Encase 4 | A296A352F2C8060B180FFE6F32DE6392 (1 Read error) | 1207 |
| Encase 5 | 7A1366AE9CC3A96FD9BF56B9891A633B | 1206 |
| FTK | 44133feb352d37bc365ec210df81d7fd | 1208 |
| X-Ways | 2211A026EC7F309517050D55CEEE2954(2 Read errors) | 1208 |
| MD5sum/readcd | I/O error | 1208 |

Şekil 3. Aynı optik diskten farklı programlarla alınan adli kopyalarda okunan sektör sayıları ve hash değerleri farklı olabilmektedir.

Bir yargılama konusunda elektronik delil olan 16 adet optik disk üzerinde tekrar hash hesaplatılması yaptırılmış ve hesaplanan hash değerlerinden 10 tanesinin daha önce alınan adli kopya sırasında hesaplanmış olan hash değerleriyle uyuşmadığı görülmüştür. Bu uyuşmazlığın kullanılan yazılımın sürüm farkından kaynaklandığı ileriye sürülen süreçte tespit edilmiştir.

| | |
|-------------------|----------------------------------|
| Device | |
| Name | C_4 |
| Actual Date | 01/30/10 11:09:42 |
| Target Date | 01/30/10 11:09:42 |
| File Path | F:\C_4\C_4.E01 |
| Case Number | C_4 |
| Evidence Number | C_4 |
| Examiner Name | BSS |
| Label | TSSTcorp |
| Drive Type | CD-ROM |
| File Integrity | Completely Verified, 0 Errors |
| Acquisition MD5 | 82eb8a2d6c79159f151f1bcec3f2f661 |
| Verification MD5 | 82eb8a2d6c79159f151f1bcec3f2f661 |
| Device | |
| Evidence Number: | C_5 |
| File Path: | C:\imajlar\C_5\imaj\C_5.E01 |
| Examiner Name: | bss |
| Actual Date: | 01/30/10 11:20:48 |
| Target Date: | 01/30/10 11:20:48 |
| Total Size: | 722.372.608 bytes (688,9MB) |
| Total Sectors: | 352.721 |
| File Integrity: | Completely Verified, 0 Errors |
| EnCase Version: | 4.20 |
| System Version: | Windows XP |
| Acquisition Hash: | 7ACA993D4A30FA6BAD4FACE922E8F00F |
| Verify Hash: | 7ACA993D4A30FA6BAD4FACE922E8F00F |

Şekil 4. Bir davada delil olan optik disklerden 2 tanesine ait hash değerleri

| |
|---|
| CD ADI: C-4 |
| MD5 ÖZETİ: 82EB8A2D6C79159F151F1BCEC3F2F661 |
| CD ADI: C-5 |
| MD5 ÖZETİ: 5369094148F74E053FEF1BC172F7863D |

Şekil 5. Şekil 4'teki 2 adet delil olan optik diskten tekrar hesaplanan hash değerleri

Şekil 4 ve Şekil 5'te görüldüğü gibi C_4 isimli optik diske ait tekrar hesaplanmış olan hash değeri önceki hash değeri ile birebir aynı iken, C_5 isimli optik diske ait hash değerleri birbirini tutmamaktadır. Bunun sebebi ise Şekil 4'te görülen ilk adli kopya alımı sırasında C_4 isimli CD'nin Encase v6 sürümüyle adli kopyasının alınması, C_5 isimli CD'nin Encase v4 ile adli kopyasının alınması sonrasında; Şekil 5'te görülen işlemlerde her iki CD'nin de adli kopyalarının Encase v6 ile alınmış olmasıdır. C_4 isimli CD'ye ait hash değeri her iki adli kopya alım işlemi sırasında Encase'in aynı sürümü kullanıldığından aynı hash değerleriyle sonuçlanmıştır. C_5 isimli CD'de ise ilk adli kopya alımının Encase v4 ile ikinci adli kopya alma işleminin ise Encase v6 sürümüyle yapılması sonucu farklı hash değerleri hesaplanmıştır.

