GÜVENLİ SİLME
DOSYA KURTARMA

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Mustafa Oğuz İnan

Tarih: 29.05.2016

Windows, İos ve Linux işletim sistemlerine sahip bilgisayarlarda güvenli slime ve silinen dosyaları geri getirme

Dosya Sistemi

Dosya Nedir?

Dosya;disk üzerinde depolanmış verilerin bütününe verilen isimlendirmedir.
İşletim sistemi tipik olarak iki çeşit dosya içerir.

- Birincisi; bir sistem görevi yerine getirirken yada bir uygulama çalışırken bilgisayarı kontrol eden komutları içeren program dosyasıdır.
- İkincisi ise bir kelime işlem bölgesi gibi bir uygulama yardımı ile yaratmış olduğunuz bilgilerinizi içeren veri dosyasıdır.

Dosya Sistemi Nedir?

Dosya sistemi (File system), dosyaların hard disk üzerinde nasıl yerleşeceğini ayarlayan bir sistemdir.
Diğer bir tanıma göre dosya sistemi, bir dosyanın bir disk üzerinde nasıl saklandığı ve bir bilgisayarın dosyaları yönetebilmek için erişimi nasıl sağladığını kontrol eden bir sistemdir.

Verilerin HDD'de saklanması

KAFA: HDD'nin her iki yüzü için ayrı bir elektromanyetik kafa, okuma/yazma için bulunmaktadır.
İZ:Her bir diskin her iki yüzeyinde iç içe geçmiş halkalar halinde izler bulunmaktadır.
Sektör:Bir diskin her yüzeyi, dairesel bir pastanın dilimlenmesine benzer şekilde kesimlere ayrılırlar.

- Disketlerde izler genellikle 8-18 dilime(sektöre) bölünür.
- Hem HDD hem de disketlerde her bir sektör 0.5 KB'lık veri depolar.

Cluster:Dosya sistemi sektörlerin tamamını bir seferde kullanmaz ve "Cluster" adı verilen gruplara toplar.

- Dosya sistemleri verileri, programları ve dizinleri bu cluster içinde saklar.
- Bir cluster birçok sektörden oluşur ve bu yüzden çok küçük yada çok büyük olabilir. Ancak ne kadar küçük olursa o derecede bilgiler daha iyi yerleştirilir, boş alan kalmaz.

Hangi işletim Sistemi Hangi Dosya Sistemlerini Kullanır?

- Linux: Ext2 ,Linux Swap, Reiser
- MSDOS: FAT
- Windows95, Windows98: FAT 16
- Windows NT ve Windows 2000: NTFS
- OS/2: HPFS
- Novell Netware: Netware File System

FAT (File Allocation Table) 16

- "Dosya Yerleşim Tablosu" DOS'ta ve Windows'un ilk sürümlerinde 16 Bit idi.
- 256MB'tan küçük bölümler (partition) için veriye ulaşım çok hızlıdır. En fazla 65536 dosya olabilir,
- Bir dosya en fazla 4GB boyutunda olabilir,
- Cluster boyu büyük olduğu için yer kaybı fazladır,
- Veri güvenliği yoktur.

FAT 32

- FAT 16'dan daha gelişmiş veri koruma yöntemleri vardır.
- Disk bölümünün 512 MB tan büyük olması gerekir.
- 2 TB büyüklüğüne kadar sabit disk bölümlerinin kullanılmasını sağlar.
- Daha küçük (4 kb) cluster büyüklüğü kullanarak diskin daha ekonomik kullanımını sağlar.
- Çok büyük sabit diskleri ancak 32GB'a kadar formatlayabilir,
- En fazla 4127920 dosya olabilir,
- Bir dosya en fazla 4GB boyutunda olabilir,
- Diskteki dağınıklık arttıkça performansı düşer,
- Büyük boyutlu dosyalara erişimi yavaştır.

NTFS (New Technology File Sytstem)

- Windows NT, 2000 ve XP'de kullanılır.
- NTFS dosya sistemi kullanan Windows NT ve 2000 sürümleri FAT sürücüleri görebilir ve bu sürücülerdeki dosyaları okuyabilirler. Ancak FAT kullanan işletim sistemleri NTFS bölümlerini göremezler.
- 256TB'a kadar HDD'leri formatlayabilir,
- Tüm dizin ve dosyaları sıkıştırabilir,
- Maksimum dosya büyüklüğü 16TB'tır, (Teorik olarak 16 EB)
- Cluster boyu küçük olduğu için yer kaybı düşüktür,
- Dosya ve dizinlere kullanıcı hakları verilerek erişim denetlenebilir,
- Dosyalarda yapılan tüm değişikliklerin kaydını tuttuğu için otomatik veri kurtarma desteği vardır,

FAT16 ve FAT32'nin KARŞILAŞTIRILMASI

	FAT 16	FAT 32
Ana dizinde	En fazla 512 dosya/klasör	İstenildiği kadar dosya/klasör
Disk Büyüklüğü	2GB destekler	2TB'a kadar çıkmaktadır.
Dosya yerleşim tablosu	Ana dizinin sabit bir yerde olmalıdır.	İstenilen herhangi bir yere taşınabilir.
Cluster boyutu	*daha büyük olup yer kaybına sebep olmaktadır.* Cluster sayısı:65536	Cluster sayısı:4177918

Partition Büyüklüğü	FAT16 Cluster Büyüklüğü	FAT32 Cluster Büyüklüğü
32 MB	**2 KB**	**512 Byte**
128 MB	**2 KB**	**512 Byte**
256 MB	**4 KB**	**512 Byte**
512 MB	**8 KB**	**4 KB**
1 GB	**16 KB**	**4 KB**
2 GB	**32 KB**	**4 KB**

- NTFS'de cluster büyüklüğü daha küçük olduğu gibi dosya ve klasörleri sıkıştırabilme özelliği vardır.
- NTFS daha büyük sabit diskleri destekliyor olup iki dosya sistemi arasında dosya adlandırma kurallarında da farklılık vardır.
- NTFS'de de FAT32'de olduğu gibi ana dizin içinde istenildiği kadar dosya-klasör oluşturulabilir.
- NTFS klasör ve dosyalar için izinler düzenleyebilir.
- Güvenlik ve daha geniş bir kullanım için sağlanan bazı destekler NTFS'nin bir diğer üstünlüğüdür.
- NTFS'nin bir dezavantajı (aynı zamanda bu bir avantajdır) ise Windows9x ve MSDOS işletim sistemlerinden ulaşılamamaktadır.

FAT16-FAT32-NTFS Cluster Boyutu

Hard disk	FAT16	FAT32	NTFS
7-16MB	2KB	Tanımaz	512B
17-32MB	512B	Tanımaz	512B
33-64MB	1KB	512B	512B
65-128MB	2KB	1KB	512B
129-256MB	4KB	2KB	512B
257-512MB	8KB	4KB	512B
513-1024MB	16KB	4KB	1KB
1025MB-2GB	32KB	4KB	2KB
2-4GB	64KB	4KB	4KB
5-8GB	Tanımaz	4KB	4KB
9-16GB	Tanımaz	8KB	4KB
17-32GB	Tanımaz	16KB	4KB
32GB-2TB	Tanımaz	Tanımaz	4KB

EXT2

- Öncelikle Virtual File System (VFS) geliştirildi.
- Linux çekirdeğine katılmadan önce Linus Torvalds tarafından tekrar yazıldı.
- VFS'nin çekirdeğine katılmasından sonra Extended File System (EXT) tamamlandı.
- Ext dosya sistemindeki sorunlara çözüm olarak Ocak –1993'de Alpha içinde Xia ve Ext2 dosya sistemi piyasaya sürüldü.
- Dosya sistemlerinde büyük/küçük harf ayrımı önemlidir.
- Bazı karakterlerin özel anlamları olduğu için dosya isimlerinde kullanılmaz.
- Unix dosya tipinin standart özelliklerini taşımaktadır.
- EXT2 büyük bölümlü diskleri yönetebilir.
- 4TB'a kadar bilgi adresleyebilir.
- 2GB büyüklüğüne kadar olan dosyalarla çalışabilir.

[GÜVENLİ SİLME VE DOSYA KURTARMA]

1. Silme ve Yok Etme Kavramları

Bilgisayarlarda dosya oluşturmak ve gereksiz hale gelen dosyaları silmek yoğun olarak yaptığımız işlerdendir. Peki, bilgisayarınızdaki bir dosyayı silmeniz durumunda gerçekte neler oluyor hiç düşündünüz mü? Dosyayı gerçekten silmiş oluyor musunuz?

Daha doğru bir tabirle silinmiş dosyaya ait içerik yok oluyor mu? Silinen dosyaları geri getirmek ya da kurtarmak gibi bir konudan bahsedildiğine ve bu işlem de yapılabildiğine göre demek ki dosyamızın içeriği gerçekte silinmiyor ve bir yerlerde duruyor. "Silmek ya da Yok etmek " şeklinde bir ifade ile olayı anlatmaya çalışmamızın nedeni de işte bu.

İşletim sistemleri, diskin ilk kullanım öncesi organize edildiği yapı olan ve FAT, NTFS, Ext2/3FS gibi ifadelerle bilinen ve dosya sistemi (file system) denilen yapılar ile dosyalarımızı diskte küme adı verilen birim alanlarda tutarlar. Biz bir dosya oluşturduğumuzda, işletim sistemi bu dosyaya boyutu oranında o an diskte kullanım dışı olan kümelerden tahsis eder.

Ayrıca, sistem alanında da dosyaya ait özel bilgileri (adı, türü, tarihi vb.) ve dosyanın içeriğinin saklandığı küme listesini tutar. Dikkat edecek olursanız, dosyaya boş kümeler değil, o an kullanım dışı olan kümeler tahsis edilmektedir diyoruz. Bunun neden böyle olduğu aslında kolaylıkla tahmin edilebilir. Disk bölümündeki veri alanında bulunan belirli sayıda birim boyuta sahip kümenin durumu, yani kullanımda olup olmadığı ve hangi dosyaya ait veriyi içerdiği bilgisi, tüm dosya sistemlerinde genellikle bir tablo içerisinde tutulur.

