

T.C.
MİLLİ EĞİTİM BAKANLIĞI



MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

BAKIM ONARIM 2

ANKARA 2007

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR	iii
GİRİŞ	1
ÖĞRENME FAALİYETİ-1	3
1. ÇEVRE BİRİMLERİ İÇİN KORUYUCU BAKIM	3
1.1. Bilgisayar Çevre Birimleri ve Programlar	3
1.2. Koruyucu Bakım	4
1.2.1. Monitörler	4
1.2.2. Fareler	6
1.2.3. Klavyeler	7
1.2.4. Yazıcılar	9
1.2.5. Tarayıcılar	12
1.2.6. Kasalar	13
1.2.7. Speaker (Hoparlör) Bakımı	15
UYGULAMA FAALİYETİ	17
ÖLÇME VE DEĞERLENDİRME	18
ÖĞRENME FAALİYETİ-2	19
2. KORUYUCU BAKIM İÇİN GEREKLİ BİLGİSAYAR YAZILIMLARI	19
2.1. Yardımcı Bakım Yazılımları	19
2.1.1. Scandisk	19
2.1.2. Birleştirici (defragmenter)	23
2.1.3. Chkdsk	26
2.1.4. Regedit	31
2.2. Kullanıcı Sorumlulukları	44
2.2.1. Uygulamaları Yönetmek	44
2.2.2. Dosya ve Klasörleri Yönetmek	45
2.2.3. Çalışmanızı Yedeklemek	45
2.3. Anti-Virüs Uygulamaları	45
2.3.1. Bilgisayar Virüsü Nedir?	45
2.3.2. Anti-Virüs Programları	52
2.3.3. Symantec Antivirüs Programı	54
2.3.4. McAfee VirusScan Enterprise 8.0. Programı	70
2.4. Güvenlik Duvarı (Firewall)	84
2.4.1. FireWall Nedir	84
2.4.2. Güvenlik Duvarları Neler Yapabilir	87
2.4.3. Güvenlik Duvarları Neleri Yapamaz	88
2.4.4. Güvenlik Duvarları Nasıl Çalışır	88
2.4.5. Yerel Ağda Gelişmiş Firewall Özellikleri	89
2.4.6. Silahsızlandırılmış Bölge (Dmz – Demilitarized Zone)	91
2.4.7. Doğrudan Filtreleme	92
2.4.8. Zonaların Güvenlik Duvarı Programı	92
2.4.9. McAfee Firewall 8.0	103
2.5. Dosya Kurtarma	106
2.5.1. Veri Nedir	106
2.5.2. Veriler Nasıl Hasar Görür	106
2.5.3. Verilerin Silinmesi	107

2.5.4. Veri Kayıpları İle Karşılaşmayı Engellemek İçin Alınacak Temel Önlemler ...	107
2.5.5. Veri Kaybına Uğranıldığında Dikkat Edilmesi Gerekli Hususlar	109
2.5.6. Veri Kurtarma Mantığı	110
2.5.7. Dosya Kurtarma Programları.....	110
2.5.8. Bilgisayar Kullanımı İle İlgili Kurallar	121
UYGULAMA FAALİYETİ	122
ÖLÇME VE DEĞERLENDİRME	123
ÖĞRENME FAALİYETİ-3	124
3. KORUYUCU BAKIM İÇİN GÜÇ SORUNLARI.....	124
3.1. Koruyucu Bakım ve Güç Sorunları.....	124
3.1.1. Güç Sorunları.....	124
3.1.2. Güç Kesintisi-Karartma (Blackout).....	125
3.1.3. Brownout/Sag /Ani Kesilme (Voltaj Düşmesi)	125
3.1.4. Noise (Gürültü).....	126
3.1.5. Spike (Ani Voltaj Yükselmesi).....	127
3.1.6. Power Surge (Aşırı Gerilim Yükselmesi Güç Artışı)	128
3.2. Güç Kaynakları	129
3.2.1. Artış Bastırıcılar ve Güç Kaynakları	129
3.2.2. Kesintisiz Güç Kaynakları.....	130
3.2.3. UPS Nedir, Nasıl Çalışır.....	130
3.2.4. Standby Power Supply (Yedek Güç Kaynağı)	131
3.2.5. Line İnteractive UPS.....	131
3.2.6. Online UPS	132
3.2.7. Regülâtörler-Power/Line Conditioner	133
3.3. Sunucu Odalarında Güç Kaynağı.....	133
3.3.1. Bir Sunucu Ortamında UPS.....	133
UYGULAMA FAALİYETİ	137
ÖLÇME VE DEĞERLENDİRME	138
MODÜL DEĞERLENDİRME	140
CEVAP ANAHTARLARI	142
KAYNAKÇA	143

AÇIKLAMALAR

KOD	523EO0085
ALAN	Bilişim Teknolojileri
DAL/MESLEK	Bilgisayar Teknik Servisi
MODÜL ADI	Bakım Onarım 2
MODÜLÜN TANIMI	Bilgisayarın çevre birimleri için gerekli bakım onarımı ve işletim sistemleri için gerekli olan bakım işlemleri ve yazılım bilgilerini içeren öğrenme materyalidir.
SÜRE	40 / 32 saat
ÖN KOŞUL	Bakım Onarım 1 modülünü almış olmak.
YETERLİK	Bilgisayarın bakımı için gerekli programların kurulumunu yapmak
MODÜLÜN AMACI	Genel Amaç Gerekli ortam sağlandığında, bilgisayar ve bilgisayarın çevre birimlerinin her türlü bakım-onarım bilgilerine sahip olacak ve koruyucu bakım için gerekli olan yazılımların kurulması ve kullanılması becerisini kazanacaksınız. Amaçlar <ol style="list-style-type: none">1. Bilgisayarın çevre birimleri için gerekli koruyucu bakımı yapabileceksiniz.2. İletim sisteminin bakımı için gerekli yazılımları kullanabileceksiniz.3. Bakım için gerekli güç gereksinimlerini giderebileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Bilgisayar ve çevre birimleri, bilgisayar sınıfı, teknisyen bakım onarım çantası, test cihazları, antistatik malzemeler, firewall, antivirüs, veri kurtarma programları ve kelime işleme yazılımı
ÖLÇME VE DEĞERLENDİRME	Her öğrenme faaliyetinden sonra bir uygulama faaliyeti yaptırılacak, bu faaliyette yapabildiğiniz işlem basamaklarına göre kendinizi değerlendirebileceksiniz.

GİRİŞ

Sevgili Öğrenci,

Teknolojik gelişmelerle ortaya çıkan bilgisayar, dizüstü bilgisayar, projeksiyon cihazı, kesintisiz güç kaynağı (UPS) vs. ürünler günlük yaşantımızda önemli ve köklü değişikliklere neden olmaktadır. Bugün bu ürünleri kullanarak eskiden hayal bile edemediğimiz işlemleri yapabilmekteyiz. Bu teknolojik ürünler yaşantımızda büyük kolaylıklar ve avantajlar sağlamaktadır.

İyi bir bilgisayar kullanıcısı olmasanız bile, mutlaka bilgisayar üzerine bir sohbetle kulak misafiri olmuş ya da katılmışsınızdır. Bu sohbetlerde size yabancı ve bildik gelen bir sürü kavramla karşılaşmış olmanız olasıdır. Örneğin “Pentiyum 4 SİPİYU (Pentium 4 CPU)”, “Elsidi monitör (LCD monitör)”, “80 cigabayt (80 GB) hard disk”, “Bilgisayarıma virüs bulaştı.”, “Antivirüs, virüs”, fayırvol “firewall (Ateş duvarı)”, “Yuppies (UPS-kesintisiz güç kaynağı”, “... Dosyalarımı zipledim.”, “Windows’um çöktü ve önemli dosyalarım silindi”, “Dosya kurtarma programlarını gogilda (google) aradım.” vb.

Duymuş olduğunuz kavramlar bilgi teknolojileri (Bilişim sistemleri) ile ilgili kavramlardır. Bilgi teknolojileri, kişilerin günlük yaşamlarında, kurum ve kuruluşların işleyişinde etkili olan olgular bütünüdür. Ayrıca bilgi teknolojilerindeki gelişim ve değişim çok hızlı olmaktadır. Bu nedenle nereden başlarsanız büyük bir kâr olacaktır. Geçmişte daktilo kullanmak bir yetenek ve zorunluluk iken, şimdi bilgisayar kullanmayı bilmemek çağı geriden izlemek ve çağ dışı kalmak anlamına geliyor. Bilgisayar ve çevre birimleri kullanmak ne kadar önemli ise bu ürünlerin ve programların bakımını yapmakta oldukça önemlidir. Bu bakım, ürünlerin kullanım ömrünü uzattığı gibi daha etkili ve verimli kullanmanızı sağlayacaktır.

Bu modül, bilgi teknolojileri ve yukarıda adı geçen kavramlar konusunda sizleri de bilgi sahibi yapacak ve bu kavramlar sizin için yabancı kavramlar olmaktan çıkacaktır. Daha da ötesinde bilgisayar, çevre birimleri, güç kaynakları ve programların bakımı konularını öğreneceksiniz.

Bu modülden etkin bir biçimde yararlanabilmek için bilgisayar başında uygulanması gereken bölümlerin, mutlaka bilgisayar başında uygulamalı çalışılmalıdır. Bölüm sonlarındaki sorular ile kendinizi sınavınız ve gerekirse ilgili bölümü tekrar ediniz.

Modül içinde ilerledikçe bugüne kadar bilgisayar donanımı konusunda karşılaştığımız tüm sorunların birer birer sona erdiğini göreceksiniz.



ÖĞRENME FAALİYETİ-1

AMAÇ

Bu faaliyette verilen bilgiler doğrultusunda, bilgisayarın çevre birimleri için gerekli koruyucu bakımı yapabileceksiniz.

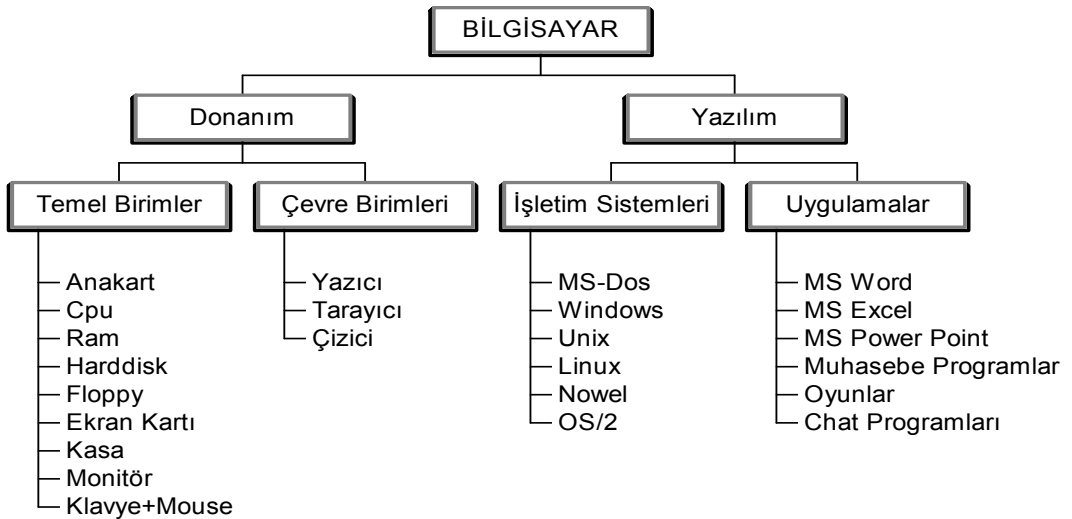
ARAŞTIRMA

Bilgisayarın diğer çevre birimleri ve parçaları için yapılacak koruyucu bakım unsurlarını araştırınız. Yaptığınız incelemeleri, rapor haline getirerek sınıfta sununuz.

1. ÇEVRE BİRİMLERİ İÇİN KORUYUCU BAKIM

1.1. Bilgisayar Çevre Birimleri ve Programlar

Aşağıda Şekil 1.1'de bir bilgisayar sistemini oluşturabilecek Hardware (Donanım) ve Software (Yazılım) birimleri grafiksel olarak gösterilmiştir.



Şekil 1.1: Bilgisayar sistemi

1.2. Koruyucu Bakım

Herhangi bir koruyucu bakım programının amacı, bilgisayar ve çevre birimleri arızalanmadan ve yazılımlar bozulmadan olası problemlerin önüne geçmektir. Bu bölümde, çevre birimleri için koruyucu bakımın önemi vurgulanmakta ve bunu gerçekleştirmek için yapılması gerekenler üzerinde durulacaktır. Uygun ve zamanında yapılan bakım çalışmaları, donanımın ömrünü uzatmaya yardımcı olur. Yardımcı yazılımlar, bir bilgisayar sistemini daha hızlı ve daha verimli hale getirebilir.

Bilgisayar yan birimleri için koruyucu bakımın amacı, aksaklık süresini kısaltmaya yardımcı olmaktır. Buna ek olarak, bu bileşenleri korumak, onları değiştirmekten çok daha ucuzdur. Bu bölüm bilgisayar ve çevre birimlerinin bakımı konularını içermektedir:



1.2.1. Monitörler

Resim 1.1'de bir görüntüleme birimi olan monitör çeşitleri gösterilmektedir. Görüntüleme birimi, bilgisayar donatımının en görünen parçası olduğundan, gerek görünüm gerekse işlevsellik açısından temiz tutulmalıdır. Bu bölümde anlatılacak olan bakım bilgileri, hem CRT (cathode Ray Tupe) hem de LCD (**Liquid Crystal Display**) tip ekranlar için kullanılmaktadır.



Resim 1.1: LCD ve CRT monitörler

Bir görüntüleme birimini temizlerken, öncelikli olarak aygıtın fişinin elektrik prizinden çıkarılmış olduğundan emin olarak işe başlayınız. Tüm ekranı silmek ve birikmiş tozu almak için yumuşak, deterjanla nemli bir bez kullanınız. Kullanacağınız bezin fazla ıslak olmamasına özen gösteriniz. Bezi etrafa damlamayacak şekilde sıkınız. Aksi takdirde monitörün içine su damlacıkları sızabilir. Monitörün yüzeyini durulamak için başka bir bezi suyla nemlendiriniz. Damlaların leke bırakmasını önlemek için çok fazla su kullanmaktan kaçınınız. Ekranı temizledikten sonra, işi tamamlamak için kuru bir bez kullanınız. Temizlik yaparken, monitör ekranını çizmemeye dikkat ediniz.

Monitörün ekranını temizlerken monitörün kasasında kullandığımız bezi kullanmayınız. LCD/TFT ve CRT ekranları temizlemek amacıyla özel olarak üretilmiş Resim 1.2'deki temizlik sprej ve jelleri kullanılabilir. Bu tip temizlik setleri yüksek kalitede mikrofiberden mamul yıkanabilir temizlik bezleri ile tozu ve kiri temizleme özelliklerine sahiptir. Ayrıca bu sprej ve jellerin antistatik özellikleri sayesinde monitörün ekranında toz toplanmasını da önlerler. Monitörün elektrik ve veri kablosunu temizliği için kasa temizliğinde kullanılan bezlerden yararlanabilirsiniz.

Aynı zamanda bu temizlik kitleri el bilgisayarlarının, dizüstü bilgisayarların tarayıcıların ve fotokopi makinelerinin yüzeylerini temizlemek içinde kullanılır.



Resim 1.2: Özel temizlik kitleri ve ekran temizliği

DİKKAT: CRT ekran temizlenirken içine sıvı girerse en iyisi onu buharlaşmaya bırakmaktır. Hiç bir zaman CRT ekranını açmayınız.

Monitörü temizledikten sonra, güç kablosunu ve data (veri) kablosunu güvenli bir biçimde takıldığından emin olunuz. Monitörün içinin temizliği açık bir ortam da üfleme kompresörle; hava yardımıyla kasa açılmadan tozlardan arındırılabilir. Aşağıdaki Resim 1.3'te çeşitli tip itmeli ve çekmeli kompresör resimleri görülmektedir.



Resim 1.3: Kompresör çeşitleri

1.2.2. Fareler

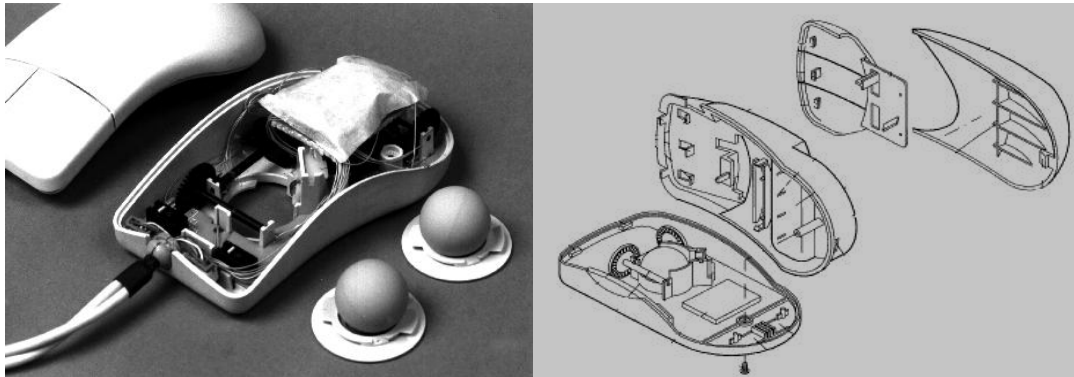
Fareler, mekanik, optik, kablolu veya kablosuz olarak kullanılmaktadır. Farelerin bu türlerine örnekler Resim 1.4'te gösterilmektedir.



Resim 1.4: Kablosuz, optik ve mekanik fare

Bir mekanik fare kirlendiğinde uygun bir biçimde işlemez ve kararsız hareket eder. Toz, fare altlığında birikirse, farenin hareket eden kısımlarına kaçabilir. Bu da farenin içindeki silindirlerde birikmeye yol açar. Bir mekanik fareyi temizlemenin en hızlı yolu, birimin alt kısmındaki kabı ve topu çıkarmak ve sonra da silindirlerde birikmiş tozu hafifçe kazıdır. Birikmiş toz, tırnakla veya başka bir yumuşak kazıma aletiyle alınabilir. Sorunu en aza indirmek için fareyi kullandığınız yüzeyin temiz olduğundan emin olunuz. Onun için fare altlığı kullanmak yararlı olur.

Diğer bir temizleme yöntemi ise pamuklu bir bezle izopropil alkol veya metanol kullanmaktır. Ancak bazen alt kapağı açmak işi çözmeyebilir. Hatta bu işlem sırasında mekanik aksamda yerinden oynamalar ve çıkmalar (Genellikle sensörlere yol veren dişli çarklar) olabilir. Bunun için fareyi Resim 1.5'de olduğu gibi açarak çıkan ve oynayan mekanik aksamlar yerine takılır. Temizleme işlemi bu şekilde rahatlıkla açık fare üzerinde tozlu ve kirli olan mekanizmalar temizlenerek yapılır. Daha sonra çıkarılan parçalar yerine takılarak fare bilgisayar kasasındaki yerine takılarak bilgisayar çalıştırılır. Şimdi fareniz yenisinden daha iyi çalışıyor olmalı...



Şekli 1.5: Mekanik fare

Optik farelerin bakımı için, farenin algılayıcı yüzeyinin nemli bir bezle temizlenmesi gerekebilir. Bunun için fare düzensiz işliyorsa bu işlem yapılmalıdır. Bir optik fareyi temizlemeden önce mutlaka bilgisayardaki yuvasından çıkarınız. Farenin lazer ışığı sağlığa zararlıdır. Bu nedenle farenin lazer ışığına çıplak gözle bakmayınız.

1.2.3. Klavyeler

Klavye bir bilgisayar sisteminin diğer tüm bileşenlerinden daha fazla fiziksel darbeye uğrar. Klavyeler de açıkta bulduklarından, zamanla üzerlerinde toz birikir. Klavyenin periyodik olarak temizlenmesi ömrünü uzatabilir ve arızalanmasını engelleyebilir.

Klavye bakımında nelere ihtiyaç duyulur:

- Kuru temizlik veya toz bezi
- Uygun temizlik sıvısı veya jeli (İzopropil alkol).
- Ucu pamuklu plastik çubuk
- İtici veya çekici kompresör veya vakumlu temizleyici
- Düz tip tornavida

İlk olarak, bilgisayar kapatılır ve klavye kasadaki yerinden çıkarılır. Eğer itmeli ve çekmeli kompresörünüz varsa klavye üzerine basınçlı hava üfletilerek yüzeydeki tozlardan ve yabancı maddelerden arındırılır. Yoksa vakumlu temizleyici kullanılır. Daha sonra klavye üzerine temizlik sıvısı veya jelden dökülür. Pamuklu plastik çubuk alınarak Resim 1.6'da görüldüğü gibi klavye tuşlarının kenarları temizlenir.



Resim 1.6: Klavye aralarının temizlenmesi

Bu işlemden sonra temizlik bezi temizlik sıvısı (İzopropil alkol) ile nemlendirilerek klavyenin yüzeyi Resim 1.7'de görüldüğü gibi temizlenir. (Temizlik sıvısını klavye yüzeyine doğrudan dökmeyiniz).



Resim 1.7: Klavyenin nemli bezle silinmesi

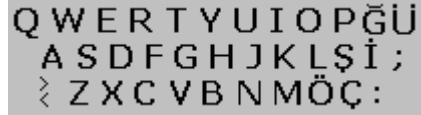
Daha sonra klavye yüzeyi kuru bir bez ile silinir. Eğer bu temizleme sırasında klavye tuşları arasında çıkaramadığınız yabancı cisimler sıkışmış ise tuşları çıkarmak zorunda

kalabilirsiniz. Bir klavyenin üzerindeki tuşlar, Resim 1.8’de gösterildiği gibi düz bir tornavida ile tuşlar çıkarılabilir. Bu işlem tozun toplandığı bölgelere kolay erişim sağlar. Büyük tuşların (Caps Lock, boşluk tuşu, Shift tuşları, enter tuşları vb.) bu şekilde çıkarılması ve geri takılması zordur. Bu nedenle onları çıkarmaktan sakınız. Bu arada tuşları çıkarttığınız pozisyonları da not ediniz.



Resim 1.8: Klavye tuşlarının çıkarılması

Biz sizin için not ettik.



Şekil 1.2: Q klavye düzeni

Klavye tuşlar çıkarıldıktan sonra klavye içinde bulunan zararlı maddeler; özellikle tuşların altındaki tozlar ve diğer yabancı maddeler, yumuşak bir fırça veya pamuklu bir bezle Resim 1.9’da gösterildiği gibi temizlenebilir. Bunun için, sıkıştırılmış hava da (kompresör) kullanılabilir. Kiri ve tozu çıkarmak için hava kullanırken, klavyenin dik konumda veya eğik pozisyonda tutulması gerekir. Bu işlem büyük kir ve toz partiküllerinin iç köşelerde, yaylarda ve tuşların altındaki köpük malzemede yapışık kalmasını engeller. Tuşları tekrar yerine takmadan önce nemli bezle her bir tuşu çıkarttığınız yerleri temizlik sıvısını kullanarak mümkün olduğunca siliniz. Bu işlem de bittikten sonra Şekil1.2’de gösterildiği gibi uygun olarak tuşları yerlerine takınız.



Resim 1.9: Tuşları çıkarılmış klavye ve temizliği

Eğer kullanmakta olduğunuz klavyeler yıkanabilir ise aşağıda Resim 1.10’da görüldüğü gibi temizlenebilirler. Klavyenizin yıkanabilir olduğundan emin olunuz. Eğer emin değilseniz kesinlikle yıkamayınız. Bu işlem klavyenizin bir daha kullanılmamak üzere bozulmasına neden olacaktır.



Resim 1.10: Yıkanabilir klavye

1.2.4. Yazıcılar

Yazıcıların içinde birçok hareket eden kısım vardır. Bu nedenle, daha yüksek düzeyde bakım gerektirirler. Yazıcıların içindeki bileşenlerin üzerinde zamanla bir toz ve kir birikintisi oluşur. Zamanla, bu kirlerin temizlenmesi gerekir. Aksi takdirde, bu kir ve toz tabakaları yazıcının arızalanmasına yol açtığı gibi, baskı kalitesinde bozulmasına neden olabilir. Bakım işlemini mürekkep püskürtmeli yazıcılar, lazer yazıcılar ve nokta vuruşlu yazıcılar için yapılacaktır.

1.2.4.1. Mürekkep Püskürtmeli Yazıcı

Bakıma başlamadan cihazın bütün elektrik ve bilgisayar bağlantılarını çıkartmayı unutmayınız. Mürekkep püskürtmeli bir yazıcıda, kağıt işleme mekanizmaları üzerinde zamanla kağıt partikülleri birikebilir. Bu partiküller, yazıcı aygıtı fişten çıkarılarak nemli ve tüy bırakmayan bir bez ile silinebilir. Yazıcı kartuşundan sızan mürekkep akıntılarına da yine aynı bezle silinmelidir. Aksi takdirde zamanla bu mürekkep akıntıları kağıt üzerinde istenmeyen izlere ve lekeler neden olabilir. Eğer yazıcı uzun süre kullanılmıyacaksa kartuşlar yazıcıdan çıkarılarak orijinal ambalajlarında ya da naylon bir poşet içinde saklanmalıdır. Kartuşun mürekkepli kısmını da orijinal bandıyla kapatılmalıdır. Yazıcıda kullanılan kağıtlar üzerinde yazıcıya zarar verebilecek toplu iğne, ataç, zımba teli vs. bulunmamasına dikkat edilmelidir. Yazıcının içindeki hareketli kısımlara sıkışmış ve elimizle ulaşamayacak yerde olan kağıt parçaları veya yabancı cisimleri itmeli ve çekmeli bir hava kompresörüyle temizleyebiliriz. Resim 1.13. 'de mürekkep püskürtmeli bir yazıcı gösterilmektedir.



Resim 1.11: Mürekkep püskürtmeli yazıcı

1.2.4.2. Lazer Yazıcı

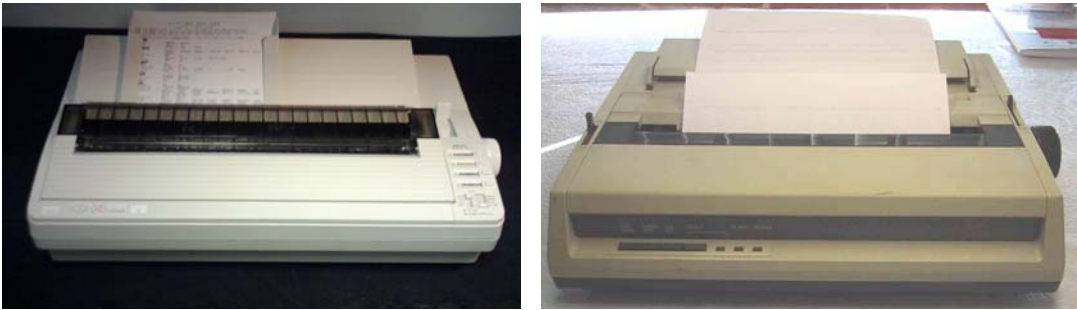
Temizlik işlemine başlamadan önce lazer yazıcının fişini çekmeniz, boşaltabileceği yüksek voltaj nedeniyle önemlidir. Ayrıca temizleme işleminden önce yazıcı kullanıldıysa bir süre yazıcının soğumasını bekleyiniz. Lazer yazıcılar, tozlu bir ortamda kullanılmıyorlarsa az bir bakım gerektirir. Bazı eski lazer yazıcı birimleri de daha yeni olanlardan daha fazla bakım gerektirir. Bir lazer yazıcıyı temizlerken, toner partiküllerini kaldırmak için özel bir vakumlu temizleyici kullanılmalıdır. Ev kullanımı için tasarlanmış vakumlu bir temizleyici kullanılırsa, toner partikülleri süzme sistemlerinin içinden geçerek havaya karışabilir. Bu yüzden toner partiküllerini temizlemek için hava çekmeli kompresörlerden yararlanılabilir. Lazer yazıcının dış yüzeyi diğer yazıcılarda olduğu gibi yumuşak, tüy bırakmayan nemli bir bezle silinir. Dolum veya değişiklik amacıyla çıkan toner ve drum (dram) siyah ışık geçirmeyen bir poşet torba içinde muhafaza ediniz.



Resim 1.12: Lazer yazıcılar

1.2.4.3. Nokta Vuruşlu Yazıcı

Nokta vuruşlu yazıcıların temizlik ve bakımı diğer yazıcılara göre daha kompleks ve zordur. Bu tip yazıcılarda mekanik ve hareketli kısımlar daha fazladır. Toz temizliği yaparken ilk olarak basınçlı hava ile hem yüzeydeki hem de yazıcı kasası içindeki tozların atılması sağlanır. Bu şekilde bir temizlik imkânınız yoksa sadece yüzeyleri hafif nemli ve tüysüz bir bezle silerek temizlik yapabilirsiniz. Yazıcı kafasının takıldığı ve bu kafanın üzerinde hareket ettiği profil demir çubuk, çarklar ve dişliler ince makine yağı ile yağlanabilir. Zaman zaman bu yazıcılarda kullanılan şeritlerin bitip bitmediği kontrol edilmelidir. Aksi takdirde bitmiş şeritlerin kullanılması ekonomik olmasından daha ziyade, yazıcı kafasında bulunan Pin' lere zarar vereceğinden zaman kaybedilmeden değiştirilmelidir.



Resim 1.13: Nokta vuruşlu (Dot Matrix) yazıcılar

Bir yazıcıda kullanılan kağıt, toner türü ve seçimi aşağıdaki sebeplerden dolayı önemlidir:

- **Kağıt seçimi:** Doğru kağıt türü, yazıcının ömrünün uzamasını ve daha verimli çalışmasını sağlayabilir. Yazıcı satılan dükkânların çoğunda, farklı kağıt türleri bulunur. Her bir kağıt türü, kullanılması planlanmış yazıcı türüyle ilişkilendirilmiştir. Kağıt türleri, mürekkep püskürtmeli ve lazer yazıcı kağıtlarını içerir. Yazıcı üreticisi genellikle kullanma kılavuzunda belli bir kağıt türünü tavsiye eder.
- **Mürekkep ve toner seçimi:** Yazıcı kılavuzunda, yazıcı üreticisinin tavsiye ettiği mürekkep ve toner türü listelenmektedir. Yanlış mürekkep ve toner doldurulursa, yazıcı çalışmayabilir ve baskı kalitesi düşebilir. Düzgün doldurulmayan kartuşlardan mürekkep sızabileceğinden, bu şekilde olan mürekkep kartuşlarını yazıcılarınızda kullanmayınız.

1.2.4.4.Yazıcı İle İlgili Kurallar

- ☞ Kullanılmadığı zamanlarda, elektronik devrelerin ısınarak zarar görmesini önlemek için kapalı tutunuz.
- ☞ Yazıcı kablosu bilgisayar portundan çıkarılacak ise; önce yazıcının kapatılması, daha sonra kablounun çıkarınız.
- ☞ Uzun süreli kullanımlarda yazıcı yazma kafası aşırı derecede ısınır bir süre dinlendiriniz.
- ☞ Yazıcılar mekanik ve elektroniğin bir arada kullanıldığı aletler olduğu için özellikle mekanik kısmının periyodik bakım ve temizliğinin yapınız.
- ☞ Nokta vuruşlu yazıcılarda kaliteli şerit kullanılması ve eskiyen şeritlerin hemen değiştirilmesi, şerit değiştirmelerde şeridin yatağına tam oturmasına özellikle dikkat ediniz.
- ☞ Düzgün olmayan, kenarları yırtık ve kırışık kağıtların yazıcıda kullanmayınız.
- ☞ Sıkışabilecek kağıt parçalarının ve yazıcının içine düşebilecek yabancı cisimlerin hemen çıkarınız.
- ☞ Kullanım durumuna göre tek kağıt ve sürekli form durumlarına özellikle dikkat edilmesi ve yine kullanılan kâğıdın kalınlığına göre Yazıcı kafasının yakınlığına uzaklığına dikkat ediniz.
- ☞ Bazı Türkçe karakter setini yükleyici programlarından ve Yazıcı tanımı isteyen çeşitli programlardan doğabilecek sorunlara dikkat ediniz.
- ☞ Yazıcı kapatıldıktan sonra en az 30 saniye geçmeden açmayınız.
- ☞ Yazıcının topraklı bir prizde kullanılması, gerekir.
- ☞ Toner kartuşunu ya da drum kartuşunu açıkta yanan ateşe atmayınız. Toner tozu yanıcı bir maddedir.
- ☞ Toner kartuşunu atarken, tonerin gözlerinize veya giysilerinize temas etmemesine dikkat ediniz. Kirlenmesi durumunda, derhal soğuk su ile yıkayınız. Ilık su ile yıkamak toneri sabitleyecek ve toner lekelerinin çıkmasını imkansız hale getirecektir.

1.2.5.Tarayıcılar

Resim 1.14'te örnek tarayıcılar gösterilmektedir. Öncelikle tarayıcı yüzeyini temiz tutulmalı ve doküman kapağı ile tarama camı üzerine ağır cisimler kesinlikle konulmamalıdır. Doküman kapağını ve tarama penceresinin camını temiz tutmanız taranan dokümanın, tarama esnasında toz veya başka partiküllerden etkilenmesini, dolayısıyla tarama kalitesinin bozulmasını önler. Cam kirlenirse, temizleme talimatları için üreticinin kılavuzuna bakınız. Kılavuzda talimatlar sıralanmamışsa, bir cam temizleyici ve camın çizilmesini önlemek için yumuşak bir bez kullanınız. Tarama camı ve doküman kapağı belirli zaman periyotlarında temizlenmelidir. Bunun için:

- Tarayıcın bilgisayarla olan bağlantısını kesin tarayıcınızın varsa adaptörünü prizden çekiniz.
- Doküman kapağını açınız, bakım için yumuşak iz ve tüy bırakmayan bir temizleme bezi kullanınız. Bezi, alkol veya cam temizlemede kullanılan temizleme malzemeleri ile kullanarak doküman kapağı ve tarama camını temizleyiniz.
- Kuru, yumuşak ve tüy bırakmayan bez parçasıyla temizlediğiniz yüzeyleri kurulayınız.



Resim 1.14: Tarayıcı çeşitleri

Camın içi kirlenirse, birimin nasıl açılacağı veya camın tarayıcıdan nasıl çıkarılacağına ilişkin talimatlar için üreticinin kılavuza başvurunuz. Mümkünse, camın her iki tarafını da tamamen temizleyiniz ve camı tarayıcıda orijinal olarak takılı olduğu biçimde yerleştiriniz.

Dış Bölgenin Temizlenmesi

Makinenin dış bölgesini özel temizleme ürünü haricindeki sabun veya deterjanla temizlemeyiniz. Basit bir temizlik için çok ıslak olmayan nemli ve tüysüz bir bez yeterli olacaktır.



ÖNEMLİ

- 1- Tarayıcıyı bir yerden bir yere taşırken; kutusu içine, köpükleri ile birlikte, tarayıcının sarsılmasını engelleyecek şekilde yerleştirilmelidir.
- 2- Parçalara yapışabilecekleri ya da statik elektrik üretebilecekleri için temizlik için kağıt mendil, kağıt havlu ya da benzeri malzemeler kullanmayınız.
- 3- Tarama yaptığınız dokümanlar üzerinde daksil, ıslak mürekkep, ataç, zımba teli ve toplu iğne v.s maddeler var ise bunları çıkarmayı unutmayınız.

1.2.6. Kasalar

Bilgisayar kasa kapakları kurulum işleminden sonra mutlaka kapalı tutulmalıdır. Kapalı tutulması sayesinde kasa içine toz ve yabancı cisimlerin girmesi engellenecektir. Kasanın elektriğe bağlı kablo bağlantılarını çıkartıldıktan sonra kasaların üst ve yan yüzeylerini hafif nemli bir bezle silerek tozu alınabilir. Kasa içine de kompresörle basınçlı hava tutulabilir.

1.2.6.1. Kasa İçi Kablolar

Kasa içinde buluna sabit diskler, CD sürücüler, Disket sürücü v.s. bağlantı kabloları sadece fazla yer kaplamakla kalmıyor yüzeyleri geniş olduğu için kasa içi havalandırmayı olumsuz yönde etkiler ve zamanla kasa içindeki ısının yükselmesine neden olur. Bu durumda bütün sisteme yansıdığı için dikkat edilmesi gereken bir konudur. Bu konuda ne yapılabilir. Öncelikle kasa içinde bulunan bütün kabloları havalandırmaya ve fanların soğutma sistemine mani olmayacak şekilde toplanır. Böylelikle kasa içinde hava akışı ve sirkülasyonu daha rahat olur.

1.2.6.2. Kasa Fanları & İşlemci Fanı & Ekran Kartı Fanı

➤ Kasa Fanları

Kasa fanları gelişigüzel takılmaması gereken parçalardır. Kasalarda kullanılan fanlar genellikle kasa içindeki havayı dışarıya üfler. Ancak bu tek başına yeterli değildir. Bu fanın içerideki sıcak havayı dışarıya üflemesinden ziyade dışarıdan içeriye soğuk hava üfleyecek bir fanla desteklenmesi başarıyı oldukça arttıracaktır. Bu fanın kasanın ön panelinde uygun bir yer varsa buraya ya da kasanın yan kapağında bulunan bölüme monte edilmesi uygun hava akışını oluşturmak için gereklidir.

➤ İşlemci Fanı

İşlemci fanı, işlemcimizin ısısı konusunda çok önemli bir yere sahiptir. Bu fanın çok da fazla problemi olmamakla birlikte dikkat edilmesi gereken en önemli konu altındaki Heatsink (Metal parça) dır. Bu parça uzun süre temizlenmediği durumlarda üzerinde biriken tozlar bir halı şeklinde heatsink'in üzerini örter bunun doğurduğu sonuçlar işlemci ısısında gözle görülür "3-10 derece arasında" yükselmeler, ayrıca fanın işlemciyi soğutmak adına daha devirli dönmesi sonucu oluşan yüksek desibeldeki sese neden olur. Bunu önlemek için sadece 3 aylık periyotlarla bir heatsink'i çıkartılıp bir fırça ile temizlenebilir. Su ile yıkanmamalıdır. Su ile yıkama termal macuna zarar verebilir. Sadece termal macun yenileneceği zamanlarda heatsink'i üzerinde kalan eski macunu temizlemek adına yıkamak düşünülebilir.

➤ Ekran Kartı fanı

Çoğu kullanıcı oyun oynamayı sever; hatta sadece bu yüzden bilgisayar alanlar da vardır. Öyle ise ekran kartının da iyi bir soğutmaya ve düzenli bakıma ihtiyacı vardır.

Öncelikle, gerekmedikçe veya bu konuda fazla bilginiz yoksa overclock gibi fazla yük bindiren dolayısı ile beraberinde ısı getiren uygulamalardan kaçınılmalıdır. İkinci olarak fanın bakımı vardır. Burada dikkat edilmesi gereken fanın dönmesi değil ne kadar rahat döndüğü ve fanla kart arasına girecek toz katmanıdır. İlk önce ekran kartı üzerindeki fanın ortasındaki jelatin çıkartılıp "Makine Yağı" kullanarak yağlanabilir. İşlem sırasında metal aksamı hafifçe oynatılır ki yağ içerilere kadar işler. Bu işlemden sonra fan bir kaç tur döndürülür. Bu durum yağın iyice nüfuz etmesini ve sürtünmenin azalmasını sağlayacaktır.

NOT: Kesinlikle mutfak yağı kullanmayınız bu yağ sıcakken kaygan, ancak soğuduğunda katılaşır ve fanınızın hiç dönmemesine yol açar.

➤ Termal Macun Uygulaması

Termal macun işlemci üzerindeki ısıyı direk olarak heatsink'e iletmeye yarayan bir macundur. Böylece işlemcinin üzerindeki ısı çok daha çabuk dağılır ve işlemciler daha çabuk soğur. Bu uygulama için işlemcinin çıkarılması gerekir. İşlemci ile fanın metal heatsink'i arasında sürülerek iki madde arasındaki ısı iletimini kolaylaştırmak için kullanılır. Bildiğiniz gibi işlemcinin üzerine takılan heatsink+fan ikilisi, işlemcinin sıcaklığını düşürmek için kullanılır. İşlemcinin ısıyı iyi bir ısı ileticisi olan heatsink'e geçer ve heatsink'in üzerindeki fan heatsink'e doğru hava üfleyerek heatsink'in üzerinde biriken ısıyı dağıtır. İşlemci ile heatsink arasındaki iletim ne kadar iyi ise, işlemcinin sıcaklığı da o kadar kolay düşürülür.

İşlemci ile heatsink dediğimiz metal parça arasındaki ısı iletiminin aksamasına neden olan ise, iki yüzey arasındaki ufak boşluklarda kalan havadır. Her ne kadar çıplak gözle bakınca işlemcinin üst yüzeyi de heatsink'in alt yüzeyi de pürüzsüz gözükseler de aslında her iki yüzey de mikroskopik boyutta oldukça engebeli bir dokuya sahiptir. Bu nedenle, iki yüzeyi birbirine bastırdığımızda, aslında birbirine fiziksel olarak temas eden alan çok düşüktür, arada kalan hava ise kötü bir ısı ileticidir. Bu nedenle heatsink ile işlemci arasında termal macun sürülür. Termal macun, aşağıda Şekil 1.3'te görebileceğiniz gibi, heatsink ile işlemci arasında bir katman oluşturacak ve ısı iletmeyen boşlukları dolduracak şekilde uygulanır.



Şekil 1.3: Termal macun uygulama yüzeyi ve termal macun

Şekil 1.3'te işlemci üzerine sürülecek termal macun ve sürüldüğü yüzey görülmektedir.

Uygulanması biraz dikkatle son derece basittir. İşlemci çıkarılıp üzerine az bir miktar sıkılır. Bunu ahşap uçlu bir aletle işlemcinin üzerine tamamen kaplayacak şekilde yayılır.

Metal ve sivri uçlu aletler kullanılması işlemciyi çizilebilir. Daha sonra heatsink'in işlemci üzerine koyulur. Taşma olup olmadığını kontrol edilmelidir. Eğer herhangi bir problem yoksa uygulama tamamlanır.

Termal macun mümkün olduğunca az ve ince sürülmelidir. Fazla kaçarsa, işlemci ile heatsink arasında çok kalın bir katman oluşturacaktır ve bu durumda olumlu etkisi görülmeyebilir. Ama işlemci ve heatsink arasındaki boşluğu dolduracak kadar fazla sürülmelidir. Önce heatsink alınır ve kare şeklinde bir bölgeye, alttaki Resim 1.16.'da görüldüğü gibi sürülür. Daha sonra, heatsink işlemcinin üzerinde mümkün olduğunca sıkı bir şekilde takılır. Her ne kadar macun elektriksel iletken özellik taşımasa da, yine de macunu kenarlara taşırmamaya dikkat etmeniz önemlidir. Özellikle AMD Athlon ve Duron işlemcilerde, macunun işlemci üzerindeki kontaklara bulaşmamasına dikkat ediniz.



Resim 1.16: Heatsink üzerine termal macun uygulanması

➤ **Kasanın Bulunduğu Alan**

Isıya ve toza büyük etken olan kasanın konumudur. Kasa; yere yakın, etrafı kapalı yerlere, çalışma masasının altına ve bu tarz hava almayan ve çok toz tutan bölgelere asla koyulmamalıdır. Koyulması durumunda kasa içi ısı yükselecektir. Fanların soğutma performansı yarı yarıya düşecektir. Çok toz alacağı için ısı ve yanında yüksek ses problemi ile karşı karşıya kalınacaktır. Bütün bunları önlemek için kasayı yüksek ve hava alan bölümlere yerleştirilmelidir. Böylece yukarıda belirtilen olumsuz durumların tam tersi tepki olacaktır.

1.2.7. Speaker (Hoparlör) Bakımı

Hoparlörler için çok özel bir bakım yoktur. Bu noktada yapılabilecek sınırlı birkaç uygulama vardır. Bakım için yumuşak bir fırça, pamuk badem yağı ve antistatik sprey yeterlidir.

1- Hoparlör ünitelerinin membranlarının üzerinde birikmiş tozları yumuşak bir fırçayla ortadaki toz kapağının ezilmemesine dikkat ederek alınmalıdır.

2- Hoparlör ünitelerinin kenarlarındaki refleks kısımları eğer poliüretan değil de lastikse, zaman içinde sertleşme yapar. Bunu önlemek için 6 aylık zaman diliminde reflekslere badem yağı gibi hafif bir yumuşatıcıyı tozu alınmış bir pamuk kullanarak çok çok ince bir tabaka olarak sürülmesinde fayda vardır.

3- Hoparlörlerin dış yüzeyi zamanla toz güneş ısı ve diğer yan etkilerden etkilenir. Bu yüzden dış yüzeyin tozunu almak ve antistatik sprey ile temizlemekte fayda vardır.



Resim 1.19: Hoparlör çeşitleri

1.2.8. Bilgisayarların Zarar Görmemesi ve Bozulmaması için Tedbirler

- Kullanılmadığı süreler içinde hem bilgisayar, hem de monitörün kapalı tutturunuz.
- Kullanılmadığı zamanlarda üzerinin örtülü tutulması ve temizleme işleminin özel sprey ile yapınız.
- Bilgisayarı mümkün olduğunca tozsuz-temiz ortamlarda kullanınız, yanında sigara içmeyiniz, kaza ile üzerine dökülmesini önlemek için yanına çay, kahve gibi dolu bardak koymayınız.
- Bilgisayar ve donanımının direkt güneş ışığına maruz bırakmayınız.
- Ekranda sabit duran bir görüntü varken, monitörün uzun süre (2-3 saat gibi) açık bırakmayınız.
- Bilgisayar masasını hareketsiz bırakmayınız ve hava akımını önleyecek kadar bilgisayar duvara dayamayınız.
- Bilgisayar kapatıldıktan sonra yeniden açılacaksa en az 30 saniye bekleyiniz.
- Bilgisayarı topraklı bir prizde çalıştırınız ve elektriği şartelden kesmeden önce bilgisayar kapatınız.
- Bilgisayar açıkken, monitör, klavye, yazıcı, port bağlantıları gibi kabloların çıkarmayınız veya takmayınız.

Yukarıda önerilen tedbirler alınması durumunda, bilgisayarları ve çevre birimlerinin kullanım ömrü uzamakla birlikte daha verimli kullanılmasını sağlayacaktır.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
<ul style="list-style-type: none">➤ Bilgisayar ve çevre birimleri için ayrı ayrı bakım envanteri tutunuz.➤ Bakım için kullanılacak malzemeleri için bir temizlik ve bakım dolabı temin ediniz.➤ Çalışma alanını dağınıklıktan kurtarınız ve temiz tutunuz.➤ Teknisyen kasaya bir topraklama bilekliği bağladığında topraklama bağlantısı aygıtı ESD' den veya diğer ismiyle statik elektrikten korur. Çalışırken bu bilekliği kullanınız.➤ Bilgisayar bileşenlerini antistatik torbalar içinde saklayınız ve taşıyınız. Bir torbaya birden fazla bileşen koymayınız; çünkü bu bileşenler birbirine zarar verebilir.➤ Bilgisayar ve çevre birimlerine ait olan kullanım kılavuzları ve diskleri küçük bir kutuda saklayınız. Kutunun üzerine toplanmış olan bilgisayarın bilgilerini gösteren bir etiket yapıştırınız ve güvenli bir yerde saklayınız. İleride bu bilgilere ihtiyaç duyulursa, bunlara kolayca erişmek mümkün olsun.➤ Bilgisayar kasasında çalışırken, kasanın keskin kenarlarını bantla kaplayınız.	<ul style="list-style-type: none">➤ Bu envanterleri istendiği zaman ulaşılabilecek bir yerde saklayınız.➤ Basınçlı hava ile yapacağınız temizlik işlemlerini açık havada yapmaya özen gösteriniz.➤ Bu işlem için hazırlanan listeyi herkesi okuyabileceği şekilde bilgisayar ortamında hazırlayınız. Bu listeyi uygun bir çerçeve içine monte ediniz.➤ Sistemin kapalı olduğundan ve güç kablosunun çıkarılmış olduğundan emin olunuz.➤ Eğer özel eğitim almadıysanız bir ekranın içini açmayınız. Bu ekran içinde 25.000 volta kadar ölümcül olabilecek gerilimler birikebilir.➤ Yakınıınızda bir yangın söndürücü ve İlkyardım çantası bulundurunuz.➤ Bilgisayar çalışırken bileşenleri takıp sökmeyiniz.➤ Kurulum ve bakım CD'lerini ve disketlerini manyetik alanlardan, soğuktan ve sıcaktan koruyunuz.➤ Anakart üzerinde Jumper ayarı değiştirmek ve bileşenlere dokunmak için kurşun kalem veya herhangi bir metal uçlu araçlarla dokunmayınız. Kurşunkalemin ucundaki grafit iletkenidir ve hasara sebep olabilir.➤ Ekran dışındaki, bileşenlerle çalışırken topraklama bilekliği kullanınız.

