T.C.
MİLLÎ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ ALANI

SİSTEM GÜVENLİĞİ

ANKARA 2008

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 öğrenme 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 Bakanlık'ta ilgili birime bildirilir.

- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşabilirler.

- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.

- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0033**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Alan Ortak**
MODÜLÜN ADI	**Sistem Güvenliği**
MODÜLÜN TANIMI	Kurulu sistemin, gelebilecek dış saldırılardan korunmasını ve herhangi bir veri kaybına karşı yedek alma yöntemlerinin tanıtıldığı öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	TCP/IP ve IP Adresleme modülünü tamamlamış olmak
YETERLİK	Sistem koruma yazılımlarını kullanarak sistemin güvenliğini ve devamlılığını sağlamak
MODÜLÜN AMACI	**Genel Amaç** Gerekli ortam sağlandığında, sistem koruma yazılımları (antivirüs, yedekleme) kullanabilecektir. **Amaçlar** ➢ Anti-virüs programını kurabilecek ve ayarlarını yapabileceksiniz. ➢ Sistemdeki verilere ait yedekleme işlemini yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Bilgisayar laboratuvarı, işletim sistemi yüklenmiş bilgisayar, antivirüs programı, yedekleme programı.
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında, o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. Modül içinde ve sonunda verilen öğretici sorularla edindiğiniz bilgileri pekiştirecek, uygulama örneklerini ve testleri gerekli süre içinde tamamlayarak etkili öğrenmeyi gerçekleştireceksiniz. ➢ Sırasıyla araştırma yaparak, grup çalışmalarına katılarak ve en son aşamada alan öğretmenlerine danışarak ölçme ve değerlendirme uygulamalarını gerçekleştirin.

GİRİŞ

Sevgili Öğrenci;

Bilgisayarlar, evimizin ve işimizin vazgeçilmez bir parçasıdır. Bilgisayarlar işlerimizi o kadar kolaylaştırıyor ki onlar olmadan işlerimizi artık bitiremez olduk. E-devlet uygulamalarının internet üzerinden yapıldığı düşünülecek olursa, internetsiz bir bilgisayarı da düşünemez hale geldik. Birbirlerine internet yolu ile bağlı bilgisayarlarımız günümüzde daha çok virüs ve saldırıyla karşı karşıya kalıyor. Kurulu bir sistemini uzun süre bozulmadan yada virüs saldırılarına uğramadan çalıştırabilen kaç kişi vardır?

Evinizi hırsızlara karşı korumak için kapılarımızı kilitli tutarız. Evimiz zemin kattaysa pencerelere demir parmaklıklar yaptırarak daha güvenli olmasını sağlamaya çalışırız. Kapımızı açılamayacak çelik kapılardan yapmaya çalışırız. Eğer evimiz dışarıdan güvenli görünüyor ise hırsızlar evimize girmek istemezler. Ne kadar güvenlikli yapmak için uğraşırsanız uğraşın bu işi meslek edinmiş uzman kişiler istemeleri halinde bir yöntemini bularak evinize girmeye başarırlar. Girmek isteme arzuları, evinizde bulacaklarını inandığı değerli eşyalarınıza göre değişecektir.

Bilgisayarımızı da ele geçirmek isteyenler öncelikle açık kapılar ararlar, sisteminizde değerli bilgiler varmı araştırırlar. Bu modüldeki amacımız, mümkün olduğunca açık kapılarımızı güvenlik altına almaktır.

Bu modül sonunda;

- Kullandığınız işletim sisteminin sürekliliği için virüs ve faaliyet şekillerini öğrenecek, korunmak için gerekli programları kurup kullanabilir hale geleceksiniz.
- Sağlıklı çalışır durumdaki işletim sisteminizin, programlarınızın herhangi bir sebeple kaybı yada saklanması gerekeceği düşünülerek, kopyalama, yedek alma, CD ye yazma ve eşkopyalama (image dosyası) işlemlerini uygulayarak öğreneceksiniz.

ÖĞRENME FAALİYETİ–1

AMAÇ

Gerekli ortam sağlandığında, sistem koruma işlemini gerçekleştiren anti-virüs programını kurabilecek ve ayarlarını yapabileceksiniz.

ARAŞTIRMA

- Bilgisayar yazılımı, bilgisayara donanımsal zarar verebilir mi? Tartışınız.

1. ANTİVİRÜS PROGRAMLARI

1.1.Antivirüs, Trojan, Antispy Yazılımları

1.1.1. Virüs, Trojan, Spy Nedir?

1.1.1.1. Virüs

Bir programın içine, kendi program kodlarını ekleyen ve çalıştırıldığı yerdeki uygun programlara da bulaşarak çoğalan, girdiği sistem ve dosyalara zarar veren program yada kod parçacıklarına **virüs** denir.

Biyolojik virüslerin başka canlılara bulaşma yolu ile çoğalma benzeşmesinden çıkılarak bu zararlı program parçacıklarına virüs ismi verilmiştir. Bir programın virüs olabilmesi için, kendisini izinsiz olarak başka programlara ekleyerek çoğalan bir işleve sahip olması gerekir. Bilgisayar virüsleri sadece program kodları ile sisteme bulaştıkları için canlılara biyolojik olarak bulaşamazlar.

Virus terimi ilk olarak 1984'te Fred Cohen tarafından hazırlanan *Experiments with Computer Viruses* (Bilgisayar Virüsleri ile Deney) adlı tez çalışmasında kullanılmış ve terimin Len Adleman ile birlikte türetildiği belirtilmiştir. Ancak daha 1972'lerde David Gerrold'e ait *When H.A.R.L.I.E Was One* adlı bir bilim-kurgu romanında, biyolojik virüsler gibi çalışan VIRUS adlı hayali bir bilgisayar programdan bahsedilmiş . Yine bilgisayar virüsü terimi, Chris Claremont'in yazdığı ve 1982 yılında basılmış *Uncanny X-Men* adlı çizgi romanda geçmiş . Dolayısıyla Cohen'in virüs tanımlaması akademik olarak ilk kez kullanılsa da terim çok önceden türetilmişti.

Elk Cloner adlı bir program ilk bilgisayar virüsü olarak tanımlanmıştır. Rich Skrenta tarafından 1982 yılında yazılan virüs Apple DOS 3.3 işletim sistemine bulaşıp disketler vasıtasıyla yayılmıştır. Bir lise öğrencisi tarafından hazırlanıp şaka olarak oyun dosyaları

içerisine gizlenmişti. Oyun, 50. çalıştırmada virüs gönderiliyor ve sonrasında boş bir ekranda Elk Cloner adlı virüs hakkında bir şiir gösterilererek görevini tamamlıyordu.

İlk PC (Kişisel Bilgisayar) virüsü **Brain** adında bir boot virüsü idi ve 1986 yılında Pakistan'ın Lahore şehrinde çalışan Basit ve Amjad Farooq Alvi isimli iki kardeş tarafından yazılmıştı. Kardeşler virüsü , resmi olarak, yazdıkları yazılımın korsan kopyalarını engellemeye yönelik hazırlamışlardı. Ancak analizciler bir tür Brain değişkeni (varyant) olan Ashar virüsünün , kodlar incelendiğinde aslında Brain'den önce oluşturulduğunu iddia etmekteler. 1990'ların ikinci yarısından itibaren makro virüsleri yaygınlaşmıştır.

Bazı virüsler; uygulamalara zarar vermek, dosyaları silmek ve sabit diski yeniden formatlamak gibi çeşitli şekillerde bilgisayara zarar vermek amacıyla programlanmışlardır. Bazıları zarar vermektense , sadece sistem içinde çoğalmayı ve metin, resim ya da video mesajları göstererek fark edilmeyi tercih ederler. Bu zararsızmış gibi gözüken virusler kulanıcı için problem oluşturabilir. Bilgisayar hafızasını işgal ederek makineyi yavaşlatabilir, sistemin kararsız davranmasına hatta çökmesine neden olabilirler. Sonuç olarak birçok virüs, hata kaynağıdır ve bu hatalar sistem çökmelerine ve veri kaybına neden olabilir.

Peki bu bilgisayar virüsleri nasıl bulaşır? Virüsün bulaşması için, virüs kodunun sistemde bir şekilde çalışır hale gelmesi gerekir. Virüsleri, bulaşma şekline göre sınıflarsak;

Dosyalara bulaşan virüsler: Bu virüslerin büyük bir kısmı çalıştırılabilen (EXE, COM uzantılı) dosyalara bulaşır. Virüs, kodlarını genellikle dosya kodlarının sonuna ekler. Dosyaya eklenen kodlar dosyanın boyutunu değiştirir (Bazı virüsler, dosya içindeki boş yerlere yazarak, dosya boyutunun değişmesini de engeller; chernobyl gibi). Dosya çalıştırıldığında virüste kendi kodlarını çalıştırırarak zarar verecek eylemlerine başlar. SYS, DRV, BIN, OVL, OVY uzantılı dosyalara bulaşan virüsler de vardır. Bazı virüsler ise yerleştikleri yerde uykuda kalarak hiçbir faaliyette bulunmaz. Virüsün aktif olacağı bir tarih vardır. Bilgisayarın sistem tarihi ile virüsün tarihi aynı güne isabet ettiğinde zarar verme işlemine başlar.

(*Örneğin CIH chernobyl virüsü 1998 de Tayvan'da çok yaygın olarak bulundu. Virüsü yazan kişi, yerel bir internet konferansında virüsü faydalı bir program diye gönderdi. Bir hafta içinde virüs, birçok ülkede bulundu. CIH virüsü, Windows95 ve Windows98 executable yani .exe uzantılı dosyalara bulaşır. Virüslü bir .exe dosyası çalıştırılıp virüs hafızada aktif olduğu zaman sistemde çalıştırılan diğer WIN95/98 .exe dosyalarına bulaşmaya çalışır. Disket, CD-ROM, internetten çekilen veya e-postanızda size gönderilen bir .exe dosyası virüslü ise ve bu .exe dosyasını çalıştırırsanız size bulaşır. Virüs sisteme yerleşdikten sonra 26 nisanda aktif hale gelerek flash bios programını siler ve bilgisayarı açılamaz hale getirir.*)

Boot sektörü virüsleri: Boot sektör, sabit diske ait tüm bilgilerin saklandığı ve bir program vasıtası ile işletim sisteminin başlatılmasını sağlayan yerdir. Boot sektörde, diskin formatı ve depolanmış verilerin bilgileriyle DOS'un sistem dosyalarını yükleyen boot programları bulunur. Disketin de boot sektörü vardır. Bir boot virüsü boot dosyalarına bulaştığında, bu disk veya disketten bilgisayar açılmaya çalışıldığında ya açılış dosyalarını bozarak bilgisayarın açılmasına engel olur yada açılışta sistemin belleğine kopyalayarak her

çalışan programa bulaşma imkanını elde eder. Sabit diskin ilk fiziksel sektörlerinde diskin Master Boot Record'u (MBR-Ana Boot Kaydı-) ve Partition (Bölüm) Tablosu vardır. Diskin MBR 'sinin içindeki Master Boot Programı partition tablosundaki değerleri okur ve boot edilebilir partition'ın başlangıç yerini öğrenir. Sisteme o adrese git ve bulunduğun ilk program kodunu çalıştır komutunu gönderir. Bu virüslere Master Boot Record Virüsleri denir.

Multi-Partite Virüsler ise Boot Sektörü virüsleri ile Master Boot Record virüslerinin bileşimidir. Hem MBR'a hemde boot sektöre bulaşır ve çalıştırılabilir dosyaları bozarak yayılırlar.
(*Örnek; Polyboot.B ve AntiEXE.*…)

Ağ Virüsleri: Mevcut yerel ağ yada internet üzerinden paylaşılan klasör, sürücü ve açık port vb. hedefleri kullanarak bulaşır. Yerleştiği açık sistemden ağdaki diğer sistemlere yayılmaya, ağı meşgul tutarak yavaş çalışmasına neden olur.
(*Örnek: Nimda, SQQLSlammer*…)

Makro Virüsleri: Microsoft Word, Microsoft Excel ve Microsoft Access gibi office programlarına daha işlevsellik katmak için bir programlama dili yardımıyla makro hazırlanıp bir düğme, kısayol vb. aracılığıyla ile çalıştırılabilir. Makrolar belge ile taşındığı için belge açıldığında virüsün makro kodu çalışmaya başlar. Günümüzde e-posta ile gönderilen sunu, belge, elektronik tablo ekli dosyalar vasıtasıyla daha çok yayılma ortamı bulmuştur (ö*rnek;Melisa).*

Amerika Birleşik Devletleri'nde virüs oluşturmak ve yaymak bir bilgisayar suçudur ve federal suçlar kapsamına girmektedir. **1986** tarihli "**The Electronic Privacy Act**" yasası bilgisayarların kötü amaçlı ve hileli bir şekilde kullanımına karşı çıkartılan en dikkate değer yasadır. Avrupa ise **1991** yılında "**Computer Misuse Act**" adında bir yasa çıkartmıştır. Bu yasada da bilgisayar virüsü oluşturmak ya da bilerek dağıtmak suç olarak kabul edilmiştir.

Ülkemizde de bilişim suçu kavramı Türk Ceza Hukukuna ilk defa **1991** yılında **3756** sayılı Kanunla girmiş. Günümüzde; **TCK'nın 525.maddesinin (a-b-c-d) bentleri** ile Bilişim Alanı Suçları olarak değerlendirilmiş olup; bir bilgisayar sistemine yada bilgisayar ağına yetkisi olmaksızın erişimi ve sistemin yapmış olduğu iletişimin yetkisiz dinlenmesi, sistemin bir kısmına yada bütününe ve programlara veya içerdiği verilere ulaşma, bir bilgisayar yada iletişim sisteminin fonksiyonlarını engellenme amacıyla bilgisayar verileri veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesi, sisteme fiziksel yollarla zarar verilmesi, sistemin işlemesinin durdurulması, kasten virüs üretmek, Truva Atları (Trojan Horses), Solucanlar (Worms) gibi yazılımlar kullanarak bilgi çalmak, fiziksel zarar vermek suç kabul edilmiştir.

1.1.1.2. Trojan (Truva Atları)

Resim 1.1:Truva atı

Adını Çanakkale'de bulunan efsane tahta attan almıştır. Tarihi Truva (Troya) kenti, etrafı büyük surlarla kaplı ve iyi korunan bir

kentti. Kentin savunması çok iyi olduğu için ele geçirilememiş. Çare olarak şehir içine asker sızdırılmak istenmiş. Büyük tahtadan bir at yapılarak içine askerler yerleştirilmiş. Kuşatmanın başarısız olduğunun işareti olarak devasa tahta at şehirin önüne bırakılmış. Düşmanların gitmesi ile tahta at merak edildiği için şehir içine alınmış. Şehir kurtarıldı diyerik eğlenceler düzenlenmiş. Gece geç vakit olup uygun ortam oluştuğunda tahta at içinde gizlenen askerler dışarı çıkıp içeriden şehrin kapılarını açmışlar. Dışarıda bekleyen diğer askerler açık kapıları kullanarak şehir hakimiyetini ellerine geçirmişler.

