VERİ KURTARMA YÖNTEMLERİNİN BAŞARIMLARININ DEĞERLENDİRİLMESİ

Şahin KARA

Yüksek Lisans Tezi
Elektronik ve Bilgisayar Eğitimi Anabilim Dalı
Danışman: Yrd. Doç. Dr. Resul DAŞ
OCAK-2013

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VERİ KURTARMA YÖNTEMLERİNİN BAŞARIMLARININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Şahin KARA

(Enstitü No: 092131106)

Tezin Enstitüye Verildiği Tarih : 06 Aralık 2012

Tezin Savunulduğu Tarih : 20 Aralık 2012

Tez Danışmanı : Yrd. Doç. Dr. Resul DAŞ (F.Ü)

Diğer Jüri Üyeleri : Doç. Dr. İbrahim TÜRKOĞLU (F.Ü)

Yrd. Doç. Dr. Ömür AYDOĞMUŞ (F.Ü)

OCAK-2013

TEŞEKKÜR

Çalışmalarım süresince hem mesleğine hem de hayata yaklaşımıyla bizlere örnek olan, değerli bilgisini ve deneyimlerini bizlerle paylaşan yardım ve katkılarıyla beni yönlendiren danışman hocam Yrd. Doç. Dr. Resul DAŞ'a, bilgi ve tecrübeleriyle tezime katkı sağlayan bölüm hocam Doç. Dr. İbrahim TÜRKOĞLU'na, tezimin olgunlaşmasına teknik destek sağlayan MYDISK veri kurtarma firmasına, tez süresince sabır gösterip manevi destekleriyle hep yanımda olan aileme ve çalışmalarım esnasında fikir ve destekleri ile beni yalnız bırakmayan arkadaşlarıma teşekkürü bir borç bilirim.

Şahin KARA

İÇİNDEKİLER

Sayfa No

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR LİSTESİ

FAT : File Allocation Table
NTFS : New Technology File System
EXT2FS : Second Extended File System
NIST : The National Institute of Standards and Technology
PCMCIA : Personal Computer Memory Card International Association
MFT : Master File Table
ACL : Access Control List
BT : Bilişim Teknolojisi
IDC : International Data Corporation
EM : Elektromanyetik dalga
MR : Magnetorezistif
SMART : Self Monitoring Analysis Reporting Technology
PFA : Predictive Failure Analysis - Olası Bozukluklar Analizi
SPS : Shock Protection System
DPS : Disc Protection System
SAN : Storage Area Network
NAS : Network Attached Storage
DNS : Domain Name System
DHCP : Dynamic Host Configuration Protocol
RAID : Redundant Array of Inexpensive Disks
FDRE : Flash Disk Data Recovery Equipment
PCB : Printed Circuit Board
HFS/HFS+ : Hierarchical File System(Mac)
UFS1/UFS2 : Unix File System
SQL : Structured Query Language
SSD : Solid-State Disk

ÖZET

Yaşadığımız çağ bilgi çağıdır. Bilgi çağının temelinde ise verilerin işlenmesi ve saklanması esasına dayanan bilgi teknolojileri yer almaktadır. Bilgisayar insan hayatının her alanına girmesiyle bilgi teknolojilerinin paralelinde bilginin artmasına neden olmuştur. İşleri kolaylaştırmak adına bilgisayarlar hangi alanda kullanılacaksa, o alana dair bilgilerin bilgisayarlara yüklenmesi ihtiyacı doğmuştur. Kişisel bilgisayarların ve mobil bilişim teknolojisinin olanca hızıyla yaygınlaşmasının yanında farklı ölçekte bilgisayar ağları ve dünya çapında internet göz önüne alındığında elektronik ortama aktarılan bilginin miktarı çok yüksek boyutlara ulaşmış ve bu durum artarak devam etmektedir. Bu kadar yüksek boyutlardaki bilgilerin saklanması ve kullanılabilmesi için veri depolama ortamlarına ihtiyaç vardır. Bu amaçla çok çeşitli veri depolama aygıtları geliştirilmiştir. Büyük veri bankalarından, küçük flash belleklere kadar kurumsal veya kişisel ihtiyaca göre çeşitli kapasitelerde depolama araçları geliştirilmiştir. Verilerin bu depolama araçlarında saklanması, beraberinde bir takım riskleri de getirmektedir. Ancak geliştirilen veri koruma teknolojileri ve kurtarma araçlarıyla bu risklerin düşürülmesi sağlanmaktadır. Bu tez çalışmasında, çeşitli nedenlerle hasara uğramış, silinmiş veya kaybolmuş verilerin depolama ortamlarından kurtarılması ile ilgili kullanılan yöntemlerin analizleri yapılmıştır. Elde edilen uygulama sonuçları neticesinde, veri kurtarma metotlarının birbirine kıyasla başarımları ortaya konulmuştur.

Anahtar Kelimeler: Veri kurtarma, Bilgi güvenliği, Bilgisayar güvenliği, Adli bilişim.

ABSTRACT

The period we live is knowledge era. The basic of this era is the information technology which bases on the storing and processing. Now computer is all around the life. In the name of make the things esaier we need to load the datas to the computer in which area we use. Because of the fact that proliferation of personal computers and mobil information technology with worldwide internet and computer network the amount of information which transferred to electronic environment is on the very high level and incresingly continue so we need to data gathering system for storing and using datas. For this reason different storage devices have been enhanced. Modern techonology presents us too many advantages to make our life more comfortable andreduce work-time. On the other hand the storage of datas in digital environment have some risks. It is imposible to say there is no risk for any technology and protection method. But with the help of data protection techonology and rescue vehicle we aim to decrease. In this dissertation we focused on to save damaged,deleted, and mislaid datas from the storage medium and the methods we used.finally we examined the results and success.

Keywords: Data recovery, Information security, Computer forensics.

1. GİRİŞ

Bilgi çizim, resim, metin, fotoğraf, video vb gibi birçok farklı şekilde dijital ortamlarda yer almaktadır. Bilgi için önemli olan husus bilginin kaydedilebilir, görülebilir, tekrar tekrar elde edilebilir, gözlenebilir ve yorumlanabilir bir şekilde olmasıdır. Bir bilginin değerli olması için odaklanmış, test edilmiş, gerçeklenmiş ve paylaşılmış olması, girdi ve çıktılarının basit olması, güncellenebilmesi gereklidir[1].

Kişi, kurum ve kuruluşlar açısından bilgi güvenliği büyük önem kazanmaktadır. Bu bağlamda bilginin izinsiz erişimi ve kullanımı, ifşa edilmesi, yok edilmesi, değiştirilmesi ve hasar verilmesi hayati öneme sahiptir. Değerli verilerin kaybolmasının faturası çok ağır olabilir. Gerekli bütün tedbirler alınmasına rağmen istenmeyen durumlarla karşılaşmak mümkündür. Bu nedenle verinin bulunduğu ortamdaki güvenliğinin, bütünlüğünün ve gizliliğinin sağlanması için doğru yedeklemek gereklidir. Sorun oluştuğu durumlarda geri getirebilmek için gerekli yedekleme sistemlerinin ve geri dönüş prosedürlerinin oluşturulması gerekir.

1.1. Tez Çalışmasının Amacı

Dünyada ve ülkemizde zarar görmüş veri depolama ortamlarındaki verilerin kurtarılması konusunda, ticari firmaların kullandıkları araç ve yöntemler ticari rekabetten dolayı, gizli tutulmaktadır. Bu durum bu alandaki çalışmaları zorlaştırmaktadır. Ancak veri kurtarmanın hem teorik yönü, hem de fiilen yapılan kurtarma çalışmalarının çoğu son kullanıcılar için bile anlaşılabilir durumdadır. Bu çalışmada, zarar görmüş veri depolama aygıtlarından veri kurtarırken doğru kararlar verip uygun yöntemleri seçebilmek için kurtarma yöntemlerinin başarımlarının analizi yapılmıştır. Böylece veri kurtarmada veri kayıplarının en aza düşürülmesi amaçlanmaktadır. Ayrıca veri koruma ve kurtarma yöntemleri ile bu alanda kullanılan yazılımsal ve donanımsal yöntemlerin başarımları incelenmiştir.

1.2. Tez Çalışmasının Kapsamı

2. bölümde, sayısal verilerle ilgili temel bilgiler açıklanmıştır. Veri türleri, sayısal veri saklama ortamlarının özellikleri ve sayısal veri saklama ortamlarının dosya sistemleri incelenmiştir. Veri kaybının yazılımsal ve donanımsal nedenleri ile bilgi teknolojilerindeki güvenlik zafiyetleri ve açıkları üzerinde durulmuştur. 3. bölümde, sayısal veri koruma teknolojileri ve veri kurtarma yöntemleri incelenmiştir. Sayısal veri kurtarmada ve adli

bilişimde yaygın olarak kullanılan veri kurtarma yazılımları incelenip karşılaştırmaları yapılmıştır. 4. bölümde, sayısal ortamlardan veri kurtarma uygulamaları olarak fiziksel hasarlı ve biçimlendirilmiş sabit diskler ile fiziksel hasarlı flash belleklerden veri kurtarma uygulamaları ve alınan sonuçları açıklanmıştır. 5. bölümde ise tez çalışmasının genel sonuçların üzerinde değerlendirmeler belirtilmiştir ve öneriler yapılmıştır.

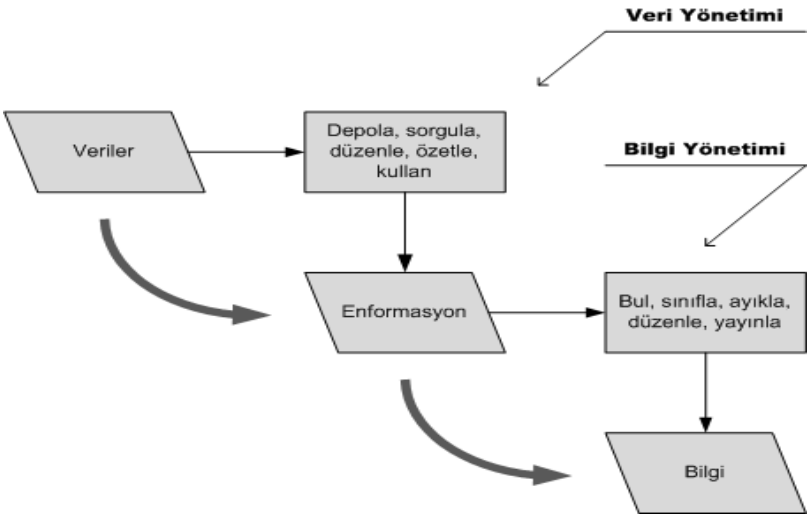
2. SAYISAL VERİLER İLE İLGİLİ TEMEL BİLGİLER

2.1. Giriş

Bilgisayar ve iletişim dünyasında yaşanan gelişmelerin yanı sıra internetin kurumsal ve kişisel düzeyde kullanımının da gün geçtikçe artması, beraberinde terminolojik açıdan çok sık karıştırılan kavramların farklı yerlerde, farklı anlamlarda kullanımına yol açmıştır. Günümüzde veri, bilgi, bilişim gibi bu kavramlar çok farklı kategorilere ayrılmakta, çeşitli gruplar altında değerlendirilmektedir. Bunların başında en çok kullanılmakta olan ve bilginin kendisini ifade etmek için kullanılan veri (data) kavramı gelmektedir.

2.2. Veri Ve Veri Türleri

Veri kavramı, çeşitli durumların, gözlemlerin veya oluşumların her türlü gösterimidir. Bu gösterimler sayısal, alfa nümerik karakterler veya semboller olacağı gibi çeşitli biçimlerdeki diğer tüm grafik gösterimler şeklinde de olabilir. Veri, miktarları, eylemleri, olguları vb. temsil eden tesadüfî olmayan rast gele bir araya gelmemiş bulunan sembollerden oluşan bir grup olarak da tanımlanır. Veri genellikle analiz edilebilecek ya da daha ileri işlemler için kullanılabilecek ham bilgi olarak bilinmektedir. Bilişim teknolojisi açısından veri, bir durum hakkında birbiriyle henüz bağlantısı kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller veya bit dizeleri olarak tanımlanmaktadır[2]. Veriler şekil 1'de gösterilen bilgi işlem sürecinde çeşitli analiz, sınıflama ve hesaplama yöntemleri ile gerçek bilgi haline gelir.



Şekil 1. Veri ve bilgi ilişkisi

2.3. Veri Kurtarma

Herhangi bir şekilde erişilemez hale gelmiş, silinmiş, bozulmuş ya da kaybolmuş ve normal yol ve yöntemlerle ulaşılamayan verilerin özel yöntemlerle geri getirilmesi olayı "Veri Kurtarma" kavramı ile ifade edilmektedir[3]. Bilgisayar sistemlerinde verileri depolamak için kullanılan ortamlarda veriler dosya adı verilen bağımsız bütünler şeklinde tutulmaktadır. Bu dosyaları gruplamak için ise klasör (veya dizin) adı verilen yapılar kullanılmaktadır. Verilerimizin bulunduğu dosyalar herhangi bir şekilde (silinme, diskin yeniden biçimlenmesi, diskteki dosya takip yapısının bozulması, dosyadaki dahili yapının bozulması, veri depolama ortamının fiziksel olarak bozulması vb.) erişilemez hale geldiğinde veri kurtarma konusu gündeme gelmektedir. Veri kurtarma sadece kayıp dosyaları geri getirmek değil aynı zamanda bozulmuş verileri de kurtarmaktır. Veri kaybının temelinde yazılımsal veya donanımsal nedenler olduğundan veri kurtarmanın da yazılımsal ve donanımsal yöntemleri bulunmaktadır. Veri kurtarma işi profesyonel bilgi birikimi, deneyim ve yazılım tabanlı bir altyapı gerektiren nitelikli bir işlem ve süreçtir. Veri depolama ortamlarının fiziksel olarak hasar görmesi durumunda, yedek parça, özel cihazlar ve özel temiz ortam gerekebilmektedir. Mantıksal yapı hasarlarında, yeniden bölümleme ve formatlamalarda ve silinmelerde ise çoğu zaman ancak birim veri alanı yani sektör tabanlı detaylı ve uzun çalışmalarla veriler gerçekçi ve doğru bir şekilde elde edilebilmektedir.

2.4. Veri Kurtarma Kapsamı

Karşılaşılan veri kayıplarında yapılabilecek kurtarma çalışmaları; dosya sistemleri hasarlarında, biçimlendirme ve silinmelerde, dosyalarda dahili bozulmalarda ve fiziksel hasarlarda veri kurtarma şeklinde sıralanmaktadır.

2.4.1. Dosya Sistemi Hasarları

Bilgisayar sistemlerinde kullanılan veri depolama ortamları, kullanılmadan önce veri ve program dosyalarının düzenli bir şekilde kaydedilmesi ve takip edilebilmesi için dosya sistemi adı verilen ve yaygın olarak FAT, NTFS, Ext2FS, kısaltmalarıyla bilinen yapılar ile düzenlenmektedir. Veri depolama ortamlarının organizasyon yapısında genellikle sistem alanı ve veri alanı olarak tarif edilen iki ana kısım bulunmaktadır. Sistem alanı genel hatlarıyla sistem açılış yapısını, dosya tanımlarını ve dosyaların veri alanındaki yer adreslerini içerir. Veri alanı, dosyaları ve alt tanımlama gruplarını içerir. Dosyalara erişebilme noktasında sistem alanındaki tanım ve adresler kolaylıkla tahmin edileceği

üzere hayati öneme sahiptir. Bu yapılar silindiğinde veya hasar gördüğünde veri depolama ortamındaki klasör ve dosyalara standart işletim sistemi araçlarıyla erişmek mümkün olmaz[4]. Eğer veri alanında depolanmış olan dosyalar hasar görmemiş ve sadece sistem alanı hasar görmüşse sistem alanını onarmak çoğu zaman veri depolama ortamındaki mantıksal düzenlemenin eski orijinal haline geri gelmesi anlamına gelir. Bu çerçevede öncelikli olarak sistem alanını kontrol etmek ve hasar buradaysa bu hasarı giderip sistemi eski orijinal haline geri getirmek ilk hedef olmalıdır.

2.4.2. Biçimlendirme ve Silinmeler

Veri depolama ortamındaki dosyaları takip etmeye yarayan yapı yok olduğunda veya dosyalara erişmeyi sağlayamayacak düzeyde hasar gördüğünde dosyaları kurtarmak çoğu zaman kapsamlı ve nitelikli bir çalışma gerektirir. Dosyalara ait iki temel bilgi vardır. Birincisi dosyanın adını, özelliklerini ve başlangıç yerini içeren tanımlama bilgisidir. İkincisi ise eğer dosya birden fazla kümeye yerleştirilecek şekilde büyüklüğe sahipse veri alanında yerleştirildiği küme yer bilgileri ile oluşturulan küme zinciri bilgisidir. Manyetik veri depolama ortamları genellikle random mantıkla esnek olarak kullanılmaktadır. Bu ise dosyalara ait kümelerin veri alanında ardışık olmayan bir şekilde yerleştirilmesini gerektirir ve böylece dosyalar küme bazlı parçalanmış olur. Dosyaya ait küme zinciri mevcut olmadığında hangi kümelerin hangi dosyaya ait olduğuna otomatik olarak karar vermek çoğu zaman imkansız hale gelir. Dosyaya ait tanım bilgisinin olmaması durumunda ise ancak dosya başlangıcındaki dosya başlığı (header) ile bir tahminde bulunmak söz konusu olur.

2.4.3. Dosyalarda Dahili Bozulmalar

Pek çok kullanıcı özellikle Word ve Excel programlarına ait dosyalarının açılmaması problemini yaşamıştır. Bu olay gerçekte veri tutulan tüm dosyaların ve veri tabanı sistemlerinin başına gelmektedir. Dosyanın bulunduğu ortamda kısmi fiziksel hasar olduğunda da benzer bir durum yaşanır. Sıkıştırılmış dosyalar ve yedekleme sistemlerinde de benzer tablolar ortaya çıkmaktadır. Bu konunun kapsamında, veri kurtarma sonrasında kısmi olarak kurtarılabilmiş dosyaların onarılıp işe yarar hale getirilmesi konusu da vardır.

2.4.4. Fiziksel Hasarlar

Elektronik kart arızaları, manyetik yüzey hasarları (servo işaret bozulmaları, servis alanı hasarları, veri alanı hasarları), manyetik okuma/yazma kafa yada kafa bloğu hasarları (konumlandırıcı magnet, yükseltici devre, okuma/yazma kafaları), motor hasarları ve bu

hasarların kombine şekilleri olarak düşünülebilir. Manyetik yüzey hasarları dışındaki hasarlarda çözüm üretmek büyük oranda eşdeğer disk olmasına bağlıdır. Eşdeğer disk olmaması durumunda veri kurtarma işleminin yapılması neredeyse imkansız gibidir. Bu nedenle dünyanın önde gelen veri kurtarma firmaları on binlerce diskten oluşan disk arşivlerine sahiptirler ve her yeni çıkan disk serisi ile bu arşiv genişletilmektedir. Bu ise ciddi parasal yatırım gerektirmektedir.

Disk gövdesinin açılması ve parça değişimleri parça haricinde hem konu ile ilgili bilgi hem de deneyim gerektirmektedir. Abartıldığı kadar olmasa da belli standartlarda temiz oda ve işaret algılama ve test cihaz ve yazılımları ve parça değişim alet ve aparatları gerektirmektedir. Disklerde fiziksel hasarlarda hasarların genellikle kombine şekilde oluştuğunu ifade etmekte yarar var. Yani diskte her şey sağlam, sadece kafanın bozuk olduğunun ortaya çıkma ihtimali %5'ten azdır. Normal servis ortamındaki parça değişimlerinde hem değiştirilen parçaların (genellikle kafa bloğu değiştirilir) hem de veri plakasının ekstra zarar görme ihtimali genellikle yüksektir. Fiziksel hasarlar büyük oranda olumsuz ortam şartlarına ve kullanıcı hatalarına dayanmaktadır. Üretim hatası nedeniyle bozulma çok ender yaşanan bir durumdur. Bu nedenlerle disk üreticileri böyle bir sorumluluk taşımak durumunda değildirler. Fiziksel hasarlar nedeniyle garanti kapsamında geri dönen disk oranı da genel istatistiklere göre binde üçten fazla değildir. Bu diskler de eş kapasite ya da o anki cari model ile değiştirilmektedir.

2.5. Veri Kurtarma İlkesi

Veri kurtarma, kaybolan veya silinen verilerin bulunma ve kurtarılması sürecidir. Bu süreç, içinde bazı riskler barındırmakla birlikte her zaman istenen sonuç gerçekleşmeyebilir ve beklenmedik durumlarla karşılaşılabilir. Bazen kurtarılmak istenen veriler tamamen erişilemez hale getirilebilir. Bu riskleri ez aza indirmek için mümkünse yedekler alınmalı ve verilerin kurtarılacağı cihaza bir şey yazılmamalıdır. Veri kaybı nedeninin iyice tespit edilip en uygun kurtarma yöntemi seçilmelidir.

