TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

VERİ KURTARMA AÇISINDAN AÇIK KAYNAK KODLU VE KAPALI KAYNAK KODLU YAZILIMLARIN KARŞILAŞTIRILMASI

Ahmet Serhat ŞİRİKÇİ

DİSİPLİNLER ARASI ADLİ BİLİMLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DANIŞMAN

Doç. Dr. Nergis CANTÜRK

2013 - ANKARA

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

VERİ KURTARMA AÇISINDAN AÇIK KAYNAK KODLU VE KAPALI KAYNAK KODLU YAZILIMLARIN KARŞILAŞTIRILMASI

Ahmet Serhat ŞİRİKÇİ

DİSİPLİNLER ARASI ADLİ BİLİMLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DANIŞMAN

Doç. Dr. Nergis CANTÜRK

2013 – ANKARA

İÇİNDEKİLER

ÖNSÖZ

Ülkemizde Adli Bilişim incelemeleri elektronik delillerin araştırılması ve analiz edilmesinde dünya çapında kullanılan ana yazılım ve donanım sistemlerinden yararlanılmaktadır. Resmi kurumlar tarafından sıklıkla kapalı kaynak kodlu yazılımlar tercih edilmekte ve çeşitli yazılım firmalarından yüksek bir maliyet karşılığında temin edilebilmektedir. Adli bilişim incelemelerinde önemli bir yere sahip veri kurtarma işlemlerinde de aynı durum geçerlidir. Bu tezde veri kurtarma amacıyla ücretsiz ve kullanıcı tarafından konfigüre edilebilen açık kaynak kodlu yazılımların da bu alanda etkin bir şekilde kullanılabilir olup olmadığının araştırılması ve kapalı kaynak kodlu yazılımlar ile karşılaştırılması amaçlanmıştır.

Adli Bilimler Enstitüsü Müdürü Prof. Dr. Hamit HANCI ile yüksek lisans eğitimine başvurmam konusunda beni cesaretlendiren ve gerekli çalışmalarda desteğini esirgemeyen kurum amirlerime, çalışmam boyunca yardım ve desteğini esirgemeyen tez danışmanım Doç. Dr. Nergis CANTÜRK'e teşekkür ederim.

Ayrıca tez çalışmalarım sırasında sabırla beni her konuda destekleyen, güvenlerini her zaman hissettiğim biricik eşim, kızım, anne, babam ve kardeşime en içten dileklerimle teşekkür ederim.

SİMGELER VE KISALTMALAR

CD	Yoğun Disk
DVD	Çok Amaçlı Sayısal Disk
FTK	Adli Amaçlı Yazılım Kiti
IDE	Bütünleşik Geliştirme Ortamı
MB	Mega Byte
MD5	Mesaj Özü
NTFS	Yeni Teknoloji Dosyalama Sistemi
SATA	Seri İleri Teknoloji Bağlantısı
USB	Evrensel Veri Seri yolu

ÇİZELGELER

1. GİRİŞ

Suç işleme içgüdüsü insanın doğasında vardır. Suçlular, tarih boyunca amaçlarına ulaşabilmek için yasal olmayan çeşitli yollara başvurmuşlardır. Locard prensibine göre; suç işlemek amacıyla kullanılan her türlü alet ve yöntemin mutlaka bir iz bıraktığı kabul edilmektedir. (Her temas iz bırakır.) Suçluların arkalarında bıraktıkları izleri araştırmak, Adli Bilimciler'in çalışma alanını oluşturmaktadır. Tarih boyunca suç işlemek amacıyla kullanılan alet ve yöntemler arttıkça, Adli Bilimler'in çalışma alanı da genişlemektedir (Hanci ve ark., 2002).

Son yıllarda klasik suçların bilgisayar ve bilişim sistemleri üzerinden işlenmesi oldukça yaygınlaşmıştır. Bunun nedeni bilişim sistemleri kullanılarak suç işlenmesinin daha kolay olması ve bilişim sistemlerinin daha fazla kitleye daha kısa zamanda ulaşım imkânı sağlamasıdır. Günümüzde bilişim sistemleri ile dünyanın en uzak noktalarına kolaylıkla ve hızlı bir şekilde ulaşılabilmesi, bilişim suçlarının geniş bir çerçevede ve uluslararası bir boyutta incelenmesini gerektirmektedir (Tuğ ve Cantürk, 2012).

Bilişim suçlarında fiziksel bir olay yeri incelemesine ek olarak sanal bir olay yeri incelemesi de yapılmalıdır. Adli bilişim incelemeleri çok boyutludur. Bilgisayarda kullanıcıların yapmış oldukları işlemlerin incelenmesi parmak izi incelemesine, bilgisayarda bulunan belgelerin incelemesi biyolojik ve kimyasal incelemeye, internette hangi sitelere girildiğinin araştırılması ayak izi incelemesine, kimlerle ne tür sohbetler yapıldığının değerlendirilmesi balistik incelemeye, üretilmiş sahte evrakların incelenmesi doküman incelemesine, yapılmış olan parasal işlemler mali incelemeye benzetilebilir.

İçinde bulunduğumuz çağa ismini veren bilişim teknolojileri hayatımıza her an biraz daha fazla nüfuz etmektedir. İnsan hayatını kolaylaştıran teknolojik gelişmeler,

suçluların suç işlemesini de kolaylaştırmaktadır. Bilişim teknolojileri kullanılarak işlenen suçların sayısının gün geçtikçe arttığı açıktır. Bu nedenle, bilişim suçlarının işlenmeden önce önlenmesi ve işlendikten sonra faillerinin tespit edilmesi çok önemlidir (Tuğ ve Cantürk, 2012).

Adli Bilişim bilim dalı, ülkemizde olduğu gibi dünya ülkelerinde de yeni bir bilim dalı olması sebebiyle, bu disiplini oluşturan kuram, yöntem ve standartların belirlenmesi gerekmektedir. Hiçbir sözlü kural yazılı kurallar kadar geçerli olamaz (Hancı ve ark., 2002).

1.1. Adli Bilişim Hakkında Genel Bilgiler

Adli bilişim, elektromanyetik ve elektrooptik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmalarının bütünüdür (http://tr.wikipedia.org/wiki/Adli_bili%C5%9Fim, Erişim Tarihi: 07.09.2013).

Adli Bilişim;

- ✓ Delil Toplama (Collection),
- ✓ Delillerin İncelenmesi (Examination),
- ✓ Sonuçların Değerlendirilmesi (Analysis),
- ✓ Raporlama ve Sonuç (Reporting) aşamalarından oluşan bir süreçtir (Partington, 2007).

Söz konusu aşamalar hukuki mevzuat açısından değerlendirilecek olursa, Ceza Muhakemesi Kanunu Madde 134 ile '*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*' işlemleri ile ilgili bazı düzenlemeler getirilmiştir. Adli ve Önleme Aramaları Yönetmeliği Madde 17 ile ise, '*el koyma işlemini bilgisayar ağları, uzaktaki bilgisayarlar ve çıkarılabilir donanımlar'* için de geçerli kılmaktadır (Ceylan ve Şirikçi, 2011). Ancak söz konusu mevzuat kapsamında bu maddelere ek olarak, adli bilişim incelemesi yapan teknik personel ya da bu personelin uygulayacağı bilimsel metotlar ile inceleme sonucu sunacağı rapor konusunda standartları belirleyen düzenlemelere ihtiyaç vardır (Çiçek, 2008).

Bir bilgisayarın veya diğer dijital medyaların yer aldığı bir olaya ilişkin olay yeri incelemesi, fiziksel bir olay yeri incelemesi ile çok büyük benzerlik göstermesine rağmen, delillerin doğasından ötürü adli incelemeler açısından farklılıklar göstermektedir. Fiziksel bir olay yeri incelemesi birçok delilin tanımlanmasını kapsamaktadır (Carrier ve Spafford, 2003). Dijital cihazların olay yeri incelemesi ile fiziksel olay yeri incelemesi arasındaki en büyük fark, bilişim cihazları için ikinci bir olay yeri incelemesi yapılması gerekmesidir. Bunlardan ilki olay yeri incelemesi esnasında yapılan fiziksel delillerin toplandığı "fiziksel olay yeri incelemesi", diğeri ise bilişim cihazları içerisinde yapılabilen "sanal olay yeri incelemesi"dir. Sanal olay yeri incelemesinde, bilişim sistemlerinin içerisinde bulunan veriler ve bu verilerin nasıl oluştuğu çok dikkatlice incelenmeli ve analiz edilmelidir (Hancı ve ark., 2002).

Elektronik deliller doğaları gereği çok hassastır. Bu tür deliller usulüne uygun olmayan şekilde yapılan incelemeler neticesinde değişebilir, zarar görebilir veya tamamen erişilemez hale gelebilir. Dolayısıyla bu delilleri toplama ve inceleme işlemleri esnasında özel bazı önlemler alınmalıdır. Yapılabilecek her türlü hata bu delillere zarar verebilir ve delillere ulaşılamamasına neden olabilir (Ashcroft, 2001). Sayısal delillere ilave olarak olay yerinde klasik suç delillerinin yer alması da mümkündür. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare (mouse) üzerinde bulunabilecek parmak izleri gibi deliller de uygun yöntemler kullanılarak

tespit edilmelidir. Fakat söz konusu delil toplama faaliyeti, hassasiyet gerektiren potansiyel sayısal delillere zarar vermeden yapılmalıdır. Örneğin bir yoğun disk (CD) üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar veya transfer bantlarının dikkatsiz kullanımı nedeniyle CD'nin içerisindeki bilgilerin kaybına neden olabilir. Bu sebeple olay yeri incelemesinde her olay kendi içerisinde değerlendirilerek diğer inceleme alanlarına ait delillerin toplanması ve adli bilişim delillerinin toplanması arasında makul bir denge kurulmalıdır (Ceylan ve Şirikçi, 2011). Adli bilişim alanında meydana gelen suçlarda olay yeri incelemesi yapacak araştırmacılar bu konuda uzman personel olmalıdır.

Olay yerinden usulüne uygun olarak elde edilen dijital deliller, teknik inceleme yapılması maksadıyla laboratuvara gönderilir. Laboratuvarda çalışan adli bilişim uzmanları, elektronik deliller üzerinde incelemelerini farklı yazılım ve donanımlar kullanmak suretiyle icra etmektedirler.

Yazılımlara örnek olarak;

- ✓ Encase Forensics,
- ✓ Forensic Tool Kit,
- ✓ ProDiscover,
- ✓ SMART,
- ✓ The Sleuth Kit/Autopsy verilebilir (Carrier, 2005).

Yazılımlar temel olarak açık kaynak kodlu ve kapalı kaynak kodlu yazılımlar şeklinde ikiye ayrılır. **Açık Kaynak Kodlu Yazılım** terimi ilk olarak 1998 yılında sonradan açık kaynak üreticileri ismini alan bir grup yazılımcı tarafından, ücretsiz terimine alternatif olarak geliştirildi. Açık kaynak üreticileri, sadece "ücretsiz yazılım" teriminin değil, "ücretsiz" sıfatının da anlayışta karışıklıklara neden olduğunu düşünerek, geliştirdikleri açık kaynak hareketinin bir pazarlama programına sahip olması gerektiğini, bu kapsamda yazılımları paylaşmanın sosyal

faydalarının ortaya konmasının önemli olduğunu savundular (Fogel, 2010). Daha kısa bir ifadeyle açık kaynak kodlu yazılımlar kaynak kodu kullanıcı tarafından değiştirilebilen ve kullanımı herkese açık olan yazılımlardır. Yazılımların kaynaklarının açık olması, araştırmacı ve üreticilere yazılımları kendi ihtiyaçlarına göre yeniden tasarlayabilme şansı tanımaktadır. Günümüz teknolojisi kullanıcılara, yazılımların fonksiyonlarını geliştirerek geliştirilen bu yeni yazılımların diğer kullanıcılar ile paylaşabilme olanağını sağlamaktadır (Delp ve ark., 2007).

Açık kaynak kodlu yazılımlar tüm dünyada kullanıcılar ve gönüllüler tarafından geliştirilen bir yazılım türüdür. Kullanıcılar hem kendi geliştirdikleri kodların kullanılması hem de kodlarında herhangi bir hata tespit edilmesi durumunda gerekli teknik desteği alabilmek maksadıyla geliştirdikleri kodu internet veya diğer paylaşım metotları ile yayınlamaktadırlar. Milyonlarca kullanıcı ve geliştiricisinin bulunmasından dolayı açık kaynak kodlu yazılımlar çok kısa sürede ücretli yazılımlar kadar yaygın kullanılır duruma gelmiştir. Bir yazılımın açık kaynak kodlu olup olmadığı "Açık Kaynak Tanımlaması" isimli bir takım kurallar ve gereklilikler ile tanımlanmaktadır. Bu tanımlamalar da "Debian Ücretsiz Yazılım Esasları"na göre yapılmaktadır (http://www.debian.org/social_contract#guidelines, Erişim Tarihi: 26.02.2011). Ayrıca Linux işletim sisteminde çalışmanın zor olması, açık kaynak kodlu yazılımların büyük çoğunluğunun da Linux işletim sistemi üzerinde çalışmasından dolayı, adli bilişim uzmanları incelemelerinde nispeten Windows işletim sisteminde çalışabilen kapalı kaynak kodlu yazılımları tercih etmektedirler.

Avrupa ve Amerika başta olmak üzere tüm dünyada bulunan laboratuvarlarda adli bilişim alanında yapılan incelemelerde ağırlıklı olarak kapalı kaynak kodlu yazılımlar kullanılmaktadır. Bunlara örnek olarak Encase Forensics, X-Ways, Forensic Tool Kit verilebilir. Bunun nedeni ise işletim sistemi olarak Microsoft işletim sistemlerinin yaygın bir şekilde tercih edilmesidir (Windows Xp, Windows 7 gibi).

Kapalı kaynak kodlu yazılımlar, genel anlamda geliştirilmesi profesyonel yazılımcılar tarafından yapılan, her yeni sürümünde yeni özellikler eklenen ve kendilerinden maddi anlamda bir kazanç elde edilebilen, kaynağı kullanıcılara katılmış yani üzerinde herhangi bir değişiklik yapılmasına imkan sağlamayan yazılımlardır (Raghunathan ve ark., 2005).

Donanımlara örnek olarak ise;

- ✓ Tableau yazma-koruma cihazları,
- ✓ Voom Technology cihazları,
- ✓ Solo-III kopyalama cihazları verilebilir (Botchek, 2008).

Bir adli bilişim uzmanı farklı işletim sistemi mimarilerinden ve bileşenlerinden haberdar olmak zorundadır. Bu kapsamda; adli bilişim uzmanının farklı durumlarda inceleme yapabilmesi için, farklı yazılım ve donanımlar ile işletim sistemlerini kullanabiliyor olması gerekmektedir (Şirikçi ve Cantürk, 2012).

Adli bilişim incelemelerinde konfigürasyonları gereği farklı yazılımlarla farklı sonuçlara ulaşılabilir (Jones ve ark., 2006). Adli bilişim uzmanının hangi durumda hangi yazılımın kullanılması gerektiğini çok iyi bilmelidir. Dünyada ve ülkemizde adli bilişim incelemelerinde yaygın olarak kapalı kaynak kodlu yazılımlar kullanılmaktadır. Tez çalışmasının amacı, adli bilişim incelemelerinin, özellikle veri kurtarma işlemlerinin açık kaynak kodlu yazılımlar ile de yapılabilmesinin mümkün olup olmadığının araştırılmasıdır.

1.2. Adli Bilişim İncelemelerinde Kullanılan Yöntemler

İncelemeler sırasında delil bütünlüğü bozulmamalı, delil niteliğindeki diskin üzerinde herhangi bir değişiklik meydana gelmemelidir. **Yazma koruması** sabit disk veya diğer dijital medyalara veri yazılmasını önleyen cihaz ve metotlardır (Jansen ve Ayers, 2007). Yazma korumasının fonksiyonu, herhangi bir incelemede, bilinmeyen veya beklenmeyen, bir disk veya dosya yazımının engellenmesidir. Bu işlem; kopyası alınacak dosya veya diske, kopya işlemi tamamlanmadan önce herhangi bir yazma işlemini önlemektedir (Mohay ve ark., 2003).

Donanımsal yazma koruması; genel olarak yazılımsal yazma korumasından daha güvenilir bir yöntemdir. Yazılımsal yazma koruması, işletim sisteminin kesme çağrılarına (interrupt call) müdahale etmek suretiyle yazma koruması sağlamaktadır (Mohay ve ark., 2003). Donanımsal yazma korumasında; delil üzerindeki verilere erişebilmek maksadıyla delil ile inceleme yapılacak bilgisayar arasına donanımsal yazma koruma cihazları yerleştirilir. Bu cihazlar bilgisayardan delile doğru gönderilecek olan yazma işlemi olabilecek her türlü komutu tutar ve delile ulaşmasını engellerler. Başka bir ifade ile bu cihazların kendisine bağlantı kurulan delil niteliğindeki cihazlara yazma yetkileri yoktur. İnceleyici yanlışlıkla dahi yazma işlemi yaptırırsa bu cihazlar işlemin delile ulaşmasını engelleyerek delilde değişiklik meydana gelmesini önlemektedir. Bilgisayar ile delil arasında fazladan bir aracı birimin bulunması işlemlerin hızını azaltabilmektedir. Donanımsal yazma koruma cihazları hem Windows hem de Linux işletim sistemlerinde sorunsuzca kullanılabilmektedir (Şirikçi ve Cantürk, 2012).