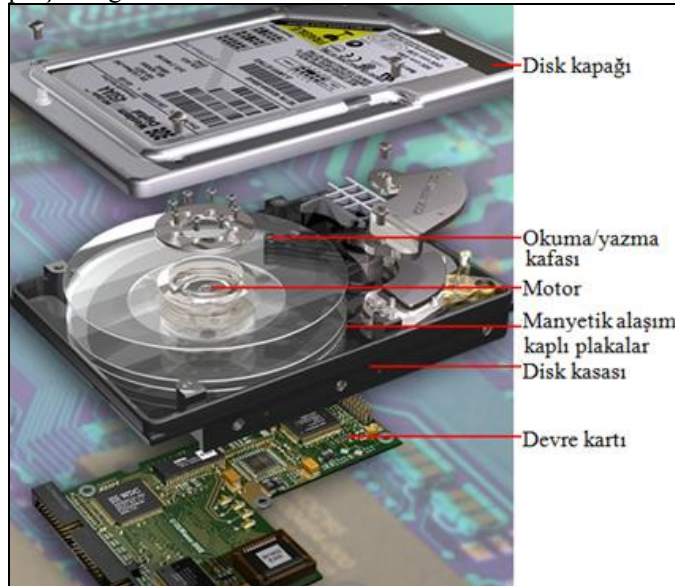
Adli kopyası mevcut olan bir elektronik delil üzerinden tekrar adli kopya alındığında hesaplanan hash değeri daha önceki hash değeri ile uyuşmayabilmektedir.

B. Sabit Diskler

Sabit diskler uçucu olmayacak şekilde ve hızlıca veri depolayan ve depolanan veriye tekrar ulaşmayı sağlayan aygıtlardır. Elektrik kesildiğinde üzerinde yazılı olan veri silinmez. Dolayısıyla bilgisayar kapandığında disk üzerinde kayıtlı olan veriler silinmeyecektir[22].

Sabit diskler manyetik olarak veri depolama yaparlar. Veri sabit disklerin içerisindeki cam, seramik veya metal plaka üzerinde kaplı olan özel alaşımli yüzey üzerinde depolanmaktadır.

Günümüzde genellikle 2.5" ve 3.5" boyutlu sabit diskler kullanılmaktadır ve sabit disklerin IDE, SATA, SAS SCSI gibi çeşitli çeşitleri mevcuttur. Aşağıda Şekil 6'da Sabit disk parçaları görülmektedir.



Şekil 6. Sabit Disk Parçaları[23]

Sabit diskler üretildikten sonra sabit diskin veri depolama yüzeyindeki sorunlu noktaları belirlemek için üretici tarafından bir yüzey testinden geçirilir. Sabit diskler fabrikadan ilk çıktıklarında bile yüzeylerinde sorunlu noktalar mevcuttur. Ayrıca üzerinde veri depolanan bu mekanik yüzeyler zaman geçtikçe ve kullanıldıkça çevresel etkenlerin de etkisiyle

özelliğini kaybedebilmek kullanılamaz hale gelebilmektedir. Hatta hiç kullanılmayan sabit diskler de, üretim maddelerinin ömrü kadar süreyle kısıtlı bir ömre sahiptirler. Fabrikadan çıkmadan önce yapılan yüzey testinde tespit edilen sorunlu noktalar sabit diskler üzerinde bulunan ve normal şartlarda kullanıcıların erişemediği servis alanında bir listede tutulurlar. Bu listede kayıtlı olan alanlara kullanıcı tarafından veri kaydı yapılmamaktadır. Genellikle sabit diskler üzerinde iki farklı bozuk sektör kaydı tutulan liste mevcuttur. Bunlardan birincisi sabit disk fabrikadan çıkmadan önce yapılan yüzey testinde tespit edilen bozuk sektörlerin tutulduğu P-List diğeri ise sabit disk kullanılırken bozulan ve sabit disk içerisindeki yazılım tarafından bozulduğu tespit edilen sektörlerin ve bu sektörler yerine kullanım için atanan sektörlerin bilgilerinin tutulduğu G-List'tir.