Bilgisayarınız çok iyi korunuyor olsa bile sisteminizde bulunan programın içerisine gizlenmiş truva atları, program çalıştığında ortaya çıkarak değişik programlar kurabilir yada sisteminizin içindeki gizli bilgileri dışarıya iletebilir. Win.ini, system.ini, startup (başlangıç) ve registry içerisinde değişiklikler yaparak sistemin her açılışında kendini çalıştırmaya olanak sağlarlar Kurulan program ile bilgisayarınızda çalışır hale gelen trojan sayesinde IP taraması yaparak bilgisayarınızda ki kapıları açar, açık portları trojan özelliğini bilen kullanıcıda bu giriş ortamını kullanarak bilgisayarınızın içine girebilir. Bu sayede artık bilgisayarınız ele geçirilmiş olur.

Örnek olarak APStrojan (AOL password ateling) programı kullanıcı isimleri ve parolalarını elde etmek için kullanılır. Windows bellek monitöründe çalışır, kullanıcı AOL kullanıcı bilgisini girdiğinde bu bilgi bir email adresine gönderilir. Uzaktan yönetimi ele geçiren program kuruldu ise alınan güvenlik önleminin hiçbir önemi kalmayacaktır. İnternet üzerindeki bir kullanıcı sizin haberiniz bile olmadan gerekli dosyalarınızı görebilir, bunları kopyalayabilir veya silebilirler. Trojanlar genellikle; çalıştırılabilir yani dosya uzantısı EXE, COM, SCR, SYS, MSI gibi ücretsiz olarak dağıtılan, crack yapılmış programlar içine yerleştirilir.

Trojanlar bilgisayarlara girdiği zaman bir port ile çalışır ve o portun kullanımını açar. Kısaca trojanlar, sistem arkasında kod çalıştırıp uzaktan sahibi tarafından kontrol edilerek kullanılan casus programlardır. Amaçları mevcut sistemi ele geçirmektir. Virüsten ayıran özelliği, bir dosyadan diğerine bulaşarak çoğalmazlar.

1.1.1.3. Spy (Casus)

Türkçe karşılığı casus olmakla birlikte aslında istenmeyen ve tanıtımını yapmak istediği internet sayfalarını açar. Sizi istediği internet site yada siteleri açmaya zorlayan bu spylar reklam yapma amacındaki yazılımlardır. Bazen explorer giriş sayfasını, kendi sayfasını ekleyerek değiştirilmez duruma getirir. Sisteminizdeki bilgileri e-posta kullanarak sistem dışına gönderebilir. E-posta isminizi kullanarak kendi tanıtımınıda yaparak çoğalabilirler. Genellikle ActiveX leri kullanarak sisteme sızarlar. Bir internet sayfası açıldığında yükleme için Evet-Hayır gibi sorulara onay verdiğinizde spy bilgisayarınıza girmiş olabilir. Görünür büyük bir zararı olmamakla birlikte, istenmeyen sayfaların sürekli çıkması sıkıcı bir durum oluşturduğu için istenmez.

1.1.1.4. Worm (solucan)

Solucanlar(worm) internet bağlantısı aracılığıyla bulaşan ama dosyalara ve önyükleme(boot) sektörlerine tesir etmeyen yazılımlardır. Bilimsel olarak solucanlar tamamen virüs tanımına uymazlar.Solucanları virüsten ayıran özellik, kendi başlarına bağımsız şekilde çalışabilir ve bir taşıyıcı dosyaya ihtiyaç duymadan ağ bağlantıları üzerinde yayılabilir olmalarıdır. Solucanlar sisteminizdeki elzem dosyaları tahrip etmek , makinenizi büyük ölçüde yavaşlatmak ve bazı gerekli programların çökmesine neden olmak gibi bütün olası zararları yaratabilme yeteneğindedirler. (*Örneği; MS-Blaster, Sasser*…)

Örneğin Sasser, servis paketi yüklü olmayan XP lerde ekrana 60 saniye içinde sistem kapatılacak mesajı ile sisteme müdaheleyi tümüyle devre dışı bırakarak kapatır.

1.1.1.5. Dialer

Çevirmeli telefon bağlantısı yapıldığında, sisteme sızıp sizin izniniz olmadan yurtdışı bağlantılı ücretli telefon araması yaparak, telefon faturanız üzerinden para kazanma yöntemidir. Dialere kapılan kullanıcı beklemediği bir telefon faturası ile karşılaşabilir. Bedava mp3, bedava program, crack linklerinin tıklanması, burayı tıkla veya tamam düğmeleri ile sitedeki java programı çalıştırılarak sisteminizi tuzağın içine çeker. Her ne kadar kapatmaya çalışsanızda tekrar tekrar açılmaya davet eder.

Peki ya bunları yapamadan sizin isteğiniz dışında bu zararlı yazılım sizin bilgisayarınıza yerleşmiş ise? Hemen bu anda yapmanız gereken internetten çıkıp, bu durumda kesinlikle internette bağlı kalmayın.

1.1.1.6. Spam (önemsiz posta)

Reklam, duyuru, propoganda yada tıklama ile para kazanma amacı güderek talep olmadığı halde sürekli olarak e-postanıza gelen iletilerdir. E-posta adresleri internet üzerinden yada üyelik isteyen sitelerin üye listelerinin çalınması yolu ile listeler oluşturulur. Gönderilen bir e-posta, sistemde kayıtlı tüm e-posta hesaplarına topluca iletilir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajin alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır. Genelde 3 ayrı kullanım amacı sayılabilir:

UCE (Unsolicited Commercial e-mail- Talep Edilmemiş Ticari e-posta) bir ürünü yada hizmeti ucuz maliyet ve daha çok kitleye tanıtma amacı güder.

UBE (Unsolicited Bulk e-mail Talep Edilmemiş Kitlesel e-posta) politik bir görüşün propagandasını yapmak yada bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileri de olabilir.

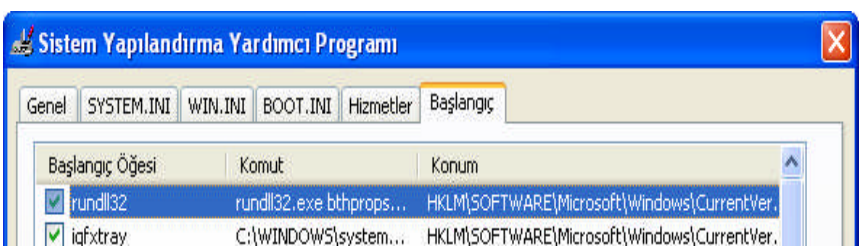
MMF (Make Money Fast – Kolay Para Kazanın) birbirini üye yaparak zincirleme para kazanma yolunu seçenlerin seçtiği yöntemdir. E-posta gelen kişinin 3 yada 5 kişi üye yapıp kayıt paralarını bir üst yöneticiye ödemeleri istenir. Burada bir başka yöntem ise uydurma bir

kehanet ile alınan e-postanın ilet yapılmaması sonucu kehanetin bu kişinin başına geleceği sömürüsü ile mesaj yayılmaya çalışılır.

Mail sunucuları önlem olarak belirledikleri bu e-postaları önemsiz posta adı altında ayrı bir bölüme atarlar. Bazen beklenilen e-postalarda bu bölüme atılmış olabilir.

Virüs ve Casuslardan korunmak için;

- Otomatik güncelleştirme yapılabilecek lisanslı işletim sistemi kullanıp, sık aralıklarla güncelleştirmeleri takip edin.
- Sisteminize girişte parola kullanın. Kilitlenmeyen kapının güvenliği olmaz.
- Giriş için kullanıcı tanımlayın ve administrator girişide dahil olmak üzere parola atayın.
- Mutlaka antivirüs koruma yazılımı kullanın ve sık sık güncelleyin.
- Güvenlik duvarı (firewall) kullanın.
- Güvenmediğiniz sitelerdeki onay ve yüklemeleri yapmayın. Crack & serial, adult gibi sitelerin çoğunluğu virüs, trojan ve spy barındırırlar.
- Güvenmediğiniz sitelerden özellikle bedava (free) dosyaları yüklemeyin. Çoğunluğu virüs yada casus yazılım taşır.
- Bilgisayarınıza taktığınız CD, flashdisk, disketleri önce antivirüs programı ile test edin
- MSN veya e-posta ile gelen dosyaları ihtiyacınız değilse açmayın. Gönderen, iletinin virüs içerdiğinin farkında olmayabilir.
- Emin olamadığınız office belgelerinin makrolarını etkinleştirmeden açın.
- Düzenli aralıklarla sisteminizin yedeğini alınız.
- Düzgün çalışır durumdaki güncel hali ile diskinizin eşkopyasını (image dosyasını) alın.
- Diskinizi bölümlendirip, belgelerinizi ve çalışmalarınızı D: sürücüsünde tutarak C: sürücüsünü koruma kartı yada koruma yazılımı (ör.deepfreeze) ile koruyun.
- Bazı yeni kurulumlarda sayfa içindeki flash, java applet ve scriptlerin yüklenme ihtiyacı olabilir. Bu tip yükleme ihtiyaçlarını güvenilir sitelerden yapınız.
- **Örneğin;** flash dosyalarınız için yüklemeye ihtiyaç duyuluyorsa **www.meb.gov.tr** sitesine bağlandığınızda, yüklü değilse yüklemeniz önerilir, bu yüklemeyi kabul ediniz.
- Bilgisayarınızın **Başlat → Çalıştır** bölümüne **msconfig** yazıp çalıştırdığınızda gelen pencerede **başlangıç** sekmesinde çalışan programları görüp sistem haricinde şüphelendiğinizi çalıştırılmaz hale getirebilirsiniz.



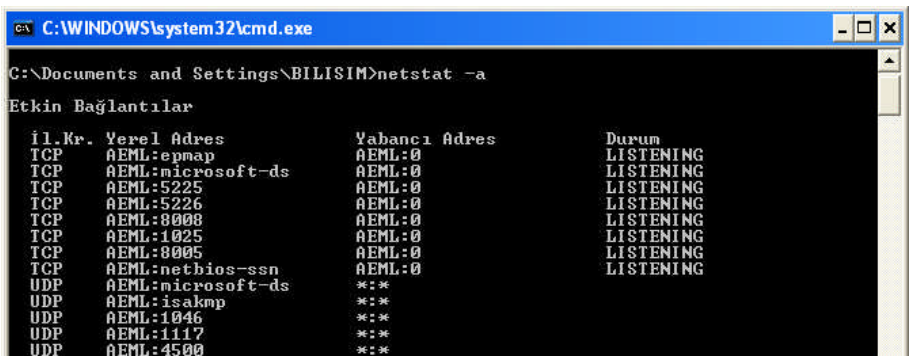
Resim 1.2: msconfig komutu ile açılışta çalışan programların listesi

Başlat →Çalıştır açılarak komut satırına **cmd** yazın. DOS komut istemi gelecektir. Gelen komut isteminde komutsatırına **netstat -a** komutunu yazarak sizin bilgisayarınız internette kimlerle hangi porta bağlı olduğuna bakabilirsiniz. Eğer Yabancı Adres bölümünde 0.0.0.0:12345 adres varsa bilgisayarınızda **netbus** isimli bir trojan vardır..

Eğer master boot record (mbr) içine bulaşan bir virüsü temizlemek için; temiz bir açılış yapabilen disket/CD ile PC'nizi açıp (FDISK dosyası içinde olan) DOS komut isteminde

A:\> fdisk/mbr

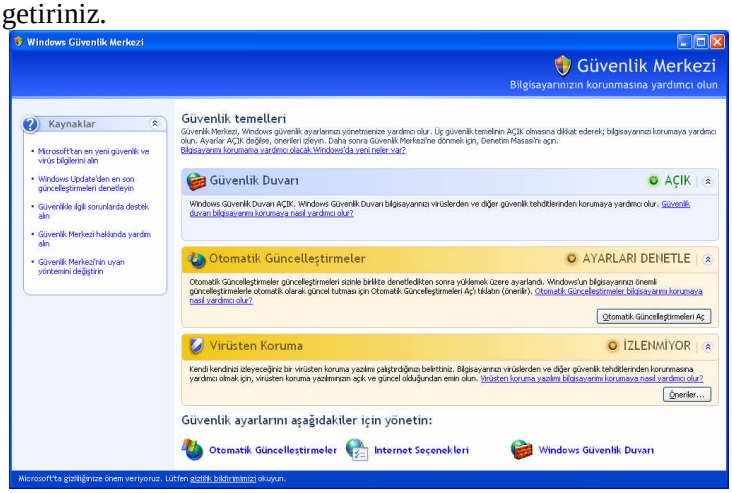
komutunu yazarak yeniden master boot recordunun yeniden yazılmasını sağlayıp kolayca temizlenebilir.



Resim 1.3: Başlat →Çalıştır dan cmd yazılıp DOS ta netstat –a komut sonucu

Başlat→Ayarlar→Denetim Masası→Güvenlik Merkezi tıklanınca gelen penceredeki Otomatik Güncelleştirmeleri Aç düğmesi ile aktif yaparak düzenli aralıklarla yeni çıkan açıklara karşı koruma altına alınız. Otomatik güncelleme için lisanslı Windows kullanıcısı olmanız gerekiyor.

Dışarıdan gelebilecek saldırılar için güvenlik duvarınızı çalışır halde olacak şekilde AÇIK konuma getiriniz.



Resim 1.4: Windows güvenlik merkezi ile sisteminizi güncel tutun

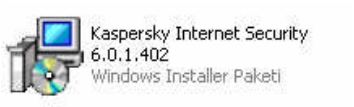
UYGULAMA FAALİYETİ

İhtiyaçlarımıza cevap verecek bir antivirüs programının 30 günlük deneme sürümünü sitesinden indirip, kuralım

- Antivirüs ve Internet Security özelliği olan bir programı kuracaksınız.
- Ayar ve güncelleştirmelerini yapacaksınız.
- Kurduğunuz programın Türkçeleştirmesini yapacaksınız.

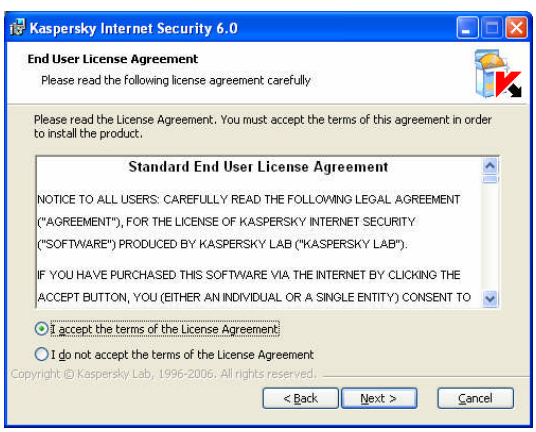
.