ÖLÇME VE DEĞERLENDİRME

A- OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki cümleleri doğru veya yanlış olarak değerlendiriniz.

1. Bir bilgisayar sisteminin bileşenlerinden olan klavye diğerler bileşenlerden daha fazla fiziksel darbeye uğrar.
2. Bilgisayar bileşenlerini temizlemek için tiftiksiz bezler kullanılmaz.
3. Bilgisayar kasası açıldığında bir teknisyenin yapması gereken Bir topraklama bilek bandı takmasıdır.
4. Bir bilgisayar, temizlik veya başka bir koruyucu bakım amacıyla söküldüğünde, parçalar ve bileşenler metal bir kutu da geçici olarak saklanabilir.
5. Bilgisayar ve çevre birimleri için yapılan koruyucu bakım, arıza ve aksaklık süresini kısaltmaya yardımcı olur.
6. Yazıcıların mürekkep ve toneri yanlış doldurulursa, yazıcının baskı kalitesi düşebilir.
7. Kasa içinde çalışırken antistatik bileklik kullanılmaz.
8. Monitör ve güç kaynağı üzerinde çalışırken antistatik bileklik kullanılır.
9. Eğer fare işaretçisi ekran üzerinde doğru hareket etmiyorsa, ilk olarak farenin temizliği yapılmalıdır.
10. Bilgisayar ve çevre birimlerinin bakım ve temizliği yapılırken yüzeyleri çizen sert cisimler kullanılmaz.

Cevaplarınızı cevap anahtarı ile karşılaştırınız.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

ÖĞRENME FAALİYETİ-2

AMAÇ

Bu faaliyette verilen bilgiler doğrultusunda, İşletim sisteminin bakımı için gerekli yazılımları kullanabileceksiniz..

ARAŞTIRMA

Bilgisayarlarda 3. parti diye adlandırılan programlardan, bakım ve test işlemlerinde kullanabileceğiniz yazılımlardan birkaç tanesini bularak kullanımı ve kurulumları hakkında bir rapor hazırlayınız. Hazırladığınız raporu sınıfta arkadaşlarınıza sununuz.

2. KORUYUCU BAKIM İÇİN GEREKLİ BİLGİSAYAR YAZILIMLARI

2.1.Yardımcı Bakım Yazılımları

Koruyucu bakım için bilgisayar yazılımı ve yardımcı yazılımlar, Bilişim teknolojileri (BT) teknisyeninin birincil araçlarıdır. En yaygın olanları, antivirüs programları ve güvenlik duvarlarıdır (Firewall). Sistem sorunlarını teşhis etmek ve gidermek için birçok uzman program mevcuttur ve bunların çoğu, başarılı koruyucu bakım ilkesinin bir parçası olarak bulunmaktadır. Bu öğrenme faaliyeti Windows'un yardımcı bakım yazılım konularını içermektedir. Yardımcı yazılımlar, DOS ve Windows'a ait olan, sistem bütünlüğünü korumayı sağlayan programlardır. Bu programlar, düzenli bir biçimde kullanıldıklarında sistem hızını ve verimliliğini artırabilir.

2.1.1. Scandisk

Sabit sürücünüz kullanıldıkça zamanla bozuk bölümler oluşturabilir. Bozuk bölümler sabit diskin performansını düşürür ve veri yazmayı (Dosya kaydetme gibi) zorlaştırır hatta imkânsız hale getirir. Hata Denetleme Yardımcı Programı sabit sürücüde bozuk bölümleri tarar ve belirli dosyaların veya klasörlerin yanlış yerleştirilip yerleştirilmediğini belirlemek üzere dosya sistemi hatalarını tarar.

Bilgisayarınızı her gün kullanıyorsanız veri kayıplarını önlemeye yardımcı olması için bu yardımcı programı haftada bir çalıştırmayı denemelisiniz.

Bu yardımcı program, dosya ve klasörlerin bütünlüğünü veya sabit diski fiziksel hatalar açısından tarayarak sistemin tamamını kontrol eder. Sistemin okuyabileceği tüm formatlanmış disklerde kullanılabilir. Bu program, sistemin uygun bir biçimde kapanmadığı zamanlarda her seferinde veya ayda en az bir kere kullanılmalıdır.

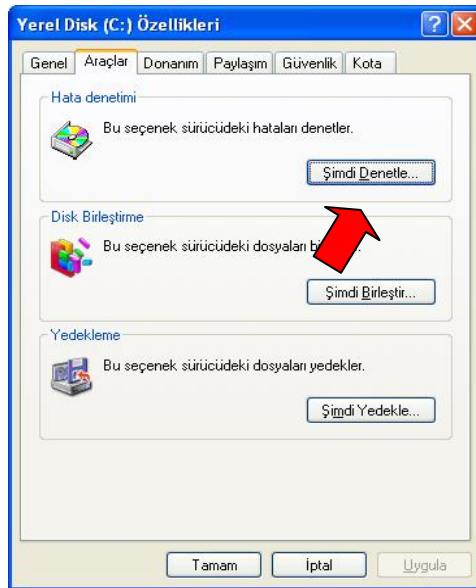
Scandisk işlemi MS-DOS ve Windows'un bütün sürümlerinde vardır. Scandiski çalıştırmadan önce çalışmakta olan ve açık olan bütün programlar kapatılmalıdır. Daha sonra

Bilgisayarım penceresi açılarak Scandisk yapılacak sabit disk sürücüsü üzerinde farenin sağ tuşuna basılarak açılan menüden “Özellikler” seçeneğine tıklanır. Bu işlem aşağıdaki Şekil 2.1’de gösterilmiştir.



Şekli 2.1: Scandisk

Özellikler seçeneği seçilip çalıştırıldığında aşağıda Şekil 2.2’deki pencere ekrana gelir.



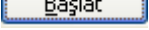
Şekil 2.2: Scandisk çalıştırma

Bu pencerede Scandisk işlemi için **Şimdi Denetle...** butonuna tıklanır.

Disk denetleme butonuna basılınca ekrana aşağıdaki Şekil 2.3'teki pencere gelecektir. Bu pencerede disk denetim seçenekleri vardır. Bu seçeneklerden yapmak istenen işlemlerden biri ve ya her ikisi seçilerek başlat butonuna basılır.



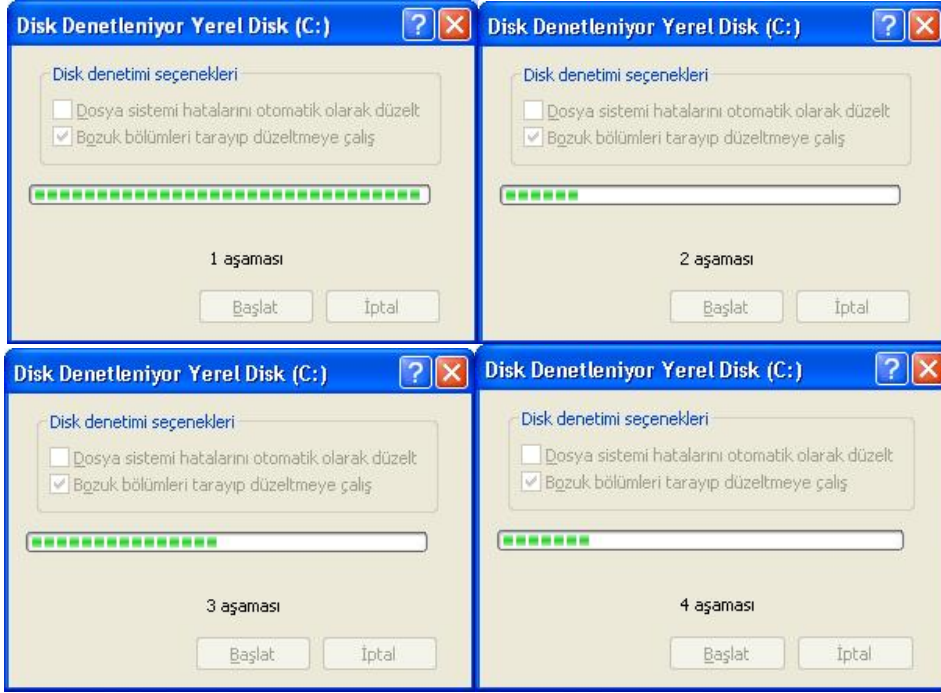
Şekil 2.3: Disk denetleme diyalog kutusu

Eğer dosya sistemi hatalarını otomatik düzelt seçeneği seçilip  butonu tıklanırsa ekrana Şekil 2.4'teki diyalog kutusu açılacaktır. Bu diyalog kutusunda, disk denetim işleminin bilgisayarın bir sonraki oturumunda yapılacağı ile ilgili kullanıcıyı bilgilendiren mesaj vardır.



Şekil 2.4: Disk denetim bilgilendirme mesajı

Eğer “Bozuk bölümleri tarayıp düzeltmeye çalış” seçeneği seçilirse, aşağıdaki disk denetleniyor pencereleri aşama aşama gerçekleşecektir.



Şekil 2.5. Disk hatalarını tespit edin ve onarın

Denetleme işlemleri bitiminde aşağıdaki Şekil 2.6'daki diyalog kutusu ekrana gelir. Tamam, tıklanarak denetleme işlemi bitirilir.



Şekil 2.6: Disk denetim aşamaları

Yukarıda anlatılan işlemleri kısaca aşağıdaki gibi özetleyebiliriz:

Hata Denetleme yardımcı programını çalıştırmak için:

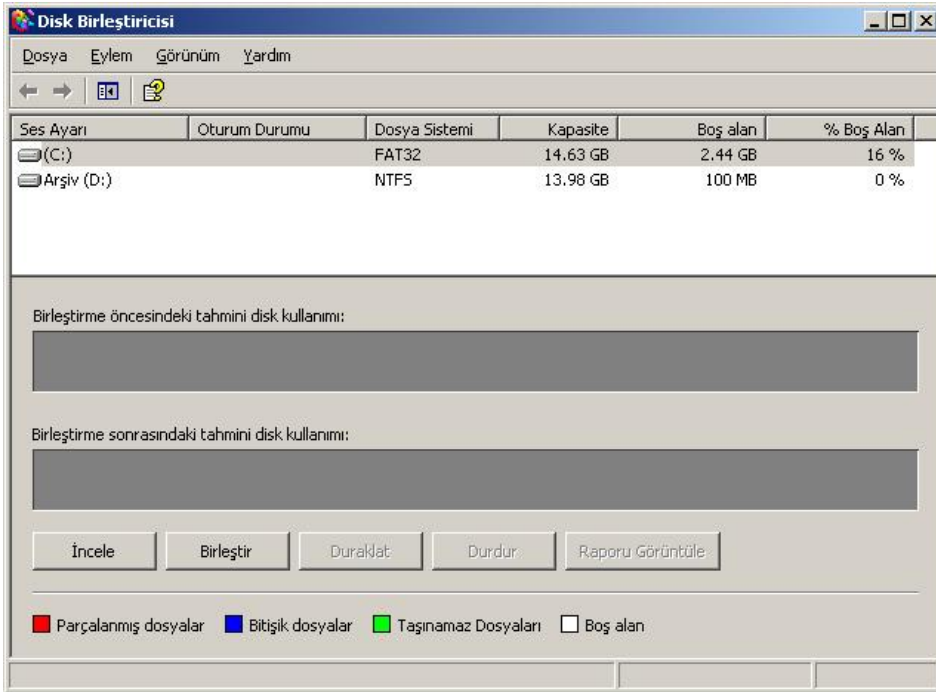
1. Başlat'ı sonra da Bilgisayarımı tıklatınız.
2. Bilgisayarım penceresinde, bozuk bölümleri aramak istediğiniz sabit diski sağ tıklatınız ve Özellikler'i tıklatınız.
3. Özellikler iletişim kutusunda, Araçlar sekmesini tıklatınız.
4. Şimdi Denetle butonunu tıklatınız.
5. Disk Denetle iletişim kutusunda, Bozuk bölümleri tarayıp düzeltmeye çalış onay kutusunu ve/veya "Dosya sistemi hatalarını otomatik düzelt" seçiniz ve Başlat'ı tıklatınız. Çoğu durumda, "Bozuk bölümleri tarayıp düzeltmeye çalış" seçeneğini seçilir.
6. Bozuk bölümler bulunduğu düzeltmek üzere seçiniz.

2.1.2. Birleřtirici (defragmenter)

Bir dosya sabit diske kaydedildiğinde, iřletim sistemi bu dosyayı iki veya daha çok para olarak depolama aygıtının farklı paraları üzerine depolar. Sistem, bu depolanmış paraların nerelerde kaydedildiğine dair bir kaydı, FAT ya da NTFS’de tutar. Eđer iřletim sistemi bu dosyaya ihtiya duyarsa, FAT ya da NTFS dosya sistemini bu dosyayı bulmak için sorgular ve bölünmüş dosyaları ardışık olarak birbirine bağlar.

Bir program ya da veri, sabit disk sürücüsüne kaydedildiğinde, bu bilgiler sabit diskin çeřitli kısımlarına iki veya daha fazla paraya bölünerek yazılabilir. Buna, fragmentation (Paralama) denir. Paralama, bir sürücünün performansını düşürür. Birleřtirici programı, paraları kullanılabilir alanlarda tekrar bir araya getirerek, sabit diskteki boşlukları en iyi şekilde kullanır ki bu da programların daha abuk okunmasını ve alıřtırılmasını sağlar. Teknisyenler, birleřtirici programları genellikle scandisk programını kullandıktan sonra başlatırlar. Birleřtirici aynı zamanda, sık sık dosyaların oluşturulduđu ve iptal edildiđi sistemler için düzenli aralıklarda otomatik olarak alıřmak üzere de ayarlanabilir.

řekil 2.7’de C sürücüsü için kullanılan birleřtirici iřlemi görölmektedir.



řekil 2.7: Birleřtirici

Birleřtirme iřlemi yapılacağı zaman, ilk olarak defrag yapacak kadar zamanınız olup olmadığından emin olunuz. Defrag iřlemi bir miktar zaman alacaktır. Defrag’ a başlamak için “**BAřLAT-programlar-donatılar-sistem araçları ve disk birleřtirici**” seçilir. Bu iřlem alıřtığında yukarıdaki řekil 2.7’deki disk birleřtirici penceresi ekrana gelecektir.

Görüldüğü gibi iki (2) sabit disk sürücüsü vardır. Eğer daha fazla sabit disk sürücüsü varsa bu pencere içinde bu sürücüler de görünecektir.

Bir sonraki aşamada hangi sabit diske “Disk Birleştirme” yapılacaksa o disk seçilir (Sürücü üzerinde bir kere sol tıklanarak) , sonra **İncele** butonuna sol fare tuşu ile tıklanır. Bu işlemden sonra seçili sürücü için disk birleştirme işlemi başlayacaktır. Bu sırada seçili diskin disk birleştirmeye ihtiyacı olup olmadığına dair ekrana Şekil 2.8’deki bilgilendirme mesajı penceresi gelecektir.



Şekil 2.8: Disk birleştirme bilgi mesajı

Eğer sürücünün birleştirmeye ihtiyacı var ise **Birleştir** butonuna doğrudan tıklanarak işlem başlatılır. Ekrana aşağıdaki Şekil 2.9 penceresi gelecektir. Bu pencerede aşağıdaki bilgilerle ilgili açıklamaları göreceksiniz.

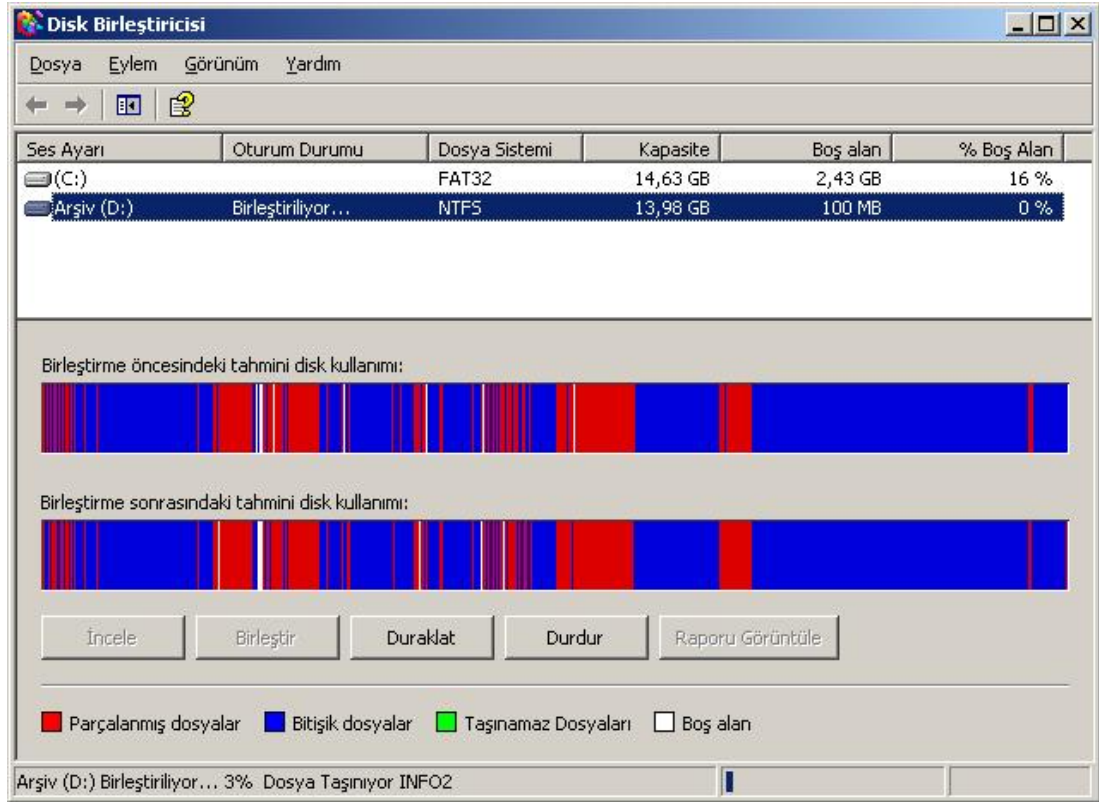
Birleştirme öncesi ve sonrası tahmini disk kullanımı,

Parçalanmış dosyalar

Bitişik dosyalar

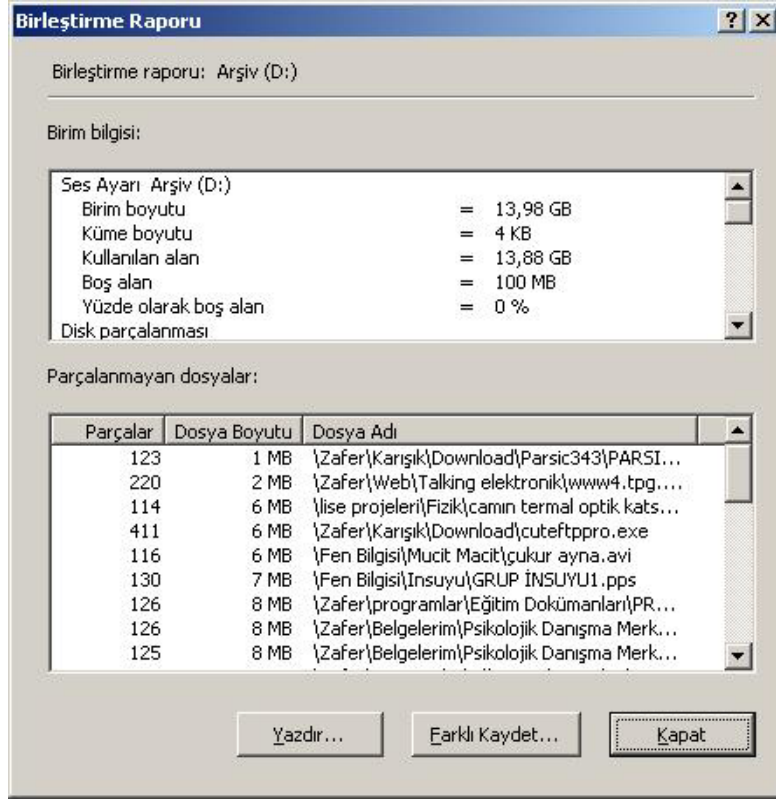
Taşınamaz Dosyaları

Boş alan ile ilgili bilgiler görüntülenecektir.



Şekil 2.9: Disk birleřtiricisi

Bu işlem tamamlandıktan sonra ekrana “Birleřtirme Rapor Penceresi” şekil 2.10 gelir. Bu pencerede seçilen sürücü için birim boyutu, küme boyutu, boş alan, dolu alan gibi birleřtirme rapor bilgileri vardır. İstenirse kullanıcı bu rapor bilgilerinin yazdırabilir. İsterse de kaydedebilir.



Şekil 2.10: Disk birleştirme raporu

2.1.3. Chkdsk

Dosya sistemini temel alarak, diske ait durum raporu oluşturur ve görüntüler. Chkdsk komutu diskteki hataları da listeler ve düzeltir. Parametresiz kullanıldığında, chkdsk geçerli sürücüdeki diskin durumunu görüntüler.

Kullanılış biçimleri: Bu komut aşağıdaki biçimlerde kullanılır.

chkdsk [birim:][[Yol] DosyaAdı] [/f] [/v] [/r] [/x] [/i] [/c] [/l[:boyut]]

Parametreler

Birim: Sürücü adını (Sonunda üst üste iki nokta olarak), bağlama noktasını veya birim adını belirtir.

[Yol] DosyaAdı: Chkdsk komutunun parçalanma denetimi yapmasını istediğiniz dosyanın veya dosya kümesinin konumunu ve adını belirtir. Birden çok dosya belirtmek için joker karakterlerini (* ve ?) kullanabilirsiniz.

/f: Diskteki hataları düzeltir. Diskin kilitlenmesi gerekir. Chkdsk sürücüyü kilitleyemezse, bilgisayarı yeniden başlattığımızda sürücüyü denetlemek isteyip istemediğinizi soran bir ileti görüntülenir.

/v: Disk denetlendikçe, her dizindeki her dosyanın adını görüntüler.

/r: Bozuk kesimleri bulur ve okunabilir bilgileri kurtarır. Diskin kilitlenmesi gerekir.

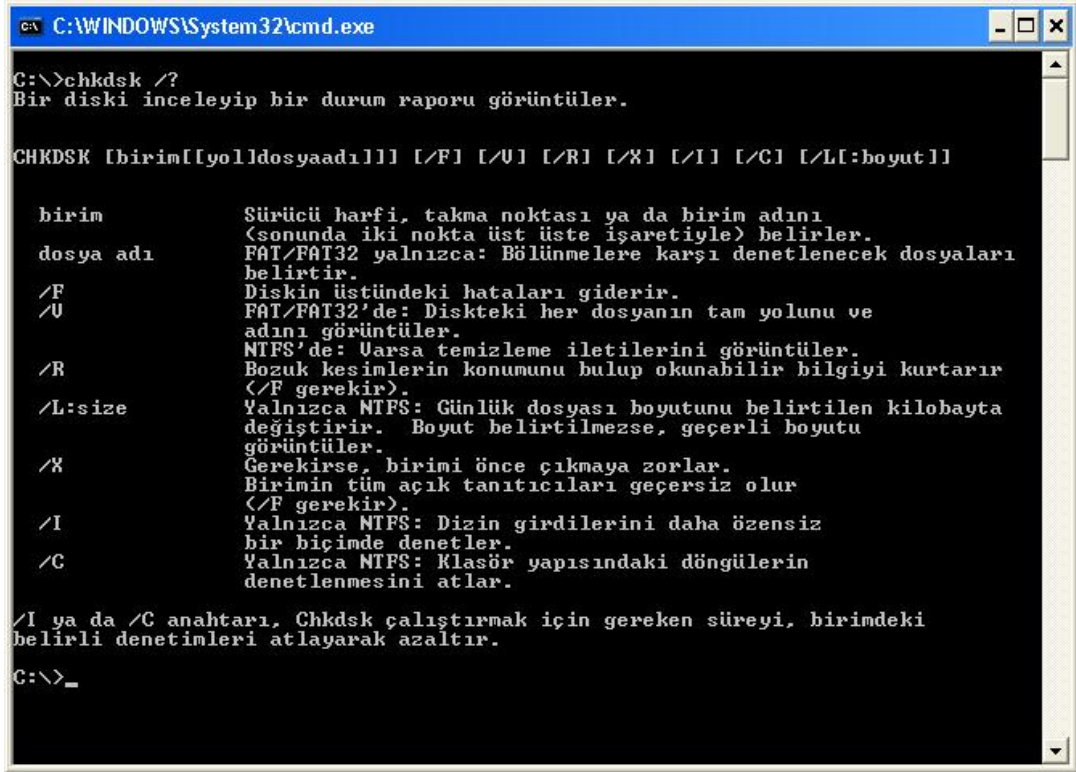
/x: Yalnızca NTFS ile kullanınız. Gerekliyse, birimi önce çözmeye zorlar. Sürücüye açık işleyicilerin tümü geçersizdir. /x ayrıca, /f işlevlerini de içerir.

/i: Yalnızca NTFS ile kullanınız. Chkdsk çalıştırmak için gereken süreyi azaltmak üzere, izin girişlerini daha düşük düzeyde denetler.

/c: Yalnızca NTFS ile kullanınız. Chkdsk çalıştırmak için gereken süreyi azaltmak üzere, klasör yapısı içinde döngü denetimlerini atlar.

/l[:boyut] :Yalnızca NTFS ile kullanınız. Günlük dosyası boyutunu, yazdığınız boyuta değiştirir. Boyut parametresini atlarsanız, /l geçerli boyutu görüntüler.

/? :Komut isteminde yardımı görüntüler. Bu konular Şekil 2.11'de Chkdsk yardım ekranında görülmektedir.



```
C:\WINDOWS\System32\cmd.exe
C:\>chkdsk /?
Bir diski inceleyip bir durum raporu görüntüler.

CHKDSK [birim[[yol]dosyaadı]] [/F] [/U] [/R] [/X] [/I] [/C] [/L[:boyut]]

birim          Sürücü harfi, takma noktası ya da birim adını
dosya adı     (sonunda iki nokta üst üste işaretiyle) belirler.
              FAT/FAT32 yalnızca: Bölümlere karşı denetlenecek dosyaları
              belirtir.
              /F          Diskin üstündeki hataları giderir.
              /U          FAT/FAT32'de: Diskteki her dosyanın tam yolunu ve
              adını görüntüler.
              /R          NTFS'de: Uarsa temizleme iletilerini görüntüler.
              /L:size     Yalnızca NTFS: Günlük dosyası boyutunu belirtilen kilobayta
              değiştirir. Boyut belirtilmezse, geçerli boyutu
              görüntüler.
              /X          Gerekirse, birimi önce çıkmaya zorlar.
              Birimin tüm açık tanıtıcıları geçersiz olur
              (/F gerekir).
              /I          Yalnızca NTFS: Dizin girdilerini daha özensiz
              bir biçimde denetler.
              /C          Yalnızca NTFS: Klasör yapısındaki döngülerin
              denetlenmesini atlar.

/I ya da /C anahtarı, Chkdsk çalıştırmak için gereken süreyi, birimdeki
belirli denetimleri atlayarak azaltır.
C:\>_
```

Şekil 2.11: Chkdsk ekranı

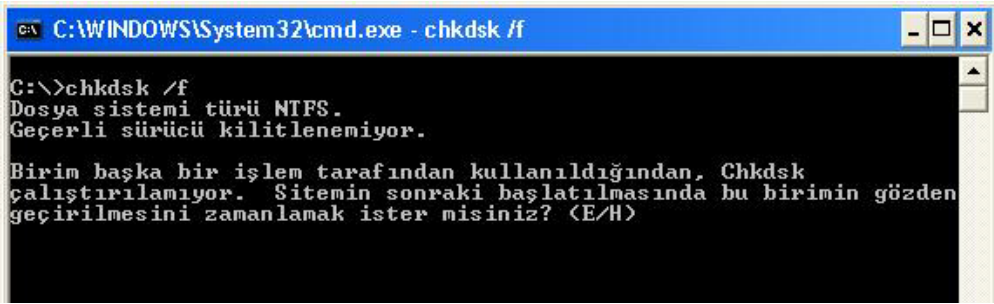
➤ Açıklamalar

FAT nedir? MS-DOS ve diğer Windows tabanlı işletim sistemlerinin, dosyaları düzenlemek ve yönetmek için kullanılan bir dosya sistemidir. Dosya ayırma tablosu (FAT), bir birimi FAT veya FAT32 dosya sistemlerini kullanarak biçimlendirdiğinizde Windows'un oluşturduğu bir veri yapısıdır. Windows her dosyaya ilişkin bilgileri FAT içinde saklayarak dosyayı daha sonra bulabilir.

NTFS nedir? Performans, güvenlik, güvenilirlik ve FAT dosya sisteminin hiçbir sürümünde bulunmayan ileri düzey özellikleri sağlayan gelişmiş bir dosya sistemidir. Örneğin NTFS, standart işlem günlüğü ve kurtarma tekniklerini kullanarak birim tutarlılığını garanti eder. Bir sistemde hata ortaya çıkarsa, NTFS dosya sisteminin tutarlılığını geri yüklemek için günlük dosyası ve denetim noktası bilgilerini kullanır. Windows 2000 ve Windows Xp'de NTFS, dosya ve klasör izinleri, şifreleme, disk kotaları ve sıkıştırma gibi gelişmiş özellikleri de sağlar.

Chkdsk komutunu çalıştırmak ve kullanabilmek için Yöneticiler Grubu'nun üyesi olmanız gerekir.

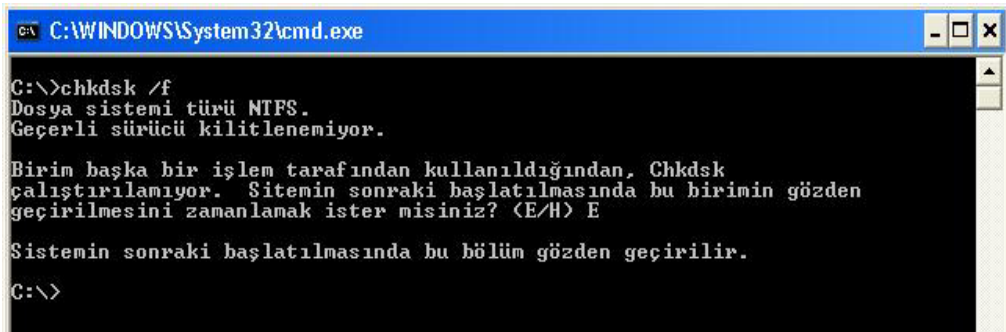
Chkdsk komutunun disk hatalarını düzeltmesini istiyorsanız, sürücüde açık dosya olmaması gerekir. Açık dosya varsa, aşağıdaki Şekil 2.12'deki gibi hata iletisi görüntülenir:



```
C:\>chkdsk /f
Dosya sistemi türü NTFS.
Geçerli sürücü kilitlenemiyor.

Birim başka bir işlem tarafından kullanıldığından, Chkdsk
çalıştırılmıyor. Sistemin sonraki başlatılmasında bu birimin gözden
geçirilmesini zamanlamak ister misiniz? (E/H)
```

Şekil 2.12: Chkdsk hata iletileri 1



```
C:\>chkdsk /f
Dosya sistemi türü NTFS.
Geçerli sürücü kilitlenemiyor.

Birim başka bir işlem tarafından kullanıldığından, Chkdsk
çalıştırılmıyor. Sistemin sonraki başlatılmasında bu birimin gözden
geçirilmesini zamanlamak ister misiniz? (E/H) E

Sistemin sonraki başlatılmasında bu bölüm gözden geçirilir.
C:\>
```

Şekil 2.13: Chkdsk hata iletileri 2

Şekil 2.12'deki mesaja (E/H) E cevabı verildiğinde, chkdsk bilgisayarınızı yeniden başlattığınızda sürücüyü otomatik olarak denetler ve hataları düzeltir. Sürücü bölümü bir önyüklemeye bölümüyse, chkdsk sürücüyü denetledikten sonra bilgisayarı otomatik olarak yeniden başlatır.

➤ **Disk hatalarının raporlanması**

Chkdsk, dosya ayırma tablosu (FAT) ve NTFS dosya sistemleriyle ilgili disk alanını ve disk kullanımını denetler. Chkdsk, her iki dosya sistemine özgü bilgileri bir durum raporuyla sunar. Durum raporu, dosya sisteminde bulunmuş hataları gösterir. Chkdsk etkin bölümde /f komut satırı seçeneği olmadan çalıştırılırsa, birimi kilitleyemeyeceğinden yanıltıcı hatalar rapor eder. Chkdsk komutunu, hataları denetlemek üzere tüm disklerde zaman zaman kullanmalısınız.

➤ **Disk hatalarını düzeltme**

Chkdsk, disk hatalarını yalnızca, /f komut satırı seçeneği belirtilmişse düzeltir. Chkdsk komutunun hataları düzeltmek için sürücüyü kilitleyebilmesi gerekir. Onarımlar genellikle diskin dosya ayırma tablosunu değiştirdiğinden ve kimi zaman veri kaybına neden olduğundan, chkdsk aşağıdakine benzer bir iletiyle sizden onay ister:

3 zincirde 10 kayıp ayırma birimi bulundu.

Kayıp zincirler dosyalara dönüştürülsün mü?(E/H)

E tuşuna basarsanız, Windows her bir kayıp zinciri, kök dizinde, **Filennnn.chk** biçiminde bir adla, dosya olarak kaydeder. Chkdsk sonlandığında, gereksinim duyduğunuz verileri içerip içermediklerini görmek için bu dosyaları gözden geçirebilirsiniz. H tuşuna basarsanız, Windows diski onarır; ancak kayıp ayırma birimlerinin içeriğini kaydetmez. /f komut satırı seçeneğini kullanmazsanız, chkdsk dosyanın onarılması gerekiyorsa bir ileti görüntüler, ancak hataları düzeltmez.

Not: Chkdsk /f komutunu çok büyük (Örneğin, 80 gigabayt) veya çok fazla (örneğin, milyonlarca) dosya içeren bir diskte kullanırsanız, chkdsk komutunun denetimi bitirmesi çok uzun bir zaman (Örneğin, birkaç gün) alabilir. Chkdsk, tamamlanıncaya kadar denetimi bırakmadığından, bu süre boyunca bilgisayar kullanılamaz.

➤ **FAT diski denetleme**

Windows, FAT disk için chkdsk durum raporunu aşağıdaki biçimde görüntüler:

Birim Seri Numarası B1AF-AFBF
Toplam disk alanı 72214528 bayt
3 gizli dosya da 73728 bayt
12 dizinde 30720 bayt
386 kullanıcı dosyasında 11493376 bayt
Bozuk kesimde 61440 bayt
Diskteki kullanılabilir alan 60555264 bayt
Her ayırma biriminde 2048 bayt
Diskteki toplam yerleşim birimi 35261
Diskteki kullanılabilir yerleşim birimi 29568

➤ **NTFS diski denetleme**

Windows, NTFS disk için chkdsk durum raporunu aşağıdaki biçimde görüntüler:

Dosya sistemi türü NTFS.

CHKDSK dosyaları denetliyor...

Dosya denetimi tamamlandı.

CHKDSK izinleri denetliyor...

Dizin denetimi tamamlandı.

CHKDSK güvenlik tanımlayıcılarını denetliyor...

Güvenlik tanımlayıcısı denetimi tamamlandı.

Toplam disk alanı 12372 kilobayt.

3 kilobayt 1 kullanıcı dosyalarında.

2 kilobayt 1 dizinde.

4217 kilobayt sistem kullanımında.

Diskteki kullanılabilir alan 8150 kilobayt.

Her ayırma biriminde 512 bayt.

Diskteki toplam yerleşim birimi 24745.

Diskteki kullanılabilir yerleşim birimi 16301.

➤ **Chkdsk komutunu açık dosyalarla kullanma**

/f komut satırı seçeneğini belirtirseniz, diskte açık dosyalar varsa chkdsk bir hata iletisi verir. /f komut satırı seçeneğini belirtmezseniz ve açık dosyalar varsa, chkdsk diskte kayıp ayırma birimleri rapor edebilir. Bu, açık dosyalar henüz dosya ayırma tablosuna kaydedilmemişse ortaya çıkar. Chkdsk çok sayıda ayırma biriminin kayıp olduğunu rapor ederse, diski onarmanız iyi olur.

➤ **Fiziksel disk hataları bulma**

Dosya sisteminde fiziksel disk hatalarını bulmak için /r komut satırı seçeneğini kullanılır.

➤ **Bozuk disk kesimlerini raporlama**

Chkdsk komutunun rapor ettiği bozuk kesimler, diskin işletim için ilk hazırlandığında bozuk olarak işaretlenmiştir. Bunlar bir tehlike oluşturmaz.

➤ **Çıkış kodlarını anlama**

Aşağıda Tablo 2.1'de, sonra chkdsk' in rapor ettiği çıkış kodları listelenmiştir.

Çıkış kodu	Açıklama
0	Hata bulunmadı.
1	Hata bulundu ve düzeltildi.
2	Disk temizliği (Örneğin, gereksiz veri toplaması) yapıldı veya /f belirtilmediğinden temizlik yapılmadı.
3	Disk denetlenemedi, hatalar düzeltilemedi veya /f belirtilmediğinden hatalar düzeltilemedi.

Tablo 2.1: Hata rapor kodları

Örnekler

1. D sürücüsündeki diskin denetlenmesini ve Windows'un hataları düzeltilmesini istiyorsanız aşağıdaki komut satırı yazılır:

chkdsk d: /f

Chkdsk hatayla karşılaştığında duraklar ve ileti görüntüler. Chkdsk, diskin durumunu liste biçiminde sunan bir rapor görüntüleyerek sonlanır. Chkdsk sonlanıncaya dek belirtilen sürücüde hiçbir dosyayı açamazsınız.

2. Bir FAT diskte, geçerli dizindeki tüm dosyaları bitişik olmayan bloklar açısından denetlemek istiyorsanız aşağıdaki komut satırı yazılır:

chkdsk *.*

Chkdsk bir durum raporu görüntüler ve sonra bitişik olmayan bloklara sahip dosya belirtimiyle eşleşen dosyaları listeler.

2.1.4. Regedit

Kayıt, donanım ve PC ortamı hakkında yapılandırma verisi taşıyan bir veri tabanıdır. REGEDIT uzman teknisyenler tarafından kullanılan bir komuttur.

“Kayıt Defteri Düzenleyicisi”, bilgisayarınızın nasıl çalıştığı konusunda bilgiler içeren sistem kayıt defterinizdeki ayarları görüntülemek ve değiştirmek için gelişmiş bir araçtır. Kayıt defteri; bir bilgisayarın yapılandırılmasına ilişkin bilgilerin bulunduğu veritabanı deposudur. Kayıt defterinde Windows’un çalışması sırasında sürekli başvurduğu bilgiler bulunur. Örneğin, kullanıcıların profilleri, bilgisayarda yüklü olan programlar ve bu programların oluşturabileceği belge türleri, klasör ve program simgeleri için özellik ayarları, donanıma ilişkin bilgiler vs.

Windows yapılandırma bilgilerini, ağaç biçiminde düzenlenen bir veritabanında (Kayıt defteri) depolar. “Kayıt Defteri Düzenleyicisi”, kayıt defterini incelemenizi ve değiştirmenizi sağlar; ancak genellikle bunu yapmanıza gerek yoktur ve doğru olmayan değişiklikler yapmak sisteminizi bozabilir. Kaydı düzenlemeye ve geri yüklemeye hazır olan ileri düzeyde bir kullanıcı, yinelenen girdileri eleme veya kaldırılmış veya silinmiş programlara ait girişleri silme gibi görevler için “Kayıt Defteri Düzenleyicisi”ni güvenle kullanabilir.

Windows’ta, sistem yapılandırma bilgileri merkezi olarak kayıt defterinde bulunur. Böylece bilgisayarın veya ağın yönetimi kolaylaşır; ancak kayıt defterinde yapılacak yanlış bir düzenleme işletim sistemini devre dışı kalmasına neden olabilir.

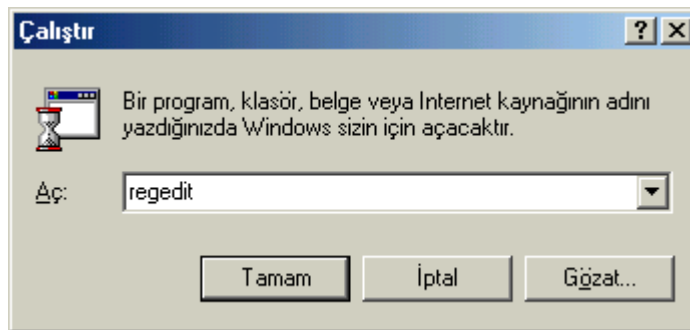


Şekil 2.14: Kayıt düzenleyicisi

Şekil 2.14'te gösterilen “Kayıt Düzenleyicisi”, kayıta, Windows Explorer'inkine benzer bir yolla erişim sağlar. Pencerenin sol tarafında klasör simgeleri vardır. Bu klasörlere anahtar denir. Bir anahtarın önünde yer alan artı işaretine tıklayarak diğer alt anahtarlara ulaşabilirsiniz. Böylelikle kompleks bir yapıya sahip kayıt veritabanının temellerine ulaşabilir ve kayıtları silip yenilerini de ekleyebilirsiniz. Kayıta herhangi bir şey değiştirildiğinde, sistem hataları veya arızaları meydana gelebilir. Değişiklikler silinemeyeceğinden, bu programın çok dikkatli bir biçimde kullanılması önerilir.

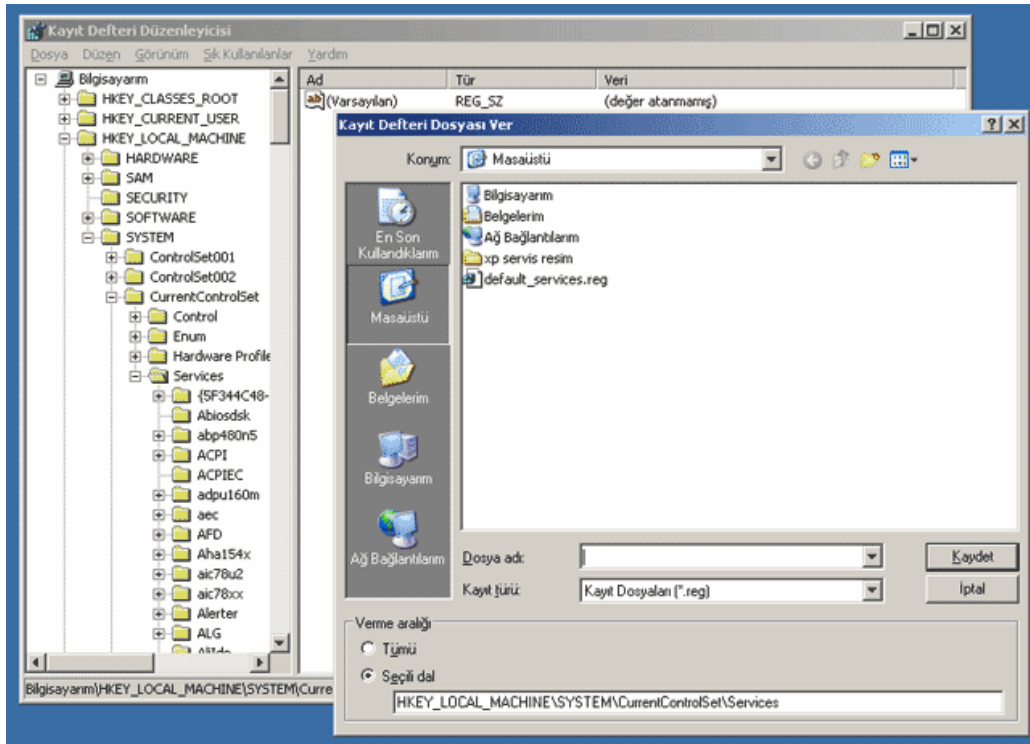
DİKKAT: Kayıt defterinde değişiklik yapmadan önce kesinlikle bir yedek kopyasını oluşturunuz.

Kayıt defterini yedeklemek için, “Yedekleme” gibi bir program kullanabilirsiniz. Kayıt defterinde değişiklikler yaptıktan sonra, “Otomatik Sistem Kurtarma” (ASR) diski oluşturunuz. Sorun giderme amacıyla, kayıt defterinde yaptığınız değişikliklerin listesi de tutulabilir.



Şekil 2.15. Regediti Çalıştırma

Kayıt denetleyicisi **Başlat-Çalıştır** yolunu izleyerek çıkan pencereye **regedit** yazılarak çalıştırılır. Şekil 2.15'te görüldüğü gibi. Kayıt Defteri Düzenleyicisi, bizlere hizmetler ile ilgili ayarlara yönelik kayıtların tutulduğu alana ulaşmamıza ve yedeklememize yarayan oldukça yararlı ve güçlü bir program, bu sebeple yapılan işlemlerin sırasını dikkatlice takip etmek gerekir. Ancak, öncelikle Kayıt Defteri yedeklenmelidir. Önce [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services] yolunu izleyerek “Services” anahtarını bulup seçilir. **Dosya** menüsünden, **Ver** komutunu kullanarak seçili olan dalı kayıt defterinden dışarıya alınmasını sağlayacak olan pencere ile karşılaşılacaktır. Dosya adı kutusuna dosya ismini girdikten sonra **Kaydet** butonuna tıklayarak seçtiğiniz dalı “*.reg” uzantısı ile kaydetmiş olursunuz.



Şekil 2.16: Kayıt defterinden dışarıya kayıt aktarılması

Pencerenin aşağı kısmında “Seçili Dal” işaretli ise sadece seçili olan anahtar ve tüm alt anahtarlar ait bilgiler belirttiğiniz dosyaya kopyalanır. Eğer “Tümü” seçeneğini seçerseniz tüm kayıt defteri kopyalanır ki bu işlem biraz uzun sürebilir.

Dışarıya aldığımız bu kayıt dalı kopyasını istediğiniz zaman çift tıklayarak kayıt defterinize geri ekleyebilirsiniz. Eğer işletim sisteminiz, kapattığınız bir hizmet sonucunda başlayamaz hale geldiyse, işletim sisteminizi Güvenli Mod da açtıktan sonra kayıt defterine dışarıya aldığımız kopyayı geri ekleyebilirsiniz.

2.1.4.1. Kayıt Defteri Düzenleyicisi Anahtarları

Kayıt Defteri Düzenleyicisi'nin gezinme alanı, bilgisayarda, her biri önceden tanımlı anahtar temsil eden klasörlerin bulunduğu alandır. Klasörler, kayıt defterindeki anahtarları temsil eder ve Kayıt Defteri Düzenleyicisi penceresinin sol tarafındaki gezinme alanında gösterilir. Soldaki başlık alanında, bir anahtardaki girdiler görüntülenir. Girdiyi çift tıklattığınızda, bir düzenleme iletişim kutusu açılır.

Önceden Tanımlı Anahtar: Kayıt defterinin ana bölümlerinden birini oluşturan anahtardır. Örneğin **HKEY_CLASSES_ROOT** önceden tanımlı bir anahtardır.

Anahtar: Kayıt defteri düzenleyicisinde çalışırken sol bölmede görüntülenen bir klasörün alt anahtarlar ve değer girdileri içeren bölümleridir. Örneğin **Enviroment**, **HKEY_CURRENT_USER** anahtarının bir alt anahtarıdır. Aşağıda Tablo 2.2'de Kayıt Düzenleyici penceresinde bulunan anahtarlar ve açıklamaları görülmektedir.

Klasör/önceden tanımlı anahtar	Açıklama
HKEY_CURRENT_USER	Oturumu açık durumdaki kullanıcının yapılandırma bilgileri kökünü içerir. Kullanıcının klasörleri, ekran renkleri ve Denetim Masası ayarları burada saklanır. Bu bilgiye kullanıcı profili olarak başvurulabilir.
HKEY_USERS	Bilgisayardaki tüm kullanıcı profillerinin kökünü içerir. HKEY_CURRENT_USER, HKEY_USERS'ın alt anahtarıdır.
HKEY_LOCAL_MACHINE	Bilgisayara özel yapılandırma bilgilerini (herhangi bir kullanıcı için) içerir.
HKEY_CLASSES_ROOT	HKEY_LOCAL_MACHINE\Yazılım'ının alt anahtarıdır. Burada saklanan bilgiler, Windows Gezgini'ni kullanarak bir dosya açtığınızda doğru programın açılmasını sağlar.
HKEY_CURRENT_CONFIG	Sistem başlangıcında yerel bilgisayar tarafından kullanılan donanım profili hakkındaki bilgileri içerir.

Tablo 2.2. Önceden Tanımlı Anahtarlar

Aşağıda Tablo 2.3'te kayıt düzenleyicisi için sistem tarafından geçerli olarak tanımlanan ve kullanılan veri türleri listelenmiştir.