Yazılımsal yazma koruması; bilgisayar ile delil arasına herhangi bir ara birim konulmadan sadece inceleme bilgisayarında yazılımsal olarak yapılan değişiklikler ile delilin yazma işlemlerinden korunmasıdır. İnceleme bilgisayarında Windows işletim sistemi kullanılıyorsa; USB ile çalışan cihazlarda, sistem kayıt defteri (registry) ayarlarından "*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control*" altına "*\StorageDevicePolicies\WriteProtect*" Dword değerinin 1 olarak

eklenmesi neticesinde yazılımsal yazma koruması sağlanmış olacaktır (Hurlbut, 2005). Yazılımsal yazma koruması kullanarak yapılan incelemelerde kullanılan bilgisayar sisteminin hata vermesi sonucu, delil içerisine yazma işlemi yapabilmektedir (Menz ve Bress, 2004).

Windows işletim sisteminde SATA ve IDE bağlantı birimlerine sahip delillere yazma koruması sağlayabilecek lisanslı yazılımlar bulunmaktadır. Eğer inceleme bilgisayarında Linux işletim sistemi kullanılıyorsa; öncelikle “"*automount*” yani “*otomatik yükleme*” özelliği kapalı olmalı ve incelenecek medya bilgisayara bağlandıktan sonra “*sudo mount -t type -o ro device dir*” komutu ile sadece okuma yetkisi ile bilgisayara tanımlanmalıdır. Bu komutta *“-o ro*” read-only anlamına gelmektedir. (http://www.manpagez.com/man/8/mount/, Erişim Tarihi: 26 Şubat2012) USB, IDE ve SATA bağlantı birimlerine sahip tüm delillere tek bir yöntemle yazma korumalı olarak erişebilmek mümkündür. Çünkü “otomatik yükleme” özelliğinin kapalı olması ile bilgisayara hangi bağlantı ara birimi bağlanırsa bağlansın; medya, işletim sistemi tarafından mount edilmeyecek ve mount işleminin kullanıcı tarafından elle yapılması beklenecektir (http://linux.die.net/man/8/mount, Erişim Tarihi: 26.02.2012).

Bir adli bilişim incelemesindeki ilk adım, orijinal verilerin inceleme sırasında değişmesini önlemektir. Bu işlem orijinal diskin, başka bir diske, bit bazında **Birebir Kopyalanması** (İmaj almak) ile sağlanabilir. Birebir kopyanın alınması işleminde kullanılan yazma-koruma donanımları delilin türüne göre değişen bağlantı arabirimi ve kablolarını içerir. Bağlantı kabloları, incelemesi yapılacak olan delilin birebir kopyasının alınacağı bilgisayara veya bir depolama birimine yerleştirilir. Bu donanımlar, birebir kopya alınırken delile erişildiği esnada delilin üzerine herhangi bir verinin yazılmasını engeller (Ceylan ve Şirikçi, 2011). Bu kapsamda orijinal diske ait bitleri doğrudan diske yazmak yerine, disk üzerinde oluşturulacak olan imaj dosyasına yazmak daha sağlıklı bir yöntem olarak kabul edilmektedir (Partington, 2007). Kopyanın doğrudan bit seviyesinde başka bir diske kopyalanması, incelemelerde imaj dosyası üzerinden işlem yapmak yerine, incelenecek medyanın

adli bilişim yazılımlarına mantıksal veya fiziksel donanım olarak tanıtılmasına neden olacaktır. Ayrıca alınan kopya boyutları itibariyle, CD veya DVD gibi optik medyalara yazdırılamayacak ve kopyanın farklı bir inceleyici tarafından incelenmesi gerektiğinde medyanın yalnız bir adet olmasından dolayı aynı anda inceleme yapma imkânı ortadan kalkacaktır. Doğru bir birebir kopya, inceleme esnasında kaynak medyanın birebir aynısının elde edilmesi ile mümkündür. Burada "birebir aynısı" terimi, orijinal medyanın her byte'ının kopyalanması anlamında gelmektedir. Orijinal medyada bulunmayan en ufak bir bilgi bile oluşturulan kopyada olmamalıdır. Ayrıca ideal bir kopyalama işlemi orijinal medya üzerinde herhangi bir değişiklik meydana getirmemelidir (Altheide ve ark., 2011).

Adli bilişim alanında yapılan incelemelerde yapılacak tüm inceleme ve analiz faaliyetleri olaya ait delillerin birebir kopyaları üzerinde yapılmalıdır. Delilde herhangi bir değişiklik meydana gelmemesi için mutlaka uygulanması gereken bu aşamada özel yazılım ve donanımlara ihtiyaç duyulmaktadır. Birebir kopya sayısal delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelmektedir. Alınan birebir kopya;

- Mevcut verileri,
- Silinmiş verileri,
- Gizli bellek bölümlerini,
- Veri depolama biriminde bulunan diğer verileri kapsar (Ceylan ve Şirikçi, 2011).

Birebir kopyalama çeşitli yazılım veya donanımların kullanılması sureti ile yapılabilmektedir. Bu işlem için yaygın olarak kullanılan yazılımlar, genellikle Windows işletim sistemi üzerinde çalışabilen ve kapalı kaynak kodlu olan Encase Forensics yazılımı ile FTK Imager yazılımlarıdır. Linux işletim sistemi üzerinde çalışabilen ve açık kaynak kodlu olan kopyalama yazılımlarına örnek olarak ise dd,

dcfldd, guymager gibi yazılımlar verilebilir. Açık kaynak kodlu yazılımların bazıları Windows işletim sisteminde de çalışabilmektedir (Şirikçi ve Cantürk, 2012).

Elektronik deliller üzerinde, yapıları itibariyle çok çabuk ve kolay bir şekilde değişiklik yapmak mümkündür. Bir sabit disk veya USB belleğin bir bilgisayara bağlanması bile hem bilgisayar üzerinde hem de disk veya USB bellek üzerinde değişiklik meydana gelmesini sağlamaktadır. Bilgisayar üzerinde; bağlantı kurulan USB belleğin ya da sabit diskin ID numarası, ne zaman, hangi medyanın bağlandığı ve bağlantı kurulan medyanın markası modeli gibi birçok veri kaydolacaktır. Bağlanan USB bellek veya sabit diskte de dosyaların son erişim tarihlerinin güncellenmesi gibi veri değişiklikleri meydana gelebilmektedir. Elektronik delillerin hassas olmaları dolayısıyla inceleme sırasında da çok dikkatli olunmalıdır. Yazma koruması kullanılarak yapılan incelemelerde dahi delilin donanımsal parçalarından kaynaklanabilecek veri değişimleri olması mümkündür. Bu nedenle, inceleme sırasında delil ile mümkün olan en az seviyede bağlantı kurulmalıdır. Bu durum incelemelerin kopyalar üzerinde yapılmasını zorunlu kılmaktadır. Birebir kopya, bilinen anlamda kopyadan çok farklı bir kopyalama metodudur. Diğer bir deyişle silinmiş görünen (unallocated clusters) ve analiz edilmesi için gerekli diğer tüm alanların da kopyasının alınması demektir.

Birebir Kopyalama; **Birebir Kopyalama Cihazları Kullanılarak** ya da yazılımlar kullanılarak gerçekleştirilebilir. Adli bilişim uzmanları hem olay yerinde hem de laboratuvar ortamında çok çeşitli kopyalama donanımları kullanabilmektedir. Bu donanımlardan bazıları doğrudan kopyalama cihazına bağlanabilmekte bazıları ise Firewire veya USB kapıları aracılığı ile işlem görmektedirler (Garza ve ark., 2010). Bu yöntemde söz konusu kopyalama cihazının bir tarafına yazma korumalı olarak delil, diğer tarafında da yazma koruması kullanılmadan kopyanın alınacağı veri depolama birimi yerleştirilir ve ekran veya tuşlar yardımıyla kopyalama işlemi gerçekleştirilir.

Yazılımlar Kullanılarak Kopya Alma işlemlerinde Encase, FTK gibi kapalı kaynak kodlu yazılımlar yanı sıra açık kaynak kodlu olan AIR (Automated Image & Restore), dd ve Guymager gibi yazılımlar da kullanılabilir. Bu yazılımlar birebir kopyalama işleminin yanı sıra algoritma imzası almak ve bu algoritmayı doğrulamak işlemleri için de kullanılabilirler (Yang ve Yen, 2010). Yazılımsal olarak kopya alınmasında, adli amaçlı olarak kullanılan yazılımlar, işletim sistemini kullanmadan doğrudan medya ile bağlantı kurmakta ve medyaya istenen işlemleri yaptırmak suretiyle kopyalarının alınmasını sağlamaktadır. Oluşturulan birebir kopya, E01, aff gibi uzantılarına sahip sıkıştırma biçimlerinde sıkıştırılabilmektedir. Bu kapsamda birden çok kopya üzerinde çalışılması gerekiyorsa sıkıştırma işleminin yapılarak inceleyicilerin bilgisayarındaki sabit disk kapasitesinden kazanmak önemlidir. Ancak dd komutu ile sıkıştırma yapmadan delilin boyutu kadar büyüklükte kopyalama yapabilmektedir.

1.3. Birebir Kopya Alınması Amacıyla Kullanılan Çeşitli Yazılımlar

dd Imager Yazılımı (Komutu); dd Imager, UNIX/LINUX tabanlı bir yazılım olup açık kaynak koduna sahiptir. Windows işletim sisteminde de gerekli konfigürasyonların yapılması ile kullanılabilmektedir. Günümüzde birçok sabit disk kopyalama yazılımının kaynağı olarak kullanılmaktadır (Bukhari ve ark., 2004). dd Imager, dd komutunun arayüzü olup kopyalama işlemi için sadece dd komutu da kullanılabilir. dd, bilgisayarda en alt seviyede kopyalama yapılmasına imkân sağlayan bir komuttur. Başka bir ifade ile medyaların sektörel kopyalarının alınması için yazılmıştır (Bassi, 2008).

Guymager Yazılımı; Guymager, adli bilişim uzmanlarının, medyaların ham veya EWF (Expert Witness Format) biçimlerinde kopyalarını alınmasına imkân sağlamaktadır (Bassi, 2008). Daha ayrıntılı olarak, dd üzerine geliştirilmiş bir grafik arayüze sahip, dijital delil birebir kopyalama yazılımıdır. Daha çok Debian ve Ubuntu türü sistemlerde kullanılmak üzere geliştirilmiştir. Bilgisayara sonradan

bağlanan medyalar üst bölümde sıralanır ve bu diskler üzerinde işlem yapılamaz. Böylece yanlış diskin kopyasının alınması önlenir.

Diğer özellikleri;

- ✓ Farklı dil desteği ve kolay kullanım arayüzüne sahip olması,
- ✓ Sadece belirli Linux platformlarında çalışabilmesi.
- ✓ Hızlı ve aynı anda birden çok imaj alabilme özelliğine sahip olması,
- ✓ Çok işlemcili makinelerde bütün işlemcileri kullanabilme özelliğine sahip olması,
- ✓ Raw (dd), EWF (E01) ve AFF formatlarında imaj alabilme özelliğine sahip olması,
- ✓ Disk klonlama özelliğinin bulunması,
- ✓ Ücretsiz olması,
- ✓ MD5 ve SHA-256 algoritmalarını kullanarak hash değeri üretebilmesi,
- ✓ Alınan birebir kopyanın doğru olarak alınıp alınmadığının doğrulamasının yapılabilmesi,
- ✓ Alınan kopyayı istenilen boyutlarda parçalara bölebilmesi,
- ✓ Qt arayüzünü kullanmasıdır (http://guymager.sourceforge.net/, Erişim Tarihi: 26.02.2012).

dcfldd Komutu; dcfldd, dd komutunun geliştirilmesi neticesinde adli bilişim uzmanları tarafından kullanılması maksadıyla 2002 yılında yazılmıştır. dd'nin özelliklerine ek olarak algoritma imzası hesaplama ve kopyalama işleminin doğrulanması gibi işlemlerin yapılmasına da imkân sağlar (Bassi, 2008). Bu yazılımın dezavantajı ise sadece ham (raw) biçimde kopyalama yapılmasına imkân sağlamasıdır. Yani kopya dosyasına, yapılan işlemler ile ilgili üst veri (metadata) bilgisi yazılamamaktadır (Bukhari ve ark., 2004).

Dcfldd' nin dd ye ek olarak geliştirilmiş özellikleri şunlardır:

- ✓ **İşlem sırasında hash değeri hesaplama** - dcfldd veri transferi esnasında veri bütünlüğünü sağlamak için hash hesaplama işlemi yapabilmektedir.
- ✓ **İşlem sonuç çıktısı** - dcfldd işlem esnasında ne kadar veri transferi yapıldığını ve geride transfer edilecek ne kadar verinin kaldığını gösterir.
- ✓ **Esnek disk temizleme** - dcfldd disk temizleme işlemi yapabilmektedir.
- ✓ **İmaj/wipe doğrulama** - dcfldd imaj alma ve wipe işlemlerinin sonuçlarını doğrulayabilmektedir.
- ✓ **Çoklu çıktılama** - dcfldd aynı anda farklı dosya veya disklere veri aktarımı yapabilmektedir.
- ✓ **Çıktı dosyasının bölünmesi** – dcfldd, dd'nin split parametresine göre dışa aktarılan verilerin daha güvenilir dosyalara bölünebilmesi imkânı vermektedir.
- ✓ **Çıktı üzerinden işlem ve loglama** – dcfldd, log dosyaları ile dışa aktarılan verileri farklı lokasyonlara aktarılmasını sağlayabilmektedir (http://dcfldd.sourceforge.net/, Erişim Tarihi: 26.02.2012).

sdd Komutu; dd'nin genelde debian sistemlerde kullanılan gelişmiş bir türevi olup dd'ye ek olarak;

- ✓ Daha iyi istatistik tutma ve zaman yönetimi,
- ✓ Girdi ve çıktı arasında arama yapabilme özelliği,
- ✓ Boş girdi ve çıktıları daha hızlı işleme,
- ✓ Daha iyi veri bütünlüğü sağlama,
- ✓ Tekrar eden veri transferlerini önleme özelliklerine sahiptir (http://www2.opensourceforensics.org/tools/unix, Erişim Tarihi: 26.02.2012).

dd_rescue Komutu; dd'nin komut satırından çalışan geliştirilmiş bir versiyonudur. dd'ye göre hatalı girdi ve çıktıları daha az göz önünde bulundurarak, bozuk ve hasarlı medyalardan veri kurtarma işlemlerinde kullanılmaktadır. Kopyalama

sırasında hatalı bir alana rastlaması durumunda okuma alanını daha küçük parçalara bölerek veriyi okumaya çalışır (Bukhari ve ark., 2004).

Komut parametreleri dd den farklıdır;

Örnek: *dd_rescue /dev/hda birebirkopya.img*

Örnek: *ddrescue --no-split /dev/hda1 imagefile logfile*

dc3dd Komutu; dd yazılımının adli bilişim için geliştirilmiş (patch) bir versiyonudur. ABD Savunma Bakanlığı Siber Suçlar Merkezi tarafından geliştirilmiştir (http://dc3dd.sourceforge.net/, Erişim Tarihi: 26.02.2011). dc3dd, dcfldd yazılımının sahip olduğu tüm özelliklere sahip olmakla beraber, dcfldd'de olmayan dd yazılımının sahip olduğu bazı önemli özellikleri de bünyesinde barındırmaktadır. dcfldd yazılımında kullanılan komut satırı argümanlarının aynısı dc3dd yazılımında da kullanılabilmektedir (Altheide ve ark., 2011).

dc3dd yazılımının, dd yazılımına ek özellikleri;

- ✓ dc3dd disk wipe etme işleminde belli bir hexadecimal veya string değer kullanabilmektedir.
- ✓ MD5, SHA-1, SHA-256, ve SHA-512 hash algoritmalarını desteklemektedir.
- ✓ Girdi/çıktı verisine göre süreç cetveli bulunmaktadır.
- ✓ Hata ve hash loglarını birlikte gösterebilmektedir.
- ✓ Ciddi ardışık hatalarda ayrı bir log dosyası üretmektedir.
- ✓ Girdi ve çıktı verisi arasında doğrulama özelliğine sahiptir.
- ✓ Dışa aktarılan dosyalarda numerik veya alfabetik uzantılarla kaydetmektedir (http://dc3dd.sourceforge.net/, Erişim Tarihi: 26.02.2011).

AIR - Automated Image and Restore; AIR (Automated Image and Restore) dd ve dc3dd yazılımları ile adli bilişim amaçlı imaj alınabilmesi için hazırlanmış grafik arayüze sahip bir programdır.

Yazılımın özellikleri;

- ✓ IDE, SCSI, CD-ROM ve tape yedekleme ünitelerini otomatik görüntüleme,
- ✓ dd veya dc3dd yazılımlarını ayrı ayrı kullanım seçeneği,
- ✓ MD5 veya SHA1/256/384/512 algoritmaları kullanarak kaynak ve kopya arasında imaj doğrulama özelliği,
- ✓ gzip/bzip2 formatında imaj sıkıştırma ve açma özelliği,
- ✓ TCP/IP protokolü üzerinden netcat/cryptcat ile ağ üzerinden imaj alma özelliği,
- ✓ SCSI tape sürücü desteği,
- ✓ Disk veya bölüm wipe edebilme özelliği,
- ✓ İmaj dosyasını daha küçük dosyalara bölebilme,
- ✓ Tarih/saat ve kullanılan komutları gösteren detaylı log kayıtları tutabilme özellikleridir (http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page, Erişim Tarihi: 26.02.2011).