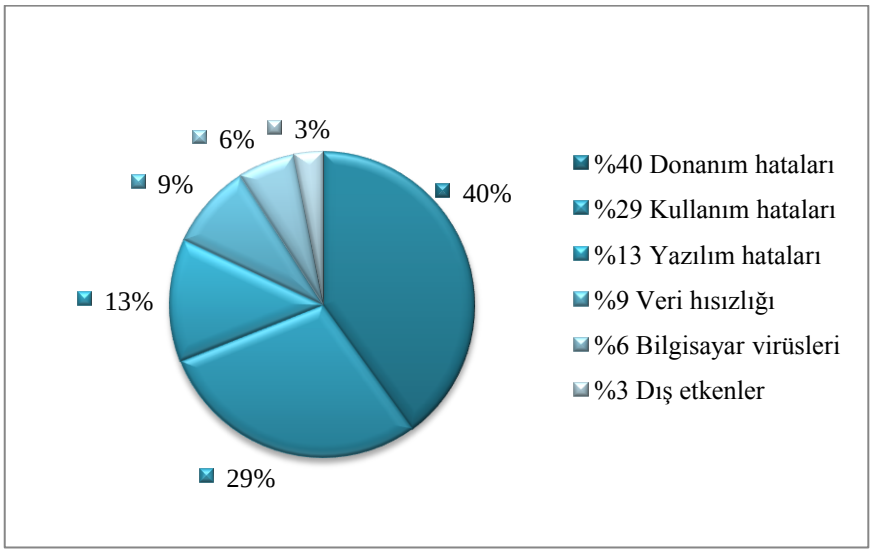
2.6. Veri Kaybının Oluşma Nedenleri

Günümüzde hem kişiler hem de kurum ve işletmeler verilerini büyük oranda bilgisayar sistemlerinde işlemekte ve saklamaktadır. Bu veriler bilgisayar sistemlerinde genellikle sabit diskler, CD ve DVD, flash bellek gibi manyetik, optik veya bellek kartı tabanlı ortamlarda depolanmaktadır. Depolanan bu verilerin normal yollarla erişilemez hale gelmesi veri kaybı olarak değerlendirilmektedir. Veri kaybı nedenleri ve türleri şu şekilde

sıralanabilir: Birinci neden; veri depolama ortamında verilerin düzenli ve dosyalar şeklinde yerleştirilmesine ve ihtiyaç duyulduğunda erişilmesine yarayan mantıksal düzenlemelerin (dosya sistemi) silinmesi veya hasar görmesidir. İkinci neden; veri depolama ortamındaki yapının yeniden oluşturulması (biçimlendirme) veya dosyaların silinmesi, ham veya belirli formatlara sahip dosyalarda (veri tabanı dosyaları, belgeler) dahili bozulmaların oluşmasıdır. Üçüncü neden de veri depolama ortamının fiziksel olarak bozulması ya da hasar görmesi, şeklinde özetlenebilir.

2.6.1. Yazılımsal Nedenler

İşletim sisteminin veya kullanılan programların çökmesi, virüs ve zararlı yazılımların bulaşması, yanlışlıkla verilerin kalıcı olarak silinmesi, silinmiş verinin üstüne yeniden yazılması, kullanım hataları ile biçimlendirme, bölümlendirme gibi disk uygulamaları veri kaybının yazılımsal nedenleridir. Ontract Data International'ın 2003'te yaptığı araştırmalarda Şekil 2'de görüldüğü gibi veri kayıp nedenlerinin %13'ünü yazılımsal nedenler, %6'sını bilgisayar virüsleri oluşturmaktadır.[5]



Şekil 2. Veri Kaybı İstatistiği

2.6.2. Donanımsal Nedenler

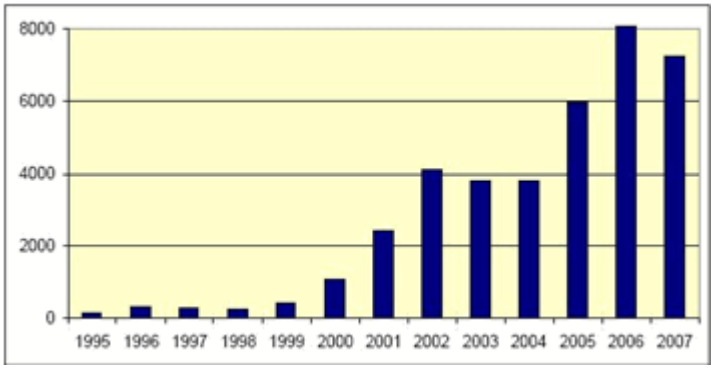
Veri kaybının genel fiziksel nedenleri arasında güç kaybı veya elektrik kesintisi, aşırı ısınma, üretim hatası, fiziksel kullanıcı hasarları (sabotaj,düşme, darbe), doğal felaketler (sel, yangın, deprem vb.), kullanım hatası ya da ihmal, mekanik arızalar, cihazın üzerine dökülen sıvı maddeler, tozlu ortamlar, elektrostatik ("statik") deşarj ve depolama

cihazından veya ortamdan kaynaklanan her türlü fiziksel hasar sayılabilir. Veri kaybının %40 oranında donanım kaynaklı olduğu şekil-2'de görülmektedir.

2.6.3. Bilgi Teknolojilerinde Güvenlik Zafiyetleri Ve Açıkları

The National Institute of Standards and Technology (NIST) güvenlik açığını; kötü niyetli bir kişinin politikaları bozmak amacıyla istismar edebileceği yazılım zayıflığı olarak tanımlar[6]. Örnek vermek gerekirse; kötü niyetli bir kullanıcı, bir açığı bir bilgisayar veya ağdaki erişim ve/veya izin yetkilerini genişletecek şekilde kullanabilir. Gartner açık tanımını insanlar ve süreçler açısından biraz daha genişleterek güvenlik açığını, bir teknoloji, süreç veya yönetimde BT güvenliğini tehlikeye atmak için kullanılabilecek zayıflık olarak tanımlar[7]. Günlük iş süreçlerinin elektronik ortamlara taşınması, manyetik ortamdaki bilgilerin paylaşılması, e-devlet uygulamaları gibi önem arz eden konular yaygınlaşmaktadır. Bu sebeple, bu sistemlerin bilişim ağ güvenliğinin gerekliliği ve önemi son derece önemlidir. Bu bağlamda olası tehdit ve tehlikelerin araştırılıp, bunlara karşı gerekli önlemlerin alınması, bilgi, bilgisayar ve bilgisayar ağ güvenliğinin sağlanması açısından büyük önem kazandığı görülmektedir[8]. Internet kullanıcılarına ait özel bilgilerin önemli olması ve gizliliğinin (internet bankacılığı, e-ticaret, kredi kartı bilgileri,vb) ön plana çıkması ile internet'te sunulan bilgilerdeki mahremiyete karşı katı kuralların artmasına sebep olmuştur. Bu nedenle Web kullanım madenciliğinin çok daha fazla etkin, verimli ve güncel kullanılması Internet ortamına büyük kazanımlar sağlayacaktır[9]. Hangi perspektiften bakılırsa bakılsın yazılımdaki bu kusurlar kötü niyetli bir kullanıcı tarafından teknolojileri kötüye kullanmak, BT ve iş süreçlerini çalmak, değiştirmek veya aksatmak için kullanılabilir ve bu durum firma için zaman, para ve güven kaybı demektir. İşletmeler, yasal düzenlemeler nedeniyle, işletmeler düzenli ve bağımsız denetimlerin yapılmasını, güvenlik standartlarına uyumluluğun denetlevmesini, ağların güvenliği için bir gereklilik olduğunu fark etmeye başlamışlardır. Başarılı ağ güvenlik yönetimi için, hem bilgi işlem sistemlerinin alt yapılarındaki, hem de web uygulamalarındaki açıkların belirlenebilmesi gereklidir. IDC'nin Türkiye için 2010 yılı araştırmasında BT yöneticilerinin gündemindeki ilk konunun BT sistem ve teknolojilerinin güvenliğinin sağlanması olduğu tespit edilmiştir. Bu araştırmaya göre telekom şirketleri, bankacılık ve resmi kurumlar başta olmak üzere 2008'den bu yana her yıl güvenlik harcamaları %10 artmış durumdadır. Aynı araştırmada en önemli üç güvenlik riski; Trojanlar, Spyware ve bilginin çalınması olarak sıralanmıştır. Özellikle şirket içindeki

çalışanların bilinçli olarak şirket bilgilerini dışarıya çıkartmaları, sızdırmaları en çok risk olarak görülmektedir. Ayrıca kullanıcıların farkında olmadan, bilmeden veri ve bilgi kaynaklarını kaybetmeleri, silmeleri de başka bir sorun olarak görülmektedir. Şekil 3'den görüldüğü gibi son yıllarda yazılımlarda görülen açıklıklar önemli oranda artmaktadır. Bu açıklıkların artma nedenlerinin başında internetin yaygın olarak kullanılması ve bilgisayarın iş uygulamaları da dâhil olmak üzere kullanım oranının çok artması gelmektedir. Diğer önemli sebep, yazılımların güvenliği dikkate alınmadan sadece fonksiyonellik göz önüne alınarak geliştirilmesidir. Bu durumda arkaplanda yazılımlar birçok açıklık içermektedir. Ayrıca, yazılımın ortaya çıkmasından sonra tespit edilen açıklıkların kapatılması için çok fazla iş gücü ve zaman harcanmasıdır. Çünkü bir güvenlik açıklığı yazılım geliştirme evresinde ne kadar erken tespit edilebilirse, o açıklığın kapatılması maliyeti o kadar az olacaktır [10].



Şekil 3. Yıllara göre açıklıklar

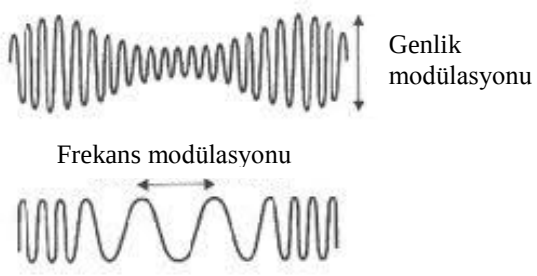
2.7. Sayısal Veri Saklama Ortamları ve Özellikleri

Sayısal veriler manyetik sabit disklerde, optik disklerde ve yarı iletken elektronik belleklerde saklanmaktadır. Bu veri kayıt ortamları kullanım amacı ve veri kayıt teknikleri açısından farklı özelliklere sahiptirler. Sabit diskler, CD/DVD'ler ve flash bellekler yaygın olarak kullanılan veri saklama ortamlarıdır.

2.7.1. Sabit Diskler

Sabit diskler dönen disklerden oluşan cihazlardır. Bu disklerin yüzeyi manyetik özelliğe sahiptir. Bilgisayar verisi olan 1 ve 0'lar manyetik olarak bu diskler üzerinde oluşturulur. Bir sabit disk sürücüsünün yazma/okuma kafası diskin yüzeyindeki elektronların manyetik olarak ne şekilde dizildiğini algılayarak verileri belirler. Tüm elektromanyetik dalgalar, ışık hızında hareket eder (yaklaşık olarak 300.000km/sn). Elektromanyetik dalgalar frekans cinsinden ölçülür. Frekans 1 saniyede üretilen dalga sayısıdır ve birimi Hertz

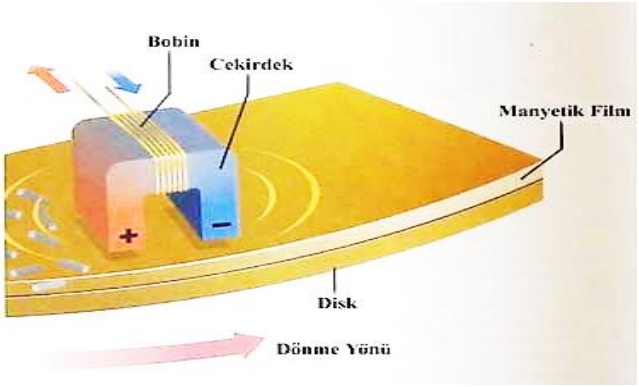
(Hz)'dır. Örneğin 1kHz'lik (kilohertz) bir elektromanyetik sinyal saniyede 1000 dalga üretir. Bir EM dalganın frekansı dalga boyuyla ters orantılıdır. Dalga boyu, bir sinyalin herhangi bir zamandan kendini tekrar etmeye başladığı zamana kadar geçen mesafedir. Sinyal frekansı yükseldikçe dalga boyu azalır. Örneğin FM radyo yayın bandında yer alan 100 MHz'lik bir sinyal yaklaşık 300 cm dalga boyundayken, 30 GHz'lik bir sinyal yaklaşık 1cm dalga boyundadır.



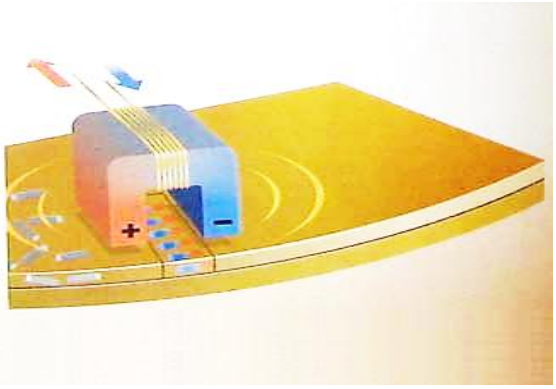
Şekil 4. Elektro manyetik bir dalganın değiştirilme (modülasyon) teknikleri

Elektromanyetik dalgalar veri taşımak için kullanılmak istendiğinde dalga biçiminde şekil 4'te görülen değişiklikler yapılır. Frekans modülasyonunda temel dalganın frekansı değiştirilerek veri iletilir. Genlik modülasyonunda ise temel dalganın genliği değiştirilerek veri iletimi gerçekleştirilir. Bir sinyal tarafından taşınabilen veri miktarı, onları meydana getiren elektromanyetik dalganın frekansıyla birlikte artar. Birim saniyede daha fazla değişim meydana gelmesi demek daha fazla veri iletimi anlamına gelir.

Disk üzerine herhangi bir veri yazılmadan önce demir parçacıkları, diskin yüzeyini kaplayan bir manyetik film üzerinde rastgele dağılmış durumda bulunur. Demir parçacıklarının veri olarak organize edilmesi için, şekil 5'te görüldüğü gibi diskin üzerinde askıda duran yazma/okuma kafasına sarılmış bir bobin telinin içinden elektrik akımı geçirilir.

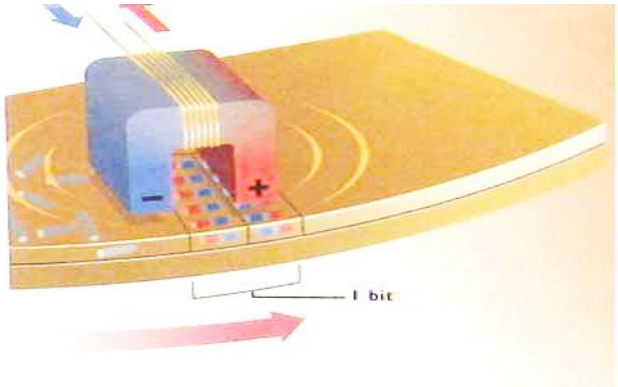


Şekil 5. Demir parçacıkları, manyetik film üzerinde rastgele dağılmıştır

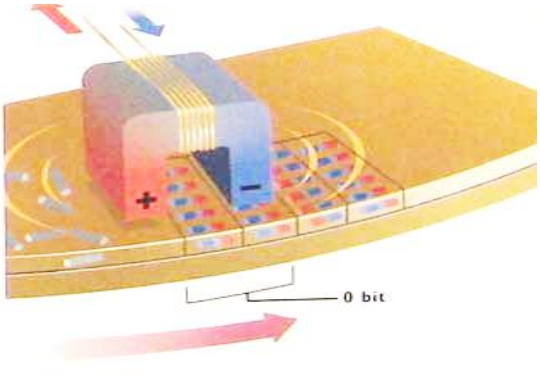


Şekil 6. Parçacıkları hizalamak için bobin telinden elektrik akımı geçirilir.

Demir parçacıkları manyetize edilir ve şekil 6'da görünen pozitif kutuplar yazma/okuma kafasının negatif kutbu etrafında, negatif kutuplar ise yazma/okuma kafasının pozitif kutbu etrafında toplanır. Manyetize olmuş parçacıklardan dönen disk üzerinde hizaya sokulmuş bir bant oluşturulduktan sonra ikinci bir bant oluşturulur. İki bant bilgisayar dünyasının en ufak verisini (1 bit) oluşturmaktadır. "1" verisini oluşturmak için bobin sargılarına uygulanan elektrik akımının yönü değiştirilir ve dolayısıyla yazma/okuma kafasının kutup başları yer değiştirir. Böylece şekil 7'deki ikinci banttaki parçacıklar zıt yönde hizaya girmiş olur. Şekil 8'de "0" verisini oluşturmak için her iki bandın parçacıkları aynı yönde hizaya getirilir.



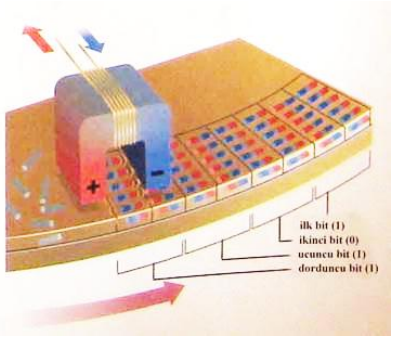
Şekil 7. "1" bilgisinin elde edilmesi



Şekil 8. "0" bilgisinin elde edilmesi

Veri okumak için yazma/okuma kafasına elektrik gönderilmez. Diskin kaplamasında yer alan manyetize olmuş parçacıkların her biri küçük bir mıknatıs olarak davranmaktadır ve manyetik alan oluşumuna neden olurlar. Yazma/okuma kafası manyetik alan içinden geçtikçe "1" ve 0" bilgilerini tutan bandların polaritelerine bağlı olarak kafanın bobin

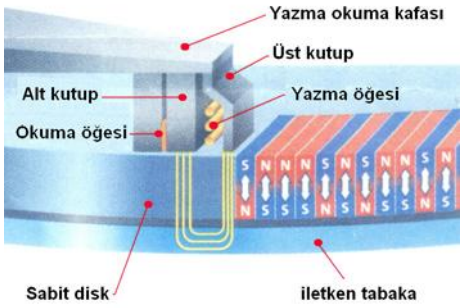
sargısında şekil 9'deki gibi değişen yönde akım oluşur. Akım yönünde meydana gelen değişimin bilgisayar tarafından algılanması sonucu "1" ve "0" bilgileri elde edilir.



Şekil 9. Manyetik disk üzerinde okuma işleminin gerçekleştirilmesi

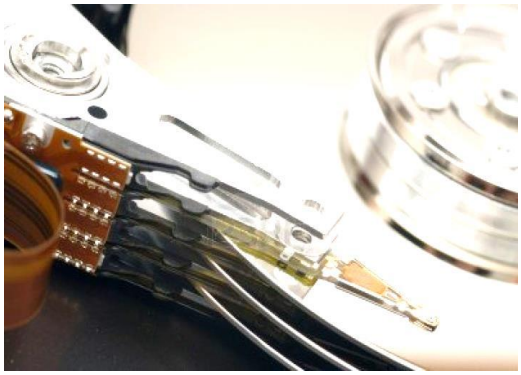
Yukarıda belirtilen kayıt işleminde, bilgilerin manyetik yüzey üzerinde yatay olarak oluşturulmasıdır, ancak yeni nesil sabit disk sürücülerinde kayıt hacmini yükseltmek için şekil 10'daki dikey (perpendicular) kayıt teknolojisi geliştirilmiştir. Bu teknolojide manyetizma dikey yönde oluşturulmaktadır.

Dikey Kayıt Teknolojisi



Şekil 10. Verilerin dikey yönde oluşturulması

Sabit disk sürücüleri, bir diğer adıyla hard disk sürücüleri (HDD), dönen disklerden oluşan cihazlardır. Her bir diskin yüzeyi, manyetik alan etkisine sahip manyetik bir bantla kaplanmıştır. Disk plakaları, manyetik özelliğe sahip olmayan alüminyum ya da cam gibi malzemelerden yapılmaktadır. Şekil 11 ve şekil 12'de görüldüğü gibi disklerin yüzeyine çok yakın olarak konumlanmış yazma/okuma kafaları vardır. Her bir kafanın üzerinde Magnetorezistif (MR) bir algılayıcı bulunur. Yazma/okuma kafası diskin yüzeyinden geçtikçe MR algılayıcısında direnç değişimi meydana gelir. Analog direnç değişimi yorumlanarak sayısal verilere çevrilir.



Şekil 11. Yazma/okuma kafası ve taşıyıcı kol

Şekil 12. Yazma/okuma kafasının büyütülmüş hali

Hard disklerde sabit hızda dönen disklerin bağlı olduğu bir iğne bulunur. Disklerin arasında ve yüzeyinde hareket eden ortak bir kola bağlı bulunan yazma/okuma kafaları vardır. Ayrıca taşıyıcı kol, kafaların yay şeklinde hareket etmesini sağlayarak dönen disklerinin tüm yüzeylerinin okunması gerçekleştirilir. Böylece her bir kafa karşılık geldiği diskin neredeyse tüm yüzeyini tarayabilir. Diskleri döndüren iğnenin hareketleri, yazma/okuma kafalarını hareket ettiren taşıyıcı kolun hareketleri ve yazma-okuma işlemi elektronik kontrol kartıyla denetlenir.

Şekil 13. Taşıyıcı kolun ve disklerin yandan görünüşü

Şekil 14. Taşıyıcı kolun ve disklerin üstten görünüşü

Şekil 13 ve şekil 14'te görülen kafaları taşıyan hareketli kol, son derece hızlı hareket eder. Bu hareketi kenardan merkeze ve tekrar başlangıç noktasına gelme hareketini saniyede 50 defa gerçekleştirebilir. Bu işlem yüksek hızlı doğrusal bir motorla gerçekleştirilir. Aynı şekilde sabit disk plakaları da çok hızlı hareket etmektedir. Disk plakaları son derece hassastırlar. Disk plakaları üzerinde toz, tüy, nemlenme ve buhar gibi kirlenmeye neden olan unsurların kesinlikle olmaması gerekir. Yazma/okuma kafası ve disk yüzeyi arasında gözle fark edilemeyecek kadar küçük bir boşluk bulunmaktadır. Dolayısıyla bu boşluğun arasına hiçbir yabancı nesnenin girmemesi gerekir. Aksi durumda o bölgedeki bilgi ve

onunla ilişkili daha büyük bir bilgi kümesi okunamayabilir. Yazma/okuma kafasının herhangi bir nedenden dolayı (sallantı, düşme vb.) disk yüzeyine değmesi sonucunda ilgili bölge hasar görebilir. Bu durumda Bad Sector diye adlandırılan ölü bölgeler oluşur. Ölü bölgeler, fiziksel kusurlardan kaynaklandığında o bölgelerin yazılımsal olarak kurtarılması söz konusu değildir. Disk plakalarında Bad Sector sayısının artması sabit diske işletim sistemi kurulmasını engelleyebilir ya da sabit diskin çalışmasını yavaşlatabilir. Bir sabit disk kullanılmaya başlanmadan önce biçimlendirilmesi gerekir. Bir sabit diskin formatlanması demek, üzerine yazılacak bilgilerin nereye ve hangi standartlara göre yazılacağının belirtilmesi demektir. Formatlama işlemi yapılmamış bir sabit diskin üzerine anlamlı bilgi kümeleri yazmak söz konusu değildir[11].