P-List içerisinde tutulan bozuk sektör bilgilerine, atlanacak sektörler için kayıt bilgileri de denilebilir. Her sabit diskin farklı sektörlerinde bozukluklar(Bozuk alanlar yada başka birşey) olacağından P-List sabit diske ait benzersiz ve sadece o diske özel bir listedir. Sabit diskin okuma yazma kafası P-list içerisinde kaydı bulunan sektörü daima atlar. Sabit disk içerisindeki adresleme P-List içerisindeki sektörler yokmuş gibi atlanarak yapılmaktadır. Dolayısıyla P-List'ine ulaşamayan veya P-List'inde sorun oluşmuş bir sabit disk üzerindeki sektörler için adresleme P-List'siz bir şekilde yapıldığında verilere doğru bir şekilde ulaşmak mümkün değildir. Bu şekilde ancak küçük boyutlu ve parçalanmadan depolanmış veri parçalarına anlamlı bir şekilde ulaşabilmek mümkündür.

Sabit disk kullanılmaya devam edildiği sürede bozulduğu tespit edilen sektörler ve bu bozuk sektörler yerine kullanıma açılacak olan yedek sektör bilgisi G-List'e eklenir. G-List'e eklenecek bozuk sektörler yerine kullanıma açılacak yedek sektörler belirli bir sayıda olmak üzere sabit diskin veri yazılan yüzeyinde önceden ayrılmışlardır ve bu ayrılmış alana, G-List'e eklenmedikçe, normal şartlarda kullanıcılar erişemezler. G-List'e ekleme işlemleri kullanıcı onayı alınmadan ve kullanıcı fark etmeden olur.

Adli kopya alma işlemi sırasında sabit disk içerisindeki okuma yazma kafası tüm sektörleri okumaya çalışırken sabit diske ait yazılım da bozuk olduğunu tespit ettiği bir sektörü G-List'e ekleyerek onun yerine başka bir sektörü kullanıma atayabilir. Böylelikle sabit disk kullanımı sırasında bozulduğu tespit edilen sektör bilgisi G-List'e eklenerek, yerine yenisi atandığından; bir sabit diskten adli kopya alınması sırasında hesaplanmış olan hash değeri, aynı sabit diskten tekrar adli kopya alındığında hesaplanan hash değeri ile uyuşmayabilir.

Adli kopyası alınarak hash bilgisi kaydedilen elektronik delil niteliğindeki bir sabit diskten süre sonra tekrar adli kopya alma işlemi yapıldığında hesaplanan hash değerleri birbirini tutmayabilmektedir. Bunun sebebi tamamen veya kısmen bozulduğu için okunamayan bir sektör olabildiği gibi daha önceden adli kopya alma işlemi sırasında okunamamış veya yanlış okunmuş ancak sonraki adli kopya alma işlemi doğru şekilde okunabilmiş bir sektörden de kaynaklanabilmektedir. Okumama veya eksik okuma sonucu hash değerlerinin uyuşmaması sorunu sadece sabit diskten de kaynaklanmıyor olabilir. Adli kopya almakta kullanılan bazı

yazılımların veya donanımların okuyabildiği sektörleri diğer yazılım veya donanımlar aynı kararlılıkta okuyamayabilmektedir. Dolayısıyla daha önceden adli kopyası alınmış bir sabit diskin tekrar adli kopyası alındığında hesaplanan hash değerleri farklı olabilecektir.

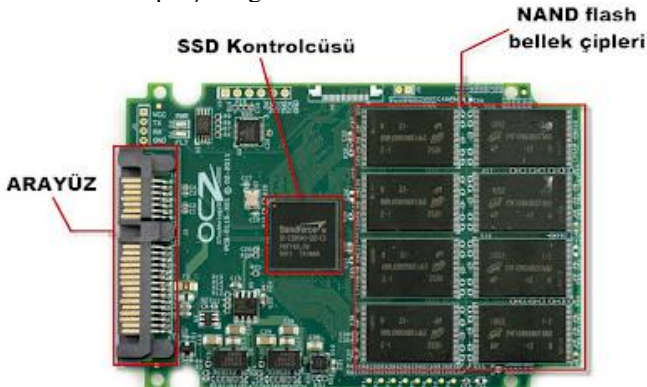
C. SSD Diskler

SSD(Solid State Drives) diskler yapısal özellikleri, kendisine bir anlamda ismini de vermiştir. SSD'lerde, diğer manyetik depolama ünitelerinden farklı olarak, herhangi bir hareket eden parça yoktur. Bu da onların Solid State, yani Katı Hal Sürücüsü olarak adlandırılmasına neden olmuştur[24]. Aşağıda Şekil 7'de farklı arayüz bağlantılarına ve farklı şekillere sahip SSD diskler görülmektedir.