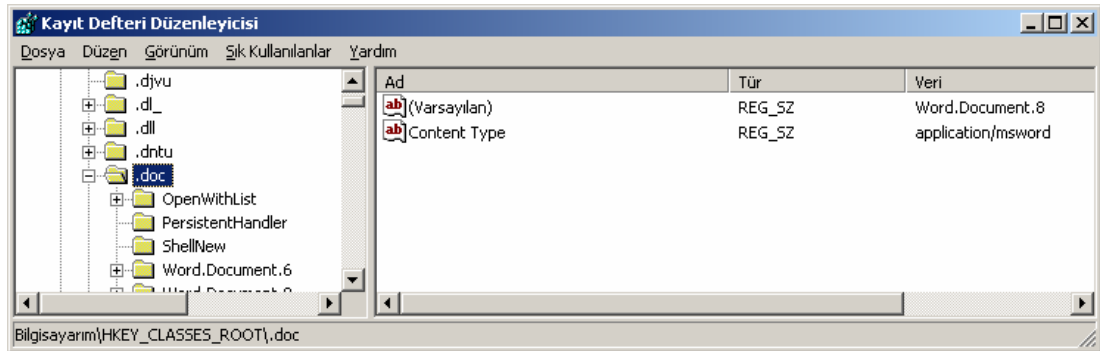
Veri türü	Açıklama
REG_BINARY	İşlenmemiş ikili veri. Donanım bileşeni bilgilerinin çoğu ikili veri olarak saklanır ve Kayıt Defteri Düzenleyicisi'nde on altılık biçimde görüntülenir.

REG_DWORD	4 bayt uzunluğunda bir sayıyla gösterilen veriler. Aygıt sürücüleri ve hizmetler için kullanılan parametrelerin çoğu bu türdedir ve Kayıt Defteri Düzenleyicisi'nde ikili, on altılı veya onlu biçimde görüntülenir.
REG_EXPAND_SZ	Değişken uzunluklu veri dizesi. Bu veri türü, bir program veya hizmet veriyi kullandığında çözülen değişkenleri içerir.
REG_MULTI_SZ	Çoklu dize. Kullanıcıların okuyabileceği bir biçimde listeleri veya çok sayıda değerleri olan değerler genellikle bu türdendir. Girişler birbirinden boşluk, virgül veya başka işaretlerle ayrılmıştır.
REG_SZ	Sabit uzunluklu metin dizesi.
REG_FULL_RESOURCE_DESCRIPTOR	Bir donanım bileşeninin veya sürücünün kaynak listesini saklamak için tasarlanmış iç içe diziler serisidir.

Tablo 2.3: Kayıt düzenleyicisinde kullanılan veri türleri

HKEY_CLASSES_ROOT

Sürükle bırak işlemleri ile ilgili yazılım ayarları, kısa yol ve tüm diğer kullanıcı ar birimi ile ilgili bilgileri içerir. Burada ilişkilendirilmiş her dosya için bir alt anahtar daha bulunur.



Şekil 2.17: HKEY_CLASSES_ROOT

Bu bölümde görüldüğü gibi “.exe”, “.zip”, “.doc”, “.dll”, v.s. gibi birçok anahtar vardır. Bu anahtarlara tıkladığınızda sağ tarafta “(Varsayılan)” adında bir “Dize Değeri” göreceksiniz. Bu “(Varsayılan)” her anahtarında mutlaka bulunur; ama hepsinde dolu değildir. Buradaki değer, uzantıyla ilgili asıl bilgileri içeren ve yine HKEY_CLASSES_ROOT anahtarını altında bulunan başka bir anahtarın adını içerir.

HKEY_CLASSES_ROOT anahtarını içinde bulunan CLSID anahtarını bu anahtarın devasa büyüklükte olmasının asıl sebebidir. Burada CLSID içinde, Windows’un ve diğer programların çeşitli amaçlar için kullandıkları inanılmaz çeşitlilikte ve sayıdaki sınıflar ve bunların tanımlamaları yer alır.

HKEY_CURRENT_USER

Bu bölümde Windows'un çeşitli kullanıcı ayarları bulunur. Yazı imlecinin yanıp sönme hızından altmenülerin açılması için üzerinde beklemeniz gereken süreye, pencerelerin büyütülüp küçültülmesi sırasındaki animasyona kadar birçok ayarı kontrol edebilirsiniz. Şekil 2.18'de HKEY_CURRENT_USER 'ın alt anahtarları görülmektedir. Bu alt anahtarların birkaç tanesini kısaca açıklayalım.

AppEvents: Sistem ve uygulamalarda kullanılmak üzere atanmış sesler ile ilgili ayarlar burada yer alır.

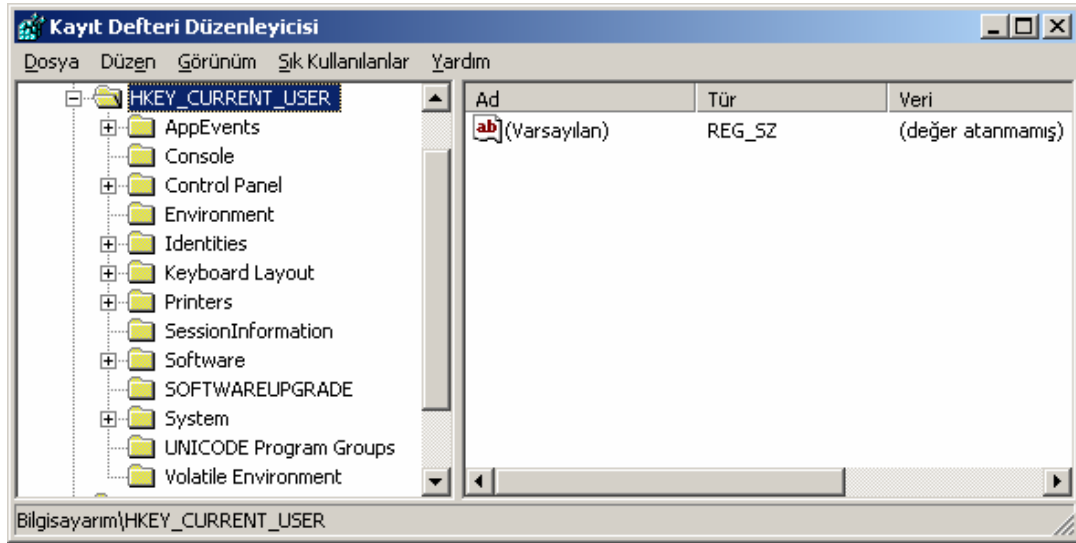
Control Panel: Burada Windows 98, ME ve 3.x'deki System.ini, Win.ini ve Control.ini dosyalarının içeriğine benzeyen denetim masası ayarları yer alır.

InstallLocationsMRU: Başlangıç klasöründe yer alan programların sabit diskteki yollarını belirler.

Keyboard layout: O an kullanılan klavye düzenine buradan da ulaşılabilir.

Network: Ağ bağlantı bilgileri burada yer alır. Remote Access: Eğer çevirmeli ağ üzerinde ağ bağlantısı kullanılıyorsa o anki bağlantı bilgileri burada bulunur.

Software: Bilgisayara bağlı kullanıcıların, yüklemiş olduğu yazılımların konfigürasyon ayarlarına ulaşmakta kullanılır.



Şekil 2.18: HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

Her kullanıcı için aynı olan bu değerler bilgisayarda yer alan donanım ve yazılım ayarları üzerine bilgiler içerir. Bu anahtarın altında Şekil 2.19'da görüldüğü üzere alt anahtar bulunur. Bu alt anahtarların birkaç tanesini kısaca açıklayalım.

Config: konfigürasyon bilgileri ve ayarlarına buradan ulaşmanız mümkün.

Enum: Donanım aygıt bilgi ve ayarları burada bulunur.

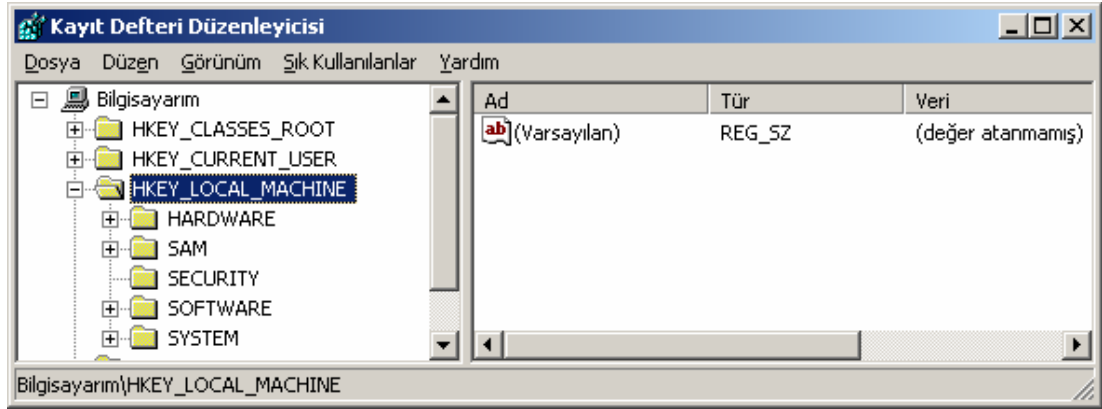
Hardware: Seri bağlantı noktaları ile bilgiler ve ayarları içerir.

Network: Kullanıcının o an bağlı bulunduğu ağ ya da ağlar üzerine bilgiler burada bulunur.

Security: Ağ güvenlik ayarlarına buradan ulaşılabilir.

Software: Yazılımlara has özel bilgiler ve ayarları içerir.

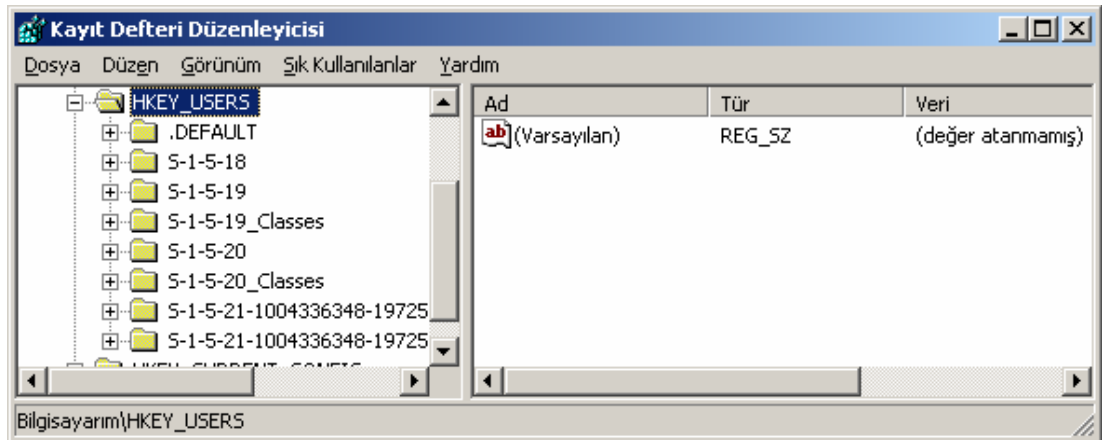
System: Sistem başlangıç ve aygıt sürücülere bilgileri ile işletim sistemi ayarları burada yer alır.



Şekil 2.19: HKEY_LOCAL_MACHINE

HKEY_USERS

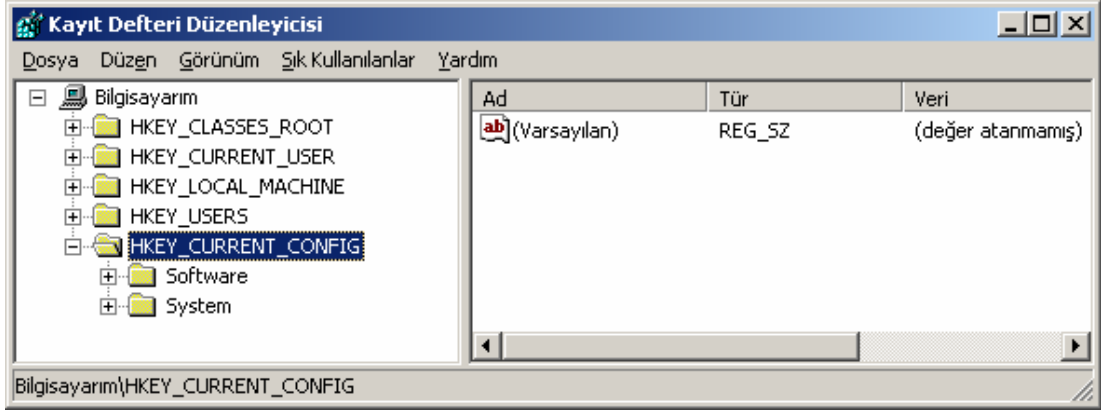
İşletim sistemlerine bağlanan her kullanıcı için masaüstü ve kullanıcı ayarlarını içerir. Bu başlık altında her kullanıcıya ait bir anahtar daha bulunur. Ancak sadece tek bir kullanıcı varsa, bu durumda sadece "default" altında tek anahtar olacaktır.



Şekil 2.20: HKEY_USERS

HKEY_CURRENT_CONFIG

HKEY_LOCAL_CONFIG ile bağlantılı olarak o anki donanım konfigürasyonu ile ilgili bilgileri içerir.



Şekil 2.21: HKEY_CURRENT_CONFIG

2.1.4.2. Kayıt Defteri Düzenleyicisinde Anahtar ve Değerleri Değiştirme İşlemleri

Bu bölümde Kayıt defteri kullanımı ile ilgili aşamaları bulacaksınız. Bu adımları kullanarak “Kayıt defteri düzenleyicisi”nde yapmak istediğiniz işlemleri kolaylıkla gerçekleştirebileceksiniz.

Bir dize, değer veya anahtarı bulmak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- **Düzen** menüsünden **Bul**'u tıklatınız.
- **Aranan** kutusuna bulmak istediğiniz dize, değer veya anahtarı yazınız.
- İsteddiğiniz arama türüyle eşleştirmek üzere **Anahtarlar**, **Değerler**, **Veri** ve **Sadece tüm dizeyi eşleştir** denetim kutularını seçip **Sonrakini Bul**'u tıklatınız.

Sık Kullanılanlar'a kayıt anahtarı eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- **Sık Kullanılanlar**'a eklemek istediğiniz kayıt anahtarını seçiniz.
- **Sık Kullanılanlar** menüsündeki **Sık Kullanılanlara Ekle** seçeneğini tıklatınız.
- **Sık Kullanılanlara Ekle** iletişim kutusunda, varsayılan kayıt anahtarı adını kabul ediniz veya yeni bir ad yazınız.
- Kayıt anahtarı **Sık Kullanılanlar** listesine eklenir. **Sık Kullanılanlar** menüsünden seçerek bu listeye geri dönebilirsiniz.

Anahtar eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Kayıt defteri ağacında (solda), altına yeni anahtar eklemek istediğiniz kayıt defteri anahtarını tıklatınız
- **Düzen** menüsünde, **Yeni**'yi işaretleyiniz, sonra da **Anahtar**'ı tıklatınız.
- Yeni anahtar için bir ad yazınız ve sonra ENTER tuşuna basınız.

Değer eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Yeni değeri eklemek istediğiniz anahtarı veya girdiyi tıklatınız.
- **Düzen** menüsünde, **Yeni**'yi işaretleyin, sonra da eklemek istediğiniz değer türünü tıklatınız: **Dize Değeri**, **İkili Değer**, **DWORD Değeri**, **Birden Çok Dize Değeri** veya **Genişletilebilir Dize Değeri**.
- Yeni değer için bir ad yazıp ENTER tuşuna basınız.

Değer değiştirmek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Değiştirmek istediğiniz girdiyi seçiniz.
- **Düzen** menüsünde **Değiştir**'i tıklatınız.
- **Değer verileri**'ne, değere ilişkin yeni veriyi yazıp **Tamam**'ı tıklatınız.

Anahtar veya değer silmek için:

- Kayıt Defteri Düzenleyicisi'ni açınız
- Silmek istediğiniz anahtarı veya girdiyi tıklatınız.
- **Düzen** menüsünde **Sil**'i tıklatınız.

Anahtarı veya değeri yeniden adlandırmak için:

- Kayıt Defteri Düzenleyicisi'ni açınız
- Yeniden adlandırmak istediğiniz anahtarı veya girdiyi tıklatınız.
- **Düzen** menüsünde **Yeniden Adlandır**'ı tıklatınız.
- Yeni adı yazınız ve sonra ENTER tuşuna basınız.

Kayıt defterine ağ üzerinden bağlanmak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- **Dosya** menüsünde **Ağ Kaydına Bağlan**'ı tıklatınız.
- **Ağ Kaydına Bağlan** iletişim kutusunda, kayıt defterine bağlanmak istediğiniz bilgisayarın adını yazınız.

Ağ kayıt defteriyle bağlantıyı kesmek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- **Dosya** menüsünde **Ağ Kaydı Bağlantısını Kes**'i tıklatınız.
- **Ağ Kaydı Bağlantısını Kes** iletişim kutusunda, kayıt defteriyle bağlantıyı kesmek istediğiniz bilgisayarın adını yazın.

Kayıt anahtarı adını kopyalamak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Kayıt defteri ağacında (Solda) bir kayıt defteri anahtarını tıklatınız.
- **Düzen** menüsünde **Anahtar Adı Kopyala**'yı tıklatınız.
- Kayıt defteri anahtar adını başka bir programa veya belgeye yapıştırınız.

Kayıt defterini geri yüklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- **Başlat**'ı ve sonra **Oturumu Kapat**'ı tıklatınız.
- Listede **Yeniden Başlat**'ı tıklatıp, daha sonra **Tamam**'ı tıklatınız.
- **Lütfen, başlatılacak işletim sistemini seçin** iletisini gördüğünüzde F8'e basınız.
- **En Yeni İyi Yapılandırma** seçeneğini vurgulamak için ok tuşlarını kullanınız ve ENTER'a basınız.

Bir işletim sistemini seçmek için ok tuşlarını kullanınız ve ENTER'a basınız.

En Yeni İyi Yapılandırma seçeneğini belirlerseniz, donanımınızla uyumsuz yeni bir sürücü eklediğinizde ortaya çıkabilecek sorunları rahatça giderebilirsiniz. Ancak, bu seçenek bozuk veya eksik sürücü veya dosyalar sonucunda ortaya çıkan sorunları çözemez.

En Yeni İyi Yapılandırma seçeneğini belirlediğinizde, Windows yalnızca HKLM\System\CurrentControlSet kayıt anahtarındaki bilgileri yeniden yükler. Diğer kayıt anahtarlarında yaptığımız değişiklikler aynen kalır.

Kayıt defterine yığın eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Kayıt defteri ağacında (Solda), HKEY_USERS veya HKEY_LOCAL_MACHINE anahtarlarını tıklatınız.
- **Dosya** menüsünde **Yığın Ekle**'yi tıklatınız.
- **Konum**'da, yüklemek istediğiniz yığını içeren sürücü, klasör veya ağ bilgisayarı ve klasörü tıklatınız.
- Aç'ı tıklatınız.
- Anahtar Adı kutusuna, yığma atamak istediğiniz adı yazıp Tamam'ı tıklatınız.

Yığın nedir? : Kayıt defterinin sabit diskinizde dosya olarak gözüken bölümü, kayıt defteri alt ağacı yığın denen bölümlere ayrılmıştır. Bir yığın, kayıt defteri sıradüzeninin tepesinde yer alan anahtarlar, alt anahtarlar ve değerler grubudur. Yığın dosyalarının çoğu “ systemroot\System32\Config “ klasöründe de depolanır. Bir yığın bir dosya olduğundan bir bilgisayardan başka bir bilgisayara taşınabilir. Düzenlemek için kayıt denetleyicisini kullanmak gerekir.

Kayıt defterinden yığın kaldırmak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Sisteminize önceden yüklemiş olduğunuz bir yığını seçiniz
- **Dosya** menüsünde **Yığını Kaldır**'ı tıklatınız.

NOT: Yığını Yükle ve Yığını Kaldır yalnızca HKEY_USERS ve HKEY_LOCAL_MACHINE anahtarlarını etkiler ve sadece bu önceden tanımlı anahtarlar seçildiğinde etkin olurlar. Kayıt defterine bir yığın yüklediğinizde, yığın bu anahtarlardan birinin alt anahtarı olur

2.1.4.3. Kayıt Defteri Güvenliğini Koruma

Kayıt defteri anahtarına izin atamak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- İzin atamak istediğiniz anahtarı tıklatınız.
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- Seçilen anahtara erişim düzeyini aşağıdaki biçimde atayınız.

- Kullanıcıya anahtar içeriğini okuma izni vermek, ancak dosya da yapılan değişiklikleri kaydetmesini önlemek üzere, *ad* için, **Okuma** için İzinler'in altında, **İzin Ver** onay kutusunu seçiniz.
- Kullanıcıya seçilen anahtarı açma, düzenleme ve sahiplenme izni vermek üzere, *ad* için İzinler'in altında, **Tam Denetim** için, **İzin Ver** onay kutusunu seçiniz.
- Seçilen anahtarda kullanıcıya özel izin vermek için **Gelişmiş**'i tıklatınız.

Not: Özel İzinler onay kutuları, bu anahtar için özel izinlerin ayarlanıp ayarlanmadığını gösterir, ancak bu onay kutularını tıklatarak özel izinler ayarlayamazsınız. Özel izinler ayarlamak için **Gelişmiş**'i tıklayınız.

Kayıt defteri anahtarına özel erişim atamak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Özel erişim atamak istediğiniz anahtarı tıklatınız.
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- **Gelişmiş**'i tıklatın, sonra da özel erişim atamak istediğiniz kullanıcı veya gurubu çift tıklatınız.
- **İzinler** altında izin vermek veya engellemek istediğiniz her izin için **İzin Ver** veya **Reddet** onay kutusunu seçiniz.

İzinler listesine kullanıcı veya grup eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- İzinler listesini değiştirmek istediğiniz anahtarı tıklatınız.
- **Düzen** menüsünde **İzinler**'i, sonra da **Ekle**'yi tıklatınız.
- **Kullanıcıları, Bilgisayarları veya Grupları Seç** iletişim kutusunda, **Konumlar**'dan görüntülemek istediğiniz kullanıcı veya grupların bilgisayarlarını veya etki alanını tıklatınız.
- Kullanıcı veya grup adını tıklatın, **Ekle**'yi, ardından da **Tamam**'i tıklatınız.
- **İzinler** iletişim kutusunda, *ad* için **İzinler** altında, seçilen kullanıcı veya gruba aşağıdaki şekilde bir erişim türü atayınız.
 - Kullanıcıya anahtar içeriklerini okuma izni vermek, ancak üzerinde yapılan değişiklikleri kaydetmesini önlemek için **İzin Ver** onay kutusunda **Okuma**'yı seçiniz.
 - Kullanıcıya seçilen anahtarı açma, düzenleme ve sahiplenme izni vermek için, **İzin Ver** onay kutusunda **Tam Denetim**'i seçiniz.

Kayıt defteri anahtarı Tam Denetim izni vermek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Tam Denetim izni vermek istediğiniz anahtarı tıklatınız
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- **Grup veya kullanıcı adları** altında, kayıt defteri anahtarınızın Tam Denetim iznini vermek istediğiniz kullanıcıyı tıklatınız.
- *ad* için **İzinler**'in altında (Burada *ad*, anahtarın tam denetimini verdiğiniz kullanıcının adını temsil eder.), **Tam Denetim** için **İzin Ver** onay kutusunu seçiniz.

Kayıt defteri anahtarındaki etkinliği denetlemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Denetlemek istediğiniz anahtarını tıklatınız.
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- **Gelişmiş**'i, sonra da **Denetim** sekmesini tıklatınız.
- Grup veya kullanıcı adını çift tıklatınız.
- Denetlemek istediğiniz veya denetimi durdurmak istediğiniz etkinlikler için **Erişim** altında **Başarılı** ve **Başarısız** onay kutularını seçin veya temizleyiniz.

Seç	Denetlenecek olay
Değeri Sorgula	Kayıt defteri anahtarından girdi okuma girişimleri
Değer Ata	Kayıt defteri anahtarında girdi ayarlama girişimleri
AltAnahtar Oluştur	Seçilen kayıt defteri anahtarından alt anahtarlar oluşturma girişimleri
AltAnahtarları Sırala	Kayıt defteri anahtarının alt anahtarlarını belirleme girişimleri
Bildir	Kayıt defterindeki bir anahtardan bildirim olayları
Bağlantı Oluştur	Belirli bir anahtarda sembolik bağlantı oluşturma girişimleri
Sil	Bir kayıt nesnesini silmek için girişimler
DAC Yaz	Anahtardaki denetim listesine isteğe bağlı erişim yazma girişimleri
Sahip Yaz	Seçilen anahtarın sahibini değiştirme girişimleri.
Okuma Denetimi	Bir anahtardaki denetim listesinde isteğe bağlı erişim açma girişimleri

Tablo 2.4: Kayıt defteri anahtarındaki etkinliği denetleme

Denetim listesine kullanıcı veya grup eklemek için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Denetlemek istediğiniz anahtarını tıklatınız.
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- **Gelişmiş**'i, sonra **Denetim** sekmesini, ardından da **Ekle**'yi tıklatınız.
- **Nesne Türleri**'ni tıklatınız, bulmak istediğiniz kullanıcıların veya grupların tür veya türlerini seçiniz ve daha sonra **Tamam**'ı tıklatınız.
- **Konular**'ı tıklatın, görüntülemek istediğiniz kullanıcıların veya grupların bilgisayarını veya etki alanını seçip, daha sonra **Tamam**'ı tıklatınız.
- Eklemek istediğiniz kullanıcı veya grubun adını yazıp, daha sonra **Denetim Girdisi** iletişim kutusunu açmak için **Tamam**'ı tıklatınız veya ayarladığınız parametreleri esas alan bir kullanıcı, bilgisayar veya grup aramak için **Gelişmiş**'i tıklatınız.

Kayıt defteri anahtarının sahipliğini almak için:

- Kayıt Defteri Düzenleyicisi'ni açınız.
- Sahipliğini almak istediğiniz anahtarı tıklatınız.
- **Düzen** menüsünde **İzinler**'i tıklatınız.
- **Gelişmiş** butonunu, sonra da **Sahip** sekmesini tıklatınız.
- **Yeni sahibi** altında, yeni sahibi, sonra da **Tamam**'ı tıklatınız

2.2. Kullanıcı Sorumlulukları

Bir bilgisayar kullanıcısının sistemin uygun bir biçimde çalışmasını sağlamak için yapabileceği birkaç şey vardır. Sistem yardımcıları performansı aşağıdaki yollarla artırabilir:

- Uygulamaları yönetmek
- Dosya ve klasörleri yönetmek
- Çalışmanızı yedeklemek

2.2.1. Uygulamaları Yönetmek

Uygulamaları yüklerken, Ekle/Kaldır Programları yardımcılarını kullanınız. Bazı uygulamalar bir yükleme koruması kullanmaz ve kur programı kurulumun tam ortasında arızalanırsa, sistemin hata vermesine yol açabilir. Bir uygulamayı sistemden çıkarmak için, Ekle/Kaldır Programları yardımcıları da kullanılabilir.

2.2.2. Dosya ve Klasörleri Yönetmek

Bir işletim sisteminin dosya yönetimi sistemi, veriyi hiyerarşik bir ağaçta tutmak için tasarlanmıştır. Disk sürücülerinin farklı yerlerde bulunan çalışma dosyaları ve programları ile düzenlenmeleri gerekir. Bu, dosya bulmayı ve yedeklemeyi kolaylaştırır.

2.2.3. Çalışmanızı Yedeklemek

Bir sistem her an hata verebileceğinden, kişisel dosyaların düzenli olarak yedeklenmesi gerekir. Veri yedeklemenin en iyi yolu, onu disket, CD veya Zip disk gibi bir çeşit çıkarılabilir ortama kopyalamaktır. Bir yangın durumunda, verinin tamamının kaybedilmesini önlemek için, ortamın, tercihen başka bir binada olmak üzere, bilgisayardan uzak bir yerde saklanması gerekir. Aynı diski tekrar tekrar kullanmayınız. Çoklu diskler kullanınız ve aynı verinin çoklu kopyalarını oluşturunuz.

2.3. Anti-Virüs Uygulamaları

2.3.1. Bilgisayar Virüsü Nedir?

Virüs, herhangi bir bilgisayara değişik yollarla girebilen ve bu bilgisayarlarda istenmeyen sonuç ve zararlara yol açan programlara verilen genel bir isimdir. Bu programların kullandığımız, bilgisayarlarda çalıştırdığımız diğer programlardan temelde bir farkı yoktur. Bu nedenle, işletim sisteminin desteklediği bütün işleri yapabilirler. Virüsleri özel kılan, girdiği sistemlere kendilerini, kullanıcının farkında olmadan veya iradesi dışında çalıştırılacağı şekilde yerleştirmesi ve sistemlere zarar vermesidir.

Bir virüs kullanıcı tarafından çalıştırılmadan veya kendisini programlayan kişi tarafından önceden belirlenmiş durum oluşmadan aktif hale gelmez. Bazı virüsler ise aktif hale geldikleri halde, belli bir süre istenmeyen etkilerini göstermezler. Virüsler genel olarak etkilerini diğer çalışan programlara "bulaşarak", onlarda çeşitli değişiklikler yaparak gösterir. Virüslerin bir diğer özelliği ise kendilerini çoğaltmaları ve hafızada değişik yerlere kaydetmeleridir. Virüsler, disketler, ağ paylaşımı, Internet (e-mail, dosya indirme, vs.) yollarıyla yayılır.

Virüslerin etkileri sadece rahatsızlık veren küçük problemler olabildiği gibi (Ekranınıza rahatsızlık veren mesajlar çıkararak çalışmanızı bölmesi/engellemesi vb.) bilgisayarınızın hafızasını ve/veya disk alanını kullanarak bu kaynaklara verimli olarak erişiminizi engellemeleri ya da kullandığımız dosyaların içeriklerini bozmaları/silmeleri gibi oldukça zararlı etkileri de olabilir. Örneğin "CIH"(Çernobil) virüsü bir versiyonu her 26 Nisan' da aktif hale gelerek bilgisayarın "bios" unu siler. Sadece hard diskteki dosyaları kullanılmaz hale getirebildiği gibi bilgisayarı tekrar açılmayacak şekilde de zarar verebilir.

Bunun dışında, kullandığımız bilgisayar programlarını bozabilir, çalışmalarını yavaşlatabilir, sabit diskinizin tamamını ya da önemli dosyaların olduğu kısımlarını silebilirler. Bazı virüsler ise kullanıcının bilgisayar konusundaki bilgisizliğini kullanarak yol açmadığı zararları vermiş gibi görünerek panik yaratırlar.

Bilgisayar virüsleri ile biyolojik virüsler karşılaştırıldıklarında şaşılacak derecede benzerlikler görülür. Bu karşılaştırma neticesinde bilgisayar virüsleri daha iyi anlaşılacaktır.

Biyolojik Virüsler	Bilgisayar Virüsleri
İnsanların bazı özel hücrelerine bulaşır.	Bazı dosyalara (*.exe , *.com) dosyalarına bulaşır.
Hücrenin genetik yapısını değiştirir.	Programın özelliklerini değiştirir. Program önceden yaptığı şeylerin yanında, virüsün istediği şeyleri de yapar.
Bulaşılan hücrelerde yeni virüsler ürer.	Virüsün bulaştığı program yeni virüsler üretir.
Bir hücreye aynı virüs sadece bir kez bulaşır.	Genelde virüsler bir programa sadece 1 kez bulaşır.
Virüsün bulaştığı canlıda, uzun müddet hastalık işaretleri gözükmez.	Virüs bulaşmış program uzun süre normal çalışabilir.
Virüs, rastladığı bütün hücrelere bulaşmaz	Programlara bazı virüslere karşı bağışıklık kazandırılabilir.
Virüs kendi yapısını değiştirerek başka bir şekle girebilir.	Virüs programları, kendilerini değiştirerek virüs arayan programlardan korunabilirler

Tablo 2.5: Bilgisayar Virüsleriyle Biyolojik Virüslerin Benzerlikleri

2.3.1.1. Virüslerin Bulaşma Yöntemleri

Geçmişten bu güne en yaygın şekilde virüs bulaşma yöntemleri sırası ile:

- Disket, CD
- E-posta
- Ağ paylaşımı
- İnternet'ten indirilen programlar olarak görünmektedir. Bunlar içinde günümüzde en yaygın olan, e-posta ve İnternet'ten indirilen dosyalar üzerinden bulaşma yöntemleri üstünde biraz daha durmakta yarar var:

• E-posta ile Virüs Bulaşması

E-posta ile virüs bulaşması, e-postaların çalıştırılabilir eklentileri sayesinde olur. Virüsün aktif hale gelmesi için eklentileri açmamak her zaman bir koruma sağlamaz. Bazı e-posta okuyucu programlar belli formattaki eklentileri otomatik olarak çalıştırır. Bu sayede virüs kullanıcıdan habersiz bilgisayara girip programın gereği olan işlemleri yapabilir (Örnek: Outlook / Outlook Express – Bubbleboy). Gerekli işletim sistemi güncellemeleri yapıldıktan sonra virüs bu tür açıklardan yararlanıp kullanıcıdan habersiz bulaşma şansını yitirmektedir. Bu habersiz bulaşma yapısı aslında e-posta ile virüs bulaşma konusunun sadece ufak bir bölümüdür. Esas kısmı kullanıcının sistem tarafından çalıştırılabilir dosyaları (.bat, .exe, .scr, .pif, vb.) e-posta ile alması ve onu bilgisayarına çekmeden ya da çekerek çalıştırması ile sisteme virüs bulaştırmasıdır. Bu şekilde, kullanıcının bireysel hatasından kaynaklanarak sisteme virüs bulaşması daha sıklıkla karşılaşılan bir durumdur.

- **WWW'den Virüs Bulaşması**

WWW'den virüs bulaşması İnternette indirilen dosyalarla olmaktadır. Bu konuyu da yine kullanıcının bilinçli olarak indirdiği dosyalar ve kullandığı web-tarayıcısının (Internet Explorer, Netscape vs.) otomatik olarak indirdiği dosyalar ile virüs bulaşması diye ikiye ayırabiliriz.

Birinci durumda kullanıcı bilinçli olarak İnternette bir dosyayı bilgisayarına çeker ve o dosya içeriğinde virüs varsa çalıştırdığında sisteme virüs bulaşır. Bunu engellemenin yolu kullanıcıların bilinçlenmesidir.

İkinci durum ise biraz daha karmaşık. Bu kısmı da ikiye ayırmak gerekmektedir:

- Java-Script
- ActiveX kullanarak görüntülenen www sayfalarından virüsün bulaşması.

Java Script: Java apletler sayesinde www sayfaları etkileşimli hale gelmiştir (Ufak animasyonlar, vb.). Günümüzde tüm web tarayıcıları Java'yı desteklemektedir. Burada yaşanan sorun, bahsedilen apletlerin güvenilir olmayan sitelerden de indirilebilmesinden kaynaklanmaktadır. Bunun için "sandbox" adında bir teknoloji ile güvenlik önlemi alınmıştır. Sandbox tarafından çalıştırılan aplet bilgisayardaki dosyaları ne okunabilir ne de yazılabilir. Buraya kadar anlatılanlar bu sistemin güvenli olduğu izlenimini veriyor. Ama sorun sandbox teknolojisinin karmaşık yapısından dolayı meydana gelmektedir. Bazen gözden kaçırılmış bir açık sayesinde virüsler bilgisayarda kod çalıştırabilir. Örnek olarak birçok gizli pencere açıp sistemin kaynaklarını tüketebiliyor.

ActiveX: Windows apletleridir. "web" sayfalarındaki animasyonları vb. göstermek için kullanılan bir yapıdır. Bilgisayara ".dll" (Dynamic Link Library) uzantısında dosyalar indirirler. Bu dosyaların sistemde her türlü yetkiye sahip olması, virüse en kolay ve en güçlü şekilde sisteme hakim olma şansı tanır. MS Internet Explorer'ın çok sayıda güvenlik güncellemesi bu nedenle yazılmıştır. Yapıdaki güvenlik sistemi "Authenticode system and Code Signing" olarak adlandırılır. Web sayfalarından DLL indirirken güvenli olarak tanımlanmış olması esasına dayanır. Ancak kullanılan www tarayıcısının ayarları en güvensiz seviyedeyse otomatik olarak sitedeki ".dll" uzantılı dosyayı bilgisayara indirir. Bu dosya "command.com" dahil bir çok komutu çalıştırma yetkisine sahiptir. Tedbir olarak "MS Internet Explorer" ayarlarındaki güvenlik seviyesinin en azından "Medium" olarak ayarlanması gerekir.

2.3.1.2. Bilgisayara Virüs Bulaştığı Nasıl Anlaşılır ve Nasıl Temizlenir

Eğer elinizde anti-virüs yazılımı yoksa bilgisayarınızda virüs olduğunu; ancak (Çoğunlukla) virüs etkisini gösterdikten sonra anlayabilirsiniz. Nadiren, dosya adı sabit ve bilinen virüsleri dosya adıyla tarayarak bulmak ve silmek çözüm olabilir.

Bir virüsün etkileri; bilgisayarda anormal yavaşlama, Windows uygulamalarında beklenmeyen hata mesajları (application error, system fault, missing files vs.), bilgisayarın kilitlenmesi, rastgele DOS işletim sistemine dönmesi, normalde açılan dosyaların açılmaması, anormal sesler/görsel davranışlar ya da bilgisayarınızın isteğiniz dışında işlemler yapmaya başlaması şeklinde kendini gösterebilir.

Bu durumda yapılacak şey, bir anti-virüs programı kullanarak bilgisayarın virüsten temizlenmesidir. Ancak virüsün bilgisayara önemli hasarlar vermiş olduğu durumlarda, virüsten temizleme işlemi her zaman başarılı olmayabilir.

Bilgisayarınızda anti-virüs yazılımı olmadığı durumlarda, bu yazılıma sahip bir bilgisayarda daha önceden hazırlanmış olan acil durum disketi ile diskinizde ve disketlerinizde virüs taraması yapabilirsiniz.

Anti-virüs yazılımlarının tarama işlemi sonrasında virüs bulamaması bilgisayarda virüs olmadığını değil; sadece tarama işleminde kullanılan anti-virüs programlarının tanıdığı virüslerin mevcut olmadığını gösterir.

Kullanılan anti-virüs yazılımlarının buldukları virüsleri silmeleri veya bulaştıkları dosyalardan temizlemeleri mümkün olmaması da zaman zaman karşılaşılan bir durumdur. Yani, kullanılan anti-virüs programının tanımadığı bir virüsün bilgisayarınıza bulaşmış olması ihtimali her zaman vardır.

2.3.1.3. Bilgisayar Virüslerinin Ortak Özellikleri

- ".exe", ".com" gibi dosyalara bulaşırlar.
- Virüsler kendini otomatik olarak kopyalar.
- Bu programlar kullanıcı müdahalesine gerek kalmadan kendi kendine çalışacak şekilde sabit diske kaydeder.
- Virüsün bulaştığı program kendi kendine yeni virüsler üretir.
- Virüsler programların özelliklerini değiştirirler.
- Çoğu kez görüldüğü kadarıyla virüsler bir programa sadece bir kez bulaşırlar.
- Virüsün bulaştığı program uzun süre normal çalışır.
- Virüslerin bulaştıkları programlar önceden yaptığı şeylerin yanında virüsün istediği şeyleri de yapar.
- Kullanıcı bilgisayarına ve sabit diskine zarar verirler.
- Programlara bazı virüslere karşı bağışıklılık kazandırılabilir.
- Virüsler devamlarını sağlamak için bazı önlemler alırlar. Bu önlemlerin başında da Anti-Virüs Programları tarafından fark edilmemek için bilgisayar sisteminde gözükmemeye çalışırlar. Çoğu virüsün tekniği iyi gizlenmektir. Bu yüzden virüs kodları çok kısa olur. Ayrıca virüs programları, kendilerini değiştirerek virüs arayan programlardan korunabilirler.

2.3.1.4. Bilgisayarlar Virüslere Karşı Nasıl Korunur

Bilgisayarlar virüslerden çeşitli acil durum disketleri, virüslere özel programlarla temizlense de, değişik virüslere karşı, bu virüsler bilgisayara bulaşmadan önce önlem almak ve baştan koruma sağlamak için McAfee Anti-Virüs, Norton AntiVirüs, F-Prot, Dr. Solomon's Anti-Virus Toolkits vb. gibi antivirüs programları, henüz herhangi bir virüs sorunu ile karşılaşmadan kurulması gerekir.

Bu programlar bilgisayara, bir virüsün kopyalanması veya bilgisayarda aktif hale gelmesi söz konusu olduğunda kullanıcıyı uyarmakta ve onu etkisiz hale getirir.

Birçok anti-virüs yazılımı yeni çıkan virüslere karşı, tarama motorlarını ve virüs tanım dosyalarını güncellemek için yeni dat (Virüs tanım dosyaları) ve superdat (Virüs tarama motorları) dosyalarını Internet üzerinden kullanıcılarının hizmetine sunmaktadır. Bu sayede anti-virüs yazılımları yeni virüse karşı bağışıklık kazanmakta ve virüs bilgisayara kopyalandığında veya aktif hale geldiğinde kullanıcıyı uyarmakta ve virüsü etkisiz hale getirmektedir. Bu güncelleme virüs bilgisayara bulaştıktan sonra da işe yarayabilir. Tespit edilen virüs silinmekte ve böylece sistemde yaptığı değişiklikler düzeltilebilmektedir. Ancak güncellemeden önce meydana gelmiş veri kayıplarını gidermek muhtemelen mümkün olmayacaktır.

Eğer herhangi bir anti-virüs yazılımı olmayan bir bilgisayarda virüs sorunu varsa önce güncellemesi yapılmış bir anti-virüs programı (Başka bir bilgisayarda) ile oluşturulan acil durum disketi ile sorunlu bilgisayar açılarak virüsler temizlenir ve daha sonra virüs programı kurulur.

2.3.1.5. Virüsler Nereye Ne Yazar

İlk açılışta çalışmak için genellikle "Windows Registry" (kayıt) ayarlarını değiştirir. Burada, aşağıdaki konumlara kendi program adlarını yazarak açılışta başlamalarını sağlamaktadırlar.

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\

- RunServices
- RunServicesOnce
- Run
- RunOnce

HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\

- Run
- RunOnce
- RunServices

2.3.1.6. Virüs Çeşitleri

Açılış "BOOT" Sektörü Virüsleri: Boot sector virüsleri disklerin açılış sektörüne yerleşir ve bilgisayar açılınca etkinleşir. Bilgisayarın yeniden açılması (reset) ile silinmezler.

Komut İşleyicisi Virüsler: İşletim sistemi dosyalarına bulaşır ve bu dosyalara girdikten sonra kolaylıkla yayılırlar. Özellikle COMMAND.COM dosyasını hedef alırlar.

Genel Amaçlı Virüsler: Kolayca farklı dosya türlerine bulaşabilirler. Alt dosyalar yerine genel amaçlı sistem dosyalarına ve BOOT (açılış) sektörüne yerleşirler.

Çok Amaçlı Virüsler: Açılış sektörü, komut işleyicisi ve genel amaçlı virüslerin en güçlü özelliklerine sahiptir. Bir dosya dan diğerine bulaşmak için birden fazla yol ve teknik kullanırlar.

Kütük Tipi Virüsler : İşletilebilir dosyalar (.com,.exe,.bat)' a bulaşarak yayılırlar. Bellekte yerleşik kalan ve kalmayan tipleri vardır. Bellekte yerleşik duran virüsler bulaştıkları bir dosyanın çalıştırılması ile belleğe yerleşerek diğer program dosyalarına bulaşır.

Makro Virüsleri: Herkes Makro virüslerinin zararlarını duymuştur ve zararlarını az çok bilmektedir. Aslında makrolar Word veya Excel'de bazı işleri otomatikleştirmek için yapılmışlardır. Yapısı aynen Visual BASIC'e benzer.

Makro virüslerine örnek olarak , Melissa virüsünü gösterebiliriz.. E-mail yoluyla bilgisayara bulaşır. E-mail açıldığında bilgisayarda bir değişiklik olmaz. E-mail ile birlikte list.doc adında bir ek vardır. Bu ek açıldığında virüs bilgisayara geçer ve adres defterindeki ilk 50 kişiye kendisini ekleyerek e-mail gönderir. Melissa virüsü bilgisayara bulaştıktan sonra her yılın 26 Mart'ında saat 3:36' da ekranda şöyle bir mesaj çıkarıyor.

"22 puan artı üçlü kelime puanı artı 50 puanda bütün harfleri kullandığım için Oyun bitti. Ben de buradayım işte."

Mantık Bombaları: Mantık bombaları programcı tarafından belirli bir görevi gerçekleştirmek için programlar içine yerleştirilen özel programlara verilen addır. Mantık bombaları kendilerine programcılar tarafından özel bir rol verilmiş programlardır.

Yerleştirilen programın görevi; programcı tarafından belirlenen bir olayın gerçekleşmesidir. Mantık bombası sisteme yerleştirildikten sonra belirlenmiş bir tarihte patlayabilir. O zamana kadar kendini belli etmez. Patladıktan sonra ise bütün program ve veriler silindiği için kimse bu bombayı kimin yerleştirdiğini bilemez.

Mantık bombaları, program üreten şirketler tarafından da kullanılabilir. Bu programlara "anti-kopya" programı denir. Program üreten şirketler bu sayede programların kopyalanmasını engellemeye çalışır. Bunun için kendi disklerinin bazı bölümlerini, DOS işletim sisteminde yer alan DISKCOPY tarafından kopyalanamaz hale getirirler. Orijinal

disklerde bulunan programlarda ise mantık bombaları saklanır. Bunların ateşleme mekanizmasında bulunan prosedürler, DISKCOPY programının okuyamadığı bölümlerdeki bilgileri okumaya çalışır. Eğer bu işlemde hata olursa, o zaman program müsaadesiz kopyalanmış bir disk olduğu kararını verir ve ateşleme sistemini çalıştırır. Böylece o diskteki program çalıştırılmaz.

Bilgisayar kurtları (Worm) : Bilgisayar kurdu, bilgisayardaki hafızada yerini değiştirebilen bunu yaparken de sistem tarafından işlenilmeye devam eden programlara denir. Program şöyle bir yol izler;

- RAM' da yeni bir alan bul.
- Kendini bu alana kopyala.
- Yeni kopyayı çalıştır.

Programın çalıştırılmasıyla kısır döngü başlamıştır. Devamlı olarak ilk başlatılan programın kopyası üretilmekte sonrada bu kopyalar çalıştırılmaktadır. Ta ki; hafızada yer kalmayınca kadar.

Trojanlar (Truva Atları) : Trojanlar internet yoluyla kullanıcı bilgisayarına girilmesini sağlayan programlardır. Virüsler den farklı olarak, trojanlar gözle görülür. Trojanların asıl amacı şifreleri ele geçirmektir (servis sağlayıcıların bağlantı şifresi gibi). Bu programlara trojan (Truva atı) denmesinin sebebi bir programın arkasına gizlenerek kullanıcıyı bir bakıma içeriden vurmasıdır.

Trojanların bilgisayara verebileceği zararları şöyle sıralayabiliriz;

- Çeşitli dosyaları silmek.
- Girdikleri sistemde yer alan dosyaları bir şekilde kendilerini bu sisteme kasıtlı olarak yerleştiren kişiye aktarmak.
- Dosyalarda değişiklik yapmak.
- Bazı özel programları kurmak.(Mesela bilgisayar ağına izinsiz girilebilmesini sağlayan bir program kurulabilir)
- Çeşitli virüsleri sisteme yerleştirmek.
- Başka Truva atları kurmak.

Truva atlarını kullanıcı bilgisayarına yollamak isteyen kişilerin deneyecekleri en pratik yol sizi “kandırmak” olacaktır. En basitinden , “Fotoğrafımı görmek ister misiniz? ” şeklindeki bir teklife şüphe ile bakmak gerekir. Kullanıcıya gelen “MyPhoto.exe” adı altındaki dosyaya tıkladığında programın çalışmadığı görülecektir. Aslında program çalışmıştır ve bilgisayarınıza bir davetsiz misafirin girmesine neden olmuştur. Bu problemler daha çok internette chat programları kullanırken oluşmaktadır.

Trojanlardan korunmak için aşağıda sayılan maddelere uyulduğu takdirde, trojanların sisteme girişi büyük ölçüde önlenir.

- Öncelikle çok iyi tanımadığınız kimselerin gönderdiği dosyaları kabul etmemek.
- Kişisel kullanıcılar ve sistem yöneticileri, makinelerinde kurulu bulunan her bir yazılımın güvenilir bir kaynaktan alındığına ve daha sonra üzerinde oynama yapılmadığına emin olmalıdır.
- Güncel Anti-Virüs programlarını kullanmak.
- Çoklu uzantısı olan dosyaları asla açmamak. Örneğin "prg.com.exe"

Bilgisayarlarda trojanların olup olmadığını tespit eden hazır programlar mevcuttur. Bu programlar yardımı ile de trojanlar tespit edilip bilgisayar sisteminden kolaylıkla kaldırılabilir.