2.7.2. CD'nin Yapısı

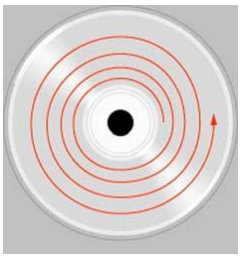
CD'ler polikarbonat plastikten üretilerek yaklaşık 1,2mm kalınlığında olup, polikarbonat malzeme biçimlendirildikten sonra şekil 15'de görüldüğü gibi ince bir yansıtıcı alüminyum tabakayla kaplanır. Polikarbonat plastik malzeme üzerinde şekil 16'da gösterilen mikroskobik boyutlarda baloncuk benzeri boşluklar meydana getirilir. Ardından alüminyum yapıyı korumak için ince bir akrilik katman oluşturulur. CD etiketi bu katman üzerine basılır.

Şekil 15. Veri kaydı yapılmış CD-ROM'un malzeme yapısı

Şekil 16. CD-ROM'un yüzey yapısı

Lazer ışın huzmesi boşluklara denk geldiğinde optoelektronik algılayıcıya geri dönmeyecek şekilde saçılır. Ancak düz bölgelere gelen lazer ışın huzmesi, optoelektronik algılayıcıya doğrudan geri döner. CD'lerin en önemli özelliği manyetik disklerden farklı olarak Şekil 17'de görülen spiral şeklinde tek bir izden oluşmalarıdır. Spiral yapı CD'nin iç kısmından dış kısmına doğru ilerlemektedir. Bu yapı sayesinde standart olarak 12 cm çapında üretilen CD'lere alternatif olarak daha küçük boyutlu ve daha az kapasiteli CD'lerde üretmek mümkündür. İzlerin genişliği 0,5 mikron (metrenin milyonda biri) ve spiral izin her bir sırası arasındaki mesafe 1,6 mikron kadardır. Bu nedenle spiral

şeklindeki izin uzunluğu oldukça fazladır (düz bir şekilde açıldığı düşünülecek olsa 5 km uzunluğu bulmaktadır).



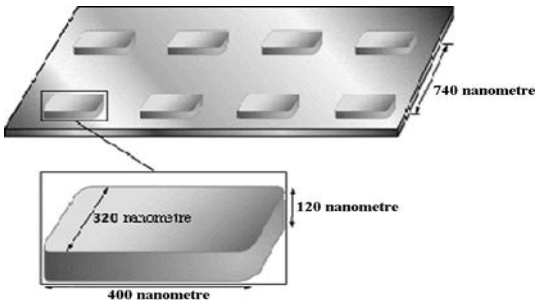
Şekil 17. CD'nin spiral şeklindeki iz yapısı

CD'lerin sektör yapısı da manyetik disklere göre farklıdır. Manyetik diskte açısal hız her yerde aynıdır. Bu nedenle diskin dış tarafı iç tarafa göre daha hızlı döner. Ayrıca diskin dışına doğru sektörlerin boyutu artmaya başlar. Ancak CD'lerde spiral izin her bir sektörü eşit boyuttadır. CD sürücülerde sabit doğrusal hız (constant linear velocity) diye adlandırılan bir okuma tekniğiyle okuma hızı duruma göre değiştirilir. CD'nin dış taraflarına yaklaşıldığında hız yavaşlatılırken iç taraflara doğru hız yükseltilir.

CD'ler, farklı koruyucu malzemeler kullanılarak yapılmaktadır. Bu durum CD'lerin kalitelerini belirleyen bir unsurdur ve okuma işleminin yapıldığı yüzeyin renginden bu farklılık anlaşılabilir[12].

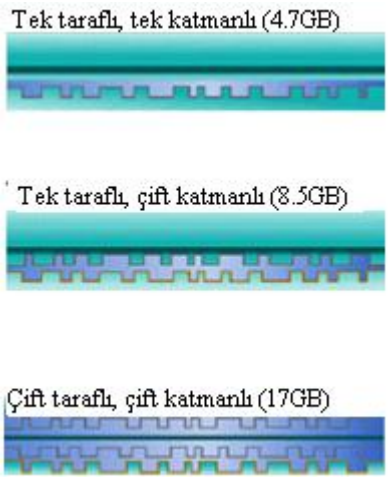
2.7.3. DVD'nin Yapısı

DVD 'Digital Video Disk' kelimelerinden oluşmuştur. CD'ye göre katman teknolojisi farklı olup, yüzeyinde yer alan boşluklar çok daha küçüktür. DVD-ROM diskler de CD-ROM diskler gibi tek bir izden meydana gelmektedir. Şekil 18'de DVD-ROM bir diskte çukurların boyutu ve izin her bir sırası arasındaki mesafe gösterilmiştir.



Şekil 18. DVD-ROM diskin yapısı

DVD'nin iz aralığı CD'nin iz aralığından 2.16 kat daha küçüktür. Aynı şekilde çukur genişliği de 2.08 kat daha küçüktür. Bu iki değeri çarparsak tek taraflı-tek katmanlı bir DVD'de çukur sayısının CD'nin 4,5 katı olduğunu hesaplarız. Ancak tek taraflı-tek katmanlı bir DVD'nin CD'nin 7 katı kadar veri saklayabildiğini söylemiştik. O zaman geri kalan fark nereden gelmektedir? Bu fark DVD'lerde kullanılan hata denetim kodundan ileri gelmektedir. CD'lerde kullanılan hata denetim kodu çok eskidir ve oldukça büyük bir yer kaplamaktadır. DVD'lerde ise yazılan bilginin çok büyük kısmını ham bilgi oluşturmaktadır. Yazılabilir DVD teknolojisi oldukça farklı standartlarda karşımıza çıkmaktadır. Bu durum çoğu kullanıcının kafasını karıştırır. Şekil 19'da farklı yapılarda DVD'ler gösterilmiştir. DVD'ler sahip oldukları katman kadar birbirinden farklı ize sahiptir. İki katmanlı bir DVD'de izler farklı yönlerde döner.



Şekil 19. Farklı katman yapılarına sahip DVD'ler

DVD disklerin en önemli ayrıcalıklarından birisi de katmanlı üretilebilmeleridir. Böylece veri kapasiteleri değiştirilebilir.

2.7.4. Flash Bellek

Flash bellekler, güç kesintisinde bilgilerini kaybetmeyen ve tekrar tekrar yazılıp silinebilen bir bellek çeşididir. Flash belleklerin yapısı RAM belleklere, kullanımı ise sabit disklere benzer. Flash bellek üzerine verilerin yazılması, RAM modüllerinin kullandığı yöntem yardımıyla gerçekleşir. Flash belleklerin yapısı mekanik değildir, elektroniktir. İçerisinde hareket eden bir parça yoktur. Bu özelliklerinden dolayı bu tarz bellekler "solid-state" olarak, yani "durağan" olarak adlandırılırlar. Hareket eden parça olmamasından

dolayı sabit diskler gibi hassas değildirler ve özellikle mobil alanda kullanımları çok yaygındır[13]. MP3 player'larda, cep telefonlarında, el bilgisayarlarında, dijital fotoğraf makinelerinde ve dijital görüntü aygıtlarında yaygınca kullanılırlar. Flash bellekler, bir EEPROM çeşidi olarak adlandırılabilir. "Elektriksel olarak silinebilen, programlanabilen, sadece okunabilen bellek" olarak çevrilebilen EEPROM'ların üzerindeki veriler elektriksel yolla değiştirilebilir. Sadece okunabilir bellek denilmesinin sebebi, bilgilerin kalıcı olmasından dolayıdır. Klasik bellek yapılarından bilindiği üzere, flash bellekler de hücrelerden oluşur. Her hücrenin kendi transistörleri vardır. Bilgisayar ortamında bilgiler 0 ve 1'lerden oluşur. 0'lar düşük voltaj, 1'ler ise yüksek voltaj anlamına gelir. Veri yazılmak istendiği anda, transistörlerin voltaj seviyeleri değiştirilerek bilgiler yazılabilir, silinebilir veya yenilenebilir. Flash belleklerin genel özellikleri ise şöyle sıralanabilir. Küçük boyut: Çeşidine göre, kredi kartının yarısı, çeyreği veya daha küçük olabilir. RAM modüllerinde gördüğümüz hücreler ve bu hücrelerin oluşturduğu satır ve sütunlar, Flash belleklerde de bulunur. Her bir hücrenin kendi transistörleri vardır. Transistörlerin voltaj ile uyarılması ile "0" ve "1" değerleri oluşur. Sonuçta her bir hücre "0" ya da "1" değerleri ile doldurulur ve bu değerlerin birleşmesi ile de veriler meydana gelir. Buraya kadar her şey standart RAM modüllerindekiyle birebir aynıdır. Flash bellekleri standart RAM modüllerinden ayıran ise, yazılan verilerin güç kesintisinde bile silinmemesidir. Bilgisayarın elektrik gücü kesildiğinde, RAM modülleri üzerindeki tüm veriler de silinir. Bu yüzden standart bellek modülleri "Volatile" (uçucu) terimi ile birlikte anılıyorlar. Flash belleklerde ise böyle bir durum söz konusu değildir. Herhangi bir elektrik kesintisinde bile flash bellek üzerindeki veriler silinmez. Bu verileri silmek ise tamamen kullanıcının kontrolündedir. Bir disket üzerindeki verileri nasıl siliyorsak, flash belleklerdeki veriler de ancak o şekilde silinebilir. "Non-Volatile" terimi de verilerin bellek üzerinde kalıcı olduğunu simgeler. Verilerin güç kesintisi nedeniyle silinmemesi, flash bellek teknolojisinin kullanım alanlarını belirleyen en önemli nedendir. Bugün flash bellek teknolojisi ile üretilen bellek kartları ve USB bellekler, standart RAM modülleri gibi değil, küçük birer depolama ünitesi olarak görev yapıyorlar. Dijital fotoğraf makineleriyle çekilen fotoğraflar ya da MP3 çalarlarda dinlenen müzik dosyaları hep flash bellekler üzerine yazılıyor. Hatta bu teknolojinin yardımıyla verilerin bir bilgisayardan diğerine taşınması da oldukça kolaydır. Sabit disk ile flash bellek arasındaki benzerlik de bu şekilde açıklanabilir. Flash bellekler için verilebilecek en güzel örnek, kuşkusuz anakart üzerindeki BIOS yongası olacaktır. Anakart ve üzerindeki donanımların temel ayarlarından senkronizasyonuna kadar hemen her türlü veriyi

barındıran BIOS, aslında küçük bir yazılımdır. Bu yazılım, yine anakart üzerinde yer alan flash bellek yongasında (EEPROM) saklanır. EEPROM'un en büyük avantajı, içindeki bilgilerin (yani BIOS'un) güncellenmesine izin vermesidir. Ancak kullanıcı istemediği sürece veriler silinmez ve değiştirilemez. Yani bilgisayarı kapattığınızda bile yazılım BIOS yongasından silinmez. Bu yongayı destekleyen küçük tablet pil ise sadece yapılan ayarların ve saat gibi temel fonksiyonların bırakıldığı gibi kalmasını sağlar. Temel BIOS yazılımı ise pil bitse bile bellek yongası üzerindeki varlığını sürdürecektir.

Flash bellek teknolojisini iki farklı kategoride değerlendirmek mümkündür. Bunlardan birincisi, NOR flash bellek teknolojisi adı verilir. Cep telefonlarında, PCMCIA kartlarında ve BIOS yongalarında kullanılan NOR Flash bellekler, verilerin yazılması ya da silinmesi işlemini her bir hücre için tek tek gerçekleştiriyor. Bir hücre iki farklı transistöre sahip ve bu transistörlere "Control Gate" ve "Floating Gate" adı veriliyor. Bu transistörler birbirlerinden ince bir oksit tabaka ile ayrılmaktadır. "Control Gate" üzerinde standart olarak "1" değeri yer alır. Eğer bu transistora herhangi bir müdahale olmazsa, hücre "1" ile yüklenir. Hücreye "0" değerinin yazılması ise, "Fowler Nordheim Tunneling" adı verilen işlem yardımıyla gerçekleşir. Bu işlemde asıl görev "Floating Gate" isimli ikinci transistora aittir. "Floating Gate" elektrik gücü ile uyarılır ve bazı elektronlar iki transistor arasındaki oksit tabakaya sıçrar. Sıçrayan elektron miktarı "Cell Sensor" isimli özel bir birim tarafından kontrol edilir. Eğer oksit tabakaya aktarılan elektron miktarı toplam elektrik gücünün yarısından fazlaysa, yüklenen değer "1" olarak kalır. Bu değerin "0" olması ise, sıçrayan elektron miktarının yüzden 50'nin altına düşmesine bağlıdır. "Floating Gate"e elektrik verilmesi her bir hücre için ayrı ayrı gerçekleştiğinden, verilerin yazılması ve silinmesi de hücre bazında gerçekleşmiş olur. NAND, yeni nesil bellek kartlarında ve USB belleklerde kullanılan NOR Flash belleklere oranla biraz daha hızlı olan teknolojiye verilen isimdir. Bu tip flash belleklerin çalışma mantığı genel olarak NOR ile aynı olsa da, verilerin yazılması ve silinmesi işlemi hücre bazında gerçekleşmez. Bunun yerine, bellek üzerine veri yazılması için birçok hücrenin bir araya gelerek oluşturdukları bloklar kullanılır. Hatta NAND Flash belleklerde tek bir elektrik yükü ile tüm belleğin silinmesi bile mümkündür. Bu yüzden de NAND teknolojisi, NOR'a göre daha yüksek bir performansa sahiptir. Ayrıca maliyetleri de NOR Flash belleklere oranla oldukça düşüktür. Ancak konu rastgele erişim yeteneği olduğunda, NOR'un üstünlüğü tartışılmaz. Çünkü NAND Flash bellekler istenen veriye ancak blok halinde ulaşabilirken, NOR flash bellekler tek bir byte'ı bile bulup işleyebilmektedirler[14].

2.8. Dijital Veri Saklama Ortamlarındaki Dosya Sistemleri

Dosya, disk üzerinde depolanmış verilerin bütününe verilen isimdir. İşletim sistemi tipik olarak iki çeşit dosya içermektedir. Birincisi, işletim sistemi bir sistemi veya bir uygulamayı çalıştırırken bilgisayarı kontrol eden program dosyalarıdır. İkincisi ise, bir kelime işlem programında bir uygulama yardımı ile oluşturulmuş bilgileri içeren veri dosyalarıdır. Dosya sistemi, bir dosyanın bir disk üzerinde nasıl saklandığı ve bir bilgisayarın dosyaları yönetebilmek için erişimi nasıl sağladığını kontrol eden bir sistemdir.

2.8.1. FAT 16

Dosya yerleşim tablosu FAT, bir diskte bulunan dosyalara ait bilgilerin kayıtlı olduğu alanları belirtir. Yani FAT, bir diskin haritasıdır. FAT dosya sisteminde bölüm, her biri belli miktarda sektör içeren kümelere (cluster) ayrılır. Dosyaların bu kümeler üzerinde nereye, nasıl yazıldığı FAT sistemi üzerinde tanımlıdır. İşletim sistemi herhangi bir dosyaya erişmek istediğinde FAT üzerine yazılan bu bilgilerden faydalanmaktadır. FAT16 dosya sistemi eski bir dosya sistemi olduğundan dolayı bir takım eksikleri ve dezavantajları bulunmaktadır. Bunlardan biri kök dizininin (root) sınırlandırılmış olmasıdır. FAT16 kullanan işletim sistemlerinin açılışındaki birincil bölüme ait kök dizini, FAT tablosu ve bölüm boot sektörü FAT16 kümesi içinde yer almazlar ve sayısı belli olan sıralı sektörlerde tutulurlar. Bu sektör sayısının belli olması, kök dizine yapılacak olan eklentilerin de belli bir sınırı olmasını gerektirir. FAT16 dosya sisteminde 16 bitlik adreslemeden dolayı, adreslenebilen maksimum küme sayısı 65536 olmalıdır, ancak 11 adet kümeı özel amaçlar için tutulduğundan küme sayısı 65525'e düşmektedir.. Bu durum FAT16 kullanan bir disk ya da bölümün 2GB'dan daha büyük olamayacağını gösterir. Boş bir sabit disk biçimlendirilirken FAT16 dosya sistemi tarafından kümelere bölünür. Bu nedenle sabit diskin boyutu büyümeye başladıkça küme boyutu da büyür.

Tablo 1. FAT(12/16) Sanal Dosya Yerleşim Tabloları

FAT 12/16 da Küme (Cluster) Boyutları			
Bölüm Boyutu(GB)	**FAT Tipi**	**Sektör/Küme**	**Küme Boyutu**
0-15	12 bit	8	512 byte
16-127	16 bit	4	2K
128-255	16 bit	8	4K
256-511	16 bit	16	8K
512-1023	16 bit	32	16K
1024-2047	16 bit	64	32K
2048-4096	16 bit	128	64K

2.8.2. FAT 32

FAT32 dosya sistemi Windows 95/98 ve Linux işletim sistemleri tarafından tanınıp kullanılabilen ve FAT16'dan daha gelişmiş bir dosya sistemidir. FAT32'de herhangi bir kök dizin sınırlaması yoktur. FAT32 dosya sistemi, FAT16 dosya sistemindeki 16 bit adresleme yerine 32 bit adresleme kullanır. Bu sayede herhangi bir disk ya da bölüm FAT32 altında 2 terabyte uzunluğunda olabilir. FAT32, FAT16'ya göre diski daha küçük boyutta kümelere ayırdığından diskte daha verimli bir kullanım alanı oluşur. FAT32 altında tek bir dosyanın erişebileceği maksimum boyut 4 GB ile sınırlıdır.

Tablo 2. FAT(32)Sanal Dosya Yerleşim Tabloları

FAT 32 de Küme (Cluster) Boyutları		
Bölüm Boyutu(GB)	**Sektör/Küme**	**Küme Boyutu**
0.256<	1	512 byte
0.256-8	8	4K
8-16	16	8K
16-32	32	16K
>32.04	64	32K

2.8.3. NTFS

NTFS (New Technology File System -Yeni Teknoloji Dosya Sistemi) Windows NT ve devamı olan Windows 2000, XP işletim sistemleri tarafından desteklenen bir dosya sistemidir. NTFS, dosya konumlarını FAT sistemindeki gibi bir ana indeks olarak saklamakla birlikte MFT (Master File Table - Ana Dosya Tablosu) ile dosyanın yerleştiği

konumları ve diğer bilgileri her kümenin içinde ayrıca saklayarak daha güvenilir bir yapı sunar. Dolayısıyla oldukça geniş bir disk haritası oluşturur. MFT bilgileri önemli bir yer kapladığından dolayı 400MB'den küçük disk veya bölümlerde NTFS kullanılması önerilmez. NTFS, sunucu olarak görev yapan Windows NT ve Windows 2000 işletim sistemlerine ait bir dosya sistemi olmasının gerektirdiği ihtiyaçlar doğrultusunda daha çok disk güvenliği ve performansıyla ilgili iyileştirmeler içerir. Dosya konumlarıyla ilgili bilgileri küme içlerinde de saklayarak daha güvenli bir dosya sistemi yapısı sunar. Küme boyutu bölüm boyutuyla sınırlı değildir ve 512 byte değerine kadar ayarlanabilir. Bu da, disk üzerinde dosyaların parçalanmasını azaltarak hem boş alanın verimli kullanılmasını, hem de özellikle yüksek kapasiteli sabit disklerde performans artışını beraberinde getirir. Yaklaşık 16 GB'a kadar uzunluktaki olan tek parça dosyaları destekler. ACL (Access Control List - Erişim Kontrol Listesi) özelliği sayesinde sistem yöneticileri tarafından hangi kullanıcıların hangi dosyalara erişebileceği ile ilgili kısıtlamaların koyulabilmesini sağlar. Bütünleşik dosya sıkıştırma özellikleri içerir. Uzun dosya isimlerini ve Unicode kaynaklı dosya isimlerini destekler. Unicode, dosya isimlendirilmesi sırasında karakterlerin tanımlanması için ikilik sistemde kodlar kullanılmasını öngören bir standarttır. Bu standarda göre Unicode kullanılarak verilmiş olan dosya isimleri Unicode kullanabilen dosya sistemleri tarafından tam olarak nasıl hazırlanmışlarsa o şekilde görünürler (örneğin, Japonca veya Arapça gibi).

NTFS dosya sistemi kullanan Windows NT ve Windows 2000 sürümleri FAT sürücüleri görebilir ve bu sürücülerdeki dosyaları okuyabilirler. Windows NT FAT16'yi, Windows 2000 FAT16 ve FAT32'yi görür. Ancak, FAT16 kullanan Windows 95, 98 ve DOS gibi işletim sistemleri NTFS bölümlerini göremezler. Dolayısıyla, dosya sistemi NTFS olan disk veya bölümlere ait verileri okuyamazlar. Bu nedenle FAT32 altına kurulmuş bir Windows 98 ve NTFS bölüme kurulmuş olan bir Windows 2000 varsa Windows 2000 FAT32 bölüme kurulu olan Windows 98'e ait dosyaları görebilri ve bu sürücüye bir isim verebilir. Ancak, Windows 98 NTFS altındaki Windows 2000 dosyalarını göremeyecek ve bu bölümü bir disk gibi algılayamayacaktır. Bu nedenle bu sürücüye herhangi bir sürücü ismi de veremez[15].