Şekil 7. Çeşitli SSD diskler

Henüz kapasitelerinin düşük ve fiyatlarının yüksek olması sebebiyle yaygın olarak kullanılmasa da zaman ilerledikçe veri okuma/yazma yönünden daha hızlı, daha az enerji tüketimine sahip ve sarsıntı gibi dış etkenlere daha dayanıklı oldukları için daha çok tercih edileceklerdir. Bilgisayar üreticilerinin pazara sunduğu bilgisayarlarda daha yüksek performans için, kullanmayı daha çok tercih etmeye başlamalarına paralel olarak adli bilişim alanında da her geçen gün daha sık karşılaşılan SSD diskler, üzerlerinde bulunan Nand flash yongalarında veriyi depolamaktadır. Şekil 8'de SSD disk üzerindeki ana parçalar görülmektedir.



Şekil 8. SSD Disk Parçaları[25]

SSD disklerin mekanik bir yapıda veri depolamaması ve okuma yazma işlemini sabit disklerdeki gibi hareketli parçalarla yapmamasından dolayı veriye erişim için beklenmesi gereken süre oldukça düşüktür. Sabit disklerde veriye erişmek için öncelikle veri yazılı plakaları döndüren motorun belirli bir hıza ulaşması gerekmekte ve daha sonra okuma/yazma kafası veri yazılı yüzeyi tarayarak okumaya başlamaktadır. SSD diskler ise mekanik tabanlı olmaması yani hareketli parça içermemesi ve flash bellek tabanlı elektronik tümleşik devrelerden imal edilmesi, uygulamada pek çok faydayı da beraberinde getirmektedir. Öncelikle, okuma ve

yazma işlemleri, sabit disklerdeki başlıkların yaptığı gibi mekanik olarak uygulanmadığı için, erişim süreleri oldukça düşüktür ve günümüzde 0.1 ms'ye kadar düşmüştür[26].

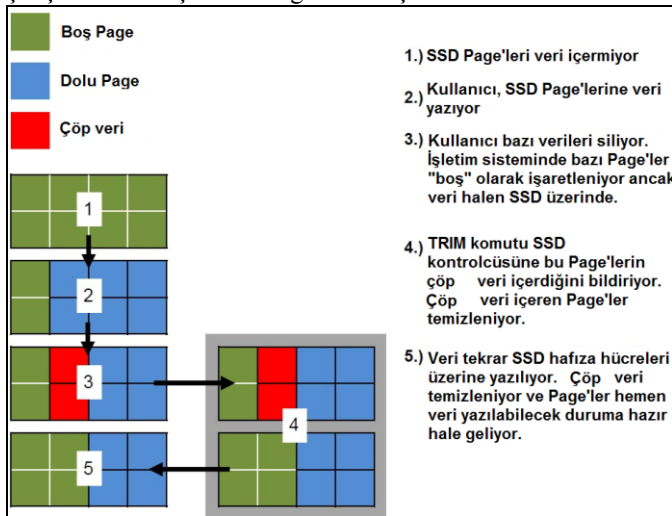
SSD diskler üzerinde veri depolama birimi olarak bulunan flash yongalar üzerine verinin nasıl kaydedileceğini veya silineceğini SSD kontrolcüsü düzenler. SSD disk ömrünü uzatmak ve performansı daha üst seviyelere ulaştırmak için veri flash yongalar üzerine ham olarak sırasıyla kaydedilmemekte, veri değişik algoritmalar kullanılarak ve farklı yongalara dağıtılarak kaydedilmektedir. Bu algoritmik ve dağınık kayıt biçimi diskten diske ve hatta modelden modele değişebilmektedir. SSD üreticileri performansı ve SSD disk ömrünü arttırmak için kullandıkları bu algoritmaları ticari sır niteliğinde olduğu için paylaşmamakta, dolayısıyla SSD disk teknolojisinde veri depolama şekillerinde standartlaşma olmamaktadır.