1.1.2. Antivirüs Programının Kurulumu

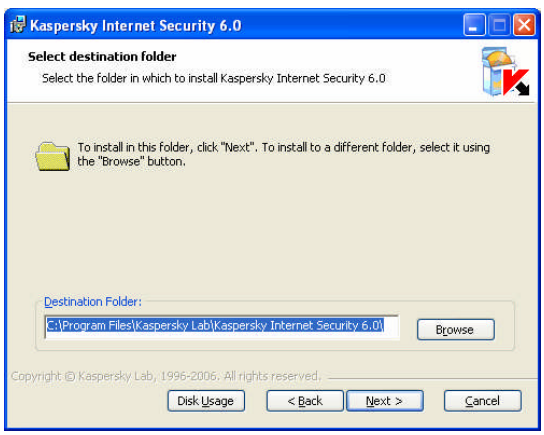


Adım 1- Kurulum dosyasını çift tıklayın

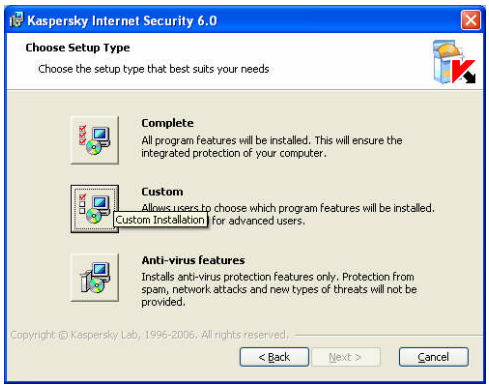
Adım 2- Next düğmesi ile devam edelim



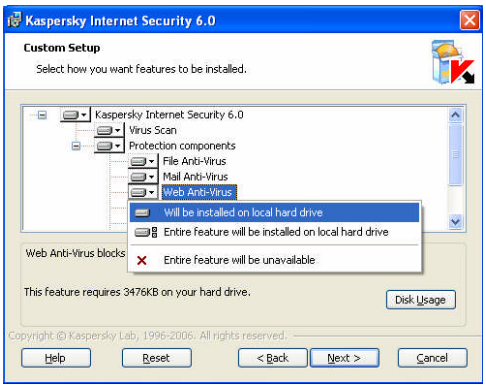
Adım 3- ***I accept*** ile sözleşmeyi okuyup tüm şartlarını kabul etmiş oluyoruz. **Next** ile devam ediniz.



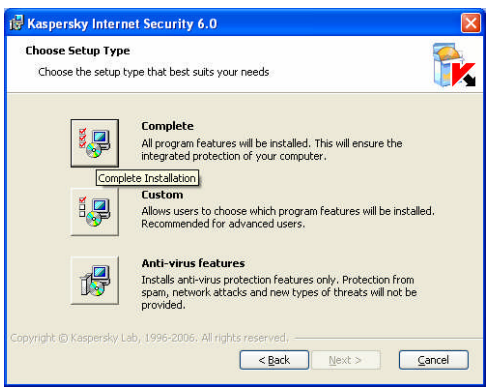
Adım 4- Programın kurulacağı klasörü yazıp **Next** ile devam ediniz.



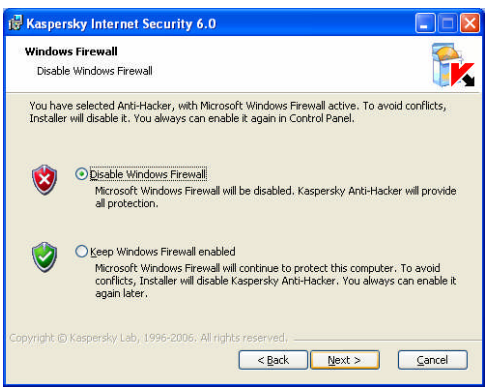
Adım 5- Custum seçilirse modüllerden istenilen yüklenir



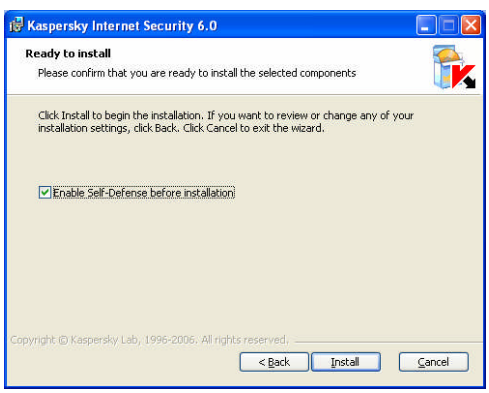
Adım 6- (X) özellik yüklenmeyecek anlamına gelir, siz yinede **Back** ile geri dönüp **Complete** ile kurun ve **Next** ile devam ediniz.



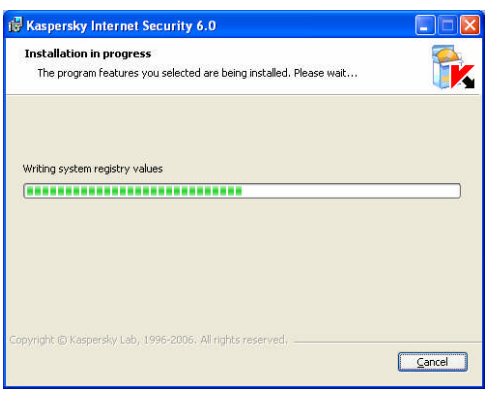
Adım 7- Siz yinede **Complete** ile tam kurulumu seçiniz.



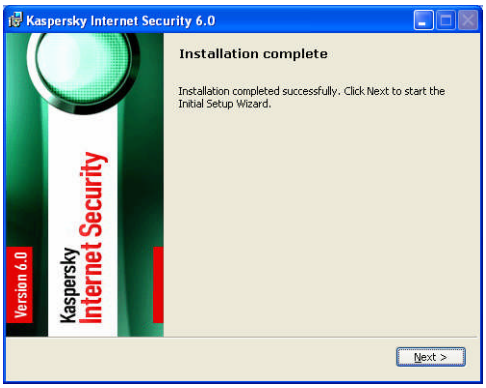
Adım 8-Kendi güvenlik duvarı olacağından, **Disable Windows Firewall** onaylanıp **Next** ile devam ediniz.



Adım 9- Eğer yaptığınız ayarlarınız tamam ise **Install** ile kuruluma devam edelim.

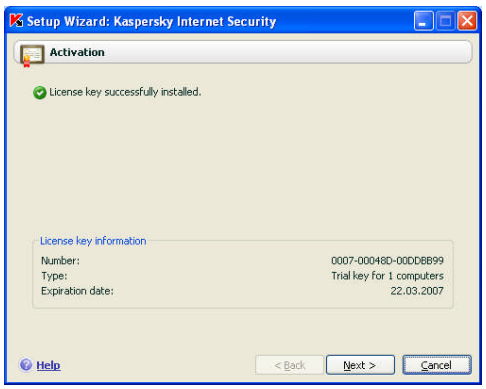


Adım 10- Programa ait dosyalar yüklenip gerekli ayarlamalar yapılıyor, bekleyiniz.

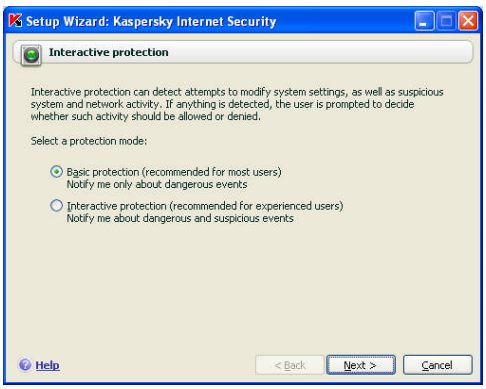


Adım 11- Kurulum tamamlandı **Next** ile devam ediniz.

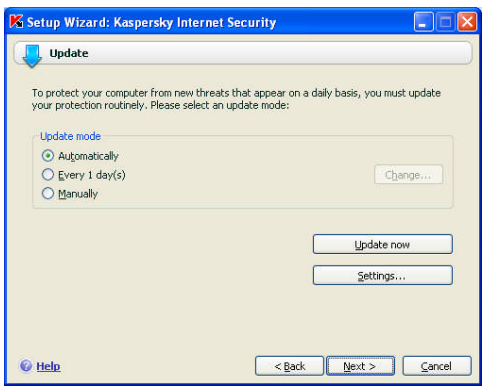
Adım 12- Lisanlı olmadığı için 30 günlük trial sürümü seçip **Next** ile devam ediniz.



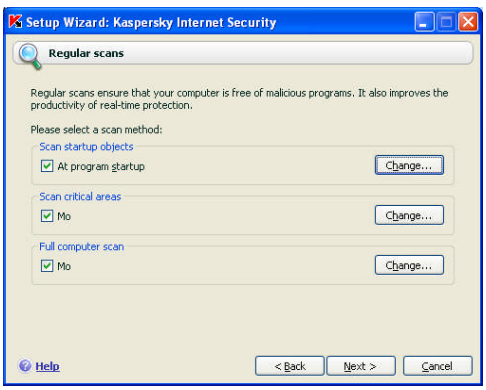
Adım 13. 30 günlük deneme sürümünün başarıyla kuruldu. **Next** ile devam ediniz.



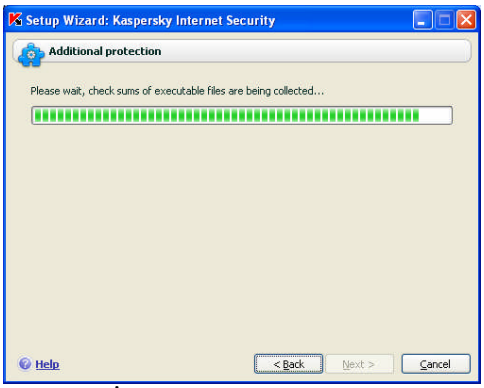
Adım 14. Basic protection ile temel koruma düzenini seçin Interactive protection ise ayarları elle yapmak isteyenler için. **Next** ile devam ediniz.



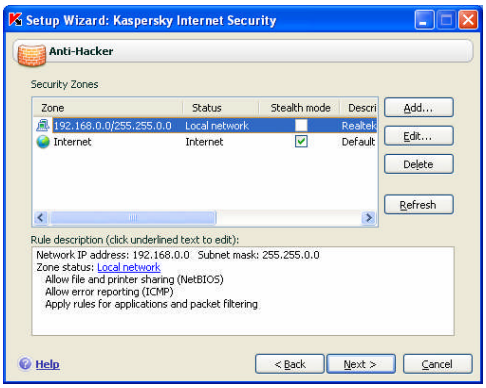
Adım 15. Yeni virüslerin tanıyabilmesi için güncelleme şeklinin seçimi Otomatik, ya da istediğiniz zamanlarda güncellenir. Update now ile şuan içinde güncelleştirebilirsiniz. **Next** ile devam ediniz.



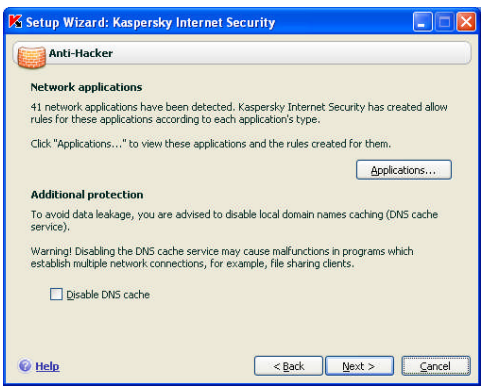
Adım 16. Automaticaly ile geçildiyse **Change** düğmesi kullanılarak otomatik yükleme ve tam taramanın zaman aralığı bilirlenebilir. **Next** ile devam ediniz.



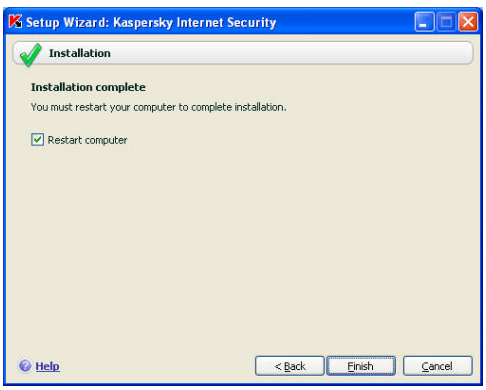
Adım 17. İşlem tamamlandığında **Next** ile devam ediniz.



Adım 18. Internet, ağ ortamında güvenilir ve yasaklanacak IP ler girilebilir. **Next** ile devam ediniz.



Adım 19. **Next** ile devam ediniz.

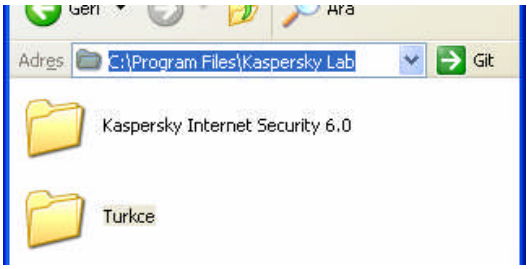


Adım 20. Kurulum işlemimiz bitti. **Finish** ile sonlandırıp bilgisayarınızın yeniden açılmasını sağlayın. Güncelleme ve tam tarama işlemlerinizi yapın.

1.1.3. Antivirüs Programının Ayarları

Kaspersky Internet Security programını sadece kurmak yetmiyor. Doğru kullanım ve kullanırken çıkan mesajların daha iyi yorumlamak, bilerek ve anlayarak kullanmak için ayarlarınıda tam yapmak gerekiyor..

Daha rahat kullanmak ve ayarlarımızı anlayarak gerçekleştirmek için programımızın arayüzünü (skin) Türkçe yapalım.

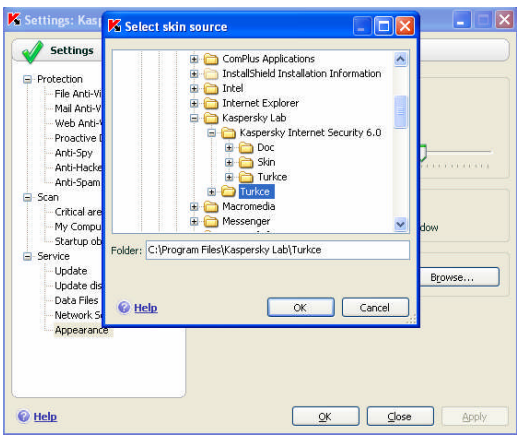


1- İnternetten bulduğumuz **Kaspersky 6.0.1 Türkçe** kabuğunu **C:\Program Files\Kaspersky Lab** klasörünün içine kaydedin.

2- Programı çalıştırmak için ya **Başlat programlar**dan program adı tıklanır yada saat yanında bulunan göstergelerdeki kaspersky 

simgesi çift tıklanır.

3-Görünüm ayarlarına ulaşmak için **Settings** tıklanır.



4- Yanda görünen penceredeki sol menünün son seçeneği olan **Appearance (Görünüm)** tıklanır.
5- **Browse** düğmesi tıklanır.
6- Select skin source penceresinden Kaspersky Lab klasörü içine yerleştirdiğimiz Türkçe klasörünü seçin.
8- **Ok** seçeneği ile bir önceki pencereye ulaşın.
9- Yapılan değişiklik **Ok** ya da **Apply** tıklandığında artık tüm seçenekler Türkçe olmuştur.

Artık ayarlarda dahil tüm seçeneklerimiz Türkçe. Aşağıda görülen durum penceresinde taranan dosya sayısı, güncelleme durumu, hangi alanlarda tarama yapıldığı ve bunların ayar seçenekleri listelenir.