Tablo 3. NTFS Sanal Dosya Yerleşim Tabloları

NTFS Küme (Cluster) Boyutları		
Bölüm Boyutu(GB)	**Sektör/Küme**	**Küme Boyutu**
0.512<	1	512 byte
0.512-1	2	1K
8-16	4	2K
16-32	8	4K
0.256<	16	8K
0.256-8	32	16K
8-16	64	32K
>32	128	64K

2.8.4. EXT2/EXT3/ EXT4

Linux işletim sisteminde en popüler dosya sistemleri, EXT2 ve EXT3 formatındadır. EXT3 dosya sistemi, EXT2′nin geliştirilmiş hâlidir ve günlükleme özelliğine sahiptir. Günlükleme desteği olan dosya sistemleri, disk üzerinde gerçekleşen işlemleri kayıt altında tutar. Böylece, herhangi bir sistem çökmesi esnasında, geri kurtarma daha kolay sağlanır. Bunlara ek olarak, Linux işletim sistemi çok sayıda farklı dosya sistemini desteklemektedir. Böylece farklı işletim sistemleri arasında aynı dosyaları paylaşmak ve kullanmak kolaylaştırılmıştır. Bu farklı dosya sistemleri, makine üzerinde doğal Linux dosya sistemleri gibi çalışabilirler. EXT4 veya diğer adıyla "dördüncü genişletilmiş dosya sistemi" EXT3 dosya sisteminin halefi olarak geliştirilmiş günlük desteği olan bir dosya sistemidir. Sabit disklerin terabyte sınırlarına ulaşmasıyla EXT3 dosya sisteminin 21. yüzyıl sabit disklerinin kapasite gereksinimlerini karşılayamayacağı için çıkarılmıştır. Kernel geliştiricileri tarafından EXT4 dosya sistemi yapısının deneme sürümü çıkarılmıştır. Yeni dosya yapısının bölüm (hacim-alan) başına 1024 petabyte kapasite desteklediği belirtiliyor. (1 petabyte = 250 byte). Ayrıca EXT4 dosya sistemi "*extent file writing*" özelliği desteklidir. Bunun anlamı; bir dosya oluşturulduğunda bellekte dosyanın sonuna sonradan veri eklenebilir düşüncesiyle devamlılık sağlayacak bir alan eklenmektedir. Böylece dosyanın üzerine veri tekrar yazıldığında bu veriler bellekte ayrı alanlara dağıtılmak zorunda kalmıyor ve diskin performansını olumlu yönde etkiliyor. Diğer modern dosya yapıları gibi EXT4 de "journal file system" desteklidir. Yani herhangi bir dosya değiştirildiğinde eklentiler dosyanın yapısını değiştirmeden önce bir günlüğe eklemektedir. Böylece dosya üzerinde herhangi bir bozulma oluştuğunda sistem, dosyayı kolaylıkla onarıp tekrar geri sunmaktadır. Bu özelliklerin yanında EXT4 dosya yapısı

EXT3 ile de uyumlu çalışabilmektedir. Yani EXT4 dosya yapısına sahip bir disk, EXT3 olarak çevrildiğinde herhangi bir sorunla karşılaşılmamaktadır. [16].

3. SAYISAL ORTAMDAKİ VERİLERİN KORUNMASI VE KURTARILMASI

Bilişim dünyasında veriler en önemli değeri oluşturmaktadır. Günümüzde, verilerin çoğunluğu dijital ortamlarda saklanır. Modern teknolojiler, çalışma zamanımızı kısaltmak ve yaşamı daha konforlu hale getirmek gibi birçok avantaj sunar. Hiçbir teknolojinin ve korunma yönteminin tamamen risk taşımadığını söylemek doğru olmaz. Bu anlam da verinin dijital ortamda saklanması da beraberinde bir takım riskleri doğurur. Verilerin dijital ortamda güvenliğini sağlamak için veriyi korumak için geliştirilmiş güncel teknolojilerin kullanılması gerekmektedir.

3.1. Dijital Veri Koruma Teknolojilerinin İncelenmesi

Verilerin korunması için geliştirilen belli başlı teknolojileri aşağıda irdeleyeceğiz.

3.1.1. SMART Teknolojisi

SMART (Self Monitoring Analysis Reporting Technology) teknolojisi 1992 yılında IBM tarafından 3.5 inçlik diskler için tasarlanmış olan bir teknolojidir. Sabit diskin sürekli kendini gözetleyerek, disk içinde donanımsal bir arıza olduğunda kullanıcının bundan haberdar olmasını sağlayan bir çeşit erken uyarı sistemidir. Böylece kullanıcı sabit disk içindeki verileri vakit kaybetmeden yedekleyebilir ve veri kaybının önüne geçebilir. Bu, bir anlamda kendi durumlarını ve oluşabilecek hataları denetleme mekanizmasıdır. SMART kendi içerisinde PFA (Predictive Failure Analysis - Olası Bozukluklar Analizi) teknolojisini içerir. Bu sayede sürekli kendini denetleyen bir disk, bozulma durumunda uyarır verir. Bu özellik için BIOS ve kontrol çipleri SMART teknolojisine uyumlu olmalıdır. Bu teknolojide bozulmalar 2 gruba ayrılır. Bunlar, tahmin edilebilir bozulmalar ve tahmin edilemez bozulmalardır. Tahmin edilemez hatalar genelde statik elektrik, ısınma veya darbesel nedenlerden dolayı bir anda ortaya çıkar. Tahmin edilebilir hatalar ise okuyucu kafanın normalden hızlı veya yavaş hareket etmesi şeklinde mekanikseldir.

SMART, sabit disk içindeki olası problemlerin yaklaşık % 70'ini haber verebilmektedir. Öte yandan sabit disklerdeki problemlerin çoğu çarpma, düşme gibi anı fiziksel etkenlerden kaynaklandığı için SMART bazı durumlarda etkisiz kalabilir. Günümüzde sabit disklerin neredeyse hepsi SMART özelliğini desteklemektedir. SMART, disk sürücülerin sağlığı ve potansiyel problemlerini raporlayan ve otomatik olarak gözden geçiren disk sürücüler ve yazılım sistemleri geliştirmek için kullanılan açık bir standarttır. Disk hatalarını önlemek için kullanıcının önceden önlem almasını sağlar. SMART, ciddi

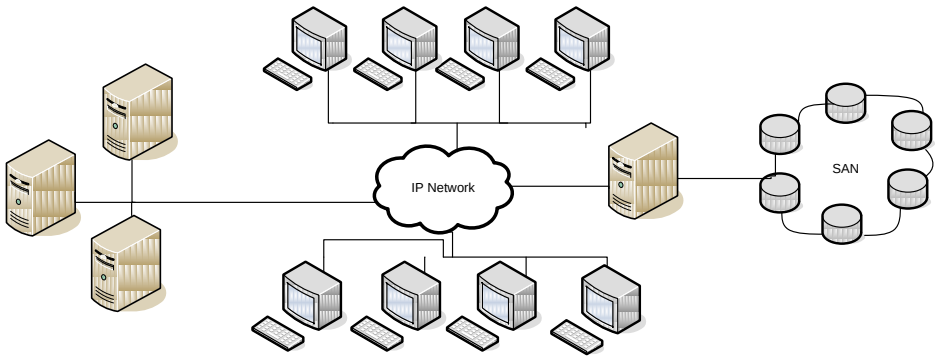
bir problemi tespit ettiğinde işletim sistemi aracılığıyla uyarır. Bu uyarı alındığı takdirde, sistem kapatılmadan önce kullanıcı/yönetici tarafından acilen yedek alınmalıdır.

3.1.2. SPS

SPS (Shock Protection System), diski darbelere karşı koruyan bir sistemdir. Disklerdeki fiziksel hasarların oluşma nedeni, diskin aldığı fiziksel darbelerdir. Disk bir darbe aldığında okuma/yazma kafası sıçramakta ve disk yüzeyinde birkaç kez zıplayarak mikro partiküllerin kopmasına neden olmaktadır. Fiziksel hasarlar (bad sector) böyle oluşur ama zamanla kafa disk içinde serbest dolaşan bu partiküllere rastladıkça, darbe almasa da tekrar sıçrayıp daha fazla zarar verir. Quantum, bu riski azaltmak için SPS adını verdiği bir süspansiyon mekanizması geliştirmiştir. Böylece kafa darbelerde disk plakaları üzerinde pek sıçramaz. Quantum, SPS sistemi ile sistem montajı sırasında oluşan disk arızalarını %70, arızalı ürün iade oranını ise %30 azalttıklarını ileri sürmektedir.

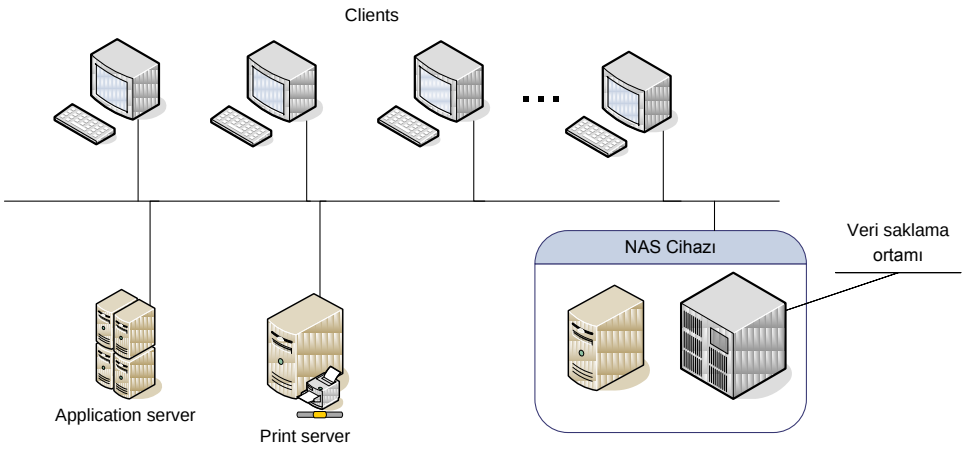
3.1.3. SAN Ve NAS Teknolojileri

İş ve özel amaçlarda kullanılacak veri boyutlarının artmasıyla, disketlerden CD'lere, DVD'lere, Blue-Ray disklere, flash disklere, taşınabilir sabit disklere kadar veri depolama aygıtları geniş bir yelpazeye dağılmıştır ve bu aygıtların boyutları da gün geçtikçe artmaktadır. Özellikle iş amacıyla kullanılan verilerin yeterince büyük herhangi bir ortamda saklanabilmesi ihtiyacının yanı sıra bu verileri diğer kullanıcılara da paylaştırma gereği ortaya çıkmaktadır. Var olan verilerin makinenin üzerinde takılı olan diskler haricinde merkezi bir yerde saklanmak istendiğinde SAN ve NAS gibi iki adet çözüm bulunmaktadır. SAN (Storage Area Network), verinin çok sayıda kopyasını(mirror) oluşturmaya da olanak sağlar. SAN'da, sunucu ve saklama aygıtlarını birbirine bağlayan yüksek hızlı ara bağlantı, LAN'a bağlı olan ayrı bir dış bağımsız ağ olarak çalışır. SAN'ların sağladığı yararları söyle özetleyebiliriz. LAN'ı rahatsız etmeden, bant genişliği eklemeye olanak tanırlar, Kullanıcılar bant genişliği azalmasını hissetmeden, çevrimiçi yedeklemeler alınabilir. Daha fazla saklama kapasitesine gereksinim duyulduğunda, belirli bir sunucuya ek sürücüler eklemeye gerek yoktur. Bunun yerine, ek sürücü aygıtlar SAN'a eklenir ve herhangi bir noktadan bu aygıtlara erişilebilir. Tüm aygıtlar merkezi olarak yönetilebilir. Yani aygıtları tek tek yönetecek yerde, saklama ortamı tek bir SAN olarak yönetilir. Bu arada SAN içinde, onlarca sunucu ve aygıt bulunabilir.



Şekil 20. SAN Topolojisi

NAS (Network Attached Storage), network üzerinde şekil 21'de görüldüğü gibi merkezi bir lokasyonda sunucu ve istemciden bağımsız bir şekilde saklanan verilerin paylaşıma açılabilmesi için NAS cihazları kullanılmaktadır. NAS cihazı aslında LAN'a bağlı yüksek erişim hızında depolama yapabilen bir dosya sunucusudur. Genel kullanım için oluşturulmuş olan işletim sistemi, NAS cihazlarında sadece dosya paylaşımıyla ilgili işlemleri yapabilmek için sadeleştirilmiştir. Dosya I/O 'ları (input/output) gerekli protokoller eklenmiş ve bu iş için optimize edilmiştir. NAS Server olarak da adlandırılan bu cihazlara her ne kadar sonuna server ibaresi eklenmiş olsa da veri depolayıp paylaşıma açmaktan daha başka özellikler (DNS Server, DHCP Server vb.) kazandırmak mümkün değildir. NAS çözümünün en önemli faydaları arasında kolay yönetim, yedekleme özellikleri ile kritik verilerin disklere yedeklenebilmesi ve düşük maliyet gelmektedir[17].



Şekil 21. NAS topolojisi

3.1.4. RAID

Bir bilgisayardaki diskin arızalanması durumda verinin kurtarılması için yapılacak işlem bir önceki yedekleme işlemindeki verinin yeni bir diske aktarılmasıdır. Bilgi ne

kadar güncel olursa olsun çoğu kez veri kaybı kaçınılmazdır ve yedeklenen bilgilerin geri yüklenmesi ve eski çalışma şekline dönülmesi zaman alacaktır. Bir kullanıcı sistemi için bu çoğu kez göz ardı edilebilir bir durum olsa da bir sunucu sisteminde aynı durumun yaşanması arzu edilir bir durum değildir. Ucuz disklerin yedekli dizisi, RAID (Redundant Array of Inexpensive Disks) bu tür problemlerle baş edilebilmesi için geliştirilmiştir. RAID, adından da anlaşılacağı üzere, ortak bir görevi yerine getirmek üzere bir araya getirilmiş ucuz bir küme disktir. RAID, gerçek zamanlı bir yedekleme sistemi, yüksek veri çıktısı elde etme için bir yöntem veya servis sürekliliğini artırmak için yedeklilik amacıyla kullanılabilir. Bir RAID, istenilen RAID seviyesine göre iki diskten başlayarak birçok diskten teşkil edilebilir. Ek olarak RAID yazılım veya donanım tabanlı olabilir. Yazılım RAID genellikle aynalama ve dilimleme gibi basit işlevleri (0 ve 1 seviyeleri) sağlar. Yüksek RAID seviyelerini işletimi daha karmaşık olduğundan yazılım, bunların uyarlanması için çok yavaş kalacaktır. Bu yüzden RAID seviyeleri için özel geliştirilmiş donanımlar kullanılır. RAID uyarlamaları nasıl yapılandırıldıklarına ve ne ölçüde performans ihtiyaç duyulduğuna göre farklılık gösterirler. Aşağıda RAID seviyeleri açıklanmaktadır.

RAID Seviye 0: Seviye sıfır, RAID'deki tüm disklerin büyük tek bir sanal disk olarak çalışacak şekilde yapılandırıldıkları en temel çalışma şeklidir. Her disk sürücü toplam bilginin bir bölümünü içerir. Bu ayırma işlemine Striping adı verilir. Yedeklilik olmadığından, hızlı bir işletim sağlanır ve özellikle masaüstü sistemlerinde faydalı olabilir. RAID'deki disk sayısı arttıkça arıza olasılığı artacaktır. Eğer bilgi çok önemli değilse ve harici bir yedekleme ortamı kullanılıyorsa, risk azaltılmış olacaktır.

RAID Seviye 1: Aynalama (Mirroring) olarak da anılan RAID Seviye 1, eş bir disk kullanılarak bir diskin dinamik olarak bir kopyasının tutulmasını sağlar. Seviye birden fazla diskin aynalanmasını destekler ancak bire bir ilişkilendirme sağlamalıdır. Bu yüzden aynalanacak her bir disk için ayrı eş bir disk tutulmalıdır. Aynalama az sayıda disk için iyi bir alternatiftir. Fakat disk sayısı artıkça maliyet de artacak ve sistem hantallaşacaktır.

RAID Seviye 2: SCSI olmayan (Small Computer System Interface) sabit sürücüler tipik olarak, sakladıkları veri üzerinde hata düzeltme işlevinden yoksundurlar. RAID Seviye 2 Hamming kodlarını kullanarak hata tespiti ve düzeltimini gerçekleştirebilmektedir. Böylelikle veri iletimi sırasında hasar görmüş veri blokları ileride bir probleme sebep olmadan düzeltilmiş olurlar.

RAID Seviye 3: Seviye 3, birçok diskin tek büyük, hızlı bir disk olarak çalışmasını sağlayacak bir bölümleme düzeni kullanır ancak dosyalar Byte bloklarına ayrılır ve dizideki disklere dağıtılır. Disk sayısı arttığından hata tespiti daha önemi bir hale gelecektir. Ayrı bir eşlik diski hata tespiti ve düzeltimi için kullanılır. Bazı kısıtlamalar olmasına rağmen eşlik kullanımı ile arızalı bir diskte kayıp verinin yeniden inşası mümkün olmaktadır. Ancak eşlik birden fazla diskte arıza olduğu durumda işe yaramayabilir. RAID'den veri okunacağı zaman tüm diskler erişilebilir durumdadır. Bilgi yazılırken eşlik sürücüsü de mutlaka güncellenmelidir. RAID'de aynı anda ya yazma ya da okuma gerçekleştirilebildiğinden, eşlik sürücüsü yazma işlemlerinde bir darboğaza sebep olabilir. Bu durum RAID Seviye 3'ü veri okuma yazma hacminin sabit kaldığı uygulamalar için uygun yapmaktadır. Sıklıkla küçük hacimli okuma ve yazma işleminin gerçekleştirildiği uygulamalar için başka çözümleri düşünmek gerekir.

RAID Seviye 4: Seviye 3 ve 4, Seviye 4'te byte kodlama yerine bir blok kodlama düzenin kullanılması dışında oldukça yakın kavramlardır. Seviye 4'te dosyalar byte'lara bölüneceklerine bloklara bölünürler. Blokların büyüklüğü RAID oluşturulurken belirlenir. Blok kodlama, RAID'e yazma / okuma erişimi için byte kodlamadan daha iyi sonuçlar vermektedir ancak eşlik diski yine bir darboğaz oluşturabilmektedir.

RAID Seviye 5: RAID Seviye 4'de olduğu gibi, RAID Seviye 5 birçok fiziksel sürücüye ulaşmak için blok kodlama kullanır ve eşlik tutulur. Ancak ayrı bir eşlik diski yerine eşlik bilgisi dizideki disklere dağıtılır. Bu yüzden Seviye 5 Seviye 3 ve 4'e göre sık aralıklı birçok okuma ve yazma işlemine çok daha iyi cevap verebilir. Buna rağmen seviye 5, eşlik tutulması yüzünden, diziye yazma gerçekleştirilirken, önemli ölçüde bir yüke sahiptir.

RAID 6, 7: RAID 6 ve 7, pazarda özel olarak geliştirilmiş ve diğer RAID türlerinin türevleridirler.

RAID Seviye 1/0: Seviye 10 olarak da adlandırılan Seviye 1/0, striping(şeritleme) ve aynalama sağlayan, Seviye 0 ve 1'in bir birleşimidir. Seviye 1 gibi birçok disk tek bir büyük hızlı sanal diski oluşturduğu gibi bu disklerin tümü aynalanır. Seviye 1/0, Seviye 0'ın hızını sağladığı gibi disk arızaları durumunda yedeklilik de sağlamaktadır.

RAID Seviye 5/0: Seviye 1/0 gibi, Seviye 5/0, Seviye 5 ve 0'ın bir birleşimi olup birçok Seviye 5 RAID'leri Seviye 0 düzeni ile bölümlenmiştir.

3.1.5. Yedekleme (Backup)

Bilgi, bir kurumun önemli varlıkları arasındadır. Herhangi bir nedenle kullanılamaz duruma gelmesi bilginin kritikliği derecesinde kuruma zarar verir. Bu sebeple bilgi sınıflandırılmalı ve kaybı durumunda tekrar elde edilmesi için gereken planlama yapılmalıdır. Depolanan verinin herhangi bir nedenle zarar görmesi kurum süreçlerinde ciddi zararlara neden olabilmektedir. Felaket durumu sonrasında kurum verisinin geri yüklenememesi kurumun ticari faaliyetine son vermesine neden olabilecek kadar ciddi sonuçlar doğurabilmektedir. Depolanan verinin her geçen gün arttığı ve verinin kurum süreçleri için daha kritik bir rol oynadığı günümüzde verinin yedeklenmemesi büyük risk oluşturmaktadır. Bu sebeple kurumlarda yedekleme sistemleri kurulmakta ve yedekleme işleri günlük olarak takip edilmektedir. Yedekleme sisteminin kurulumu yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.

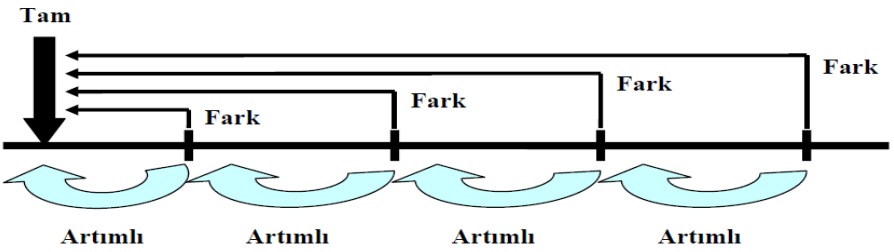
Veri yedeklemesinin amacına uygun olarak gerçekleştirilebilmesi için düzenleyici ve yönetimin konuya bakış açısını yansıtan bir yedekleme politikasına ihtiyaç vardır. Yedekleme politikası kurum için yedeklemenin önemini ve en az yerine getirilmesi gerekenleri ifade etmelidir. Yedekleme politikasının yerine getirilmesi için detaylı bir analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planın işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir[18].