SSD disk üzerindeki flash yongalara okuma/yazma erişimlerinin tamamı SSD kontrolcüsü üzerinden gerçekleşmektedir. Sabit disklerde yazılabilir, okunabilir ve silinebilir en küçük birim 512byte iken SSD disklerde yazılabilir ve okunabilir en küçük birim 4KB büyüklüğündeki Page'lerden oluşurken; silinebilir en küçük birim ise 512KB büyüklüğündeki Blok'lardır. Page'ler Block'ların içerisinde yer alır. SSD diskler üzerinde veri sadece boş alanlara kaydedilmektedir. Daha önce veri kaydedilmiş ve silinmiş de olsa bir veri daha kaydedileceğinde, silindiği için boşalmış olan alana değil daha önce kullanılmamış olan veya daha az kullanılmış olan bir alana kaydedilir. Bunun sebebi ise SSD disklerdeki flash yongalarına maksimum veri yazma/okuma sayısının sabit disklerle göre oldukça düşük olması ve dolayısıyla kullanım ömürlerinin sabit disklerle göre kısa olmasıdır. SSD diskler kullanım ömrünü arttırmak için flash yongalar üzerinde mantıksal bir adresleme kullanırlar. Kullanılan bu adresleme sisteminde mantıksal olarak tutulan adresler sürekli değişmektedir ancak bu değişimler kullanıcı ve işletim sistemi tarafından fark edilmemekte, bu işlem SSD kontrolcüsü tarafından yapılmaktadır. Mekanik yapıya sahip sabit disklerde bozulan sektör yerine kullanıma açılmak üzere ayrılmış sektörler mevcut iken SSD disklerde ise disk üzerinde yazılı veri depolama kapasitelerinin %25'ine kadar fazla veri depolanabilecek flash yongalara sahip olarak üretildikleri görülebilmektedir[27]. Mekanik yapıya sahip disklerde bulunan yedek sektörler üzerine, bozulan bir sektör yerine kullanıma açılmadıkça, veri kaydedilememekte ve o sektörler erişilememektedir. SSD disklerde ise fazladan konulmuş flash yongalar mantıksal adreslemenin değişmesiyle sırası geldiğince kullanılmaktadır.

Bir yazma işlemi sırasında mantıksal adresleme içerisinde 100. Sırada olarak görülen bir sektör bir başka yazma işleminde 110. Sektör olarak adreslenebilmektedir.

Yeni nesil SSD disklerde TRIM desteği mevcuttur. "TRIM" bir SATA komutudur. TRIM komutunun kullanılabilmesi için hem işletim sisteminde hem de SSD diskte TRIM desteğinin bulunması gerekir. TRIM desteği olmaksızın bir silme işlemi yapıldığında işletim sistemi silinen dosyayı kendi haritasında silindi olarak işaretler ancak SSD diske ayrıca sil komutu göndermez. Sil komutu gönderilmediği için SSD üzerinde halen bulunan ancak gereksiz olan veri SSD disk üzerinde

çalışan Garbage Collection adı verilen yazılım tarafından bir süre sonra tespit edilerek silinirken aynı zamanda defragmentasyon işlemi de yapılarak SSD disk üzerindeki veri bloklarının daha verimli kullanılması sağlanır. Ancak Garbage Collection tarafından gereksiz ve kullanılmayan verinin tespiti ve defragmentasyona tabi tutulması zaman alabilmektedir. TRIM teknolojisi aktif olan bir sistemde ise: işletim sisteminde yapılan silme işlemiyle ilgili olarak silinmiş olarak görünen alanlar işletim sistemi tarafından SSD kontrolcüsüne bildirilir. SSD kontrolcüsü kendisine işletim sistemi tarafından silindiği bildirilen alanları çöp olarak işaretler. Daha sonra SSD diskin boşta olduğu zamanlarda çöp olarak işaretlenen alanlar Garbage Collection tarafından silinerek veri blokları düzenlenir. SSD kontrolcüsünü çöp olarak işaretlemesi ve Garbage Collection tarafından işaretlenen alanların silinmesi ve yeniden düzenlenerek bütün halinde Block'lara kaydedilmesi işlemlerinin tamamı işletim sistemi ve kullanıcı tarafından kontrol edilemeyecek bir yapı içerisinde gerçekleşmektedir. Yani eğer bir alan TRIM tarafından gönderilen komutla çöp olarak işaretlenmişse bu alan bir süre sonra geri getirilemeyecek şekilde silinecek ve ideal şekilde Block'lardaki veri düzenlenecektir. Bu işlemler yapılırken aynı zamanda mantıksal adreslemeler de değişebilmektedir. TRIM çalışma sistemi Şekil 9'da gösterilmiştir.