2.3.2. Anti-Virüs Programları

Anti-virüs programları virüsleri tespit eden, virüs bulaşmış dosyaları temizleyen veya silen programlardır. Bazı anti-virüs programları trojanları da tespit edebilir. Trojanların virüslerden farkı gözle görülebilir olması ve normal bir dosya gibi silinebilir olmasıdır. Günümüzde birçok anti-virüs programı bulunmaktadır. Fakat en yaygın olanları;

- Norton Anti-Virüs
- McAfee Antivirus
- F-prot
- Panda Anti-Virüs Titanium
- AVP'dir.

Bu programlar içinde Norton Anti-virüs ile McAfee Antivirüs programları en çok ve sıklıkla kullanılan anti-virüs programlarıdır. Bu programlar bilgisayara kurulduğunda isteğe göre acil durumlar için disket oluşturulabilmekte, e-mail kontrolü yapılabilmekte ve kendini internet üzerinden güncelleştirebilmektedir.

2.3.2.1. Antivirüs Programlarının Yapıları

- **Scanners:** Virüsleri izlerine göre arayıp bulur ve imha eder. Güncelleme gerektiren bu tarama sistemi kullanıcı açısından en rahat ve kullanışlı olanıdır.
- **Checksummers:** Standart işletim sistemi dosyalarının boyut değişikliklerini virüs olarak yorumlar. Sistem dosyalarında yapılacak değişiklikleri iyi bilen bir kullanıcı için faydalı bir yapıdır.
- **Heuristics:** Virüslerin karakteristik yapısı bu programlarda genel hatlarıyla tanımlanır. Ancak son nesil virüsler burada kullanılan mantıkları çözümlenerek yazıldığından bazen yetersiz kalmaktadır.

2.3.2.2. Bir Anti-Virüs Yazılımı Alırken Nelere Dikkat Etmemiz Gerekir

Öncelikle bir Anti-Virüs programı otomatik güncelleştirmeye sahip olmalıdır. Bu sayede her gün çıkan yeni virüslere karşı otomatik olarak koruma altına alınmış olursunuz. Bunun dışında sürekli bir virüs bekçisine sahip olmalıdır. Bir e-mail alındığında şüpheli dosyanın hızlı bir şekilde taranması güvenliği artıracaktır. Tecrübesiz kullanıcılar için sihirbaz yol gösterici olmalıdır. Uzmanlar için ağ koruması ve yazılımın kişisel olarak ayarlanabilir olması da önemli bir özelliktir.

Karantina fonksiyonu şüpheli dosyaları öncelikle korumalı ve bunları bir klasörde toplayıp e-mail ile Anti-Virüs laboratuvarına göndermelidir. Boot edilebilir bir kurtarma diski (Rescue disk) vazgeçilmez bir ihtiyaçtır.

Kurtarma disketinin, Anti-Virüs yazılımı ile birlikte verilerek, kullanıcının kurtarma disketi yapmaya ihtiyaç duymaması sağlanmalıdır. Çünkü virüslü bir makinede bir kurtarma diski yapmak çok uzun sürebilir ve belki hiçbir şekilde yapılamaz. Çünkü yapacağınız disket te virüslü olacağından, yapılacak virüs taraması etkisiz olacaktır.

Düzenli güncellemeler ve destek hizmeti ideal bir koruma sağlar. Güncellemeler genellikle bir-iki haftada yenilenir. Bu dosyaları istediğiniz zaman internette indirebilirsiniz. İnternet bağlantısı olmayanlar ise ücretli telefon desteğinin yanında güncellemeleri de disket ya da CD üzerinde edinmek zorundadır. Diğer kullanıcılar her şeyden önce e-mail ile destek alabilir.

2.3.2.3. Virüslerin Tespiti

Antivirüs programları bilgisayara kurulduktan sonra aktif şekilde düzenli güncellemeleri yapıldığı sürece en etkili virüs tespiti yöntemidir. Ancak günümüzde daha farklı yaklaşımlar da olduğu için onlardan da bahsedilmelidir. Ardından antivirüs programlarının yapısından ve çalışma prensiplerinden bahsedilecektir.

2.3.2.4. Online Tarayıcılar

Antivirüs programına bütçe ayırmak istemeyen ve sürekli olmasa da bilgisayarında tarama yapmak isteyen kullanıcılar için antivirüs programları yazan şirketlerin sunduğu bir hizmettir. Bilgisayardaki tüm dosyaları uzaktan tarayan bir yapısı vardır. “Bilgisayardan bilgi alıyor mu?” konusunda sorular olsa da sonuçları başarılı sayılmaktadır.

Aşağıdaki bağlantılar izlenerek online virüs taraması yaptırılabilir:

- <http://www.symantec.com/avcenter> --> Check for Security Risk -->Scan for virus
- <http://www.mcafee.com> --> VirusScan Online

2.3.2.5. Antivirüs Programlarının Çalışma Yöntemi

Virüs pattern (virus örüntüsü) virüsü tanımlayan kısa “binary” koddur. Antivirüs programları bilgisayardaki tüm dosyalarda tarayıcısıyla virüs örüntüsünü arar. Virüsü bulduğunda; karşılaşılan durum için veritabanında tanımlanmış olan işlemleri yapar. Bu nedenle güncellenmiş bir antivirüs programı yeni çıkan virüslere karşı kullanıcının elindeki tek savunmadır

2.3.3. Symantec Antivirüs Programı

2.3.3.1. Symantec Antivirüs Programının Kurulumu

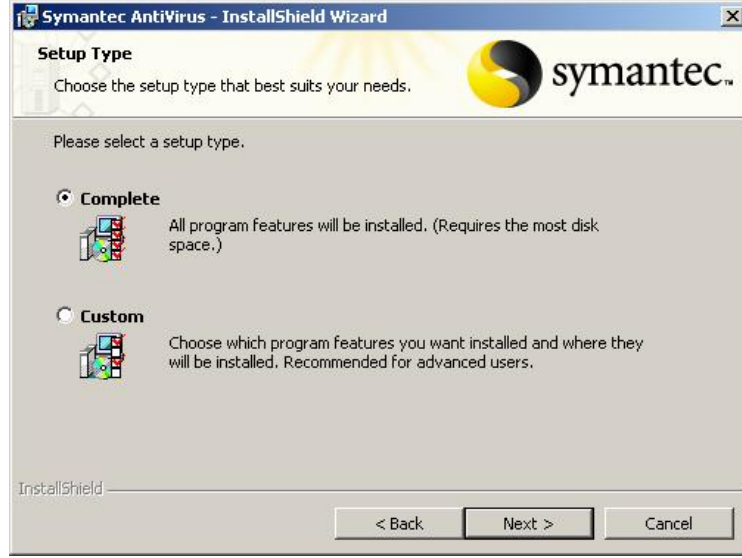
Symantec AV kurulmadan önce varsa bilgisayarda kurulu farklı antivirüs yazılımları kaldırılmalıdır. Aksi takdirde farklı antivirüs yazılımları birbirlerinin tanımlama dosyalarını virüs olarak görebileceğinden problem yaratabilir.

- "Welcome" penceresinde "Next" butonunu basılır.
- "License Agreement" penceresinde "I accept the terms in the license agreement" seçilir ve "Next" butonuna basılır.
- "Client Server Options" panelinde "Client Install" seçilerek "Next" butonuna basılır (Şekil 2.22).



Şekil 2.22: Client Server Options

- "Setup Type" penceresinde "Complete" seçilir ve "Next" butonuna basılır (Şekil 2.23).



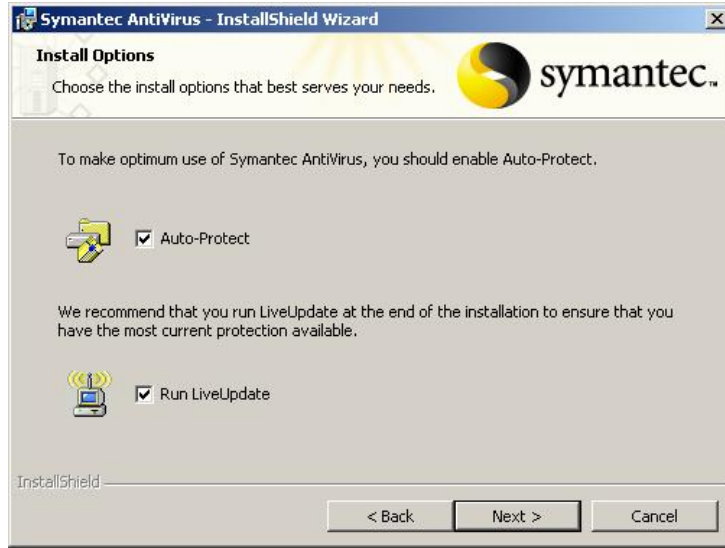
Şekil 2 23: Setup Type

- "Network Setup Type" penceresinde, bölüm/birim koordinatörü tarafından belirtilmiş "Symantec System Center" sunucusu (Merkezi virüs güncelleme sunucusu) yoksa "Unmanaged" seçilir ve "Next" butonuna basılır (Şekil 2.24).



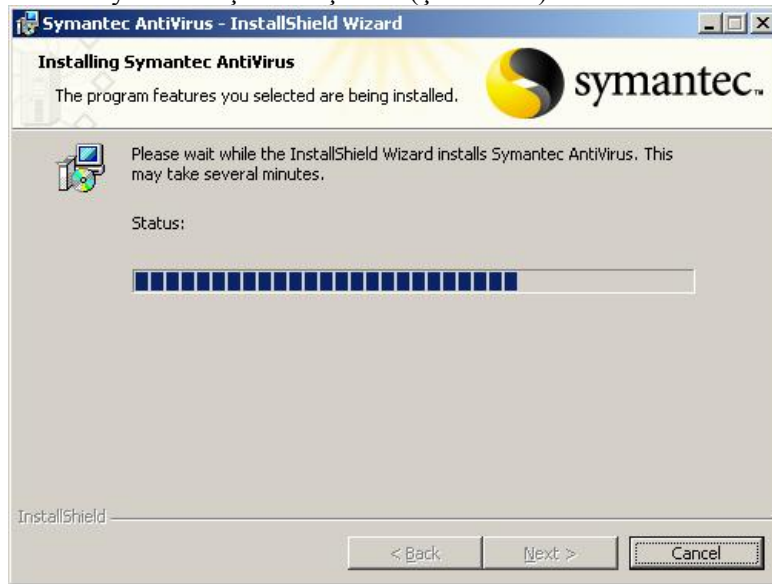
Şekil 2.24: Network Setup Type

- "Install Options" penceresinde bulunan "Auto-protect" seçeneği, kurulumdan sonra bilgisayarda çalıştırılan herhangi bir uygulamanın çalıştırılmadan önce antivirüs yazılımı tarafından kontrol edilmesini; "Run LiveUpdate" seçeneği, kurulum sonrasında antivirüs yazılımının güncellenmesini sağlar. Bu seçenekler varsayılan olarak seçilidir. Bu pencerede ki ayarlar değiştirilmeden "Next" butonuna basılır (Şekil 2.25).



Şekil 2.25: Install Options

- "Ready to Install the Program" penceresinde belirtilen özelliklerle Symantec AV yazılımının yüklenmeye hazır olduğu belirtilmektedir. "Next" butonuna basılarak yükleme işlemi başlatılır (Şekil 2.26).



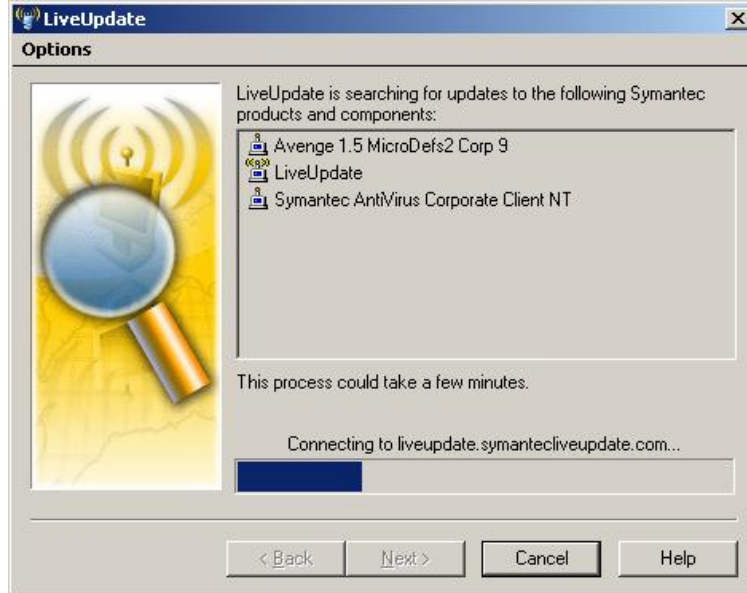
Şekil 2.26: Installation penceresi

- Yükleme işleminin bittiğini gösteren pencere "Finish" butonuna basılarak kapatılır.
- Kurulumun tamamlanmasının ardından LiveUpdate güncelleme paneli otomatik olarak açılır. Güncellemelerin yapılabilmesi için "Next" butonuna basılır (Şekil 2.27).



Şekil 2.28: - LiveUpdate

- Güncelleme işlemi, Internet üzerinden Şekil 2.29'da olduğu gibi yapılır. Virüs definition'lar yani yeni çıkmış olan virüsler antivirüs programına yüklenir.



Şekil 2.29: LiveUpdate bağlantısı

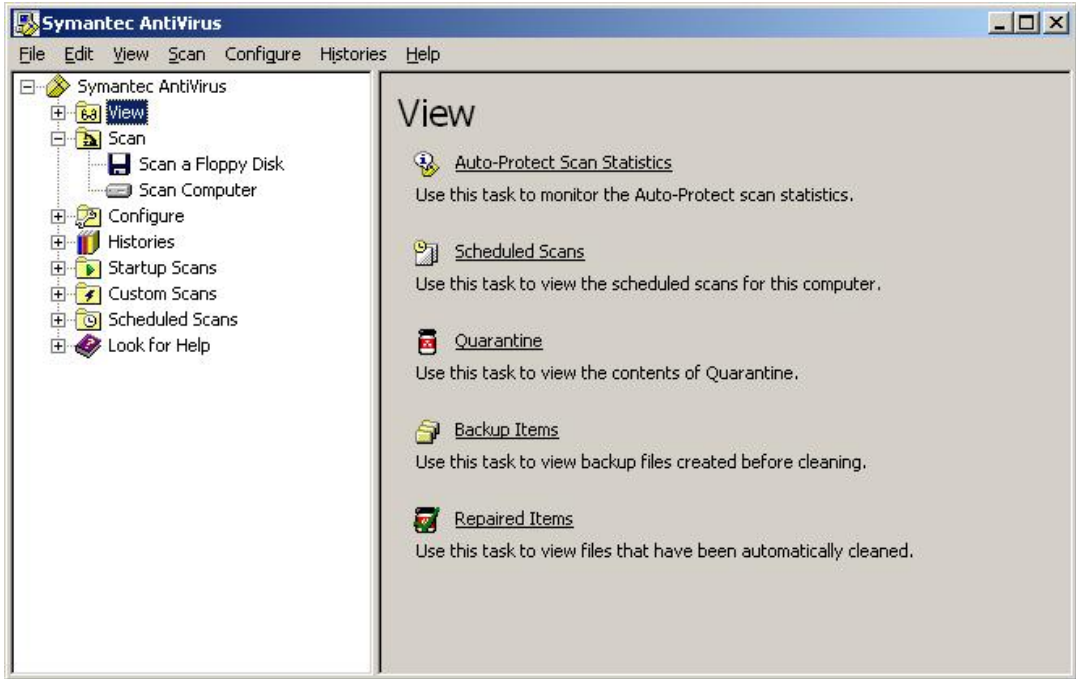
Güncelleme işlemi bittikten sonra "Finish" butonuna basılarak güncelleme bitirilir.

2.3.3.2. Symantec Antivirüs Program Ayarları

Bu kısımda Symantec AV yazılımını kolay ve sorunsuz kullanmasını sağlamak amacıyla, yazılımın tanıtımı ve kullanımı anlatılmaktadır. İlk bölümde Symantec AV yazılımı ekranlarına erişim ve genel olarak pencerenin işlevi anlatılmaktadır, ikinci bölümde virüs taraması, virüs tanımlarının güncellenmesi vs. sıklıkla kullanması gereken işlemler anlatılır.

- **Symantec Av Programının Çalıştırılması:** Symantec AV yazılımı seçeneklerine ulaşmanın bir kaç yolu vardır.
 - Görev çubuğundan Symantec AntiVirus ikonuna tıklanarak ulaşılır.
 - Başlat > Tüm Programlar > Symantec Client Security > Symantec AntiVirus.

Açılan pencere Şekil 2.30'da görüldüğü gibi ikiye bölünmüştür. Sol taraftaki bölümde 7 kategori halinde bölünmüş grup aktivitelerini, sağ taraftaki bölümde bu kategorilerin açıklamalarını ve ilgili seçenekleri sunulmaktadır. Alt kategorilere ulaşmak için "+" işaretine tıklamak gerekir.



Şekil 2.30: Symantec AV konsolu

- **"View" Kategorisi**
Antivirüs aktivitelerini izlemek için kullanılır.

Auto-Protect Scan Statistics: Programların çalıştırılması sırasında yapılan otomatik virüs kontrolü ile ilgili istatistiklere buradan erişilebilir.

Scheduled Scans: Zamanlanmış taramaların adı, zamanı gibi bilgilerin görüntülediği kategoridir. Bu taramalara, kullanıcı ya da sistem yöneticisi tarafından yenileri eklenebilir.

Quarantine: Virüs tarafından etkilendiği için karantina altına alınan dosyaları görüntüler.

Backup Items: Virüs tarafından etkilenmiş dosyaların tamir edilmesi sırasında alınan yedeklerin görüntülenmesini ve gerekiyorsa silinmesini sağlar.

Repair Items: Virüsten temizlenmiş ancak yeri belli olmayan dosyalar burada görüntülenir (e-posta ile gelen ve temizlenen dosyalar gibi...).

Licence: Symantec AV lisanslaması hakkında bilgi verir.

➤ **"Scan" Kategorisi**

Elle virüs taramasının çalıştırılması için kullanılır.

Scan a Floppy Disk: Disket ya da diğer taşınabilir veri taşıma ortamlarında virüs kontrolü yapılmasını sağlar.

Scan Computer: Tüm bilgisayarın, belli disk alanlarının ya da belirli bir dizinin taranmasını sağlar.

➤ **"Configure" Kategorisi**

Otomatik virüs koruması/taramasının kurallarını belirlemek için kullanılır.

Auto-Protect: Dosyaya erişildiğinde, dosya kopyalandığında, kaydedildiğinde, taşındığında veya açıldığında, dosyanın virüs taramasından geçirilmesini sağlar.

Lotus Notes Auto-Protect and Microsoft Exchange Auto-Protect: Grup yapılı e-posta istemcilerinde koruma sağlar.

➤ **"History" Kategorisi**

Geçmiş virüs taramalarını, virüs tehditlerini ve kayıtlarını gösterir.

Thread History: Bilgisayarı etkilemiş olan virüslerin ve casus programların tarihçesi görüntülenir.

Scan History: Yapılmış olan virüs taramalarının tarihçesi görüntülenmektedir.

Event Log: Hata mesajları, konfigürasyon değişiklikleri gibi bilgilerin görüntülenmesini sağlar.

➤ **"Startup Scan" Kategorisi**

Bilgisayar başlatıldığında virüs taraması yapılması için kullanılır.

New Startup Scan: Bilgisayardaki kritik dizinlerin (Windows sistem dizini, şablonların bulunduğu dizinler) bilgisayar açıldığında taranmasına imkan verir.

➤ **"Custom Scan" Kategorisi**

Elle çalıştırılacak taramaların önceden yapılandırılması için kullanılır.

New Custom Scan: Sıklıkla ama periyodik olmayan şekilde taranan dizinler için tarama şablonu oluşturmayı sağlar .

➤ **"Scheduled Scan" Kategorisi**

Zamanlanmış taramaların görüntülenmesi ve gerekli ayarların yapılması için kullanılır.

New Scheduled Scan: Bilgisayarda periyodik virüs taramaları yapılmasını sağlar (Virüs taraması yapmak başlığı altında daha ayrıntılı incelenmiştir.).

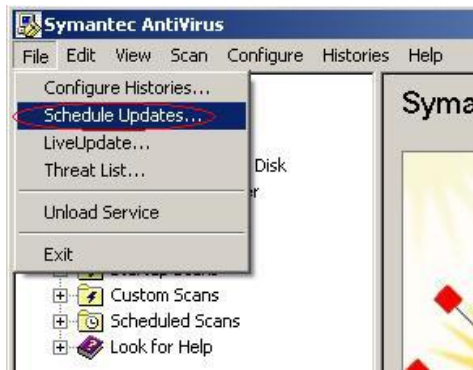
2.3.3.3. Symantec AV İle İlgili İşlemler

Virüs Korumasını Güncel Tutmak: Symantec AV yazılımı güncel virüslere karşı güvenliği sağlamak için düzenli olarak güncellenmelidir. Yazılım kurulduktan sonra güncel virüs tanımlama dosyaları ile güncellenmediği takdirde yeterli güvenlik sağlanamayacaktır. Symantec firması, virüs tanımlama dosyalarını haftalık olarak güncellemektedir. Ayrıca yeni ve önemli bir tehdit ortaya çıktığında bu güncelleme sıklığı artabilmektedir.

Güncelleme işlemi yazılımın LiveUpdate özelliği ile yapılabilmektedir. LiveUpdate özelliği virüs tanımlama dosyalarını güncellemekle birlikte, Symantec AV yazılımı için çıkabilecek yamaları da kontrol eder ve yeni yama çıkarılmışsa yükler. LiveUpdate özelliği önceden ayarlanan tarihlerde otomatik olarak çalışacak şekilde ayarlanabildiği gibi, ayarlanan tarih beklenmeden de kullanılabilir.

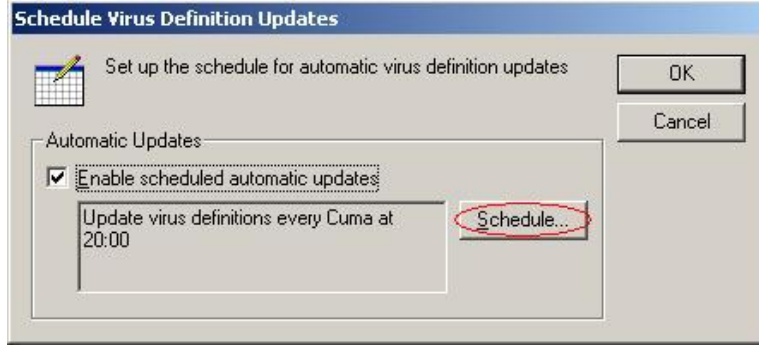
LiveUpdate ile Otomatik Güncelleme Ayarları: Symantec AV yazılımı kurulduğunda LiveUpdate seçeneği her Cuma 8:00'da çalışacak şekilde varsayılan ayarla kurulmaktadır. Bu ayar aşağıdaki şekilde değiştirilebilir.

"File" menüsünden "Schedule Updates..." seçeneği seçilir (Şekil 2.31.).



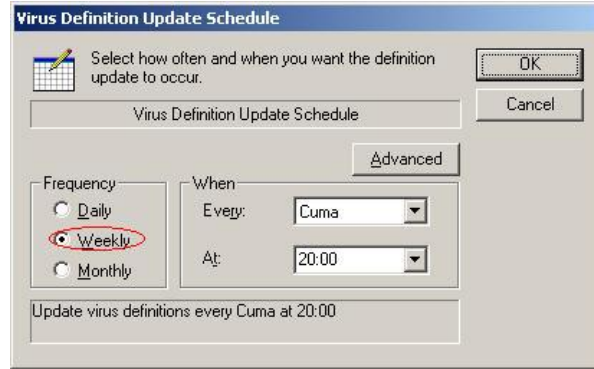
Şekil 2.31: Symantec AV güncelleme

"Schedule Virus Definition Updates" penceresinden "Schedule..."butonu tıklanır(Şekil 2.32).



Şekil 2.32: Symantec AV otomatik güncelleme

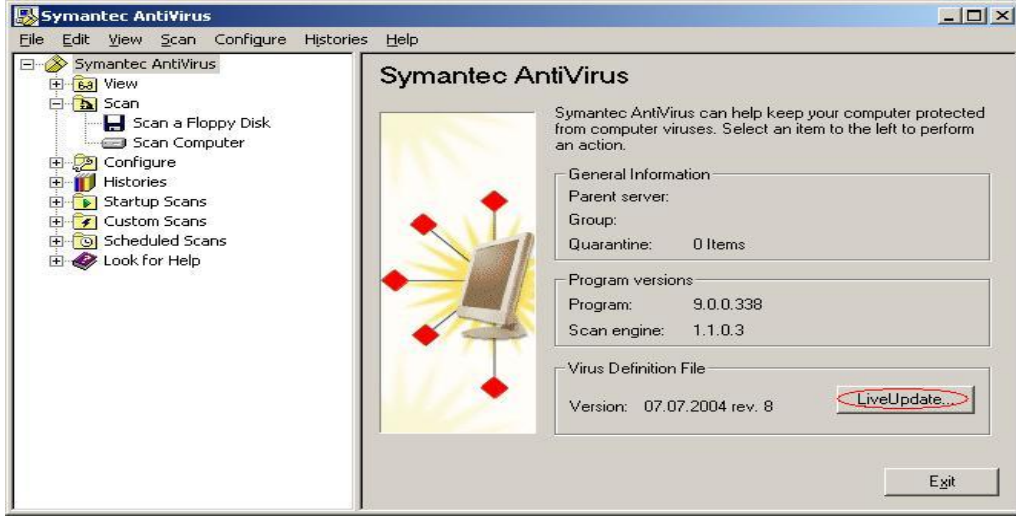
"Virus Definition Update Schedule" penceresinden otomatik güncelleme için Daily, Weekly ya da Monthly seçeneklerinden biri ile otomatik güncellenmenin sırası ile günlük, haftalık ya da aylık olarak yapılması ayarlanır (Şekil 2.33). Söz konusu ayar yapılırken, güncellenmenin yapılabilmesi için verilen gün ve saatte bilgisayarın açık olması gerektiği unutulmamalıdır. Aynı pencerede "Advanced" butonuna tıklanarak herhangi bir sebeple otomatik güncellenmenin yapılamadığı durumlarda ne kadar süre ile tekrar deneneceği de seçilebilir.



Şekil 2.33: Symantec AV günlük güncelleme ayarları

LiveUpdate ile Otomatik Güncellemeyi Beklemeden Güncelleme: Yeni bir virüs tehdidi ortaya çıktığında otomatik güncellenme seçenekleri ile ayarlanmış zamanı beklemeden güncelleme işleminin yapılması gerekebilir. Bu durumda aşağıdaki yol izlenerek güncelleme yapılabilir.

Yazılım çalıştırıldığında ilk açılan pencerenin sağ panelindeki "LiveUpdate" butonu tıklanır (Şekil 2.34.).



Şekil 2.34: Symantec AV güncelleme

Açılan "LiveUpdate" penceresinde "Next" butonuna tıklanır. Eğer yeni bir güncelleme varsa otomatik olarak yüklenecektir. İşlem sonrasında "Finish" butonuna tıklamak yeterlidir (Şekil2.35-2.36.)



Şekil 2.35: Symantec AV güncelleme 3



Şekil 2.36: Symantec AV güncelleme 4

Not: Eğer kurulum sırasında, kurulumdan sonra LiveUpdate'in çalışmasına yönelik seçenek seçilmemişse, güncellemenin vakit kaybetmeden elle yapılması gerekir.

Virüs Taraması Yapmak: Symantec AV yazılımı ile farklı şekillerde virüs taraması yapılabilir. Bunlar:

- Elle tarama
- Otomatik tarama
- Açılışta tarama
- Özel yapılandırılmış tarama

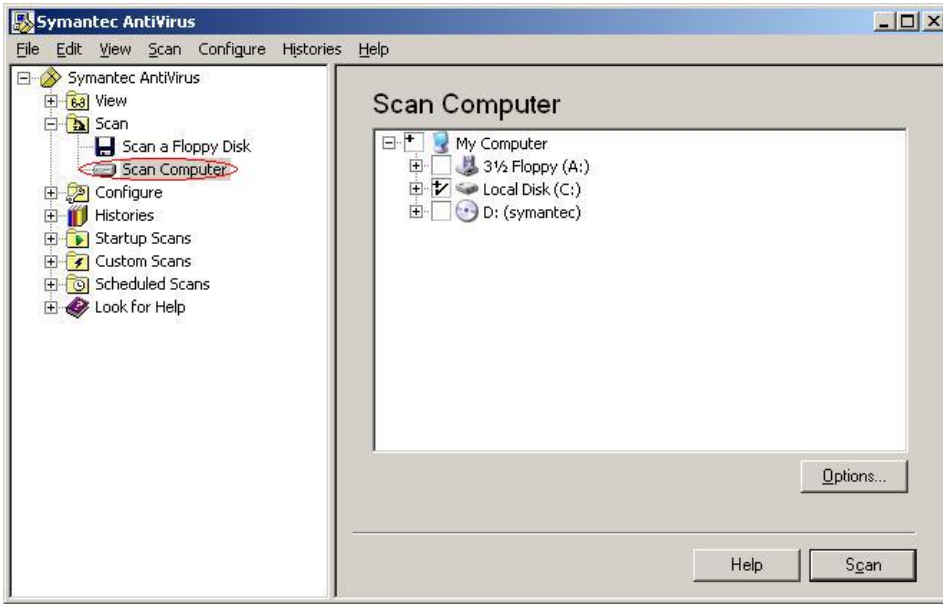
Virüslerden etkin bir şekilde korunabilmek için tüm bu tarama metotlarının birlikte kullanılması gerekebilir. Örneğin; haftada bir, tüm bilgisayarda otomatik tarama yapılırken, bilgisayarın her açılışında belli dizinlerin otomatik olarak taranması, farklı bir kullanıcıdan gelen disket ya da USB Disk gibi medyaların kullanılmadan önce taranması ve herhangi bir şüphe durumunda belli dosya/dizinlerin ayrıca taranması ile etkin bir koruma oluşturabilir. Sıralanan tarama yöntemleri aşağıdaki şekilde uygulanabilir:

Elle tarama

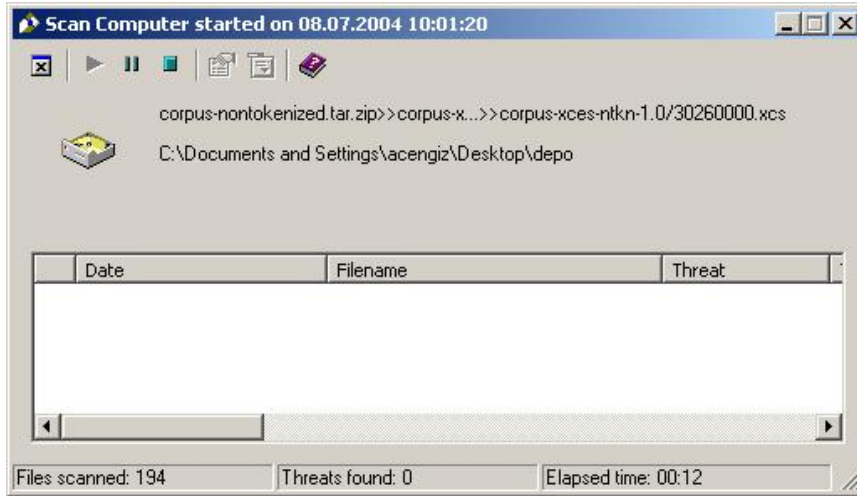
Bu tarama yöntemi ile istenen disk/dizin/dosyalar istenilen herhangi bir zamanda elle taranabilir. Yazılım çalıştırıldığında ilk açılan pencerenin sol panelindeki "Scan" ve "Scan Computer" seçenekleri tıklanır (Şekil 2.37).

Aynı pencerenin sağ panelinde kullanılmakta olan bilgisayarın dizin yapısı görülecektir. Virüs taraması yapılması istenen dizin/dosyalar yanlarındaki boş kutucuklar aşağıdaki notasyona uygun şekilde değiştirilerek seçilir ve "Scan" butonu tıklanarak tarama başlatılır (Şekil 2.37.-2.38.).

- Söz konusu disk/dizin/dosya seçilmemiştir.
- Söz konusu disk/dizin/dosya seçilmiştir.
- Söz konusu disk/dizin ve altındaki tüm disk/dizin/dosyalar seçilmiştir.
- Bu dizin altındaki en az bir dizin/dosya seçilmiştir.



Şekil 2.37: Symantec AV virüs taraması

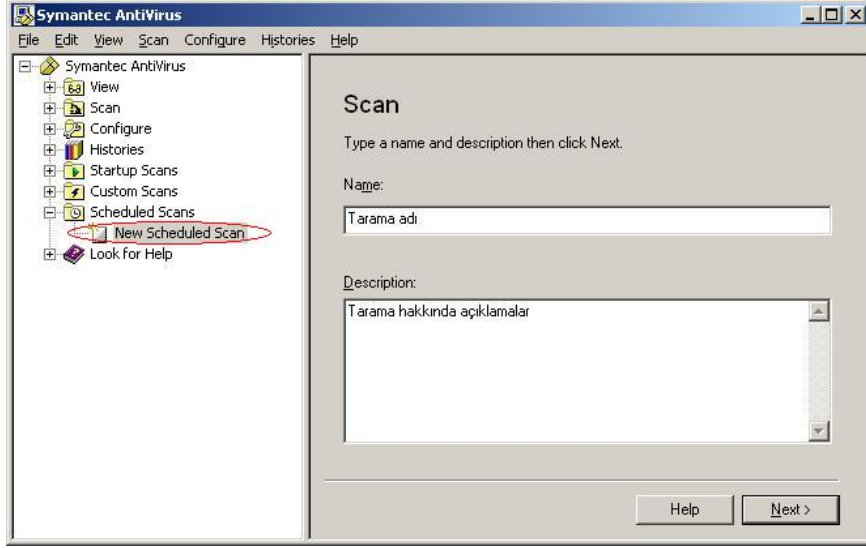


Şekil 2.38: Symantec AV tarama işlemi

Otomatik tarama

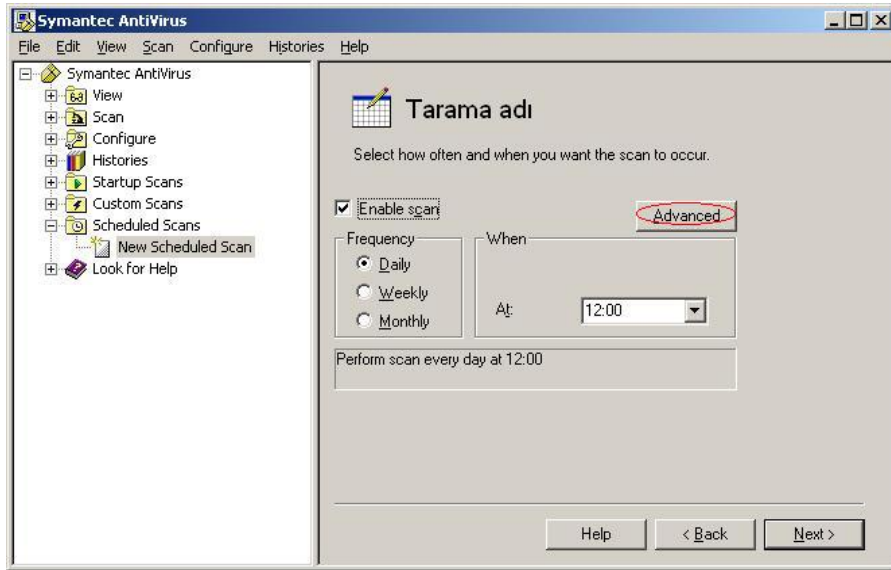
Bu tarama yöntemi ile istenilen disk/dizin/dosyalar önceden tanımlanmış herhangi bir zamanda kullanıcının müdahale etmesine gerek kalmadan taranabilir.

Yazılım çalıştırıldığında ilk açılan pencerenin sol panelindeki "Scheduled Scans" ve "New Scheduled Scan" seçenekleri seçilir (Şekil 2.39).



Şekil 2.39: Symantec AV otomatik tarama

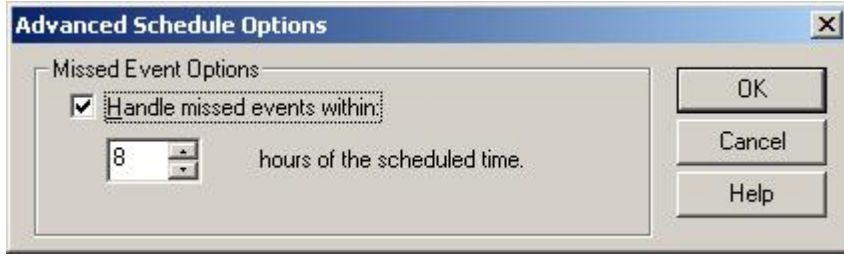
Sağ pencerede, ayarlanacak otomatik tarama için belirleyici bir isim ve tanım girilebilir. Eğer girilmezse yazılım kendisi otomatik olarak yeni isim verecektir. Bu işlemden sonra "Next" butonu ile devam edilir (Şekil 2.39).



Şekil 2.40: Symantec AV günlük tarama

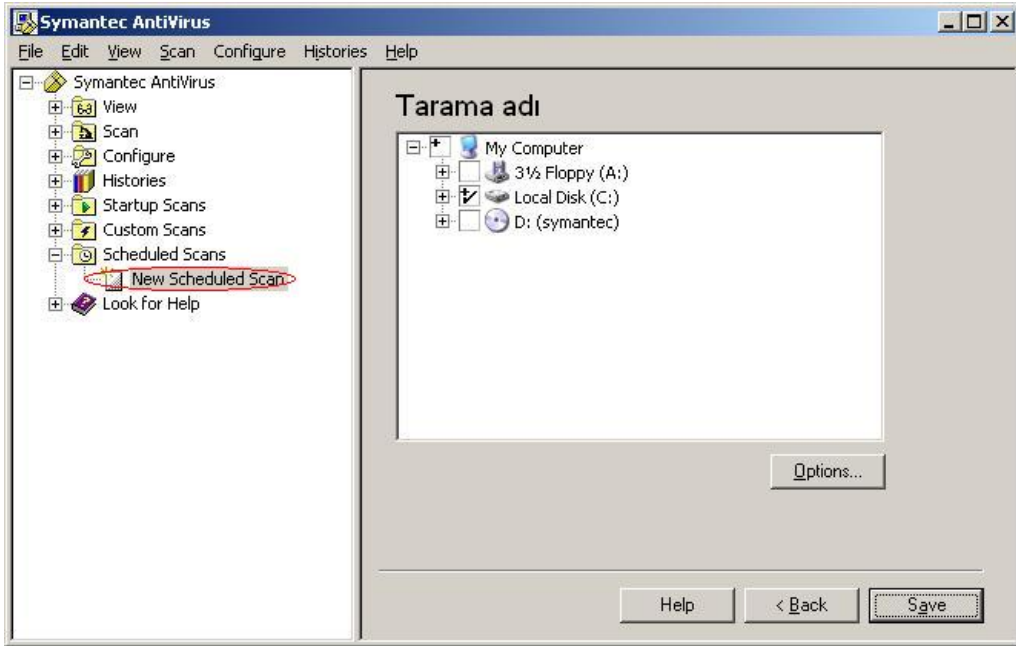
Yeni pencereden Daily, Weekly ya da Monthly seçenekleri ile otomatik taramanın sırası ile günlük, haftalık ya da aylık olarak yapılması ayarlanır (Şekil 2.40).

Söz konusu ayar yapılırken, taramanın yapılabilmesi için verilen gün ve saatte bilgisayarın açık olması gerektiği unutulmamalıdır. Aynı pencerede "Advanced" butonuna tıklanarak herhangi bir sebeple otomatik taramanın yapılamadığı durumlarda ne kadar süre ile tekrar deneneceği de seçilebilir (Şekil 2.41.). Seçimler tamamlandıktan sonra "Next" butonu ile devam edilebilir.



Şekil 2 42: Symantec AV virüs tarama

Yeni pencerede elle tarama seçeneğinde anlatıldığı şekilde otomatik tarama yapılması istenen disk/dizin/dosyalar seçilir ve Şekil 2.43'teki "Save" butonuna tıklanarak işlem tamamlanır. Aynı işlem tekrarlanarak istenildiği kadar otomatik tarama tanımlanabilir.



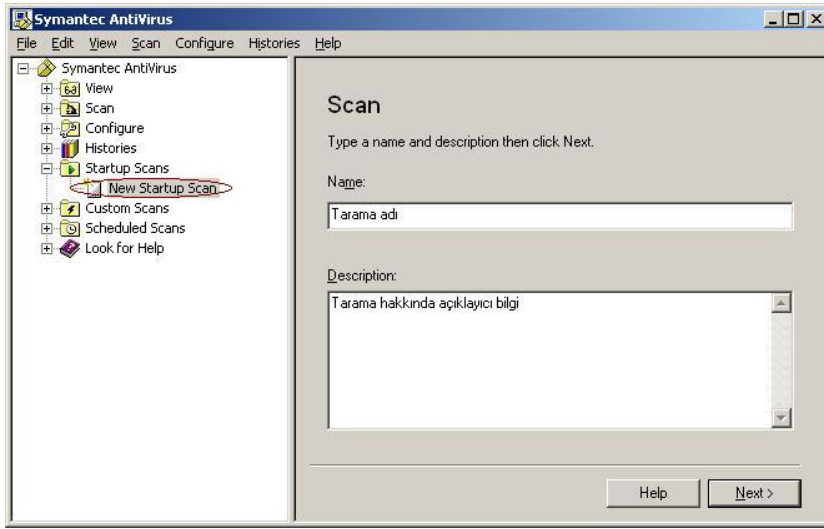
Şekil 2.43: Symantec AV yeni tarama yaratmak

Açılışta tarama

Bilgisayar her açıldığında virüs taraması yapılması istenen disk/dizin/dosyalar bu tarama yöntemi ile tanımlanabilir.

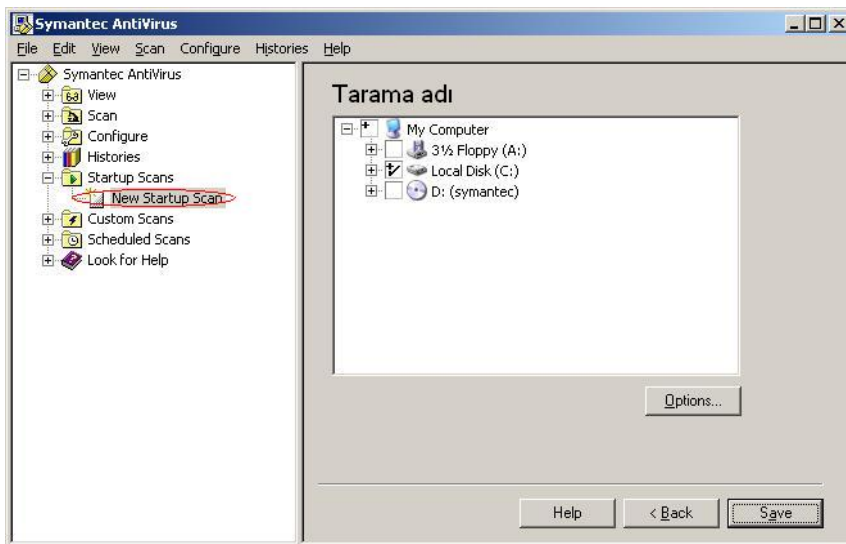
Program çalıştırıldığında, ilk açılan pencerenin sol bölmesindeki "Startup Scans" ve "New Startup Scan" seçenekleri seçilir (Şekil 2.44).

Sağ pencereye, ayarlanacak otomatik tarama için bir isim ve tanım girilir. Eğer girilmezse program kendisi otomatik olarak yeni isim verecektir.



Şekil 2.44: Symantec AV başlangıçta tarama

Bu işlemten sonra "Next" butonu ile devam edilir

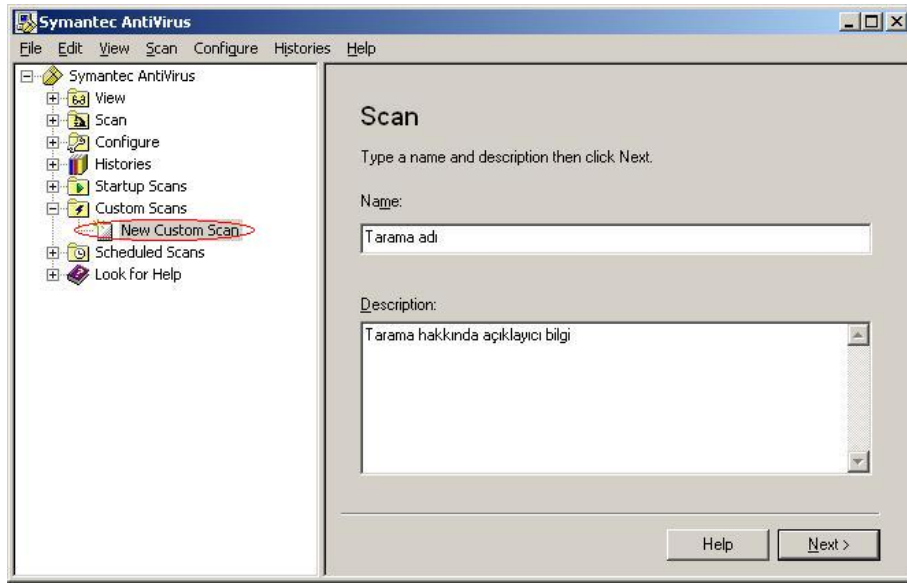


Şekil 2.45: Symantec AV başlangıçta taranacak yerlerin belirlenmesi

Yeni pencerede elle tarama seçeneğinde anlatıldığı şekilde bilgisayar açıldığında tarama yapılması istenen disk/dizin/dosyalar seçilir ve Şekil 2.45'teki. "Save" butonuna tıklanarak işlem tamamlanır. Aynı işlem tekrarlanarak bilgisayar açıldığında yapılması için istenildiği kadar tarama tanımlanabilir.

Özel yapılandırılmış tarama

Bu tarama yöntemi ile virüs taraması yapılması istenen belli disk/dizin/dosyalar tanımlanarak, istendiği zaman tek bir tıklama ile bu taramanın yapılması sağlanabilir.

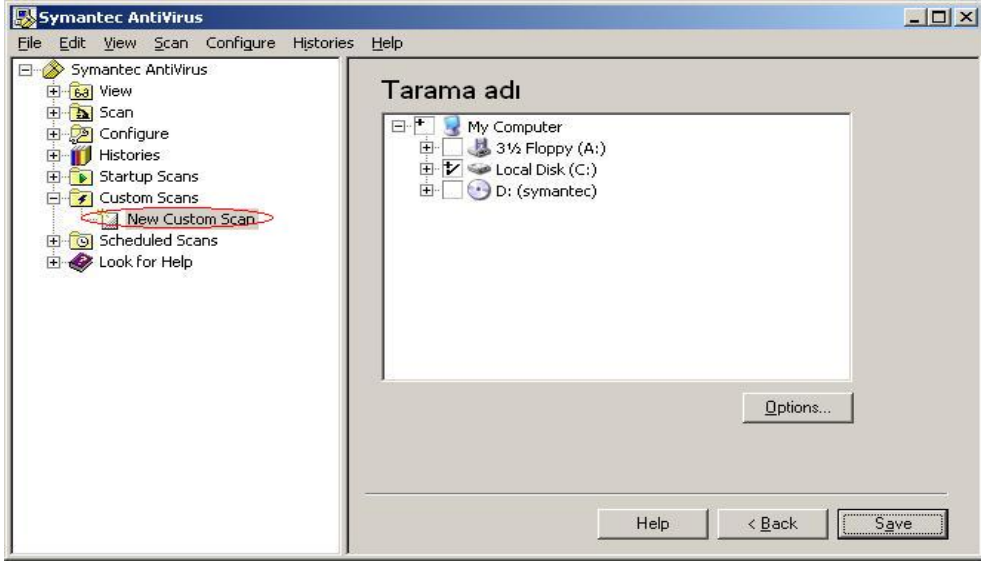


Şekil 2.46: Symantec AV özel tarama

Program çalıştırıldığında ilk açılan pencerenin sol bölümünde ki "Custom Scans" ve "New Custom Scan" seçenekleri seçilir (Şekil 2.46).

Sağ pencerede, ayarlanacak özel yapılandırılmış tarama için belirleyici bir isim ve tanım girilebilir. Eğer girilmezse yazılım kendisi otomatik olarak yeni bir isim verecektir. Bu işlemden sonra "Next" butonu ile devam edilir (Şekil 2.46).