Veri Yedekleme Türleri: Veri yedekleme temel olarak tam yedekleme (full) , fark yedekleme(differential) ve artan yedekleme (incremental) olmak üzere üçe ayrılmaktadır.

Tam yedekleme: Tam yedekleme, yedeği alınmak üzere seçilmiş bütün bilgilerin bir kopyasının yedekleme medyasına kaydedildiği bir yedekleme türüdür. Tam yedeklemede orijinal verinin birebir kopyası alındığı için yedekleme medyasında orijinal verinin boyutu kadar yer kaplamaktadır. Bu çalışma biçimi yedek alma süresini uzatmakta ve ihtiyaç duyulan yedekleme sıklığının sağlanmasını zorlaştırmaktadır. Yedekleme donanımının yetersiz olduğu, yedeklenecek veri boyutunun çok yüksek olduğu veya verinin sık yedeklenmesi gereken ortamlarda yedekleme işlerinin tümünün tam yedek olarak belirlenmesi her zaman mümkün değildir. Diğer yandan, tam yedekleme bilginin geri döndürülme ihtiyacı ortaya çıktığında orijinal verinin tamamını içerdiğinden başka yedekleme işlerine ihtiyaç duymadan kullanılabilecek bir yöntemdir. Tam yedekleme diğer bütün yedekleme türleri için bir başlangıç noktası olarak düşünülmelidir.

Fark yedekleme: Başarılı olarak sonlandırılmış en son tam yedeğe göre değişikliklerin yedeklenmesidir. Sadece en son alınan tam yedeğe göre farkın yedeklenmesi nedeni ile tam yedeklemeye göre daha hızlıdır ve yedekleme medyası üzerinde daha düşük alan işgal etmektedir. Fark yedeklemede her zaman en son tam yedeğe göre fark alındığı için yedeklenen veri miktarı sürekli artmaktadır. Belirli aralıklarla tam yedek alınması fark yedeklemesi sırasında yedeklenecek veri miktarını düşürmektedir. Verinin geri döndürülmesi gerektiğinde fark yedeğe ek olarak tam yedeğe de ihtiyaç vardır. Geri döndürme sırasında iki yedeğinde kullanılması nedeni ile tam yedeğe göre daha yavaş bir yedekleme türüdür.

Artan yedekleme: Başarılı olarak sonlandırılmış en son yedeğe göre değişen bilgilerin yedeklenmesidir. En son yedeğin tam, fark veya artan olmasının önemi yoktur. Sadece en son değişikliklerin yedeklenmesi nedeni ile yedekleme işinin tamamlanma süresi kısadır. Yedekten geri döndürme işlemi gerektiğinde tam yedek ve arada alınmış bütün artan yedeklere ihtiyaç vardır. Bu sebeple düşük geri döndürme hızına sahiptir. Ayrıca birçok yedekleme işinde alınan verilerden geri döndürme işi yaptığından geri döndürme başarısı diğer türlere göre düşüktür[19].



Şekil 22. Veri yedekleme türleri

Her yedekleme türünün avantaj ve dezavantajları vardır. Tam yedekleme türünün geri döndürme hızı çok yüksek iken yedekleme hızı düşüktür ve her yedekleme işi için orijinal veri alanı kadar yer ayırmak gerekmektedir. Bu sebeple yedekleme işlerinin tamamı için tam yedekleme yapmak her zaman tercih edilen bir yöntem değildir. Öbür yandan artan yedekleme çok hızlı gerçekleştirilebilmesine rağmen verinin geri döndürülmesi sırasında çok sayıda yedekleme işinin çalıştırılmasına ihtiyaç duymaktadır. Bu tür nedenlerle yedekleme işlerinin gerçekleştirilmesi sırasında bu seçenekler genellikle beraber kullanılmaktadır. Hafta sonu tam yedek, hafta içi fark yedek ve mesai saatleri içerisinde artan yedek almak beraber kullanıma örnek olarak verilebilir.

Tablo 4. Yedekleme türlerinin karşılaştırılması

Yedekleme Türü	Geri Döndürme Hızı	Yedekleme Hızı	Depolama Alanı Kullanımı
Tam	En Yüksek	En Düşük	En Yüksek
Fark	Orta	Orta	Orta
Artımlı	En Düşük	En Yüksek	En Düşük

3.2. Sayısal Veri Kurtarma Yöntemlerinin İncelenmesi

Veri kurtarma ile ilgili en önemli nokta kurtarma işlem sürecindeki veri kaybı olan ortamın mevcut durumunun korunması ve ek hasar oluşturulmamasıdır. Bu nedenle yapılan veri kurtarma çalışmalarında konuya gereken özenin gösterilmesi gerekmektedir.

3.2.1. Yazılım Tabanlı Veri Kurtarma Yöntemi

Yazılımsal olarak veri kurtarma işlemleri, veri kurtarma için özel geliştirilmiş programlar kullanılarak gerçekleştirilmektedir. Bu çalışmada veri kurtarmada ve adli bilişimde sık kullanılan programlardan bazıları tanıtılmıştır. Otomatik veri kurtarma programlarının başarılı olabilmesi için dosya ve klasör adlarının ve özelliklerinin hasar görmemiş olması gerekir, dosyalar birden fazla kümeden oluşuyorsa kümeler ardışık olmalıdır, klasör kümeleri parçalanmamış olmalıdır, veri kurtarma programı ortamdaki yapıyı ve parametreleri doğru çözümlemelidir manyetik plaka yüzeylerinde hasar olmamalıdır. Veri kurtarma süresi hasarın durumuna ve verilerin çokluğuna göre değişebilmektedir. Dosya sistemi yapı hasarları genellikle kısa sürmektedir. Formatlanmış disklerden verileri toplamak ve silinmiş dosya gruplarını doğru şekilde elde etmek genellikle daha uzun zaman almaktadır. Fiziksel hasarlarda özellikle veri plakalarındaki kapsamlı hasarlarda işlem genellikle uzun sürmektedir.

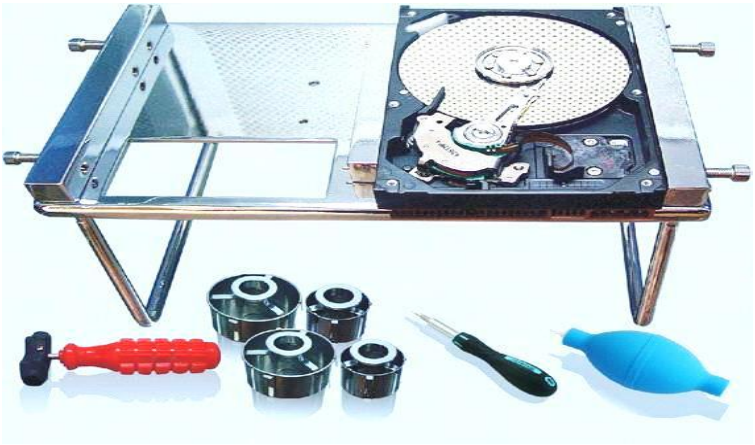
Veri depolama ortamlarının organizasyon yapısında genellikle veri alanı ve sistem alanı olarak tabir edilen iki ana kısım bulunmaktadır. Sistem alanı genel olarak açılış yapısı, dosya tanımları ve dosyaların veri alanındaki adreslerini içerir. Veri alanı ise dosyaları ve alt tanımlama guruplarını içerir. Dosyalara erişme durumunda sistem alanındaki tanım ve adresler hayati öneme sahiptir. Bu yapılar silindiğinde veya bir hasara maruz kaldığında veri depolama ortamındaki dosya ve klasörlere standart işletim sistemi araçlarıyla ulaşılamaz. Eğer veri alanında depolanmış dosyalar hasar görmemiş, sadece sistem alanındaki dosyalar hasar görmüşse sistem alanını onarmak çoğu zaman veri depolama ortamındaki mantıksal düzenlemenin eski haline gelmesi anlamına gelir. Bu

durumda ilk olarak sistem alanı kontrol edilmeli ve hasar buradaysa giderilerek sistem eski haline getirilmelidir. Dosyalara ait iki temel bilgi vardır; birincisi dosyanın ad, özellik ve başlangıç yerini içeren tanımlama bilgisidir. İkincisi ise eğer dosya birden fazla kümeye yerleştirilecek büyüklükte ise veri alanında yerleştirildiği küme yer bilgileri ile oluşturulan küme zinciri bilgisidir. Manyetik veri depolama ortamları genellikle random mantıkla esnek olarak kullanılmaktadır. Bu da dosyalara ait kümelerin veri alanında ardışık olmayan bir şekilde yerleştirilmesini gerektirir ve böylece dosyalar küme bazlı parçalanmış olur. Dosyaya ait küme zinciri mevcut olmadığında hangi kümenin hangi dosyaya ait olduğuna otomatik olarak karar vermek çoğu zaman imkansız olduğu için bu işlem manuel olarak yapılır. Dosyaya ait tanım bilgisinin olmadığı durumlarda ise ancak dosya başlangıcındaki header ile bir tahminde bulunmak durumunda kalınır ki bu zaman alıcı bir yöntemdir.

3.2.2. Donanım Tabanlı Veri Kurtarma Yöntemi

Veri depolama ortamlarını ortam+aygıt (tek parça) ve sadece ortam (okuyucu aygıt ayrı bir birim) şeklinde sınıflayabiliriz. Bu sınıflamada hard diskler ve flash bellekler birinci gruba girmektedir . Diğer grupta ise verilerin depolandığı ortam ile bunu işleyen aygıt ayrıdır. Disketler ve disket sürücüler, CD/DVD ve okuyucu/yazıcı aygıtları, manyetik bantlar ve okuyucu/yazıcı aygıtları gibi. Hard diskte verilerin depolandığı plakalar özel bir muhafazada korunmuştur ve verilere özel bir kart ve özel elemanlar (motor, magnet, okuma/yazma kafaları) ile erişilmektedir. Özellikle günümüzde üretilen hard disklerde erişim ve okuma/yazma işlemleri kompleks yazılım donanım bileşenlerinden oluşmaktadır. Bu bileşenlerdeki hasarlar ve sorunlar diskin erişilemez veya kısmen okunamaz hale gelmesine neden olmaktadır. Hard disklerde fiziksel erişimi kontrol edebilmek amacıyla şifre verilebilmektedir. Bu şifre verilerin işlendiği plakalarda kullanıcı sektörlerinin dışındaki özel bir alanda depolanmakta ve diskin fiziksel başlatılması aşamasında sorgulanarak disk kullanıma açılmakta ya da erişime kapanmaktadır. Bu sistem genellikle dizüstü bilgisayarlarda ve resmi kurum bilgisayarlarında kullanılmaktadır. Hard disk şifresinin çözülmesi özel bir konudur. Hard diskler elektronik kart ve gövde olmak üzere iki temel kısımdan oluşmaktadır. Elektronik kartın arızalanması halinde kartın tamiri veya eşdeğerinin temini disk gövdesine erişimi mümkün kılacaktır. Ancak bu tür durumlarda disk gövde elemanlarının da hasar görebileceğinden dolayı disk gövdesinde hasar olup olmadığını tespit etmek önemlidir. Sorun gövde elemanlarındaki hasarlardan veya dâhili alt seviye kontrol kodlarından kaynaklanmışsa hard disk gövdesinin açılması gerekebilir.

Bu aşama tozsuz oda(clean room) ortamında özel araçlarla ve uzman kişiler tarafından gerçekleştirilir. Arızalı hard diskin gövdesi aynı marka ve model eşdeğer başka bir diskin gövdesi ile değiştirilir. Okuma/yazma kafası çıkarılırken ve yerleştirilirken plaka yüzeyinin hasar görmemesi için dikkat edilmesi gerekir.



Şekil 23. Hard disk açma ve parça değiştirme seti

Son yıllarda data yedeklemesi ve taşıması için kullanılan flash disk diye bilinen ürünlerin ani voltaj değişikliğinden dolayı bozulma vakalarına sıkça rastlanmaktadır. Flash belleklerden veri kurtarmak için iki yöntem kullanılmaktadır. Biri bu diskleri tamir etmek suretiyle datayı kurtarma yöntemidir. Ancak bu metot parça sıkıntısı nedeniyle oldukça zaman alıcı bir yöntemdir. Diğeri geliştirilen flash disklerden data kurtarma cihazı FDRE (Flash Disk Data Recovery Equipment) sayesinde artık flash diski tamir etmeden, direkt olarak flash çipin kendisinden datayı almaya yarayacak cihaz geliştirilmiştir (Şekil 22). Flash çipinin üzerinde bulunduğu PCB den ayrılarak FDRE cihazına bağlanması sayesinde içindeki veriyi bilgisayar ortamına aktarılır. Bu cihazla (FDRE) ile birlikte geliştirilen program sayesinde flash çip içerisindeki data çeşitli evrelerden geçerek bilgisayar ortamına çevrilip, kişinin daha önce kullandığı ve oluşturduğu dizin yapısı halinde tekrar geri kazanılmaktadır[20].

Şekil 24. Flash bellek çipi

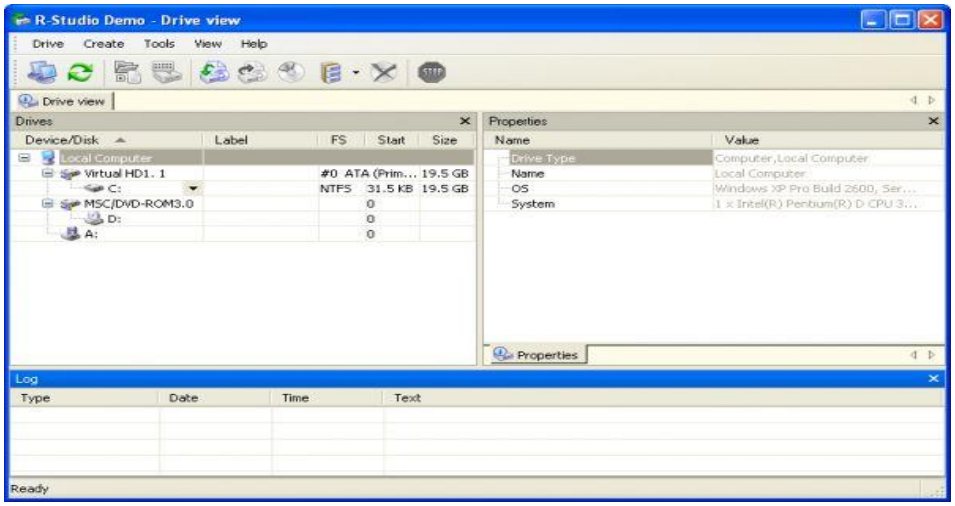
Bozulmuş veya çizilmiş CD/DVD'lerden veri kurtarmak için sık kullanılan bazı pratik yöntemler vardır. Ancak, yazılımsal olarak bu iş için geliştirilmiş programlar da bulunmaktadır. Çizilmiş CD'lerdeki verilere erişimi kolaylaştırmak için genellikle CD temizleme setleri kullanılır. Bunların içinde özel temizleyici sıvı jeller bulunmaktadır. CD'lerin en önemli özelliği manyetik disklerden farklı olarak spiral şeklinde tek bir izden oluşmalarıdır. Spiral yapı CD'nin iç kısmından dış kısmına doğru ilerlemektedir. Bu yapıdan dolayı spiral izlere dikey çiziklerden çok paralel çizikler daha fazla veri kaybına neden olmaktadır. Dolayısıyla CD temizlenirken dairesel çizikler oluşturmamaya dikkat edilmelidir. Kırık CD'den veri kurtarma diğer bir yöntemdir ve özel bazı cihazlara ihtiyaç vardır. Kırık medya dağılmamışsa iki parçası bir araya getirilip etiketlenerek düzleştirilirse CD çalıştırılabilir. Bu yolla çalıştırılmazsa kırılan yerden lazerle hasarlı kısım bir dilim şeklinde kesilip çıkarılır. Daha sonra aynı ölçülerde sağlam boş bir CD camı aynı ebatta bir dilim lazerle kesilerek önceki CD' deki çıkarılan dilimin yerine yerleştirilir. Camın aka yüzüne aynalarda kullanılan gümüş kaplamalı etiket yapıştırılıp düzleştirilir. Herhangi bir pürüz ve seviye farkının kalmamasına dikkat edilerek bu işlem tamamlanır. Bu yöntemle CD'deki verinin tamamı olmasa da önemli bir kısmı kurtarılmış olur. Özellikle resim dosyaları için bu yöntemin başarımı yüksektir.

3.3. Sayısal Veri Kurtarma Yazılımlarının İncelenmesi

Veri kurtarma işlemlerinin yazılımlarla yapılabilmesi için özel geliştirilmiş programlar kullanılmaktadır[21]. Bu programlardan veri kurtarmada ve adli bilişimde sık kullanılan programlardan bazıları bu bölümde incelenmiştir.

3.3.1. R-Studio Yazılımı

R-Studio; virüsler, kötü niyetli saldırılar ve donanım ya da sistem çökmeleri sonucu kaybolan verileri geri getirebilmesi ile ünlü, kapsamlı bir veri kurtarma programıdır. FAT/NTFS (Windows), HFS/HFS+ (Mac), UFS1/UFS2 ve Ext2FS/3FS dosya sistemlerini destekleyen program, disk bölümleri biçimlendirilmiş, hasar görmüş ya da silinmiş olsa dahi veri kurtarma yapabilmektedir. Dinamik Diskler ve RAID disklerde veri kurtarma işlemi gerçekleştirebilen R- Studio ayrıca şifrelenmiş ve sıkıştırılmış dosyaları da geri getirebilmektedir.

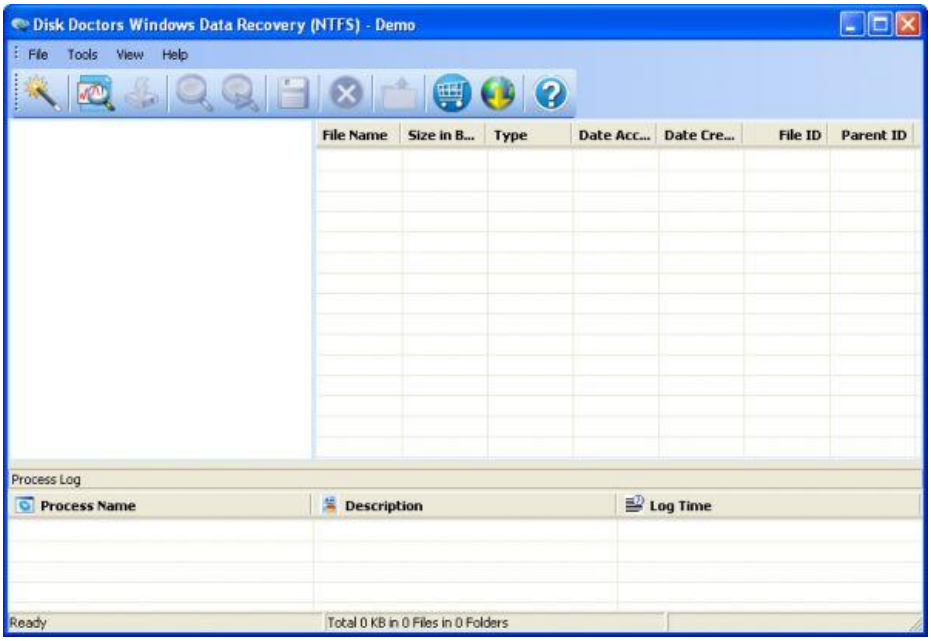


Şekil 25. R-Studio ara yüzü

Derinlemesine analiz yaparak depolama birimlerindeki kayıp verileri bulabilen R-Studio, bulunan dosyalar ile ilgili geniş bilgiler vermekte ve dosyaları ön izleyerek geri getirilmek istenenleri kurtarma olanağı vermektedir. Güçlü analiz özelliği sayesinde her türlü dosya sistemini detaylı bir şekilde tarayabilen programın tarama süresi biraz uzun olabilir ancak sonuçlar göz önüne alındığında buna değdiği görülüyor. Depolama birimlerindeki silinmiş ya da biçimlendirme, kötü niyetli saldırı veya çökme sonucu erişilemez hale gelmiş veriler R-Studio ile kolayca geri getirebiliyor. Program ayrıca herhangi bir donanım hatasından şüpheleniyor ya da sabit disk sürekli "bad sector" hatası veriyor ise kullanılabilen bir disk görüntüsü alma seçeneği sunuyor. Bu işlev sayesinde diskin birebir kopyası oluşturulabilir ve ciddi bir donanımsal sorun karşısında kurtarma işlemi bu görüntü dosyası üzerinden gerçekleştirilebilir.

3.3.2. Disk Doctors Windows Data Recovery Yazılımı

Disk Doctors Windows Data Recovery, diğer veri kurtarma programlarının geri getiremediği ve hatta görüntüleyemediği dosyaları bulabilmeyi taahhüt etmektedir. Sahip olduğu TurboScan ve File Tracer teknolojileri ile en başarılı veri ve disk bölümü kurtarma çözümlerinden birisidir. Disk Doctors Windows Data Recovery; sabit disklerden, USB Flash belleklerden, harici disklerden ve bellek kartlarından dosya kurtarabilmektedir.



Şekil 26. Disk doctors windows data recovery ara yüzü

FAT ve NTFS dosya sistemleri için kullanabilecek iki program olarak gelen Disk Doctors Windows Data Recovery, basit, turbo ve dosya izleme olmak üzere üç farklı tarama yapabilmektedir. Standart bir tarama yapan basit taramanın yanı sıra daha derinlemesine bir tarama yapan turbo tarama ve istenen dosya türlerine göre arama yapabilen dosya izleme ile kayıp verileri bulma olasılığı yükseliyor. Sihirbaz yardımı ile tarama işlemlerini adım adım gerçekleştirebilmeye olanak veren program, kolaylıkla kullanılabiliyor. Disk Doctors Windows Data Recovery, ayrıca depolama birimlerinin görüntüsünü (imaj) alma ve bu görüntü dosyalarını kullanarak veri kurtarabilmektedir.