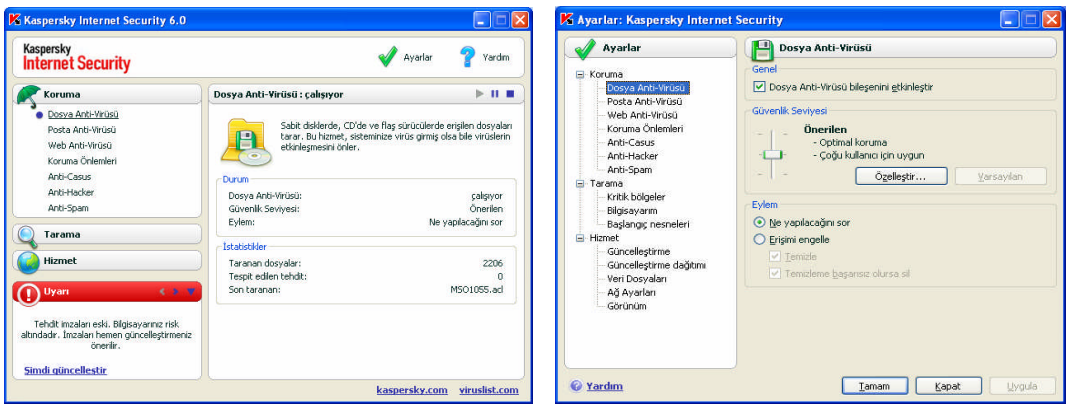
Koruma penceresi içinde antivirüs, eposta (antispam), web antivirüs, koruma önlemleri (proactive Defense), anticasus (antispy), antihacker ayar seçenekleri ayrı ayrı yapılabilmektedir. İstenmiyen koruma devre dışı bırakılabilir.

Resim 1.5: Kaspersky Internet Security programının kurulduğundaki durum penceresi

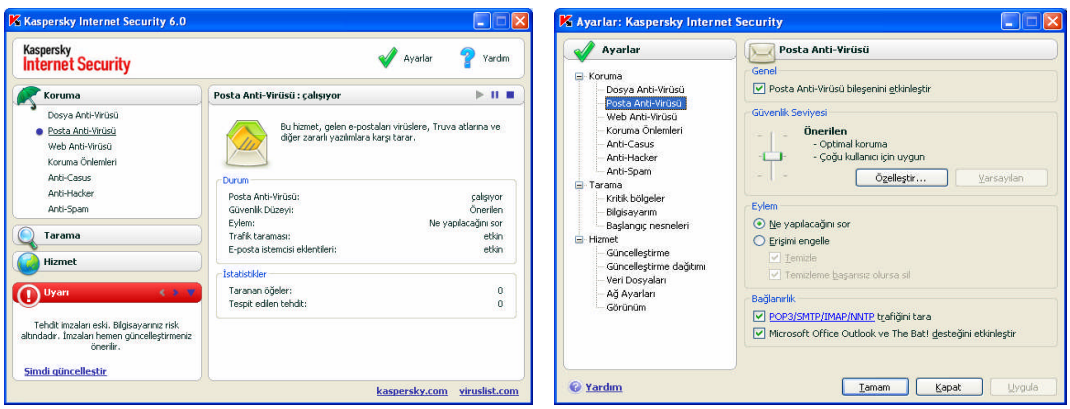
Koruma penceresinden Dosya Anti-Virüs tıklandığında antivirüs durum penceresi ekrana gelir.

- 1 numaralı **koruma** penceresi içindeki her özelliğin ayrı ayrı pencereleri açılarak durum ve ayar değişiklikleri yapılabilir,
- 2 numara ile gösterilen **ayarlar** seçeneğinden antivirüs ve ateşduvarı (firewall) izin ve yetkileri ayarlanabilir,
- 3 numaradaki yenilikleri sisteminize tanıtıp güncelleştirmenizin eski olduğunu, korumanın çalış vaziyette olduğun bildirir ekrandır. Buradan güncellemede yapılabilir.
- 4 numaralı bilgilendirme penceresi uyarı penceresi olup, güncelleme işleminin yapılmamış olduğunu göstermektedir. Şimdi güncelleştir seçeneği tıklanarak son çıkan virüs ve diğer casus yazılımlar için yeni koruma yöntemlerini sisteme ekleyebilir, < > oklar ile diğer yardım ipuçlarınıda takip edebilir,
- Tarama bölümünden virüs taraması başlatılabilir,
- Hizmet bölümünden de güncelleme, ürün, sistem, lisans, son kullanma tarihi gibi bilgilere ulaşılabilir.

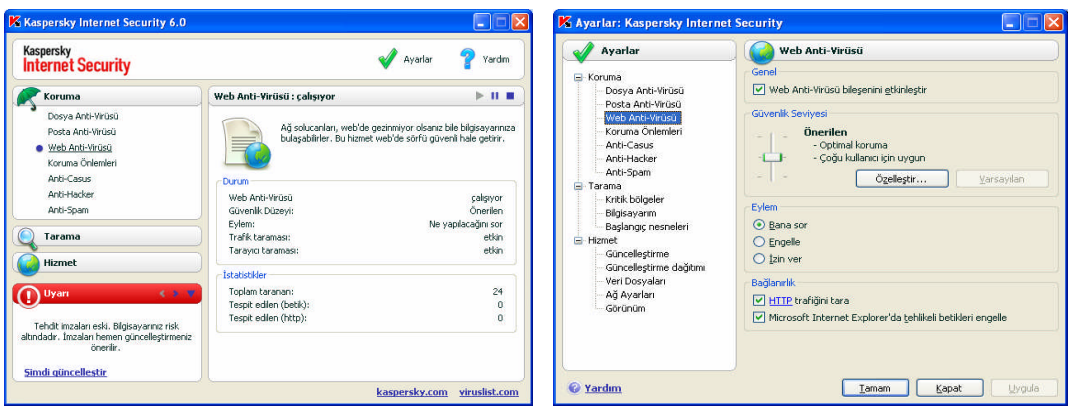
Koruma penceresi durum ve ayar pencereleri aşağıda gösterilmiştir.



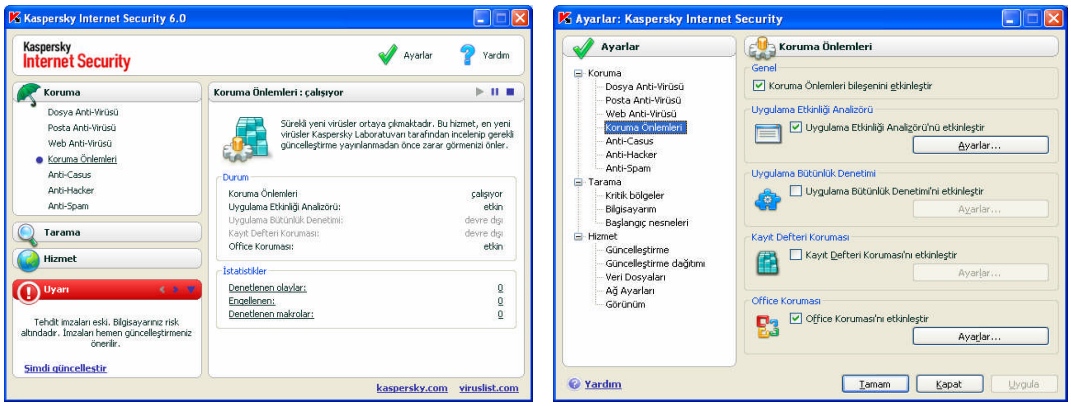
Resim 1.6: Antivirüs durum ve ayar pencereleri



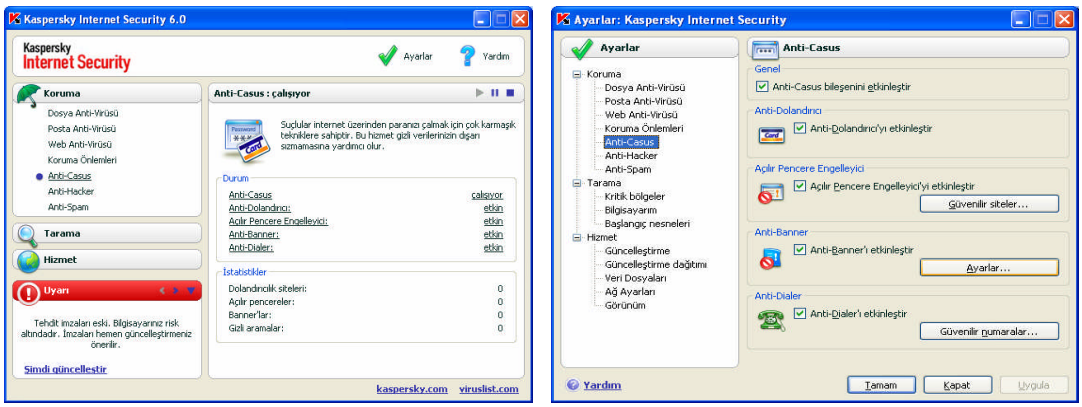
Resim 1.7: Gelen giden posta kontrolü durum ve ayar pencereleri



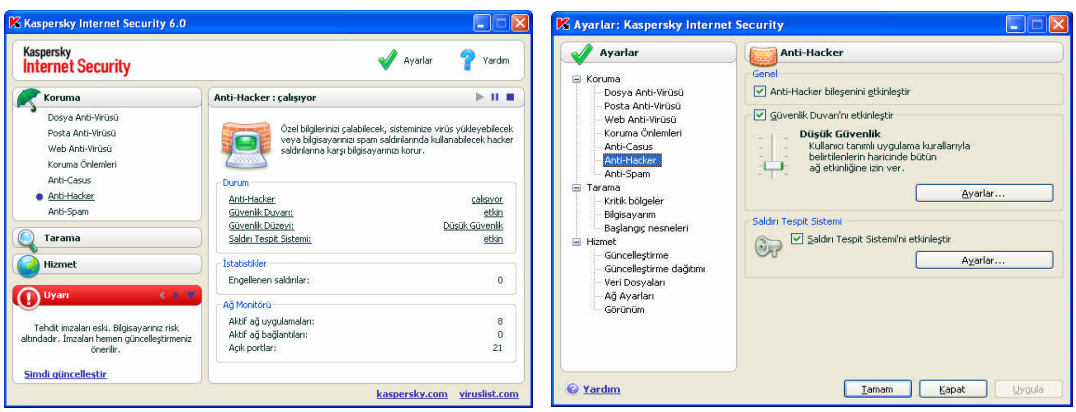
Resim 1.8: WEB antivirüs durum ve ayar pencereleri



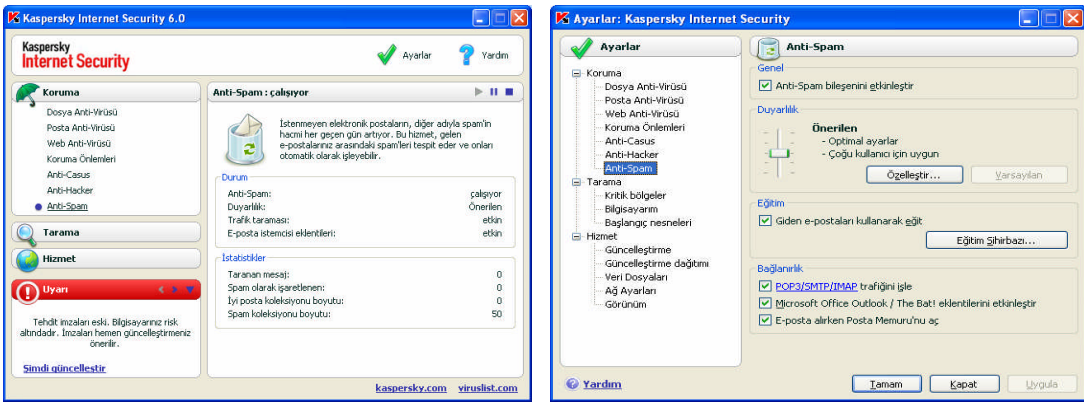
Resim 1.9: Koruma önlemleri durum ve ayar pencereleri



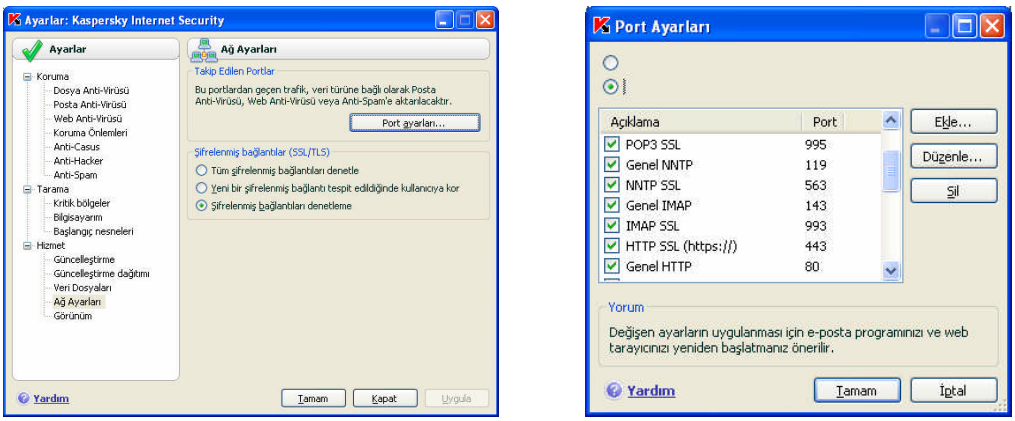
Resim 1.10: Casus koruma (antispy) durum ve ayar pencereleri



Resim 1.11: Hacker koruma durum ve ayar pencereleri



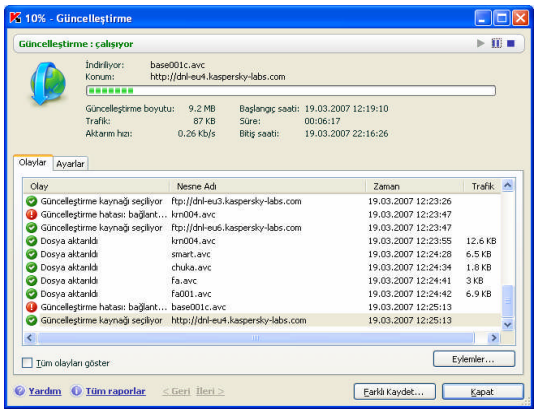
Resim 1.12: Gereksiz maillere önleme (antispam) durum ve ayar pencereleri



Resim 1.13: Ağ ayarlarından girilip port ayarları tıklandığında düzenlenen portlar

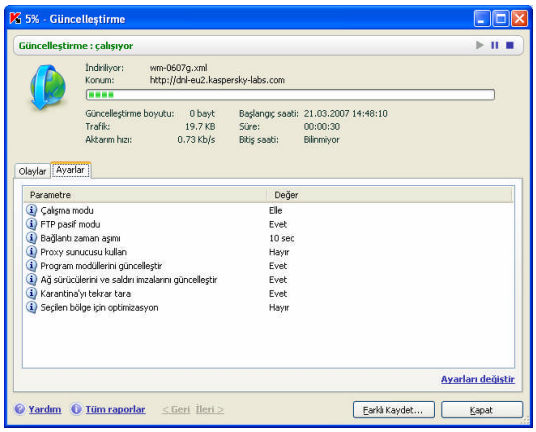
1.1.4. Antivirüs Programını Güncelleme

Günümüzde her dakika yeni bir zararlı yazılımın çıkabildiği ve internete bağlı olunduğu için her an o virüs yada zararlı yazılımlara yakalanabileceğimiz kaçınılmaz bir gerçektir. Bir sistemde antivirüsün yüklü olması sorunu tamamen çözmüş sayılmaz. Belli zaman aralıklarında zehir üretildi ise, panzehirininde elimizin altında bulunması gerekir. Bu düşünce ile sürekli olarak kurulan güvenlik programımızında yeniliklerden haberdar olması için güncelleme (update) yapılır.Şimdi güncelleştirme ayarını birlikte yapalım.