Şekil 9. TRIM çalışma sistemi[28]

Yazma korumalı olarak adli kopyası alınmak istenen bir SSD disk üzerinde daha önce çöp olarak işaretlenmiş ancak henüz silinmemiş veriler olabilmektedir. Garbage Collection programı da çalışmaya devam etmektedir. Yazma koruma sadece işletim sistemi veya kullanıcı gibi dışarıdan diske veri yazılmasını/silinmesini engellemektedir. TRIM ve Garbage Collection sistemleri ise SSD içerisinde çalışan sistemlerdir. Donanımsal yazma koruması veya yazılımsal yazma koruması bu sistemlerin çalışmasını engellememektedir. Adli kopya alınması esnasında bu sistemler çalışmaya devam edeceğinden SSD disk üzerindeki verilerde değişiklikler olmaya devam etmektedir. İlk adli kopya alma işleminde çöp olarak işaretlenen ancak henüz Garbage Collection tarafından silinmediği için sektör üzerinde okunmuş olan bir veri aynı SSD diskten ikinci defa alınacak olan adli kopya üzerinde bulunmayabilmektedir. İki adli kopya alma işlemi süresince

çalışmakta olan SSD disk üzerindeki sistemler önceden çöp olarak işaretlenmiş olan alanlarda değişiklikler yapmaya devam etmektedir. Dolayısıyla ilk adli kopya sonucu hesaplanan hash değeri ile ikinci adli kopya işlemi sonucu hesaplanan hash değeri farklı olacaktır.

III. SONUÇ VE ÖNERİLER

Adli bilişim alanında adli kopya ile ilgili uygulamalarda elektronik delillerin orijinali üzerinde tekrar adli kopya alma işlemleri yapılmakta ve sonucunda hesaplanan hash değeri ilk adli kopya alma işlemi hesaplanmış olan hash değeri ile karşılaştırılarak farklılık görüldüğünde elektronik aygıtın delil niteliği kalmadığı değerlendirilmektedir. Bunun yanında açık olan sistemlerden alınan adli kopyalarla ilgili olarak, RAM'lerden alınan adli kopyalarla ilgili olarak ve cep telefonlarından alınan adli kopyalarla ilgili olarak tekrar adli kopya alınması ve hash değerlerinin kıyaslanması gibi bir uygulama söz konusu değildir. Çünkü açık olan sistemler, RAM'ler ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alınırken sistem çalışmaya devam ettiği için, halen sistem tarafından zararsız ufak değişiklikler yapılmakta olduğu bilindiğinden; tekrar bir adli kopya alındığında aynı hash değeri elde edilemeyeceği bilindiğinden, böyle bir tehdit yoluna başvurulmamaktadır. Bu sistemlerden alınan ve elde olan ilk adli kopyalar üzerinden tüm inceleme ve değerlendirmeler yapılmakta, orijinal elektronik delil üzerinde tekrar hash hesaplatılması gibi bir işlem yapılmadan adli kopya delil olarak olayın aydınlatılmasında kullanılmaktadır.

CD-DVD gibi optik diskler, mekanik bir yapıya sahip olan sabit diskler ve katı hal diski olarak adlandırılan SSD disklerde de çeşitli sebeplerden dolayı hash problemleri yaşanabilmekte olduğu görülmektedir. Uygulamada, delil olabilecek elektronik aygıt üzerinden adli kopya alındığı sırada hesaplanan hash değeri ile, alınan adli kopyanın kaydedildiği veri depolama birimi üzerine tam ve doğru olarak kaydedildiğinin tespiti için hesaplanan hash değerleri birbiri ile aynı ise bu aşamadan sonra ilerleyen zamanda delil bütünlüğünün korunup korunmadığının kontrolü için elektronik delilin orijinali üzerinde tekrar adli kopya alma işlemi yapılması gerekmemekte, bu kontrolün eldeki adli kopya üzerinde hash hesaplatılarak yapılması gerekmektedir. Orijinal elektronik delil üzerinde meydana gelen bozulmalar ve değişimler hukuksal açıdan delil bütünlüğünün bozulduğuna anlamına gelmemelidir. Çalışan sistemlerden, RAM'lerden ve cep telefonlarından alınan adli kopyalarda olduğu gibi; diğer elektronik deliller de sadece adli kopyaları üzerinden değerlendirilmelidirler. Elektronik delil üzerinde herhangi bir veri değişikliği olup olmadığı ise orijinal delil üzerinden tekrar adli kopya alınarak ve orijinal delilin hash değeri hesaplatılarak değil, eldeki adli kopya üzerinde tekrar hash hesaplatılarak kontrol edilmelidir. Daha önceden orijinal delilden adli kopya alınırken hesaplanan hash değeri, adli kopya üzerinden tekrar hesaplatılan hash değeri ile birbirini tutuyor ise delil bütünlüğü korunuyor anlamına gelmektedir. Bu aşamada veri bütünlüğünün kontrolü için orijinal delil üzerinde tekrar hash hesaplatılması gibi bir yol izlenmemelidir.