3.3.3. EASEUS Data Recovery Wizard Yazılımı

EASEUS Data Recovery Wizard; Geri Dönüşüm Kutusundan boşaltılan ya da disk bölümü hasarı, sistem çökmesi, virüs saldırısı gibi nedenlerle silinen dosyaları geri getirebilen bir veri kurtarma programıdır. Sabit disk, RAID, USB flash bellek ve hafıza kartları gibi depolama birimlerindeki kayıp, silinmiş ya da hasar görmüş dosyaları kurtarabilen program, FAT12, FAT16, FAT32, NTFS dosya sistemleri üzerinde çalışabilmektedir.

Şekil 27. Easeus data recovery wizard ara yüzü

Etkili kurtarma işlemleri gerçekleştirebilen ve kullanımı oldukça kolay olan EASEUS Data Recovery Wizard, açılışta kullanıcıya Deleted File Recovery, Complete Recovery ve Partition Recovery olmak üzere üç seçenek sunmaktadır. Deleted File Recovery seçeneği ile yanlışlıkla silinen dosyaları geri getirebiliyorken Complete Recovery seçeneği ile dosya sistemi çöken ya da biçimlendirilen disklerdeki tüm verileri geri getirebilmektedir. Partition Recovery seçeneğini kullanarak ise silinen ya da kaybolan sabit disk bölümlerini kurtarabiliyor. Program, tarama sonucu bulunan dosyaları ağaç görünüm şeklinde listeliyor ve detaylı filtrelemeler ile istenen dosyaları kolayca bulabilme imkânı veriyor. Ayrıca hem resim dosyaları hem de Word ve Excel dosyaları için geçerli olan önizleme özelliği sayesinde dosyaları, kurtarma işlemi öncesi önizleme imkânı vermektedir.

3.3.4. VirtualLab DataRecovery Yazılımı

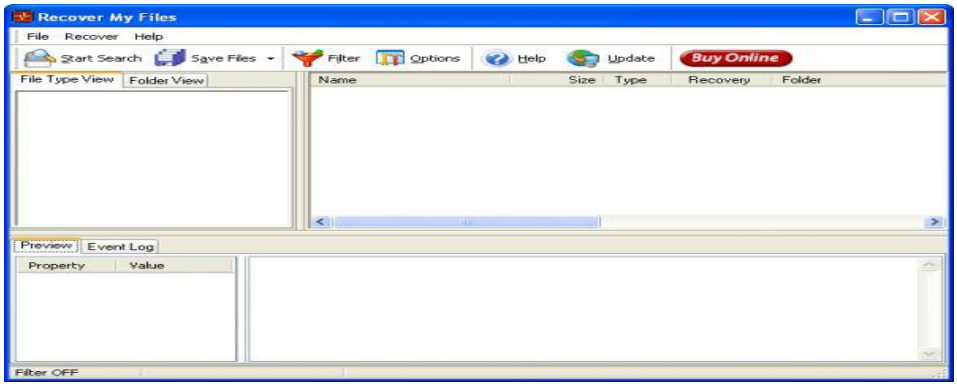
VirtualLab DataRecovery, sabit diskler, CD ve DVD'ler, RAID, flash bellek, hafıza kartı ve Mac disk bölümleri gibi depolama teknolojilerinin yanı sıra FAT 12/16/32, NTFS, NTFS5 (VISTA), NSF, Mac HFS/HFS+ ve Ext2FS dosya sistemlerini desteklemektedir.

Şekil 28. Virtuallab data recovery ara yüzü

VirtualLab Data Recovery ile hasar gören ya da silinen disk bölümlerini, yanlışlıkla silinen dosyaları, Mac HFS ve HFS+ disk bölümlerini, Outlook Express ve Mozilla Thunderbird programlarında silinen e-postaları, silinmiş ya da okunamayan CD ve DVD'lerdeki dosyaları ve hafıza kartlarından silinmiş fotoğrafları geri getirebilmektedir. Geniş kullanım alanına sahip olan programın ara yüzü oldukça kullanışlıdır. Göze hitap eden ve kayıp verileri hızlı bir şekilde aramaya olanak veren bu ara yüz sayesinde veri kurtarma konusunda deneyimsiz olan kullanıcılar dahi programı kullanmakta zorluk çekmezler. VirtualLab Data Recovery; PC Disk Bölümlerini Kurtarma, Silinen Dosyaları Kurtarma, Mac Disk Bölümlerini Kurtarma, E-postaları Kurtarma, CD/DVD-ROM Kurtarma ve Fotoğraf Kurtarma modüllerinden biri seçildiğinde hızlı bir şekilde tarama yaparak kayıp verileri bulup verilerin durumlarını görüntüleyebilmektedir.

3.3.5. Recover MyFiles Yazılımı

Recover MyFiles, silinen dosyaları ve biçimlendirilmiş ya da hasar görmüş sürücülerdeki verileri geri getirebilen gelişmiş bir veri kurtarma programıdır. Sabit diskler, dijital fotoğraf makineleri, USB Flash bellekler ve hafıza kartları üzerinde veri kurtarma işlemi gerçekleştirebilen program, Word, Excel, PowerPoint, Outlook, AutoCAD, Money, QuickBooks, SQL, MPEG, AVI, MP3 ve e-posta ve fotoğraf dosyaları dahil 350'den fazla dosya türünde veri kurtarma yapabilmektedir. Program ile veri kurtarmak oldukça kolaydır ve herhangi teknik bir bilgi gerekmiyor. Recover MyFiles ayrıca kurtarılan verileri doğrudan optik disklere yazdırabilen bir CD/DVD yazdırma işlevi içermektedir.



Şekil 29. Recover myfiles ara yüzü

Bir sihirbaz yardımı ile kolayca tarama yapmaya olanak veren Recover My Files, özellikle aranan dosyaların türü seçiminde oldukça geniş olanaklar sunuyor. Recover My Files, altı ana kategorideki onlarca dosya türünü seçme olanağı tanıyor. Dosya türü dışında dosya adı ve uzantısı, dosya boyutu, dosyanın oluşturulma/değiştirilme/son erişilme tarihlerine ve anahtar kelimeye göre filtrelemeler de yapabilen program, böylece yalnızca aranan dosyaların bulunmasını ve veri kurtarma işlemini daha hızlı bir şekilde tamamlanabilmesini sağlamaktadır. Recover My Files, arama sonuçlarının listelendiği ekranda, dosyalar ile ilgili geniş bilgiler vermenin yanı sıra bu ekranın alt kısmında dosyaların ön izlemesini de görüntülemektedir.

3.3.6. Digital Rescue Premium Yazılımı

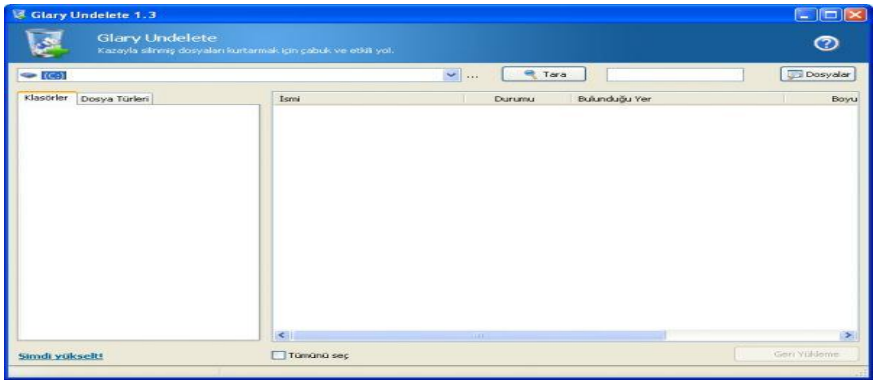
Digital Rescue Premium, kazara silinen dosyaları geri getirebilen etkili bir programdır. Önemli ofis belgelerini, e-postaları, fotoğrafları, müzikleri, videoları veya farklı türlerdeki dosyaları kurtarabiliyor. FAT 16, FAT 32 ve NTFS gibi yaygın olarak kullanılan dosya sistemlerini destekleyen Digital Rescue Premium, sabit disklerde, harici disklerde, USB Flash belleklerde ve hafıza kartlarında veri kurtarma işlemleri gerçekleştirebilmektedir.

Şekil 30. Digital rescue premium ara yüzü

Digital Rescue Premium, açılışta üç seçenek sunuyor: Recover Lost Files, Recover Lost Email ve Permanenetly Delete Data. Recover Lost Files seçeneği, mevcut depolama birimlerini tarıyor ve bulunan dosyaları geri getirebilmektedir. Program, bulunması istenen dosyaların türlerini, ismini ve son düzenlenme tarihini belirleme olanağı sağlıyor. Recover Lost Email seçeneği ile e-posta veritabanlarını tarıyor ve silinmiş olan e-postaları geri getirebiliyor. Son seçenek olan Permanenetly Delete Data ise tıpkı Recover Lost Files seçeneğinde olduğu gibi depolama birimlerini tarıyor ve belirlenen türde yine belirlenen isim ya da düzenleme tarihine sahip dosyaları buluyor. Ancak bu kez bulunan dosyalar, geri getirilmek yerine kurtarılamayacak şekilde siliniyor. Böylece önemli ve gizli verilerin başkalarının eline geçmesi önlenmiş oluyor.

3.3.7. Glary Undelete Yazılımı

Glary Undelete; FAT ve NTFS dosya sistemlerinde silinen dosyaları geri getirebilen ücretsiz ve kullanımı kolay bir veri kurtarma programıdır. Bu program, Geri Dönüşüm kutusundan, Komut İsteminde ya da Shift tuşu yardımı ile doğrudan silinen dosyaları geri getirebiliyor. Hatta Glary Undelete virüsler ya da sistem çökmeleri nedeniyle silinen dosyaları bile kurtarabilmektedir. FAT, FAT16, FAT32, NTFS, NTFS5, NTFS + EFS dosya sistemlerini destekleyen program ayrıca CompactFlash, SmartMedia, MultiMedia ve Secure Digital hafıza kartlarındaki silinmiş fotoğrafları kurtarabilmektedir.

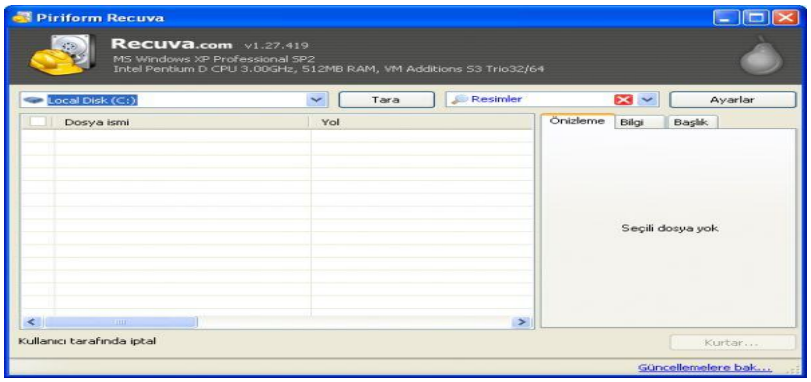


Şekil 31. Glary undelete ara yüzü

Basit bir ara yüze sahip olan program, seçilen depolama biriminde tarama yapıp daha önce silinmiş olan dosyaları bulup listeleyebiliyor. Ön izleme imkânı bulunmayan dosya listeme ekranı, bulunan dosyaların durumlarını, türlerini ve boyutlarını görüntüleyebiliyor. Programın dosyaların ön izlemesine olanak vermemesi, kurtarılacak olan dosyaların belirlenmesini zorlaştırmasına rağmen dosyaların durumlarını göstermesi, hangi dosyanın kurtarılma olasılığının ne olduğunu görmeyi sağlamaktadır.

3.3.8. Recuva Yazılımı

Okunuşu İngilizce "recover" kelimesi ile aynı olan Recuva, yanlışlıkla silinen dosyalarını geri getirebilen ücretsiz bir Windows aracıdır. Program, Geri Dönüşüm Kutusundan silinenler dosyaların yanı sıra fotoğraf makinelerinin hafıza kartlarından ya da MP3 oynatıcılardan silinen dosyaları da geri getirebilmektedir. Hatta program, kötü niyetli yazılımlar ya da sistem çökmeleri nedeniyle kaybolan dosyaları da kurtarabilmektedir.



Şekil 32. Recuva ara yüzü

Program açılışında sihirbaz, dosya türünü, dosya konumunu ve arama derinliğini belirleyerek hızlı bir şekilde tarama yapabiliyor. Program tarama sonrası bulunan dosyaları listeliyor ve seçilen dosyaları kurtarabilmeyi mümkün kılıyor. Ayrıca programın gelişmiş kipine geçerek daha detaylı taramalar yapılabilir. Program bulunan dosyaların ön izlemesini ve bilgilerini görüntüleyebilmektedir.

3.3.9. Veri Kurtarma Programları Karşılaştırma Tablosu

Yukarıda özellikleri anlatılan otomatik veri kurtarma yazılımları, destekledikleri dosya ve işletim sistemleri ile veri kurtarma özellikleri aşağıda tablo 5'te gösterilmiştir.

Tablo 5. Program karşılaştırma tablosu

	R-Studio	Windows Data Recovery	Data Recovery Wizard	VirtualLab Data Recovery	Recovery My Files	Digital Rescue	Glary Undelete	Recuva
İşletim Sistemleri								
Vista	✔	✔	✔	✔	✔	✔	✔	✔
Xp	✔	✔	✔	✔	✔	✔	✔	✔
2000	✔	✔	✔	✔	✔	✔	✔	✔
Mac	✔			✔				
Linux	✔							
Dosya Sistemleri								
NTFS5	✔	✔	✔	✔		✔	✔	✔
NTFS	✔	✔	✔	✔	✔	✔	✔	✔
FAT32	✔	✔	✔	✔	✔	✔	✔	✔
FAT16	✔	✔	✔	✔	✔	✔	✔	✔
FAT12	✔		✔	✔	✔		✔	✔
Veri Kurtarma Özellikleri								
E-posta kurtarma		✔		✔	✔	✔		
Disk Görüntüsü	✔	✔	✔					
Sıkıştırılmış Dosya	✔	✔	✔	✔	✔	✔	✔	✔
Şifreli Dosya	✔	✔	✔	✔	✔	✔	✔	✔
Ağ Desteği	✔							
Veri Kurtarma Alanları								
Geri Dönüşüm Kutusu	✔	✔	✔	✔	✔	✔	✔	✔
Hasarlı Dosyalar	✔	✔	✔	✔	✔	✔	✔	✔
Biçimlendirme (Format)	✔	✔	✔	✔	✔	✔	✔	✔
Virüs/Çökme	✔	✔	✔	✔	✔	✔	✔	✔
Silinen Disk Bölümü	✔	✔	✔	✔	✔		✔	

3.4. Adli Bilişimde Kullanılan Yazılımların İncelenmesi

Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci olarak tanımlanabilir. Bu yönüyle adli bilişimin hukuki boyutundan ziyade, teknik yönü ön plana çıkmaktadır. Zira elektronik sistemlerdeki bulguların, bunlardan ayrıştırılarak birer hukuki delile dönüştürülme süreci, oldukça zahmetli, son derece teknik bilgi gerektiren ve uzmanlık

isteyen bir iştir. Adli bilişimin çalışma alanlarının genişlemesiyle adli bilişim analiz yöntemlerinin amacı yalnızca ceza davalarına delil sağlamak olmaktan çıkmış, hukuk uyuşmazlıklarında hatta şirketlerde de kullanılır olmuştur. Özellikle büyük şirketler, bugün veri kurtarma ya da veri imha etme gibi esasen adli bilişimi yakından ilgilendiren konularda bu bilim dalına başvurmakta; giderek adli bilişim uzmanlarını bünyelerinde çalıştırmaktadır. Adli bilişim açısından elektronik delil (e-delil), bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir. Dijital deliller, klasik delillerden farklılık arz eder. Klasik deliller, gözle görülebilen, üzerinde el koyma, muhafaza altına alma kararı verilerek kolayca götürülebilen deliller iken; dijital deliller, bu kadar somut bir yapıya sahip değildir. Elbette ki dijital deliller de bir donanıma ihtiyaç duyar. Bir dijital delilin içerisinde bulunduğu bir donanım aygıtı mutlaka vardır. Ancak asıl önemli olan, bu donanım aygıtı içerisindeki e-delillerdir. Sayısal delillerin mutlaka bir elektronik donanım içerisinde bulunabilir yapısı, klasik delillerden ayrıldığı bir noktadır. Zira klasik deliller, herhangi bir yerde olabilir. Yine bir başka farklılık olarak; bir suça ilişkin delillere herhangi bir şekilde ulaşmak mümkün olabilir iken, dijital deliller, birtakım teknik inceleme ve analiz yöntemlerine başvuru zorunluluğu doğurmaktadır. Dolayısıyla dijital delilin elde edilmesi klasik delillere nazaran çok daha zordur. Ayrıca, dijital deliller çok çabuk bozulabilmekte, değiştirilebilmekte, kaybolabilmekte ve hatta yok edilebilmektedir. Sayısal delilin içerisinde mevcut olabileceği en önemli elektronik donanım bilgisayardır. Bilişim denince akla ilk gelen donanım bilgisayardır. Öyle ki, bilgisayarın olmamasının, bugünkü anlamda bilişimin ve bilişim hukukunun olmaması anlamına gelebileceğini söylemek çok da yanlış bir kanı olmayacaktır. Bilgisayar, adli bilişim açısından da hem içerisinden delil elde edilen hem de delil elde etme metotlarında kullanılan bir araç olması nedeniyle çok önemlidir. Bilgisayar vasıtalı suçlarda bırakılan izler, bilgisayarların incelenmesinde ortaya konulabilmekte; yargılamada kullanılabilecek bir yasal delil haline getirilmektedir. Bilgisayardaki deliller, hard disk denilen depolama ünitesinde, çalışır konumda bulunan bir bilgisayarın önbelleğinde (RAM) bulunabilir. Bilgisayarlar, bugün ulaştıkları oldukça geniş kapasitelerine bağlı olarak, çeşitli videolar, müzik dosyaları (mp3 vb.), fotoğraflar, çeşitli doküman dosyaları, grafikler içerebilirler ve bunların her biri ihtiyaç duyulmakta olan çok önemli bir delil olabilir. Bilgisayar ve bilgisayarları birbirine bağlayan internet ağının bugünkü geldiği nokta, deliler bağlamında bilgisayara ayrı bir önem atfetmektedir. Bir bilişim suçlusunun yerinden kalkmadan dünyanın diğer ucunda suç işliyor oluşu,

internetin de adli bilişim açısından önemini arttırmaktadır. Bilgisayarda yer alan deliller hard disk üzerinde bulunmaktadır. Yukarıda saydığımız, dijital delil konusu olabilecek tüm verilere ilaveten önbellek (RAM) kayıtları, sistem kayıt dosyaları, çeşitli zararlı bilgisayar yazılımları (virüs, solucan, spy vs.) da delil olarak bilgisayarda mevcut olabilir. Delil incelemesi yapılacak bilgisayar, bir internet sunucusu ise içerisinde barındırdığı web sitelerinin kayıtları ve bu sitelerde yayınlanan tüm dosyalar/bilgiler de bu bilgisayarlarda bulunur ve delil teşkil edebilir[22-35].

Adli bilişimde kullanılan yazılımları, ana hatlarıyla ticari ve ücretsiz/açık kaynak kodlu yazılımlar olarak iki grupta incelemek mümkündür. Her iki grupta da yüzlerce yazılım olmasına karşın, kabul görmüş bazı yazılımlar, güvenirliğinin de ispatlanmış olması nedeniyle mahkemelerde kabul görmektedir. Adli bilişimde kullanılan yazılımların taşıması gereken özellikler bulunmaktadır. Bunlar; dijital delillerin elde edilmesi işlemleri esnasında, veriler üzerinde değişikliğe neden olmamalıdır. Sadece elde edilmek istenen verilerin toplanmasına olanak sağlamalıdır. Adli bilişim çevresinde kabul görmüş ve güvenirliğini ispat etmiş olmalıdır. Elde edilen bulgu ve sonuçların her zaman tekrar edilebilir olmalıdır

3.4.1. Ticari Yazılımlar

Bu alanda en çok bilinen Encase, FTK(Access Data Forensics Tool Kit) ve X-Ways Forensic gibi yazılımlar, inceleme konusu elektronik delil üzerinde tutarlı ve tekrar edilebilir sonuçlar verdiği için ticari yazılımlar arasında ön plana çıkmışlardır[36]. Ticari yazılımlar, ücretsiz yazılımlara oranla daha fonksiyonel ve gelişiminin daha hızlı olması nedeniyle daha kullanışlıdır. Bunun bedeli olarak yüksek fiyatla satılmakta ve güncellenmektedirler. Başlıca avantajları arasında, kolay temin edilebilir olması, fazla eğitim almadan temel fonksiyonlarıyla kullanılabilir ara yüze sahip olmaları, birçoğunun arkasında danışılabilecek bir şirket veya sertifikalı eğitim programının olması, sonuçları herkesin anlayabileceği ve yorumlayabileceği açıklıkta sunmaları ve büyük bölümünün Windows işletim sistemi üzerinde çalışması sıralanabilir. Dezavantajları ise, maliyetinin yüksek olması, kodların açık olmaması nedeniyle yazılımda kullanıma bağlı olarak değişiklik yapmanın mümkün olmaması gibi problemlerdir.

Encase: En popüler adli bilişim yazılımlarından biridir. Bire-bir disk kopyası oluşturma, analiz ve raporlama aşamalarının tümünde kullanılabilen ve güvenilirliği en fazla olan

yazılımlardan biridir. Encase hemen hemen tüm dosya sistemlerini tanıyan, birçok imaj formatı ile uyumlu ve RAID sistemlerini destekleyen Windows tabanlı bir yazılımdır.

Access Data Forensics Tool Kit: Adli bilişimde kullanılan ikinci en popüler yazılımdır. Encase üzerinde bulunmayan bazı fonksiyonlara sahip olduğu gibi, kullanımının daha kolay olması nedeniyle de adli bilişim uzmanları tarafından tercih edilmektedir. Bu program da adli bilişimin tüm aşamalarında(imaj alma, analiz, raporlama) kullanılmaktadır. FTK, Encase'e oranla daha düşük maliyete sahip olmakla birlikte, imaj almak için kullanılan programı(FTK Imager) ücretsiz dağıtılmaktadır.