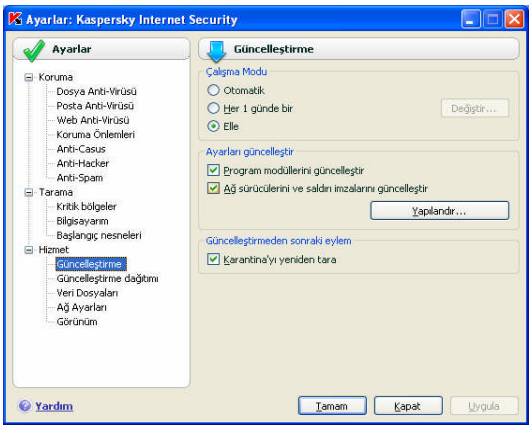


Adım 1. Uyarı penceresindeki **Şimdi güncelleştir** seçeneğini tıklayıp çıkan penceredeki **Evet** düğmesi ile işlemi başlatın.

Adım 2. Güncelleştirme işlemi sırasında çalıştırılan olaylar listelenir.



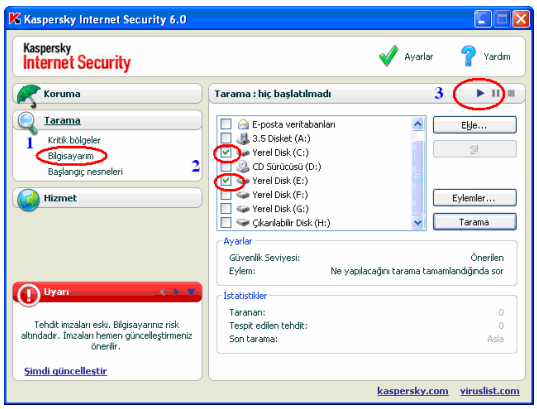
Adım 3. Güncelleme sırasındaki yapılan ayarlarında listesi yapılır.



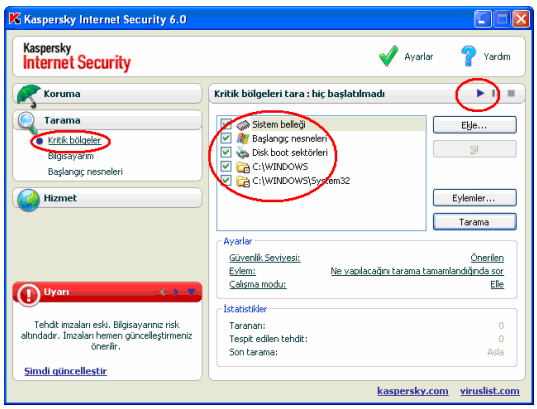
Adım 4. Ayarlar →Hizmet penceresindeki Güncelleştirme tıklandığında yukarıdaki pencere gelir. Burada güncelleme aralığı ve ayarlarının nasıl olacağı belirtilir.

1.1.5. Tarama İşlemi

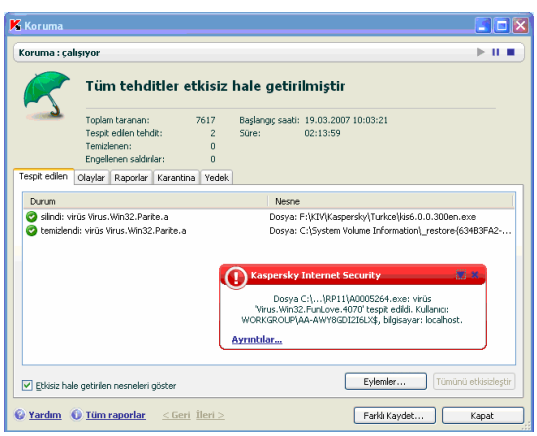
Bilgisayarımıza herhangi bir program kopyalandığında, eposta geldiğinde, program kurulduğunda yada disket, flashdisk takıldığında program otomatik olarak tarama işlemini kendisi başlatır. Ancak bir şekilde sistem içinde sinsice yerleşmiş olan yada güncelleme sonrası tespit edilebildiği virüsler için elle taramayı başlatmak gerekir. Sistemimizi bir virüs taramasından geçirelim.



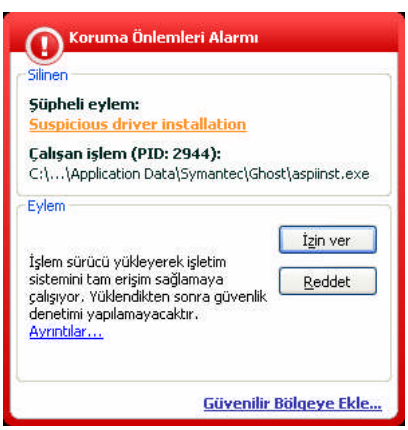
Adım 1.1 Ayarlar →Tarama→Bilgisarım seçilip taraması yapılacak sürücülere onay verildikten sonra 3 numaralı (▶) mavi ok tıklanır.



Adım 1.2. Kritik bölgeler seçilip bellek, başlangıç nesneleri, boot sectör, Windows klasörü gibi özel yerler taramadan geçirilebilir.



Adım 2. Sistemde Parite ve Fun Love virüslerini tespit ederek sildiğini belirtiyor.

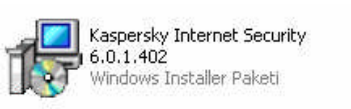


Adım 3. Bir program kurulmak istendiğinde, kurulan programın güvenilir olduğu izini verilirse kuruluma geçer.

Bununla birlikte antivirüs yazılım şirketleri, internet üzerinden ücretsiz tarama yapılabilen imkanlar sunmaktadır.

http://security.symantec.com/sscv6/home.asp?langid=ie&venid=sym&plfid=23&pkj=RGTPWFYJOKMFIDPMSVO&bhcp=1
http://www.olympos.org/article/articleview/188/1/5/online_virus_tarama#
http://usa.kaspersky.com/services/free-virus-scanner.php
http://www.pandasoftware.com/products/activescan?
http://us.mcafee.com/root/mfs/scan.asp?affid=102

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Sisteminize anti-virüs programını kurunuz	
➢ Kurulan programa ait ayarları düzenleyiniz.	➢ Dil : Türkçe ➢ Anti-Banner : Aktif ➢ Otomatik Başlama : Aktif
➢ Antivirüs programını güncelleyiniz.	
➢ Sisteminize virüs taraması yapınız.	➢ Scan

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıdaki sorulardan; sonunda parantez olanlar doğru yanlış sorularıdır. Verilen ifadeye göre parantez içine doğru ise "D" , yanlış ise "Y" yazınız. Şıklı sorularda doğru şıkkı işaretleyiniz. (*Doğru-Yanlışlar 5puan, çoktan seçmeli sorular 10 puandır*)

1. Kendini dosyalara bulaştırarak çoğalan zararlı programlara SPY denir. .....D( ) Y( )

2. Solucanlar, kendi başlarına bağımsız şekilde çalışabilir ve bir taşıyıcı dosyaya ihtiyaç duymadan ağ bağlantıları üzerinde yayılabilir? .....D( ) Y( )

3. Trojanlar, klavyeden girdiğimiz karakteri sistem dışına aktarırlar? .....D( ) Y( )

4. Solucanlar, dosyalara ve boot sektöre tesir eder? .....D( ) Y( )

5. Boot sectör virüsleri MBR üzerine yerleşir? .....D( ) Y( )

6. Bilgisayar virüsleri biyolojik olarak canlılarada bulaşabilir? .....D( ) Y( )

7. Sistem içindeki bilgileri dışarı sızdırmak için kullanılan program parçacığı aşağıdakilerden hangisidir?
A) Virüs B) Trojan C) Spy D) Spam

8. Spam nedir?
A) İçeriden bilgi sızdıran casus yazılımlardır.
B) Talep olmadığı halde gönderenin menfaatine çalışan ve sürekli gelen e-postalardır.
C) İstemsiz web sayfalarını açan yazılımlardır.
D) Dosyaları bozarak zarar veren yazılımlardır.

9. Dışarıdan açık portlarınız üzerinden gelecek saldırılara karşı bilgisayarınızda ……. kurulu olması gerekir?
A) FireWall B) Antispy C) Virüs D) AntiSpam

10. Sizin isteğiniz dışında internet sayfalarının açılmasına ve sizi istediği internet sitesine açmayı zorlayan yazılımlara ne denir?
A) Dialer B) Trojan C) Spy D) Spam

11. Hangisi antivirüs programı <u>değildir</u>?
A) Norton B) Avast C) Ghost D) NOD32.

12. Virüsler hangi dosya uzantısına daha kolay bulaşır?
A) EXE B) BMP C) WAV D) DLL

13. İsteğimiz dışında telefonumuzu çevirerek telefon faturası üzerinden kendi hesaplarına para kazandıran zararlı yazılım hangisidir?
A) Trojan B) Spam C) Spy D) Dialer

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 geri dönerek tekrar inceleyiniz. Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Sistemdeki verilerin yedeğini alma işlemini yapabileceksiniz.

ARAŞTIRMA

- Bilgisayarınızda öncelikle kurtarmak istediğiniz dosyalar hangileridir? Tartışınız.
- Bilgisayarınızı kurup ayarlarını yaparak kullanılır hale geldiğinde yedek almak gerekir mi? Tartışınız

2. YEDEK ALMA

Bilgisayarımız, bizim işlerimizin çoğu yükünü çeker ve oldukçada kolaylaştırır. İşlerimizi kolaylaştıran bu bilgilerin başka bir ortama kopyalanması bizim için bir güvencedir. Gelin bu yöntemleri öğrenerek işlerimizi daha da kolaylaştıralım.

2.1. Verilerin Kopyalanması

2.1.1. Verileri Bir Klasöre Kopyalamak.

Bilgisayarımızdaki çalışmalarımızı, resimlerimizi, müziklerimizi hep belgelerim klasöründe tutarız. Belgelerim klasörü her kullanıcı için ayrı bir klasörde tutulur. Bizim için bu kadar önemli olan bu klasörümüzün içindeki verileri nasıl kopyalayacağız?

DOS altında Toplu İşlem Dosyası oluşturarak yedek alalım:

Yapılacak işlem : Belgelerim klasöründeki word dosyalarını d: sürücüsündeki **denizli** ismiyle açılmış klasöre kopyalayınız. (*şart: DOS komutlarını tanıyor olmak*)

- Not Defterini açınız.
- Masaüstündeki Belgelerim klasörünü sağ tıklayıp Özellikler seçeneği ile bulunduğu hedef yolu seçerek kopyalayınız. (*C:\Documents and Settings\BILISIM\Belgelerim*)
- Not Defteri içine aşağıdaki komutu yazınız.
  XCOPY C:\Docume~1\BILISIM\Belgelerim*.doc d:\denizli /S
  (BILISIM kullanıcı adı olup siz bilgisayarınıza girdiğiniz kullanıcı adı ile değiştirebilirsiniz.)

Not: COPY yerine XCOPY seçilmesindeki amaç, alt klasörleriyle birlikte dosyaların kopyalarının alınması. Bunun için /S parametresi kullanılıyor

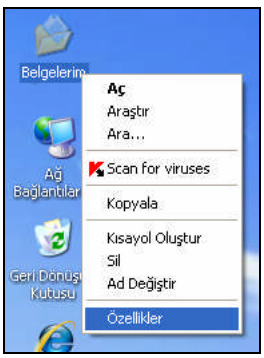
- Not defterini, **Dosya →Kaydet** seçeneği ile dosya adını **OTOKAYIT.BAT** yazıp tür kısmını ***.*** seçerek masaüstüne kaydedin.
- Masaüstendeki OTOKAYIT çift tıklayıp birkaç kez tekrar edin. *Çıkan soruları tartışın*

Soru : Documents and Settings yerine neden Docume~1 yazılması gerekiyor?

DOS altında kopya yapabilmek için komutları ve parametrelerini bilmek gerekiyor ve bir harf hatası olsa bile komut çalışmaz. Bu işlemi WINDOWS kullanarak yapalım.

Yapılacak işlem : Belgelerim klasörünün kopyasını alarak **D:** sürücüsü içine **denizli** klasörü açarak yedekleyelim.

Soru: Masaüstündeki Belgelerim klasörü simgesi sağ tıklanıp **Kopyala** dendiğinde neden **Yapıştır** yerine **Kısayol Yapıştır** geliyor? Sağ tuş ile sürükleyip taşıdığınızda **Buraya Kopyala** ve **Buraya Yapıştır** seçenekleri gelmiyor? Tartışın?



Adım 1-

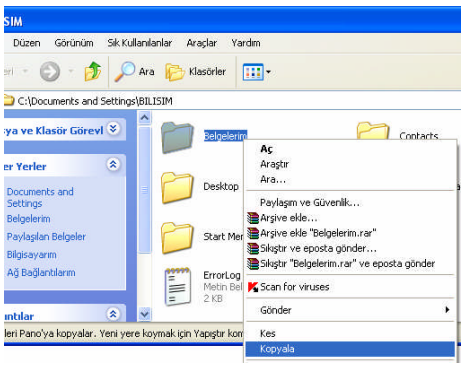
Masaüstündeki Belgelerim klasörünü sağ tıklayıp → Özellikleri seçin

(Her kullanıcının Belgelerim klasörü C:\Documents and Settings\ klasörü içindeki kendi kullanıcı adı içindeki Belgelerim klasöründe tutulur.)

Adım 2-

Gelen pencereden Hedef Bul seçilerek dosyalarımızın bulunduğu klasörün gerçek yerine ulaşırız.

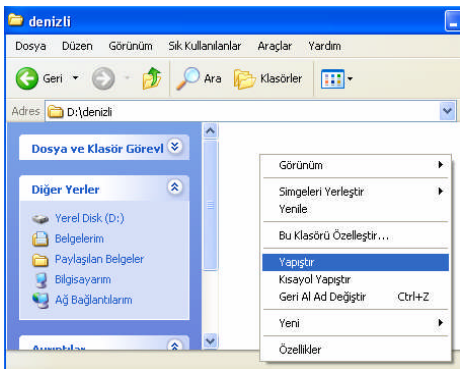
(Masaüstündeki Belgelerim klasörü, gerçekte buradaki klasörü açmakla görevlendirilmiş bir kısayoldur.)



Adım 3-

Gelen penceredeki Belgelerim klasörü sağ tıklayıp Kopyala seçeneğini seçerek tüm çalışmalarımızı panoya (yani RAM belleğe) kopyalıyoruz.

(Arşive ekle "Belgelerim.rar" ile bu klasör içindeki tüm dosyaları tek dosya halinde paketleme işleminide yapabiliriz .)



Adım 4-

D: sürücüsüne yada istediğiniz bir sürücüye daha önceden açılmış yada yeni bir klasör (boş alanda sağ tıklayıp Yeni→Klasör ile -denizli-) açarak bu pencere içinde boş bir yerde sağ tıklayıp Yapıştır ile dosyalarımızın kopyasını almış oluruz..

2.1.2. Klasörü CD ye Yazmak.

Verilerinizin kalıcı olarak arşivlemek istiyorsak, verileri CD ye yazarız. WINDOWS XP sürükle-bırak yöntemi ile CD içinde yazma işlemi yapabilir. Ancak daha detaylı bir CD yazma işlemi için CD yazma programları kullanılır. Biz burada Nero StartSmart programını anlatacağız.