AIR yazılımının en önemli özelliği, otomatik olarak medyaları tanımlayarak üzerinde işlem yapılmasına imkân sağlamasıdır. Yazılım çalıştırıldığında, medyaların tanımlı olarak bulunduğu işletim sistemi dosyalarına inceleyerek, bilgisayara bağlanmış durumda olan tüm medyaların bir listesini çıkartır (Bassi, 2008).

Advanced Forensic Format Library (afflib); Advanced Forensic Format Library (afflib) adli bilişim amaçlı geliştirilmiş bir tür dosya formatı ve bu formatı kullanan

programlar bütünüdür. AFF (Advanced Forensic Format) biçimi kopyaların yukarıda bahsedilen diğer kopyalama türlerine nazaran temel iki üstünlüğü vardır. Bunlar;

- ✓ İmaj dosyalarına üst veri (metadata) bilgileri gibi dosya bilgileri de eklenebilmesi,
- ✓ Sıkıştırma teknolojisi sayesinde imaj dosyalarının daha az yer kaplamasıdır (http://www.afflib.org/, Erişim Tarihi: 26.02.2011).

AFF yazılımı, kullanıcıları veri segmentlerini, sıkıştırmasını veya diğer teknik verileri anlamaya zorlamak yerine, *af_open(), af_read()* and *af_seek()* gibi komutlar aracılığıyla AFF türü kopya dosyaları birer veritabanı gibi kullanılabilmekte ve sorgulanabilmektedir (Garfinkel, 2006).

1.4. Hash Değeri Hesaplamak

Birebir kopya alma işleminin amacı, kopyası alınacak olan medyanın birebir aynı (orijinal halini) kopyalamaktır. Bir birebir kopyanın doğru alındığı, alınan kopya ile orijinal delilin hash değerlerinin aynı olması ile kesinleşir. Hash fonksiyonları ile elde edilen hash değerleri, cheksum veya dijital delilin parmak izi olarak da adlandırılmaktadır. Elde edilen hash değeri, inceleyici tarafından kaydedilmelidir çünkü yapılan incelemeden sonra, aynı delil başka bir uzman tarafından incelendiğinde aynı hash değerinin elde edildiği ortaya konabilmelidir (Vacca, 2005). Message Digest 5 ve Secure Hash Algorithm isimli algoritmalar adli bilişim incelemelerinde en çok tercih edilen hash algoritmalarıdır (Arthur ve Venter, 2012).

Windows işletim sisteminde kullanılabilen ve çok sayıda algoritma imzası hesaplamaya yarayan yazılım mevcuttur. Ancak bu değerin yine uluslararası kabul görmüş yazılımlar ile hesaplanması tercih edilmektedir. Bu yazılımlara örnek olarak

Encase, FTK Imager verilebilir. Bu yazılımlar MD5 ve SHA-256 algoritmalarını kullanarak algoritma imzası hesaplayabilmektedir. Linux işletim sisteminde ise; bu işlem yine komutlar vasıtasıyla kolaylıkla yapılabilmektedir. Örnek olarak "*md5sum filename*" komutu ile istenilen dosyanın MD5 değeri hesaplanabilmektedir (http://manpages.ubuntu.com/ manpages/natty/en/man1/md5sum.1.html, Erişim Tarihi: 26.02.2011).

md5sum /dev/hda1

IDE bağlantılı sabit diskler için,

md5sum /dev/sda

SATA veya SCSI bağlantılı sabit diskler için kullanılan komutlardır (Kornblum, 2004) .

Başka bir komut olarak da "*hashdeep filename*" komutu kullanılabilir. Bu komut ile yapılandırma dosyasının da kullanılması sonucu istenilen algoritma ile hash değeri hesaplanabilmektedir. Bu komut MD5, SHA-1, SHA-256 algoritmalarını kullanarak hash değeri hesaplayabilmektedir.

*hashdeep -m -k known-hashes.txt **

Bu komutla *known-hashes.txt* isimli dosya içerisinde kayıtlı bulunan hash veri tabanı ile inceleme konusu tüm dosyalar hash değerleri bakımından karşılaştırılarak aynı hash değerine sahip dosyalar tespit edilmektedir. Bu işleme de hash set taraması ya da mukayesesi denmektedir. Bu komutun çıktısı olarak;

/Users/jessek/tmp/bar
/Users/jessek/tmp/foo

komutları kullanılarak alınmıştır. Bunun anlamı, bar ve foo isimli dosyalar veritabanımızda bulunan bir dosya ile aynı hash değerine sahiptir. Bu da bu dosyalar üzerine yoğunlaşılarak sonuca ulaşılmasına yardımcı olmaktadır (http://md5deep.sourceforge.net/, erişim 20 Şubat 2011).

1.5. Elektronik Medyalar İçerisindeki Mevcut Verilerin İncelenmesi

Adli bilişim alanında mevcut verilerin incelemelerinde kullanılabilen açık kaynak kodlu yazılımların genel özellikleri aşağıda anlatılmıştır. Anlatılan her bir yazılım farklı özelliklere sahip olup veri analiz kabiliyetleri kaynak kodunda yapılabilecek değişikler ile geliştirilebilmektedir.

Sleuth Kit (TSK) ve Autopsy; dosya sistemleri üzerinde farklı analizler yapabilen bir grup Linux işletim sistemi yazılımları topluluğudur. Autopsy adli yazılım ise Sleuth Kit'e ait yazılımlardan oluşan ve kullanıcıya kolay kullanım sağlayan grafiksel bir arayüzdür (Dowling, 2006).

Sleuth Kit ve Autopsy ile iki türlü analiz yapılabilmektedir;

- ✓ Sleuth Kit kurulu bir Linux işletim sistemi yüklü olan bilgisayar ile bir disk imajı üzerinde çalışılabilir (Dead Analysis),

- ✓ Sleuth Kit yazılımının çalıştırıldığı bir Live Linux CD ile aktif olarak kullanılmakta olan bir sisteme müdahale edilerek inceleme yapılabilir (Live Analysis).

Özellikleri:

- ✓ **Dosya Listeleme:** Disk içerisinde mevcut ve silinmiş olarak bulunan dosya ve klasörleri Unicode desteği ile gösterebilmektedir.
- ✓ **Dosya içeriği:** Disk içerisinde bulunan dosyaların içeriklerini ASCII, onaltılık tabanda veya ham olarak gösterebilmektedir. Ayrıca istenilen dosyayı dışarı çıkartabilmektedir.
- ✓ **Hash Veritabanı:** NIST hash set veritabanı ile kullanıcı tarafından yaratılan hash set veri tabanlarını kullanmak suretiyle şüpheli medya içerisindeki dosyaları eşleştirerek hızlı bir şekilde sonuç alınabilmektedir.
- ✓ **Dosya tasnifi:** Disk içerisinde bulunan dosyaları uzantı ve tiplerine göre sınıflandırabilmektedir. Örneğin; resim dosyaları (*.jpeg vb.)
- ✓ **Timeline Analizi:** Tüm dosyaları zaman sıralamasına koyarak adım adım bilgisayarda yapılan işlemleri analiz edebilmektedir.
- ✓ **Anahtar kelime araması:** Özellik arz eden anahtar kelimeler disk içerisinde silinmiş alanlar dâhil kolaylıkla aratılabilmektedir.
- ✓ **Üstveri Analizi:** Dosyaların üstverilerini (metadata) çıkartarak analiz edebilmektedir.
- ✓ **Kopya detayı:** Alınan kopyanın detaylarını verebilmektedir.
- ✓ **Loglama:** Çok gelişmiş bir log yani kayıt dosyası tutma özelliği bulunmaktadır.
- ✓ Perl yazılımı ile yazıldığından, perl dili kullanılarak istenilen yamalar (patch) üretilebilmektedir. Böylece yazılıma yeni özellikler eklenebilir.
- ✓ **NTFS**, **FAT**, **UFS 1**, **UFS 2**, **EXT2FS**, **EXT3FS**, ve **ISO 9660** dosya sistemlerini desteklemektedir.
- ✓ **Raw** (Örn: dd), **Expert Witness** (Örn: EnCase) ve **AFF** türü sabit disk imajlarını desteklemektedir. (Galvao, 2006)

Sleuth Kit içerisinde bulunan adli komutlar:

- ✓ **dcat:** Blok içeriğini görüntüler.
- ✓ **dls :** Adreslenmemiş blokları listeler. Adreslenmemiş bloklarda anahtar kelime arar ve listeler.
- ✓ **dcalc:** Adreslenmemiş bloğun diskteki yerini gösterir.
- ✓ **dstat :** Belli bir bloğun detaylı özelliklerini gösterir.
- ✓ **icat :** inode veya cluster numarası verilen bir dosyanın içeriğini görüntüler. Dizinleri listelemez sadece içeriği görüntüler.
- ✓ **İls :** Disk üzerinde dosyaların nerelerde yazıldığını gösterir.
- ✓ **istat:** Girilen bir inode numarası hakkında detaylı bilgileri verir (http://www.sleuthkit.org/autopsy/, Erişim Tarihi: 02.02.2011).

PYFLAG Forensic And Log Analysis Gui; sabit disk, geçici bellek ve ağ incelemelerini tek bir platformda birleştiren açık kaynak kodlu bir yazılımdır. İlk başta sabit disk incelemeleri için yazılan PyFlag yazılımına, daha sonra ağ incelemeleri özelliği de eklenmiştir (Cohen, 2008).

PyFlag web tabanlı, veri tabanı teknolojisi kullanan bir adli bilişim analiz programı olup yüksek boyuttaki log dosyalarını ve disk imajlarını analiz edebilmektedir. Yazılımın genel özellikleri;

- ✓ **Ağ İncelemesi:** Pyflag, TCPDump formatında ağdan paket toplama özelliğine sahiptir. Birçok ağ protokolünü de desteklemektedir.
- ✓ **Log Analizi:** PyFlag gelişmiş bir log kayıt analiz etme özelliğine sahiptir. Birçok log kayıt formatını desteklemekte ve çok hızlı analiz yapabilmektedir.
- ✓ **Disk İncelemesi:** PyFlag disk imajlarını inceleyebilmektedir. Birçok imaj formatını desteklemektedir. Veri getirme (carving) özelliği de bulunmaktadır.

✓ **Bellek İncelemesi:** PyFlag sınırlı da olsa adli bellek inceleme (memory forensics) fonksiyonlarını da desteklemektedir (http://www.pyflag.net/cgi-bin/moin.cgi, Erişim Tarihi: 26.02.2011).

1.6. Silinmiş ve Gizli Verilerin Kurtarılması

Alınan birebir kopyalar içerisinde, işletim sisteminin kullanıcıya görme imkanı tanımadığı ve adreslenmemiş alanlarda silinmiş halde bulunan verilerin tespit edilerek analiz edilmesi gereklidir. Bu verilerin tespitinde kullanılan yazılımlara birkaç örnek aşağıda anlatılmıştır.

TestDisk Yazılımı; silinmiş veya kaybolmuş disk bölümleri ile verileri kurtararak tespit edebilen ücretsiz bir yazılımdır. Temel hedefi kaybolan bölüm bilgilerini geri getirmek ve yüklenebilme (bootable) özelliğini kaybeden disk ve bölümleri tekrar düzeltmektir. Yazılımlardan ya da virüslerden dolayı oluşan disk sorunlarını TestDisk ile düzeltmek oldukça basittir. Yazılımın genel özellikleri;

- ✓ Bölüm (partition) tablosunu düzeltir, silinmiş bölümleri (partition) geri getirebilir.
- ✓ FAT32 boot sektörü, yedeğinden geri getirebilir.
- ✓ FAT12/FAT16/FAT32 boot sektörleri yeniden oluşturabilir.
- ✓ FAT tablosunu düzeltebilir.
- ✓ NTFS boot sektörünü yeniden oluşturabilir.
- ✓ NTFS boot sektörünü yedeğinden geri getirebilir.
- ✓ MFT (Master File Table), MFT mirror kullanarak düzeltebilir.
- ✓ ext2/ext3 Backup SuperBlock'larını düzenler.
- ✓ FAT, NTFS ve ext2 dosya sistemlerinde veri kurtarma yapabilir.

- ✓ Silinmiş FAT, NTFS ve ext2/ext3 bölümlerindeki dosyaları başka bir yere kopyalayabilir. (Reyes, 2007)

Testdisk yazılımını çalıştırabilmek için Linux konsoluna;

sudo Testdisk

yazmak yeterlidir. Yazılım daha sonra yapılmak istenen işlemleri sırası ile kullanıcıya sorarak çalışmaktadır.

PhotoRec Yazılımı; sabit disklerden, CD-ROM'lardan, dijital kamera belleklerinden, video, doküman ve arşiv dosyaları gibi silinmiş ya da kaybolmuş verileri kurtaran bir programdır. PhotoRec dosya sistemini ve disk bölümlerini göz ardı ederek çalıştığı için oldukça başarılıdır (http://www.cgsecurity.org/wiki/PhotoRec, Erişim Tarihi: 20.02.2011).

PhotoRec, dosya yapısı veri kurtarma sistemi ile başlık-son bilgi, veri kurtarma sistemlerini birlikte kullanarak veri kurtarma işlemi yapabilmektedir (Kloet, 2007).

Photorec yazılımını çalıştırabilmek için Linux konsoluna;

sudo Photorec

yazmak yeterlidir. Yazılım daha sonra yapılmak istenen işlemleri sırası ile kullanıcıya sorarak çalışmaktadır.

Foremost Yazılımı; dosyaları başlık-son bilgi veri kurtarma sistemi ile veri yapılarına göre veri kurtarma yapabilen ve terminal arayüzünden çalışan bir yazılımdır (Kloet, 2007).

Örnek: *sudo foremost -t all –i image.img*

Foremost yazılımını kullanarak silinmiş alanlarda bulunan veriler kurtarılabilmektedir. Örnekteki komut satırında bulunan "*–t all*" ibaresi foremost yazılımının yapılandırma dosyasında bulunan, bilinen dosyaların hexadecimal başlık değerlerine göre kayıtlı tüm dosya tiplerinin kurtarılmasını işaret etmektedir (foremost.sourceforge.net/, Erişim Tarihi: 22.02.2011).

Söz konusu işlem doğrudan sabit disk üzerinde yapılabileceği gibi alınan birebir kopya üzerinde de yapılabilmektedir.

Scalpel Yazılımı; Foremost yazılımının geliştirilmiş bir versiyonudur. Foremost yazılımından daha hızlı olması ve sistem belleğini daha verimli kullanması en büyük özelliğidir (Garfinkel, 2007).

Örnek: *scalpel FILE -o Directory*

Desteklediği dosyalama sistemleri: FATx, NTFS, ext2/3 ve raw türü dosyalama sistemleridir.

Yapılandırma dosyası, ihtiyaca göre değiştirilerek geliştirilebilir ve güncellenebilir.

1.7. Sonuçların Değerlendirilmesi (Analysis)

Bu aşama incelemecinin elde ettiği verilerin, sonuca ne kadar ve nasıl etki ettiğini değerlendireceği aşamadır. Elde edilen verilerin doğru olarak elde edilmesinin yanı sıra doğru olarak değerlendirilmesi bilirkişiliğin altın kuralı olan tarafsızlığın korunması açısından çok önemlidir. Elde edilen verilerin anlamlı bir hale getirilerek sunulabilmesi için bir hazırlık aşaması olan bu süreçte, inceleme

sırasında dikkat çeken tüm veriler titizlikle değerlendirilmeli ve hiçbir husus atlanmamalıdır (Carrier ve Spafford, 2003).

1.8. Raporlama ve Sonuç

Adli incelemelerin genelde son aşaması olan raporlama ve sonuç aşamasında, incelemenin en başından itibaren yapılan işlemlerin ve elde edilen veriler ile sonuçların bir doküman haline getirilerek rapor oluşturulması gerekmektedir. Üretilen bu doküman mahkemeye sunulacak ve bilirkişi için adli zincirin son halkasını oluşturacaktır (Köhn ve ark., 2008).

Delillerin toplanması, elde edilmesi ve değerlendirilmesi aşamalarında yapılan her işlem ve elde edilen her veri, mahkemenin ve diğer adli makamların tam olarak anlayabileceği bir şekilde sunulmalı ve raporlanmalıdır. Bu kapsamda önceki tüm aşamalarda ayrıntılı ve doğru not alma işleminin yapılması çok önemlidir. Raporda değerli verilerin elde ediliş ve tespit zamanı ile bu verilere ait hash algoritma değerleri ayrıntılı bir şekilde belirtilmelidir (Sindhu ve Meshram, 2012).

Yen ve arkadaşlarına göre (2012) raporlama aşaması dört bölümden oluşmaktadır:

- ✓ **Rapor yazma ve sunma:** Hazırlanan rapor mahkemeye, savunma ve iddia makamlarına sunulmalıdır. Dolayısıyla rapor içeriği kolay okunabilir ve anlaşılabilir olmalıdır.
- ✓ **Adli sonuçların doğrulanması:** İnceleme sonucunda adli sonuçların doğru olarak elde edilebilmesi çok önemlidir. İncelemeci kullandığı yazılım ve donanımlar ile yöntemleri açık bir şekilde raporda belirmelidir. Böylece aynı dosyayı farklı bir incelemecinin incelemesi sonucunda aynı sonuçların elde edilip elde edilmeyeceği doğrulanabilinmektedir.