Paraben: Paraben tarafından geliştirilen adli bilişim yazılımları tek olarak bulunabildiği gibi paket olarak da dağıtılmaktadır. Paraben yazılımlarının fiyatı FTK ile aynı seviyelerde olmakla beraber, paket içinde bulunan cep telefonları ve cep bilgisayarlarının incelenmesine yönelik yazılımlarla bu alanda ön plana çıkmaktadır.

3.4.2. Açık Kaynak Kodlu Yazılımlar

Adli bilişim alanında kullanılan ticari yazılımların yanı sıra, bu alanda kendini ispatlamış ve popüler hale gelmiş açık kaynak kodlu yazılımların sayısı da küçümsenmeyecek kadar çoktur. Özellikle bu grupta yer alan Autopsy, Sleut Kit ve Helix gibi yazılımlar, resmi nitelikte adli inceleme yapan kurum ve kuruluşlar tarafından da kullanılmaktadır. Bu tür ücretsiz ve güvenilir yazılımlar, bazen ticari yazılımlardan elde edilen sonuçları doğrulamak ve desteklemek amacıyla da tercih edilmektedir.

Açık kaynak kodlu yazılımlar internet üzerinden kolaylıkla indirilebilen ve kurulabilen bir yazılım veya başlatılabilir CD halinde olabilmektedir. Fakat açık kaynak kodlu yazılımların kullanım zorluğunun daha fazla olması nedeniyle, bu konuda deneyimli olmak gerekebilmektedir. Ucuz veya ücretsiz olması, kolay temin edilebilir olması, lisans gereksinimi olmaması, popüler olanlarının adli bilişim alanında doğruluğunun ve güvenirliğinin ispatlanmış olması, farklı işletim sistemlerine yönelik uygulamaların bulunması ve üzerinde kişiye özel değişikliklerin yapılabilmesi, açık kaynak kodlu yazılımların avantajları arasında sıralanabilir.

Linux dd: Linux dd, tüm Linux işletim sistemleri üzerinde bulunan bir programdır/komuttur. Bu komutla veriyi kaynaktan hedefe blok halinde kopyalama işlemi yapılabilir. İmaj almak için kullanılan ticari ya da açık kaynak kodlu tüm yazılımların temelinde "Linux dd" komutu vardır. Fakat komut kullanımı yerine, ara yüzü olan yazılımların kullanımının daha kolay olması nedeniyle bu komutun kullanımı yaygın

değildir. Linux dd ile analizi yapılacak olan bir depolama biriminin imajının alınması ya da orijinal kopyasının oluşturulması mümkündür.

Autopsy ve The Sleuth Kit: Sleuth Kit komut satırında çalışan bir disk/dosya analiz aracıdır. Autopsy ise Sleuth Kit'in kullanımı için geliştirilmiş bir web ara yüzüdür. Autopsy, açık kaynak kodlu adli bilişim yazılımları içerisinde en geniş kapsamlı olan yazılımdır. Bu program ile kapsamlı bir disk/dosya analizinin yapılması mümkündür.

Helix: Linux tabanlı Knoppix işletim sistemi üzerine inşa edilmiş, adli bilişim inceleme yazılımlarından oluşan bir yazılımdır. Helix, içerisinde sadece adli bilişim alanında kullanılan yazılımlar bulunan ve bu amaçla tasarlanan özel bir yazılım paketidir[37].

4. SAYISAL ORTAMLARDAN VERİ KURTARMA UYGULAMALARI

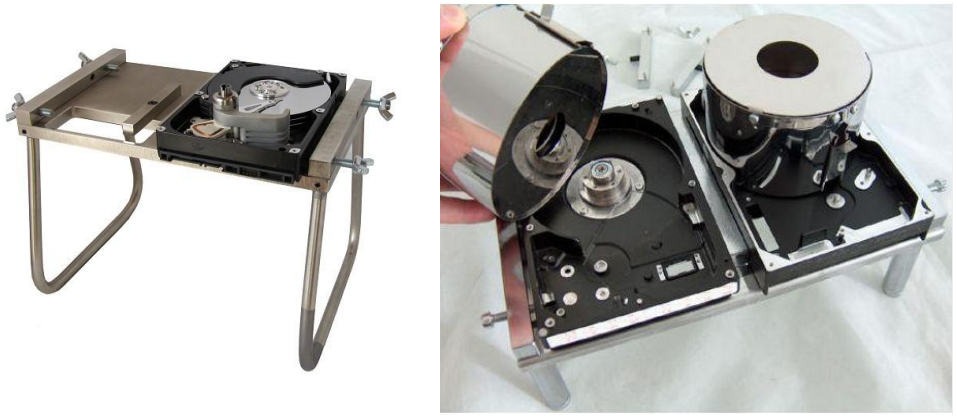
Bu bölümde veri kurtarma uygulaması olarak fiziksel hasarlı sabit disk ve flash bellek ile biçimlendirilmiş disk bölümünden veri kurtarma işlemleri gerçekleştirildi.

4.1. Fiziksel Hasarlı Sabit Disklerden Veri Kurtarma Uygulaması

Bir sabit diskte fiziksel hasar varsa diskteki verilere normal yollarla erişilemez. Fiziksel hasar tespit edilip giderildikten sonra bu erişim mümkün olur. Fiziksel hasarlarda arızanın bulunduğu cihazı tespit etmek ayrı bir çalışma konusudur. Bu uygulamanın birinci aşamasında sabit disklerde sıklıkla meydana gelen devre kartı sorunu ve arızanın giderilmesi incelendi. Elimizde bulunan belli bir marka ve modele sahip sabit diskin devre kartı şekil 33'de görüldüğü üzere elektriksel bir nedenden dolayı üzerindeki bazı devre elemanları yanmış bulunmaktadır. Bu tür sorunlarda devre kartının sökülüp tamir edilmesi bir çözüm yolu olmakla birlikte bu sabit diskin aynı marka ve model numarasına sahip başka sağlam bir sabit diskin devre kartlarını değiştirmek daha çok tercih edilen diğer bir yöntemdir. Bu uygulamada ikinci yöntem tercih edildi. Elde edilen aynı marka ve model sağlam sabit diskin devre kartı dikkatle sökülerek arızalı sabit diskin devre kartı sökülüp yerine takıldı. Bilgisayara bağlanıp gerekli Bios ayarları yapıldıktan sonra çalıştırıldı ve sabit disk sorunsuz çalışmaya başladı. Bu işlemin sonunda herhangi bir veri kaybı yaşanmadı, bunun en önemli nedeni verilerin kayıtlı bulunduğu disk yüzeyinde herhangi bir fiziksel hasarın oluşmamış olmasıdır. Bu uygulamada en önemli nokta devre kartları değiştirilen bu sabit disklerin marka ve modellerinin aynı olmasıdır. Aynı markanın farklı bir model devre kartı olsa bile sabit diski çalıştırmayacaktır. Şunu da belirtmek gerekir ki yeni üretilen bazı sabit disklerde bu tür sorunlarda devre kartlarını değiştirmek sorunu çözmeyebilir. Bu sabit disklerde disklere erişim kodları kullanılmaktadır, kodlar değişince erişim mümkün olamamaktadır. Bu durumda profesyonel veri kurtarma laboratuvarlarındaki gelişmiş yazılım ve donanım kaynaklarına başvurmak gerekecektir.

Şekil 33. Yanmış sabit disk devre kartı

Sabit disk fiziksel hasar uygulamasının ikinci aşamasında sabit disk plakalarının değiştirilme işlemi gerçekleştirildi. Sabit disk motor veya taşıyıcı kol arızalarında arızalı sabit diskin plakaları aynı marka ve model sağlam başka bir sabit diskin plakaları ile değiştirilerek bu sorun giderilir. Bunun için bir profesyonel veri kurtarma firmasının laboratuvarı kullanıldı. Bunun en önemli nedeni buradaki tozsuz odadır. Bilindiği gibi sabit disk gövdesinin içine toz partiküllerinin kaçması daha başka arızalara ve disk bozulmalarına sebep olmaktadır. Arızalı sabit disk ile aynı marka ve model sağlam sabit disk şekil34'deki onarım tezgâhına monte edildi. Sabit disk onarım tezgâhı bu işlemler için geliştirilmiştir. Sabit disk plakaları arasındaki disk kafaları disk yüzeyine dokundurulmadan dikkatle çıkarıldı. Disk motor ve milleri söküldükten sonra disk plakaları özel aparatlarla el değmeden kenarından kavranıp çıkarıldı. Aynı şekilde yeni sabit diskin plakaları çıkarıldı ve yerine diğer plakalar takıldı. Okuma/yazma kafaları plakaların arasına dikkatle yerleştirildi ve gövde kapağı kapatıldı. Sabit disk bilgisayara bağlanıp çalıştırıldı. Disk yüzeyinde bad sektörlerin oluşmuş olduğu görüldü. Bu hard diskin bütün verileri başka sağlam bir diske kopyalanarak verileri kurtarıldı.



Şekil 34. Sabit disk onarım tezgâhı

Burada dikkat edilmesi gereken birkaç önemli nokta bulunmaktadır. Birincisi bu işlem herhangi bir ortamda yapılmamalıdır ve bu işlem için gerekli aparatların bulundurulması gerekir. Disk yüzeyine temas olmamalıdır ve toz partiküllerinden korunmalıdır. Gövde içinde okuma/yazma kafası hareketli bir elemandır ve partiküllerle çarpışması disk yüzeyinde fiziksel bozulmalara neden olur. Zamanla bad sektörler oluşturur. Tozsuz oda(Clean Room) tercih edilme nedeni burada normal ortama göre parçacık oranı yaklaşık 350 kat daha azdır. Şekil 35'te görülen tozsuz odada tüm cihazlar

aynı zamanda elektrostatik boşalma, fiziksel şoklar, sıcaklık dalgalanmaları ve elektrik bozukluklarına karşı korunur.

Şekil 35. Tozsuz oda

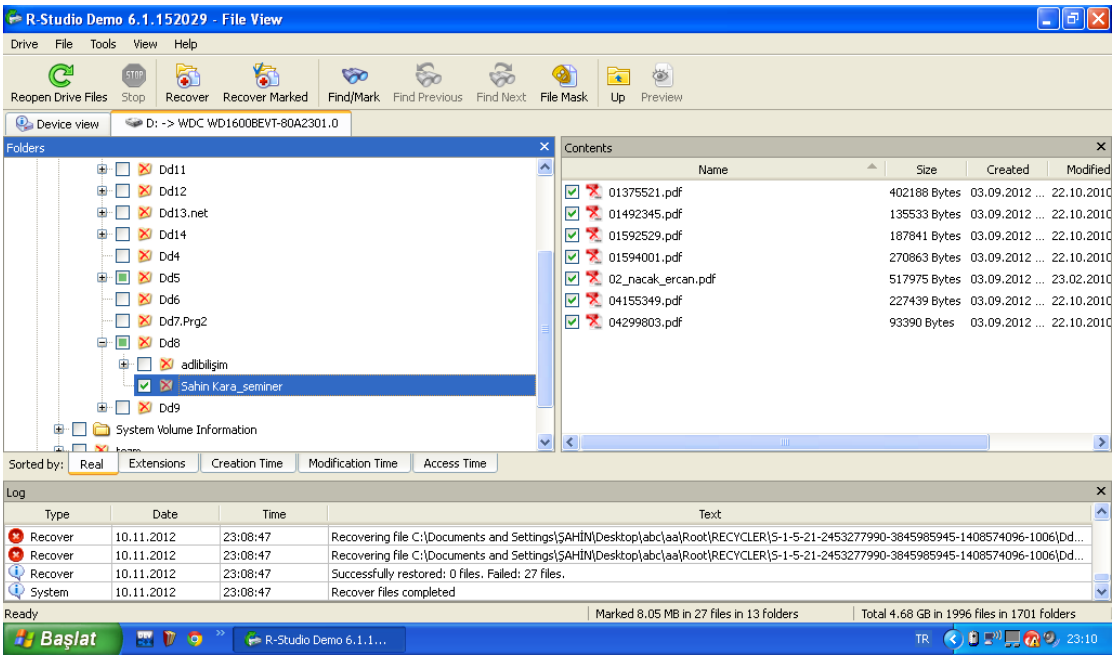
4.2. Fiziksel Hasarlı Flash Belleklerden Veri Kurtarma Uygulaması

Donanımsal hasarı olan bir USB belleğin verilerine bu donanım arızası giderilmeden erişilemez. Bunun için iki yöntem kullanılır. Birincisi, bellek çipinin üzerinde bulunduğu elektronik devrenin tamir edilmesidir. İkinci yöntem ise bellek çipinin sökülüp özel kart okuma kitlerine takılarak verilerin bilgisayar ortamına alınmasıdır. Eğer arıza bellek çipinin kendisinde ise verileri kurtarmak mümkün olmayabilir. Bu uygulamada ikinci yöntem kullanılarak USB belleğin kasası çıkarıldıktan sonra flash çipi üzerinde bulunduğu baskı devreden sıcak hava verilerek çıkarıldı. Bu tip bellekler için geliştirilmiş özel yazılım ve Şekil 36'da görülen hafıza çipi okuma cihazına takılıp USB/IDE ara adaptörü ile bilgisayara bağlandı. Bu işlemler için geliştirilmiş yazılımlar ile hafıza çipinin imajı alındı ve mantıksal yapı tekrar oluşturuldu. Bu yöntemle bellek çipi yanmamış bellek kartlarının çoğunda yüksek bir başarımda veriler kurtarılmaktadır. SSD disk arızalarında da bu yöntemle veri kurtarılmaktadır. Aslında bir SSD Disk günümüzde yaygın olarak kullanılan USB Flash diskler gibidir, tek farkı daha fazla hafıza çipine sahip olması ve bu hafıza çiplerini kompleks yazılımıyla bir arada kullanımını sağlamasıdır. SSD disklerde mekanik parçaların olmaması problem yaşanması ihtimalini azaltmaktadır. Bu yüzden Hard Disklerde sıklıkla yaşanan Okuyucu Kafa arızaları, motor arızaları gibi problemleri SSD disklerde görmemekteyiz.

Şekil 36. FDRE (Flash disklerden data kurtarma cihazı)

4.3. Biçimlendirilmiş Diskten Veri Kurtarma Uygulaması

Bu uygulamada formatlanan diskten verileri kurtarmak için otomatik veri kurtarma yazılımı kullanıldı. Otomatik veri kurtarma yazılımı olarak R-Studio 6.1 kullanıldı. Bu program format ya da fdisk sonrası her türlü dosyayı kurtarabilmektedir. Ancak, silinen dosyaların üzerine bir daha veri yazılmamış olma şartı vardır. Yani veriler silindiğinde verilerin silindiği bölüme herhangi bir yükleme yapılmamalıdır. Eğer yüklenecek program silinmiş olan partisyonun üzerine yüklenirse o zaman o datayı kurtarmak zorlaşır. Recover yapmak istenen bölüme hiç bir şekilde müdahale yapılmamış olması en sağlıklı dosya kurtarmanın sırrıdır.



Şekil 37. Kurtarılabilecek dosya ve klasör listesi

Şekil 37'de görüldüğü üzere kurtarılabilecek dizin, alt klasör ve dosyalar listelenmektedir. Kurtarılmak istenen dosyalar seçilip kurtarma işlemi gerçekleştirildi. Formatlanan diskte formatlamadan sonra üzerine herhangi bir veri yazma işlemi yapılmadığı için bütün dosyalar başarılı bir şekilde kurtarıldı. Kullanılan otomatik kurtarma programı lisanslı değilse veya demo ise kurtarma özellikleri kısıtlı olacaktır. Otomatik veri kurtarma yazılımları farklı seçeneklerle karşımıza çıkmaktadırlar. Çoğu zaman diskin tamamından çok, silinen belli dosyalar kurtarılmak istenir. Bunun için dosya uzantısına göre veya belli tarihler arasında silinmiş dosyaları taratma özelliği olan yazılımlar daha faydalı olabilir.

4.4. Uygulama Sonuçları

Veri kurtarma uygulaması olarak birinci uygulamada fiziksel hasarlı sabit disklerden veri kurtarma işlemi gerçekleştirildi. Bunun için donanımsal olarak veri kurtarmak için en çok kullanılan iki yöntemle veri kurtarma işlemi gerçekleştirildi. Birinci aşamada elektriksel bir nedenle devre kartı yanmış olan sabit diskin durumu incelendi. Sabit diskin gövdesinde herhangi bir hasar gözlenmedi ve devre kartının değiştirilmesine karar verildi. Üzerinde çalışılan diskin devre kartı marka ve model olarak bire bir aynısıyla değiştirildi. Sabit disk bilgisayara takıldığında sorunsuz bir şekilde çalıştığı ve herhangi bir veri kaybı gözlenmedi.

Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen çıkarımlar elde edilmiştir:

- Kullanıcılar bu tür durumlarla karşılaştıklarında genellikle sabit diskin yanmış olduğunu ve verilerin kaybolmuş olduğunu düşünürler. Ancak yapılan uygulamada bu tür durumlarda sabit diskteki veriler genellikte kayıtlı olduğu ortam olan manyetik disklerden kaybolmaz sadece bu verilere erişim sağlanamamaktadır.
- Devre kartının tamir edilmesi veya aynı modeliyle değiştirilmek suretiyle verilere erişim sorunu ortadan kalktığında sabit diskteki veriler kurtarılmış olacaktır.
- Sabit disklerin devre kartları haricen satılmadığı için ihtiyaç durumunda yeni bir sabit disk temin etmek gerekebilir. Özellikle eski modelleri bulmak oldukça zordur. Son kullanıcılar için arızalı diskin aynı modelini bulmak zor olsa da veri kurtarma işiyle uğraşan firmalar bu durumlar için sabit disk arşivleri oluşturmuş bulunmaktadırlar.
- Son kullanıcılar, devre karı arızasında sabit diskin eşdeğer devre kartını temin ettiklerinde kendileri de devre kartlarını değiştirip sabit diski tamir edebilirler.

Fiziksel hasarlı sabit diskten veri kurtarmanın ikinci aşamasında disk gövdesi açılıp disk plakaları yeni gövdeye aktarma işlemi gerçekleştirildi. Okuma/yazma kafa ve taşıyıcı kol arızası bulunan sabit disk bir profesyonel veri kurtarma firmasının laboratuvarı kullanılarak disk plakalarının değişimi yoluyla veri kurtarma işlemi gerçekleştirildi Uygulamanın bu aşaması özel tozsuz odada ve bu işi için geliştirilmiş cihazlar kullanıldı. Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen çıkarımlar elde edilmiştir:

- Son kullanıcıların böyle bir işlemi herhangi bir ortamda yapması önerilmez. Kullanıcıların yeterli deneyim imkânı yoksa böyle bir girişim verileri tamamen kaybetmelerine sebep olabilir. Bu tür problemlerde profesyonel veri kurtarma firmalarından yardım alınmalıdır.
- Bu uygulama neticesinde sabit disk çalıştırıldıktan sonra yazma/okuma kafasının disk yüzeyine temasından dolayı *bad* sektörlerin oluştuğu yardımcı yazılımlarla gözlendi. Bu yöntemle verileri yüzde yüz kayıpsız kurtarmak düşük bir ihtimaldir. Disk plakaları genellikle fiziksel hasar görür ve kalıcı veri kayıplarına neden olur. Ama veri kurtarma ilkesi olarak, bir verinin tamamı elde edilemezse bile veri en az kayıpla kurtarılmaya çalışılır.
- Bu çok hassas bir yöntemdir. Son kullanıcıların bu yöntemle veri kurtarma girişimleri daha fazla veri kaybına neden olabilmektedir. Çünkü sabit disk gövdesinin açılıp disk plakalarının yeni gövdeye aktarılma işlemi, tozsuz oda ortamı, özel araç gereçler ve deneyim gerektiren bir yöntemdir. Bunun için için profesyonel yardım almak gerekmektedir.
- Sabit disklerden veri kurtarma vakalarının sadece %10'luk bir bölümü tozsuz odada gerçekleştirilmektedir. Geriye kalan büyük bölümü normal ortamda yapılmaktadır.[38]

Üçüncü uygulamada fiziksel olarak hasar görmüş bir flash bellekten veri kurtarma uygulaması yapıldı. Bunun için flash çipin kendisinden datayı almaya yarayan (FDRE) cihaz kullanıldı. Bu işlemler için geliştirilmiş yazılımlar ile hafıza çipinin imajı alındı ve mantıksal yapı tekrar oluşturuldu. Bu yöntemle bellek çipi yanmamış bellek kartlarının çoğunda yüksek bir başarımda veriler kurtarılmaktadır. Ancak, bellek çipinde fiziksel hasar varsa veriler kalıcı olarak kaybolmaktadırlar.

Dördüncü uygulamada biçimlendirilen bir sabit disk bölümünün otomatik veri kurtarma programıyla kurtarılma işlemi gerçekleştirildi. Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen çıkarımlar elde edilmiştir:

- Biçimlendirmelerde ve silinmelerde silinen veri alanına veri yazılmazsa ve yanlış müdahale yapılmazsa veriler sıradan bir veri kurtarma programıyla bile yüksek bir başarım oranıyla kurtarılabilmektedir.
- Bu uygulama kontrollü gerçekleştirildiği için silinen bölüme herhangi bir veri yazılmadı ve kurtarma işlemi başka bir sürücü üzerinden gerçekleştirildiği için bölümdeki dosyalar başarılı bir şekilde kurtarıldı.
- Kullanıcıların çok sık karşılaştığı bu gibi durumlarda en çok dikkat etmeleri gereken nokta silmenin veya biçimlendirmenin gerçekleştiği disk üzerine herhangi bir veri yazmamalarıdır.
- Mümkünse kurtarma çalışmaları başka bir disk üzerinden yürütülmelidir veya diskin imajı alındıktan sonra kurtarma işlemi gerçekleştirilmelidir.