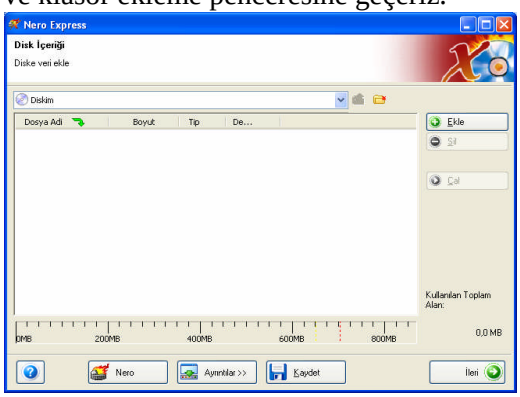
Programınızı Başlat → Programlar→Nero →Nero SmartStart tıklayarak çalıştırın ve aşağıdaki ekrana ulaşın.

Öncelikle Nero SmartStart programının başlatma ekranını tanıyalım

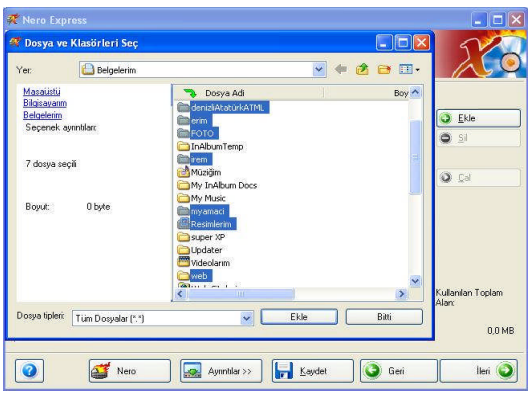
Resim 2.1: Nero SmartStart programının karşılama ekranı.

1- Yazma işleminin Cd yada DVD olacağı seçilir. Biz CD seçiyoruz.
2- Sık Kullanılanlar; içinde ençok kullanılan yöntemler karışık verilmiştir
3- Veri; Bilgisayar dosyaları kopyalamak ve açılış CD si yapmak için kullanılanılır
4- Ses; MP3, WMA, digital ses yada müzik setlerinin çaldığı tract ses CD kaydı yapılır
5- Foto ve Video; görüntüleri VCD yada DVD formatında kaydeder.
6- Kopyala Yedekle; CD yada DVD yi birebir kopyalar. CD imajı hazırlar
7- Ek Ayarlar; Silme, etiket hazırlama, CD hızını test etme gibi ek işlemleri yapar.
8- Çıkış; pencereyi kapatmak içindir.

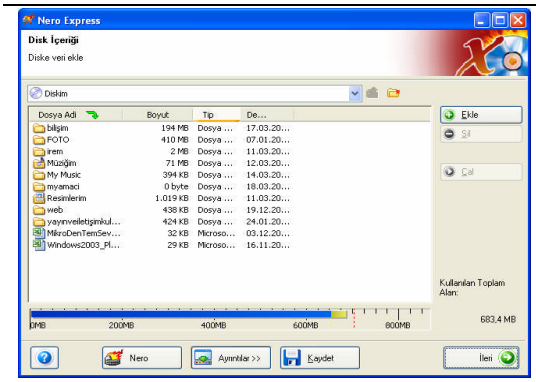
Adım 1- Nero SmartStart penceresindeki **9** numaralı **Veri Diski Yarat** düğmesi ile dosya ve klasör ekleme penceresine geçeriz.



Adım 2- Ekle düğmesi ile yandaki pencereye gelinir

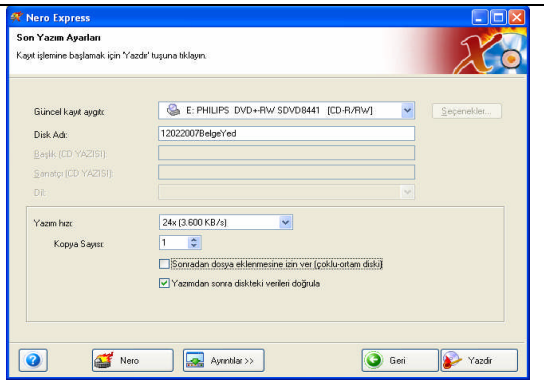


Adım 3- Kopyasını alacağınız ilk dosyayı tıklayarak seçin. Diğer dosyaları Ctrl basılı iken tıklayarak seçin ve **Ekle** düğmesini tıklayın. Başka klasörden eklenecek dosya yok ise **Bitti** ile çıkın. (*Sürükle bırak ile Ekle kullanılmadan dosyalar eklenebilir*)



Adım 4- CD ye yazacağımız dosya ve klasörler görünür. Aşağı cetveldeki mavi grafik verinin sorunsuz yazılacağı yerlerdir. Bazı eski CD ler 650MByte oldukları için uyarı amaçlı sarı renktedir. 700MByte hizasındaki kesik çizgileri aşar ise verileriniz CD ye sığmayacağı için kırmızı renkte gösterilir. Fazla görülen dosyaların listeden silinmesi gerekir...

İleri düğmesi ile devam edilir



Adım 5- Güncel kayıt aygıtı;yazma işlemini yapacak CD yada DVD yazıcının adıdır.

-Disk Adını siz hatırlayacağınız bir isim giriyorsunuz. Ben burada yedekleme tarihini yazdım

-Yazım Hızını belirleyiniz.

-Sonradan dosya eklenmesine izin ver seçeneği işaretlenirse sonradanda ek kayıt yapılabilir. Burada CD ye yazılacak veri çok olduğu için kapatabilirizde.

-Yazımdan sonra diskteki verileri doğrula işaretlenir ise yapılan kayıtta bir hatanın olup olmadığı test edilir. Zamanı ikiye katlıyor olmasına rağmen verinin doğru kaydı önemlidir. Kullanılması önerilir.

Yazdır düğmesi ile kayıt işlemini başlatın, İleri ile tasarıyı kaydetmeden sonlandırın.

2.2. Windows Yedek Alma (Back-Up) Kullanma

Sistemimizin herhangi bir sorunla karşılaşması durumunda çalışamaz hale gelebilir. Bu sebeple önemli görülen zamanlarda sistemin düzgün çalışır haldeki durumu tek dosya halinde yedeklenmesi gerekebilir. Bu işlemi gerçekleştiren birçok yöntem vardır. Bu yöntemler; image almak, geri dönüşüm noktaları oluşturmak, güvenlik kartı kullanmak, backup ile yedek almak vb.

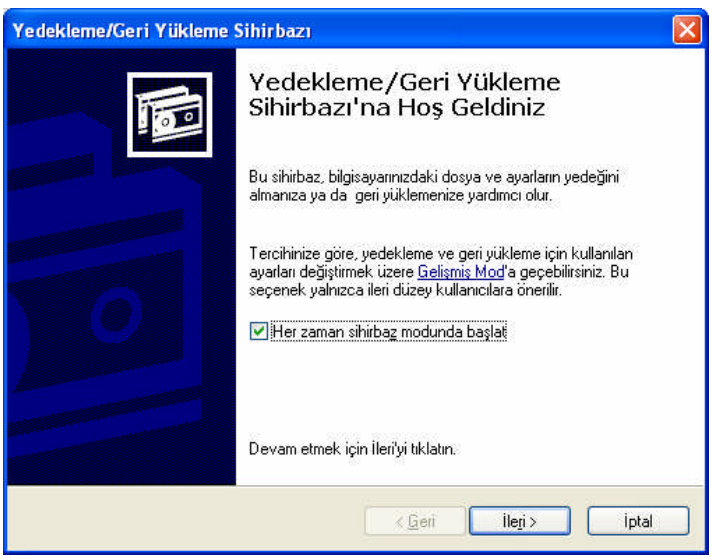
Herhangi bir program kurmadan yedek işleminizi yapmak istiyorsanız sistem araçları içindeki yedekleme (backup) isimli programı kullanabilirsiniz. Windows XP Profesional da yüklü olarak gelen bu program XP Home sürümlerinde kurulu değil. XP Home CD si takılarak **Denetim Masası→Program Ekle Kaldır** ile yüklenmesi gerekiyor.

2.2.1. Windows Yedekleme/Geri Yükleme Sihirbazı

İstenilen zamandaki dosya yada tüm sistem yedeğini alıp ihtiyaç olduğunda geri almak için yedek dosyasının oluşturulması gerekiyor. Bunun için;

Başlat → Programlar→Doantılar →Sistem Araçları → Yedekleme sırası takip edilerek yedekleme sihirbazı başlatılır.

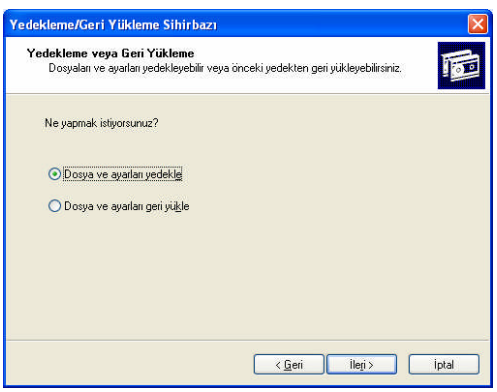
Adım 1- Yedekleme sihirbazı penceresi ileri ile devam ettirilir.



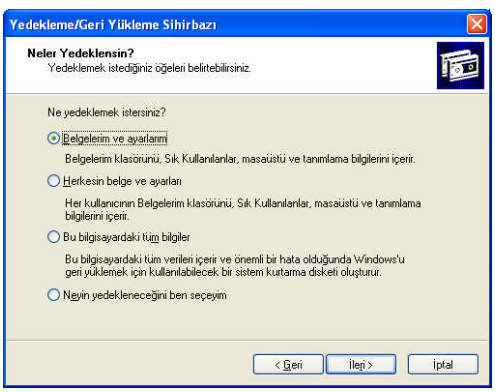
Resim 2.2: Programın ilk başlatıldığındaki yedekleme/geri yükleme sihirbazı

2.2.2. Veri ve Ayarları Yedeklemek

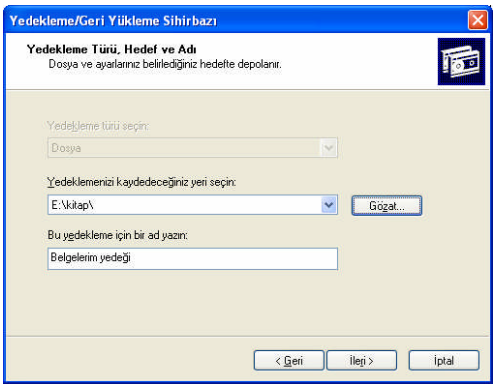
Verilerin yedeğini alacağımız için "Dosya ve ayarları yedekle" işlemine başlanır.



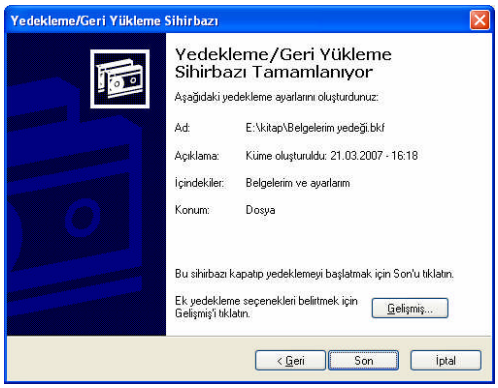
Adım 2- Dosya ve ayarları yedekle seçilip **İleri** tıklanır.



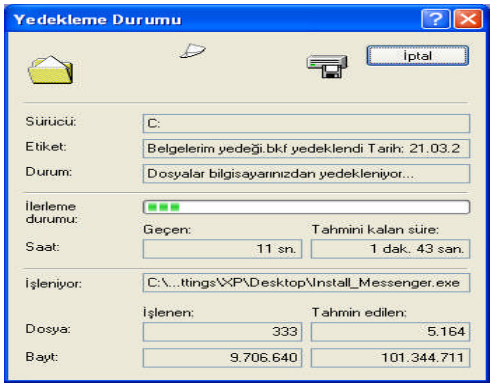
Adım 3-Yedeği alınacak belgelerim, tüm bilgiler , seçeyim vb. biri seçilip. **→İleri** tıklanır.



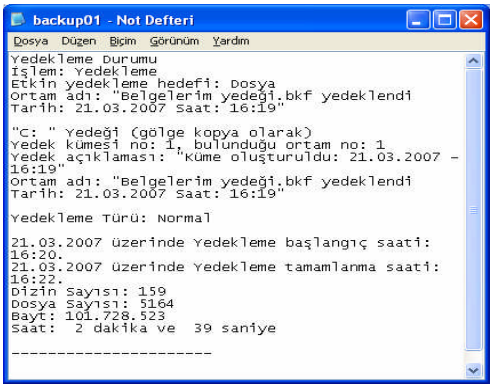
Adım 4- Gözat ile yedeğin kaydedileceği klasörü seçip (**E:\kitap) →İleri** tıklanır.



Adım 5- Son ile sihirbaz tamamlanır.



Adım 6- Yedekleme işlemi başlamıştır.

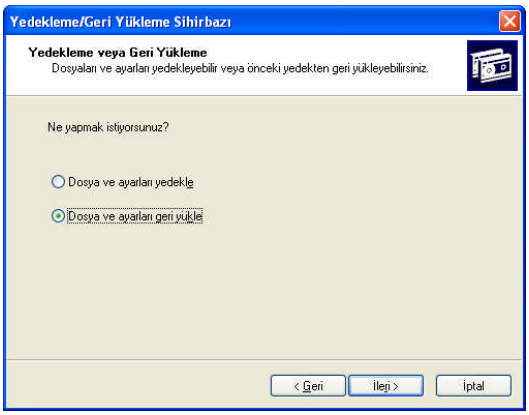


Adım 7- Yedekleme bitince ya **Kapat** ile çıkılır ya da **Rapor** düğmesi ile yedekleme işleminin istatistikleri görüntülenir.

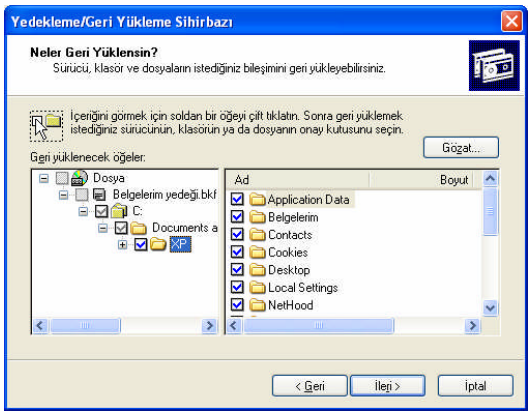
Yedeğin geri alınması gerektiğinde yine

Başlat → Programlar→Donatılar →Sistem Araçları → Yedekleme

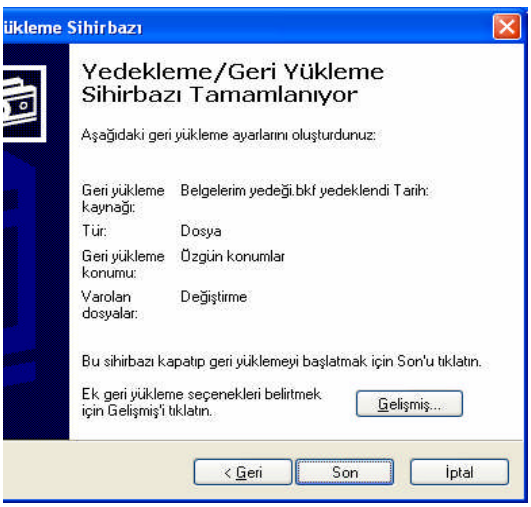
komutu çalıştırılır.