Yeni pencerede elle tarama seçeneğinde anlatıldığı şekilde, özel tarama yapılması istenen disk/dizin/dosyalar seçilir ve Şekil 2.47'deki "Save" butonuna tıklanarak işlem tamamlanır. Aynı işlem tekrarlanarak istenildiği kadar özel yapılandırılmış tarama tanımlanabilir.



Şekil 2.47: Symantec AV özel tarama seçeneklerinin belirlenmesi

İstendiği zaman taramanın yapılabilmesi için Şekil 2.48'deki sol panelden tanımlanan tarama seçilir, sonra ya üzerine çift tıklanır ya da sağ paneldeki "Scan" butonuna tıklanır.

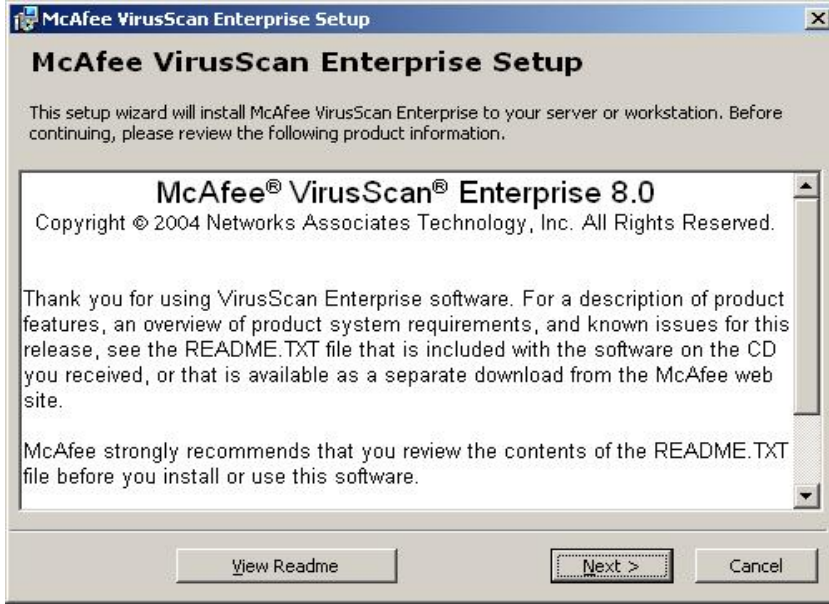


Şekil 2.48: Symantec AV özel taramaların görüntülenmesi

2.3.4. McAfee VirusScan Enterprise 8.0. Programı

2.3.4.1. McAfee VirusScan Enterprise 8.0. Kurulumu

- "Setup.exe" dosyası çalıştırılır.
- Kurulumun başladığını belirten pencere olan **şekil 2.49.**'daki "Next" butonuna basılır.
- Lisanslama ile ilgili pencerede "Licence expiry type" "Perpetual" olarak değiştirilir.
- Lisans anlaşması okunur, onay kutusu onaylanır ve Şekil 2.50'deki "OK" butonuna basılır.



Şekil 2.49: McAfee VS lisans bilgileri

Kurulumun nasıl yapılacağı seçeneklerinin bulunduğu pencerede, sunucu nitelikli bir bilgisayara antivirüs yazılımı kurulmuyorsa "Typical" seçilmesini önerilir.

Kurulumun yapılacağı dizin varsayılan olarak "C:\ProgramFiles\NetworkAssociates\VirusScan" olarak görülmektedir. Disk alanında yer sıkıntısı yoksa ve program kurulumu konusunda bir politika belirlenmemişse bu değer değiştirilmeden "Next" butonuna basılır.

"Custom" seçeneği tercih edilerek devam edilmesi durumunda; yüklenmesi istenen program seçeneklerinin bir listesi görüntülenir.

AutoUpdate: Otomatik virüs tanım (Virüs Definition) dosyalarının güncellenmesini sağlar.

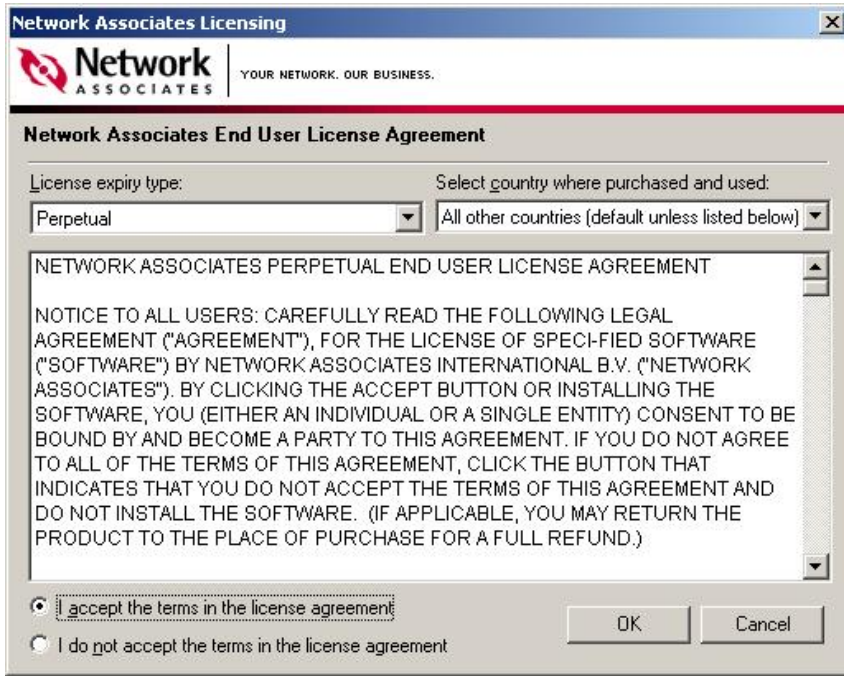
E-mail Scanner: E-posta görüntüleme yazılımı ile birlikte çalışıp gelen ve giden e-postaların virüs taramasından geçirilmesini sağlar.

On-Access Scanner: Okunan, yazılan ve değiştirilen dosyaların sürekli virüs taramasından geçmesini sağlar.

On-Demand Scanner: İstenildiği anda virüs taraması yapılmasını sağlar.

Bu seçeneklerin hepsinin seçilip yüklenmesi önerilir.

"Install Alert Manager" penceresi McAfee VirusScan yazılımı virüs yakaladığı zaman sistem yöneticisine e-posta göndererek yöneticiyi uyarma işlemini sağlayan Alert Manager yazılımının kurulumu ile ilgilidir. Sunucu nitelikli makineler dışındaki, bilgisayarlara kurulmaması önerilir.



Şekil 2.50: McAfee VS lisans anlaşma bilgileri

Yukarıdaki pencerede "Next" butonuna basılarak bir sonraki pencere ekranına geçilir.



Şekil 2.51: McAfee VS kurulum sonrası varsayılabacak ayarlar

"Product Configuration" penceresi otomatik güncelleme işleminin yerel disk alanından hangi dizinden yapılacağını belirleyen "Import Auto Update Repository List" bölümünü ve kurulum sonrasında "On-Access Scan" özelliğinin çalışmasını sağlayan "Enable On-Access Scanner at the end of installation" kısmını içermektedir (Şekil 2.51).



Şekil 2.52: McAfee VS güvenlik ayarları

"Security Configuration" penceresinde yazılımın ayarlarına parola kontrolü ile erişilmesini sağlayan "Configuration Password Protection" bölümü, Başlangıç (Start) menüsünde VirusScan ikonlarının görüntülenmemesini sağlayan "Start Menu" bölümü ve sistem tepesinde (System Tray) ikonların görüntülenme izinlerini düzenleyen "System Tray Icon and Menu" bölümü bulunmaktadır. Kullanıcıların antivirüs yazılımının ayarlarına müdahale etmesini istemeyen sistem yöneticileri tarafından kullanılacak özelliklerdir (Şekil 2.52).

"Ready to install" penceresi, yazılımın kurulumu hazır olduğunu gösterir. "Install" butonuna basılarak kurulum başlatılır. İşlem 1-5 dakika arasında sürmektedir.

Kurulum tamamlandıktan sonra güncelleme işlemini internet bağlantısı olan bilgisayarın otomatik olarak yapmasını sağlayan "Update Now" ve istenildiği anda tarama yapılmasını sağlayan "Run On-Demand Scan" seçenekleri olan pencere açılır. (Şekil 2.53). "Finish" butonuna basılarak, internet bağlantısı varsa, virüs tanımlarının güncellenmesi ve "On-Demand Scan" özelliğinin aktif hale getirilmesi önerilir.



Şekil 2.53: McAfee VS kurulumu sonu

Güncelleme işlemi internet bağlantısında oluşabilecek problemlerden dolayı yavaş olabilir; hatta gerçekleştirilemeyebilir. Bu durumlarda güncelleme bölümündeki yönergenin uygulanması önerilir.

2.3.4.2. McAfee VirusScan 8.0.i (VS) Ayarları ve Kullanımı

Bu belgede son kullanıcının McAfee VS 8.0.i yazılımını kolay ve sorunsuz kullanmasını sağlamak amacıyla, yazılımın tanıtımı ve kullanımı anlatılmaktadır. İlk bölümde McAfee VS 8.0.i yazılımı ekranlarına erişim anlatılmaktadır, ikinci bölümde virüs taraması, virüs tanımlarının güncellenmesi gibi sıklıkla kullanılması gereken işlemler anlatılır.

McAfee VS 8.0. programının çalıştırılması: McAfee VS yazılımı seçeneklerine ulaşmanın iki yolu vardır.

- Birinci yolu, McAfee VS 8.0.i yazılımı, System Tray (sistem tepsi) içinde kalkan şeklinde bir ikon olarak görülür. İkonun üstüne gelip sağ tıklanınca Şekil 2.54'te görülen sekiz seçeneğe menü görüntülenir. Varsayılan olarak "On-Access Scan Statistis" seçilmiştir. Çift fare tıklamasında açılır.

Not: Antivirüs yazılımı merkezi olarak yönetiliyor ise, bölüm/birim koordinatörü bu ikonun görünmemesini sağlamış olabilir.

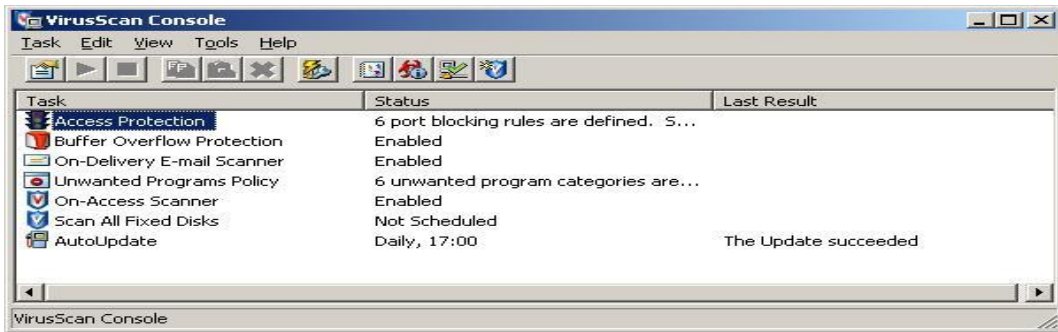


Şekil 2.54: McAfee VS

- İkinci yolu ise Başlat menüsüne tıklanır.
 - Programlar > Network Assoc > VirusScan Console kısmından çalıştırılır.

Açılan Şekil 2.55'teki pencerede;

"Access Protection", "Buffer Overflow Protection", "On-Delivery E-mail Scanner", "Unwanted Programs Policy", "On-Access Scan", "Scan All Fixed Disk" ve "AutoUpdate" seçenekleri, varsayılan olarak ayarlanmış görevler şeklinde görüntülenmektedir.

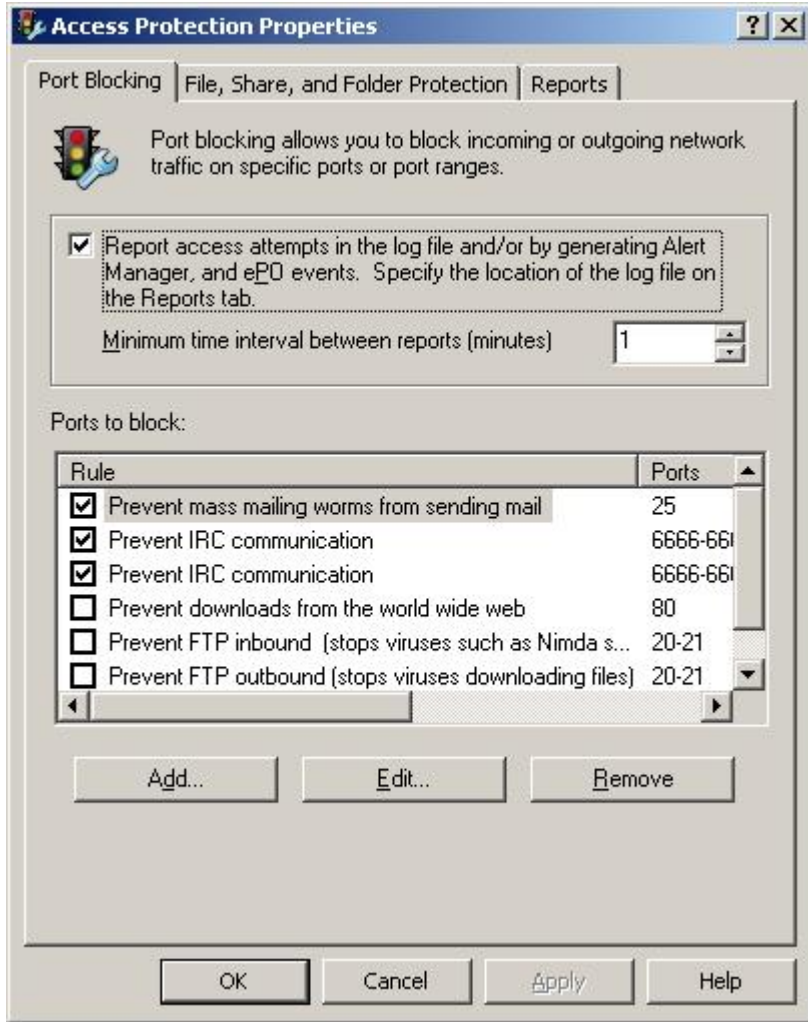


Şekil 2.55: McAfee 8.0.i VirusScan konsolu

Access Protection: Belirli portlara, dosyalara, dizinlere ve paylaşımlara erişimi kısıtlayarak, izinsiz girişleri engellemeyi sağlar.

"Buffer Overflow Protection" seçeneği çift tıkladığında kullanıcının karşısına Şekil 2.56'daki pencere görüntüsü açılır. Açılan bu pencerede üç sekme bulunmaktadır. "Port blocking", bilgisayara gelen ve giden trafikte belirli portların bloklanmasını sağlar. Bir port

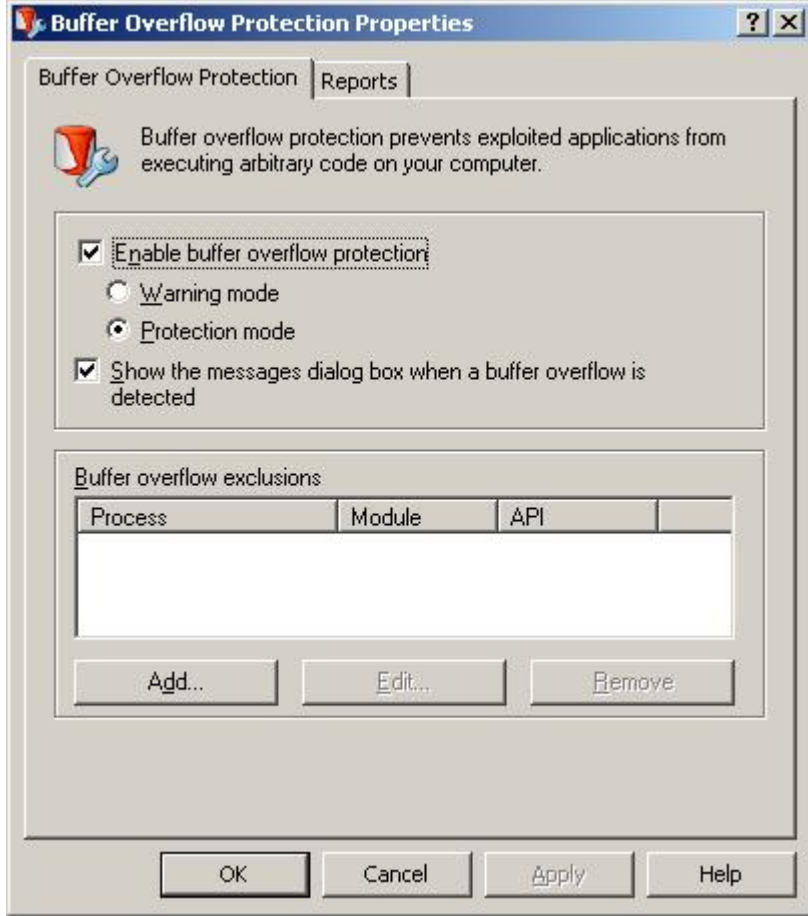
bloklandığında, o porttan gelen hem TCP hem UDP paketleri bloklanır. "File, share, and folder protection" ise paylaşımlara, dosyalara ve dizinlere okuma ve yazma erişimlerini engellemeyi sağlar. Varsayılan olarak tüm paylaşımları olduğu gibi bırakmaktadır ancak seçenekleri arasında "Make all shares read only" (Tüm paylaşımları sadece okuma hakkı ver) ve "Block read and write access to all shares" (Tüm paylaşımların okuma ve yazma haklarını durdur) vardır. "Reports" sekmesi, yukarıda belirtilen sorunlar tespit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağını ayarlanmasını sağlar.



Şekil 2.56: McAfee 8.0.i VS koruma özellikleri

Buffer Overflow Protection: Bellek taşması saldırıları sayesinde rasgele kod çalıştırılmasını engeller. Kullanıcı modunda API isteklerini izler ve bellek taşması sırasında ne zaman yapıldığını tespit eder. Birçok Microsoft ürününü bu şekilde takip edebilir. Varsayılan olarak bellek taşması koruması açık olarak kurulur.

Şekil 2.57'deki pencere görüntüsü "Buffer Overflow Protection" çift tıklandığında kullanıcın karşısına gelen penceredir. Açılan pencerede iki sekme bulunmaktadır. "Buffer Overflow Protection" sekmesi, bellek taşması saldırılarına karşı bilgisayarı koruma durumunu göstermektedir. "Reports" sekmesi, bellek taşması saldırısı tespit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağını ayarlanmasını sağlar.

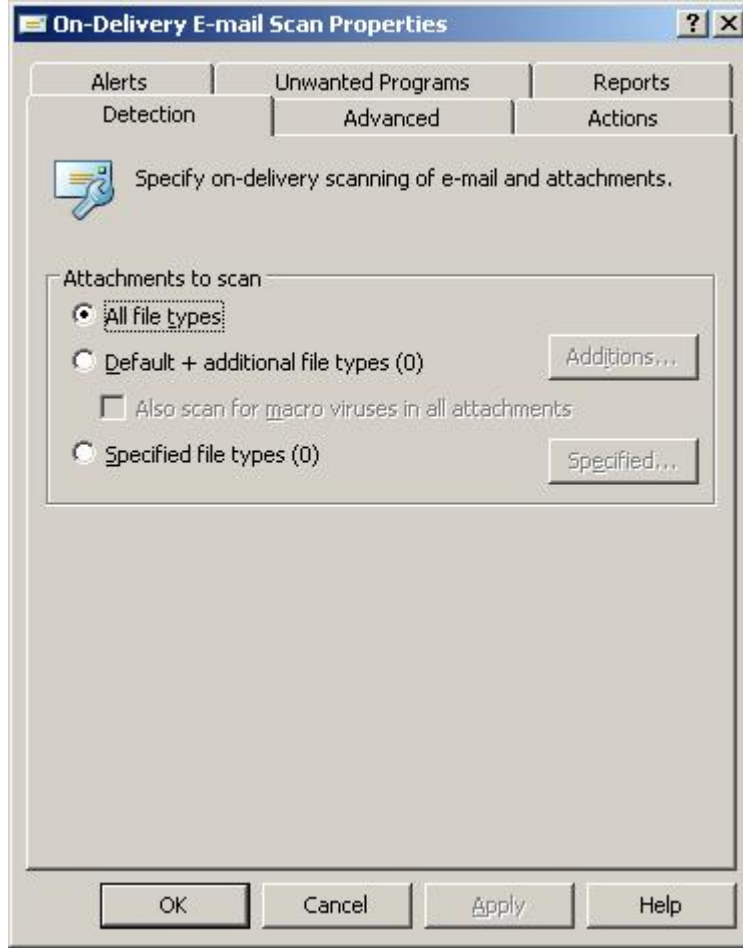


Şekil 2.57: McAfee 8.0.i VS konsolu

On-Delivery E-mail Scanner: Gönderilen e-postaların eklentilerinde olası virüs olmasını engeller. Varsayılan olarak tüm eklentileri kontrol eder.

Şekil 2.58'deki pencere görüntüsü "On-Delivery E-mail Scanner" çift tıklandığında kullanıcının karşısına gelen penceredir. Açılan pencerede altı sekme bulunmaktadır. "Detection" sekmesi, gelen e-postada taranması uygun görülen dosyaları göstermektedir. "Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus" ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses" kutusu içinde "Find potentially unwanted programs" seçeneği varsayılan olarak

seçilmemiştir. Eğer aktif hale getirilirse 'pop-up' açılan pencerelere neden olan bazı casus programlar bulunabilmektedir. "Compressed files" kutusunda sıkıştırılmış dosyaların taraması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır. Ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmemektedir.

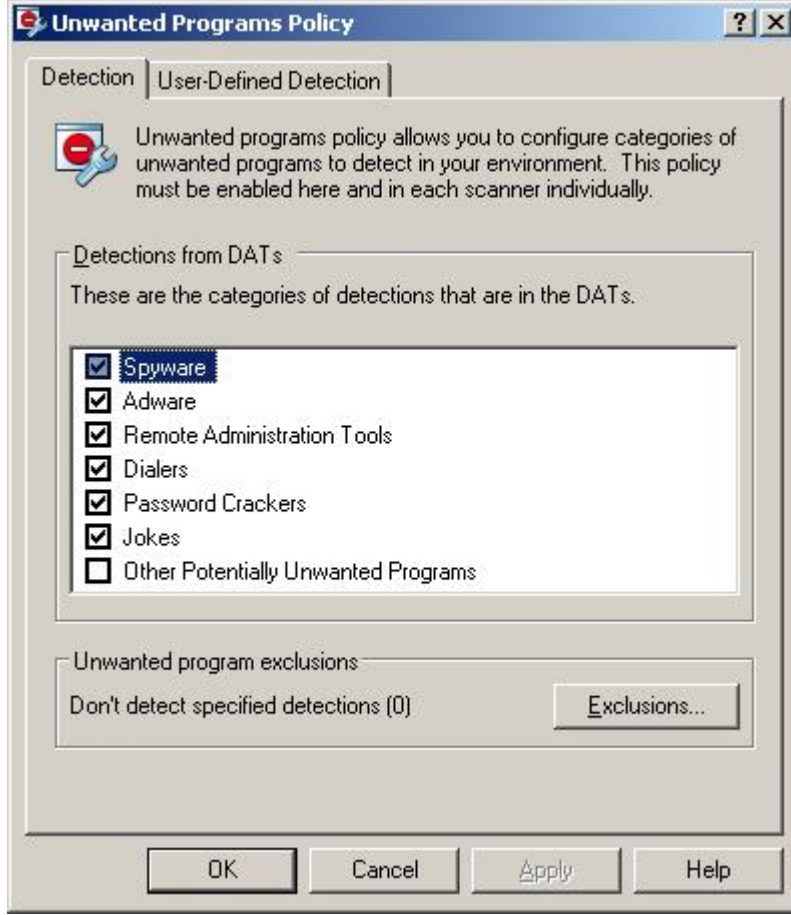


Şekil 2.58: McAfee 8.0.i VS konsolu

"Actions" sekmesi altında virüs aktivitesini yaratan dosya bulunduğunda yapılacak işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Temizleme işlemi başarılı olamazsa karantina dizini olarak belirtilen dizine taşınması seçilidir. "Alert" kısmında virüs bulunması durumunda, bilgisayardan yöneticisine gönderilecek e-postanın düzenlemesini sağlayan pencere vardır.

"Unwanted Programs" sekmesinde istenmeyen programların taranmasını sağlayan ayarlar bulunmaktadır. "Reports" sekmesi, virüs aktivitesi tespit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağını ayarlanmasını sağlar.

Unwanted Programs Policy, bölümü, casus programları bulmayı sağlayan bir özelliktir. Bu seçenekle, tüm taramalarda bu tür programların taranmasını sağlayacak ayarlar yapılmaktadır.



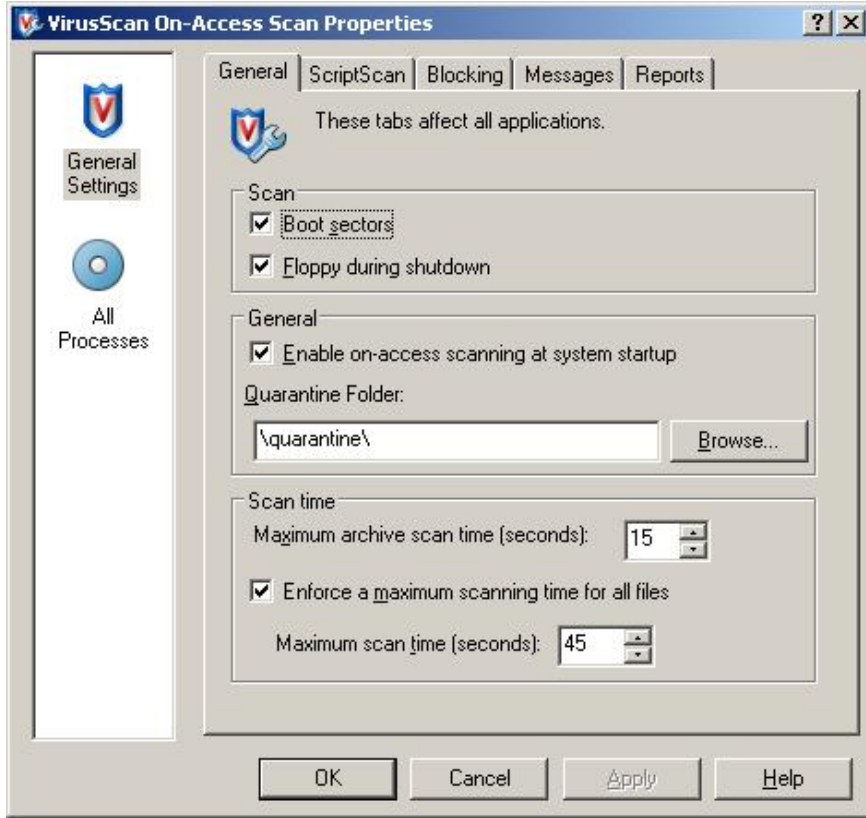
Şekil 2.59: McAfee 8.0.i VS konsolu

Şekil 2.59'daki pencere görüntüsü "Unwanted Programs Policy" çift tıklandığında kullanıcının karşısına gelen penceredir. Açılan pencerede iki sekme bulunmaktadır. Birinci sekmede algılama (Detection), genelde karşılaşılan istenmeyen programların listesi bulunur. İkinci sekmede ise kullanıcının tanımladığı algılama (User-Defined Detection), istenmeyen programların arasına, kullanıcı tarafından belirlenenlerin eklenebilmesini sağlar.

On-Access Scan: Herhangi bir dosyaya erişimde antivirüs yazılımının ilgili dosyayı virüs taramasından geçirmesini sağlar. Kullanıcının her kullandığı programı virüs taramasından geçirildikten sonra kullanmasını sağlar. Dosya çalıştırılmadan önce yapılan bu taramada amaç virüs tanımlarında bulunan virüsleri yakalamaktır.

Şekil 2.60'daki pencere görüntüsü "On-Access Scan" çift tıklandığında kullanıcının karşısına gelen penceredir. Açılan pencerede iki bölme bulunmaktadır. Birincisi solda "General Setting" ve "All Processes" ikonların bulunduğu kısım, ikincisi bu ikonların içeriklerinin bulunduğu sağdaki kısımdır.

Varsayılan olarak Genel Ayarlar "General Settings" ikonunun bilgileri görüntülenir. "General Settings" ikonu tüm virüs taramalarını ve tarama sonuçlarında yapılacak işlemleri belirlemektedir.



Şekil 2.60: McAfee 8.0.i VS konsolu

"General" sekmesi içinde bilgisayarın açılış ve kapanış işlemi sırasında antivirüs yazılımının yapacağı işlemler tanımlıdır. "General" kutusu, açılış sırasında "On-Access Scan" özelliğinin çalıştırılması ve karantina dizininin belirlenmesini sağlar. "Scan time" kutusu, dosyanın taranmasına en fazla kaç saniye ayrılacağını göstermektedir.

"Script Scan" sekmesi JavaScript ve VBScript eklentilerinin bilgisayarda çalıştırılması sırasında taranmasını sağlar.

"Blocking" sekmesi bilgisayara uzaktan erişen bir kullanıcının virüslü dosya kopyalaması durumunda erişiminin bloklanmasını sağlar.

"Messages" sekmesi tıklandığında ekrana Şekil 2.61'de görülen pencere gelir. Bu pencerede "Message for local users" onay kutusu, virüs bulunduğu anda bilgisayarı kullanan kullanıcıya verilecek mesajı ve bu kullanıcı yönetici haklarına sahip değilse yapabileceği işlemleri içerir. Bu seçenekler arasında dosyanın silinmesine izin verme vardır; ancak sistem dosyalarını etkileyen bir virüsün bilinçsiz bir kullanıcı ile birleşerek sistemi bozma olasılığı göz önünde tutulduğundan varsayılan olarak aktif değildir. "Response to

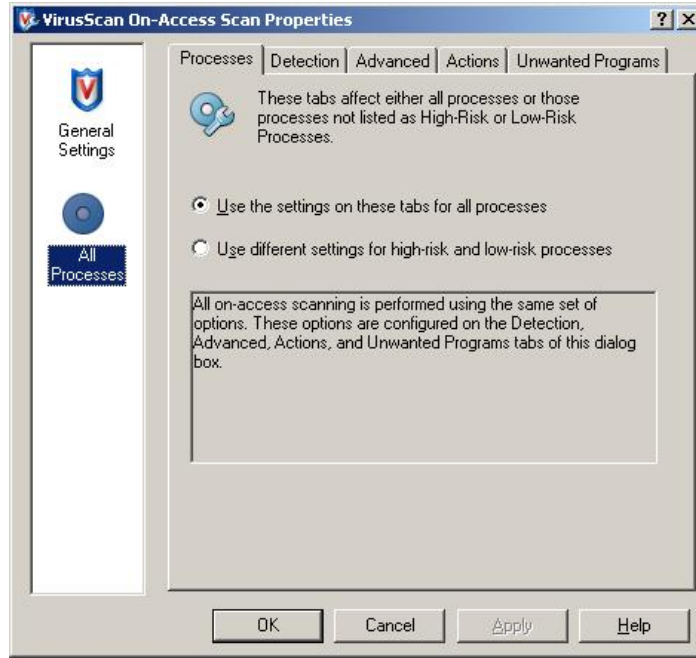
network users" kutusu ağ üzerinde bilgisayarı kullanan kullanıcılara gönderilecek mesajı ve iletişimin kesip kesilmeyeceğini belirler.

"Reports" sekmesi, bilgisayarda virüs aktivitesi tespit edildiği zaman hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağını ayarlanmasını sağlar. Virüs aktivitesine ek olarak günlük dosyasına o an bilgisayarı kullanan kullanıcı adını, virüs taraması yapılmamış şifrelenmiş dosyaları ve oturum özetini yazar.



Şekil 2.61: McAfee 8.0.i VS On-Access Scan Özellikleri- General Settings

"All Process" ikonuna tıkladığında "Processes" sekmesi altında tüm işlemlere ya da düşük risk düzeyi ve yüksek risk düzeyi olarak ayrılmış işlemlere uygulanacak ayarlara erişilmektedir (Şekil 2.62).



Şekil 2.62: McAfee 8.0.i VS On-Access Scan özellikleri - All Processes

"Processes" sekmesi altında, varsayılan olarak tüm süreçlere aynı virüs tarama politikası uygulanmaktadır.

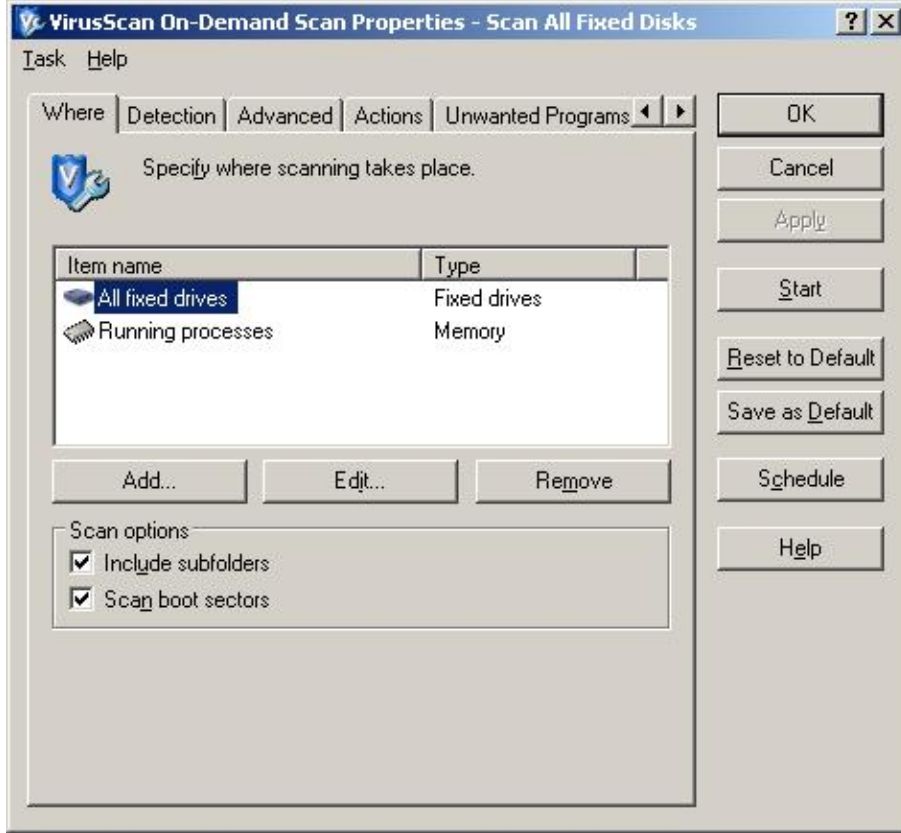
"Detection" sekmesi altındaki "Scan Files" kutusunda diske yazıldığı sırada ve diskten okunduğu sırada dosyaların taranması varsayılan olarak seçilidir. Bu seçeneklere ek olarak ağ sürücülerinin de taranması olanağı vardır. "What to scan" kutusu altında varsayılan olarak tüm dosyalar işaretlidir ancak isteğe bağlı olarak varsayılan dosyalar ve bunlara ek olarak kullanıcının belirlediği dosyaları tarama seçeneği ya da yine isteğe bağlı olarak sadece özel dosya tiplerinin taranmasını sağlayan bir seçenek bulunmaktadır. Varsayılan ayarlarla kullanması önerilir. "What not to scan" seçeneği, kullanıcının belirleyeceği dizinler ve/veya dosya türleri için tarama yaptırmama olanağı sağlar.

"Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus" ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses" kutusu içinde "Find potentially unwanted programs" seçeneği varsayılan olarak seçilmemiştir. Eğer aktif hale getirilirse 'pop-up' açılan pencerelere neden olan bazı casus programlar bulunabilmektedir. "Compressed files" kutusunda sıkıştırılmış dosyaların taranması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmez.

"Actions" sekmesi altında, virüs aktivitesini yaratan dosya bulunduğu yapılabilecek işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Temizleme işlemi başarılı olamazsa karantina dizini olarak belirtilen dizine taşınması seçilidir.

"Unwanted Programs" sekmesinde istenmeyen programların taranmasını sağlayan ayarlar bulunmaktadır.

Scan All Fix Disks: Kullanıcının bilgisayarındaki dosyaların hepsini kendi istediği zaman taramasını sağlar. "Add" butonu, belirlenen tarama yapılacak alanlar dışında tarama yapılması istenen alanların eklenmesini sağlar. "Remove" butonu, listede bulunan ve taranması istenmeyen alanların çıkarılmasını sağlar (Şekil 2.63).



Şekil 2.63: McAfee 8.0.i VS On-Demand Scan özellikleri

"Start" butonu kullanıcının o anda tarama başlatmasını sağlar. "Reset to Default" butonu, kullanıcının varsayılan ayarlara dönmesini, "Save as Default" butonu da varsayılan ayarların kullanıcının belirlediği ayarlar olmasını sağlar. Tarama işlemi "Schedule" butonuna basılarak zamanlanmış görevler arasına alınabilir (Şekil 2.63).

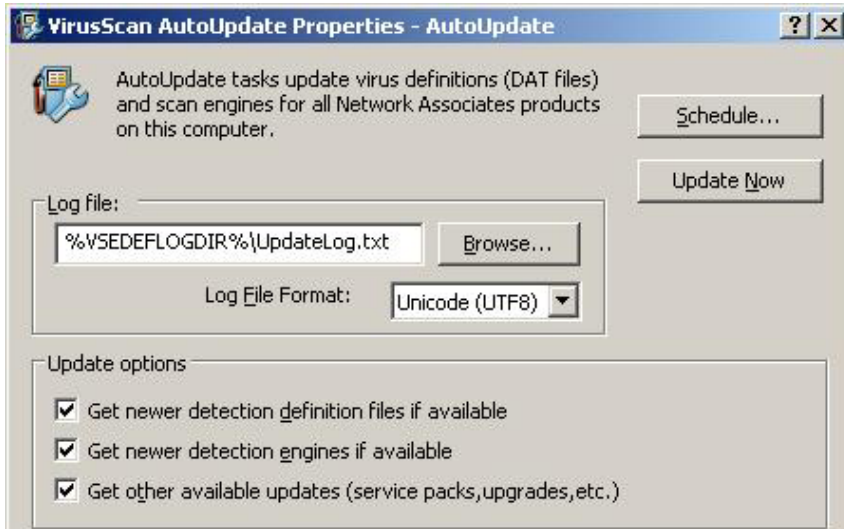
"Detection" sekmesi altındaki "Scan Files" kutusunda diske yazıldığı sırada ve diskten okunduğu sırada dosyaların taranması varsayılan olarak seçilidir. Bu seçeneklere ek olarak ağ sürücülerinin de taranması olanağı vardır. "What to scan" kutusu altında varsayılan olarak tüm dosyalar işaretlidir ancak isteğe bağlı olarak varsayılan dosyalar ve bunlara ek olarak kullanıcın belirlediği dosyaları tarama seçeneği ya da yine isteğe bağlı olarak sadece özel dosya tiplerinin taranmasını sağlayan bir seçenek bulunmaktadır. Varsayılan ayarlarla kullanılması önerilir. "What not to scan" seçeneği içinde kullanıcının belirleyeceği dizinler ve/veya dosya türleri için tarama yaptırmama olanağını sağlar.

"Advanced" sekmesi altında "Heuristics" kutusu içinde virüs tanımlarında bulunmayan ama eski bir virüs motorunu kullanan virüsleri yakalamaya yarayan "Find unknown program virus ve "Find unknown macro virus" seçenekleri varsayılan olarak seçilidir. "Non-viruses kutusu içinde "Find potentially unwanted programs" seçeneği varsayılan olarak seçilmemiştir. Eğer aktif hale gelirse pop-up açılan pencerele neden olan bazı casus programlar vardır. "CPU utilization" tarama sırasında işlemcinin hangi oranda kullanılacağını belirlenmesini sağlar. "Compressed files" kutusunda sıkıştırılmış dosyaların taranması ile ilgili seçenekler bulunmaktadır. Varsayılan olarak ".UPX" dosyalarını taramaktadır. Ancak ".ZIP" ve MIME olarak kodlanmış dosyaları taramadan geçirmektedir.

"Action" sekmesi altında virüs aktivitesini yaratan dosya bulunduğu yapılacak işlemler tanımlanmıştır. Varsayılan olarak virüslü dosyanın otomatik olarak temizlenmesi seçilmiştir. Virüslü dosyaya uygulanan temizleme işlemi başarılı olmazsa karantina dizini olarak belirtilen dizine taşınması seçilidir.

"Report" sekmesi, bilgisayarda virüs aktivitesi tespit edildiği zaman, hazırlanacak günlüklerin hangi konumda ve bu günlüklerin en fazla hangi boyutta olacağını ayarlanmasını sağlar. Virüs aktivitesine ek olarak günlük dosyasına o andaki kullanıcı adını, virüs taraması yapılmamış şifrelenmiş dosyaları ve oturum özetini yazar.

AutoUpdate: Kullanıcının virüs tanımlama dosyalarını güncellemesini unutmaması ya da atlaması sonucu antivirüs yazılımının yeni çıkan virüslere karşı etkisiz kalmasını engellemek için hazırlanmış bölümdür (Şekil 2.64). "Update Now" butonu o anda güncelleme yapılmasını sağlar.



Şekil 2.64: McAfee 8.0.i VS - AutoUpdate özellikleri

"Log file" sekmesi güncellenmenin günlüğünü tutar. Bu dosyayı başarısız güncellemelerde, sorunu bulmak açısından incelemekte fayda vardır. "Run options" güncelleme sonrasında istenen bir programın çalıştırılmasını sağlar. Genelde virüs tarama programının çalıştırılması bilgisayarın yeni çıkan virüs aktivitesinden etkilenip etkilenmediğini görmek açısından faydalıdır.

Güncellemenin periyodik olarak yapılması için "Schedule" butonuna basılır. Açılan pencerede, kullanılan bilgisayar bir domain üyesi bilgisayarsa ait olduğu domain'de güncelleme yetkilerine sahip kullanıcı adı ve parolası girilmelidir. Ardından "Schedule" sekmesi tıklanarak hangi sıklıkla güncelleme yapılacağı belirlenmelidir. Normal durumlarda haftada bir defa güncelleme yapmak yeterlidir. Ancak acil önlem planları uygulanmaya başladığında gerekli görülürse bu süre düşürülmelidir (Şekil 2.65).



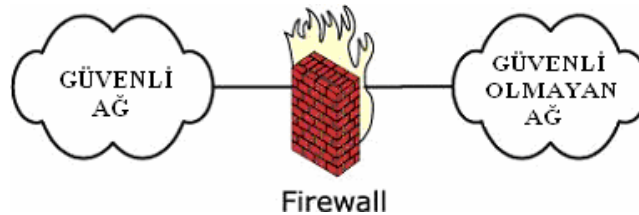
Şekil 2.65: McAfee 8.0.i VS - AutoUpdate Özellikleri - zamanlanmış güncelleme

2.4. Güvenlik Duvarı (Firewall)

2.4.1. FireWall Nedir

Firewall tek bilgisayarınıza veya yerel ağınıza internetten veya diğer ağlardan erişimi kısıtlayarak, bilgisayarınızı veya yerel ağınıza, internetten veya diğer ağlardan gelecek saldırılara karşı koruyan bir bilgisayar ve üzerindeki yazılıma verilen genel addır.

Firewall internet ile yerel ağınızın arasında bulunur (Şekil 2.66). Bu sayede internetten gelen ve internete giden paketleri mutlaka firewall kurulu bilgisayardan geçmek zorundadır. Bu sayede gelen ve giden paketleri kontrol eder. İstedığınız pakete izin verip istemediğiniz paketi engelleyebilirsiniz. Bu kısıtlama paket filtreleme yöntemi ile yapılır



Şekil 2.66: Firewall = Güvenlik Duvarı (Ateş Duvarı)

Masaüstü bilgisayarlara kurulan güvenlik duvarı, bilgisayara internet veya yerel ağ üzerinden gelen ve bilgisayardan internet'e veya yerel ağa gönderilen paketleri, kendi tanım dosyasında bulunan güvenlik sorunu oluşturan paketlerle karşılaştırır ve bunlar arasından sorunlu olanları kullanıcıya haber verir. Güvenlik duvarı dışardan bilgisayara gelen ve bilgisayardan dışarıya giden tüm paketleri inceler.

Firewall'lar, en temelde, internete bağlanacak bir bilgisayar ile internetle kurulan gerçek bağlantı arasında konumlandırılır. Ne zaman bir bilgisayar internete bağlanmak isterse, veriler önce firewall'a ardından internete gider. Tabii, internette biri bir bilgisayara bağlanmak istediğinde de veriler önce firewall'a ardından o bilgisayara ulaşır. Firewall'lar iletilerin hepsinin geçişine izin vermez.

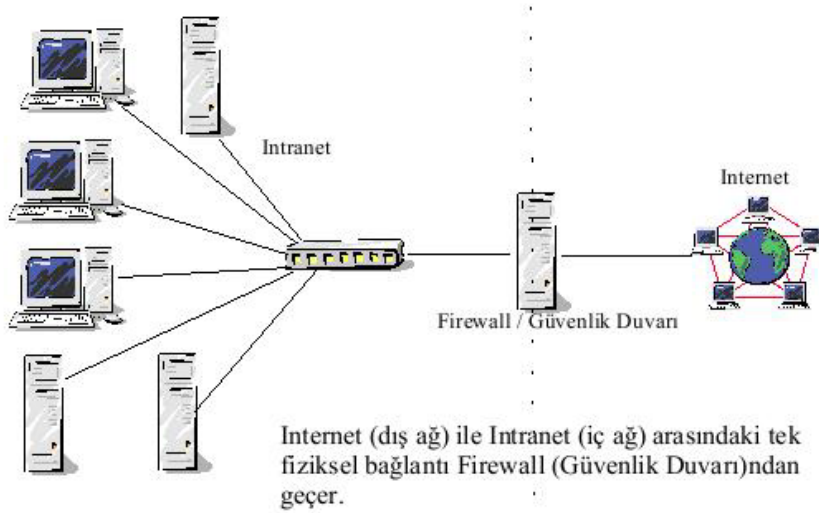
Firewall, bir donanım cihazı olabileceği gibi yazılım olarak ta karşımıza çıkabilir. Güvenlik duvarlarının farklı farklı görevleri vardır. Ancak bütün güvenlik duvarlarının bu görevleri yerine getirmesi söz konusu değildir. Güvenlik duvarlarının belli başlı görevleri şunlardır:

Filtreleme: Bir firewall iletileri filtreden geçirebilir ve bunları gönderip göndermemeye karar verebilir. Firewall'lar internette gelen talepleri ya da internete yönelik talepleri geri çevirebilir. Yani bir firewall belli ölçütlere uymayan her türlü iletiyi engelleyebilir. Böylece tanınmayan kaynaklardan gelen iletiler, bilinmeyen uygulamalar engellenir.

Proxy sunucular(Vekil Sunucular) : Bir firewall bir proxy sunucusu işlevini üstlenebilir. Bu şekilde kurulmaları durumunda, internete erişimi sadece firewall sağlayabilir. Diğer bilgisayarlar internete erişmek için önce firewall ile bağlantı kurmak durumunda kalır. Bu talep üzerine firewall bağlantıyı sağlar, erişim talebinde bulunur ve sonuçları geri iletir. Bunun yararlarından biri, firewall tek bir bilgisayar olarak gözüktüğünden ve internet bağlantısı için her bilgisayara bir IP numarası alınması gerektiğinden, internet bağlantısının maliyetinin düşmesidir. Bir diğeri, sadece firewall internete bağlandığından, diğer makineler Internet ortamında görünmemektedir.

Yönelme: Bir firewall proxy sunucusu olarak kurulduğunda, ayrıca yönlendiricilik görevi de üstlenir. Yani bilgisayar ağı iletilerini ağ içinde doğru makinelere yönlendirir. Firewall'lar ayrıca Internet trafiğini ağ içindeki belli makinelere yöneltebilir. Peki hacker'lar bir firewall' u nasıl aşar? Bir delik bularak. Eğer her şeyi engelliyorsa bir firewall iyi değildir; hacker'lar da firewall üzerinden geçişine izin verilmiş bir şey bulur ve bunu kullanır.

Güvenlik duvarı ilk kurulduğunda öğrenme aşamasındadır. Bu nedenle birçok uyarı mesajı verir. Kullanıcı bu mesajları saldırı olarak algılamamalıdır.



Şekil 2.67: İç ve dış ağ arasında bulunan bir Firewall

Normal şartlar altında, masaüstü bilgisayarlarda sunucu nitelikli programlar çalıştırılmaması gerekir. Ancak çalıştırıldığı durumlarda dışarıdan gelen paketlerde güvenlik duvarının verdiği uyarılar daha dikkatli incelenmelidir. Kullanıcı, dosya indirme, güncelleme ve anlık mesaj programları dışından kalan programlara kurulan bağlantılarda, bağlantının kurulmaya çalışıldığı port ve programı bilmiyorsa bağlantıya izin vermemelidir.