KAYNAKLAR

- [1] BOREK, http://www.sans.org/reading_room/whitepapers/incident/computer-forensics-weve-incident-investigate_652.
- [2] Türk Dil Kurumu, Kriminal Terimleri Sözlüğü, <http://www.tdkterim.gov.tr/?kategori=terimarat2&s3oz5k0t=KRM&kelime=adli+bili%FEim>.
- [3] Keser Berber, Adli Bilişim, CMK md 134 ve Düşündürdükleri..., <http://www.leylakeker.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html>
- [4] Dr. Andy JONES, D. C. (2008). Potential Sources of Evidence. D. C. Dr. Andy JONES içinde, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility* (s. 10). Waltham(United States): Syngress.
- [5] Dr. Andy JONES, D. C. (2008). Potential Sources of Evidence. D. C. Dr. Andy JONES içinde, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility* (s. 10). Waltham(United States): Syngress.
- [6] HENKOĞLU, T. (Eylül 2011). Dijital Delilin Niteliği. T. HENKOĞLU içinde, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (s. 6-7). İSTANBUL: PUSULA.
- [7] Dr. Andy JONES, D. C. (2008). Potential Sources of Evidence. D. C. Dr. Andy JONES içinde, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility* (s. 10). Waltham(United States): Syngress.
- [8] KARAGÜLMEZ, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık.s. 290-291.
- [9] Dr. Andy JONES, D. C. (2008). Potential Sources of Evidence. D. C. Dr. Andy JONES içinde, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility* (s. 10). Waltham(United States): Syngress.
- [10] Dr. Andy JONES, D. C. (2008). Potential Sources of Evidence. D. C. Dr. Andy JONES içinde, *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility* (s. 10). Waltham(United States): Syngress.
- [11] KARAGÜLMEZ, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık.s. 291.
- [12] KARAGÜLMEZ, D. D. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık.s. 291.
- [13] HENKOĞLU, T. (Eylül 2011). Dijital Delilin Niteliği. T. HENKOĞLU içinde, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (s. 48). İSTANBUL: PUSULA.
- [14] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators*. Burlington, A.B.D: Syngress Publishing. s.10
- [15] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. United States of America: Syngress Publishing. s.379
- [16] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. United States of America: Syngress Publishing. s.380
- [17] Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. United States of America: Syngress Publishing. s.379
- [18] Cohen T., Cardwell K., Crowley P., Gregg M., O'Shea K., Ralph T., Schroder A., Steele J., Wright C., Alternate Data Storage Forensics, United States of America: Syngress Publishing. s.80
- [19] http://www.chip.com.tr/haber/optik-disklerin-omrunu-ne-belirliyor_34753.html
- [20] Philipp, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics Second Edition*. ABD: mhprofessional.
- [21] Philipp, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics Second Edition*. ABD: mhprofessional.
- [22] Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., & Wright, C. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators*. Burlington, A.B.D: Syngress Publishing. s.62
- [23] http://www.griffwason.com/images/GriffWason_WesternDigitalCaviar-ExplodedCutaway2.jpg
- [24] <http://www.emrahduman.av.tr/makale/solitstate.pdf>
- [25] http://4.bp.blogspot.com/-pG1GY9_mH68/UC6jY-HdALI/AAAAAAAAAMD4/jwiFKNxlExc/s400/vertex-3-pcb-top.jpg
- [26] http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf
- [27] http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf
- [28] <http://www.corsair.com/us/blog/how-to-check-that-trim-is-active/>