Buradan ortaya çıkan sonuç ise, gerçekte önemli olan, bir kümenin içinde bir şeyler olup olmadığı değil, küme kullanım ve tahsis tablosunda bu kümenin durumu ile ilgili verilen bilgidir. Yani küme kullanımda mıdır yoksa şu an sahipsiz midir. Kullanımda ise hangi dosyaya ait kaçıncı kümedir gibi. Kümelerdeki verileri bilfiil silmek, ya da bu olayı ifade etmek üzere seçmiş olduğumuz asıl kelime ile olayı ifade edersek, verileri yok etmek, işletim sistemlerine kaldırılması mümkün olmayan yükler bindirmekte ve asıl kullanım amaçlarını saptırmaktadır. Verdiğimiz bu bilgiler çerçevesinde kolaylıkla tahmin edileceği ve anlaşılacağı üzere, biz bir dosyayı veya dosya grubunu sildiğimizde, gerçekte sadece dosyaya ait kümeler yeni kullanımlar için kullanım tablosunda boş ya da daha doğru bir tabirle, şu an herhangi bir dosya tarafından kullanılmayan ve yeni açılacak veya büyütülme şeklinde değiştirilecek dosyalara tahsis edilmek üzere bekleyen kümeler olarak işaretlenmektedir.

Veri alanındaki kümeler gözümüzle gördüğümüz şeyler olmadığı için içinde bir şeyler olup olmadığının aslında hiçbir önemi yoktur. Peki, sildiğimiz dosyalardaki bilgiler gizli bilgiler ise veya sildiğimiz bilgilere herhangi bir şekilde ulaşılmasını istemiyorsak ne olacak. İşte bu noktada silinen bilgilerin gerçekten silinmesi konusu gündeme gelmektedir. Şimdi en başa dönüyoruz ve olayı daha kolay anlaşılabilmesi açısından ayırıyoruz. Dosyaları silmek derken dosyalara ait kümelerin başka kullanımlar için serbest bırakılmasını, dosyaları yok etmek derken de dosyalara ait olan kümelerdeki verilerin bilfiil ortadan kaldırılmasını söylüyoruz.

Diyelim ki 2 yıldır bilgisayarınızı kullanıyorsunuz. On binlerce dosya oluşturdunuz. Sildiniz, yeniden yüklediniz. Diskinizi formatladınız. Yeniden sistem yüklediniz. Yüzlerce kez internete girdiniz. Pek çok program yüklediniz ve kaldırdınız. Şu an ise diskinizde 25.000 adet dosya var ve diskinizin %43'ü dolu. Tahmin edeceğiniz üzere, şu ana kadarki işlemleri standart işletim

sistemi araçlarıyla yaptığınız için, diskinizde eski dosyalara ve silinmiş dosyalara ait veriler tamamen veya kısmen, şu an kullanım dışı olan kümeler içerisinde durmaktadır.

Kullanmakta olduğunuz diskin kapasitesi size az gelmeye başladı ve yeni bir disk almaya karar verdiniz. Yeni bir disk aldınız ve elinizdeki diski de çorbada tuzu olsun diye ikinci el olarak satmaya karar verdiniz. Eski diski formatladınız ve tertemiz(!) bir hale getirdiniz. Sonra da uygun bir fiyata tanımadığınız birine sattınız. Dikkat!!! Eski diskinizdeki bilgiler hala duruyor! İşin asıl kötü yanı, gerek meraklısı gerekse kötü niyetlisi tarafından bu bilgiler ortaya çıkarılabilir. Dünyaca ünlü haber ajanslarından birinin verdiği bir habere göre, özellikle gelişmiş ülkelerde bu yöntemle pek çok özel bilgi çalınmakta ve kötü amaçlar için kullanılabilmektedir. Böyle bir disk pekâlâ rakip firmanıza, bir bankaya, resmi bir kurumu ve saygın bir kişiye ait olabilir.

O halde şimdi diskteki verilerin gerçekte yok olmadığı durumların neler olduğu ve gerekmesi durumunda nasıl yok edilebileceği konusunun detaylarına geçelim. 2 yıldır kullanılmakta olan disk örneğimizdeki diskin durumunu dikkate alarak olayı açıklamaya çalışalım.

1) **Dosya silerken, dosyanın içeriğinin de yok edilmesi**: Standart işletim sistemi araçları asla böyle bir işlem yapmaz. İşletim sistemleri, bahsettiğimiz üzere silinen dosyalara ait kümeleri yeni kullanımlar için serbest bırakır. Dosya sildikten sonra diski birleştirmek, büyük boyutlu önemsiz dosyaları diske kaydedip silmek (film dosyası gibi), silinen dosyaya ait kümelerin mevcut veya yeni dosyalar tarafından kullanılması sonucunu doğurabilir. Ancak bu tür işlemlerin ilkel yaklaşımlar olacağı ortadadır. Silmek istediğiniz dosyalarınızı disk yüzeyinden de silmek yani yok etmek istiyorsanız, bu tür işlemleri gerçekleştirmek üzere yazılmış özel programlar kullanmanız gerekir.

2) **Diskte şu an kullanım dışı olan kümelerin, başka bir tabirle diskteki boş alanın içeriğinin yok edilmesi:** Yine, 2 yıldır kullanılan disk örneğimizde tahmin edileceği üzere, diskin şu an kullanılmayan kümeleri büyük ihtimalle eski veya silinen dosyalar tarafından kullanılıyor durumdadır. Diskin formatlanmadan önceki haline ait dosyaların bulunduğu kümelerin ve silinen dosyalara ait kümelerin, sadece yeni dosyalara tahsis edilmiş olanları içerisindeki bilgiler gerçekten silinmiştir, yani yok olmuştur. Peki, bu bilgileri şimdi nasıl yok edeceğiz. Tüm yok etme programlarında olduğu gibi, bahsettiğim programda da böyle bir seçenek bulunmaktadır. Yani şu an kullanım dışı olan kümelerdeki verilerin yok edilmesi. Bu işlem diskin kapasitesine ve kullanılmayan miktarına göre uzun zaman alabilecektir. Ama yine de bu işlemin yapıldığı esnada başka bir işlem yapılmaması sorun çıkmaması açısından daha iyidir.

3) **Daha önce başka dosyalar tarafından kullanılmış olan ve şu an herhangi bir dosyanın son kümesi olan kümedeki artık verinin yok edilmesi:** Disk bölümlerindeki veri alanlarında dosyaların belirli sayıda sektörden oluşan birim alanlarda tutulduğunu ve bu birim alanları küme şeklinde isimlendirdiğimizi söylemiştik. Bir dosya, bölümdeki veri alanına yerleştirilirken, boyutu küme boyutuna bölünür ve dosyanın kaç kümeye yerleştirileceği tespit edilir. Bunu bir örnek dosya üzerinde açıklamaya çalışalım. Küme boyutumuz 8.192 bayt (yani 16 sektör) ve dosya boyutumuz da 18.512 bayt olsun. İşlemi yapalım.

18.512 / 8.192 = 2 ve kalan = 2.128

Bu hesaba göre dosyaya üç küme tahsis etmemiz gerekiyor. Dikkat edilirse, son kümenin 2.128 baytı dosyaya ait, kalan 6.064 baytı ise ait değildir. Veri alanı küme blokları şeklinde adreslendiği için bu durum kaçınılmazdır. Yani son kümedeki 6.064 bayt kayıp alan olarak duracaktır ve hiçbir dosyaya ait olmayacaktır. Peki, bu küme daha önce başka bir dosya tarafından kullanılmış bir ara küme ise. Yani eski dosyanın son kümesi değilse. O zaman bu 6.064 baytlık kısımda bir bilgi olabilir demektir. Eski ve silinmiş dosyalara ait verileri tamamen yok etmek istediğimizde son kümelerdeki artık alanlardaki verilerin de yok edilmesi gerektiği ortadadır. Üzerine yazılmış disk bölümlerinde yapılan veri kurtarma çalışmalarında genellikle bu alanlar dikkate alınmaktadır. Özellikle küme boyutu büyük olan bölümlerde bu yaklaşım ile imkânsız gibi görünen durumlarda bile verilerin bir kısmına ulaşılabilmektedir. Çoğu yok etme programı, dosyalara ait son kümelerdeki artık alanları temizleme ile ilgili seçeneklere sahiptir.

4) **Formatlanmış bir disk bölümündeki veya yeni bir amaç için kullanılacak diskin tamamındaki verilerin yok edilmesi:** Formatlanmış bir disk bölümündeki eski verilerin yok edilmesi işlemi, bölüm içerisinde kullanımda olmayan kümelerin içeriğinin yok edilmesi işlemi gibidir. Bu işlemi diskin tamamına uygulamak için disk tek bölüm halinde düzenlenip formatlanır ve kullanımda olmayan küme yok etme işlemi uygulanır. Diskteki sektörlerin tamamının içeriğini yok etmek istediğimizde ne yapacağız. Bu işlem için de geliştirilmiş programlar bulunmaktadır. Hard disk üreticileri de genellikle kendi markaları üzerinde bu işlemi gerçekleştiren programlar sağlamaktadır. Hard format olarak bilinen ve diskteki alt seviye mantıksal yapıyı yeniden düzenleyen programlar da bu işlemi gerçekleştirmek üzere kullanılabilir.

2. İşletim Sistemlerinde Güvenli Silme

Bilgisayardan silinen hiçbir dosya gerçek anlamda sabit diskten silinmemektedir. Dosyaların delete tuşu ile silinmesi, (shift + delete) tuş bileşimi ile silinmesi, çöp kutusundan silinmesi ve hatta sabit diskin defalarca kez biçimlendirilmiş olması bile bu durumu değiştirmemektedir. Silinen dosyaların bir bölümü çeşitli veri kurtarma yazılımları aracılığıyla geri getirilebilmektedir. Silinen dosyaların geri getirilemez hale gelmesi için üzerine yeni veri yazılması gereklidir. Güvenli veri silme yazılımları, silmek üstediğiniz dosyalar üzerine defalarca kez rastgele verilere yazarak kullanılamaz hale getirmeyi amaçlarlar.