İçeriden dışarıya kurulan bağlantılarda, ilgili program ve bağlanılmak istenen port hakkında kullanıcının bilgisi bulunuyorsa güvenlik duvarından geçişe izin verecek olan seçenek tercih etmelidir. Ancak rapor edilen program hakkında kullanıcının bilgisi yoksa öncelikle programın bir işletim sistemi uygulaması olup olmadığı araştırılmalıdır. Program, o anda çalıştırılan bir uygulamaya bağlı bir sistem uygulaması ise bu programa ve bağlanılmak istenilen porta izin verilebilir.

Bunlara ek olarak, antivirüs programları gibi güvenlik duvarı programları da yeni çıkan saldırı tiplerine karşı güncellenmelidir. Güncellenmemiş güvenlik duvarı programları yeni saldırı yöntemlerine karşı etkisiz kalabilmekte ve bilgisayar güvenliğini tam olarak sağlayamayabilmektedir.

Unutulmamalıdır ki güvenlik duvarı hiçbir zaman yüzde yüz güvenlik sağlamaz. Güncellenmemiş ve güvenlik açıkları olan işletim sistemleri, zayıflıkları giderilmemiş programlar ve zayıf parolalara sahip kullanıcı hesapları, güvenlik duvarının arkasında olsa bile güvende sayılmaz.

Güvenlik duvarları tek bir yönlendiriciden, birçok yönlendiriciden, tek bir host sisteminden veya üzerinde güvenlik duvarı yazılımı çalışan birçok hosttan, Güvenlik duvarı hizmeti vermek için özel olarak tasarlanan donanım aygıtlarından veya bunların çeşitli kombinasyonlarından oluşabilir. Bu kombinasyonlar tasarım, fonksiyonellik, mimari yapı veya fiyata göre değişkenlik gösterir. Bu yüzden her bir güvenlik duvarı çözümünün neyi yapıp neyi yapmadığını anlamak oldukça önemlidir. Güvenlik duvarı çözümlerinin ağ üzerinde hem pozitif hem de negatif etkileri bulunmaktadır.

2.4.2. Güvenlik Duvarları Neler Yapabilir

Dođru şekilde uygulandıđında Güvenlik duvarları ađa gelen ve ađdan giden trafiđi kontrol edebilir. Yetkisi bulunmayan veya dıř kullanıcıları i ađa ve servislere eriřimlerini engelleyebilir. Aynı zamanda i kullanıcıların da dıř veya yetkileri bulunmayan ađa veya servislere eriřimlerini engelleyebilir. Departmanlar veya diđer özel ađlar servislerin eriřim kontrollerini sađlamak amacı ile birok güvenlik duvarı yapılandırılabilir.

Kullanıcı Kimlik Dođrulaması: Güvenlik duvarları kullanıcılardan kimlik bilgilerini talep edecek şekilde yapılandırılabilir. Bu ađ yöneticilerinin belirli kullanıcıların belirli servislere ve kaynaklara eriřimini kontrol etmesine olanak sađlar. Kimlik dođrulama ayrıca ađ yöneticilerinin kullanıcı aktivitesini ve izinsiz giriř denemelerini izlemesine olanak sađlar.

Denetleme ve Loglama: Güvenlik duvarları denetleme ve loglama olanakları sađlayabilir. Güvenlik duvarlarını bu şekilde yapılandırarak gerekli bilgiler ileriki gnlerde incelenip analiz edilebilir. Güvenlik duvarları ayrıca topladıkları bilgilerden eřitli istatistiklerde oluřturabilir. Bu istatistikler ađ eriřimi ve kullanımı ile ilgili güvenlik kararlarını vermekte olduka faydalı olabilir.

Gvenlik: Bazı Güvenlik duvarları i ve gvenilir ađları dıř ve gvenilir olmayan ađlardan ayırmada kullanılır. Ek katman gvenliđi servisleri istenmeyen taramalardan koruyabilir. Güvenlik duvarı ozmlerinin birok faydası olmasının yanında negatif etkileri de bulunmaktadır.

Trafik Darbođazı: Güvenlik duvarları bazı ađlarda trafik darbođazına sebep olabilir. Btn ađ trafiđinin güvenlik duvarı zerinden gemesi zorunlu kılındıđı durumlarda ađ trafiđinde tıkanıklık yařanma ihtimali olduka fazladır.

Tek Hata Noktası: Ađlar arası geiřin sadece Güvenlik duvarı zerinden yapıldıđı durumlarda eđer güvenlik duvarı dođru yapılandırılmazsa ađlar arasındaki trafik akıřında problemler yařanır.

Kullanıcıyı Hayal Kırıklıđına Uđratma: Ađ servislerine veya kaynaklarına eriřim hakkı kısıtlanan kullanıcılarda veya eriřim hakkı olupta gerekli řifrelerini hatırlayamayan kullanıcılarda güvenlik duvarları memnuniyetsizliđe yol aabilir.

Artan Ynetim Sorumluluđu: Güvenlik duvarları fazla olan ađlarda ynetim sorumluluđu arttıđı gibi herhangi bir problem olması durumunda bu problemin kaynađını bulmakta zorlařabilir. Eđer ađ yneticileri uyarıları ve logları incelemek iin yeteri kadar zaman ayırmazlarsa Güvenlik duvarının gerekte iřini yapıp yapmadıđı hakkında kesin bir bilgiye sahip olamazlar. Btn Güvenlik duvarları devamlı ynetimsel desteđe, genel bakıma, yazılım gncellemelerine, güvenlik yamalarına ihtiya duymaları yneticiler zerine ek bir yk getirir.

2.4.3. Güvenlik Duvarları Neleri Yapamaz

Güvenlik duvarları hakkında en yaygın anlayış ağ güvenliğini %100 garanti etmesidir. Güvenlik duvarı ağınızın %100 güvenli olduğunu garanti edemez. Daha fazla koruma sağlamak amacıyla güvenlik duvarı diğer güvenlik sistemleri ile beraber kullanılabilir. Bütün bunlara rağmen hiç bir sistem ağın %100 güvenli olduğunu garanti edemez.

Güvenlik duvarları içindeki ataklara karşı herhangi bir koruma sağlayamaz. Güvenlik duvarının etkin olması için bütün trafiğin onun üzerinden geçmesi gerekir. Güvenilir ağda veya iç kullanıcılar, genelde güvenlik duvarı üzerinden geçmeden servislere erişebilir. Günümüzde güvenlik vakalarının büyük bir yüzdesi güvenli ağ içinde bulunan kullanıcılardan gelmektedir.

Güvenlik duvarları ağın arka kapısından gelen istenmeyen veya yetkisiz erişimleri engelleyemez. Arka kapılar, genelde iç kullanıcılar güvenilir olmayan ağlara bağlandıklarında veya yetkisiz bir modem ile dışarıya eriştiklerinde oluşur.

Birçok yapılandırmada güvenlik duvarları virüslere ve zararlı kodlara karşı koruma sağlayamaz. Güvenlik duvarlarının çoğu paket içeriğini incelemediğinden, bir tehdidin içeri girmekte olduğundan haberleri olmaz.

Sonuçta, hiçbir güvenlik duvarı yetersiz veya kötü yönetilen güvenlik politikasına karşı koruma sağlayamaz. Eğer bir şifre dışarı çıkarılırsa o ağ artık risk altındadır. Kullanıcıların makinelerini açık bırakmalarından veya dikkatsiz bir şekilde şifrelerini vermelerinden dolayı birçok güvenlik gediği oluşmaktadır. Kişilerin zarar vermeye yönelik herhangi bir amaçları olmamasına karşın ağ güvenliği üzerindeki sonuçları oldukça zarar verici olabilir.

2.4.4. Güvenlik Duvarları Nasıl Çalışır

Güvenlik duvarlarının işlevlerini inceledikten sonra çalışma prensiplerini inceleyelim.

Ağ Güvenlik duvarları erişim kontrol kararlarını verirken iki güvenlik mantığı yaklaşımını kullanır. Bu iki yaklaşımın mantığı zıt olmasına rağmen ikisinde amacı erişimi kontrol etmektir. Bu iki yaklaşım şunlardır:

- Özel olarak izin verilmeyen her şeyi reddet.
- Özel olarak reddedilmeyen her şeyi kabul et.

Her iki yaklaşımın da taraftarları olmasına rağmen en fazla tavsiye edilen “Özel olarak izin verilmeyen her şeyi reddet” yaklaşımıdır. Bu yaklaşım istenmeyen ve izin verilmeyen erişimlere karşı bir ön koruma sağlar. Özel olarak bir erişime izin verilmediği sürece bütün erişim bu yaklaşım tarafından engellenir.

“Özel olarak reddedilmeyen herşeyi kabul et” mantığı, istenmeyen ve izin verilmeyen erişimlere karşı tepkisel bir tutum sergiler. İlk yaklaşıma göre daha az güvenlik sağlar. Fakat aynı zamanda ilk yaklaşıma göre daha esnekler.

2.4.5. Yerel Ağda Gelişmiş Firewall Özellikleri

Güvenlik duvarı programlarının, yerel ağ güvenliği ile ilgili olarak birtakım özellikleri vardır. Yerel ağ üzerinde çalışan güvenlik duvarı dediğimiz servisler, aslında bir kaç alt kavramdan oluşur;

- Tabya (Bastion Host)
- Ağ Adres Çevrimi (NAT)
- Maskeleye
- Paket Filtreleme

Bütün güvenlik duvarları (Ticari olanlar ve olmayanlar), bu uygulamaların hepsini veya bir kısmını uygular.

2.4.5.1. Tabya (Bastion Host)

İdealde, ağımızdaki güvenlik, ağ seviyesinde ve ağdaki her bir makinede uygulanır. Pratikte ise bu ya yapılamamakta ya da ihtiyaç duyulan kimi protokollerin güvenlikten yoksun olduğu bilirse dahi kullanılmaktadır. Böyle durumlarda güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinelerin olduğu bir ağla, dış dünya arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır. Dolayısıyla içerideki ağa girmek isteyen her kötü niyetli dış saldırı, önce özel olarak korumalı tasarlanmış güvenlik duvarı makinesini bertaraf etmek zorundadır. Bu makineye "kale", "nöbetçi kale" anlamına gelen tabya (bastion host) da denir. Tabyamız, fiziksel olarak iki farklı ağa bağlıdır: İç ağ (Intranet) ve dış ağ (Internet). Tabya iki özelliğe sahiptir:

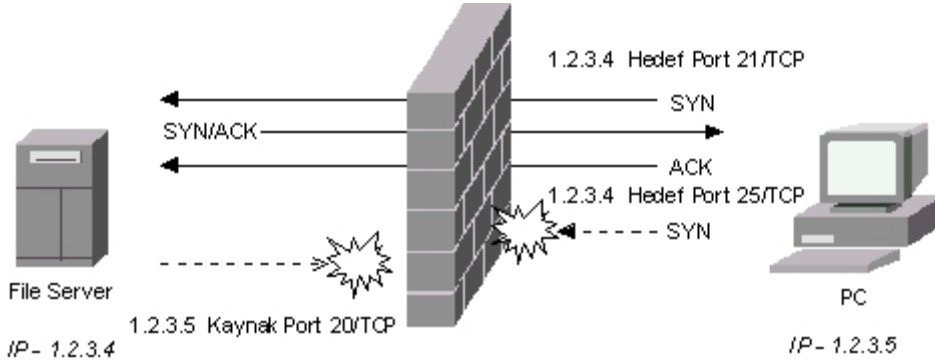
- Yüksek güvenliğe sahip olmalıdır. Yani bu makineye izinsiz erişim son derece zor hale getirilmelidir.
- İki (Bazen üç) fiziksel ağ bağlantısına sahip olmalı ve bu farklı ağlar arasındaki iletişimin nasıl yapılacağına dair karar verebilmelidir.

2.4.5.2. Ağ Adres Çevrimi (Nat-Network Adress Translation)

Günümüzde iç ağların hemen hepsi tahsisli olmayan IP numaraları (10.0.0.0, 192.168.0.0 vs.) kullanır. Bu IP numaraları internet üzerindeki router (Yönlendiriciler) tarafından bilinmez. Dolayısıyla bu ağlardan internetteki herhangi bir makineye bir erişim olduğu zaman internetteki makine bu ağa nasıl geri döneceğini bilmez ve pratikte iletişim yapılamaz. Güvenlik duvarı ise dinamik veya statik olarak internette bilinen ve kendisine yönlendirme yapılabilen bir IP numarasına sahiptir. İç ağdaki makinelere erişim sağlayabilmek için güvenlik duvarı, kendisine iç ağdan gelen her paketin kaynak adresini kendi adresi olarak değiştirir. Kendisine internetten gelen paketlerin de hedef adresini iç ağdaki ilgili makinenin adresi olarak değiştirir ve bu yolla iç ağdaki makinelerin, internet üzerindeki makinelerle haberleşmesini sağlar. Bu işleme IP Masquerade (Maskeleye) veya NAT - Network Address Translation (Ağ Adres Çevrimi) denir.

2.4.5.4. Stateful (Dinamik) Filtreleme

Eskiden filtreleme yöntemleri ağırlıklı olarak statikti. Yani genel olarak ağınıza ICQ paketlerinin girmesine izin verip vermeme kararı söz konusuydu. Aradaki fark, paketin sırf protokolüne bakarak karar vermek yerine, güvenlik duvarının bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Yani bir telnet bağlantısında her iki taraftan da paketler gelir ve gider. Fakat dinamik filtreleme ile bir telnet bağlantısı iç ağımdan başlatılmışsa izin verir. Başlangıç istemi dış ağdan gelmişse reddedebilirsiniz. Dinamik filtreleme özelliği olmayan güvenlik duvarlarının kullanılması önerilmez.



Şekil 2.69: Dinamik paket filtreleme mantığı

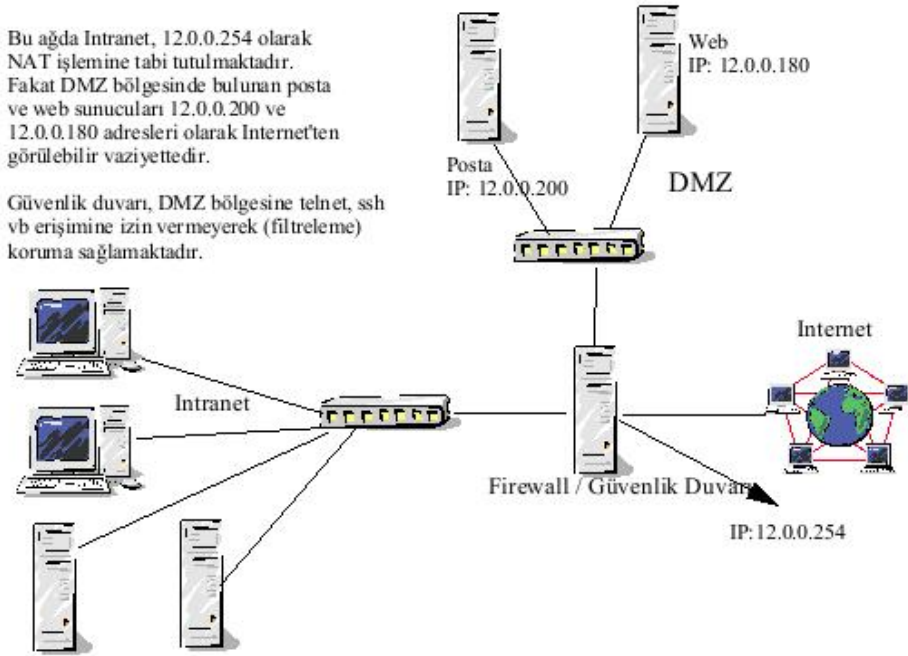
Şekil 2.69’da dinamik paket filtreleme sisteminin nasıl işlediği görülmektedir. Dikkat edilirse; Statik filtrelemede ve Dinamik filtrelemede, PC’nin istekleri değişmezken, Dinamik filtrelemede farklı olarak dosya sunucusunun kaynak portu 20/TCP olan paketi engellenmektedir.

2.4.6. Silahsızlandırılmış Bölge (Dmz – Demilitarized Zone)

Ağınızda internetten erişimi olması gereken web, posta gibi sunucular bulunabilir. Bu sunuculara erişimi iki yoldan vermeniz mümkündür:

Silahsızlandırılmış bölge uygulaması (DMZ - Demilitarized Zone) çağınızda bu servislere doğrudan filtreleme yaparak.

DMZ, güvenlik duvarı tarafından daha az korunan, daha fazla erişime izin verilen bir bölgedir. Güvenlik duvarına üçüncü bir ağ çıkışı eklenmesi ve internete servis verecek olan makinelerin buraya konması ile oluşturulur. Örneğin DMZ’deki makinelere NAT uygulanmayabilir, tahsisli IP numaralarına sahip olabilir. Güvenlik duvarı, telnet gibi kimi protokollerin buraya erişimini filtreleyerek DMZ bölgesindeki makinelere güvenlik sağlar. Dikkat edilecek nokta, DMZ’de bulunan makinelerin daha fazla erişime (Dolayısıyla saldırıya) açık olmasıdır. Buradaki makineler dikkatli kurulmalı, güvenliğe aykırı protokoller vs. burada yer almamalıdır.



Şekil 2.70: Silahsızlandırılmış bölge (DMZ) mantığı

2.4.7. Doğrudan Filtreleme

DMZ oluşturmak için ek ekipman ve IP numarası gerekir. Güvenlik duvarında üçüncü bir ağ birimi, ayrı bir switch, daha fazla adette tahsisli IP numarası ve iç ağınızda başka herhangi bir görev görmeyecek olan sunucu makineler gerekir. Eldeki imkanlar buna yetişmeyebilir. Böyle durumlarda, güvenlik duvarınızdaki filtreleme politikasını değiştirerek iç ağınızdaki kimi makinelere dışarıdan sınırlı erişim imkânı verebilirsiniz. Örneğin, güvenlik duvarınız ağınızın genelinde dışarıdan gelen SMTP (Posta) protokolünü filtrelerken sadece posta sunucunuza dışarıdan SMTP protokolü erişimini verebilir. NAT ile birleştirileceğinden bu sanki güvenlik duvarınız posta sunuculuğu yapıyormuş izlenimini verir.

2.4.8. Zonealarm Güvenlik Duvarı Programı

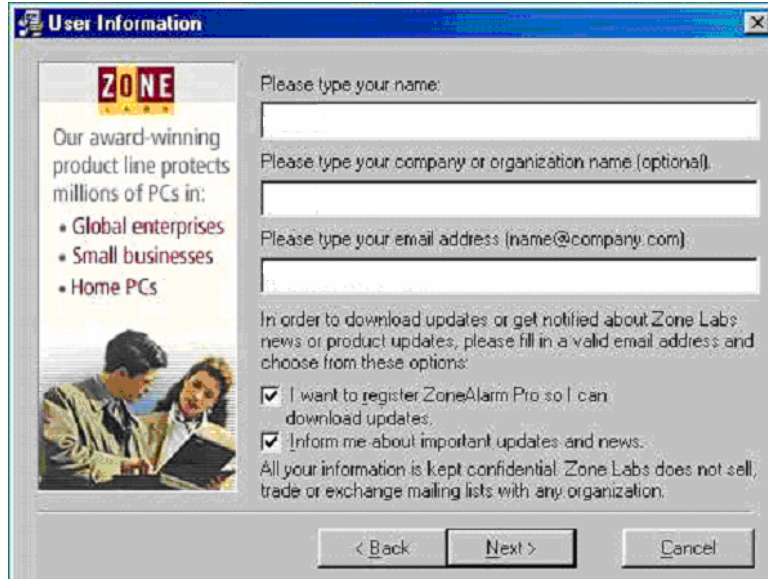
2.4.8.1. Zonealarm Güvenlik Duvarı Programının Kurulumu

Zonealarm programı, alanında en popüler güvenlik duvarı programlarından biridir. Programın, pop-up ve cookie kontrolü yapma, web sitelerini tarama, banner engelleme özellikleri ile birlikte antivirüs programınızla ortak bir çalışma yapabilme özelliği vardır.

Kurulumu başlamadan önce, işletim sisteminizin firewallı açıksa kapatmalısınız. Disk ya da CD'de "Setup" dosyasını çalıştırınız. Ekrana Şekil 2.71'de görülen pencere gelecektir. Bu pencerede "Next" butonuna tıklatınız.



Şekil 2.71: Zone alarm programı kurulum penceresi



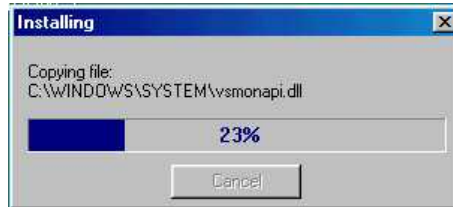
Şekil 2.72. Kullanıcı bilgileri giriş penceresi

Ekrana Şekil 2.72'deki kullanıcı bilgileri giriş sayfası gelecektir. Adınızı, soyadınızı ve e-mail adresinizi yazınız. Eğer kayıtlı kullanıcı olmak ve güncelleştirmelerden haberdar olmak istiyorsanız kutuları işaretleyiniz. Bilgilerinizi girdikten sonra "Next" butonunu tıklayınız.



Şekil 2.73: Lisans sözleşmesi

Ekrana Şekil 2.73'teki Lisans Sözleşmesi sayfası gelecektir. Bu pencerede “ I accept the terms of the preceding License Agreement.” kutucuğunu işaretlemeniz, lisans sözleşmenizi kabul ettiğiniz anlamına gelir. “Install “ butonunu tıklayarak kurulum işlemi başlatınız. Bu işlem başlayınca Şekil 2.74'teki dosya kopyalama penceresi ekrana gelecektir.

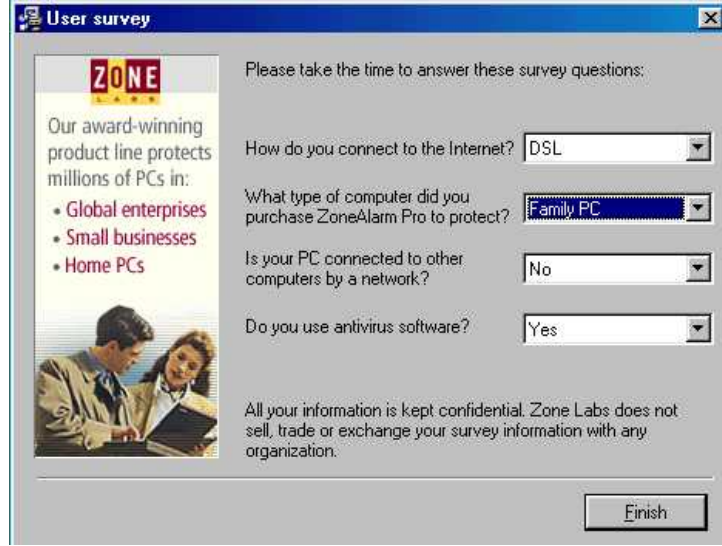


Şekil 2.74: Kurulum başladı... Dosyalar kopyalanıyor

Dosyaların kopyalanması işlemi tamamlandığında Şekil 2.75'teki pencere ekrana gelir. Bu pencerede kullanıcıya aşağıdaki sorular sorulmaktadır:

- İnternete bağlantı şekliniz
- Satın aldığımız programı kullandığımız bilgisayarın tipi
- Bilgisayarın bir ağa (networke) bağlı olup olmadığını
- Antivirüs programı kullanıp kullanmadığınızı

Bu sorulara karşılık, kendi durumunuza uyan seçenekleri işaretleyin ve Finish butonunu tıklayınız...



User survey

Please take the time to answer these survey questions:

How do you connect to the Internet?

What type of computer did you purchase ZoneAlarm Pro to protect?

Is your PC connected to other computers by a network?

Do you use antivirus software?

All your information is kept confidential. Zone Labs does not sell, trade or exchange your survey information with any organization.

Şekil 2.75: Kullanıcının kullandığı sistem ile ilgili sorular

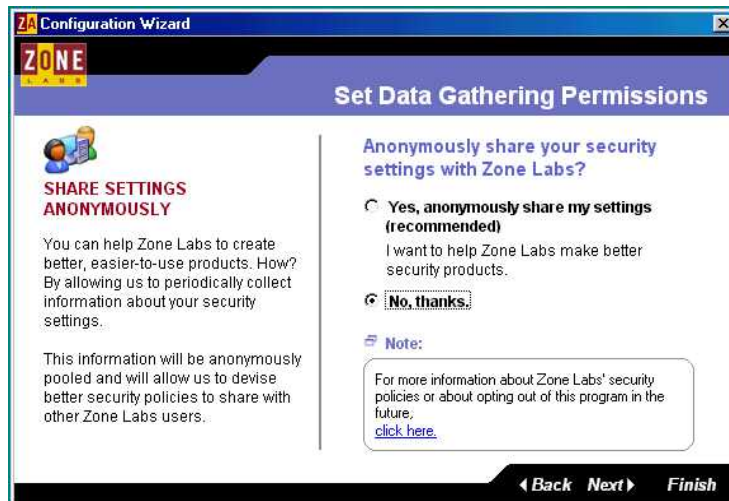
ZoneAlarm programı bilgisayarımıza kurulmuş oldu. Şekil 2.76’da görülen “Kurulum Tamamlandı” penceresinde ZoneAlarm programını çalıştırmak isteyip istemediğimiz soruluyor. “Yes” butonunu tıklayarak programı çalıştırıyoruz.



ZoneAlarm Pro Setup

Setup is complete. Do you want to start ZoneAlarm Pro now?

Şekil 2.76: Kurulumun tamamlandığını gösteren pencere



ZA Configuration Wizard

ZONE

Set Data Gathering Permissions

SHARE SETTINGS ANONYMOUSLY

You can help Zone Labs to create better, easier-to-use products. How? By allowing us to periodically collect information about your security settings.

This information will be anonymously pooled and will allow us to devise better security policies to share with other Zone Labs users.

Anonymously share your security settings with Zone Labs?

Yes, anonymously share my settings (recommended)
I want to help Zone Labs make better security products.

No, thanks.

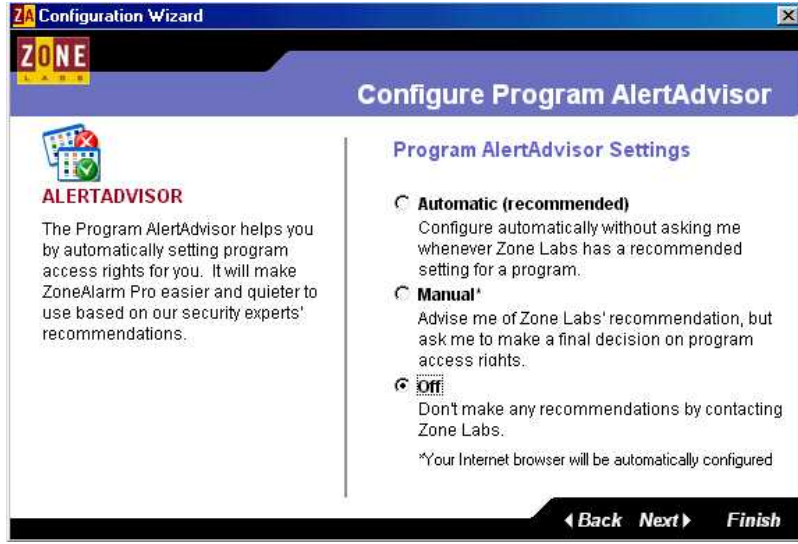
Note:

For more information about Zone Labs' security policies or about opting out of this program in the future, [click here](#).

Şekil 2.77: Konfigürasyon penceresi

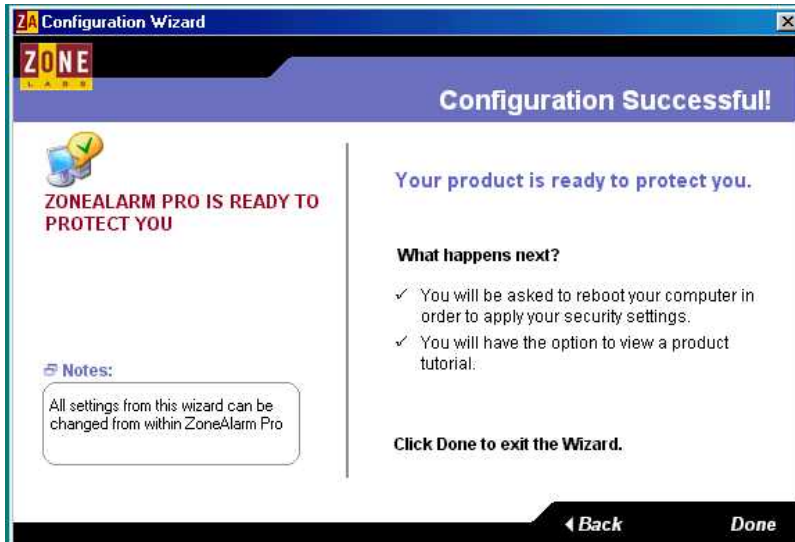
ZoneAlarm Pro programı çalıştığında ekrana lisans sihirbazı gelecektir. Lisans numaranızı girerek lisans işleminizi tamamladığınızda ekrana işlemi başarı ile tamamladığınızı ifade eden bir mesaj ekrana gelecektir.

Lisans işlemleri tamamlandıktan sonra ekrana “**Konfigürasyon sihirbazı**” penceresi gelecektir. Şekil 2.77’de görülen pencerede, size; Zone Labs ‘ ın daha güvenli programlar yapacağı gerekçesi ile “güvenlik bilgilerinizi Zone Labs ile paylaşmak istiyor musunuz? ” sorusu soruluyor. Burada “No, thanks” seçeneğini seçerek, “Next “ butonunu tıklamanız önerilir.



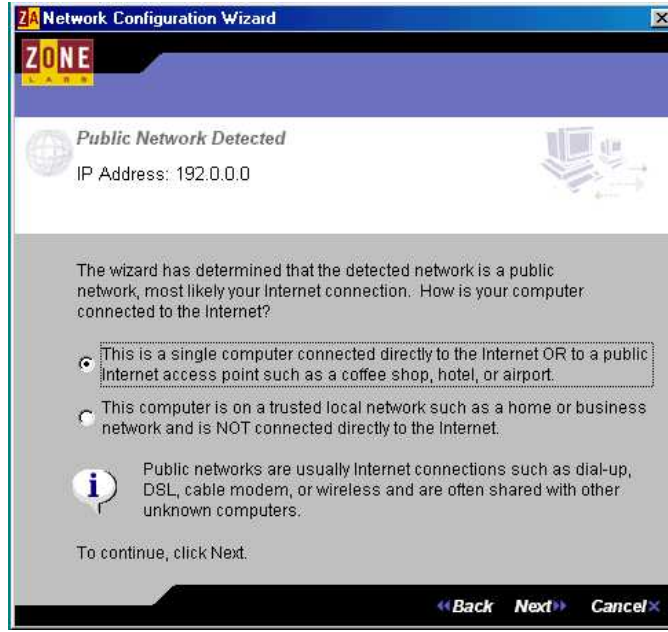
Şekil 2.78: Uyarı danışma (AlertAdvisor) penceresi

Şekil 2.78’de görülen pencere de bizden, güvenlik ayarlarını otomatik olarak değiştirebilme yetkisi istiyor. Bu pencerede “ off “ seçeneğini seçmeniz önerilir. Next butonunu tıklayınız.



Şekil 2.79: Konfigürasyon başarı ile tamamlandı

Ekrana Şekil 2.79’da görülen pencere gelecektir. Bu pencere bize konfigürasyon işleminin başarı ile tamamladığımızı göstermektedir. “Done” butonu tıklandıktan sonra yeniden başlama “Restart” işlemi yapılır. Bilgisayar yeniden başlatıldığında, ekrana Şekil 2.80’de görülen, bilgisayarımızın, ne tür bir bağlantı ile internete bağlı olduğunu soran “Network Configuration Sihirbazı” gelir.



Şekil 2.80: Network Configuration sihirbazı

Bu pencerede:

- İnternete direkt bağlanıyorsanız (dial-up, dsl, kablo) ilk seçeneği
 - Bir yerel ağ ile internete bağlıysanız ikinci seçeneği seçiniz.
- “Next” butonunu tıklayın. Bu şekilde Ağ Bıçım Sihirbazı tamamlanmış olur.

2.4.8.2. ZoneAlarm Programının Ayarları

ZoneAlarm programı, bilgisayar her çalıştığında otomatik olarak, görev çubuğuna yerleşecektir. Şimdi bu ikona çift tıklayarak ZoneAlarm ayarlarına bir göz atalım.

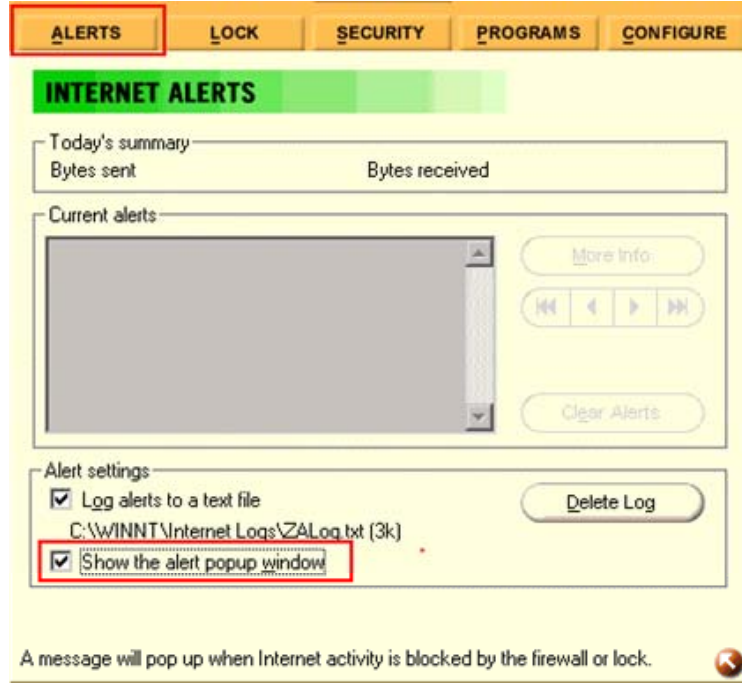


Şekil 2.81: ZoneAlarm görev çubuğunda çalışmakta...

Alerts Sekmesi: Bu pencerede, programın sizi hangi durumlarda alarm ile uyaracağını belirliyorsunuz.

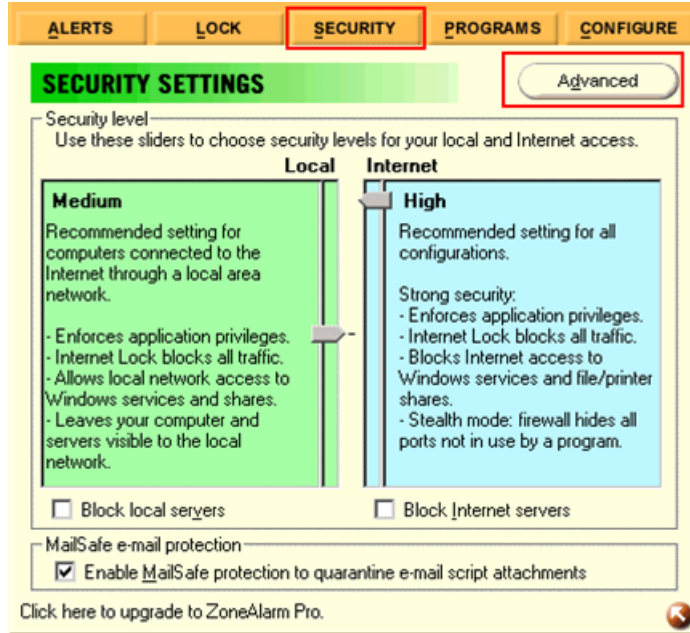
“Show Alert Pop-up Window “ seçeneđi, internet üzerinden biri, sizin bilgisayarınızda gizli bağlantı kurabileceđi açık bir port var mı diye kontrol ettiđinde; yani size port taraması yaptıđında, bir uyarı penceresi ile sizi uyarır.

İlk defa güvenlik duvarı programı kullanıyorsanız ilk başta bunu açık bırakınız. Bu taramanın ne kadar sık gerçekleştiđini göreceksiniz. Bir süre sonra iptal edebilirsiniz.

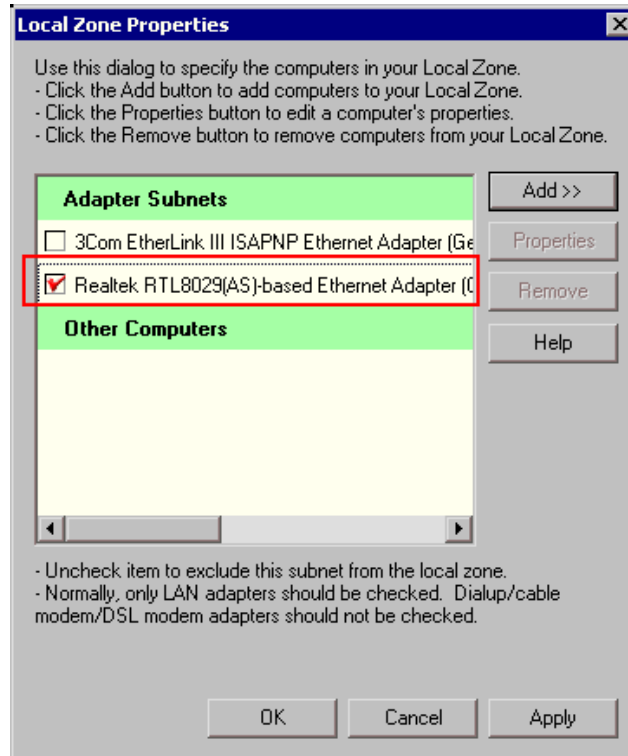


Şekil 2.82: Alerts (Alarmlar) sekmesi

Security sekmesi: Security (güvenlik) sekmesinde, internet bağlantınız ve yerel ağınız için deđişik güvenlik seviyelerinin tanımlanmış olduđunu göreceksiniz.



Şekil 2.83: Security (Güvenlik) sekmesi



Şekil 2.84. Yerel ağ özellikleri

Yerel ađınız varsa Şekil 2.84'teki "Advanced " butonunu ile ayar yapmanız şart; yoksa firewall yerel ađınızın düzgün çalışmasına engel olabilir.

Advanced butonuna tıkladığında Şekil 2.84'deki pencere ekrana gelecektir. Bu ekranda yerel ađ bağlantınızı sağlayan ađ kartını seçmeniz gerekiyor. Aksi halde ZoneAlarm yerel ađ üzerinden gelen bağlantıları da engelleyecek ve ađda kimse sizi göremeyecektir.

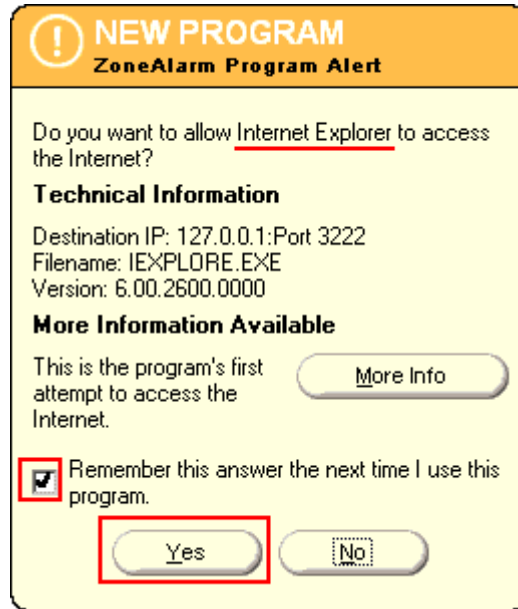
Apply ile onayladıktan sonra internete bağlanalım. Bağlantıdan kısa bir süre sonra ilk uyarı geliyor (Şekil 2.85).

Bu uyarıya göre, XP İşletim Sistemi'nin bir servisi (İnternet Explorer) internete bağlanmak istiyor. İşletim sisteminin normal bir bağlantısı olduğundan emin iseniz, bu ekranda "Yes" ile onaylayabilirsiniz. Şekil 2.85'e dikkat edilirse, alarma konu olan servis, Windows'un Internet Explorer programıdır. Yani, "Yes" ile onaylayabiliriz.

"Remember this answer the next time... " seçeneđini işaretlerseniz, bu programla ilgili seçiminizi hatırlayacak ve sizi bununla ilgili bir daha uyardırmayacaktır. Eğer kuşkulandığınız bir bağlantı ise, "No" ile engelleyebilirsiniz.

Ancak burada karmaşık bir durum var. İşletim sisteminin birçok modülü sizin bilginiz dışında internete bağlanıyor. Bunları engellemek ileride, işletim sisteminin, bazı servislerinin çalışmamasına yol açabilir. Burada yapılması gereken, bağlanmak isteyen programın, işletim sisteminin bir parçası olduğundan eminseniz, onaylayınız.

Bir süre sonra zaten bu tip tüm servisler onaylanmış olacağından, ZoneAlarm bunları hatırlayacak ve uyarı vermeyecektir.



Şekil 2.85. ZoneAlarm uyarı

Şimdi de internet üzerinden bilgisayara bağlanmaya çalışan birisinin engellendiğini söylüyor (Şekil 2.86)



Şekil 2.86. Dikkat! Davetsiz misafiri var...

Buradan More Info'ya basarsanız, sizi ZoneAlarm'ın sitesine götürecektir ve size bağlanmaya çalışan kişinin IP adresinden konumunu (En azından hangi ülkeden olduğunu) bildirecektir.

Programs Sekmesi: Bu sekmede, engellediğimiz, izin verdiğimiz, sonuçta ZoneAlarm'ın listesine girmiş programlar ve bu programlara ait erişim seviyeleri görülebilir.

ALERTS	LOCK	SECURITY	PROGRAMS	CONFIGURE
Program	Allow connect	Allow server	Pass Lock	
<input type="checkbox"/> File Transfer Program 5.1.2600.0	Local: ✓ ? Internet: ✓ ? ? ?	<input type="checkbox"/>	
<input type="checkbox"/> Generic Host Process for Win32 Services 5.1.2600.0	Local: . . . ? Internet: . . . ? ? ?	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Internet Explorer 6.00.2600.0000	Local: ✓ ? Internet: ✓ ? ? ?	<input type="checkbox"/>	

Şekil 2.87: Programlar sekmesi

2.4.8.3. Zone Alarm İle İlgili İşlemler

Hangi programın internete erişeceğinin belirlenmesi: ZoneAlarm her programda hiç çekinmeden, Pop-up aracılığıyla yönelteceği soruyla bu uygulamanın internete erişip erişemeyeceğini soracaktır. Her defasında hangi programın internete erişmeye çalıştığını ve bunun gerçekten gerekli olup olmadığını gözden geçiriniz. Örneğin; İnternet programlarının, e-posta alabilmeniz, FTP sunucularına bağlanabilmeniz gibi bütün fonksiyonlarını yerine getirebilmeleri için tam izinle çalışmaları gerekir. Ne kadar fazla programı bu düzeyde kullanırsanız, daha sonraları o kadar az şekilde ZoneAlarm tarafından rahatsız edilirsiniz.

ZoneAlarm'ın Pop-up sorularını doğru yanıtlamış olsanız dahi pek çok açık konfigürasyon seçeneğini elle değiştirmeniz gerekebilir. Ayrıca bazı programlar internet erişimlerinin engellenmesi halinde çalışmayı reddedip erişim haklarının açılmasını isteyebiliyor. Bunun için:

- Program'a tıklayarak uygulamaların listesini elden geçirebilirsiniz.

- Allow connect kısmından yerel ağ veya internet erişimi için hangi programın online bağlantıya ihtiyaç duyduğunu belirtin. E-posta programınıza ve FTP istemcilerinize erişim hakkı tanıyınız. Windows Media Player veya Real Player gibi araçlarda da bu tip sorularla sıkça karşılaşabilirsiniz. Çünkü bu çoklu ortam yazılımları, bazı codeçleri sonradan güncellemek ya da yeniden yüklemek isteyebilir.

İnternet ile Yerel Ağın ayırt edilmesi: ZoneAlarm'ın, internet ve yerel ağlar ile ilgili fonksiyonlarında çeşitli farklar vardır. Genel olarak internet ortamında daha yüksek güvenlik sağlanması gerekir. Yerel ağda orta seviyeli güvenlik önlemleri de yeterli olacaktır. Ancak ZoneAlarm hangi alanın nereye ait olduğunu ayırt etmekte güçlük çekiyor.

Bunun için, Security menüsündeki Advanced butonundan yardım alabilirsiniz. Buradan tüm önemli ağ bağlantılarının listesini elde ediyorsunuz ve yerel ağa ait olanları işaretleyebiliyorsunuz.

Örneğin NDIS (Yerel ağ kartları için varsayılan) veya ağ kartınızın adını taşıyan kaydı etkinleştiriniz. Asla PPP-Adapter veya "WAN PPP/SLIP (DSL için ideal) gibi kayıtları aktive etmeyiniz. Farklı bilgisayarları veya güvenilir alanları "Add"le diğerlerinin arasına dahil ediniz.

Pop-up pencerelerinin kapatılması: ZoneAlarm'ın sıklıkla karşınıza çıkaracağı uyarıların sizi rahatsız etmeye başlaması halinde Alerts menüsünden "Show the Alert Pop-up" seçeneğini kapatınız.

Başlat/Programlar/Başlangıç menüsündeki ZoneAlarm simgesine sağ tuşla tıklayarak kısayol özelliklerini "...\\ZoneAlarm\\zonealarm.exe" -noPop-up -no-splash" şeklinde değiştirmeniz halinde uyarı penceresi ortadan kaybolacaktır.

Sunucu hizmetlerinin bloke edilmesi ve tekrar açılması: Aynı listeden hangi programların sunucu olarak kullanılabileceğini de belirleyebilirsiniz. Ancak ZoneAlarm'da sunucu (server) özel bir kavramdır.

Bahsedilen internet iletişimi sırasında aktif şekilde veri bekleyen ve onları alan tüm programlar sunucu olarak tanımlanıyor. Güvendiğiniz FTP programına sunucu haklarını tanıyabilirsiniz. RealPlayer veya Outlook gibi uygulamalar işlevlerini tam yerine getirebilmek için aynı sunucu haklarına ihtiyaç duyacaklardır. Aynı şekilde tüm bu izinler dosya paylaşım sistemleri, messenger yazılımları ve IRC gibi chat istemcileri için de geçerlidir.

Ancak bu sunucu hakları firewall'unuzda güvenlik gediklerine neden olur. İlgili portlar açık ve tarayıcılar için uygulama çalıştığı sürece görünür olacaktır. Bu nedenle bu haklarla ilgili dikkatli olmalı ve işinizi tamamladıktan sonra onları sonlandırmalısınız.

Kritik durumlarda Security menüsündeki "Block Internet Server" seçeneği, sunucu hakları tanıdığımız bu tip programların erişimini de geçici olarak engeller.

2.4.9. McAfee Firewall 8.0

2.4.9.1.McAfee Firewall 8.0 Kurulumu

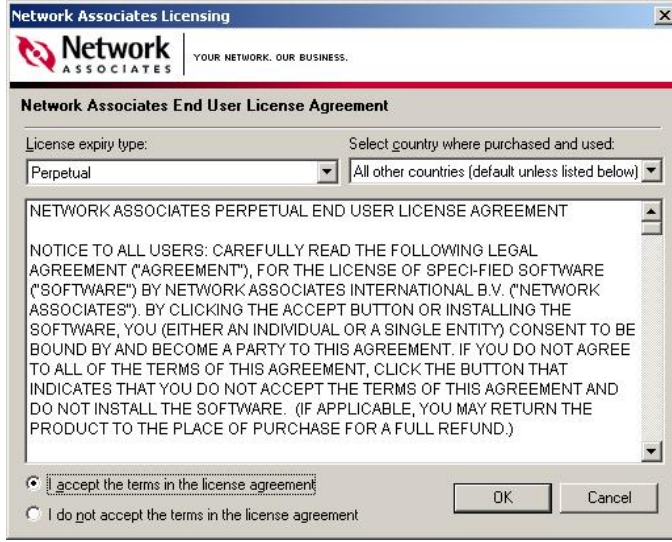
McAfee Firewall yazılımını kurabilmek ve çalıştırabilmek için gerekli en düşük donanım özellikleri şunlardır:

- Intel Pentium 166MHz işlemci
- 800 x 600 çözünürlük kapasiteli ekran (1024 X 768 önerilen)
- 32 MB disk alanı
- Windows 98 SE ya da Windows Me için 32 MB RAM
- Windows NT, Windows 2000 ya da Windows XP için 64 MB RAM
- McAfee Firewall 8.0 sürümün iki çeşidi bulunmaktadır:

Desktop Firewall: Kişisel güvenlik duvarı yazılımıdır, masaüstü PC'lerde kullanılır.