- ✓ **Mahkeme için hazırlık:** Hazırlanan rapor ile ilgili mahkeme huzurunda sorulabilecek tüm sorulara hazırlıklı olunmalıdır.

- ✓ **Bilirkişiliğin tamamlanması ve son değerlendirme:** Tüm bu aşamalardan sonra inceleme sırasında elde edilen yeni bilgi ve tecrübeler daha sonra yapılacak olan incelemelerde de kullanılabilmelidir (Yen ve ark., 2012).

2. GEREÇ VE YÖNTEM

Adli bilişim incelemelerinde veri kurtarma işlemlerinin açık kaynak kodlu yazılımlar ile yapılabilmesinin mümkün olup olmadığı ve veri kurtarma konusunda kapalı ve açık kaynak kodlu yazılımların karşılaştırılması amacıyla; 5 adet aynı marka ve model 128 Mega Byte kapasiteli USB flash bellek kullanılmıştır. Çalışmada objektif sonuçlar elde edilebilmesi amacıyla sabit bir bilgisayar sistemi kullanılmıştır. Aynı şartlar altındaki 5 farklı flash bellekte farklı durumlar yaratılarak kapalı kaynak kodlu RecoverMyFiles ve X-Ways Forensics yazılımları Windows 7 (32 bit) sistemi ile açık kaynak kodlu olan Photorec, Foremost ve Scalpel yazılımları ise Linux işletim sistemi (Ubuntu v10.10) içerisinde test edilmişlerdir.

Çalışmada kullanılan bilgisayar sisteminin özellikleri şunlardır:

- İşletim sistemi: Microsoft Windows 7 Ultimate, 32 bit,
- İşlemci: Intel Mobile Core 2 Duo T9300, 2.50GHz,
- Geçici bellek: 4 GB DDR2, 332 MHz,

Çalışmanın ilk basamağında flash belleklerin FTK Imager 3.0 yazılımı ile dd (raw) formatta birebir kopyaları alınmış ve testler bu birebir kopyalar üzerinde icra edilmiştir. Ayrıca yazılımların başlık-son kısım (header-footer) analizi yaparak dosya kurtarma işlemlerini yerine getirme özellikleri test edilmiştir. RecoverMyFiles yazılımının kullanımında, yazılıma testlere ait kopyalar tanıtılmış ve "*Recover Drive*" özelliği kullanılarak dosyalar kurtarılmaya çalışılmıştır. X-Ways yazılımının kullanımında, "*Tools/Disk Tools/File Recovery by Type*" özelliği kullanılmıştır. Photorec yazılımının kullanımında her flash bellek yazılıma tanıtılmış ve içerisinde veri kurtarma yapılması sağlanmıştır. Photorec, veri kurtarma maksatlı olarak kullanılabildiğinden herhangi farklı bir işlem yapılmasına ihtiyaç duyulmamıştır. X-Ways yazılımı ise adli inceleme maksadı ile kullanılabildiğinden farklı menülerden işlemlerin yapılması sağlanmalıdır.

Scalpel yazılımı için;

scalpel -b -c /etc/scalpel.conf -o scalpel-out/ -q 4096 sda1.dd örnek komutu,

Foremost için ise;

foremost -c /etc/foremost.conf -i sda1.dd -o foremost-out -q -b 4096 örnek komutu kullanılmıştır.

2.1. Test Senaryoları

Test senaryoları, son 3 yıl içerisinde adli bilişim alanında Jandarma Kriminal Laboratuvarlarına gönderilen inceleme talepleri değerlendirilerek oluşturulmuştur. Bu kapsamda adli makamlar tarafından, Çizelge 2.1'de gösterilen dosya türlerinin tespitine, diğer dosya türlerine oranla daha fazla ihtiyaç duyulduğu belirlenmiş olup tez kapsamında oluşturulan senaryolarda belirtilen dosya türleri kurtarılmaya çalışılmıştır.

Çizelge 2.1. *2011-2012-2013 Yıllarında Jandarma Kriminal Laboratuvarlarına Gönderilen Delillerden, En Fazla Tespiti Talep Edilen Dosya Türleri Oranları*

Gönderilen Delillerden Tespiti İstenen Dosya Türleri (adet)	2011 (%)	2012 (%)	2013 (%)
PDF	88	86	91
AVI	75	85	79
BMP	77	75	77
JPG	97	94	93
XLS	89	90	91
XLSX	87	88	90
DOC	87	92	94
DOCX	89	91	90
MPG	67	65	74
ZIP	78	79	82

Çalışmada kullanılan dosyaların isim ve boyutları aşağıdaki gibidir (kaydedilen ilk 50 dosya, Çizelge 2.2):

Çizelge 2.2. *Testler Kapsamında Flash Bellekler İçerisine Kaydedilen Dosya İsimleri ve Boyutları*

Dosya Adı	Boyut
1.pdf	14 KB
2.pdf	6 KB
3.pdf	34 KB
4.pdf	8 KB
5.pdf	15 KB
1.avi	575 KB
2.avi	36.020 KB
3.avi	18.260 KB

4.avi	7.634 KB
5.avi	1.563 KB
1.bmp	5.626 KB
2.bmp	3.841 KB
3.bmp	2.109 KB
4.bmp	2.069 KB
5.bmp	141 KB
1.JPG	1.140 KB
2.JPG	1.202 KB
3.JPG	1.306 KB
4.JPG	1.349 KB
5.JPG	1.433 KB
1.xls	130 KB
2.xls	45 KB
3.xls	10 KB
4.xls	61 KB
5.xls	66 KB
1.xlsx	11 KB
2.xlsx	11 KB
3.xlsx	12 KB
4.xlsx	12 KB
5.xlsx	13 KB
1.doc	798 KB
2.doc	696 KB
3.doc	674 KB
4.doc	680 KB
5.doc	687 KB
1.docx	10 KB
2.docx	11 KB
3.docx	12 KB
4.docx	12 KB

5.docx	12 KB
1.mpg	8.884 KB
2.mpg	713 KB
3.mpg	916 KB
4.mpg	1305 KB
5.mpg	1709 KB
1.zip	193 KB
2.zip	3.036 KB
3.zip	192 KB
4.zip	392 KB
5.zip	2.078 KB

Dosyaların toplam boyutu, 105 MB'dır.

Çalışma kapsamında 2nci testten itibaren kullanılan 3 adet dosyanın boyutları ise aşağıda olup (Çizelge 2.3):

Çizelge 2.3. *2nci Testten İtibaren Kullanılan 3 Adet Dosyanın İsimleri ve Boyutları*

Dosya Adı	Boyut
DSC_2805.JPG	5.33 MB
Origins of images.doc	0.97 MB
seiko11032011_HDTV.avi	55,4 MB

Toplam boyut 61,7 MB'dır.

Ayrıca Jandarma Kriminal Laboratuvarına gönderilen inceleme talepleri değerlendirildiğinde, inceleme konusu dosya türlerinin, dijital medyalar içerisinde bulunma durumları, Çizelge 2.4'de görülebilmektedir. Bu çalışmadaki test senaryoları, söz konusu durumlar örnek alınarak hazırlanmıştır.

Çizelge 2.4. *2011-2012-2013 Yıllarında Jandarma Kriminal Laboratuvarlarına Gönderilen Deliller kapsamında, Dosya Türlerinin Deliller İçerisinde Bulunma Durumları*

Dosya Türlerinin Bulunma Durumları	**2011 (%)**	**2012 (%)**	**2013 (%)**
"Delete" Tuşu yada Fare ile Silinmiş Olanlar	44	39	41
Çöp Kutusundan Silinmiş Olanlar	56	67	61
NTFS ile Biçimlendirilerek Silinmiş Olanlar	34	28	23
FAT ile Biçimlendirilerek Silinmiş Olanlar	5	12	8
Üzerine Başka Dosya Kaydedilerek Silinmiş Olanlar	17	21	28

Her flash bellek içerisinde, veri kurtarma işlemi kapsamında testler yapılabilmesi için farklı durumlar oluşturulmuş olup bu durumlar aşağıda sırasıyla açıklanmıştır;

1. İlk testte flash bellek (NTFS) içerisine her biri farklı 5'er adet aynı uzantıya sahip sağlam ve görüntülenebilen toplam 50 adet dosya (Çizelge 2.2, Toplam 105 MB) kaydedilerek, klavyenin "DELETE" tuşu ile silinmiştir.

2. İkinci testte flash belleğe (NTFS) önceden silinmiş olan 50 adet dosyanın üzerine yazması için 3 adet büyük boyutlu (Çizelge 2.3, Toplam 61,7 MB) dosya eklenmiştir**.**

3. Üçüncü testte, flash belleğe (NTFS) sonradan eklenen 3 adet dosya, klavyenin "DELETE" tuşu ile silinmiştir.

4. Dördüncü testte (NTFS) flash bellek, üçüncü testte olduğu haline ek olarak NTFS dosyalama sistemi ile biçimlendirilmiştir.

5. Beşinci testte (NTFS) flash bellek, üçüncü testte olduğu haline ek olarak FAT dosyalama sistemi ile biçimlendirilmiştir.

Yukarıda oluşturulan durumlar kapsamında her bir bellek için RecoverMyFiles v.4.6.8, X-Ways Forensics v16.7, Photorec v6.11, Foremost v1.5 ve Scalpel v1.6 yazılımları ile veri kurtarma işlemleri yapılmıştır. Söz konusu yazılımların versiyonları, test anındaki (2012) yayınlamış son versiyonlarıdır.

Yapılan testlerden elde edilen verilerin istatistiksel değerlendirilmesi SPSS 15.0 paket programı ile yapılmıştır. Çalışmada anlamlılık katsayısı (α) 0.05 olarak alınmıştır. İstatistiksel testler "H0: Değişkenin dağılımı normaldir" "H1:Değişkenin dağılımı normal değildir." hipotezlerini n birimlik örnek veriler aracılığı ile test etmektedir. Test sonucunda değişkenin dağılımının Normal dağılıma uygun olduğu kabul edilir ise (H0 kabul) parametrik testler uygulanır. Normal dağılıma uygun olmadığı (H0 red) sonucuna varılır ise verilere parametrik testler uygulanmaz. Bu durumda veriler uygun parametrik olmayan alternatif bir test ile test edilir (Özdamar, 2002).

Kurtarma oranı değişkeni kaynak kodu faktörüne göre her iki grupta da normal dağılım göstermemektedir ($p<0.05$). Bu nedenle grupların, kurtarma oranı açısından karşılaştırmasında parametre dışı testlerden Mann-Whitney U Testi kullanılmasına karar verilmiştir. Kurtarma oranı değişkeninin dosya formatı faktörüne göre dağılımı MPG dosyası dışındaki tüm gruplarda normal dağılım göstermemektedir ($p<0.05$). Bu nedenle grupların, kurtarma oranı açısından karşılaştırılmasında parametre dışı testlerden Kruskal-Wallis H Testi kullanılmasına karar verilmiştir. Programların Veri Kurtarma oranı değişkeni kullanılan yazılım

faktörüne göre tüm gruplarda normal dağılım göstermemektedir ($p<0.05$). Bu nedenle grupların, kurtarma oranı açısından karşılaştırılmasında parametre dışı testlerden Kruskal-Wallis H Testi kullanılacaktır.

3. BULGULAR

Aynı şartlar altındaki 5 farklı durum/test için açık (Photorec, Scalpel, Foremost) ve kapalı kaynak kodlu yazılımların (RecoverMyFiles, X-Ways) header-footer analizi ile veri kurtarma özellikleri test edildiğinde; başarı oranı hesaplamasında, yazılımların kurtardığı dosyalardan görüntülenebilen ve hasarsız olanlar dikkate alınmış olup; başarı haneleri (%) cinsinden (kurtarılan dosya sayısının, toplam dosya sayısına oranı) belirtilmiştir.

3.1. Birinci Test

Yazılımlara ait veri kurtarma başarı yüzdeleri Çizelge 3.1.'de sunulmuştur. Bu test kapsamında RecoverMyFiles 50, X-Ways 45, Photorec 47, Foremost 32 ve Scalpel 34 adet dosya kurtarabilmiştir.

Çizelge 3.1. *1nci Testte Elde Edilen Sonuçlar*

USB TAŞINABİLİR BELLEK	Recover My Files v.4.6.8		X-Ways Forensics v.16.7		Photorec v6.11		Foremost v1.5		Scalpel V1.6	
TOPLAM 50 DOSYA	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**
PDF (5 adet)	5	100	5	100	5	100	3	60	3	60
AVI(5 adet)	5	100	5	100	5	100	3	60	5	100
BMP(5 adet)	5	100	5	100	5	100	0	0	0	0
JPG(5 adet)	5	100	5	100	5	100	3	60	3	60
XLS(5 adet)	5	100	5	100	5	100	5	100	5	100
XLSX(5 adet)	5	100	5	100	5	100	5	100	3	60
DOC(5 adet)	5	100	5	100	5	100	5	100	5	100
DOCX(5 adet)	5	100	5	100	5	100	5	100	5	100
MPG(5 adet)	5	100	0	0	2	40	3	60	5	100
ZIP(5 adet)	5	100	5	100	5	100	0	0	0	0
TOPLAM	**50**	**100**	**45**	**90**	**47**	**94**	**32**	**64**	**34**	**68**

3.2. İkinci Test

Elde edilen sonuçlar Çizelge 3.2.'de sunulmuştur. Bu test kapsamında RecoverMyFiles 38, X-Ways 33, Photorec 36, Foremost 17 ve Scalpel 18 adet dosya kurtarabilmiştir.

Çizelge 3.2. *2nci Testte Elde Edilen Sonuçlar*

USB TAŞINABİLİR BELLEK	Recover My Files v.4.6.8		X-Ways Forensics v16.7		Photorec v6.11		Foremost v1.5		Scalpel V1.6	
TOPLAM 53 DOSYA	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**
PDF (5 adet)	4	80	5	100	5	100	3	60	3	60
AVI(6 adet)	4	66,6	4	66,6	4	66,6	4	66,6	3	50
BMP(5 adet)	2	40	2	40	2	40	0	0	0	0
JPG(6 adet)	1	16,6	0	0	1	16,66	0	0	0	0
XLS(5 adet)	5	100	5	100	5	100	0	0	0	0
XLSX(5 adet)	5	100	5	100	5	100	2	40	2	40
DOC(6 adet)	2	33,3	2	33,3	2	33,3	2	33,3	2	33,3
DOCX(5 adet)	5	100	5	100	5	100	3	60	4	80
MPG(5 adet)	5	100	0	0	2	40	3	60	4	80
ZIP(5 adet)	5	100	5	100	5	100	0	0	0	0
TOPLAM	**38**	**71,7**	**33**	**62,2**	**36**	**67,9**	**17**	**32**	**18**	**33,9**

3.3. Üçüncü Test

Çizelge 3.3.'de görüldüğü üzere RecoverMyFiles 38, X-Ways 33, Photorec 36, Foremost 17 ve Scalpel 20 adet dosya kurtarabilmiştir.

Çizelge 3.3. 3*ncü Testte Elde Edilen Sonuçlar*

USB TAŞINABİLİR BELLEK	**Recover My Files v.4.6.8**		**X-Ways Forensics v16.7**		**Photorec v6.11**		**Foremost v1.5**		**Scalpel V1.6**	
TOPLAM 53 DOSYA	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**	**ADET**	**BAŞARI (%)**
PDF (5 adet)	4	80	5	100	5	100	3	60	3	60
AVI(6 adet)	4	66,6	4	66,6	4	66,6	2	33,3	3	50
BMP(5 adet)	2	40	2	40	2	40	0	0	0	0
JPG(6 adet)	1	16,6	0	0	1	16,6	0	0	0	0
XLS(5 adet)	5	100	5	100	5	100	0	0	0	0
XLSX(5 adet)	5	100	5	100	5	100	4	80	4	80
DOC(6 adet)	2	33,3	2	33,3	2	33,3	2	33,3	2	33,3
DOCX(5 adet)	5	100	5	100	5	100	4	80	4	80
MPG(5 adet)	5	100	0	0	2	40	2	40	4	80
ZIP(5 adet)	5	100	5	100	5	100	0	0	0	0
TOPLAM	**38**	**71,7**	**33**	**62,2**	**36**	**67,9**	**17**	**32**	**20**	**37,7**

3.4. Dördüncü Test

Bu test kapsamında RecoverMyFiles 34, X-Ways 32, Photorec 35, Foremost 25 ve Scalpel 21 adet dosya kurtarabilmiştir.