Adım 1- Ne yapmak istiyorsunuz sorusuna bu kez Dosya ve ayarları geri yükle seçilerek **İleri** tıklanır.



Adım 2- Geri yüklenecek klasörlere onay konularak **İleri** tıklanır.

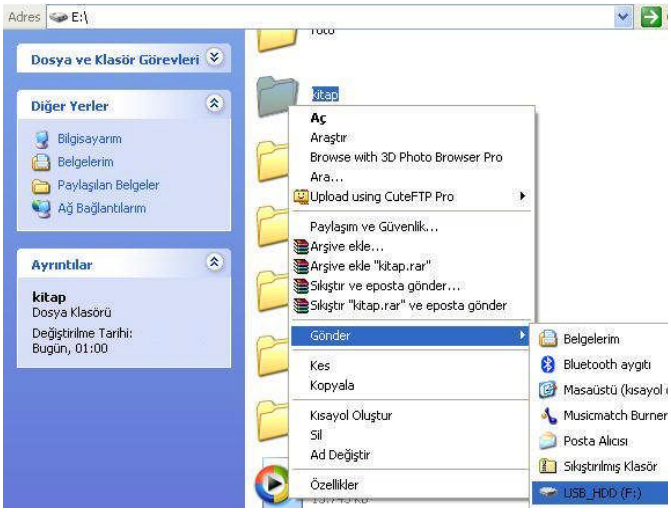


Adım 3- Gelen pencereden **Son** tıklanır.

Adım 4- Kapat ile işlem sonlandırılır..

2.2.3. Yedeklenen Bilgileri USB-HDD ye Yazmak

Dosyamız E: sürücüsünün kitap klasörünün içine (E:\kitap) **Belgelerim_yedeği.bkf** ismiyle dosya halinde kaydetmiştik. Bu dosyayı ya da kitap klasörünü sisteme takılı usb portuna takılı **USB_HDD (F:)** isimli sabit diske kaydedelim.



Bunun için;

1- **Kitap** klasörünü **sağ** tıklayın.

2- Farenin okunu **Gönder** seçeneğini üzerinde bekletin.

3- Açılan pencereden sisteme takılı olan ve **USB_HDD (F:)** ismine tıklayın.

Kitap klasörünüz, USB_HDD içine kaydedilmiş oldu.

Resim 2.3: Klasörün sağ tık ile USB'ye kopyalanması

Kitap klasörünün bir yedeği USB den takılan ve ismi USB_HDD olan yardımcı belleğe kopyalandı.

2.3. Sistem İmajı Alma

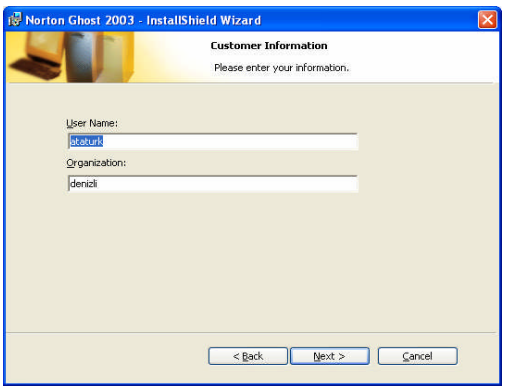
Her defasında sistem kurmak, donanımları tanıtmak, ayarları yapmak yerine sistemi bir kez eksiksiz kurup C: sürücüsünün imajını (birebir kopyasını) almak çok büyük kolaylık sağlar. Birde okul laboratuvarı, internet cafe gibi birbirinin aynı makinalardan oluşuyor ise CD ye alınacak bir image dosyası ile tüm makinalar kurulabilir. 1 PC nin kurulumunun 10 dakika aldığını farzedersek 1,5 saat içinde 9-10 makine kurulabilir. Oysa ki sadece Windows kurulumu 45 dakika, office ve diğer uygulamarla 1,5 saati aşar.

İmaj almak için **Norton Ghost**, **Acronis True Image, Image Drive** programları örnek verilebilir.

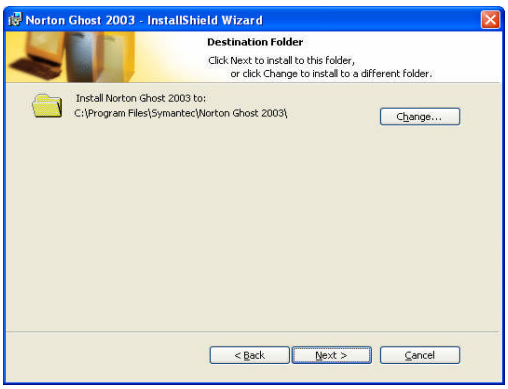
2.3.1. İmaj Programını Kurmak

Açılış disketide hazırlayabildiği için Norton Ghost 2003 programını kuralım.

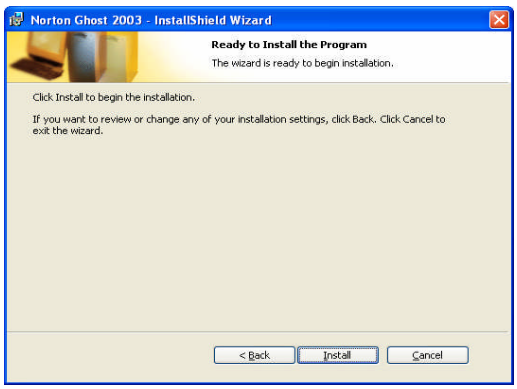
Adım 1- Norton Ghost 2003 kurulum başlatılıp → **Next** ile devam ediniz.



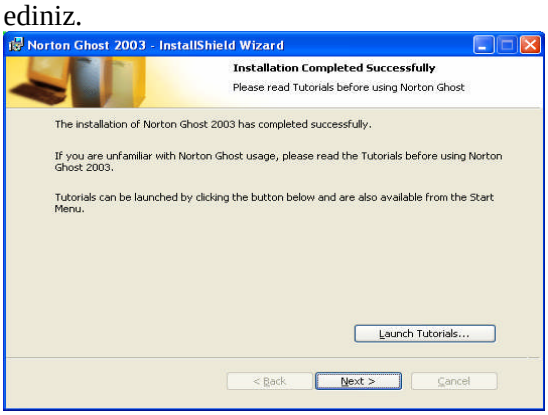
Adım 2- Sizin belirlediğiniz kullanıcı adı ve kuruluş adı girilip→ **Next** ile devam ediniz.



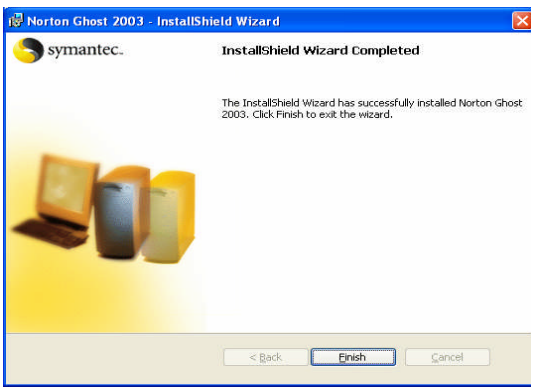
Adım 3- Yükleneceği klasör ya olduğu gibi bırakılır yada değiştirilip → **Next** ile devam ediniz.



Adım 4- Kurulum **Install** ile başlatılır

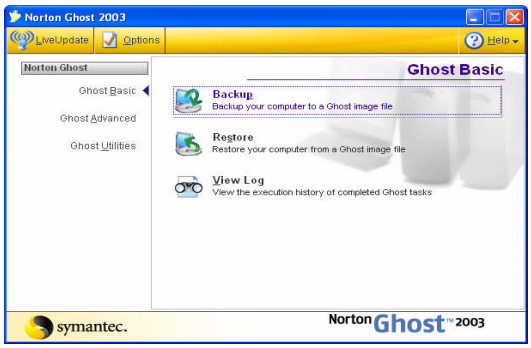


Adım 5- Kurulum başarıyla tamamlandı mesajı görülünce →**Next** ile devam ediniz..



Adım 6- Kurulumun tamalandığını belirten pencereden sonra **Finish** ile kurulumu bitiriniz.

Programımızı Başlat → Programlar → Norton Ghost 2003 → Norton Ghost ile çalıştıralım ve aşağıdaki pencereye ulaşalım.



Backup :Mevcut disk yada partitionun birebir kopyası tek dosya haline paketlenir. Buna imaj denir.

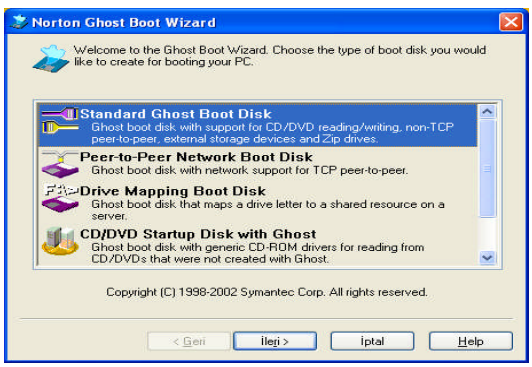
Restore :Daha önceden alınmış imaj dosyasından geriyükleme yapılır.

Ghost Utilities sekmesindeki **Norton Ghost Boot Wizard** ile açılış disketi yapılır.

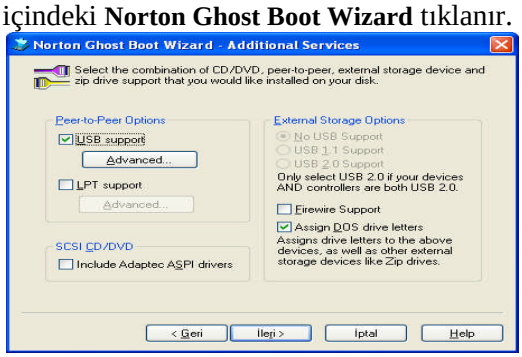
Resim 2.4: Klasörün sağ tık ile USB'ye kopyalanması

Windowsun herhangi bir sebeple bozulacağı ve açılamaz duruma geleceği düşünülecek olursa akla gelen ilk soru, windowsta çalışan bu program ile geri yükleme nasıl yapılabilir ki? Evet bu program işlemlerini windows altında yapıyor ama bununla birlikte DOS açılışı olan bir disket hazırlanması, ağ üzerinden kurulum, CD/DVD'den kurulum gibi özelliği de var. Şimdi açılış disketimizi hazırlayalım.

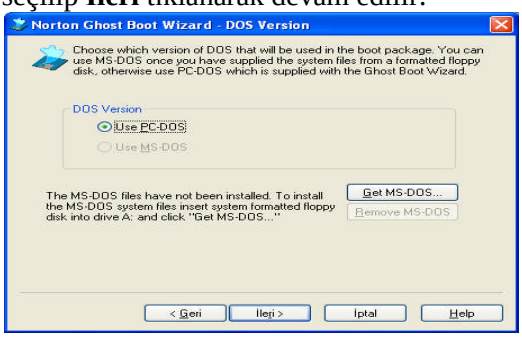
Adım 1: Programı çalıştırıp **Ghost Utilities** içindeki **Norton Ghost Boot Wizard** tıklanır.



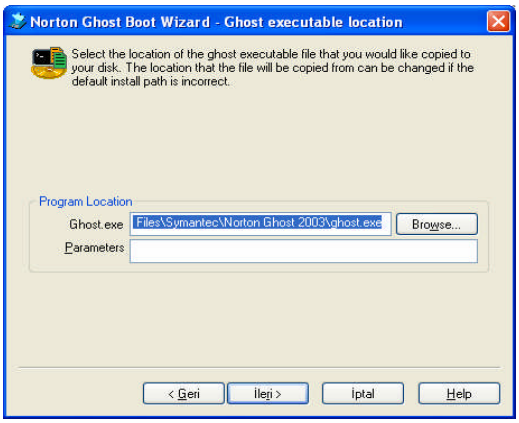
Adım 2: Standart Ghost Book Disk seçilip **İleri** tıklanarak devam edilir.



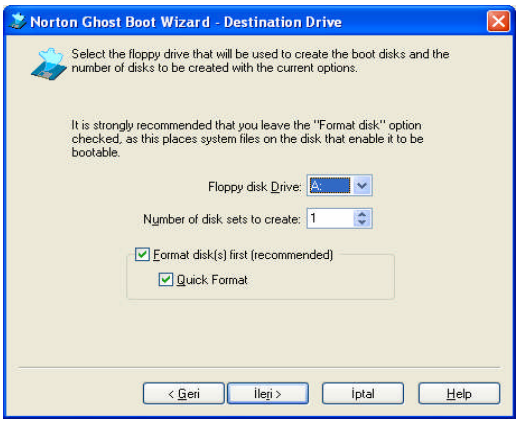
Adım 3: Advaced ile USB sürücüleride eklenerek USB desteğide alınabilir. **İleri** tıklanarak devam edilir.



Adım 4: DOS açılışı yapmak için PC-DOS seçilerek. **İleri** tıklanarak devam edilir.

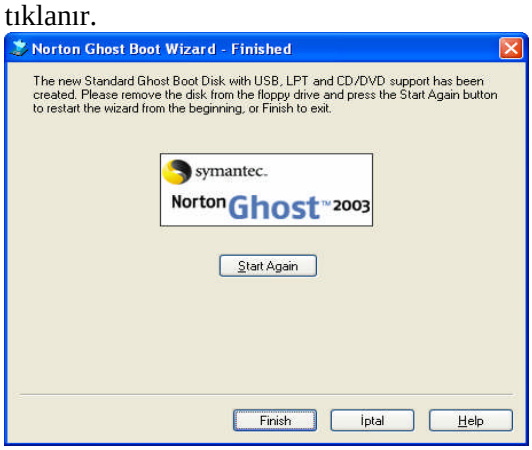


Adım 5: Kopyası alınacak Ghost DOS programı (ghost.exe) seçili gelir. **İleri** tıklanır.



Adım 6: Açılış dosyaları ve ghost programın yazılacağı yer (A:) seçilip **İleri** tıklanır.

Adım 7: Diskete yazılacak toplu işlem dosyası **AUTOEXEC.BAT** dosyasının içeriği listelenir. **İleri** tıklanır.



Adım 8: Disket biçimlendirilip dosyalar kopyalanır ve **Finish** ile işlem bitirilir.

Disketdeki dosyaların tümünü Nero ile CD ye yazdırısanız Ghost Boot CD elde edilir.