Eğer sildiğiniz bir dosyanın bu tür programlarla kurtarılamamasını istiyorsanız, güvenli silme işlemi yapmanız lazım. Yine piyasada bu işlemi yapan birçok program mevcut. Bu programlar silmek istediğiniz dosyanın diskte bulunduğu yere -tıpkı oraya başka bir dosya kopyalamışsınız gibi- rastgele veriler yazıyorlar. Böylece orada bulunan eski dosya artık kurtarılamaz hale geliyor. Bu işlemi ister belirli bir dosyayı silerken yaptırabiliyorsunuz, ister diskteki boş alanda eskiden bulunmuş olan dosyaları güvenli bir şekilde ortadan kaldırmak için, isterseniz diskin tamamını güvenli bir şekilde silebiliyorsunuz.

Ancak, güvenli disk temizleme işlemi yapan programlar, diskteki verilerin üzerine yeni veriler yazarken farklı metotlar kullanıyorlar. Örneğin Eraser isimli program size 6 farklı metottan birini seçme imkânı sunuyor. Bu metotların çoğu eski verilerin üzerine yeni verileri yazma işlemini birden fazla kez yapıyorlar. Örneğin Gutmann Metodunu seçmişseniz verilerin üzerine 35 kere tekrar tekrar veri yazılıyor.

Madem bu verilerin üzerine bir kere yazıldığında dosyalarımızı kurtaramıyoruz, neden tekrar tekrar yazmaya gerek var? Bu sorunun cevabını araştırdım ve vardığım sonuç şu: Hard diskin içinde verilerin yazıldığı plaka sökülüp, özel mikroskoplarla (Magnetic Force Microscope) incelenerek eski verilere ulaşılabiliyor. Ancak bu son derece zahmetli, pahalı ve yavaş bir işlem. Üstelik verilerin tamamının kurtarılabilmesi de garanti değil. Özellikle yeni üretilen disklerde eski verilerin ne olduğunu bu mikroskoplarla tespit etmek çok daha zor.

Özet olarak eğer diskinizi bu özel mikroskopla inceleyecek birileri sizi kovalamıyorsa, silmek istediğiniz kısma sadece 1 kere yeni veriler yazmanız kesinlikle yeterli.

Bu bölümde tavsiye edilenler gibi güvenli bir silme aracı kullandığınızda, hassas bilgilerinizi basitçe silmek yerine bu bilgileri bir başkasıyla değiştirdiğinizi ya da bu bilgilerin 'üzerine yazmış' olduğunuzu söylemek daha doğru olacaktır. Yukarıda anlatılanların dosya dolabında saklanan belgelerin kurşun kalemle yazılmış olduğunu hayal edecek olursanız, güvenli silme yazılımı sadece içeriği silmekle kalmaz ayrıca her sözcüğün üzerini de karalar. Ve kurşun kalem izi gibi, dijital bilgiler de silinseler ve üzerlerine başka bir şey yazılsa bile, her ne kadar az da olsa, okunabilir. Bu nedenle burada tavsiye edilen araçlar gelişigüzel seçilen verilerle dosyaların üzerine defalarca yazar. Bu işlem, kalıcı silme işlemi (wiping) olarak adlandırılır ve bilginin üzerine ne kadar çok yazılırsa birinin özgün içeriği kurtarması da o kadar güçleşir. Uzmanlar genellikle üç ve daha fazla yazma işleminin yapılması gerektiği konusunda hemfikirdir; bazı standartlar ise yedi ve daha fazlasını gerektirir. Kalıcı silme yazılımı, otomatik olarak bilginin üzerine makul bir sayıda yazma işlemi yapar ama istediğiniz takdirde bu sayıyı değiştirebilirsiniz.

3.1 Windows İşletim Sistemlerinde Güvenli Silme

Birçoğumuz, bilgisayarımızdaki bir dosyayı çöp kutusuna attığımızda ve çöp kutusunu temizlediğimizde bu dosyanın silindiğini düşünürüz. Ancak bir dosyayı silmek, o dosyayı tamamen yok etmez. Bir kişi bu işlemi gerçekleştirdiğinde, bilgisayar sadece silinen dosyayı kullanıcıya görünmez yapar ve dosyanın sürücüde depolandığı bölümü "mevcut" olarak gösterir (Bu işletim sisteminizin o dosya üzerine tekrar yazabileceği anlamına gelir). Bu yüzden sildiğiniz dosyanın üzerine yeni bir dosyanın yazılması haftalar, aylar hatta yıllar bile sürebilir. Sildiğiniz dosyanın üzerine yeni bir dosya yazılana dek, "silinmiş" olan dosya sürücünüzde yer almaya devam eder; sadece normal işlemlere gözükmez. Ve biraz uğraş ve doğru araçlarla ("silinmeyi geri alan" programlar ya da adli yöntemler gibi) bu dosyaları geri getirmeniz bile mümkündür. Bilgisayarlar normal bir şekilde dosyaları "silmez"; sadece bu dosyaların kapladığı yerlerin gelecekte başka dosyalar tarafından kullanılmasına izin verirler.

Bu durumda bir dosyayı sonsuza dek silmenin en iyi yolu, önceden yazılmış olan bir dosyanın geri alınmasını zorlaştıracak şekilde, bu dosyanın üzerine yeni bir dosyanın yazılmasıdır. Bunun için 3. Parti yazılımlar mevcuttur. Bu tarz yazılımlar anlamsız dosyaları sürücünüzün "boş" olan kısmının üstüne yazar ve silinen verilerinizin gizliliğini korur.

Ancak katı hal diskleri (SSD'ler), USB flash bellekleri ve SD kartlarındaki verileri güvenli bir şekilde silmek oldukça zordur! Aşağıda değineceğim güvenli silme işlemleri yalnızca geleneksel sabit sürücüler için geçerlidir ve bu işlemler modern dizüstü bilgisayarlarında standart haline gelmeye başlayan SSD'leri, USB anahtarlarını veya USB belleklerini ya da SD kartları veya flash hafıza kartlarını kapsamaz.

Windows işletim sistemine sahip bilgisayarda Eraser açık kodlu yazılımı kullanacağım.

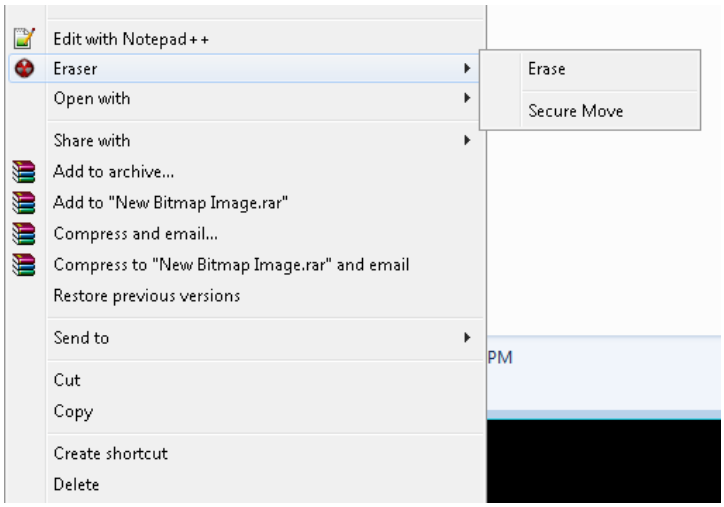
Eraser üceretsiz, kullanması oldukça kolay açık kaynak kodlu bir güvenli silme aracıdır. Eraser ile dosyalara üç farklı şekilde kalıcı silme işlemi uygulayabilirsiniz: bir dosyayı seçerek, Geri Dönüşüm Kutusu'nun içeriğini seçerek ya da diskteki 'atanmamış' alanın tamamına kalıcı silme işlemi uygulayarak. Eraser ayrıca aşağıda ele alınan Windows'un swap dosyalarının içeriğine de kalıcı silme işlemi uygulayabilir.

Güvenli silme araçları, görünür dosyalarınıza özel olarak kalıcı silme işlemi uygulamadığınız sürece bu dosyalara zarar vermez; ancak yine de bu tür yazılımları kullanırken tedbirli olmak önemlidir. Her şeye rağmen kazalar olabilmektedir; insanların Geri Dönüşüm Kutularını ve veri kurtarma araçlarını faydalı bulmalarının nedeni de budur. Bir şeyleri sildiğiniz her seferinde verilerinize kalıcı silme işlemi uygulamayı alışkanlık haline getirdiyseniz kendinizi basit bir hatadan kurtaramaz durumda bulabilirsiniz. Bilgisayarınızdan büyük miktarda veriye kalıcı silme işlemi uygulamadan önce güvenli bir yedeklemeye sahip olduğunuzdan daima emin olun.

Eraser ile bir dosyayı/klasörü/sürücüyü/boş alanı güvenli sileme:

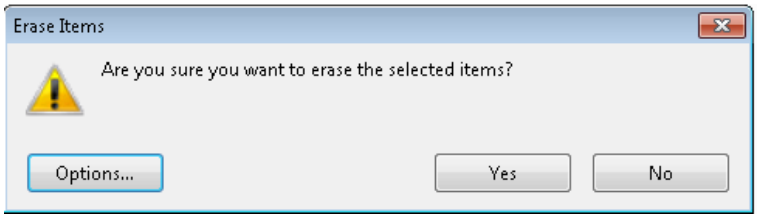
Eraser programını bilgisayarımıza indirip kurduktan sonra otomatik olarak silmek istediğimiz her dosya için kullanılabilecektir. Bilgisayarı restart etmemize gerek yoktur.
Eraser programı tek bir dosyayı güvenli silmek istediğimizde ya da bir klasörden ve ya sürücüden(usb bellek,sd kart vb.) güvenli olarak taşımak istediğimde bize çok büyük kolaylıklar sunmaktadır. Herhangi bir dosyanın üzerini sağ click yaptığımızda aşağıdaki seçenekler gelecektir.

[GÜVENLİ SİLME VE DOSYA KURTARMA]



Erase seçeneği dosyayı kalıcı olarak yok etmek için kullanılır. Bu seçeneği tıkladığımızda bize emin olup olmadığımıza dair uyarı kutusu çıkar. Eğer onaylarsak dosya geri döndürülemeyecek şekilde silinir.