Tablo 6. Başarım değerlendirme tablosu

Başarım Değerlendirme Tablosu		
Kayıt Ortamı / Hasar Türü	**Sabit Diskler**	**Flash Bellekler Ve Bellek Kartları**
Fiziksel Hasarlar	Sabit disk fiziksel hasarlarında veri kurtarma tozsuz oda ortamında özel araçlarla ve uzman kişiler tarafından gerçekleştirilir. Verileri kurtarmak için donanımsal araçlar kullanılır. Başarımı yüksektir. Manyetik disk plakalarında fiziksel hasar oluşmamışsa bu yöntemle verilerin tamamı kurtarılabilir. Plakalarda *bad sector* gibi fiziksel bir hasarın oluştuğu alanlardaki veriler kalıcı olarak kaybolmaktadır.	Bellek çipinin üzerinde bulunduğu devre kartı tamir edilerek veriler kurtarılır. Ancak bu metot parça sıkıntısı nedeniyle zaman alıcı bir yöntemdir. Bunun yerine flash çipin kendisinden datayı almaya yarayacak cihazlar (FDRE) geliştirilmiştir. Geliştirilen yazılımlarla birlikte kullanılırlar ve veri kurtarma başarımı yüksektir. Ancak, bellek çipi arızasında veriler genellikle kalıcı olarak kaybolmaktdır.
Biçimlendirme Ve Silinmeler	Biçimlendirmelerde veri kurtarma işlemi özel geliştirilmiş programlar kullanılarak gerçekleştirilmektedir. Veri kurtarma süresi verilerin çokluğuna göre değişebilmektedir. Formatlanmış disklerden verileri toplamak ve silinmiş dosya gruplarını doğru şekilde elde etmek genellikle daha uzun zaman almaktadır. Müdahale görmemiş ve üzerine veri yazılmamış disklerden veri kurtarma oranı oldukça yüksektir.	Veri kurtarma özel geliştirilmiş programlar kullanılarak gerçekleştirilmektedir. Ancak, silinen dosyaların üzerine veri yazılmamış olma şartı vardır. Veriler silindiğinde verilerin silindiği bölüme herhangi bir yükleme yapılmamalıdır. Silinen alana veri yazılmamışsa silinen veriler yüksek oranda kurtarılabilir. Bu alana veri yazılmışsa orantılı olarak kurtarma oranı azalacaktır.
Dosyalarda Dahili Bozulmalar	Veri kurtarma sonrasında kısmi olarak kurtarılabilmiş dosyaların onarılıp işe yarar hale getirilmesi için geliştirilmiş yazılımlar kullanılmaktadır. Word, excel ve veri tabanı dosyalarının kurtarılma oranları yüksektir.	
Dosya Sistemi Hasarları	Dosyalara erişmek için sistem alanındaki tanım ve adresler hayati öneme sahiptir. Bu yapılar silindiğinde veya hasar gördüğünde veri depolama ortamındaki klasör ve dosyalara standart işletim sistemi araçlarıyla erişmek mümkün olmaz. Bunun için veri kurtarma yazılımları kullanılmaktadır. Müdahale görmemiş ve üzerine veri yazılmamış ortamlardan veri kurtarma oranı oldukça yüksektir. Aksi durumda başarım orantılı olarak düşecektir.	

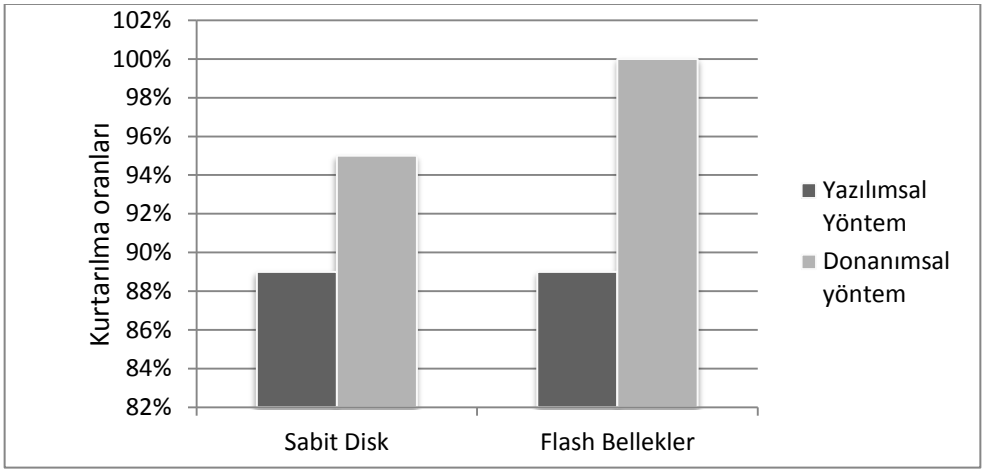
4.5. Verinin Bulunduğu Sayısal Ortama Göre Veri Kurtarma Başarım Oranları

Yapılan uygulamalarda şekil 38'de gösterildiği gibi sabit diskten veriler, fiziksel hasar durumunda %95, biçimlendirme durumunda ise %89 başarım oranında kurtarılmıştır. Flash bellekten fiziksel hasarda donanımsal olarak verilerin tamamı, yazılımsal veri kaybında verilerin %70'i kurtarılmıştır. Fiziksel ya da yazılımsal hasarlarda sayısal verilerin bulunduğu ortamların bozulma oranları farklılık gösterir. Veri kurtarma imkânları ile veri kurtarmada kullanılan araçlar ve bu işlemleri gerçekleştiren kişilerin deneyim düzeyleri veri kurtarma oranlarına direkt etki eder. Şartlar ve araçlar değiştiği durumlarda

başarım oranları arasında büyük farklar oluşabilir. Bundan dolayı bu oranlar mutlak değildir.

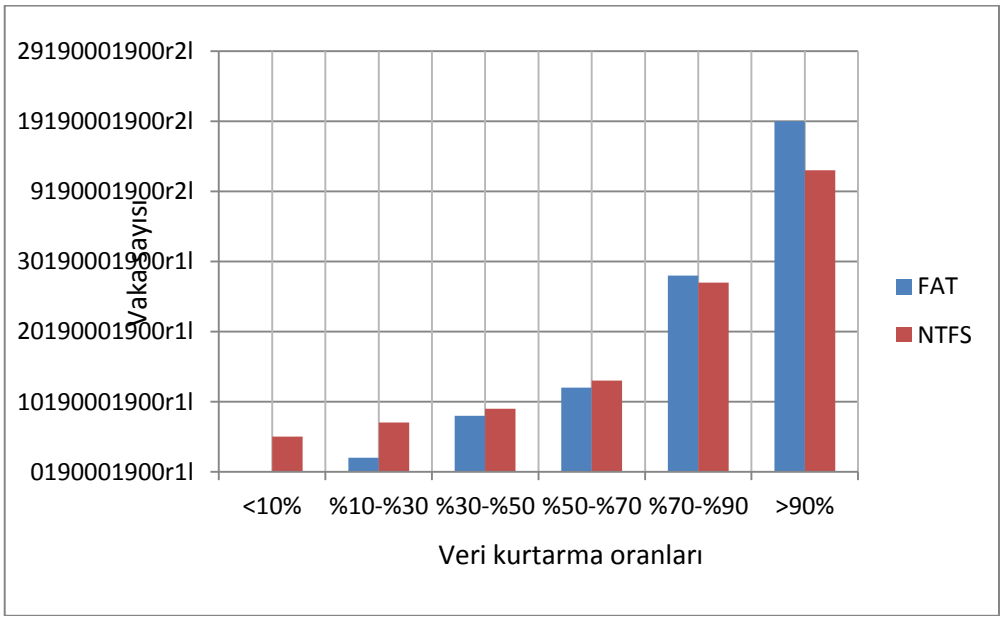
Tablo 7. Sayısal ortama göre veri kurtarma başarım tablosu

Verinin Bulunduğu Ortam	Kullanılan Yazılım	Fiziksel Hasar	Biçimlendirme
Sabit Disk	R-Studio 6.1	%95	%89
Flash Bellek	SoftOrbits Flash Drive Recovery v1.3	%100	%70



Şekil 38. Uygulama sonucunda elde edilen veri kurtarma oranları

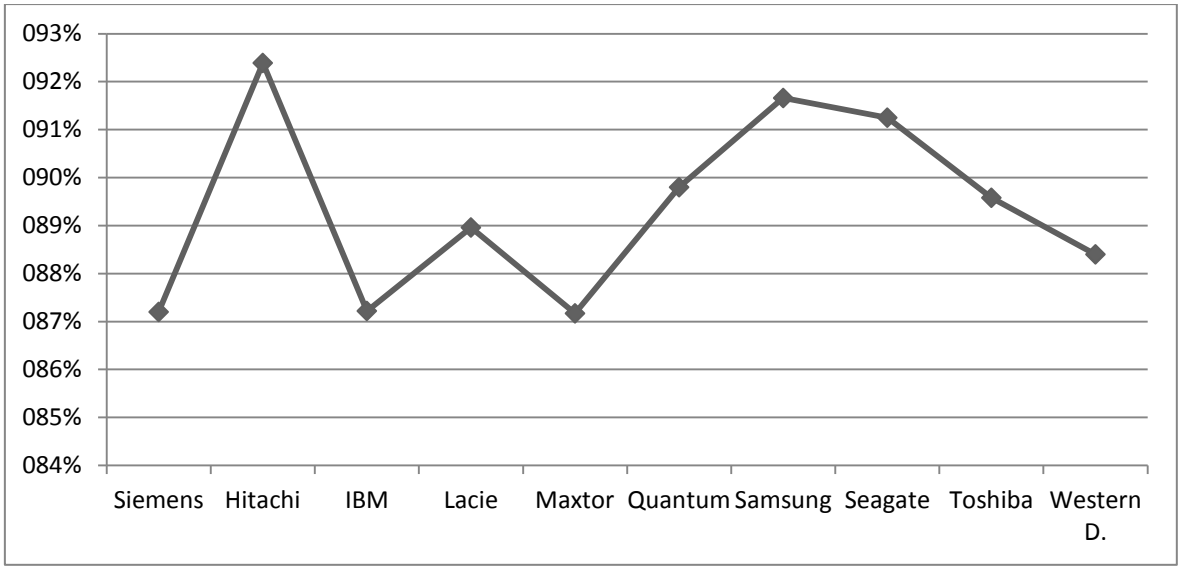
4.6. Dosya Sistemine Göre Veri Kurtarma Başarım Oranları



Şekil 39. Dosya sistemine göre veri kurtarma başarım oranları

Şekil 39'da görüldüğü gibi FAT dosya sistemi kullanan kayıt ortamlarındaki verilerin %90'ını kurtarma ihtimali %50'dir. FAT dosya sisteminde veri kaybı vakalarının yaklaşık olarak %75 -80'inde veriler en az %75 oranında kurtarılabilmektedir. NTFS dosya sistemi olan ortamlarda bu oranlar biraz daha düşmektedir. NTFS dosya sistemi kullanan kayıt ortamlarındaki verilerin %90'ını kurtarma ihtimali %40'dir. NTFS dosya sisteminde veri kaybı vakalarının yaklaşık olarak %75'inde veriler en az %70 oranında kurtarılabilmektedir[39].

Veri kurtarma firmalarının her iş bitiminde kendi veri tabanlarına ekledikleri başarım oranlarının sabit disk markalarına göre dağılımı şekil 40'da gösterilmiştir. Buna göre ortalaması alınırsa sabit disklerden genel olarak veri kurtarma oranı %89,36 çıkmaktadır.



Şekil 40. Veri kurtarma başarım oranlarının sabit disk markalarına göre dağılımı[40]

5. SONUÇLAR

Bireysel ve kurumsal verilerin tümüne yakını bilgisayarlar üzerinde depolanması, bu verilerin kaybedilemeyeceği anlamına gelmez. Çok hassas matematik ve yazılım hesapları üzerine kurulu bilgisayar sistemlerinde farklı nedenlerle veri kayıpları yaşanmaktadır. Bu da veri kurtarma sektörünün ortaya çıkmasına neden olmuştur. Veri kurtarmayı anlamak için verinin ne olduğu nelerle temsil edildiği ve saklandığı ortamların özelliklerinin iyi anlaşılması gerekir. Veri kayıt ortamlarının özellik ve çalışma mantıklarının yeterince bilinmemesi bazen veri kaybının en önemli nedeni olabilmektedir. Herhangi bir nedenle veri kaybının ortaya çıktığı durumda veri kurtarma süreci başlar ve durum karşısında seçtiğimiz yöntemler, attığımız adımlar, veri kurtarma başarımını etkileyecektir.

Bu tez çalışmada yazılımsal ve donanımsal olmak üzere iki kurtarma yöntemi literatür taraması ve araştırmalar yapılarak bu yöntemler üzerine uygulamalar yapılmıştır. Veri kurtarma işleminde uygulamalar sonucundaki alınan neticelere göre donanımsal bir arıza sadece yazılımsal yöntemlerle veriyi kurtarmak mümkün olmayacağı veya kurtarılsa bile başarımı çok düşük olacağı görülmüştür. Bir diskten yanlışlıkla silinen bir verinin üzerine veri yazılmamışsa genellikle %80-90 başarım oranıyla yazılımsal olarak kurtarmak mümkündür. Bu formatlama veya disk bölümü silme durumu için de geçerlidir. Ancak silinen verilerin üzerine başka veriler yazılmışsa başarım oranı orantılı olarak düşecektir. Zaten güvenli veri imha yöntemlerinden biri de verinin üzerine başka veri yazmaktır. Veri kurtarma firmaları özellikle müdahale görmemiş sabit disk, sunucular, usb bellek ve hafıza kartlarından veri kurtarma başarı oranlarını 90% olarak ifade etmektedirler. Buradaki en önemli konu veri kaybı gerçekleşen cihazın müdahale görmemiş olmasıdır. Dolayısıyla kurtarma işlemleri başka bir disk üzerinden yürütülür. Yazılımsal olarak pek çok veri kurtarma yazılımı bulunmaktadır. Bireysel olarak her kullanıcı bu programları kullanarak veri kurtarma yapabilir ama kaybedilen verinin önemine göre profesyonel veri kurtarma firmalarından da yardım alınmasında fayda vardır.

Veri kurtarmanın diğer yöntemi donanımsaldır. Veri kayıt ortamında meydana gelen fiziksel arızalar donanımsal olarak veya yazılım destekli karma bir yöntemle kurtarılır. Bu yöntemin başarım oranı fiziksel hasarın türüne ve verdiği zarara göre değişir. Fiziksel arıza veriyi tamamen imha da edebilir. Ancak pek çok fiziksel arıza durumunda veri imha olmaz sadece erişim problemi ortaya çıkar. Donanımsal çözüm yöntemi için özel veri kurtarma cihaz ve ekipmanları gerekmektedir, başarımı dolayısıyla maliyeti de yüksek bir

yöntemdir. Fiziksel hasarların çoğunda sadece yazılımsal veri kurtarma yöntemi tek başına veri kurtarmaya yetmez. Bunun için donanımsal kurtarma yöntemi gerekir. İki yöntemin birlikte kullanıldığı durumlarda başarım oranı daha yüksek olacaktır. Bu çalışmada üzerinde durulan önemli bir konu da veri koruma teknolojileridir. Veri kayıplarının en aza indirilmesi amacıyla bu teknolojileri bir veri koruma politikası kapsamında kullanmak faydalı olacaktır.

6. KAYNAKLAR

[1] *İnternet*; http://www.genbilim.com/content/view/1139/, Ekim 2012.

[2] *İnternet*; http://www.chip.com.tr/blog/thecrowsalvation/ veri_bilgi_ve_bilisim_3332.html, Ekim 2012.

[3] Gu, J., Ma, Z.-D., and Hulbert, G. , "Quasi-Static Data Recovery for Structural Dynamic Analyses," The 6th US National Congress on Computational Mechanics, Dearborn, Michigan, 2001.

[4] *İnternet*; http://www.mydisk.com.tr/veri-kurtarma-hakkinda.php, Kasım 2012.

[5] D. M. Smith, "The cost of lost data," Journal of Contemporary Business Practice, Vol. 6, No. 3, 2003

[6] Peter Mell and Miles C. Tracy, "Procedures for Handling Security Patches," National Institute of Standards and Technology NIST Special Publication, September 2002.

[7] Gartner Research Note , "Vulnerability Management Defined," September 3, 2003.

[8] Daş, R., Kara, Ş., Gündüz, M.Z., "Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.

[9] Daş, R., Türkoğlu, İ., Poyraz, M., (2008). "Analyzing of the user access logs of a website using web usage mining method: Example of Firat University", e-Journal of New World Sciences Academy (NWSA), Natural and Applied Sciences, 3(2), 310-320.

[10] Beydağlı E., Kara M., Bahşi H., Alparslan E, TÜBİTAK BİLGEM, "Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standardı" , 2010.

[11] *Kitap*; Dinçel Teoman, "Bilgisayar Öğreniyorum", Kodlab Yayınevi, İstanbul, 2010.

[12] *Kitap*; Hoşgören Mehmet, Mahmut KARAKAYA, "Donanım Mimarisi", MEB Yayınları, İstanbul, 2006.

[13] Jones, A; Valli, C; Dabibi, G. 'The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market'. In proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia, 2009.

[14] Ronald van der Knijff, Eoghan Casey, Embedded Systems Analysis, Handbook of Digital Forensics and Investigation, 2009.

[15] *İnternet*; http://www.microsoft.com, Ekim 2012.

[16] *İnternet*; http://psce.wordpress.com/tag/linux-dosya-sistemleri, Ekim 2012.

[17] *İnternet*; EMC Student Documents, Wikipedia, Ekim 2012.

[18] *Kitap;* David B Little , David A. Chapa , "Implementing Backup and Recovery", 2003.

[19] *Kitap;* Curtis Preston, "Backup & Recovery", O'Reilly, 2007.

[20] B.J. Jones, A.J. Kenyon, Retention of data in heat-damaged SIM cards and potential recovery methods, Forensic Science International, Volume 177(1), Pages 42–46, May 2008

[21] *İnternet*; "List of data recovery software", Wikipedia, http://en.wikipedia.org/wiki/ List_of_data_recovery_software, March 2012.

[22] Kubilay Say Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Adli Tıp Anabilim Dalı, Bilişim suçlarında elde edilen delillerin olay yerinden toplanması ve laboratuarda incelenmesi, 2006.

[23] Grobler C P, Louwrens C P , Digital Evidence Management Plan,Information Security for South Africa (ISSA), Digital Object Identifier:10.1109/ISSA.2010.5588661, 1-6, 2010 .

[24] Fridrich J, Digital image forensics, Signal Processing Magazine, IEEE Volume: 26 , Issue: 2, 2009.

[25] Peisert S, Bishop M, Marzullo K, Computer Forensics in Forensis , Systematic Approaches to Digital Forensic Engineering, 2008. SADFE '08. Third International Workshop on, 102 – 122, 2008.

[26] Dixon P.D., An overview of computer forensics ,Potentials, IEEE Volume: 24, Issue: 5, 7 – 10, 2005.

[27] Howard Chivers, Christopher Hargreaves, Forensic data recovery from the Windows Search Database Digital Investigation, Volume 7, Issues 3-4, 114-126, April 2011.

[28] Hassan Khan, Mobin Javed, Syed Ali Khayam, Fauzan Mirza, Designing a cluster-based covert channel to evade disk investigation and forensics Computers & Security, Volume 30, Issue 1, 35-49, 2011.

[29] Nicole Lang Beebe, Sonia D. Stacy, Dane Stuckey Digital forensic implications of ZFS Digital Investigation, Volume 6, Supplement 1, 99-107,2009.

[30] Timothy D. Morgan , Recovering deleted data from the Windows registry Digital Investigation, Volume 5, Supplement 1, 33-41, 2008.

[31] Aaron Burghardt, Adam J. Feldman, Using the HFS+ journal for deleted file recovery Digital Investigation, Volume 5, Supplement 1, 76-82,2008.

[32] O.P. Jasuja, Gagan Deep Singh, G.S. Sodhi, Development of latent fingerprints on compact disc and its effect on subsequent data recovery Forensic Science International, Volume 156, Issues 2-3, 237-241, 2006.

[33] Jungheum Park, Seok Hee Lee, Sangjin Lee , Recovery of Damaged Compressed Files for Digital Forensic Multimedia and Ubiquitous Engineering, MUE 2008. International Conference on Digital Object Identifier: 10.1109/MUE.2008.49, 365 – 372, 2008.

[34] Simon M., Slay J., Recovery of Skype Application Activity Data from Physical Memory Availability, Reliability, and Security, ARES '10 International Conference on Digital Object Identifier: 10.1109/ARES.2010.73,283–288, 2010.

[35] Wasim Ahmad Bhat and Syed Mohammad Khurshaid Quadri, University of Kashmir, After-deletion data recovery: myths and solutions, April 2012.

[36] Paul Owen, Paula Thomas, An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines, Information Security Research Group, Faculty of Advanced Technology, University of Glamorgan, Pontypridd, CF37 1DL, UK, March 2011.

[37] *Kitap,* Henkoğlu Türkay, "Adli Bilişim", Pusula Yayınları, 2011.

[38] *İnternet*; http://www.dq-int.co.uk/blog/2012/11/22/data-recovery-success-rates-october-2012.

[39] *İnternet*; http://www.z-a-recovery.com/art-data-recovery-statistics.htm. Aralık 2012.

[40] *İnternet*; http://web.archive.org/web/20070807092026/http://www.fields-data-recovery.co.uk/success.html. Aralık 2012.

ÖZGEÇMİŞ

Şahin KARA, 1977 yılında Bitlis'te doğdu. 2002 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Sistemleri Öğretmenliği bölümünü bitirdi. Bitlis Eren üniversitesinde öğretim elemanı olarak görev yaptı. Halen Sakarya Üniversitesinde öğretim elemanı olarak görev yapmaktadır. Aynı zamanda Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında yüksek lisans eğitimi yapmaktadır. Adli bilişim ve güvenlik konularında araştırmalar yapmaktadır.