Desktop Firewall for ePo (e-policy orchestrator): Bu sürüm de kişisel güvenlik duvarı yazılımıdır, masaüstü PC'lerde kullanılır. Buna ek olarak yerel ağlarda bulunan bir bilgisayardan, güvenlik duvarı yazılımının tek bir merkezden yönetilmesine olanak tanır.

Kurulum başladıktan sonra Şekil 2.88'deki Lisans penceresi gelir. Burada, "I accept the terms in the license agreement" seçeneği seçilir ve "OK" butonuna tıklanarak kurulum devam edilir.



Şekil 2.88: Lisans sözleşmesi penceresi

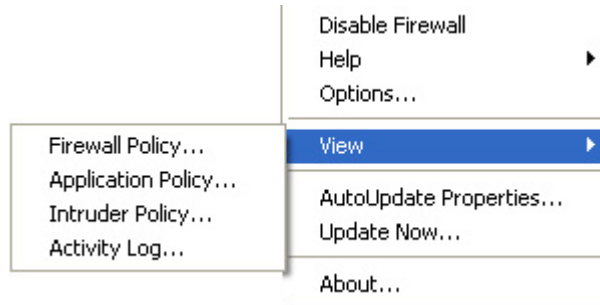
Lisans penceresinin ardından gelen dört adımda McAfee Firewall yazılımı ve kurulumu hakkında bilgi verilmekte, yazılımın kurulacağı dizin seçilebilmektedir. Varsayılan ayarlar kalacak şekilde her adımda "Next" tuşuna basarak devam edilebilir. Kurulumun tamamlanması için bilgisayarın yeniden başlatılması gerekir.

2.4.9.2. McAfee Firewall 8.0 Ayarları

Güvenlik duvarının 3 ayrı politika yapısı bulunmaktadır:

1. Firewall policy
2. Application policy
3. Intruder policy

Bu politikalara görev çubuğu üzerinde sistem saatinin yanında bulunan "McAfee Desktop Firewall" ikonu sağ tıklanınca açılan menüden ulaşılabilir (Şekil 2.89).



Şekil 2.89: Güvenlik politikalarının belirlenmesi

Firewall policy

Varsayılan deęer olarak firewall policy, koruma düzeyi "Learning Starter" olarak kurulur. Bu politikada bilgisayar hakkında bilgi toplamaya yönelik tüm ICMP trafięi filtrelenmektedir. DHCP, DNS, NTP ve kimlik belirleme servisleri trafiklerine izin verir. Hazır olarak gelen 6 politikaya ek olarak kullanıcı kendi şartlarına göre politika belirleyebilir. 6 politika sırasıyla şunlardır:

- **Minimal**
 - Bilgi toplamaya yönelik tüm ICMP trafięi filtrelenmektedir.
 - Windows paylaşımı isteklerine aynı alt ağda bulunan bilgisayarlara izin vermektedir.
 - Ağdaki dięer bilgisayarları engellemektedir.
 - Windows domain (Alan), workgroup (Çalışma grubu) ve bilgisayarları taramaya izin vermektedir.
 - Tüm yüksek port UDP trafięine izin vermektedir.
 - BOOTS, DNS, NetTime UDP trafięine izin vermektedir.
- **Client Medium**
 - İp ağ bağlantısı için gerekli tüm ICMP trafięine izin verir (Giden ping isteęi, traceroute isteęi ve gelen ICMP mesajları). Geri kalan tüm ICMP trafięini bloklar.
 - IP bilgilerine ulaşmak için gerekli UDP trafięine ve 1024 üstündeki tüm UDP trafięine izin verir.
 - Sadece altaędaki Windows dosya paylaşımlarına izin verir. Altaę dışındaki bilgisayara izin vermez.
- **Client High**
 - İp ağ bağlantısı için gerekli tüm ICMP trafięine izin verir. Ancak tüm ping işlemlerini durdurur. Geri kalan tüm ICMP trafięini bloklar.
 - IP bilgilerine ulaşmak için gerekli UDP trafięine izin verir.
 - Windows dosya paylaşımını durdurur.
- **Server Medium**
 - İstemci bilgisayarlarla iletişimi sağlayacak gerekli ICMP trafięine izin verir. Geri kalan tüm ICMP trafięini bloklar.
 - IP bilgilerine ulaşmak için gerekli UDP trafięine ve 1024 üstündeki tüm UDP trafięine izin verir.
- **Server High**
 - İstemci bilgisayarlarla iletişimi sağlayacak belirtilen ICMP trafięine izin verir. Geri kalan tüm ICMP trafięini bloklar.
 - IP bilgilerine ulaşmak için gerekli UDP trafięine izin verir.

Application policy

Varsayılan kurulumda etkinleştirilmemiştir. Güvenlik duvarını bu özelliği hangi programların çalışacağı ve hangi programın başka bir programla bağlantılı çalışacağı belirlenmesini sağlar. Etkinleştirildikten sonra varsayılan ve zamanla oluşmuş listesinde yoksa herhangi bir program çalıştırıldığında kullanıcıdan programı çalıştırma konusunda onay almadan çalıştırılmasına izin vermez. Truva atı programların bu yöntem ile yakalamak kolaylaşır.

Intruder policy

Kötü niyetli bir kullanıcı tarafından bilinçli ya da ağdaki virüs aktivitesiyle bilgisayara yapılmış bilinçsiz saldırı sonucunda güvenlik duvarı tarafından paketleri bloklanmış IP adreslerini gösterir. Belli bir süre için ya da sürekli olarak saldırgan IP bloklanabilir.

2.5. Dosya Kurtarma

2.5.1. Veri Nedir

Dosya kurtarma işlemlerine başlamadan önce dosyaları oluşturan “ veri “ mantığını kısaca açıklamaya çalışalım. Günümüzde lojik veriler “1” ve “0” lardan oluşan rakamlarla işlenir. “1” ve “0” rakamlarının her ikili kombinasyonu ise bize 1 Bit ‘lik veri sağlar. Yani “11”, “10”, “00” ve “01” ifadelerinin her biri birer Bit’tir. 8 adet Bit’in bir arada bulunması ise bir Byte’lık veriyi oluşturur. Yani, “110100001111001” 16 haneli olan bu rakam 1 Byte’lık veriyi oluşturur. Tabii ki verilerimizin neredeyse hiç biri sadece 1 Byte’tan oluşamaz. Bu durumda KB ve MB gibi yüksek orandaki Bit dizilimlerinden bahsetmek gerekiyor.

16 haneli 1 Byte diziliminden 1024 adet yan yana gelirse (yani 16384 bit) bize 1KB’lık veriyi sağlar. Hemen ardından bu rakam 1024 ve katları olarak MB, GB ve TB olarak ilerlemeye devam eder. Bir başka deyişle 1MB dediğimiz veri aslında $16384 \times 1024 = 16.777.216$ adet Bit’in bir araya gelmesiyle oluşur. Bu rakamı artık her 1024 ile çarpışınızda bir üst kademe veri birimine ulaşmış olursunuz.

Şimdi veri kaydetme, silme, hasar görme ve daha da önemlisi veri kurtarma mantığını açıklamaya başlayabiliriz.

2.5.2. Veriler Nasıl Hasar Görür

Verilerinizi tamamen kaybetmeniz ile kısmen kaybetmeniz ya da sadece hasar görmeleri arasında ufak farklar vardır. Veriler mantıksal ya da fiziksel olarak ulaşılamaz hale gelebilir. Diskinizin darbe görüp okuyucu kafanın metal plakalara zarar vermesi, tamamen fiziksel hasarlardır. Mantıksal hasarlar ise dosya yapısındaki bozukluklar, yanlışlıkla silinen dosyalar ya da yazılım hataları gibi durumda karşımıza çıkan ve hemen yukarıda açıkladığımız veri dizilimine hasar veren durumlar olarak açıklanabilir.

Hemen bir örnekle açıklayalım. Elimizde bir resim dosyası olsun ve bit dizilimi “1001111011...” olarak ifade edilsin. Bu dizilimdeki bitlerden herhangi biri kendi içinde hasar görürse ya resim hiç görüntülenemez ya da kısmen hatalı görüntülenir. Yani 1001111011 yerine ufak bir hatayla 1001111010 şekline dönüşmüş bir veri artık hasar görmüştür.

2.5.3. Verilerin Silinmesi

Bilgisayar dilinde verilerin silinmesi diye bir şey yoktur. Diskiniz üzerinde milyonlarca “1” ve “0” yuvası bulunur ve bunlar ilk formatın ardından tamamen doludur. Verilerin yazılması veya silinmesi bu yuvaların anlamlı olarak doldurulması ya da kasıtlı olarak değiştirilmesidir.

Veri yazmayı anlamak zor değil; fakat veri silmek oldukça farklı bir konudur. Disk gibi veri depolama aygıtlarından veri silmek demek o verinin adresini ve başlık verilerini kasıtlı olarak ve “boş” geçecek şekilde değiştirmek demektir.

Tamamen örnekleme amaçlı bir ifadeyle anlatmaya çalışalım. 1001111011 yine bizim resim dosyamız olsun ve biz bunu silelim. Silme işleminden sonra disk üzerindeki manzara _____ böyle bir boşluk olmayacak aksine 0011111011 gibi artık burada istenen bir veri olmadığını ve üzerine yeni veriler yazacağını sisteme ifade eden bir değişiklikle o veri orada durmaya devam edecektir.

2.5.4. Veri Kayıpları İle Karşılaşmayı Engellemek İçin Alınacak Temel Önlemler

➤ Elektriki Koruma

Veri kaybı nedenleri arasında önemli nedenlerden biri olan bilgisayardaki elektrik arızaları çoğunlukla önlenemez. Bildiğiniz gibi elektrik şebekesi 50Hz, 220 Volt AC gerilim ile bilgisayarınızı besler. Bu gerilim bilgisayar içindeki 'Güç Kaynağı' ile bilgisayarınızın elektronik bileşenlerinin kullanabileceği 5V 12V gibi değerlerde doğru gerilime (DC) çevrilir.

Öncelikle bilgisayarınızın tükettiği güce uygun bir güç kaynağı (PSU) kullanmak gerekir. Günümüzde, gelişen işlemciler, ekran kartları, DVD/CD sürücüler, büyüyen sabit diskler alışlagelmiş güç tüketimlerinden daha fazlasına ihtiyaç duymaktadır. Bilgisayarınız 350Watt bir güç kaynağı ile sorunsuz çalışırken, yeni ekran kartınız ile bilgisayarınız açılmayabilir veya zarar görebilir.

Bilgisayarınız kısa süreli elektrik gidip gelmelerinde zarar görebilir. Bir Kesintisiz güç kaynağı (KGK-UPS) kullanarak bu olasılığı azaltabilirsiniz.

Arızaların çoğu topraklama hatası, yüksek voltaj, düşük voltaj, bilgisayar aksamının yanlış montajı vb. basit bir şekilde önlenebilecek hatalardan oluşmaktadır. Daha dikkatli davranarak bunlara engel olabilirsiniz.

Voltaj sorunlarına karşı mutlaka güç kaynağı ve darbe önleyiciler kullanın. Ancak unutmayınız ki bunların kullanılması arıza riskini azaltır, tamamen ortadan kaldırmaz.

➤ Veri güvenliđi

Önemli dosyalarınızı belli aralıklarla yedekleyin ve yedeklerinizi mutlaka kontrol ediniz. Yapılan her yedekleme istediđiniz sonucu vermeyebilir. Yedekleme yaptığınız ortamın asıl kullandığınız ortam (Sabit disk) olmamasına dikkat ediniz. Yedeklerinizi, eski yedeklerin üzerine almayınız, birkaç yedek seti oluřturunuz. Böylece yedeklerinizde olabilecek bozulmalarda, bir önceki yedeđinizden yararlanabilirsiniz.

Veri güvenliđi için en basit çözüm, harici USB2.0 ve/veya Firewire bađlantısı ile kullanılan taşınabilir disk kutuları kullanmaktır.

Bilgisayarınızda bir RAID çözümü kullanmak düşündüğünüzden çok daha fazla güvenliđi size sağlayabilir. Bu yöntemde, kullanılacak RAID tekniđine göre disk(ler) ekleyerek disklerden birini tamamen kaybetmeniz bile verilerinizi güvenli bir şekilde bütün olarak korunmuş olur. Burada dikkat etmeniz gereken önemli konulardan biri, anakart üzerinde gelen RAID olanaklarını kullanmanız durumunda, anakartın deđiřtirmek zorunda kalırsanız, yeni anakartta farklı bir çip-set kullanılması durumunda verilerin kullanılmaması ve RAID'in çalışmamasıdır. Eđer verileriniz sizin için kritik bir önem taşıyorsa, ek bir RAID kontrol kartı kullanmanızı tavsiye edilir.

➤ Disk güvenliđi

Verilerinizin güvenliđi için sabit diskinizi belli aralıklarla hatalara karşı tarayınız, bu taramalar dosya kayıpları ve bozulmalarını en aza indireceđi gibi, olası bir fiziksel disk arızasını size önceden haber verebilecektir. Yalnız, tarama işlemi yapılırken diskinizin arıza yapabileceđi olasılıđına karşı mutlaka yedeklerinizi alınız.

Tarama işlemi yapılırken diskinizden duyabileceđiniz, garip sesler (Metal sürtmesi, tıkırtı vb.) ile işletim sistemi ve/veya donanımınızın vereceđi hata mesajları size diskinizin bozulacađı sinyallerini verir. Bu durumda diskin tamamen arıza yapmasını beklemeden deđiřtirilmesi önerilir. Hayati önem taşıyan bilgilerinizin bulunduđu bilgisayarlarınızın disklerini, ortalama kullanım sıklıđına göre 2-3 yıl da bir kez arıza olmasa bile yeni disk ile deđiřtiriniz. Bu size, fazladan bir maliyetmiş gibi görünse de, arıza durumunda verilerin kurtarılması için ödenecek para ve kayıp zamanın maliyetini hesapladıđınızda önemli oranda kazanç sağlayacaktır.



Şekil 2.90: Bozuk diskler

➤ **Fiziksel güvenlik**

Bilgisayarınızı ve sabit diskinizi sarsıntı, darbe, ısı ve nemden koruyunuz. Sabit diskler mekanik ağırlıklı aygıtlardır. Mekanik ağırlıklı aygıtlar, sarsıntı darbe, ısı ve nemden etkilenir. Bilgisayarınıza yaptıracağınız periyodik bakımlar bilgisayarınızın ısı ve nemden etkilenmesini azaltacaktır. Bununla birlikte tamir esnasında meydana gelecek darbe ve sarsıntı büyük sorunlara yol açabilir. Bu nedenle bakım yapılmadan önce mutlaka verilerinizi farklı bir ortamda yedekleyiniz. Sabit disklerin, en zorlu arızaları mekanik tabanlı arızalardır. Bunlar zaman zaman elektronik devre arızalarına da yol açar. Bu nedenle, elektronik kartın değiştirilmesi suretiyle yapılacak denemeler mekanik arızanın büyümesine ve böylece verilerin ulaşılamaz hale gelmesine neden olabilir.

Mekanik olarak daha yavaş olan diskleri (Bugünkü koşullarda 7200 rpm yerine 5400 rpm) tercih ediniz. Hızlı disklerde arıza oluşma riski artmaktadır. Yavaş diskler, erişim hızımızı yavaşlatmakla birlikte, bilgilerinizin güvenliğini arttıracaktır.

➤ **Antivirüs kullanımı**

Veri kayıplarının önemli bir kısmına virüsler neden olmaktadır. Kullandığınız işletim sistemi ne olursa olsun mutlaka güvenilir bir antivirüs yazılımı edininiz ve internet üzerinden sürekli olarak güncelleme yapınız.

➤ **Daha fazla bellek**

Sisteminizin sahip olduğu RAM ne kadar fazla olursa, sabit diske erişim de aynı oranda azalacaktır. Sistem hafızası dolduğunda, sabit disk önbellek yaratmak için hafıza olarak kullanmaya başlar. Bu durum, herhangi bir arızada veri kaybına uğrama olasılığınızı artırır.

2.5.5. Veri Kaybına Uğranıldığında Dikkat Edilmesi Gerekli Hususlar

Sabit diskinizin elektrik ve data (veri) kablolarının yerlerine tam olarak oturduğunu kontrol ediniz.

- Mümkünse sabit diski başka bir bilgisayara takarak deneyiniz.
- Sabit disk kontrol kartının sağlam olduğuna emin olunuz.
- Bilgisayarınızı tekrar başlatarak BIOS tarafından görülüp görülmediğini kontrol ediniz.
- Sabit diskten tuhaf sesler duyuyorsanız, bilgisayarınızı kapattıktan sonra kesinlikle açmayın. Her açma denemeniz sesin sebep olduğu mekanik arızayı önemli düzeyde tetikleyecektir.

2.5.6. Veri Kurtarma Mantiđı

Veri kurtarma mantıđı elbette ki buradaki birkaç satırda anlatılabilecek kadar basit deđildir. Fakat en temel mantıđı aıklamaya alıřarak veri kurtarmanın ve hata dzeltme iřleminin temelinde kknde ne olduđundan bahsedelim.

Yukarıdaki rneklere grdđnz gibi verilerin tamamı ortadan kaybolmayabilir. Bu durumda zel zmlerle hasar grmř blmler geri getirilebilir. Veri kurtarma temelleri birok durumda hata dzeltme –error correction- a uzanır.

Elektronikte her veri demetinin bir kuralı vardır. Tamamen rnekleme amalı olarak ortaya kendi varsayıđımız bir kuralı atalım. Her JPEG resim verisindeki, her 5'er birlik dizilim ardından "01" biti gelmek zorundadır ve hibir 4. bit "11" olamaz. Evet, sizin de anladıđımız gibi sık karřılařılan bir zekâ testinden hibir farkı yok. Bu gibi kurallar erevesinde analiz edilen bit (veri) dizilimindeki hatalar ve olasılıklar hesaplanarak eksik ya da hasar grmř veriler onarılabilir.

2.5.7. Dosya Kurtarma Programları

Piyasada bol miktarda otomatik veri kurtarma yazılımı mevcut. Bu tr yazılımlar veri oluřum kurallarına gre alıřır. Otomatik veri kurtarma yazılımları veri kurtarma iřlemlerinde olduka olumlu sonular vermektedir.

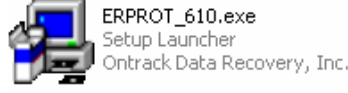
Veri kurtarma yazılımlarına rnek olarak ařađıdaki programları verebiliriz:

- EasyRecovery
- Recove My Files
- Smart Data Recovery
- Undelete My Files
- Getdata

Ontrack firmasının Easy Recovery yazılımı 1999 yılından beri ev kullanıcılarının veri kurtarma problemlerini ozmelerine yardımcı olmaya alıřıyor. En son srmn yaptıđı da farklı deđil. Bunun iin Easy Recovery ilk etapta srcleri tarayarak bulduđu blmlerin bir listesini ıkartıyor. Daha sonra istediđiniz blm seerek bulunan dosyaların listelenmesini sađlayabiliyor.

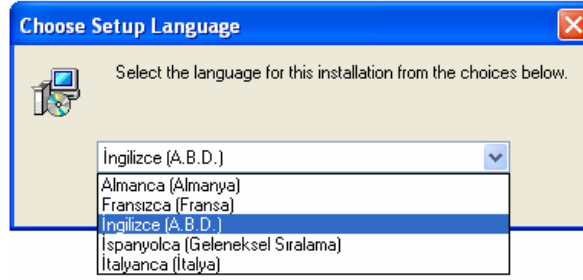
2.5.7.1. Easyrecovery Professional 6.1.0 Programının Kurulumu

Programın aşağıdaki kurulum “Setup” dosyası çift tıklanarak kurulum başlatılır.



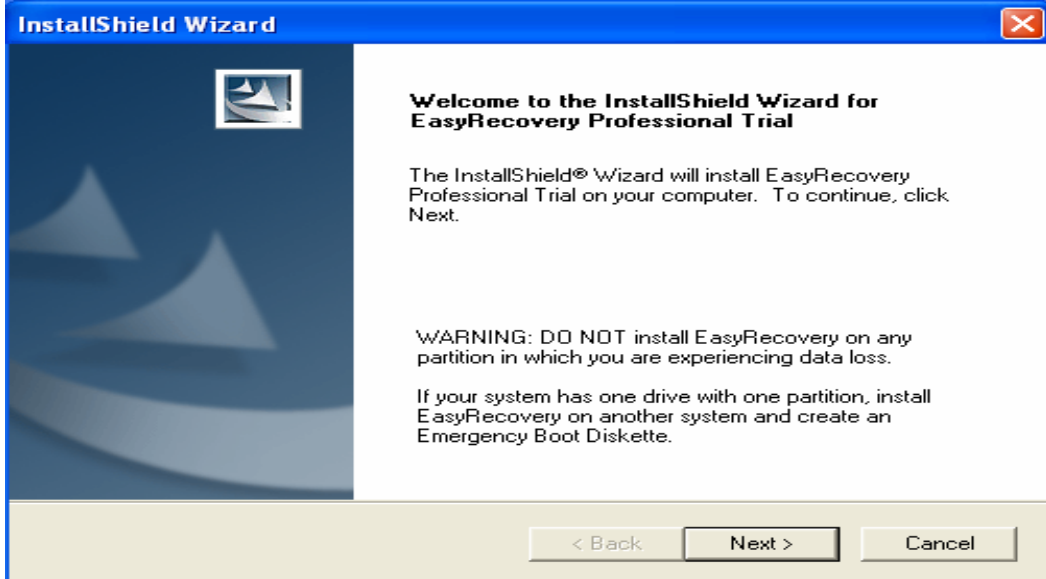
Şekil 2.91: EasyRecovery Pro 6.1.0 kurulum dosyası simgesi

Aşağıdaki pencereden programın kurulmasında kullanılacak dil seçeneği belirlenir.



Şekil 2.92: Kurulum dili seçme penceresi

Kurulum için dosyalar hazırlanmaya başlayacaktır. Hazırlık işlemi tamamlandığında Şekil 2.93’deki pencere ekrana gelir. Bu pencerede Next tuşu tıklanır.



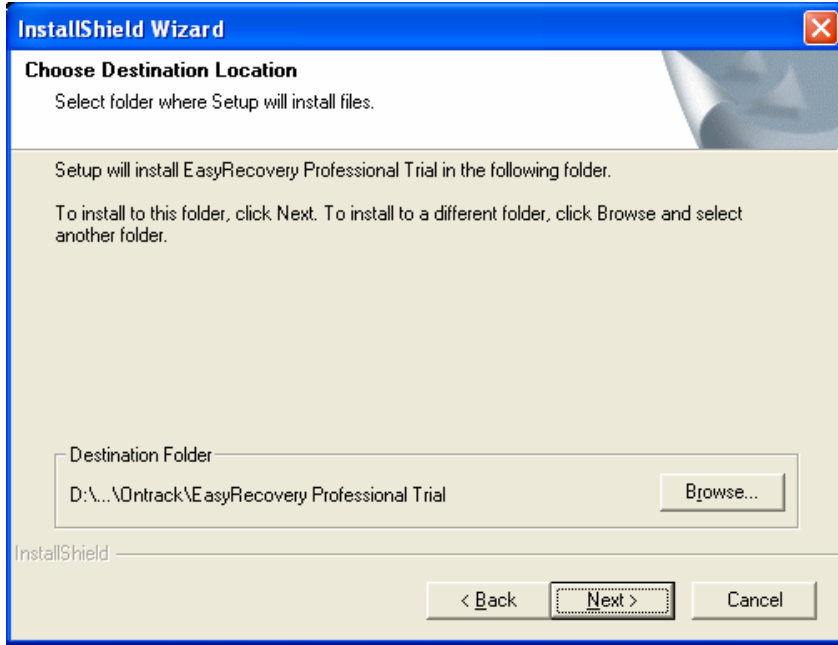
Şekil 2.93: Kurulumu başlatma penceresi

Ekrana Şekil 2.94'te görülen Lisans Sözleşmesi penceresi gelir. Bu lisans sözleşmesi kanuni olarak satın alınmış programlarda, üreticiyle kullanıcı arasında yapılan bir sözleşmedir. Kullanıcı bu sözleşme ile bu programı yasal çerçeveler içinde kullandığını kabul eder. Ancak bizim burada kurmuş olduğumuz bu program deneme (trial version) sürümüdür.



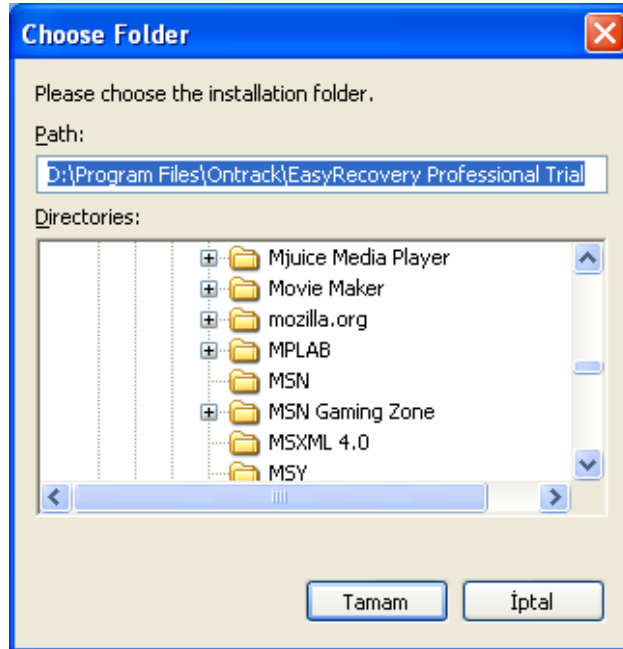
Şekil 2.94: Lisans sözleşmesi penceresi

Lisans Sözleşmesi “Yes” butonu ile kabul edildikten sonra Şekil 2.95'te görülen, programın kurulacağı dizini seçeceğimiz pencere ekrana gelir.



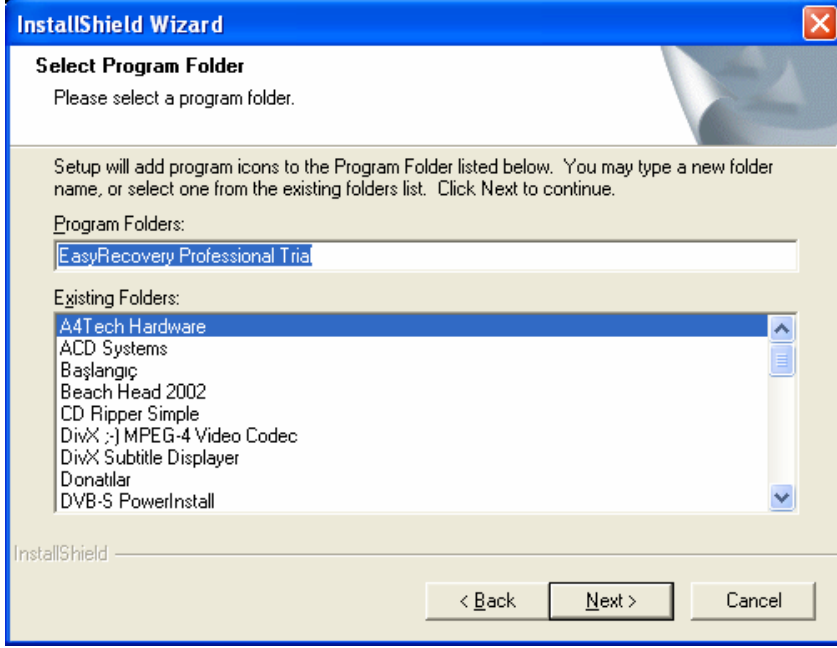
Şekil 2.95: Programın kurulacağı hedef dizinin seçimi

Eğer farklı bir dizine programı kurmak istiyorsanız , “Browse” tuşu tıklanır. Şekil 2.96’da görülen “ Dizin Seç” penceresi ile programın kurulacağı yer belirlenir.



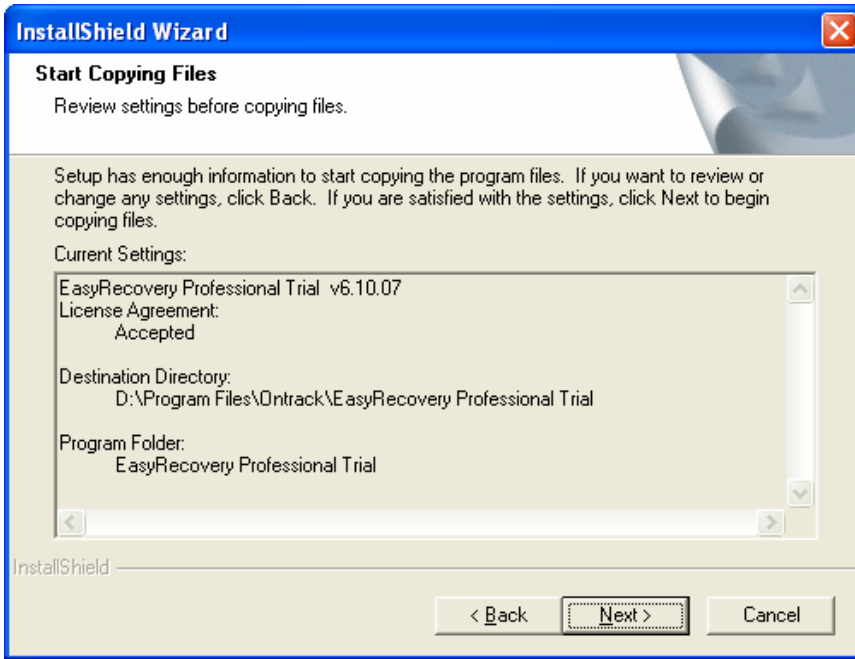
Şekil 2.96: Programın farklı bir dizine kurulması

Şekil 2.97’de görülen pencerede, programın, “Başlat” menüsünde nereye yerleştirileceği belirlenir. İstendiği takdirde, burada programın listede görünecek olan ismi değiştirilebilir.



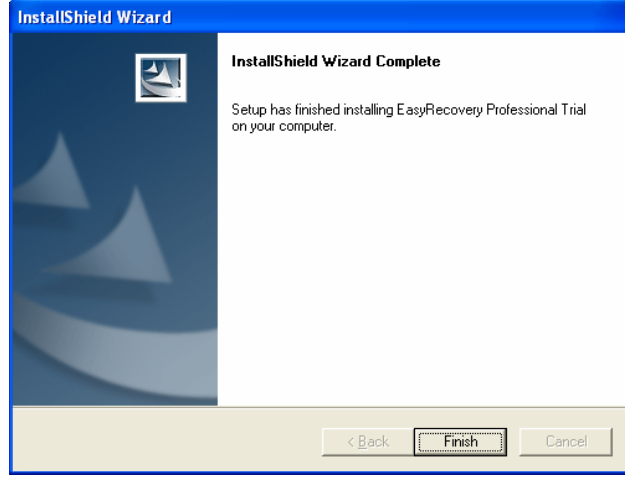
Şekil 2.97: Programın kurulacağı program grubunun seçilmesi

Şekil 2.98’de “ Next “ butonu ile kurulum dosyalarının kopyalanma işlemi başlatılır.



Şekil 2.98: Kurulum dosyalarının kopyalanma işleminin başlatılması

Kurulum işlemi tamamlandığında Şekil 2.99’da görülen pencere ekrana gelecektir.



Şekil 2.99: Kurulum işleminin tamamlandığı pencere

“ Finish “ butonu tıklanarak kurulum sonlandırılır. Kurulum işlemi bittiğinde, masaüstünde, Şekil 2.100’deki simge görülecektir.



EasyRecovery
Professional

Şekil 2.100: Easyrecovery programının masaüstündeki simgesi

2.5.7.2. Easyrecovery Professional 6.1.0 Programının Kullanımı

EasyRecovery programını çalıştırmak için masaüstünde bulunan program simgesi çift tıklanır. Ayrıca programı çalıştırmak için “ Başlat - Tüm Programlar - EasyRecovery - EasyRecovery Professional “ menüsü de kullanılabilir. Programın basit bir ara yüzü vardır. Kurtarma işlemi gayet basit birkaç işlem yardımı ile yapılabilir.



Şekil 2.101: EasyRecovery programının ana penceresi

Program çalıştığında ekrana, Şekil 2.101’de görülen ana program penceresi gelir. Silinen dosyaların veya format sonrası kaybolan dosyaların kurtarılması için programın ana penceresinde “**Data Recovery**” seçeneği işaretlenir. Ekrana Şekil 2.102’de görülen pencere gelecektir. Bu pencerede bulunan butonların görevlerine kısaca bir göz atalım.

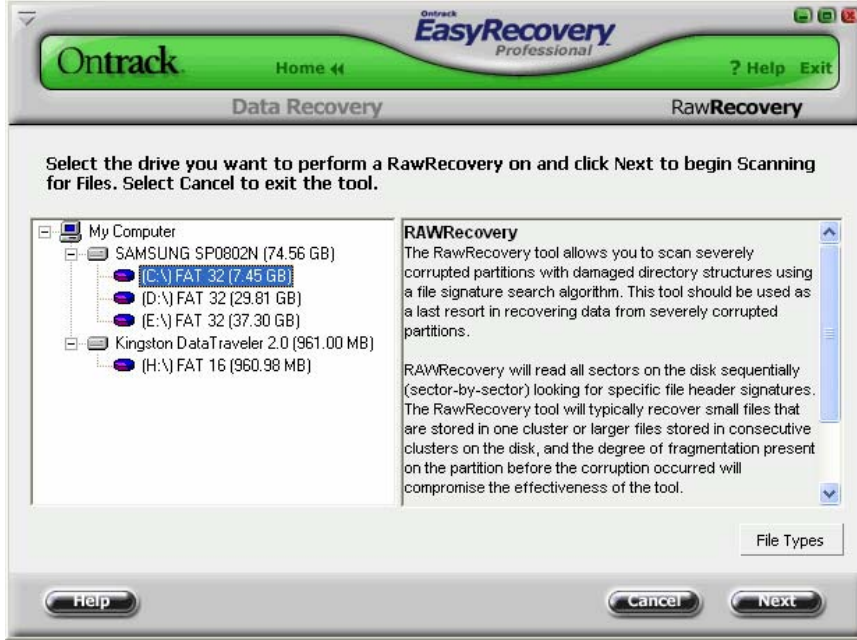
- **RawRecovery:** Silinen dosyaların kurtarılması işleminde en iyi sonuç veren seçenektir. Daha önceden belirlenmiş stratejilere göre kurtarma işlemi yapar.
- **DeletedRecovery:** Silinen dosyaların kurtarılması için kullanılır. Ancak daha kesin sonuç elde etmek için “RawRecovery” seçeneği tercih edilmelidir.
- **FormatRecovery:** Format işleminden sonra kaybolan dosyaların kurtarılması işlemi için kullanılır.
- **EmergencyMedia:** Kurtarma ve açılış disketi oluşturmak için kullanılır.
- **AdvancedRecovery:** Gelişmiş kurtarma seçeneklerini içerir. Farklı dosya sistemi içeren sistemlerde bu kurtarma işlemi kullanılabilir.
- **ResumeRecovery:** Yarım kalan kurtarma işlemine devam etmek için kullanılır. Daha önceden yarım kalan bir kurtarma işlemi “.dat” uzantılı dosya olarak bilgisayarınıza kaydedilmiştir. Bu “.dat” dosyası kullanılarak yarım kalan kurtarma işlemi kaldığı yerden devam ettirilebilir.



Şekil 2.102: “Data Recovery” penceresi

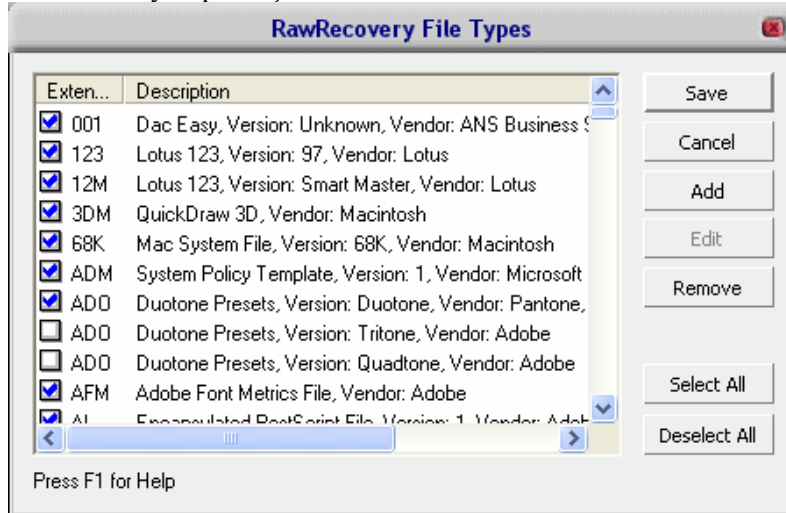
“RawRecovery” seçeneği tıklandığında, ekrana Şekil 2.103. ‘deki pencere ekrana gelir.

“RawRecovery” penceresinde, “My Computer “ kısmında kurtarma işlemi yapılacak olan disk bölümü seçilir. Ayrıca Şekil 2.103 incelendiğinde, USB flash belleklerde de dosya kurtarma işlemi yapılabildiği görülecektir.



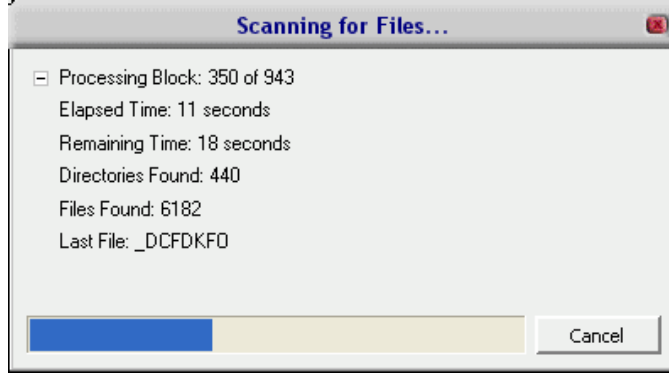
Şekil 2.103: “ RawRecovery” penceresi

Kurtarma işlemine geçmeden önce, kurtarılacak dosya tipleri belirlenmelidir. Bunun için Şekil 2.103’teki pencerede “ File Types ” butonu tıklanır. Bu buton tıklandığında Şekil 2.104’te görülen “ RawRecovery File Types “ penceresi ekrana gelir. Bu pencerede kurtarılması istenilen dosya tipleri işaretlendikten sonra “ Save “ butonu tıklanır.



Şekil 2.104: “ RawRecovery File Types ” penceresi

Örneğimizde C sürücüsünde ki kayıp silinmiş dosyaları bulmaya çalışacağız. Bunun için C sürücüsü işaretlendikten sonra “ Next “ butonu tıklanır. Program, C sürücüsündeki kayıp dosyaları taramaya başlayacaktır (Şekil 2.105).

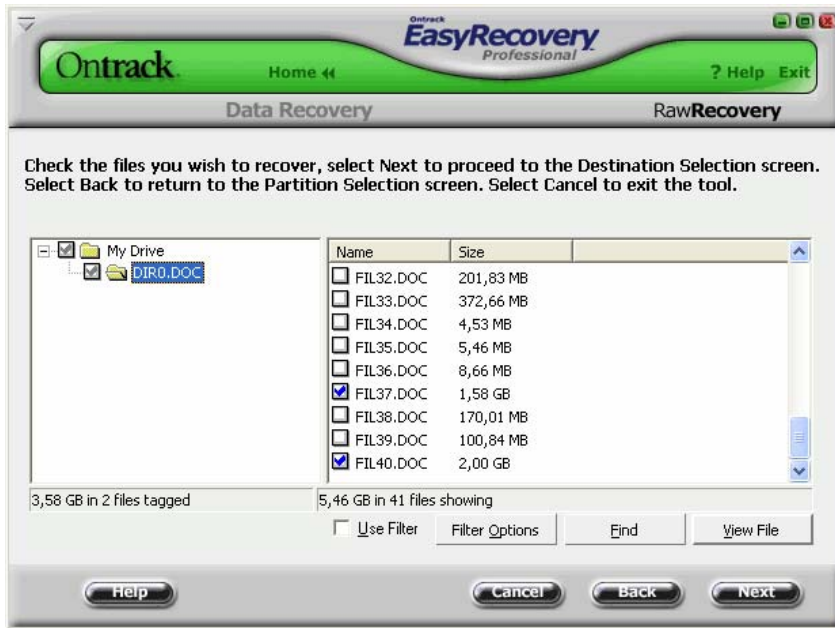


Şekil 2.105: Kayıp dosyalar taranıyor...

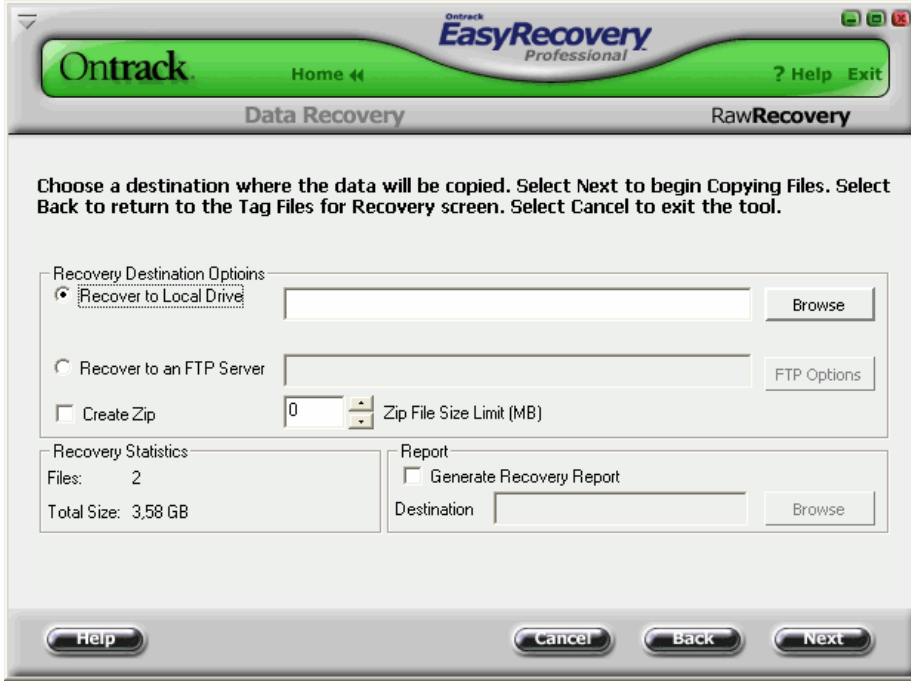
Tarama işlemi tamamlandığında, program bize silinen dosyaların bir listesini verir (Şekil 2.106). Bu listede, kurtarmak istediğimiz dosyaları işaretlememiz gerekiyor. Kurtarılabilecek dosyalar belirlendikten sonra “ Next “ butonuna basılır.

Ekrana gelen pencerede (Şekil 2.107) kurtarılabilecek dosyaların, nereye kaydedileceği belirlenir. Bunun için, “ Recovery Destination Options “ bölümünde “Recover to Local Drive “ seçeneği işaretli olmalıdır.

Bu pencerede “ Browse “ butonu tıklanarak, kurtarılabilecek dosyaların kopyalanacağı hedef dizin seçilir (Şekil 2.108).

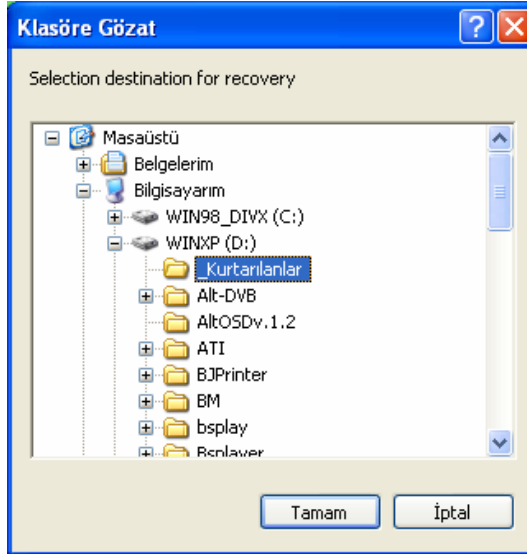


Şekil 2.106: Tarama işleminden sonra kurtarılabilmeye hazır dosyalar



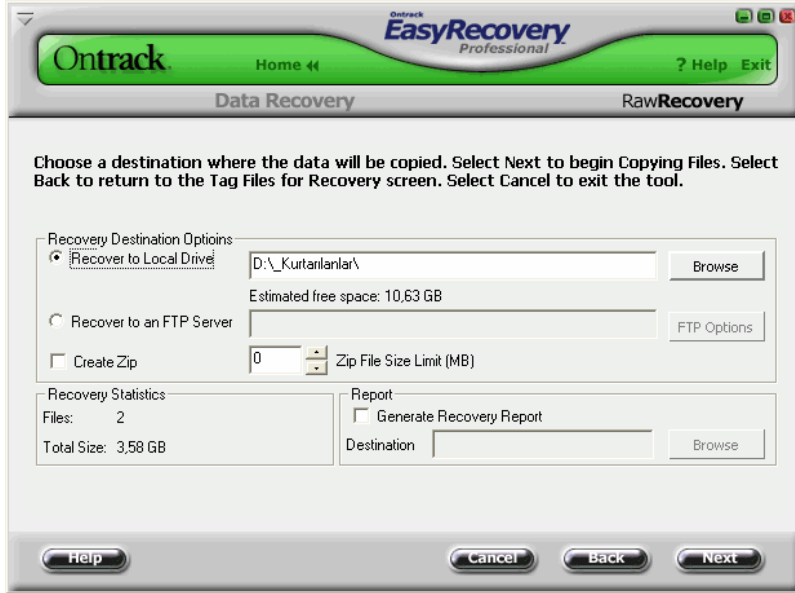
Şekil 2.107: Kurtarılabak dosyaların kaydedileceđi yerin belirlenmesi

Kurtarma işlemi için hedef dizin belirlendikten sonra ekrana Şekil 2.109'da görülen pencere gelir.



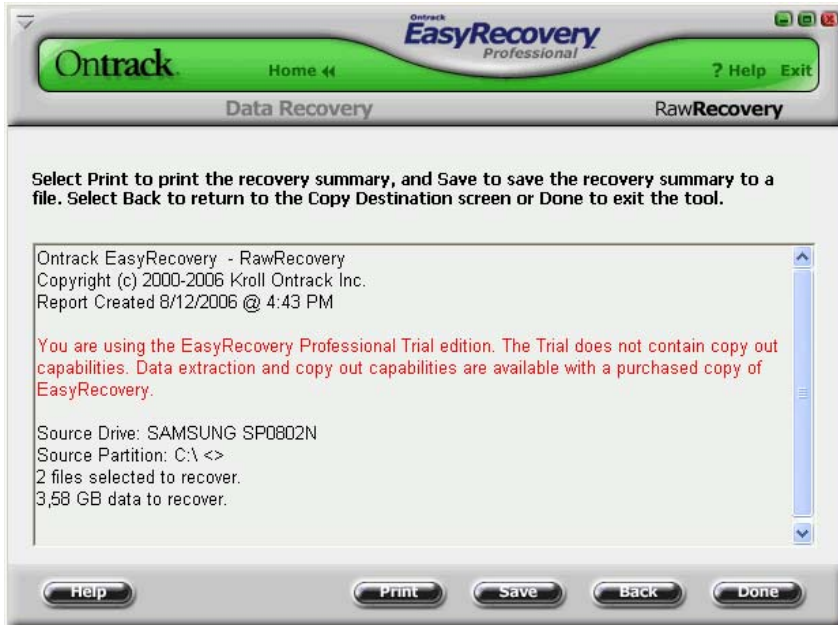
Şekil 2.108: Kurtarılabak dosyalar için hedef dizin seçiliyor...

Şekil 2.109’da görülen pencerede “Next” butonu tıklanarak seçilen dosyaların, hedef klasöre kopyalanma işlemi başlatılır.



Şekil 2.109: Dosyaların hedef dizine kopyalanması

Dosyaların kopyalanması tamamlandığında, yapılan kurtarma işlemi ile ilgili olarak bir rapor ekranda görüntülenir (Şekil 2.110).



Şekil 2.110: Dosya kurtarma işlemi ile ilgili rapor bilgisi...

Şekil 2.110'daki rapor penceresinde şu bilgiler yer alır:

- Kurtarma işleminin yapıldığı tarih ve saat (Örn: 8/12/2006 @ 4:43 PM)
- Kurtarma işlemine tabi tutulan sürücü ve sürücü kısmı (SAMSUNG, C:\)
- Kurtarılan dosyaların adedi (2 files)
- Kurtarılan dosyaların toplam boyut (3,58 GB)

Hiçbir kurtarma yazılımı, silinen dosyaların kurtarılması işleminde , % 100 sonuç vermez. Mutlaka bazı dosyalar kurtarılamayacaktır. Bunun çeşitli nedenleri vardır. Yine de yukarıda anlatılan program ve benzerleri çok olumlu sonuçlar vermektedir.