Dosyayı silmek ya da taşımak istediğimizde çıkan uyarı kutusu aşağıdaki gibidir. İstersek options bölümüne gelerek diğer işlemlerde bu uyarı kutusunun gelmemesini sağlayabiliriz.

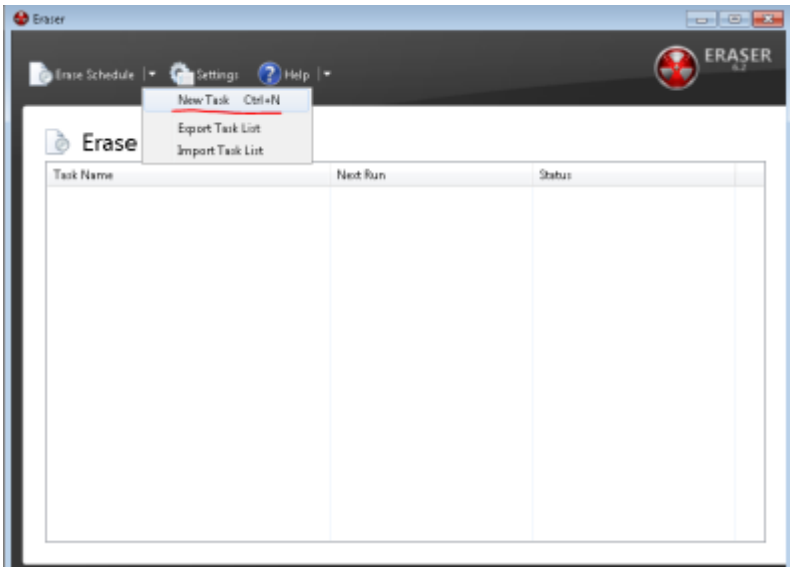


Bir diğer seçenek ise Secure Move'dir. Bu seçenek dosyayı bir yerden başka bir yere taşır ve önceki klasöründe bulunan dosyayı güvenli olarak siler. Geçmişe dönük dosyaların kopyalarını kolayca silebilir.

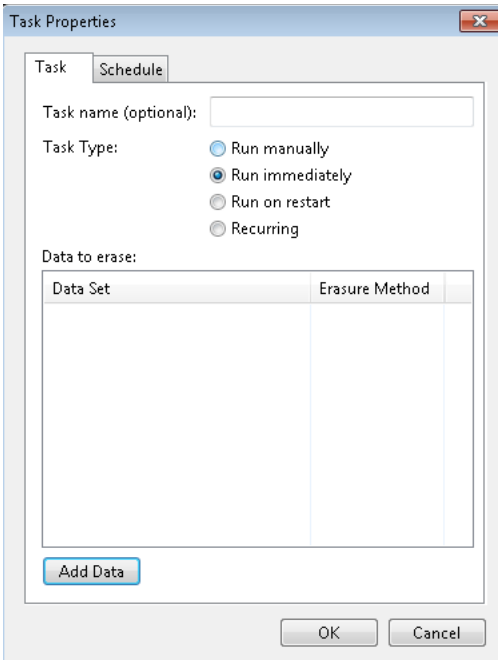
Windows işletim sistemine sahip bilgisayarların diskindeki boş alanların(kümelerin) güvenli bir şekilde silinmesi:

Bilgisayarımızın boş bölümlerini kalıcı olarak silmek için öncelikle Eraser'de Schedule Task açmamız gerekiyor. Bunu bize sormasındaki amaç bu işlemlerin uzun zaman almasıdır(ortalama 2-5 saat). Bu şekilde zamanlama yaparak bilgisayarı kullanmadığımız zaman işlemleri gerçekleştirebiliriz. Bizim için büyük kolaylık sunmaktadır.

[GÜVENLİ SİLME VE DOSYA KURTARMA]

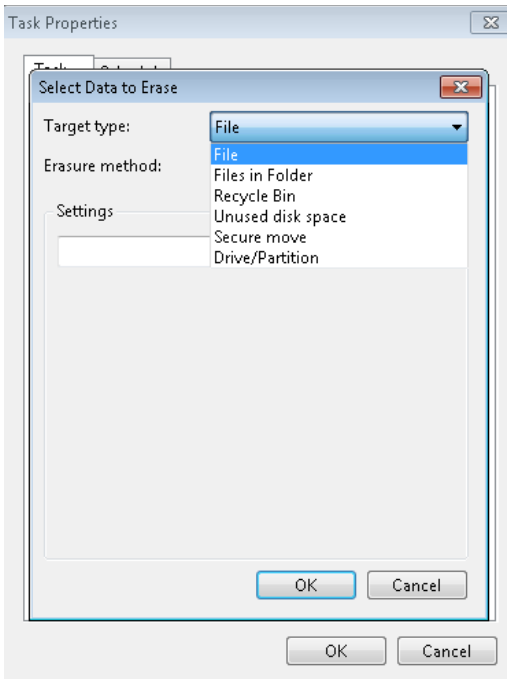


Task ismini girdikten sonra **Task Type** kısmından gerçekleştireceğimiz güvenli silme işleminin ne zaman yapılması gerektiğini sormaktadır.

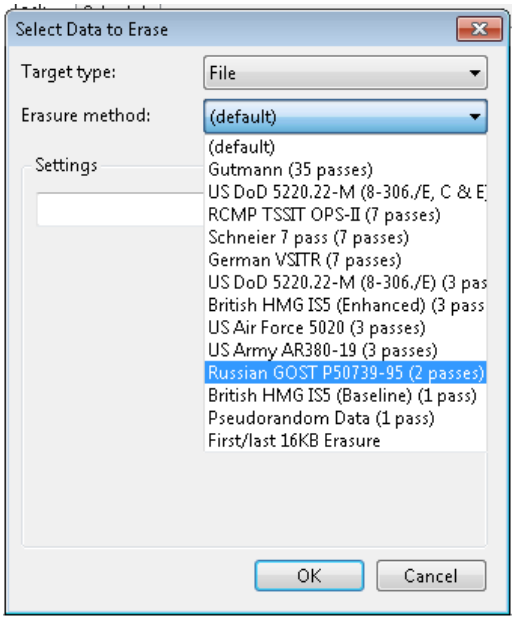


Daha sonra **Add Data** kısmından hangi tür işlem yapacaksak onu seçmemiz gerekiyor.

Bu aşamada **File**'nin seçilmesi bir dosyanın güveli silme işleminin yapılmasını, **Files in Folder** seçilmesi klasör içindeki dosyaların hepsinin güvenli silinmesini, **Recycle Bin** ise geri dönüşüm kutusunda bulunan dosyaların güvenli olarak silinmesini, **Unused disk space** ise diskin kullanılmayan kümelerinin güvenli olarak silinmesini, **Secure move** ise bir dosyayı bir klasörden diğer klasöre güvenli olarak taşımayı **Drive/Partition** ise bir sürçünün ya da bir bölümün komple geri döndürülemeyecek şekilde silinmesini sağlar. Bu bilgiler ışığında yapmak istediğimiz işlemi seçiyoruz.

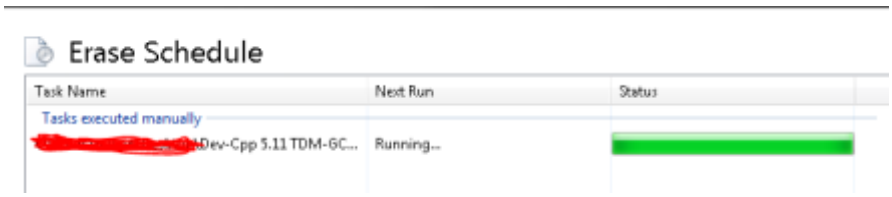


Target Type seçtikten sonra bize **Erasure method** seçmemizi istiyor bu kısım yok etme işleminde gerçekleştirilecek metoddur. Daha öncede bahsettiğim gibi 1 fazın yeterli olduğu fakat standartlarda 7 fazın geçtiğini belirtmiştim. Verinin kritikliğine göre istediğimiz fazı seçiyoruz.



Son olarak silme işlemini hangi dosya/klasör ya da sürücü için gerçekleştirilmesini istiyorsak **Browse** kısmından seçiyoruz.

Gerekli ayarları girip ok tıkladıktan sonra Eraser ana ekranında işlemin durumu hakkında bilgi alabiliriz. Dosyaların boyutu ve işlemin metoduna göre süre değişebilir.



İşlem tamamlanınca ekrandan kaybolacaktır.

3.2 İOS İşletim Sistemlerinde Güvenli Silme

Silmek istediğimiz dosyayı güvenli bir şekilde yok etme:
İos işletim sistemine sahip bilgisayarlarda güvenli silme işleminin herhangi bir 3. parti yazılıma ihtiyaç duymadan yapılabilmektedir. Mac'imiz aslında çöp kutusunu hep normal bir şekilde boşaltıyor. Elbette sıradan dosyalar için önemli bir detay olmasa da, önemli veriler, gizli dosyalar ve geri getirilmesinin problem yaratacağı şeylerle uğraşıyorsak, çöpümüzü mutlaka güvenli bir şekilde boşaltmalıyız.

Mac'imizdeki çöpü güvenli bir şekilde boşalttığımızda ise veriler sadece silinmekle kalmıyor, geri getirilememeleri için üzerlerine rastgele (anlamsız) şeyler de yazılıyor. Böylece bir daha geri getirilmesi çok zor bir hale getiriliyor. Fakat bu yöntemi tercih ettiğimizde elbette çöpün her boşaltılması normalden çok daha uzun sürüyor.

Dock'ta Finder simgesini tıklayın, sonra Finder > Çöp Sepetini Güvenli Boşalt öğesini seçin. Uyarı mesajı gördüğünüzde Tamam'ı tıklayın.