Çizelge 3.4. *4ncü Testte Elde Edilen Sonuçlar*

USB TAŞINABİLİR BELLEK	Recover My Files v.4.6.8		X-Ways Forensics v16.7		Photorec v6.11		Foremost v1.5		Scalpel V1.6	
TOPLAM 53 DOSYA	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)
PDF (5 adet)	2	40	4	80	4	80	3	60	2	40
AVI(6 adet)	4	66,6	4	66,6	4	66,6	3	50	4	66,6
BMP(5 adet)	2	40	2	40	2	40	0	0	0	0
JPG(6 adet)	1	16,6	0	0	1	16,6	0	0	0	0
XLS(5 adet)	5	100	5	100	5	100	5	100	0	0
XLSX(5 adet)	5	100	5	100	5	100	4	80	4	80
DOC(6 adet)	2	33,3	2	33,3	2	33,3	2	33,3	2	33,3
DOCX(5 adet)	5	100	5	100	5	100	4	80	4	80
MPG(5 adet)	3	60	0	0	2	40	4	80	5	100
ZIP(5 adet)	5	100	5	100	5	100	0	0	0	0
TOPLAM	**34**	**64,1**	**32**	**60,3**	**35**	**66**	**25**	**47,1**	**21**	**39,6**

3.5. Beşinci Test

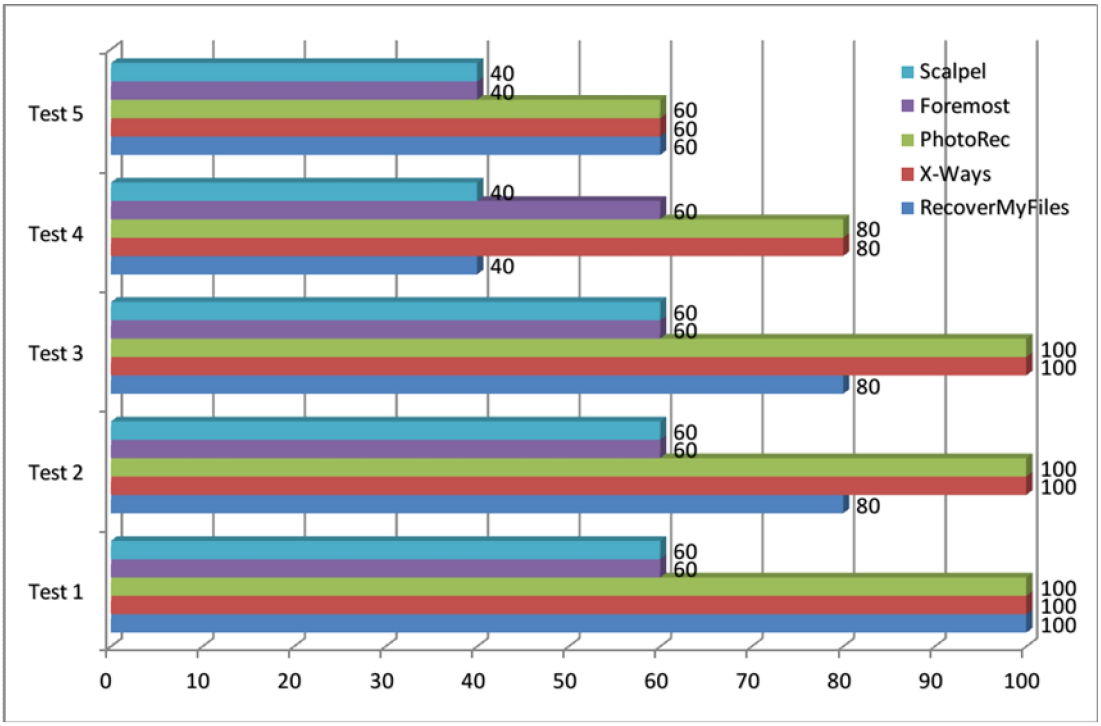
Çizelge 3.5.'de görüldüğü üzere RecoverMyFiles 39, X-Ways 28, Photorec 30, Foremost 25 ve Scalpel 28 adet dosya kurtarabilmiştir.

Çizelge 3.5. *5nci Testte Elde Edilen Sonuçlar*

USB TAŞINABİLİR BELLEK	Recover My Files v.4.6.8		X-Ways Forensics v16.7		Photorec v6.11		Foremost v1.5		Scalpel V1.6	
TOPLAM 53 DOSYA	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)	ADET	BAŞARI (%)
PDF (5 adet)	3	60	3	60	3	60	2	40	2	40
AVI(6 adet)	5	83,3	5	83,3	5	83,3	3	50	5	83,3
BMP(5 adet)	2	40	2	40	2	40	0	0	0	0
JPG(6 adet)	1	16,6	0	0	1	16,6	0	0	0	0
XLS(5 adet)	5	100	5	100	5	100	5	100	5	100
XLSX(5 adet)	5	100	5	100	5	100	4	80	4	80
DOC(6 adet)	3	50	3	50	2	33,3	3	50	3	50
DOCX(5 adet)	5	100	5	100	5	100	4	80	4	80
MPG(5 adet)	5	100	0	0	2	40	4	80	5	100
ZIP(5 adet)	5	100	0	0	0	0	0	0	0	0
TOPLAM	**39**	**73,5**	**28**	**52,8**	**30**	**56,6**	**25**	**47,1**	**28**	**52,8**

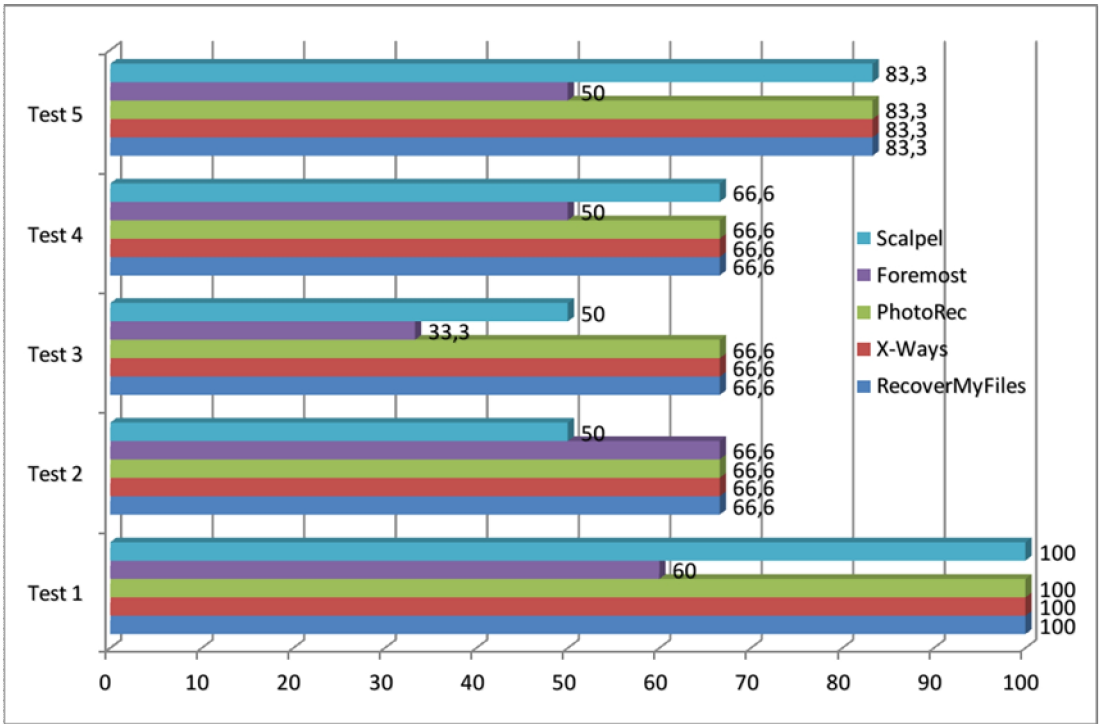
Dosya tipi bazında yazılımların testlere göre başarı yüzdeleri incelendiğinde;

Çizelge 3.6. *Yazılımların PDF Dosya Tipi Kurtarma Başarı Yüzdeleri*



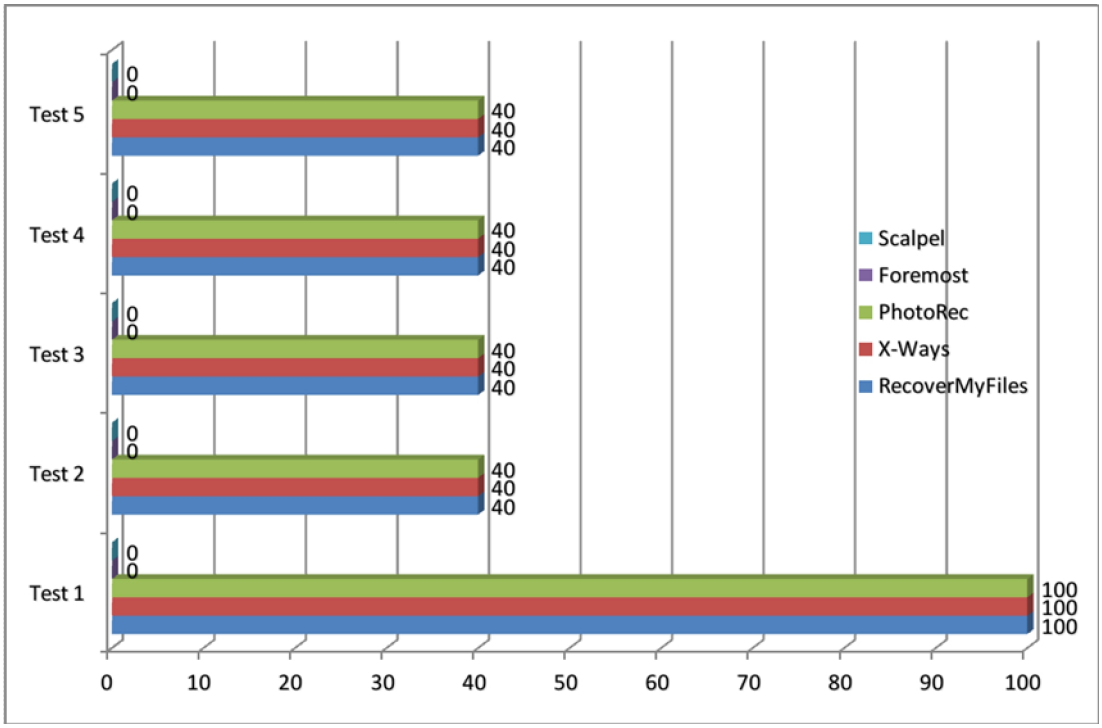
İlk üç test kapsamında, PDF tipi dosya kurtarma işlemi için Photorec ve X-Ways yazılımlarının %100 kurtarma başarı oranına sahip olduğu görülmektedir. Testler genelinde birinci testten beşinci teste doğru, PDF tipi dosyaların kurtarılma başarısında bir düşüş olduğu görülebilmektedir (Çizelge 3.6).

Çizelge 3.7. *Yazılımların AVI Dosya Tipi Kurtarma Başarı Yüzdeleri*



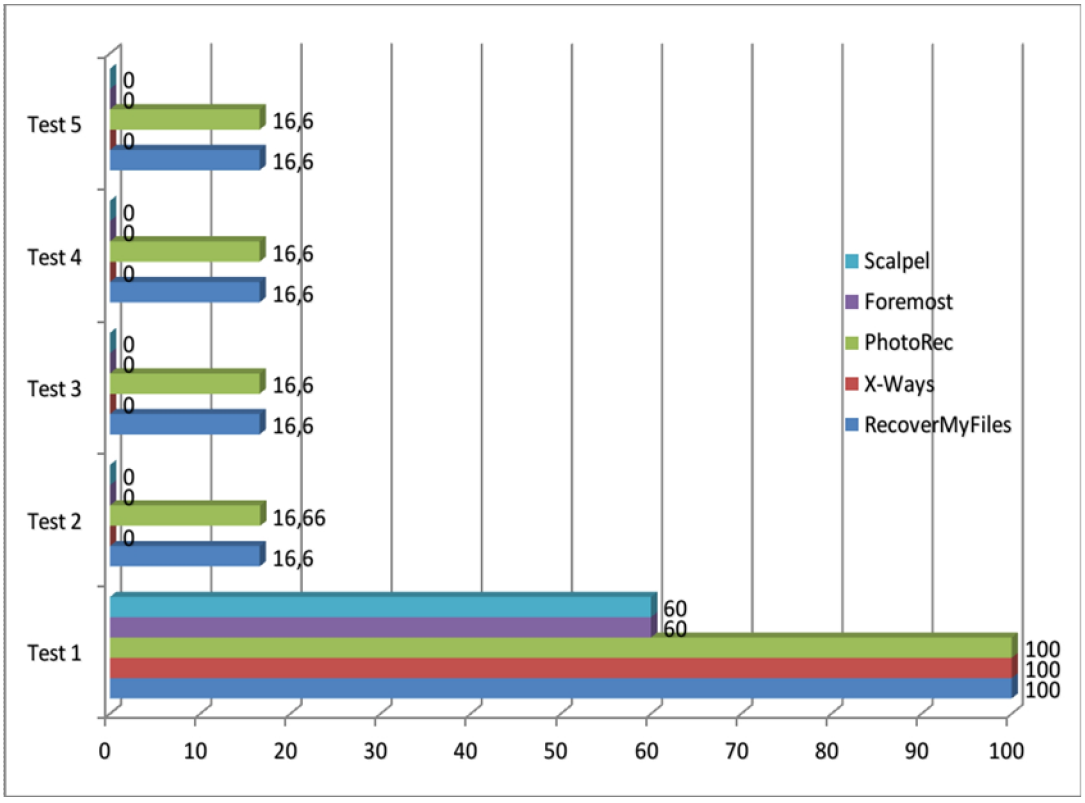
Çizelge 3.7'de görüldüğü üzere AVI tipi dosya türlerinin kurtarılmasında yazılımlar, Test 1 ve Test 5'de diğer testlere göre daha başarılı olmuşlardır.

Çizelge 3.8. *Yazılımların BMP Dosya Tipi Kurtarma Başarı Yüzdeleri*



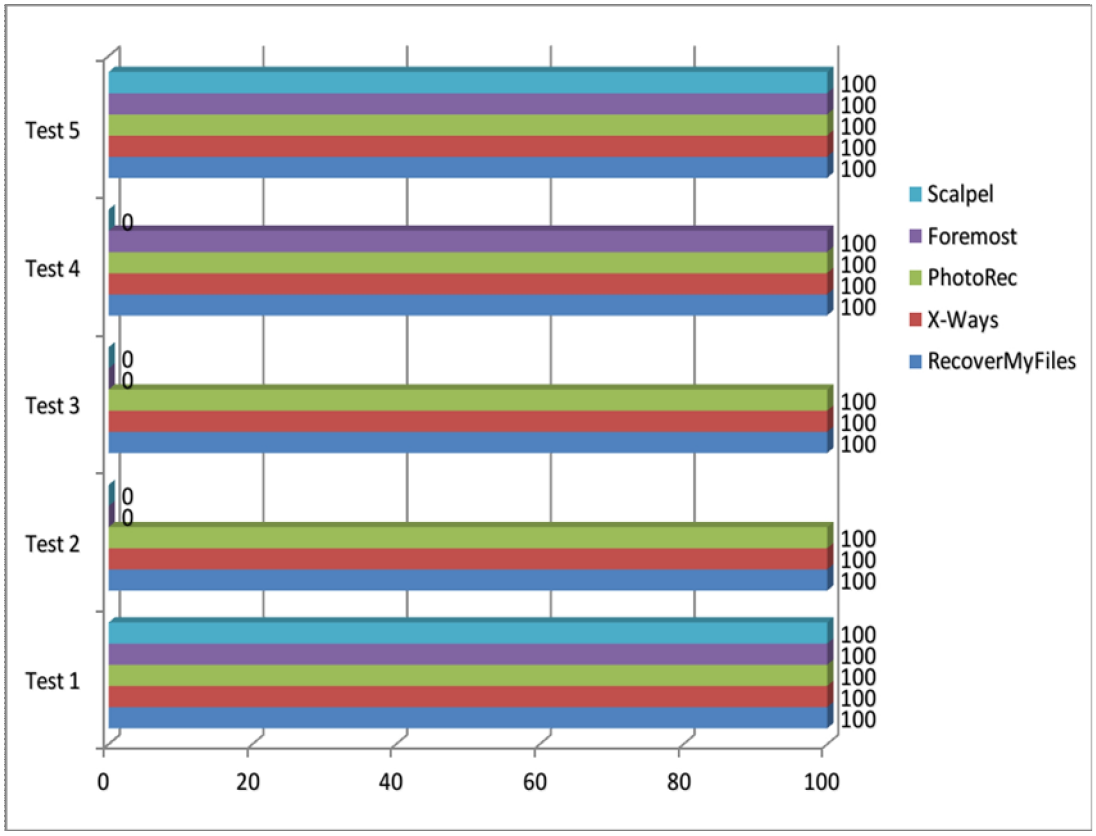
Çizelge 3.8'de, BMP tipi dosya kurtarma işlemi için Scalpel ve Foremost yazılımlarının başarısız oldukları görülmektedir.