2.5.8. Bilgisayar Kullanımı İle İlgili Kurallar

Virüslerden korunma, bilgi ve programların zarar görmesini önleyici tedbirler:

- Bilgisayarın ilk açıldığında önce bir virüs taramasından geçirilerek temiz olduğundan emin olunması
- Virüs programlarının diskte yüklenmemesi, taramaların disketler yardımı ile yapılması
- Virüs olduğu tespit edilmişse temiz bir sistem disketi ile açılıp virüslerin yok edilmesi
- Virüslü olabileceği konusunda şüpheniz olan bir disketin (Başkasına ait veya daha önceden temiz olduğu araştırılmamış kendinize ait disketin) bilgisayara takılması gerekiyor ise önce virüs taramasına tabi tutulması ve temiz olduğundan emin olduktan sonra kullanılması
- Olabilecek hata veya disk bozulmalarına karşı kaybolmasını istemediğiniz program ve kütüklerinizin mutlaka en az 2 diskete yedeğinin alınması
- Kullanımına izin verilmeyen ve lisanslı olmayan programların kullanılmaması
- Bilgisayarlarda hiçbir suretle oyun oynanması ve oyun programları bulundurulması
- Programlarda ve kütüklerde hata oluşmaması için bir program çalışırken bilgisayarın kapatılmaması gerekir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
<ul style="list-style-type: none">➤ Laboratuvarınız ve çevrenizde de bulunan bilgisayarları bakım kaydı çizelgelerine uygun olarak Scandisk taraması yapınız.➤ Laboratuvarınız ve çevrenizde de bulunan bilgisayarları, bakım kaydı çizelgelerine uygun olarak Defrag - disk birleştirmesi yapınız.➤ Disklerde meydana gelmiş hataları düzeltmek için CHKDSK komutunu kullanınız.➤ Uninstall (Program kaldırma) ile bilgisayarınızdan silinemeyen program ve dosyaları REGEDIT kullanarak kaldırınız.➤ Bakım kaydı çizelgenize uygun olarak zaman zaman önemli verilerinizi yedekleyiniz.➤ Bütün bilgisayarlarınıza Antivirüs yazılımı kurunuz.➤ Antivirüs programlarınızı yeni virüslere karşı güncelleyiniz.➤ Bilgisayarları belirli periyotlarla virüs taramasından geçiriniz.➤ Bilgisayarlara yükleyeceğiniz her türlü dosya ve yazılımı virüs taramasından geçiriniz.➤ Mevcut ağınıza bir firewall aygıt ya da firewall programı kurunuz.	<ul style="list-style-type: none">➤ Disk birleştirme işlemini scandisk taraması yaptıktan sonra yapınız.➤ CHKDSK komutunu 80 GB kapasite altında bulunan diskler için kullanınız.➤ Regedit- kayıt defteri düzenleyicisini dikkatli kullanınız.➤ Kayıt defterinde yaptığınız değişiklikleri not ediniz.➤ AntiVirüs programını belirli zaman periyotlarında güncellemeyi unutmayınız.➤ Depolama birimlerinizi ısı, nem ve sarsıntıdan koruyunuz.➤ Verilerin güvenliği ve sisteminizin zarar görmemesi için bilgisayar çalışırken kasayı hareket ettirmeyiniz.➤ Lisanssız yazılım kullanmayınız.

ÖLÇME VE DEĞERLENDİRME

A- OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki cümleleri doğru veya yanlış olarak ve boşlukları doldurarak değerlendiriniz.

1. Koruyucu bakım yazılımları düzenli bir şekilde kullanıldıklarında sistem hızını ve verimliliğini artırabilir.
2. Scandisk komutu, dosya ve klasörlerin bütünlüğünü ve sabit disk fiziksel hatalar açısından tarayarak sistemin tamamını kontrol eder.
3. Scandiski çalıştırmadan önce, çalışmakta olan ve açık olan programların açık olmasında hiçbir sakınca yoktur.
4. Chkdsk /f komutu, aktif sürücüdeki hataları düzeltmesi için kullanılır.
5. Kayıt defterinde yapılacak yanlış bir düzenleme işletim sistemine hiçbir zararı olmaz. Sistem yeniden başlatıldığına normal olarak açılır.
6. Kayıt denetleyicisinde yedekleme yapmak için, Dosya-A1 seçeneği kullanılır.
7. Antivirüs programları bütün virüsleri tanır.
8. Dosya kurtarma yazılımları, fiziksel olarak zarar görmüş bir diskteki verileri kurtaramaz.
9. Antivirüs programı olan bir bilgisayara, firewall kurmaya gerek yoktur.
10. Antivirüs programları sık sık güncellenmelidir.
11. Dosya kurtarma ile kaybolan bilgilerimizin tamamını kurtarabiliriz.
12. Fiziksel olarak zarar görmüş olan diskten veri kurtarılması daha zordur.
13. Tek bilgisayarınıza veya yerel ağınıza internetten veya diğer ağlardan erişimi kısıtlayarak, bilgisayarınızı veya yerel ağınızı, internetten veya diğer ağlardan gelecek saldırılara karşı koruyan bir bilgisayar üzerindeki yazılıma verilen genel ada..... denir.
14. GETDATA programı bir programıdır.
15. Depolama birimlerini..... , ve sarsıntıdan korunmalıdır.

Cevaplarınızı cevap anahtarı ile karşılaştırınız.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

ÖĞRENME FAALİYETİ-3

AMAÇ

Bu faaliyette verilenler çerçevesinde, bilgisayar kullanıcılarının karşılaşılabilecekleri güç sorunlarını giderebileceksiniz.

ARAŞTIRMA

Bilgisayarın diğer çevre birimleri için (Çizici, Cd\DVD sürücü veya yazıcı, projeksiyon cihazı vs.) yapılacak bakım unsurlarını araştırınız. Yaptığımız incelemeleri, rapor haline getirerek sınıfta sununuz.

3. KORUYUCU BAKIM İÇİN GÜÇ SORUNLARI

3.1. Koruyucu Bakım ve Güç Sorunları

Bilgisayar sistemlerini ve tüm gerekli yan birimleri çalıştırmak için elektriğe ihtiyaç duyulsa da bu aynı zamanda ciddi sorunlara da sebebiyet verebilir. Bazı güç sorunları engellenemez; ancak hasarı en aza indirmek için önlemler alınabilir. Bu bölüm aşağıdaki konuları içermektedir:

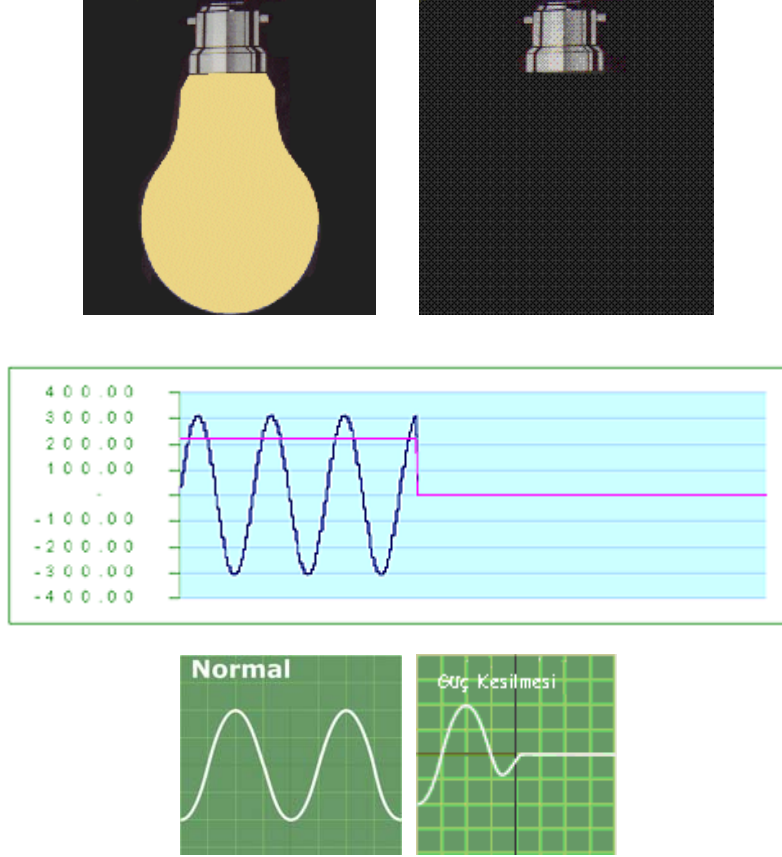
- Güç Sorunları
- Artış bastırıcılar ve güç kaynakları
- Bir sunucu ortamında UPS

3.1.1. Güç Sorunları

Bilgisayar bileşenleri, çeşitli elektriksel dalgalanmalara duyarlıdır. Hassas iç bileşenler elektriksel akıntılardan zarar görebilir. Bilgisayarlar, şimşek, yıldırım gibi yüksek düzey veya statik elektrik gibi düşük düzey elektriksel yayımlardan zarar görebilir ve harap olabilir. Aşağıda sıralanan güç kesintisi türleri, bir sistemin arızalanmasına veya hata vermesine yol açabilir.

3.1.2. Güç Kesintisi-Karartma (Blackout)

Karartma, doğal bir olay (Kötü hava gibi...) ya da insan hatasından kaynaklanan bir kaza (Örneğin, yapılandırma sırasında) nedeniyle oluşan ve belirsiz bir süre boyunca devam eden tam güç kaybıdır. Bu süre içinde sistemler kullanılamaz durumdadır.



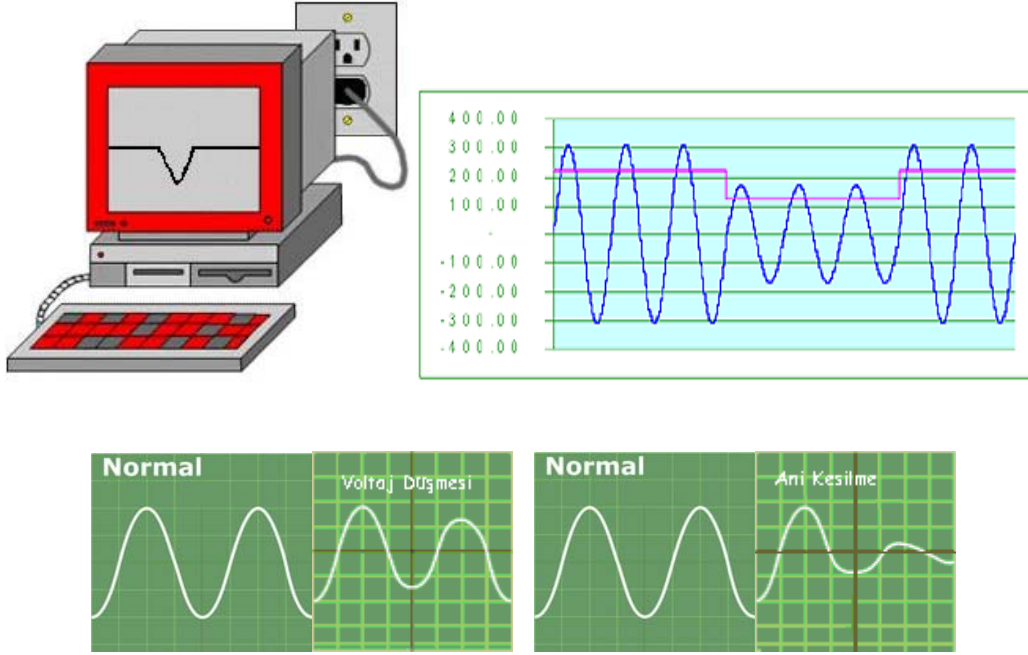
Şekil 3.1: Karartma-Güç Kesilmesi

Kesintiye genellikle aşırı ve çok fazla talep, hat üzerinde kısa devre, şimşek, deprem ve güç dağıtım şebekesi üzerindeki kazalar neden olur. Bu durumun sistemler üzerinde olumsuz etkileri olur. Çalışılmakta olan sistem üzerindeki bellekte (RAM) veya Önbellekte (Cache) bulunan işlemler ve verilerin kaybolmasına neden olur. Sabit disk üzerinde Dosya Ayırma tablosu (FAT) kaybolabilir ve sabit diskte depolanmış verilerin yok olması sonucunu ortaya çıkabilir.

3.1.3. Brownout/Sag /Ani Kesilme (Voltaj Düşmesi)

Voltaj düşmesi, Şekil 3.2'de gösterildiği gibi güçte bir düşüştür, bir ani kesilme, bir saniyeden kısa süren bir voltaj düşmesidir. Bu olaylar, güç hattındaki voltaj, normal voltajın yüzde 80 oranında altına düşmesiyle meydana gelir. **Aşırı yüklü devreler buna yol açar.**

Şirketler, yüksek talep dönemlerinde kullanıcıların sebep olduğu gücü düşürmek için kasti olarak voltajı düşürebilirler. Voltaj düşmeleri ve ani kesilmeler, elektrikle çalışan bütün aygıtları etkileyen güç sorunlarının sebebi olarak gösterilir.



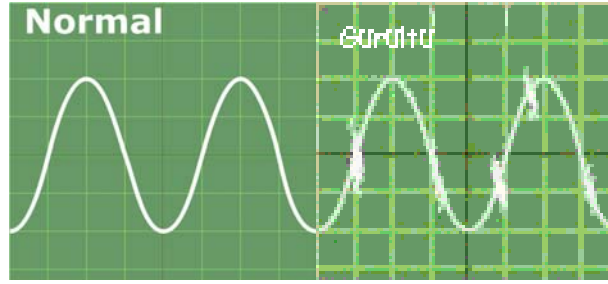
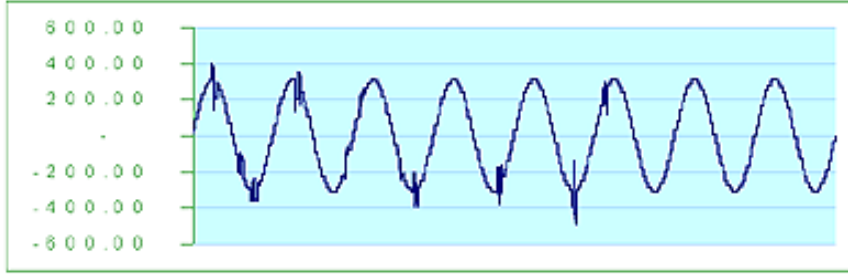
Şekil 3.2: Voltaj düşmesi ve ani kesilme

Voltaj düşmesi elektrik hatlarında kısa süreli voltaj azalmasıdır. Vakumlu temizleyiciler ve fotokopiler gibi cihazlar çalıştırıldıklarında aniden hattın voltajı düşer. Bu durum voltaj düşmesine neden olur. Voltaj düşmesi, özellikle motorların kullanıldığı CD player, DVD player gibi cihazların çalışmamasına neden olur.

Bu ani voltaj düşmesi ve kesilme bilgisayarların kapanmasına ve zarar görmesine neden olabilir. Hatta veri kayıplarına da sebep olabilir. Ayrıca voltaj düşmesi elektrikle çalışan sistemlerin ömürlerinin kısalmasına ve verimliliklerinin azalmasına da bir nedenidir.

3.1.4. Noise (Gürültü)

Gürültü, Şekil 3.3'te gösterildiği üzere, radyo yayımları (RFI), yüksek elektromanyetik girişim (EMI), hat üzerindeki bağlantılar, üreteç ve şimşek girişimlerinden kaynaklanır. Gürültü hattın, düzgün sinüs dalgasına karışır. Gürültü kalıcı ve aralıklarla devam edebilir. Gürültü, bir bilgisayar sisteminde hatalar oluşmasına sebebiyet veren kirli güce yol açabilir. Ayrıca gürültü, çalışan programlar ve veri dosyalarında hatalara ve bozulmalara neden olabilir.



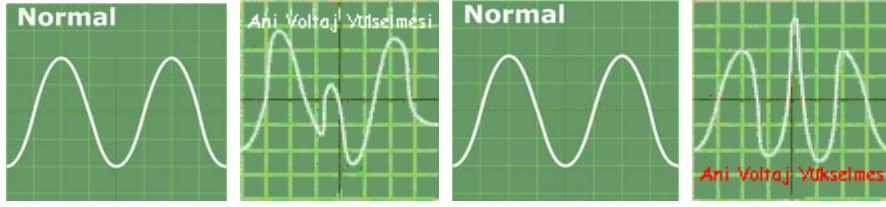
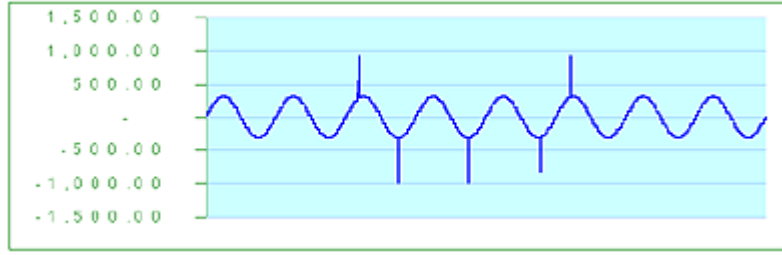
Şekil 3.3: Gürültü

Gürültü, genel olarak EMI ve RFI dalgalarından kaynaklanır. Elektriksel gürültü elektrikle çalışan devre ve teçhizatlarında ağır hasarlara neden olabilir. Gürültü, düzensiz, rasgele ve çoklu elektriksel frekans sinyalleri, orijinal elektrik sinyalini kesmesi ve bozması sonucu ortaya çıkar. Ayrıca bilgisayar sistemlerinin devreleri üzerinde sakıncalı, istenmeyen etkiler bırakır. Gürültüye sebep olan etmenler, hava ve veri kablolarına doğru yayılır(Özellikle yalıtılmamış kablolar). Bu tip veri kabloları ve antenler yayın sinyallerini üzerlerinde toplarlar. Bu istenmeyen sinyaller, iş istasyonları (workstations), sunucular ve diğer çevre birimleri arasında iletişim sinyallerine karışarak veri kabloları üzerinde geri planda gürültü yaratırlar. Özellikle HUB ve ROUTER cihazlarını etkilerler.

Çeşitli tip motorlar, motor kontrol devreleri, mikrodalgalar, şimşek, radyo ve diğer yayın alıcılar ve vericiler, flüoresan ışıklar ve hatta bilgisayarın güç kaynağı bile gürültünün ana sebepleri arasındadır.

3.1.5. Spike (Ani Voltaj Yükselmesi)

Şekil 3.4'te gösterildiği üzere, normal düzeylerin çok üstünde olan ani ve hızlı voltaj yükselmeleridir. Bir ani voltaj yükselmesi, genellikle 1-2 saniye sürer. Genellikle şimşeklerden ve statik elektrikten kaynaklanırlar ancak, yardımcı sistem bir kesintiden sonra tekrar çevrimiçi olduğunda da meydana gelebilir.

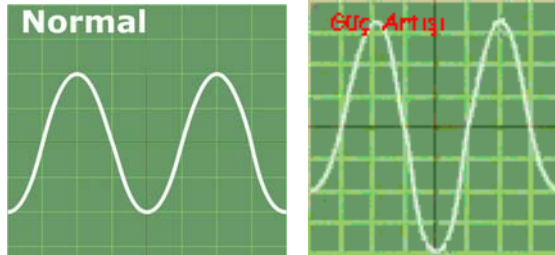
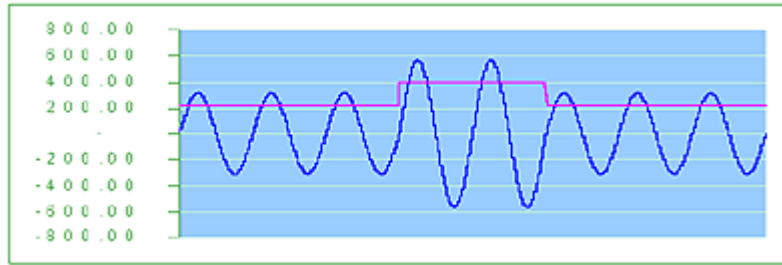


Şekil 3.4. Ani Voltaj Yükselmesi

Ani voltaj yükselmesi elektronik sistemlerin arızalanmasına neden olur. Özellikle, hassas aygıt ve cihazlar bu durumdan kaynaklanan nedenlerden dolayı kullanılamaz duruma gelebilir. Ani güç artışı bilgisayarda büyük ölçüde veri kayıplarına neden olur. Diskler üzerinde bozuk ve kayıp alanların oluşmasına neden olurlar.

3.1.6. Power Surge (Aşırı Gerilim Yükselmesi Güç Artışı)

Bir güç artışı, Şekil 3.5'te de gösterildiği üzere, elektrik akımının normal akışının üstünde olan ciddi voltaj artışıdır. Güç artışlarına ayrıca geçici voltaj (transient voltage) da denir. Örneğin, ülkemizde standart bir duvar prizi ölçümü, 220 V'dan daha yukarı bir seviyeye yükselirse bu güç artışı olarak bilinir. Bir güç artışı 3 nanosaniyeden uzun sürer. Nanosaniye, saniyenin milyarda biridir.



Şekil 3.5: Ani voltaj yükselmesi ve güç artışı

Güç artışı çok kısa bir zaman içinde aniden ortaya çıkar. Elektrikle çalışan makineler; (klimalar, Buzdolapları gibi benzer makineler elektrik gücünde aniden indirime gittiklerinde, kapatıldıklarında ani voltaj yükselmesi görülür. Bu durum da kritik ve önemli aygıt ve cihazlar üzerinde hasara neden olabilir. Diğer taraftan bellekteki bilgiler kaybolur, veri hataları görülür, güç kaynakları yanar ve iletişim sistemleri zarar görür. Artış bastırıcılar hassas bilgisayar bileşenlerini güç artışlarından korumaya yardımcı olur.

Bilgisayar sistemlerini etkileyebilen farklı güç sorunlarını anlamak sorunlara karşı koruma sağlamayı kolaylaştırabilir. Bir sonraki bölümde, bilgisayar donatımını güç sorunlarına karşı koruyan aygıtlar incelenmektedir.

3.2. Güç Kaynakları

Bu bölümde, hassas bilgisayar donatımını güç sorunlarına karşı koruyan üç farklı aygıt tanıtılmaktadır.

3.2.1. Artış Bastırıcılar ve Güç Kaynakları

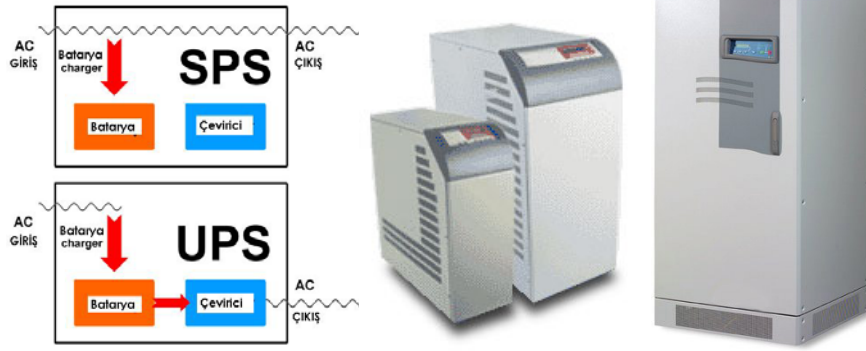
Şekil 3.6'da örnek **surge suppressor (Artış bastırıcı)** şekilleri gösterilmektedir. Artış koruyucular olarak da adlandırılan artış bastırıcılar, fazla voltajı toprağa yönlendirerek elektriksel artışlara ve ani voltaj yükselmelerine karşı koruma sağlayabilirler. Artış bastırıcılar, aşırı gerilimi yönlendirmek için, metal oksit varistör (MOV) denilen bir bileşen kullanırlar. Bir kenetleme voltajı MOV'u harekete geçirir. Voltaj en düşük seviyenin üstündeyse, MOV'a yönlendirilir ve bilgisayar bileşenlerini atlar. Bu da, bir aygıtı sağlanan voltajın belli bir seviyenin altında olduğunu garantiler. Koruyucular esasen, ani voltaj yükselmelerinin donanıma zarar vermesini önler. Ayrıca, yüksek gerilimli güç artışlarının bilgisayar donatımına zarar vermesini de engeller.



Şekil 3.6. Artış Bastırıcılar

3.2.2. Kesintisiz Güç Kaynakları

Bir uninterruptible power supply-UPS (Kesintisiz güç kaynağı), SPS'ye (yedek güç kaynağına) benzer. Ancak, bir UPS'in işleyebilmesi için akü gücüne ihtiyacı vardır. Şekil 3.7'te gösterildiği üzere, birime giren güç, aküleri, kullanılmadıklarında doldurur. Aküden gelen güç, bilgisayara AC gücü gönderen bir çeviriciye gönderilir. Bu aygıt, AC güç sorunlarına karşı koruma sağlar. Bir UPS, bir güç kesintisi durumunda kısıtlı miktarda güç sağlayabilir. UPS genellikle, çalışmanızı kaydedip çıkış yapmanızı ve bilgisayarı kapatmanızı mümkün kılacak kadar güç sağlar. Bir UPS, voltaj düşmeleri ve voltaj oynamalarına karşı da koruma sağlayabilir. Çoğu kişi, SPS'in değiştirme süresi nedeniyle, SPS yerine UPS kullanmayı tercih eder. Bir UPS, gecikmesiz sabit bir güç akımı sağlar.



Şekil 3.7: Kesintisiz güç kaynağı -Uninterruptible Power Supply- (UPS)

3.2.3. UPS Nedir, Nasıl Çalışır

UPS, elektriksel güç kaynağınız ile bilgisayar sisteminiz arasında bulunan ve bu sistemin dahilindeki bileşenleri elektrik akımındaki anormalliklerden ya da iniş çıkışlardan koruyan bir donanımdır. UPS'ler, bilgisayar sisteminizi besleyen akımın voltajdaki düşme ya da bir elektrik kesintisi sonucu azalması ya da tükenmesi halinde sisteme yedek güç sağlar. Bunun yanı sıra elektrik akımında kısa süreli ve hafif ya da uzun süreli ve yüksek artışlar şeklinde gözlenen dalgalanmalar sırasında yine UPS'ler devreye girer. UPS'ler bir anlamda, bir elektrik kesintisi durumunda sistemin normal bir şekilde çalışmaya devam etmesini sağlayarak size, üzerinde çalışmakta olduğunuz işi kaydetmeniz ve sisteminizi sağlıklı bir biçimde kapatmanız için ihtiyaç duyduğunuz zamanı verir.

Bazı UPS'ler bünyelerindeki güç kaynaklarını bir PC'ye "her zaman" enerji sağlamak için kullanırken bazıları da bu güç kaynaklarını "sadece voltaj düzensizlikleri tespit edildiğinde" devreye sokar. Yani UPS, eğer bir anormallik ya da düzensizlik göremiyorsa normal güç kaynağından (Mesela, evinizdeki ya da işyerinizdeki elektrik hattı) elde edilen akıma hiç müdahale etmez ve bu akımın direkt olarak sisteminize ulaşmasına izin verir. İdeal şartlarda, sisteminiz dahilindeki fiziksel bağlantılar üzerinde dolaşan elektrik akımı, zamanın bir fonksiyonu olarak pürüzsüz bir sinüs dalgası şeklinde davranmalıdır. UPS'lerle yapılan "güç ya da enerji düzenlemeleri" sayesinde akımın zamanın bir fonksiyonu olarak sabitliği temin edilebilir. Bu şekilde, değerli sisteminizi çeşitli dış etkenlerin yol açtığı voltaj anormalliklerinden etkin bir şekilde korumanız mümkündür.

3.2.4. Standby Power Supply (Yedek Güç Kaynağı)

Standby UPS'ler, temel yüksek voltaj korumasının haricinde bir ayarlama ya da düzenleme yapmadan, elektrik prizinin takılı olduğu duvardan çıkan elektrik akımının direkt olarak load'a (PC'niz ve çevre birimleri) ulaşmasına izin veren pasif sistemlerdir. Standby UPS'lerde bulunan elektronik dönüştürücünün devreye girmesi ve bilgisayar sisteminize ihtiyaç duyduğu AC gücünü sağlamaya başlaması için elektrik hattında bir güç kesintisi meydana gelmelidir. Elektrikler kesilmediği sürece bu elektronik dönüştürücü herhangi bir işlem yapmaz. Elektrikler var olduğu sürece aktif duruma geçmediği için kendisine "offline" dönüştürücü de denmektedir. Standby UPS 'lerden aynı zamanda offline UPS'ler olarak söz edilmesinin sebebi de budur. Elektrik hattındaki güç kesintisi sona erdiğinde, elektronik dönüştürücü aktif konumundan tekrar offline pozisyonuna geçer ve bunun üzerine UPS duvardan gelen elektrik akımının tekrar direkt olarak yüke (load'a) ulaşmaya başlamasına izin verir. Bu UPS türü PC'lerde çok kullanılır, bunun başta gelen sebeplerinden biri de fiyatlarının diğer iki UPS türünden oldukça hesaplı olmasıdır Dezavantajı ise, gerilim değişiminde devreye girene kadar 2 ila 7 milisaniye arasında bir zaman harcamasıdır.

Offline UPS Blok Diyagramı



Şekil 3.8: Standby UPS blok şeması



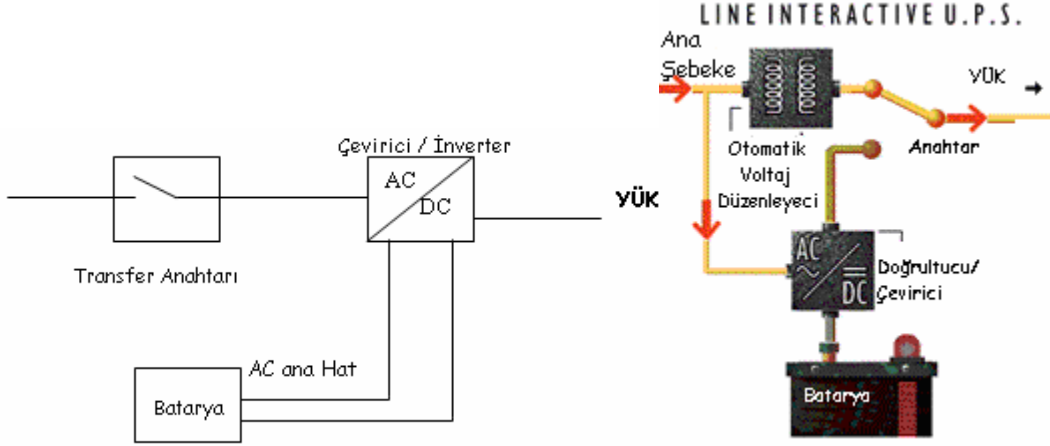
Şekil 3.9: Standby UPS (Offline UPS)

3.2.5. Line İnteractive UPS

Line interactive UPS'lerin güç temin etme ve düzenleme yetenekleri standby UPS'lerin sahip olduğu özelliklerden daha gelişmiştir. Burada, elektronik dönüştürücü duvardan çıkan AC güç hattı ile sürekli bir etkileşim halindedir. Bu sayede dönüştürücü, henüz load'a (yüke) ulaşmaya fırsat bulamadan güçteki problemden haberdar olabilir. Neticede, dönüştürücünün "sistemin o andaki ana güç kaynağı" olarak devreye girmesi çok daha hızlı gerçekleşir. Bunun bir diğer anlamı da transfer zamanının kısalmasıdır. Line interactive UPS'ler, voltajdaki iniş çıkışların sonucunda akımda meydana gelen dengesizliklerin load'a (yüke) zarar vermesini engellemek amacıyla sisteme giden akımı düşürebilir veya yükseltebilirler. Bu ürün ailesinde off-line sistemlerine ek olarak bir gerilim

dengeleme ünitesi var. Her iki tasarımın da iyi noktalarını bir araya getirdiği için bazı kaynaklarda Hybrid UPS olarak da adlandırılıyor. Bu ünitenin görevi, gerilim toleransının üstüne çıktığında sistemi sürekli olarak çalıştırmasıdır. Bu sayede herhangi bir zaman kaybı da meydana gelmez.

Line interactive UPS'ler ekipmanınız için daha güvenilir bir koruma sağlarlar. Ayrıca pil ömürleri de daha uzundur.



Şekil 3.10: Line Interactive Ups

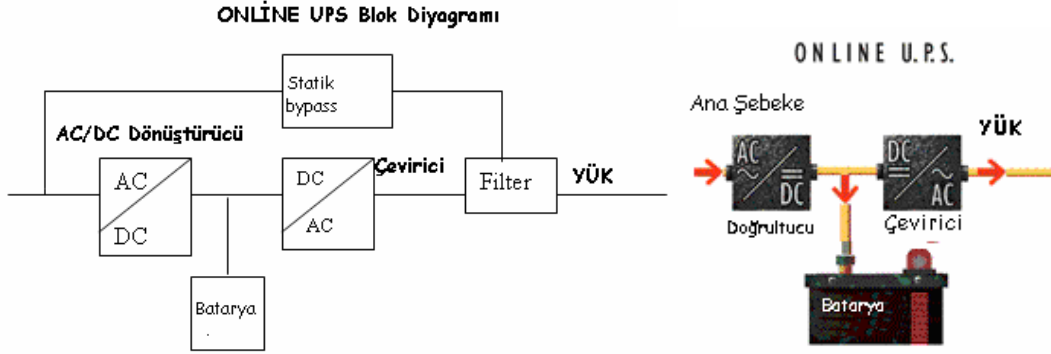


Şekil 3.11: Line Interactive Ups

3.2.6. Online UPS

Online UPS'lere gelince, bu tür UPS'lerin dönüştürücüleri "her zaman" aktiftir. Sistemin (yani load'un-yükün) ihtiyaç duyduğu elektrik akımı, UPS'in duvardaki elektrik hattından gelen akımla sürekli beslenen pillerinden sağlanır. Bu elektrik tedariki sırasında akım önce AC'den DC'ye ve sonra da DC'den tekrar AC'ye çevrilmek zorundadır. Buna "ikili dönüşüm" süreci denir. Bir elektrik kesintisi ya da güç arızası halinde, online bir UPS "Sıfır transfer zamanı"na ulaşabilme yeteneğine sahiptir (Çünkü sistemin enerjisi daima UPS pilinden sağlanmaktadır.). Online UPS'ler, korumakla yükümlü oldukları sistemin hizmetine ani varyasyonlardan uzak ve daha kararlı bir elektrik akımı sunarlar Ne var ki

online UPS'lerin de finansal önem arz eden bazı dezavantajları yok değildir. UPS pilinin sürekli kullanım halinde olması, pilin ömrünü büyük ölçüde kısaltır. Bunun yanı sıra, online UPS'ler tarafından kullanılan ikili dönüşüm süreci de daha verimsiz enerji kullanımı ve daha kabarcık elektrik faturaları gibi iki olumsuz ve ciddi sonuç doğurmaktadır.



Şekil 3.12: Online UPS blok şeması



Şekil 3.13: Örnek Online UPS 'ler

3.2.7. Regülâtörler-Power/Line Conditioner

Power/Line Conditioner ya da regülâtör, elektrik hattındaki gürültüyü filtreler ve yüksek ile düşük voltajı sabitler. Bu ürünler kapasitelerine göre oldukça pahalı cihazlardır.

Genelde, güç sorunlarına karşı en iyi korunmayı, bir güç kesintisi durumunda tüm donatımı çalıştırmaya devam edecek kadar akü gücüne sahip uygun bir biçimde topraklanmış bir bina sağlar.

3.3.Sunucu Odalarında Güç Kaynağı

3.3.1.Bir Sunucu Ortamında UPS

Bir UPS, Şekil 3.14'te gösterildiği gibi serbest veya Şekil 3.15'te gösterildiği gibi raf yapısında olabilir. UPS doğrudan güç kaynağına takılır. Sunucu ve bileşenleri daha sonra UPS'e takılır. UPS'i sunucunun üzerindeki bir kapıya bağlayan bir dizisel kablo ya da USB kablosu, ağ işletim sisteminin UPS'i görüntülemesini sağlar. Bu nedenle, sistem gücünün kesildiğini ve UPS'in akü gücü sağlıyor olduğunu bilebilir. Raf yapısında bir UPS, akülerin ağırlığı nedeniyle, genellikle bir sunucu askısında en alttaki aygıt olarak kurulur.



Şekil 3.14: Serbest UPS



Şekil 3.15: Raf yapısında UPS

UPS'i Yapılandırma

UPS görüntüleme yazılımını yükledikten sonra, ağ yöneticilerinin aşağıdaki deęiřtirgeleri yapılandırmaları gerekir:

- İstemcilere, sunucunun pil gücüyle devam ettiđini belirten bir uyarı göndermeden önce bir bekleme süresi. Bu da genellikle, gücün yeniden yüklenmesi için zaman tanımak ve anlık güç kayıplarında uyarı iletilerinin gönderilmesini önlemek için birkaç saniyedir.
- Ağ sunucusunun kapanma süreci başlamadan önce bir bekleme süresi. Genellikle birkaç dakikadır.
- Kapatma sürecinin bir parçası olarak çalıştırılacak bir program veya komutlar takımının ismi. Bu, sunucu kapatma komutunun ismi olabilir veya ağ yöneticisinin iletişim cihazına bir ileti göndermek gibi görevleri gerçekleřtiren programları içerebilir.

UPS görüntüleme yazılımı UPS'in durumunu kontrol eder. Durum öğeleri, UPS'e giren ve UPS'ten çıkan voltaj düzeyini içerir. Bazı UPS üreticileri, yöneticinin İnternet üzerinden UPS'i uzaktan yönetmesini sađlayan karmařık yazılım sađlar.

UPS'i Yükseltme

Bir UPS 'i yükseltme, UPS aküsünü değiştirmeyi veya daha büyük VA (volt/amp) değerine sahip bir UPS 'e yükseltmeyi gerektirebilir. Bir UPS yükseltmesi aşağıdaki sebeplerden herhangi birinde gerekli olabilir:

- Geçerli UPS, ağ sunucusunun uygun bir biçimde kapanması için gereken zaman boyunca güç sağlayamadığında.
- Ağ sunucusuna dahili sabit disk sürücüsü gibi güç harcayan bir donanım eklendiğinden, ağ sunucusunun güç gereksinimi arttığında.
- Bir güç kesintisi durumunda UPS ile desteklenmesi gereken donatım sayısı arttığında.

Bir UPS'i Değiştirme

Bir UPS'i değiştirmek için, ağ sunucusunun kapalı olma süresini belirlemesi ve daha sonra ağ sunucusunu kapatması gerekir. Bir UPS 'i yeniden yüklerken veya değiştirirken aşağıdaki adımları takip ediniz:

Adım 1 Ağ sunucusunu kapatınız.

Adım 2 UPS'e bağlı tüm aygıtları kapatınız.

Adım 3 UPS'i kapatınız.

Adım 4 Tüm güç kordonlarının UPS ile bağlantısını kesiniz.

Adım 5 UPS güç kordonunun güç kaynağıyla bağlantısını kesiniz.

Adım 6 UPS görüntüleme kablosunun bağlantısını kesiniz.

Adım 7 Gerekirse, UPS 'i sunucu askısından çıkarınız.

Adım 8 Yeni ya da tam olarak şarj edilmiş UPS 'i kurunuz.

Adım 9 UPS 'i güç kaynağına takınız.

Adım 10 Aygıtların güç kordonlarını, UPS tarafından desteklenmek üzere UPS 'e takınız.

Adım 11 UPS görüntüleme kablosunu bağlayınız.

Adım 12 UPS 'i açınız.

Adım 13 Ağ sunucusunu ve UPS 'e takılı diğer aygıtları çalıştırınız.

Adım 14 Ağ sunucusu üzerindeki UPS görüntüleme yazılımını yükseltiniz ve yeniden yapılandırınız.

Bir UPS yklemeden nce, pillerini Őarj etmek iin onu bir g kaynađına takınız. İlk Őarj sresi 12 saat veya daha fazladır. UPS 'in paketini zmek ve kullanıma hazırlamak iin reticinin talimatlarına uyunuz.

Varolan g kaynađının yeterli ve amperinin dođru olup olmadıđını belirlemek iin yeni UPS 'in g gereksinimini kontrol ediniz. Yeni UPS, eskisinden farklı bir g fiŐi veya grntleme kablosu gerektirmeyebilir. UPS grntleme yazılımının gncellenmesi veya deđiŐtirilmesi gerekebilir. Yeni UPS 'in eski UPS' in alanına uyup uymadıđını kontrol ediniz.

Bir UPS 'teki akler yeniden doldurulabilir. Ancak sonsuz kullanıma sahip deđildir. UPS aksnn, belli bir zaman sonra deđiŐtirilmesi gerekir. Bir UPS 'in aksn deđiŐtirmek iin UPS reticisinin talimatlara baŐvurunuz. Bazı UPS akleri deđiŐtirme iŐlemleri, ađ sunucusu alıŐıyorken ve UPS sunucuya g sađlıyorken yapılabilir. Buna pil alıŐır durumdayken deđiŐtirilebilir (hot swap) denir. Pil deđiŐimlerinin ođu UPS 'in kapalı olmasını gerektirir. UPS'in kapalı olması gerekiyorsa, pili deđiŐtirmeden nce ađ sunucusunu kapatınız.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
<ul style="list-style-type: none">➤ Güç sorunlarının nedenleri ile ilgili dikkat çekici afişler hazırlayarak kullanıcıların görebileceği yerlere asınız.➤ Güç sorunlarına karşı sistemleri koruyacak cihazlar temin ediniz.➤ Her bir sisteme bu cihazları bağlayınız.➤ Güç kaynakları ve kesintisiz güç kaynaklarının belirli periyotlarla bakımlarını yapınız.➤ Güç sorunlarına karşı herhangi bir yardımı olmayan cihazları sistemlerden çıkararak kontrollerini yapınız.➤ Akü ve bataryası zayıflamış veya bitmiş cihazların gerekli bakımlarını yaparak yenileri ile değiştiriniz.➤ Ups leri ilk kullanımlarında üretici kılavuzunda belirtilen ilk şarj süresi kadar şarj ediniz.	<ul style="list-style-type: none">➤ Şarj süresi genellikle 12-14 saat arasındadır.➤ Bakım sırasında cihazların elektrik ile bağlantılarını kesiniz.➤ UPS bakımı sırasında, UPS e bağlı çalışan cihazları UPS 'ten çıkarınız.➤ Güç sorunlarına, özellikle gürültü'ye neden olabilecek cihazları kullanmayınız.➤ Batarya ve akü değişimleri sırasında bütün güç kablolarını çıkarınız.

ÖLÇME VE DEĞERLENDİRME

A- OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki soruların cevaplarını doğru ve yanlış olarak değerlendiriniz.

1. Tam güç kaybını hangi terim tanımlar?
 - A) Ani voltaj düşüşü-Brownout
 - B) Ani voltaj yükselmesi-Spike
 - C) Kesilme-Blackout
 - D) Ani kesilme-sag
2. Hangi terim güçteki bir düşüşü tanımlar?
 - A) Kesilme-Blackout
 - B) Ani voltaj düşüşü-Brownout
 - C) Ani voltaj yükselmesi-Spike
 - D) Artış-Surge
3. Hangi terim sürekli olarak şarj edilen bir aküden faydalanan bir sistemi tanımlar?
 - A) Yedek güç kaynağı -Standby power supply- (SPS)
 - B) Kesintisiz güç fişi -Uninterruptible power plug- (UPP)
 - C) Kesintisiz güç kaynağı -Uninterruptible power supply- (UPS)
 - D) Kesintisiz güç birimi -Uninterruptible powerunit- (UPU)
4. Bir artış bastırıcı ne işe yarar?
 - A) Voltajı belli bir düzeyin altında tutar.
 - B) Daha iyi iletim için voltajı yüksek tutar.
 - C) Bir binanın tesisat boşluğunda kullanılır.
 - D) Voltaj düzeylerini aynı seviyeye getirmek için yazılımla çalışır.
5. Aşağıdakilerden hangisi hat üzerinde meydana gelen gürültü kaynaklarından?
 - A) Radyo yayınları (RFI)
 - B) Yüksek elektromanyetik girişim (EMI)
 - C) Hat üzerindeki bağlantılar
 - D) Hepsi
6. Ani voltaj yükselmesinin (Spike) sebepleri aşağıdakilerden hangisidir?
 - A) Şimşekler
 - B) Statik elektrik
 - C) Yardımcı sistemdeki bir kesinti
 - D) Hepsi
7. Aşağıdakilerden hangisi UPS çeşitlerinden değildir?
 - A) Line interactive
 - B) Power/Line Conditioner
 - C) Online
 - D) Offline

8. Aşağıdaki UPS lerden hangisi gerilim deęişiminde devreye girene kadar 2 ila 7 milisaniye arasında bir zaman harcar.
- A) Offline UPS
 - B) Online UPS
 - C) Line İnteractive UPS
 - D) Hiçbiri

Cevaplarınızı cevap anahtarı ile karşılaştırınız.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

Modül ile kazandığınız yeterliği aşağıdaki kriterlere göre değerlendiriniz.

DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayır
Çevre Birimleri İçin Koruyucu Bakım		
A) Bakım sırasında sağlık ile ilgili tedbirleri aldınız mı?		
B) Çevre birimlerine bakım kayıt çizelgesi uygun olarak bakım yaptınız mı?		
C) Koruyucu bakım önlemleri aldınız mı?		
Koruyucu Bakım İçin Gerekli Bilgisayar Yazılımları		
A) Koruyucu bakım için gerekli olan yazılımları kullanımını öğrendiniz mi?		
B) Yardımcı bakım programlarını bilgisayar üzerinde kullandınız mı?		
Kullanıcı Sorumlulukları		
A) Önemli program ve verilerin yedeğini aldınız mı??		
B) Bilgisayarlardaki gereksiz yazılımları ve programları sistemden kaldırdınız mı?		
Anti-Virüs Uygulamaları		
A) Virüs çeşitlerini öğrendiniz mi?		
B) Antivirüs programı kurup kullanımını öğrendiniz mi?		
C) Virüs temizlemeyi öğrendiniz mi?		
Firewall (Güvenlik Duvarı)		
A) Firewall nedir, öğrendiniz mi?		
B) Güvenlik duvarları neleri yapar ya da yapamaz? Öğrendiniz mi?		
C) Bir güvenlik duvarı programının kurulumu ve kullanımını öğrendiniz mi?		

Dosya Kurtarma Yazılımları		
A) Verilerin hasara uğrama nedenlerini öğrendiniz mi?		
B) Veri kayıplarına karşı alınacak temel önlemleri öğrendiniz mi?		
C) Veri kurtarma mantığını kavradınız mı?		
D) Bir veri kurtarma yazılımının kurulum ve kullanımını öğrendiniz mi?		
Koruyucu Bakım İçin Güç Sorunları		
A) Güç sorunları nelerdir, öğrendiniz mi?		
B) Güç sorunlarının ana nedenlerini öğrendiniz mi?		
C) Güç sorunlarına karşı alınacak önlemleri öğrendiniz mi?		
Güç Kaynakları		
A) Sistemleri güç sorunlarına karşı koruyan aygıtları öğrendiniz mi?		
B) UPS çeşitlerini ve özelliklerini öğrendiniz mi?		
C) Bir Bilgisayar ve çevre birimlerine UPS kurup yapılandırdınız mı?		
Sunucu Odalarında Güç Kaynağı		
A) Bir sunucu odasındaki UPS'i yapılandırmayı öğrendiniz mi?		
B) UPS 'i yükseltme ve değiştirme nedenlerini kavradınız mı?		

DEĞERLENDİRME

Yaptığınız değerlendirme sonunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır. Öğretmeninizle iletişime geçiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1 CEVAP ANHTARI

1	D
2	Y
3	D
4	Y
5	D
6	D
7	Y
8	Y
9	D
10	D

ÖĞRENME FAALİYETİ-2 CEVAP ANHTARI

1	D
2	D
3	Y
4	D
5	Y
6	Y
7	Y
8	D
9	Y
10	D
11	Y
12	D
13	Firewall
14	Veri Kurtarma
15	Isı - Nem

ÖĞRENME FAALİYETİ-3 CEVAP ANHTARI

1	C
2	B
3	C
4	A
5	D
6	D
7	B
8	A

KAYNAKÇA

- Çizgi elektronik internet sitesi
- Cisco Comptia A+ notları
- http://www.masterguard.com.tr/pdf/series_a.pdf
- <http://www.apc.com/resource/include/...sku=BF350%2DGR>
- http://www.powerware.com/EMEA/UPS/3105_specs.asp
- BYTE Bilgisayar Dergisi , Virüsler El Kitabı, Ağustos 1997
- PC LIFE Bilgisayar Dergisi, Aralık 2000, Sayfa 81,83
- PC MAGAZİNE Bilgisayar Dergisi, Aralık 1999, Sayfa 180,182,184,186
- PC WORLD PLUS, Aralık 2002, Sayfa 147
- www.symantec.com
- PC WORLD Bilgisayar Dergisi, Kasım 1999, Sayfa 100
- CHİP Bilgisayar Dergisi, Kasım 2000, Sayfa 28,30,42
- PCNET Bilgisayar Dergisi, Mayıs 1999, Sayfa 96
- ODTU Güvenlik Sayfası