Empty Trash (Çöpü Boşalt)

Secure Empty Trash (Çöpü Güvenli Boşalt)

İpucu: Dock'taki çöp ikonuna (Trash) sağ tıkladığımızda command tuşuna basılı tutarak çöpün nasıl boşaltılacağını değiştirebiliyoruz

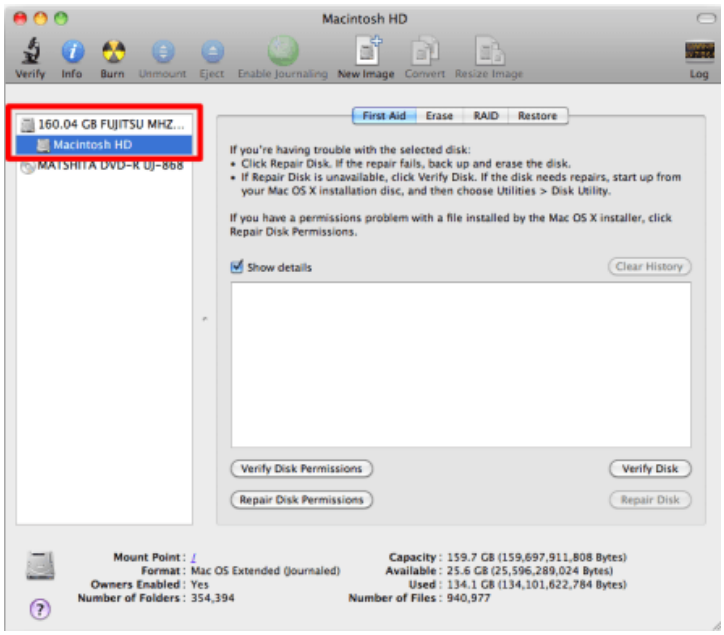
İos işletim sistemine sahip bilgisayarların diskindeki boş alanların(kümelerin) güvenli bir şekilde silinmesi:

Daha önce sildiğimiz bu verilerimizin hala geri getirilebilme ihtimali olduğu için, istersek diskimizde boş alan olarak görülen kısmı da güvenli hale getirebiliyoruz. Diskimizde boş olarak görünen alanın üzerine rastgele (ya da sıfırlayarak) veriler yazıp silerek, daha önceden sildiğimiz verilerimizin de geri getirilemeyecek şekilde diskimizi düzenleyebiliyoruz.

Bunun için aşağıdaki adımları izlememiz gerekiyor:

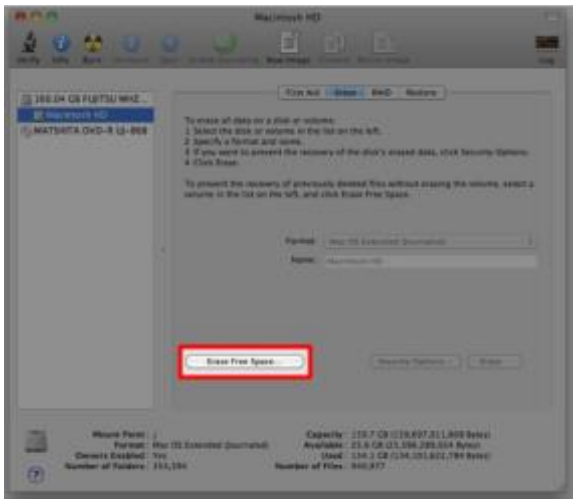
Disk Utility uygulamasını çalıştırıyoruz. Bu uygulamaya Spotlight'ı kullanarak ya da Applications klasörü içerisindeki Utilities klasöründen erişebiliyoruz.

Disk Utility uygulaması içerisinde sol taraftan kendi diskimizi seçiyoruz.



Sağ kısımdan Erase (Sil) sekmesine geçiyoruz.

Aşağıdan "Erase Free Space" (Boş Alanı Sil) butonuna tıklıyoruz.

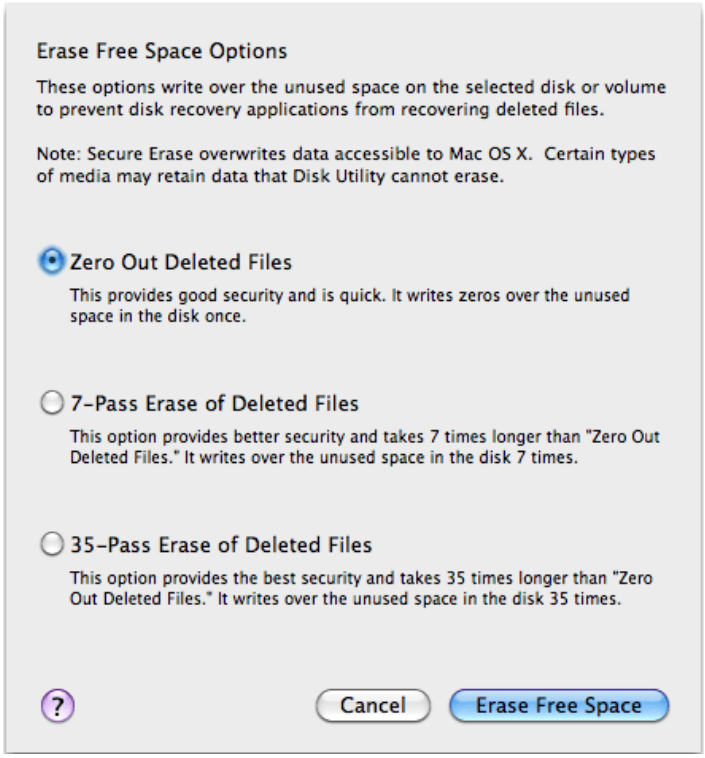


Bu aşamada karşımıza yeni bir pencere geliyor ve 3 farklı silme yönteminden bir tanesini seçmemiz gerekiyor:

Zero Out Deleted Files (Silinmiş Dosyaları Sıfırla): Hızlı ve güvenli bir silme yöntemi. Tüm boş alanların üzerine 0 (sıfır) yazıyor.

7-Pass Erase of Deleted Files (Silinmiş Dosyaları 7-Geçiş ile Sil): Daha güvenli bir yöntem. Tüm boş alanların üzerinden 7 kere geçerek üzerlerine farklı veriler yazıp siliyor. Böylece geri getirilmeleri çok daha zorlaşıyor. "Zero Out"a göre 7 kat daha uzun sürüyor.

35-Pass Erase of Deleted Files (Silinmiş Dosyaları 35-Geçiş ile Sil): En güvenli yöntem. Tüm boş alanların üzerinden 35 kere geçerek üzerlerine farklı veriler yazıp siliyor. Böylece geri getirilmeleri çok çok daha zorlaşıyor. "Zero Out"a göre 35 kat daha uzun sürüyor.



"Erase Free Space" butonuna tıklayarak diskimizdeki boş alanı silme işlemine başlayabiliyoruz. Diskimizdeki boş alanın büyüklüğüne ve seçtiğimiz silme yöntemine göre bu işlemin süreci değişebiliyor. Tahmin edebileceğiniz gibi, eğer diskimizde çok fazla boş alan varsa, silme işlemi de bununla orantılı şekilde uzun oluyor.

3.3 Linux İşletim Sisteminde Güvenli Silme

Linux işletim sistemine sahip bilgisayarlarda güvenli silme işlemini yapmak için shred komutunu kullanacağım. Bu komut kullanımı kolay ve birçok linux platformunda default olarak gelmektedir. Kali platformunda blunmaktadır.

Uygulama işletim sisteminizde yoksa kullandığınız platformun repository'sinden indirebilirsiniz. Açık kaynaklı kod olduğu için internette bulmakta son derece basittir.

Güvenli veri silmek için kullanabileceğiniz bu yazılım Kali ile birlikte kurulu gelmektedir. Bu yazılım terminal üzerinden komutlar aracılığıyla kullanılmaktadır. Yazılımın dosya yöneticisinde sağ tıklama menüsüne eklenmesi de mümkündür. Terminalde man shred komutu kullanılarak yazılımın kullanımı hakkında İngilizce dilinde detaylı bilgi edinilebilir. Şimdi yazılımın komut satırı üzerinden kullanımını örnekleyelim.

Mesela test.txt ismindeki bir dosyası silmek istediğimizi farzedelim. Bunun için terminal komut satırı ekranını açın ve cd komutu yardımıyla söz konusu dosyanın bulunduğu dizine geçin. Ardından şu komutu kullanın:

```
Shred test.txt
```

Bu komut test.txt dosyasının üzerine 25 kere rastgele veriler yazar. Bu sayıyı değiştirmek güvenliği artırır. Bunun için -n parametresini kullanırız:

```
shred -n 100 test.txt
```

Böylece 100 kere geçiş yaparız. -u parametresini kullanarak yazdırma işleminden sonra dosyayı silmesini sağlarız. (içinde rastgele veriler olsa da -u kullanılmadan silinmez.)

```
shred -u  -n 100 test.txt
```

-v parametresi ise yapılan işlemler hakkında sizi bilgilendirir.

Tüm sabit diski silmek isterseniz bunun için alttaki komutu kullanabilirsiniz.

```
shred -n 100 -u /dev/sda
```

Tüm diski değilde diskin sadece bir bölümünü komple silmek isteyebilirsiniz. Örneğin diskin 2. bölümünü silmek için:

```
shred /dev/sda2
```

Linux işletim sistemine sahip bilgisayarların diskindeki boş alanların(kümelerin) güvenli bir şekilde silinmesi:

Bir önceki alt bölümde linux işletim sistemine bilgisayarda bulunan dosya, klasör veya bölümlerin silinmesi işlemini detaylıca anlatmıştık. Bu bölümde diskimizdeki boş alanların güvenli olarak silinmesi ve bu sayede boş alanlarda bulunan kullanım dışı kümelerden geri döndürme işleminin yapılmamasını sağlayacağız.

Bu işlem için **secure-delete** komutunu kullanacağız.

Uygulamayı kurmak için terminal ekranına aşağıdaki komut yazılır:

```
sudo apt-get install secure-delete
```

Dosyayı kurduğumuzda birçok araç gelmektedir. Bunlar srm, smem, sfill vb. komutlardır. Bizim kullanacağımız **sfill** komutudur.

sfill: Diskinizdeki boş alanları silmenizi sağlar. Bu alanlar boştur ama eski dosyaların kalıntıları gizlice yerli yerindedir.

```
sfill /
```

kök dizininizde çalışarak sisteminizin bulunduğu diskteki boş alanları rastgele verilerle doldurur.

```
sfill /tmp
```

komutu tmp dizininizde aynı işi görür. Bu dizinlere diğer disklerinizi bağlayıp çalıştırabilirsiniz.