Çizelge 3.9. *Yazılımların JPG Dosya Tipi Kurtarma Başarı Yüzdeleri*



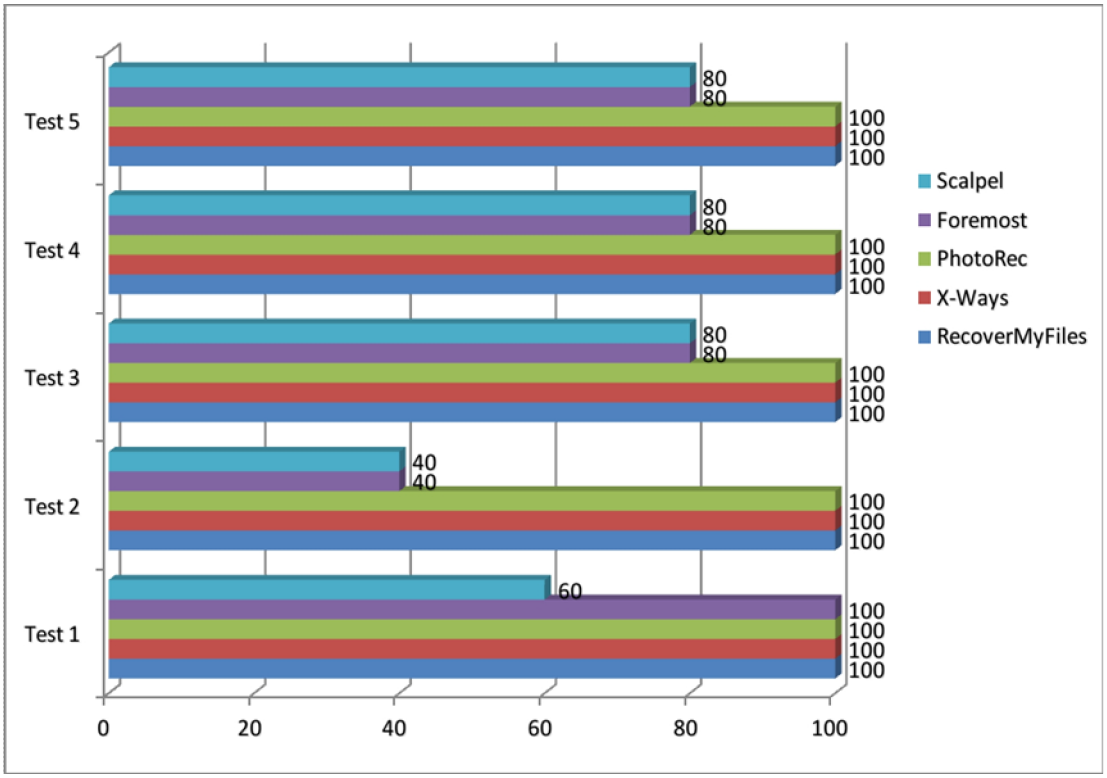
Çizelge 3.9' da, JPG tipi dosyaların kurtarılması işlemi kapsamında Photorec ve RecoverMyFiles yazılımlarının diğer yazılımlara oranla daha başarılı olduları, Scalpel ve Foremost yazılımlarının ilk test haricinde başarısız oldukları görülmektedir.

Çizelge 3.10. *Yazılımların XLS Dosya Tipi Kurtarma Başarı Yüzdeleri*



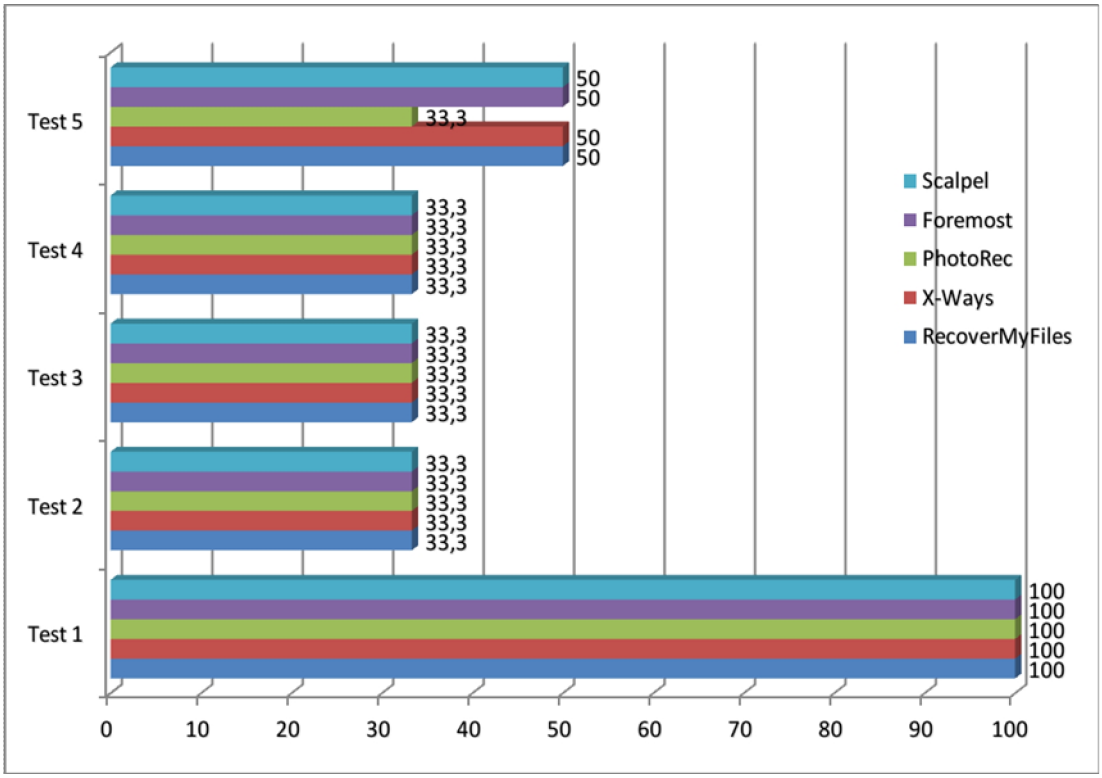
Çizelge 3.10'da görüldüğü üzere, yazılımların genel olarak, tüm testler için XLS tipi dosyaların kurtarılmasında başarılı oldukları görülmektedir.

Çizelge 3.11. *Yazılımların XLSX Dosya Tipi Kurtarma Başarı Yüzdeleri*



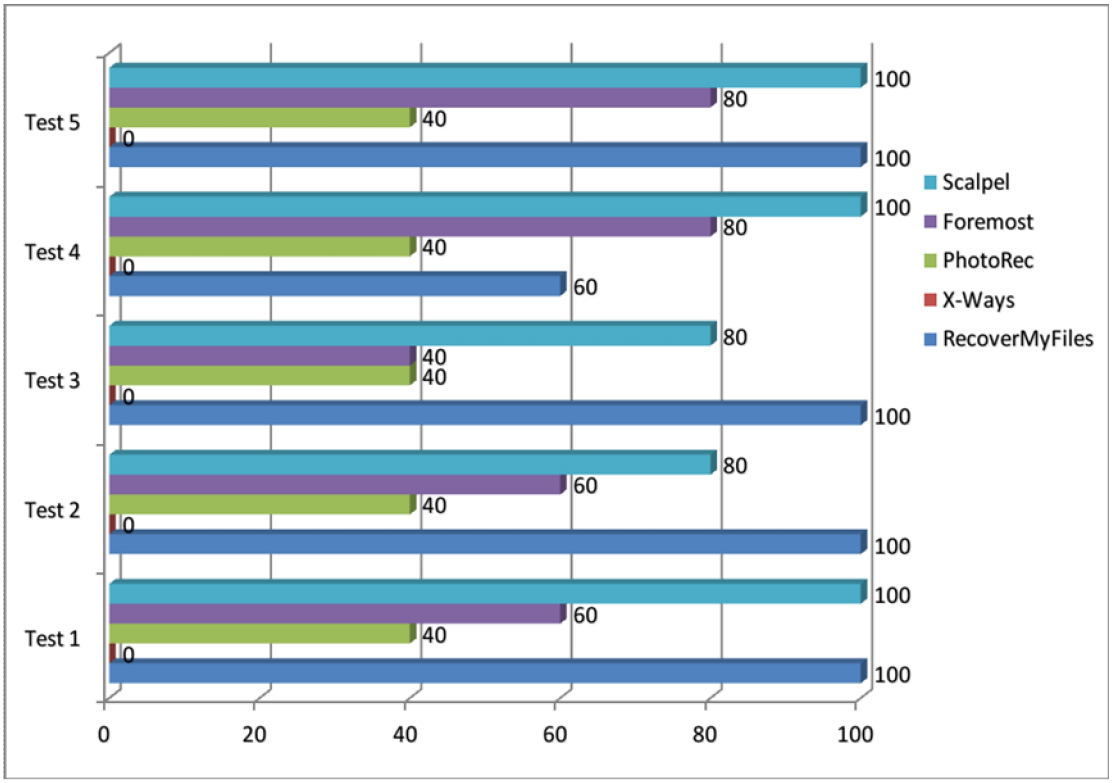
Çizelge 3.11'de, XLSX tipi dosyaların kurtarılmasında, PhotoRec, X-Ways ve RecoverMyFiles yazılımlarının testler genelinde başarılı olduğu görülmektedir.

Çizelge 3.12. *Yazılımların DOC Dosya Tipi Kurtarma Başarı Yüzdeleri*



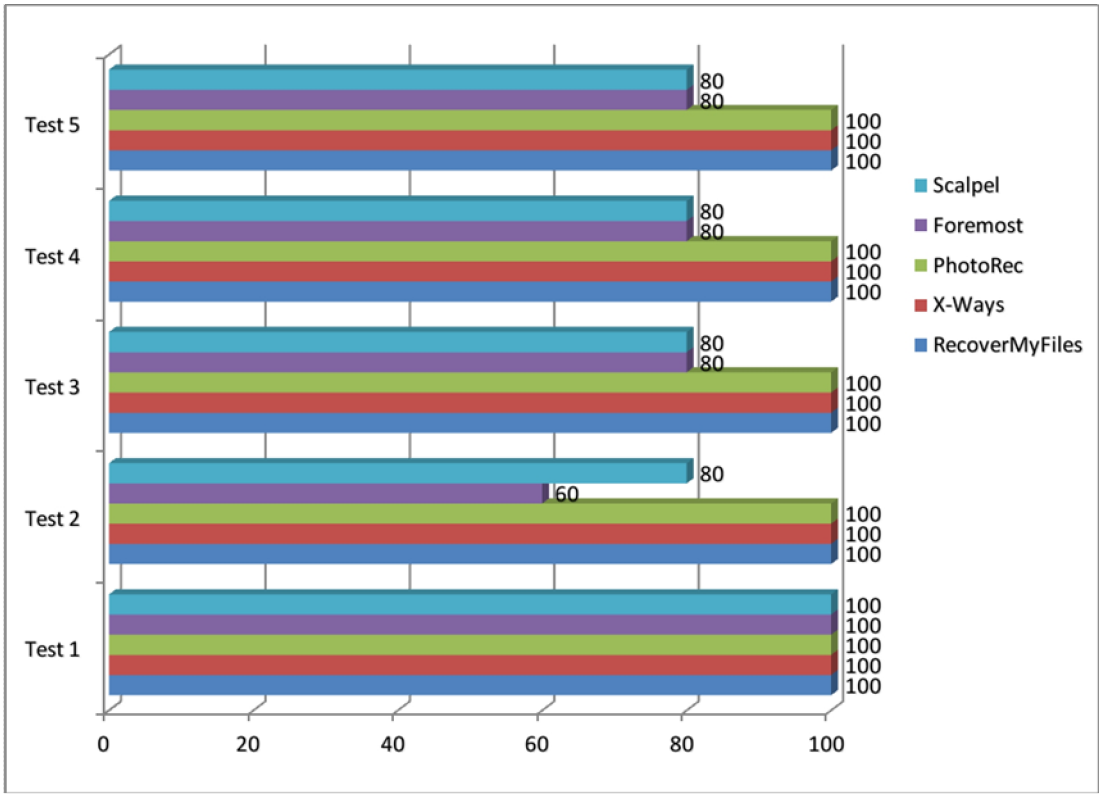
Çizelge 3.12'de, DOC tipi dosyaların kurtarılmasında, yazılımların genel olarak aynı seviyede başarı oranına sahip oldukları görülebilmektedir.

Çizelge 3.13. *Yazılımların MPG Dosya Tipi Kurtarma Başarı Yüzdeleri*



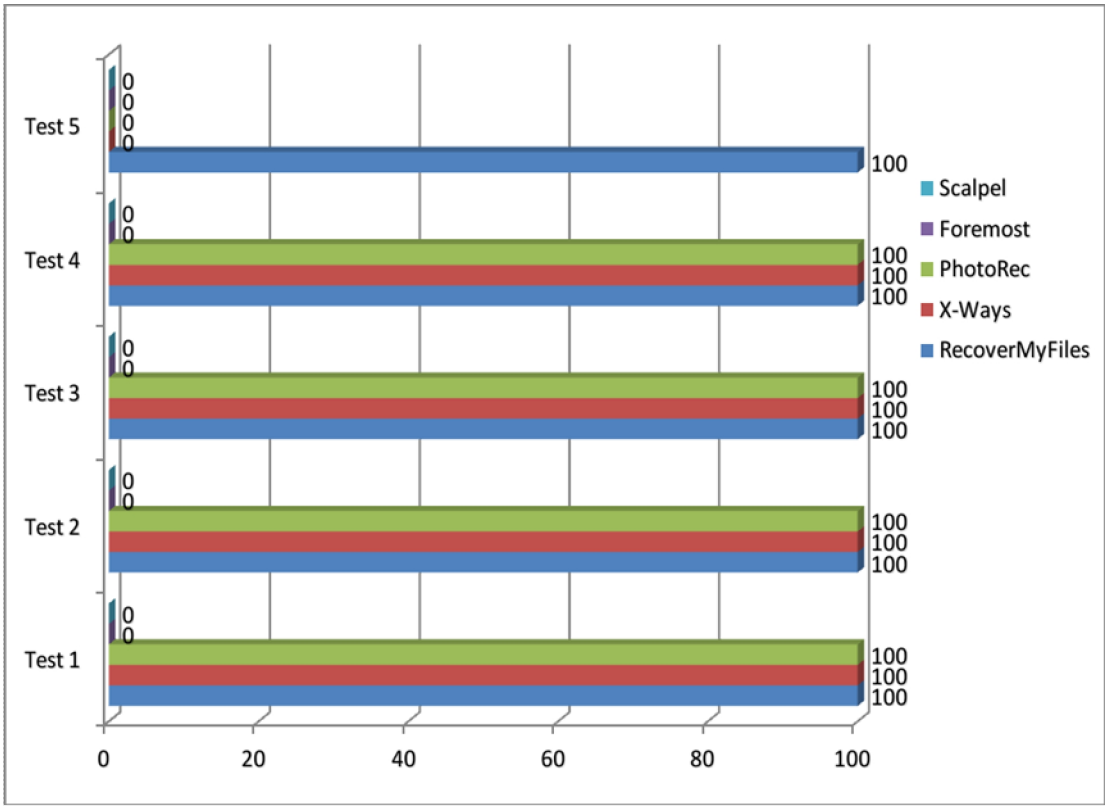
Çizelge 3.13'de, MPG tipi dosyaların kurtarılmasında, Scalpel ve Foremost yazılımlarının, dosyaların NTFS ya da FAT ile biçimlendirilerek silindiği medyalar üzerinde daha başarılı oldukları görülmektedir.

Çizelge 3.14. *Yazılımların DOCX Dosya Tipi Kurtarma Başarı Yüzdeleri*



Çizelge 3.14'de, DOCX tipi dosyaların kurtarılmasında, yazılımların genel olarak aynı seviyede başarı oranına sahip oldukları görülebilmektedir.

Çizelge 3.15. *Yazılımların ZIP Dosya Tipi Kurtarma Başarı Yüzdeleri*



Çizelge 3.15'de, ZIP tipi dosyaların kurtarılmasında, yazılımların tüm testler boyunca başarı oranlarında bir devamlılık olduğu görülebilmektedir.

Açık kaynak kodlu programlar ile kapalı kaynak kodlu programlar arasında dosya kurtarma oranı açısından anlamlı fark bulunmaktadır (U=5.360,000 p<0.001). Açık kaynak kodlu programların dosya kurtarma oranı sıra numarası 111.23 ve kapalı kaynak kodlu programların dosya kurtarma oranı sıra numarası 146.90'dır. Buna göre kapalı kaynak kodlu programların dosya kurtarma oranı daha yüksektir (Çizelge 3.16).

Çizelge 3.16. *Kaynak Kodlara Göre Kurtarma Oranları*

	Kaynak	n	Sıra Ortalaması	Mann-Whitney U	P
Kurtarma Oranı	Açık	150	111,23	5.360,00	0,000*
	Kapalı	100	146,9		

***p<0.05**

Farklı yazılımlar arasında dosya kurtarma oranları açısından anlamlı fark bulunmaktadır (Ki-Kare=34.851 p<0.05). RecoverMyFiles yazılımı ile kurtarılan dosyaların oranlarının sıra ortalaması 156.01; X-Ways yazılımı ile kurtarılan dosyaların oranlarının sıra ortalaması 137.79; Photorec yazılımı ile kurtarılan dosyaların oranlarının sıra ortalaması 145.04; Foremost ile kurtarılan dosyaların oranlarının sıra ortalaması 92.13 ve Scapel ile kurtarılan dosyaların oranlarının sıra ortalaması 96.53'tür. Buna göre dosya kurtarma oranı en yüksek yazılım RecoverMyFiles; en düşük yazılım Foremost olduğu belirlenmiştir (Çizelge 3.17).