4 Silinmiş Dosyaları Kurtarma

4.1 Windows İşletim Sistemlerinde Dosya Kurtarma

Windows bilgisayarlarda dosya kurtarma işlemini Recuva programını kullanarak gerçekleştireceğiz. Bilindiği gibi dosyalar silindiğinde gerçekte o dosya silinmiyor. O dosyaya tahsis edilen kümeler boşa çıkıyor. Eğer disk alanınınız müsaitse bu boş kümelere yeni dosyalar yazılmadığı sürece normal silme işlemi ile silinen dosyaları geri getirebiliriz.

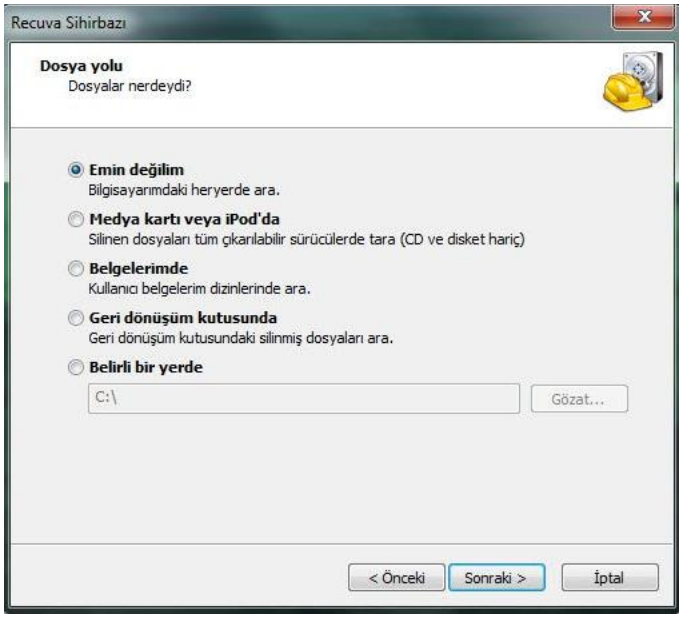
Recuva Nedir?

Recuva, piyasanın en popüler ücretsiz sistem araçlarından biri olan CCleaner'ın yapımcısı Piriform tarafından geliştirilen ücretsiz bir dosya kurtarma aracıdır. Recuva ile sabit disk, flash bellek, kamera, ipod gibi bir çok veri depolama aygıtından silinen verilerimizi kurtarma şansına sahibiz. Oldukça kullanışlı bir arayüze sahip olan program her tür bilgisayar kullanıcısının kolayca kullanması için tasarlanmış ve aynı zamanda programın Türkçe dil desteğine sahip olması da bizim için artı bir yön teşkil etmekte.

Programı kurup çalıştırdıktan sonra karşımıza açılış ekranı gelmektedir.

Programı kolay bir şekilde kullanabilmemiz için hazırlanmış olan "Recuva Sihirbazı" gelecek. Eğer sihirbazın açılışta karşınıza tekrar gelmesini istemiyorsanız "Açılışta bu sihirbazı gösterme." kısmına tik atarak "Sonraki >" butonuna tıklayarak devam ediyoruz. Karşımıza yeni gelen dosya türü seçme penceresinde

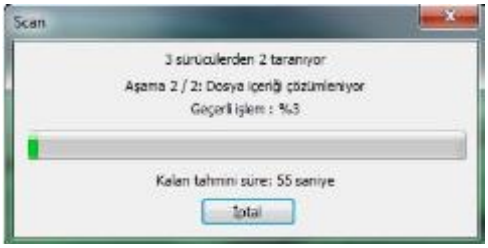
Kurtarmak istediğimiz dosya türleri olarak resimler, müzik, belgeler, görüntü, sıkıştırılmış, e-postalar ve diğer menülerinden kullanmak istediğimizi seçerek "Sonraki >" butonuna tıklayarak devam ediyoruz ve kurtarmak istediğimiz dosyaları nerede aratmak istediğimize dair bir pencereyle karşılaşıyoruz.



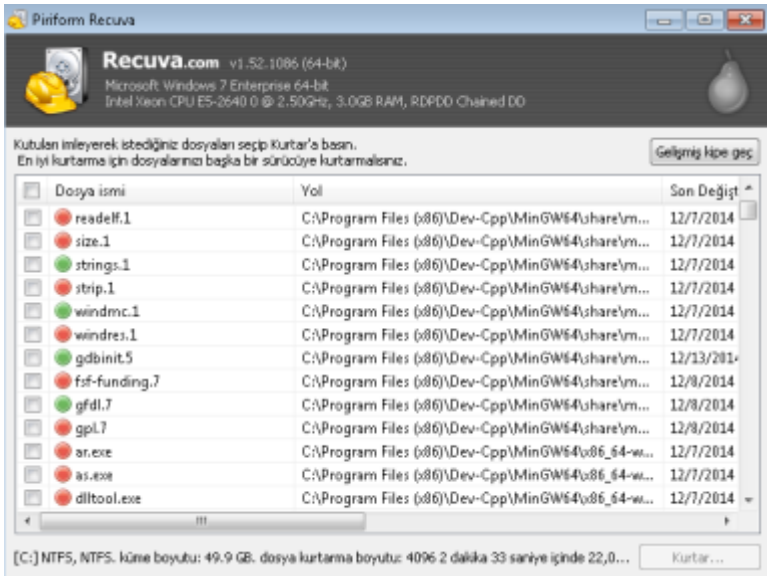
Bu pencerede silinen dosyalarınızı nerede aramak istediğinizi seçerek "Sonraki >" butonuna tıklayarak işlemimize devam ediyoruz. Son olarak karşımıza kurtarma işlemine başlamadan önce silinen dosyalarımız için disklerimizi taramayı başlatmamıza olanak tanıyacak olan

penceresi geliyor. Eğer burada "Derinlemesine Taramayı Aç" seçeneğini seçerseniz arama işlemi baya uzun sürebilir ama daha sağlıklı bir arama olacaktır. İşlemin hızlı olması için bu sekmeyi tıklamadan "Başlat" butonuna basarak devam etmenizi öneririm. Ve Recuva silinen dosyalarımızı aramaya başlıyor.

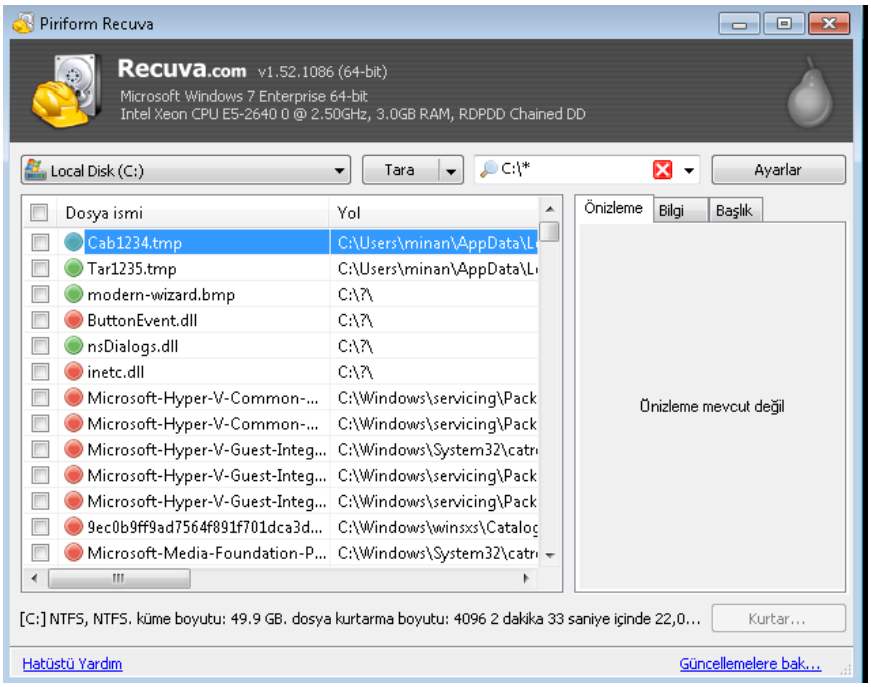
Benim gözlemlerim derinlemesine tarama seçilmediğinde belirli gün öncesi(örn 2 gün öncesi silinen dosyalar) tarama yaparak hızlı sonuç getiriyor.



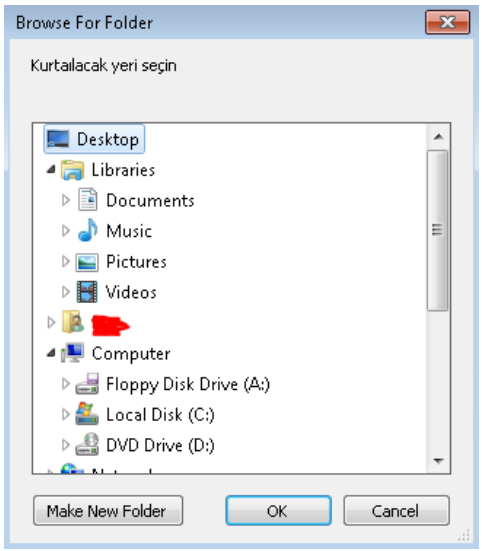
Arama işlemi sonlandığında aşağıdaki ekran karşımıza çıkarak kurtarılabilir dosyaları seçebiliyoruz.



Kurtarılabilecek veya kısmen kurtarılabilecek olan dosyaların listelendiği arama sonuç penceresi geliyor. Burada istediğimiz dosyaları seçerek kurtarma işlemine başlayabilir veya daha ayrıntılı bilgi için gelişmiş kipe geç seçeneğine tıklayarak

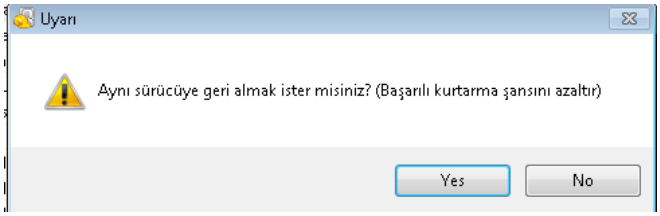


Gelişmiş arama sonuç penceresine ulaşabiliriz. Burada yanında yeşil renk olan dosyalar kurtarılabilir olan dosyaları belirtirken, kırmızı renkte olanlar kısmen kurtarılabilir olan dosyaları belirtmektedir. Dosya isimlerine tıklayarak resimde görüldüğü gibi dosyalar hakkında daha detaylı bilgiye ulaşabiliriz. Son olarak kurtarmak istediğimiz dosyaları seçerek "Kurtar..." butonuna tıklıyoruz ve



Kurtarmak istediğimiz dosyaları kaydetmek istediğimiz klasörü seçip "Tamam" butonuna tıklıyoruz ve programın bizim için dosyaları kurtarma işlemini tamamlamasını bekliyoruz.