Çizelge 3.17. *Yazılımlara Göre Kurtarma Oranları*

	Yazılım	**n**	**Sıra Ortalaması**	**Ki Kare**	**p**
Kurtarma Oranı	RecoverMyFiles	50	156,01	34,851	0,000*
	X-Ways	50	137,79		
	Photorec	50	145,04		
	Foremost	50	92,13		
	Scalpel	50	96,53		

***p<0.05**

Farklı dosya türleri arasında kurtarılma oranları açısından anlamlı fark bulunmaktadır (Ki-Kare=80.411 p<0.05). PDF dosyalarının kurtarılma oranı sıra ortalaması 136.64, AVI dosyalarının kurtarılma oranı sıra ortalaması 134.50, BMP dosyalarının kurtarılma oranı sıra ortalaması 72.48, JPG dosyalarının kurtarılma oranı sıra ortalaması 59.52, XLS dosyalarının kurtarılma oranı sıra ortalaması 166.90, XLSX dosyalarının kurtarılma oranı sıra ortalaması 174.70, DOC dosyalarının kurtarılma oranı sıra ortalaması 95.24, DOCX dosyalarının kurtarılma oranı sıra ortalaması 181.94, MPG dosyalarının kurtarılma oranı sıra ortalaması 116.72 ve ZIP dosyalarının kurtarılma oranı sıra ortalaması 116.36'dır. Buna göre kurtarılma oranı en yüksek dosyalar DOCX, XLSX ve XLS; kurtarılma oranı en düşük dosyalar ise JPG, BMP ve DOC formatlı dosyalar olarak belirlenmiştir (Çizelge 3.18).

Çizelge 3.18. *Dosya Türlerine Göre Kurtarılma Oranları*

	Dosya	n	Sıra Ortalaması	Ki Kare	p
Kurtarılma Oranı	PDF	25	136,64	80,411	0,000*
	AVI	25	134,5		
	BMP	25	72,48		
	JPG	25	59,52		
	XLS	25	166,9		
	XLSX	25	174,7		
	DOC	25	95,24		
	DOCX	25	181,94		
	MPG	25	116,72		
	ZIP	25	116,36		

***p<0.05**

Açık kaynak kodlu yazılımlar ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki-Kare=55.763 p<0.05). Açık kaynak kodlu yazılımlar ile kurtarılan dosyalardan kurtarılma oranı en yüksek olanlar DOCX, XLSX ve XLS; kurtarılma oranı en düşük olanlar ise BMP, JPG ve ZIP formatlı dosyalardır (Çizelge 3.19). Kapalı kaynak kodlu yazılımlar ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki-Kare=49.570 p<0.05). Kapalı kaynak kodlu yazılımlar ile kurtarılan dosyalardan kurtarılma oranı en yüksek olanlar DOCX, XLSX ve XLS; kurtarılma oranı en düşük olanlar ise JPG, BMP ve MPG formatlı dosyalardır (Çizelge 3.19).

Çizelge 3.19. *Kaynak Kod ve Dosya Türüne Göre Kurtarılma Oranları*

		Açık Kaynak Kodlu Yazılım				***Kapalı Kaynak KodluYazılım***			
	Dosya	**n**	**Sıra Ortalaması**	**Ki Kare**	**p**	**n**	**Sıra Ortalaması**	**Ki Kare**	**p**
Kurtarılma Oranı	PDF	15	85,73	55,763	0,000*	10	50,9	49,57	0,000*
	AVI	15	87,47			10	46		
	BMP	15	35,57			10	34,6		
	JPG	15	38,17			10	21,8		
	XLS	15	92,83			10	73		
	XLSX	15	104,8			10	73		
	DOC	15	64,43			10	31,2		
	DOCX	15	112,53			10	73		
	MPG	15	85,83			10	35,25		
	ZIP	15	47,63			10	66,25		

***p<0.05**

Çalışmamızda RecoverMyFiles yazılımı ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmuştur (Ki Kare=30.592 $p<0.05$). RecoverMyFiles yazılımı ile kurtarılma oranı en yüksek olan dosya formatları XLS, XLSX, DOCX ve ZIP; kurtarılma oranı en düşük olan dosya formatları ise JPG, DOC ve BMP'dir (Çizelge 3.20). X-Ways yazılımı ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki Kare=32.111 $p<0.05$). X-Ways yazılımı ile kurtarılma oranı en yüksek olan dosya formatları XLS, XLSX ve DOCX; kurtarılma oranı en düşük olan dosya formatları ise MPG, JPG ve DOC'tur (Çizelge 3.20). Photorec yazılımı ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki Kare=28.621 $p<0.05$). Photorec yazılımı ile kurtarılma oranı en yüksek olan dosya formatları XLS, XLSX ve DOCX; kurtarılma oranı en düşük olan dosya formatları ise JPG, DOC ve MPG'dir (Çizelge 3.20). Foremost yazılımı ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki Kare=30.040 $p<0.05$). Foremost yazılımı ile kurtarılma oranı en yüksek olan dosya formatları DOCX, XLSX ve XLS; kurtarılma oranı en düşük olan dosya formatları ise BMP, ZIP ve JPG'dir (Çizelge 3.20). Scalpel yazılımı ile kurtarılan farklı formattaki dosyaların kurtarılma oranları arasında anlamlı fark bulunmaktadır (Ki Kare=32.228 $p<0.05$). Scalpel yazılımı ile kurtarılma oranı en yüksek olan dosya formatları MPG, DOCX ve AVI; kurtarılma oranı en düşük olan dosya formatları ise BMP, ZIP ve JPG'dir (Çizelge 3.20).

Çizelge 3.20. *Yazılımlar ve Dosya Türüne Göre Kurtarma Oranları*

		Dosya	n	Sıra Ortalaması	Ki Kare	p
Kurtarma Oranı	***RecoverMyFiles***	PDF	5	19,9	30,592	0,000*
		AVI	5	21,6		
		BMP	5	15,2		
		JPG	5	9,2		
		XLS	5	36		
		XLSX	5	36		
		DOC	5	13,4		
		DOCX	5	36		
		MPG	5	31,7		
		ZIP	5	36		
	X-Ways	PDF	5	30,9	32,111	0,000*
		AVI	5	24,9		
		BMP	5	19,9		
		JPG	5	11,9		
		XLS	5	37,5		
		XLSX	5	37,5		
		DOC	5	18,3		
		DOCX	5	37,5		
		MPG	5	5,5		
		ZIP	5	31,1		
	Photorec	PDF	5	30,9	28,621	0,001*
		AVI	5	24,9		
		BMP	5	18,7		
		JPG	5	10,3		
		XLS	5	37,5		
		XLSX	5	37,5		
		DOC	5	13,5		
		DOCX	5	37,5		
		MPG	5	14		
		ZIP	5	30,2		
	Foremost	PDF	5	29,2	30,04	0,000*
		AVI	5	27,1		
		BMP	5	8,5		
		JPG	5	13		
		XLS	5	31,9		
		XLSX	5	38,2		
		DOC	5	25,6		
		DOCX	5	40		
		MPG	5	33		
		ZIP	5	8,5		
	Scalpel	PDF	5	26,2	32,228	0,000*
		AVI	5	34,1		
		BMP	5	9		
		JPG	5	13		
		XLS	5	24		
		XLSX	5	32,4		

		DOC	5	25,7		
		DOCX	5	38,9		
		MPG	5	42,7		
		ZIP	5	9		

***p<0.05**

Uygulanan testler arasında dosya kurtarılma oranı açısından anlamlı fark bulunmaktadır (Ki Kare=24.881 p<0.05). 1nci testte kurtarılan dosyaların kurtarılma oranları sıra ortalaması 169.57; 2nci testte kurtarılan dosyaların kurtarılma oranları sıra ortalaması 112.47; 3ncü testte 113.60; 4ncü testte 114.82 ve 5inci testte 117.04'tür. Buna göre dosya kurtarılma oranı en yüksek test 1nci test; en düşük test ise 2nci testtir (Çizelge 3.21).

Çizelge 3.21. *Testlere Göre Kurtarma Oranları*

	Test	**n**	**Sıra Ortalaması**	**Ki-Kare**	**p**
Kurtarılma Oranı	1. test	50	169,57	24,881	0,000*
	2. test	50	112,47		
	3. test	50	113,6		
	4. test	50	114,82		
	5. test	50	117,04		

*p<0.05

4. TARTIŞMA

Veri kurtarma işlemleri adli bilişimin temel yapıtaşı olup bu konu üzerinde çalışmalar devam etmektedir (Cohen, 2007; Garfinkel, 2007; Alghafli ve ark., 2014). Geleneksel veri kurtarma yöntemlerinde medyanın dosyalama sistemi üzerinden veri kurtarılmakta iken, veri kazıma (data carving) yöntemlerinde, verilerin başlık ve son kısım bilgileri (header-footer) gibi kendi yapılarının çözümlenmesi ile dosyalar kurtarılmaktadır (Pal ve Memon, 2009).

Adli bilişim alanında tüm dünyada resmi kurumlara ait laboratuvarlarda yapılan incelemelerde ağırlıklı olarak kapalı kaynak kodlu yazılımlar kullanılmaktadır. Açık kaynak kodlu yazılımlar ücretsiz olmaları nedeniyle yapılan incelemenin ekonomisine olumlu katkı sağlamaktadırlar. Ayrıca yazılımların kaynak kodları açık olduğundan incelemelerde yapılan işlemlerin hangi yöntemlerle yapıldığı mahkeme sürecinde ortaya konabilmekte ve kullanıcı tarafından ihtiyaçlara göre değiştirilebilmektedir.

Çalışmada veri kazıma yöntemi ile hem açık kaynak kodlu yazılımlar hem de kapalı kaynak kodlu yazılımlar kullanılarak veri kurtarma işlemi yapılarak sonuçlar birbirleri ile karşılaştırılmıştır. Veri kurtarma işleminde dosyanın tamamının kurtarılması önemlidir (Garfinkel, 2007). Bu nedenle çalışmamızda eksik ya da hasarlı olarak kurtarılan dosyalar değil, tamamı hasarsız ve görüntülenebilen şekilde kurtarılmış dosyalar dikkate alınmıştır.

Açık kaynak kodlu yazılımlar ile kapalı kaynak kodlu yazılımlar arasında dosya kurtarma oranı sıra numarası açısından anlamlı fark bulunmuş, kapalı kaynak kodlu yazılımların dosya kurtarma oranının daha yüksek olduğu belirlenmiştir ($p= 0,000$). Bu durum adeta resmi kurumlar tarafından kapalı kaynak kodlu yazılımların neden daha fazla güvenilir bulunduğunun açıklaması niteliğindedir.

Çalışmamızda hem farklı yazılımlar arasında dosya kurtarma oranları açısından hem farklı dosya türleri arasında kurtarılma oranları açısından anlamlı farklılık saptanmıştır (p= 0,000). Kapalı kaynak kodlu yazılımların dosya kurtarma açısından daha başarılı bulunmuş olması ile uyumlu şekilde çalışmamızda dosya kurtarma oranı en yüksek yazılım RecoverMyFiles bulunmuştur. Ancak açık kaynak kodlu yazılımlardan biri olan PhotoRec yazılımının başarı oranının, kapalı kaynak kodlu X-Ways yazılımından daha yüksek olması dikkat çekicidir. Çalışmamız genelinde DOCX, XLSX ve XLS türü dosyaların kurtarılma oranlarının, yazılımların kapalı kaynak kodlu ya da açık kaynak kodlu olmalarından bağımsız olarak, yüksek olduğu görülmüştür (p= 0,000). Kurtarılma oranı en düşük bulunan dosya türleri arasında ise kullanılan yazılımın açık kaynak kodlu ya da kapalı kaynak kodlu olması sonuçlarda farklılığa neden olmuştur. Kapalı kaynak kodlu yazılımlar açık kaynak kodlu yazılımlardan farklı olarak ZIP dosyalarını kurtarmada daha başarılı iken; açık kaynak kodlu yazılımlar kapalı kaynak kodlu yazılımlardan farklı olarak MPG dosyalarını kurtarmada daha başarılı bulunmuştur (p<0,001).

Veri kurtarma işlemi, silinmiş dosyaların kurtarılmasıdır. Medyanın içerisinde silinen dosyaların, medya içerisinden tamamen silinmemesi verilerin kurtarılmasına olanak sağlamaktadır. Silme işlemi veya biçimlendirme işlemleri sonucunda, silinen dosyanın fiziksel alanına yeni veriler yazılabilmektedir (Pal ve Memon, 2009). Bu nedenle test senaryoları çalışmada kurtarılan dosya türlerinin kurtarılma oranını birinci derecede etkiler. Çalışmamızda 1nci testten sonraki testlerde, flash belleklere farklı dosyalar eklenmesi veya çeşitli biçimlendirme işlemleri yapılmasının yazılımların başarısını olumsuz etkilediği görülmüştür (p= 0,000).

Yapılan testler ve istatistikî değerlendirmeler kapsamında kapalı kaynak kodlu yazılımlar daha başarılı bulunmuş olsa da açık kaynak kodlu yazılımların başarısız olduğu söylenemez. Veri kurtarma işlemlerinde sonuçlar, incelenen medyaya göre değişebilir. Çalışmamızda 5 adet aynı marka ve özellikte flash bellek kullanılmış olup, çalışmamızın sonuçları bununla sınırlıdır. Sabit disk, hafıza kartı, CD, DVD

gibi farklı medyalar içerisinde yapılacak veri kurtarma işlemlerinde farklı sonuçlar elde edilebilir (Winter, 2013).

Çalışmamız veri kurtarma işlemlerinde kapalı kaynak kodlu yazılımların başarılı olduğunu ancak açık kaynak kodlu yazılımların da gerektiğinde göz ardı edilmemesi gerektiğini gözler önüne sermektedir. Kurtarılacak dosya türüne bağlı olarak sadece açık kaynak kodlu yazılımların kullanılabileceği durumlar da söz konusu olabilir. Adli bilişim incelemelerinde incelenecek medyalara çok çeşitli şekillerde müdahale edilmiş olabileceğinden resmi kurumlarda her iki yazılım türünün beraber kullanılması ile daha sağlıklı sonuçlar elde edilecektir.

5. SONUÇ VE ÖNERİLER

Adli Bilişim, dünyada yeni oluşturulmaya başlanmış bir bilimdir ve konu hakkında yapılan her çalışma bu alanı aydınlatmaya yöneliktir. Bu çalışmada adli bilişim incelemelerinde önemli bir yer tutan veri kurtarma işlemleri için açık ve kapalı kaynak kodlu yazılımların birbirleri ile mukayese edilerek, yaygın olarak kullanılmakta olan kapalı kaynak kodlu yazılımların yanı sıra açık kaynak kodlu yazılımların da etkin olarak kullanılabilir olup olmadığı konusu incelenmiştir.

Literatürde kapalı kaynak kodlu yazılımlar ile açık kaynak kodlu yazılımların birebir karşılaştırılmasına yönelik bir çalışma bulunmamaktadır. Uluslararası düzeyde açık kaynak kodlu yazılımların kullanılmasına yönelik küçük çaplı çalışmalar yapılmıştır (Bassi 2008). Çalışmamızda 5 adet aynı marka ve özellikte flash bellek üzerinde RecoverMyFiles, X-Ways, PhotoRec, Foremost ve Scalpel yazılımları ile 5 farklı test senaryoları gereği veri kurtarma çalışması yapılmıştır. Farklı medyalar içerisinde, farklı dosyalama sistemlerinde ve farklı silinme durumlarında yazılımların veri kurtarma başarı oranları değişebilmektedir. Çalışmamızın sonucu olarak kapalı kaynak kodlu yazılımların dosya kurtarma oranları açısından daha başarılı olduğu belirlenmiştir. Ancak açık kaynak kodlu yazılımlar da başarısız değildir. Bu kapsamda adli veri kurtarma işlemlerinde tek bir yazılıma ya da tek bir yazılım türüne bağlı kalınmaması gerektiği gerçeği gözler önüne serilmiştir.

Tezimizin test senaryolarına göre kullanılan yazılımların kurtarılan dosya türüne göre birbirlerinden farklı oldukları tespit edilmiştir. Açık kaynak kodlu yazılımların MPG türü dosyaları kurtarmada daha başarılı oldukları görülmüştür. Bu nedenle incelenecek medyada kurtarılacak dosya türü ve dosyaların bulunma biçimine göre veri kurtarma incelemelerinde açık kaynak kodlu yazılımlar kullanılmalıdır. Ayrıca açık kaynak kodlu yazılımların ücretsiz olması nedeniyle incelemenin maliyetini olumlu etkileyeceği açıktır.

Çalışmamızın sonucu olarak Üniversitelerin ilgili bölümlerinde, özel ve resmi bilirkişilik kurumlarının kriminal laboratuvarlarında ve adli bilişim incelemesi yapan birimlerde veri kurtarma incelemelerinde daha ayrıntılı ve sağlıklı sonuçlar elde edilmesine olanak sağlayacağından hem açık kaynak kodlu yazılımların hem de kapalı kaynak kodlu yazılımların beraber kullanılmasını öneriyoruz.

Daha detaylı sonuçlar elde edilmesi için veri kurtarma konusunda farklı medyalar üzerinde, farklı durumlar oluşturularak ve farklı yazılımlar kullanılarak yapılacak geniş çaplı araştırmalara ihtiyaç vardır. Bu çalışmalardan elde edilecek sonuçlar tezimizin sonuçları ile birleştirilerek adli veri kurtarma incelemelerinde kurtarılacak dosya türüne göre kullanılacak yazılımları belirleyen ulusal ve uluslar arası standartlar geliştirilmelidir.