Eğer aynı sürücüye kurtarma işlemi yaparsak aşağıdaki uyarıyı verir. Bu yüzden kurtarma işlemini münkünse harici bellek üzerine yapmakta fayda var.



4.2 İOS İşletim Sistemlerinde Dosya Kurtarma

İos işletim sistemine sahip bilgisayarlarda geri döndürme işlemi için çok sayıda 3. Parti ücretli programlar mevcuttur. Bunlar arasında en popüler olanı **WonderShare Data Recovery** programını kullandım. Programın deneme versiyonuda mevcuttur.

Programı açtığımızda diğer dosya kurtarma programlarına benzer bir menü karşımıza çıkıyor. Buradan geri döndürmek istediğimiz dosya türünü seçerek işleme devam ediyoruz.

Eğer tüm silinen dosyaların taranmasını istiyorsak. **All File Types** seçeneğini seçiyoruz.
Geri döndürülmesini istediğimiz dosyanın nerede olduğunu seçiyoruz. Eğer aradan uzun bir zaman geçmiş ve nerede olduğunu tam olarak bilmiyorsanız. **I cant Remember** seçeneğini seçiyoruz.

Externel removable devices seçeneği bilgisayarımıza takmış olduğumuz usb bellek sd kart vb. çıkartılabilir cihazlarda geri getirme işlemini yapmamıza olanak sağlıyor.

In a specified location seçeneğinde geri getirmek istediğimiz dosyanın yerini tam olarak biliyorsak seçebiliyoruz.

Next dedikten sonra bir sonraki ekranda bize yapılacak taramanın detaylandırması seçeneğini sunuyor. Eğer uzun zaman önce sildiğimiz dosyayı geri getirmek istiyorsak bu seçenekler oldukça faydalı olacaktır.

Eneble Deep Scan seçeneği bize formatladığımız dosyaların geri getirilmesini sağlıyor fakat işlem oldukça uzun sürüyor.

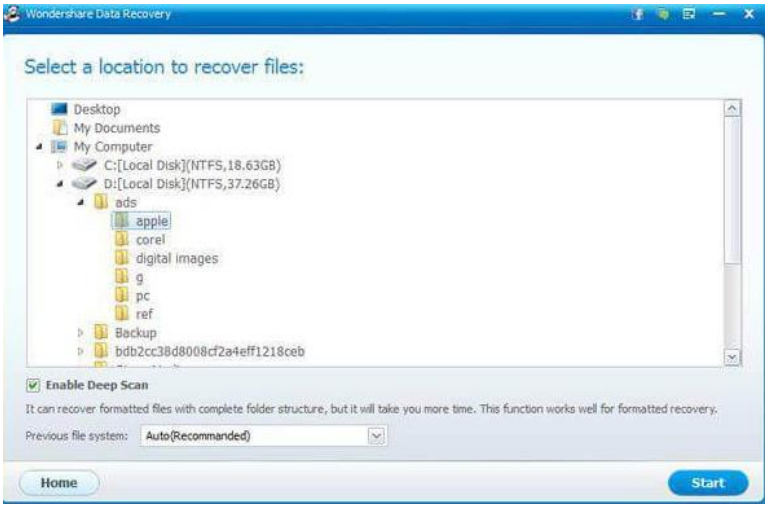
Enable Raw File Recovery seçeceği deep scan seçeneğine göre daha kullanışlı bir metoddur. Bu sayede dasyaların türüne göre sıralama yapabiliyoruz.

Next diyerek geri getirme işlemine başlanıyor.

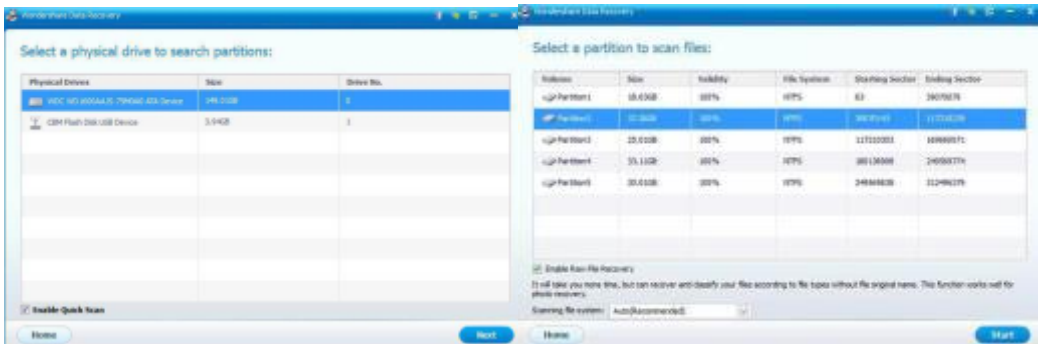
Karşımıza geri döndürülebilir dosyalar geliyor eğer çok fazla geri getirilebilir dosya var ise dosya konumundan geri getirilmesini istediğimiz dosyayı seçebiliriz.

Dosyaları geri getirme işlemi yaparken yardımıcı sihirbaz çıkmadan işlemleri manuel yapmak istiyorsak aşağıdaki ekran karşımıza çıkmaktadır.

Lost File Recovery işlemi bize belirli klasörlerde olan dosyaların geri getirilmesinde kullanılır.



Eğer bir sabit sürçünün ya da çıkartılabilir depolama cihazlarının belirli bölümlerini tarayıp geri getirme işleme yapmak istiyorsak Partition Recovery seçilir. Daha sonra hangi sürücünün ve hangi alanın seçilmesi gerektiğini sorar seçtikten sonra tüm bölüm için tarama işlemi başlar.



4.3 Linux İşletim Sistemlerinde Dosya Kurtarma

TestDisk güçlü bir kurtarma programıdır. Bozulmuş disk alanlarını, format atılmış alanları düzeltir ve geri getirir. TestDisk paketi içerisinde gelen PhotoRec ise silinmiş dosyaları kurtarmak için geliştirilmiş bir dosya kurtarma programıdır.

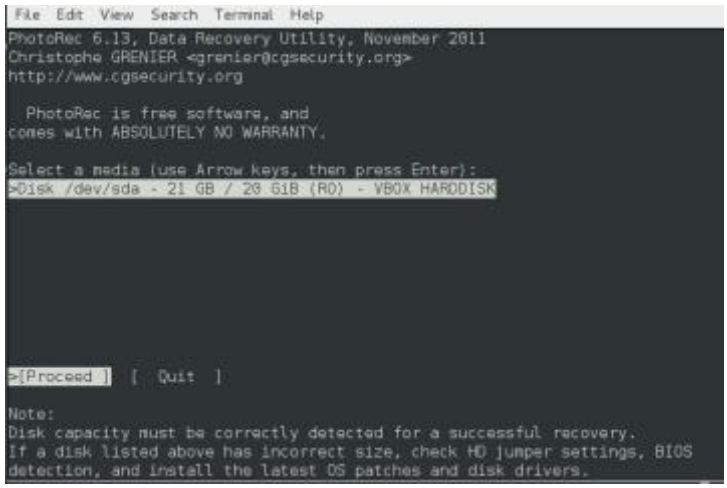
PhotoRec kullanılarak video, belge, resim vb. dosyalar sabit disk, CD-Rom ya da fotoğraf makinesinin hafıza kartından veri kurtarılabilir. PhotoRec uzun süre önce silinmiş dosyaları bulabilir ve bulunan dosyaları bozulmaya uğramadan belirlediğiniz klasöre geri yükleyebilir. Photorec, dosya sistemini göz ardı eder, böylece dosya sistemi ciddi şekilde zarar görmüş olsa da çalışır. FAT, NTFS, ext2/ext3/ext4 gibi çok sayıda dosya sistemini destekler.

Programların grafik arayüzü bulunmadığından komut satırı üzerinden kullanılmaktadır.

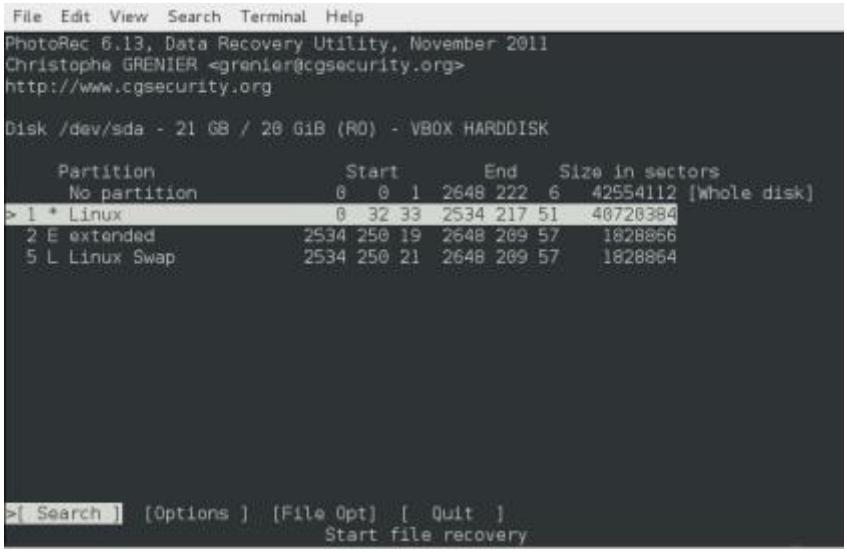
PhotoRec, TestDisk paket içinde yer almaktadır. TestDisk ve PhotoRec'i kurmak için terminal komut satırı penceresinde alttaki komutu kullanılabilir. Kali bilgisayarlarda hazır olarak gelmektedir.

sudo apt-get install testdisk

Programı ilk başlatıldığınızda bilgisayarınızdaki disk bölümleri ve çıkarılabilir depolama birimleri listelenir. Komut satırı ekranında aşağı-yukarı yön tuşlarını kullanarak verilerinizi kurtarmak istediğiniz disk bölümünün üzerine gelin. Enter tuşu ile devam edin.