ÖZET

Veri Kurtarma Açısından Açık Kaynak Kodlu Ve Kapalı Kaynak Kodlu Yazılımların Karşılaştırılması

Veri kurtarma işlemleri adli bilişim incelemelerinde araştırmanın en temel konusunu oluşturmaktadır. Günümüzde tüm dünyada resmi kurumların adli bilişim laboratuvarlarında yaygın olarak kapalı kaynak kodlu yazılımlar kullanılmaktadır. Bu çalışmada, açık kaynak kodlu ve ücretsiz olan yazılımların, kapalı kaynak kodlu yazılımlar ile birlikte kullanılabilir olup olmadığı araştırılmıştır.

Bu amaçla aynı marka ve özellikteki 5 farklı flash bellek 5 ayrı test senaryosu gereği 10 farklı türde dosya yüklenip silinerek veri kurtarma çalışması yapılmıştır. Elde edilen veriler SPSS 15.0 programı kullanılarak değerlendirilmiş, sonuçlar tablo ve grafikler şeklinde sunulmuştur.

Sonuç olarak veri kurtarma işlemlerinde dosya kurtarma oranları açısından kapalı kaynak kodlu yazılımların istatistiki açıdan anlamlı şekilde daha başarılı olduğu belirlenmiştir ($p=0,000$). Tüm yazılımların dosya kurtarma oranları açısından anlamlı olarak birbirlerinden farklı olduğu belirlenmiştir.

Adli bilişim alanında yapılacak incelemelerin sonucu veri kurtarma işlemlerinin başarısı ile doğru orantılır. Yapılacak araştırmalarda açık ve kapalı kaynak kodlu yazılımların beraber kullanılmasının daha detaylı sonuçlar elde etmek açısından yararlı olduğu kanatindeyiz. Teknolojinin insanlığa sağladığı kolaylıklar ve özgürlüklerin yanısıra bilişim dünyası da gelişmekte ve farklılaşmaktadır. Veri kurtarma konusunda farklı medya türleri ve yazılımlar kullanılarak yapılacak detaylı incelemeler de yararlı olacaktır.

Anahtar Sözcükler: Adli Bilişim, Veri Kurtarma, Açık Kaynak Kodlu Yazılım, Kapalı Kaynak Kodlu Yazılım

SUMMARY

Comparison of Open Source and Proprietary Software In Data Recovery

Data recovery process is the main subject of computer forensics examinations. In all over the world, at computer forensics examinations closed source software are widely used by governmental agencies. In this workout, we tried to prove wheather open source software can be used together with closed ones in computer forensics examinations.

In the workout, within the same brand but different 5 USB flash drives, created 5 different situations and saved 10 different kinds of files, then tried to recovery data from them. Conclusions evaluated with SPSS v15.0 program and be shown with tables and graphs.

It is found that closed source software have statistically higher file recovery success ratio than open source ones (p=0,000). There found meaningfull differences about data recovery, between all of the software.

Computer forensics examinations' success has a direct proportion with data recovery process. As a conclusion of the workout, we have an opinion of using closed and open source software together with the data recovery process can result detailed and positive effects. As well as technology provide ease and more freedom to users, also informatics is developing and becoming dissimilar. On the subject of data recovery, it will be helpful to make more workouts with different software and media types.

Keywords: Computer Forensics, Data Recovery, Open Source Software, Closed Source Software

KAYNAKLAR

Adli Bilişim, Erişim: [http://tr.wikipedia.org/wiki/Adli_bili%C5%9Fim]. Erişim Tarihi: 05.09.2013

AFF, Erişim: [afflib.org]. Erişim Tarihi: 26.02.2011

AIR - Automated Image and Restore, Erişim: [sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page]. Erişim Tarihi: 26.02.2011

ALGHAFLI, K., JONES, A., MARTIN, T., (2014), Investigating and Measuring Capabilities of the Forensics File Carving Techniques, Future Information Technology- Lecture Notes in Electrical Engineering, **276**: 329-336

ALTHEIDE, C., CARVEY, H., DAVIDSON, R., (2011). Disk and File System Analysis *In: Digital Forensics with Open Source Tools,* Ed.:R. DAVIDSON, MA: Elsevier Inc., p.: 39-67

ARTHUR, K.K., VENTER, H.S., (2005), An Investigation Into Computer Forensic Tools; Erişim: [http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf], Erişim Tarihi: 08.05.2012)

ASHCROFT, J., (2001) p.:2, The Law Enforcement Response to Electronic Evidence *In: Electronic Crime Scene Investigation: A Guide for First Responders*, Ed.: J. ASHCROFT, Washington: PhotoDisc, Inc., p.: 1-2

BASSI, S. D., (2008) An Automated Acquisition System For Media Exploitation. Yüksek lisans tezi, Naval Postgraduate School. Danışman: Ph.D.S. GARFINKEL

BOTCHEK, R., (2008), Benchmarking Hard Disk Duplication Performance in Forensic Applications, p.: 1-12 (10) Erişim: [http://www.tableau.com/pdf/en/Tableau_Forensic_Disk_Perf.pdf]. Erişim Tarihi: 05.11.2011

BUKHARI, S., YUSOF, I., ABDULLAH, M.F.A., (2004), Performance Evaluation Of Open-Source Disk Imaging Tools For Collecting Digital Evidence, Proceedings of Regional Conference on Knowledge Integration in ICT 2010 Erişim: [http://tr.scribd.com/doc/114126872/Performance-Evaluation-of-Open-source-Disk-Imaging-Tools-for-Collecting-Digital-Evidence]. Erişim Tarihi: 05.05.2012

CARRIER, B., (2005). Digital Investigation Foundation. *In: File System Forensic Analysis*, Ed.: B. CARRIER, NJ: Addison Wesley Professional, p.: 12-21

CARRIER, B., SPAFFORD, E. H., (2003), Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, **2**(2):1-20

CEYLAN, R., ŞİRİKÇİ, A.S. (2011). Bilişim Teknolojileri İncelemeleri-Veri İncelemeleri. *İçinde: Adli Bilimler Cilt II,* Ed.: B. CİHANGİROĞLU, Ankara: Jandarma Kriminal Daire Başkanlığı Yayınları, s.: 147-235

COHEN, M.I., (2008), PyFlag – An Advanced Network Forensic Framework, Digital Investigation, **5**:112-120

COHEN, M.I., (2007), Advanced carving techniques, Digital Investigation, **4**(3-4):119-128

ÇİÇEK, İ., OKATAN, A., Ülkemizde Adli Bilişim laboratuarı kurulumu ve Bilişim Suçlarıyla mücadeleye Katkıları, Ankara barosu Bilişim ve Hukuk Dergisi, **6**:28-33

Dc3dd, Erişim: [dc3dd.sourceforge.net]. Erişim Tarihi: 26.02.2011

Dcfldd, Erişim: [dcfldd.sourceforge.net]. Erişim Tarihi: 26.02.2011

Debian Free Software Guidelines, Erişim: [en.wikipedia.org/wiki/Debian_Free_Software_Guidelines]. Erişim Tarihi: 26.02.2011

Debian Sosyal Sözleşmesi, Erişim: [debian.org/social_contract#guidelines, erişim 26 Şubat 2011]. Erişim Tarihi: 26.02.2011

DELP, S.L., ANDERSON, F.C., ARNOLD, A.S., LOAN, P., HABIB, A., JOHN C.T., GUENDELMAN E., THELEN D.G., (2007), OpenSim: Open-Source Software to Create and Analyze Dynamic Simulations of Movement, IEEE Transactions On Biomedical Engineering Journal, **54**(11), p.: 1940-1950

DOWLING, A., (2006), Digital Forensics: A Demonstration of the Effectiveness of The Sleuth Kit and Autopsy Forensic Browser. Yüksek Lisans Tezi, University of Otago.

FOGEL, K., (2010), Technical Infrastructure *In: Producing Open Source Software, How to Run a Successful Free Software Project,* Ed.: K. FOGEL, ShareAlike, p.: 29-56

Foremost, Erişim: [foremost.sourceforge.net]. Erişim Tarihi: 22.02.2011

GALVAO, R.K.M., (2006), Computer Forensics with The Sleuth Kit and The Autopsy Forensic Browser, The International Journal of Forensic Computer Science, 1:41-44

GARFINKEL, S.L., (2006), AFF: A New Format for Storing Hard Drive Images Erişim: [http://repo.meh.or.id/Forensic/AFF%20-%20A%20New%20Format%20for%20Storing%20Hard%20Drive%20Images.pdf]. Erişim Tarihi: 05.05.2012

GARFINKEL, S.L., (2007), Carving contiguous and fragmented files with fast object validation, Digital Investigation, **4**:2-12

GARZA, D. ve ark., (2010), Data Acquisition and Duplication *In: Computer Forensics Investigating Data & Image Files*, Ed.: D. GARZA, NY.: EC-Council, p.: 65-94

Guymager Homepage, Erişim: [guymager.sourceforge.net]. Erişim Tarihi: 26.02.2011

HANCI, İH, TUĞ, A, ÖĞÜNÇ, G, SERTÇE, S, DURGUN, S., (2002) Olay Yeri İncelemesi-Delillerin Toplanması ve Laboratuvara Gönderilmesi. İçinde: HANCI İ.H.

(Eds): Adli Tıp ve Adli Bilimler, Seçkin Yayıncılık San ve Tic. A.Ş. Ankara; s.: 463-489.

HURLBUT, D., (2005), Write Protect USB Devices in Windows XP, Erişim: [http://accessdata.com/media/en_us/print/papers/wp.USB_Write_Protect.en_us.pdf]. Erişim Tarihi: 26.02.2012

JANSEN, W., AYERS, R, (2007), Appendix B. Glossary *In: Guidelines on Cell Phone Forensics:Recommendations of the National Institute of Standards and Technology,* Ed.: W. JANSEN, Gaithersburg: NIST Special Publication 800-101, p.: 81-92

JONES, K.J., BEJTLICJ, R., ROSE, C.W. (2006). Forensic Analysis Techniques. *In: Real Digital Forensics: Computer Security And Incident Response*, Eds.: K.J. JONES, R. BEJTLICJ, C.W. ROSE, NJ: Addison Wesley Professional, p.:205-246.

KLOET, S.J.J., (2007), Measuring and Improving the Quality of File Carving Methods. Yüksek lisans tezi, Eindhoven University of Technology Department of Mathematics and Computer Science, Danışman: Prof. Dr. W.J. Fokkink.

KORNBLUM, J.D., (2004), The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors In: International Journal of Digital Evidence Journal, **3**(2)

KÖHN, M., ELOFF, J.H.P., OLIVIER, M.S., (2008), UML Modeling of Digital Forensic Process Models (DFPMs), Proceedings of the ISSA 2008 Innovative Minds Konferansı, Johannesburg, South Africa, July 2008, p.:1-13

Md5deep and Hashdeep, Erişim: [md5deep.sourceforge.net]. Erişim Tarihi: 20.02.2011

Md5sum, Erişim: [manpages.ubuntu.com/manpages/natty/en/man1/md5sum.1.html]. Erişim Tarihi: 01.02.2013

MENZ, M., BRESS, S., (2004), The Fallacy of Software Write Protection in Computer Forensics, , MyKey Tech. Inc., Erişim: [http://www.mykeytech.com/SoftwareWriteBlocking2-4.pdf]. Erişim Tarihi: 26.02.2012

MOHAY, G., ANDERSON, A., COLLIE, B., DE VEL, O., McKEMMISH, R., 2003, Current Practice *In: Computer and Intrusion Forensics,* Norwood, MA, Artech House Inc., p.: 41-112

Open Source Digital Forensics, Erişim: [www2.opensourceforensics.org/tools/unix]. Erişim Tarihi: 26.02.2011

ÖZDAMAR, K., (2002), Paket Programlar ile İstatistiksel Veri Analizi 1, Eskişehir, Kaan Kitabevi

PAL, A., MEMON, N., (2009), The evolution of file carving, Signal Processing Magazine, IEEE, **26**(2): 59-71

PARTINGTON, T., (2007) Computer Forensics: Final Report; Erişim: [http://www.dcs.shef.ac.uk/intranet/teaching/projects/archive/ug2007/pdf/aca04tp.pdfz Erişim Tarihi: 26.02.2012

Paul Yves Flag, Erişim: [pyflag.net/cgi-bin/moin.cgi]. Erişim Tarihi: 26.02.2011

PhotoRec, Erişim: [cgsecurity.org/wiki/PhotoRec]. Erişim Tarihi: 20.02.2011

RAGHUNATHAN, S., PRASAD, A., MISHRA, B.K., CHANG, H., (2005), Open Source Versus Closed Source: Software Quality in Monopoly and Competitive Markets, IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, **35(**6): 903-918

REYES, A., WILES, J., (2007), Acquiring Data, Duplicating Data and Recovering Deleted Files In: Best Damn Cybercrime and Digital Forensics Ebook Period, Ed.: A. WILLIAMS, Burlington: Syngress Publishing, Inc., p.:333-392

RUIBIN, G., YUN, C.K., (2005), Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, **4**(1):1-13

Scalpel, Erişim: [https://viaforensics.com/computer-forensic-ediscovery-glossary/what-is-scalpel.html]. Erişim Tarihi: 01.02.2013

SINDHU, K.K., MESHRAM, B.B., (2012), Digital Forensic Investigation Tools and Procedures, In: International *Journal of Computer Network and Information Security,* **4**:39-48

Strings, Erişim: [forensicswiki.org/wiki/Strings]. Erişim Tarihi: 01.02.2013

ŞİRİKÇİ, A.S., CANTÜRK, N., ‘‘Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi’’ Bilişim Teknolojileri Dergisi, **5**(3): 29-34 (2012).

TestDisk, Erişim: [cgsecurity.org/wiki/TestDisk]. Erişim Tarihi: 20.02.2011

The Sleuth Kit, Erişim: [sleuthkit.org/autopsy]. Erişim Tarihi: 26.02.2011

TUĞ, E., CANTÜRK, N., ‘‘İnternet üzerinden çocukların cinsel istismarı sorunu ve önleme yolları’’ Türkiye Klinikleri Adli Tıp Dergisi, Adli Tıpta Güncel Gelişmeler Özel Sayısı, **9**(2):74-79, (2012)

What is Ophcrack, Erişim: [ophcrack.sourceforge.net]. Erişim Tarihi: 01.02.2013

WINTER, R., (2013), SSD vs HDD – data recovery and destruction, Network Security, **2013(**3): 12–14

VACCA, J.R., (2005), Summary, Conclusion and Recommendations *In: Computer Forensics Computer Crime Investigation,* Boston, Charles River Media, p.: 673-704

YANG, C., YEN, P., (2010), Fast Deployment of Computer Forensics with USBs, International Conference on Broadband, Wireless Computing, Communication and Applications, Erişim:

[http://www.computer.org/csdl/proceedings/bwcca/2010/4236/00/4236a413-abs.html]. Erişim Tarihi: 05.05.2012

YEN, Y., LIN, I., CHANG, A., (2012), A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime, *In: International Journal of Computer Engineering Science*, **2**(3): 26-39

ÖZGEÇMİŞ

Bireysel Bilgiler

Adı	: Ahmet Serhat
Soyadı	: ŞİRİKÇİ
Doğum yeri ve tarihi	: İzmir-1980
Uyruğu	: T.C.
Medeni durumu	: Evli
Askerlik durumu	: -
İletişim adresi ve telefonu	:Jandarma Kriminal Daire Başkanlığı Beytepe/Ankara 312 464 72 50

Eğitimi (tarih sırasına göre yeniden eskiye doğru)

- Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Disiplinlerarası Adli Bilimler Ana Bilim Dalı Fiziki İncelemeler ve Kriminalistik Yüksek Lisans Programı (2009-)
- Jandarma Subay Okulu (2002-2003/Ankara)
- Kara Harp Okulu (1998-2002/Ankara)
- Işıklar Askeri Lisesi (1994-1998/Bursa)
- İbrahim Kavur İlköğretim Okulu (1986-1994/İzmir)

Yabancı dili: İngilizce

Ünvanları : Yoktur

Mesleki Deneyimi

- Jandarma Kriminal Daire Başkanlığı Bilişim Teknolojileri İnceleme Şube Müdürlüğü Veri İnc.Ks.A.liği

Üye Olduğu Bilimsel Kuruluşlar: Yoktur

Bilimsel İlgi Alanları: Adli Bilişim

Yayınları : ŞİRİKÇİ A.S., CANTURK N., ‘‘The Importance of Creating a Byte-to-byte Copy (Imaging) at Computer Forensics Investigations- Case Report,’’ *22nd Congress of the International Academy of Legal Medicine*, Poster Presentation, Book of Abstract: 288, İstanbul, Turkey, 5-8 July 2012.

ŞİRİKÇİ A.S., CANTÜRK N. ‘‘Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi’’ Bilişim Teknolojileri Dergisi, 5 (3): 29-34 (2012).

Bilimsel Etkinlikleri: Siber Terörizm Kursu (2006-Ankara), Bilişim Güvenliği Kursu (2008-Ankara), Encase Adli Bilişim Yazılımı Kursu (2008-İngiltere), .XRY Mobil Cihaz İnceleme Kursu (2008-İngiltere), Encase İleri Seviye İnceleme Kursu (2009-İngiltere), ENFSI Bilişim Teknolojileri Çalışma Grubu Toplantıları (2008-Almanya, , 2009-İspanya, 2010-Rusya, 2011-İtalya(Ses Alanında)), Jandarma Okullar Komutanlığı Bilişim Seminerinde “Bilişim Suçlarında Delil Toplama ve Delillerin Analizi” isimli Bilimsel Sunu (2011-Ankara)

Diğer Bilgiler: -