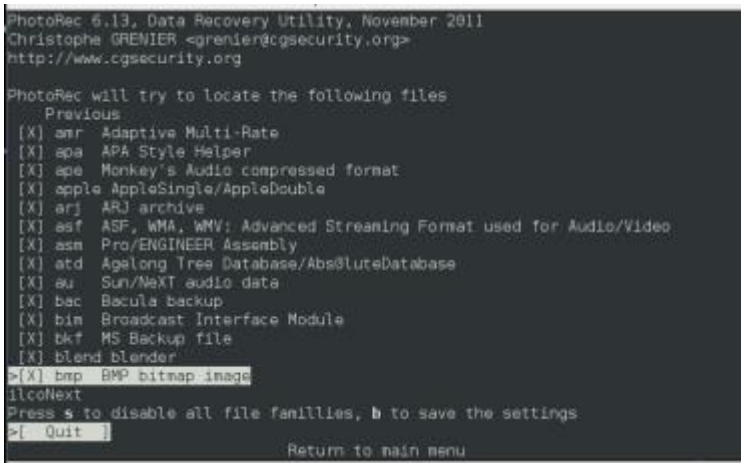
Ardından karşınıza alttaki gibi bir ekran gelecektir. Burada, önceki aşamada seçtiğiniz disk içindeki disk bölümleri listelenecektir. Bu listeden tarama için bir disk bölümü seçebilirsiniz ya da sağ tarafında [Whole disk] yazan (Türkçesiyle: tüm disk) satırdaki seçeneği kullanarak herhangi bir disk bölümü gözetmeksizin tüm diskin taranmasını sağlayabilirsiniz.



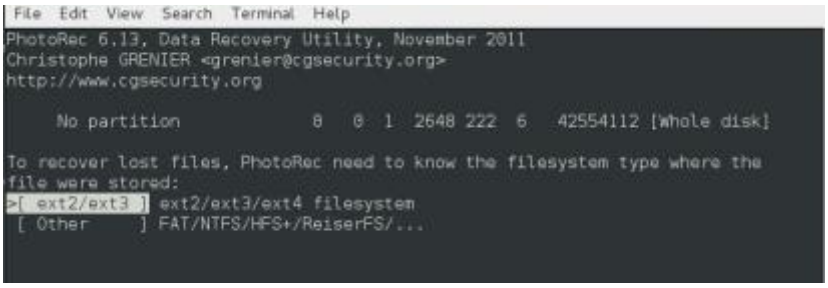
Ayrıca bu ekran yer alan [File Opt] seçeneğini kullanarak hangi türdeki dosyaların taranacağını belirleyebilirsiniz. Tarama işleminden daha sağlıklı sonuç almak bu seçeneği kullanarak dosya türlerini belirlemenizi tavsiye ederiz. Bunun için klavyeden sağ-sol yön tuşlarını kullanarak [File Opt] seçeneğinin üzerine gelin ve Enter yapın. Karşınıza çok sayıda dosya biçminin yer aldığı bir liste gelecektir. Bu listedeki tüm dosya biçimlerinin yanındaki çarpı şeklindeki seçim işaretini kaldırmak için klavyeden s tuşuna basmanız yeterlidir. Ardından yukarı-aşağı ok tuşlarını kullanarak taramak istediğiniz dosya türlerinin üzerine gelin ve her birinin üzerinde klavyeden x tuşuna basarak seçili hale getirin. Seçim işlemlerini bitirdikten sonra q tuşuna basarak önceki

ekrana dönün (isterseniz q tuşuna basmadan önce b tuşuna basarak dosya seçimi ayarlarının kaydedilmesini de sağlayabilirsiniz).

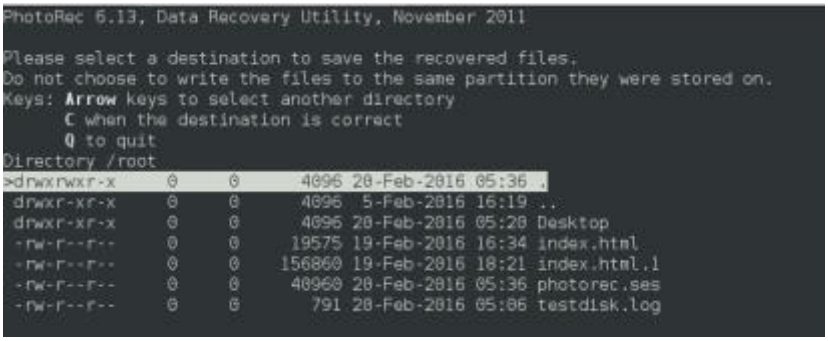
Önceki ekrana döndükten sonra [Search] seçeneği seçiliyken Enter tuşuna tıklayarak devam edin.



Ardından karşınıza gelen bu ekranda taramanın yapılacağı dosya sistemi türü seçilir. Eğer tarayacağınız dosyalar, içinde bir Linux dosya sistemi üzerindeyse ext4/ext3/ext2 seçeneğini seçiniz. Eğer tarayacağınız dosyalar çıkarılabilir bir disk (USB bellek, Taşınabilir disk) veya bir Windows disk bölümü (NTFS gibi) üzerindeyse 2. seçeneği seçip Enter ile devam ediniz.

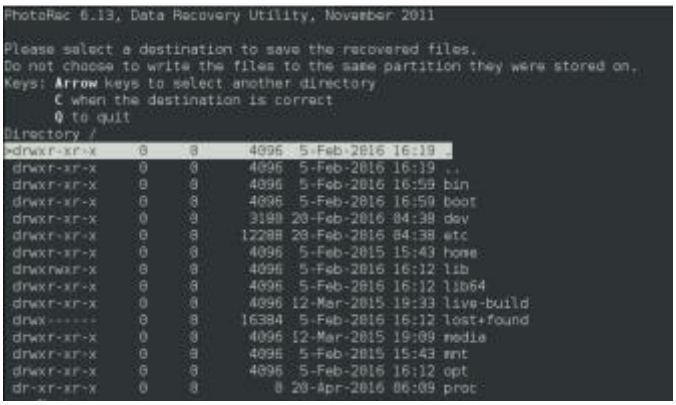


Bu aşamada, kurtarılan dosyaların nereye geri yükleneceğini belirlenir. Burada ön tanımlı olarak kullanıcı ev dizinindeki klasörler listelenecektir. Buradan herhangi bir dizini seçebilirsiniz. Tabi isterseniz dosyaların bu klasörleri kullanmak zorunda değilsiniz, klavyeden sol ok tuşunu kullanarak dosya sistemi üzerinde daha üst dizinlere gidebilirsiniz.



[GÜVENLİ SİLME VE DOSYA KURTARMA]

Not: Veri kurtarma yazılımlarını kullanırken genel bir prensip olarak, tarama neticesinde kurtarılacak verileri taradığınız disk bölümüne değil farklı bir disk bölümüne ya da diske kaydettirmeniz önemlidir. Eğer taradığınız disk bölümünde kurtarılan verilerin, yine aynı disk bölümü üzerine yazılmasını seçerseniz, kurtarılabilecek pek verinin zarar görmesine yol açmış olursunuz.



Biz burada örnek olarak /root/Desktop isimli klasörünü seçelim. Bu klasörün üzerine geldikten sonra klavyeden C tuşuna basarak onaylayın. Artık taramamız başlamıştır.

Tarama işlemi devam ederken alttaki gibi, hangi dosya türünden kaç adet dosyanın kurtarıldığı listelenir. Tarama işlemi seçtiğinizi diskin büyüklüğüne ve taranması için belirlediğiniz dosya uzantısı çeşitlerinin fazla sayıda olup olmamasına bağlı olarak bir kaç saaat ve hatta onlarca saat sürebilir.

Kurtarılan dosyalarımızın örnek olarak /root/Desktop isimli klasöre kaydedilmesini seçmiştik. Şimdi Dosyalar dosya yöneticisi üzerinden bu klasöre gittiğinizde alttaki gibi her biri kilitli görünen alt klasörlerle karşılaşırız. Kurtarılan dosyalar bu "recup_dir" adıyla başlayan alt klasörlerde yer almaktadır.

Bulunan dosyaların ayıklanması

Taradığınız diskin büyüklüğüne ve tarama için fazla sayıda dosya türü seçip seçmediğinize bağlı olarak Photorec tarama neticesinde belirlediğiniz hedef klasör içinde onlarca, yüzlerce ve hatta binlerce "recup_dir" adında alt klasör oluşturarak, kurtarılan dosyaları bu klasörler içine yerleştirecektir. Söz konusu klasörlerin yüzleri - binleri bulması halinde teker teker bu klasörler içine girip kurtarılan dosyaları incelemeniz, işinize yaramayan dosyaları silmeniz çok uzun zamanınızı alabilir. Örneğin söz konusu bu yüzlerce-binlerce klasör içinde .png uzantısına sahip tüm dosyaları, belirleyeceğiniz bir hedef dizin altına taşınmasını isterseniz bunun için şu komutu kullanabilirsiniz:

```
sudo find /kurtarılan/dosyaların/bulunduğu/yer -name "*.png" -exec mv {} /hedef/klasörün/adresi \;
```

NOT: Burada kaynak ya da hedef dizin adresleri üzerinde, adında boşluk karakteri bulunan herhangi bir klasör varsa komutu kullanırken boşluk karakterinin bulunduğu yere ters slaş ve bir boşluk (yani \ yerleştirmelisiniz. Örneğin kaynak dizin ya da hedef dizin üzerindeki bir klasörün adı "Adsız Dizin" ise komutta bu klasörün adını Adsız\ Dizin şeklinde yazmalısınız. Aksi taktirde komut, bu klasörün yerini bulamayacaktır.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.