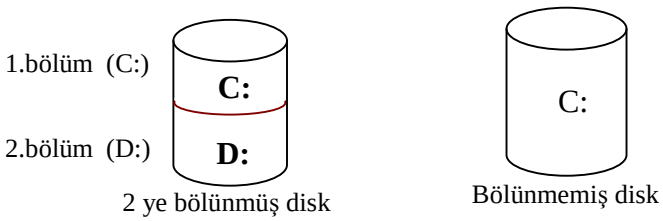
2.3.2. İmaj Almak

DOS altındaki Ghost çalıştırılarak 4 değişik şekilde imaj alınabilir;

- Sabit diskten başka bir sabit diske imaj, (disk to disk (1)).
- Sabit diskin bir bölümünden yine aynı diskin diğer bölümüne yada sistemdeki mevcut diğer sabit diskin bölümüne imaj, (partition to partition (2)).
- Sabit diskin tümü başka bir diske dosya olarak imaj,(disk to image (3))
- Sabit diskin bir bölümü aynı diskin diğer bölümüne ya da başka bir diske imaj alınabilir.(partition to image (3))

Bu seçenekleri anlamak için disk, partition kavramlarını açıklayalım.

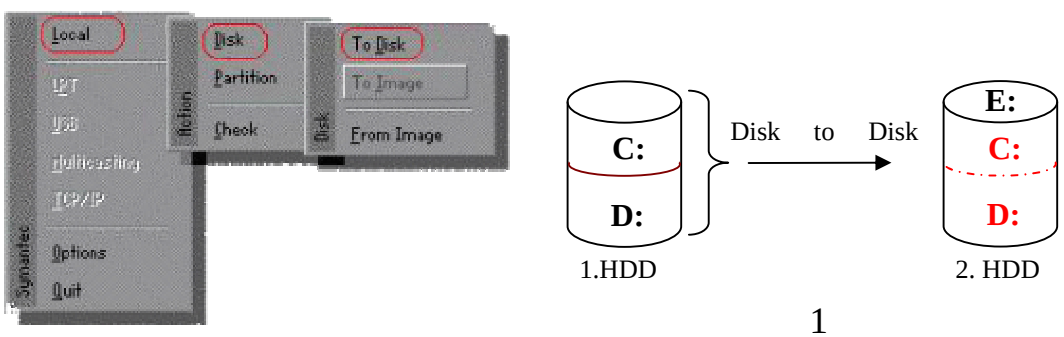
Her PC'nin mutlaka bir sabit diski olmak zorundadır. Çünkü çalıştırılacak programlar disk üzerine kurulur ve sürücü harfleriyle gösterilir. Eğer disk 1 adet ise C: sürücüsü vardır. Ancak dosyaların ayrıştırılması, yedeklenmesi yada başka bir işletim sistemi kurabilmek için ikinci bir sürücüyede (D:) ihtiyaç duyulur. Bunun için ya ikinci bir sabit diskin alınması gerekir ya da ekonomik olması bakımından mevcut disk birden fazla parçalara bölünür. Burada sabit diskin kendisine **disk**, sabit diskin bölünmüş ve sanal olarak bir sürücü harfiyle atanmış parçaların herbirine **bölüm** (**partition**) denir.



Resim 2.5: Sabitdisk ve bölüm (partition) kavramlarının şekilsel gösterimi

Disk ten Diske (1) = Local → Disk → to Disk

Daha önceden örnek olarak kurulmuş bir diskin, aynı türden başka bir PC için kurulacak diske yedeklenmesi amacıyla kullanılır. Diskin bölümleme, biçimleme yapılmasına gerek kalmadan kolay kurulum yapılmış olur. Buruda ön koşul olarak PC anakart ve disklerin birebir aynı olması gerekir. Resim 2. deki çizime göre; C: (30 GByte) ve D: (70 GByte) olarak ikiye bölünmüş olan 1.HDD, disk to disk ile 2.HDD ye klonlanırsa, 2.HDD nin kapasitesi 100 GByte tan büyük olsa dahi 30 ve 70 GByte olarak C: ve D: nin aynı özelliklerinde klonlanır. Ghost burada hem bölümlendirme (fdisk) hem biçimlendirme (format) işlemini yapılmış hemde tüm programları kurulmuş olur.



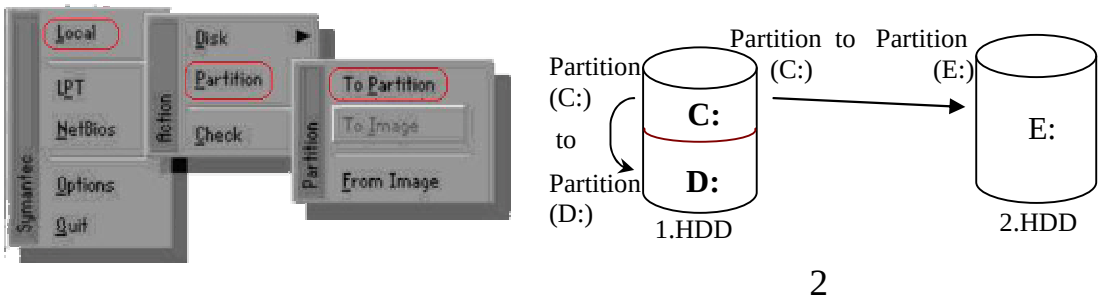
Resim 2.6: Diskten diske imaj almak için çalıştırma başlangıcı

Partitiondan partitiona (2) = Local → Partition → to Partition

Bir sabit diskiniz var diyelim ve yine imaj almak istiyorsunuz. Bu durumda sabit diskiniz tek bölümden oluşuyor ise CD yada DVD'ye kayıt yapmanız gerekiyor.

Bir PC içinde genellikle tek sabitdisk kullanıldığı ve bilgilerinde bir yerlerde silinmeden kalması istendiği için mevcut disk iki veya daha fazla bölüme bölünür. Bu parçaların her birine partition denir. 1.bölüme C: sürücüsü olarak işletim sistemi kurulur, 2.bölüm ise D: sürücüsü olarak yedekleme amacıyla kullanılır.

Bu uygulamanın disk to diskten ayıran en büyük özelliği, farklı kapasitelerdeki disk bölümlerinin kapasitelerini değiştirmeden klonlanmasıdır.

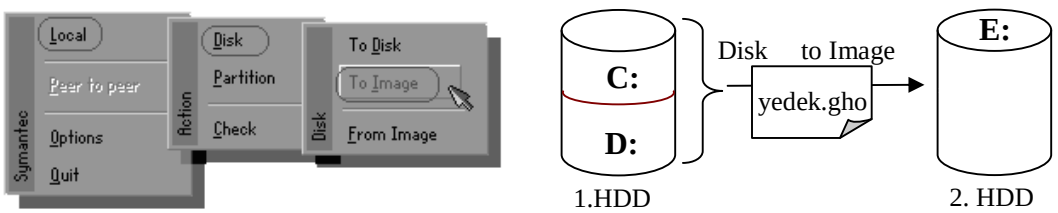


2

Resim 2.7: Diskin bir bölümünden diğer bir bölümüne yada başka bir diskin bölümüne dosya halinde imaj almak için çalıştırma başlangıcı

Diskten dosya ya (3) = Local → Disk → to Image

Düzgün çalışan ve tüm programları kurulmuş bir PC, diğer yeni PC lerde de kullanılıyor ise imaj dosya haline getirilerek Disk yada CD ye kaydedilerek kullanılır. Genellikle aynı büyüklüğe sahip ve bölümlemesi yapılacak diskleri olan laboratuvar, internet kafe, birbirinin aynı PC servislerinin kurulumu v.b. olan yerlerde tercih edilir.

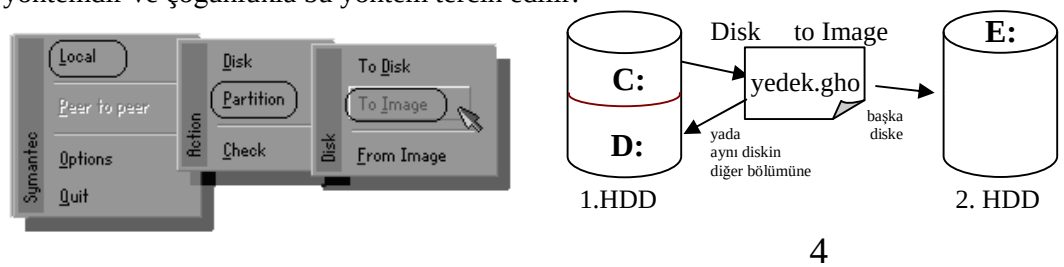


3

Resim 2.8 : Diskin bütününü, başka bir diskin bölümüne dosya halinde imaj almak için çalıştırma başlangıcı

Partitiondan dosya ya (4) = Local → Partition → to Image

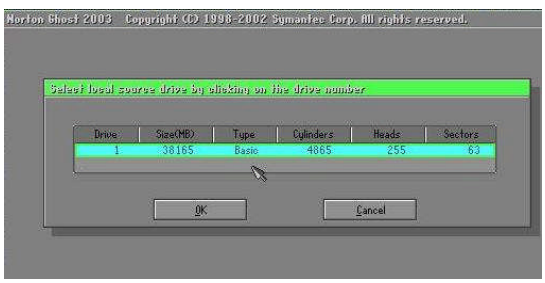
Genellikle Ghost, düzgün çalışan ve tüm programları kurulmuş bir PC'nin herhangi bir sorunla karşılaşması durumunda tekrar düzgün geri kurmak için dosya halinde diğer bölüme imajı dosya halinde yedek alınır. Ev ve ofis kullanıcılarının ençok kullandığı yöntemdir ve çoğunlukla bu yöntem tercih edilir.



Resim 2.9 :Partitiondan başka bir diske yada aynı diskin diger partitionuna dosya olarak imaj yedeği almak için çalıştırma başlangıcı

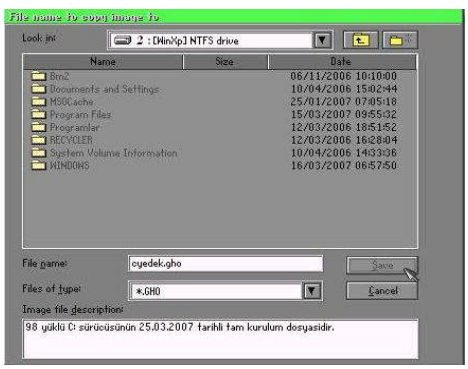
Alıştırma: C: bölümünü dosya olarak D: bölümüne yedek.gho ismiyle imaj alalım.

Adım 1- Local →Partition→To Image ile yedek almaya başlıyoruz.



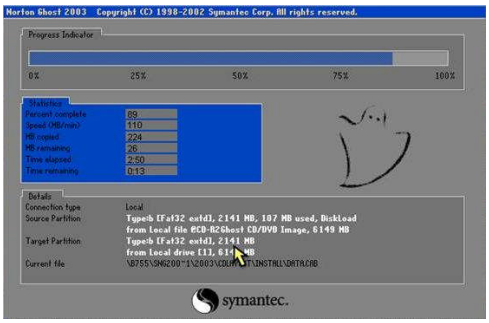
Adım 2- Yedeği alınacak sabit disk seçilip **OK** tıklanır.

Adım 3- Sabit disk içindeki partitionlar listelenir. 1.partition C: seçilip. OK tıklanır.



Adım 4- Saklanacağı sürücü seçilip **File name** kısmına dosya ismi verilir ve **Save** ile kayıt işlemi başlatılır.

Adım 5- Dosyanın daha az yer kaplaması istenirse, sıkıştırma oranı sorulur. **No**:Yok, **Fast**:orta, **High**:yüksek sıkıştırma oranıdır.

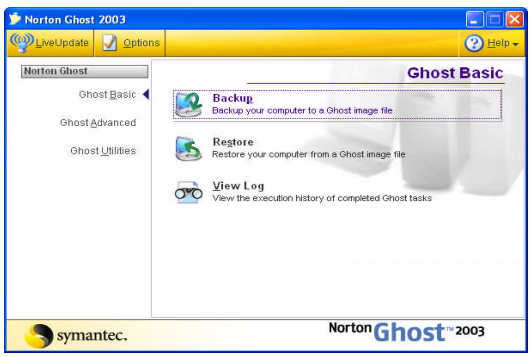


Adım 6- Dosyalar tek parça halinde paketlenerek kayıt işlemi gerçekleşir.

Adım 7- Bitince Continue ile işlem sonlandırılır yada Reset Computer ile yeniden açılış yapması sağlanır.

2.3.3. İmajı Dosyalarını CD'ye Yazmak

Programımızı Başlat → Programlar → Norton Ghost 2003 → Norton Ghost ile çalıştıralım ve aşağıdaki pencereye ulaşalım.

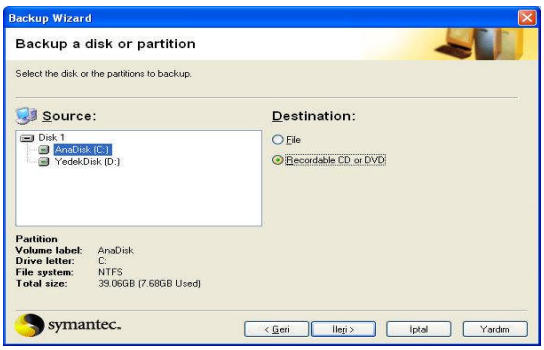


Adım 1- Backup tıklanıp **Backup Wizard** penceresi **İleri** ile devam edilir.

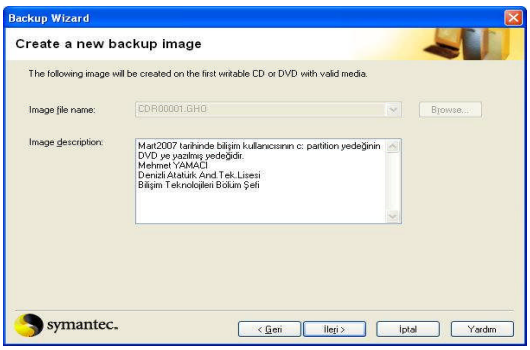
Backup : Mevcut disk yada partitionun birebir kopyası tek dosya haline paketlenir. Buna imaj denir.

Restore : Daha önceden alınmış imaj dosyasından geriyükleme yapılır.

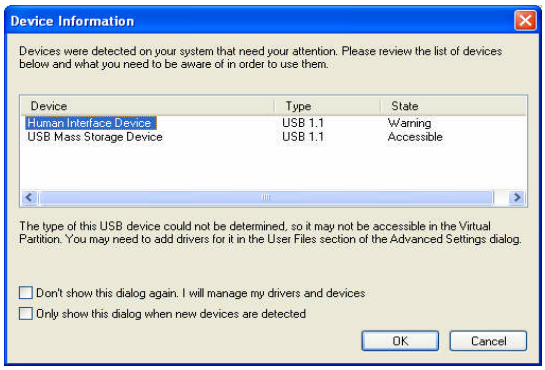
Ghost Utilities sekmesindeki **Norton Ghost Boot Wizard** ile açılış disketi yapılır.



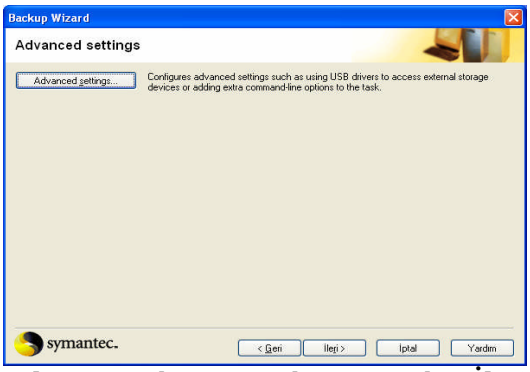
Adım 2- Yedeği alınacak **partition** (**C:**) seçilip, CD yada DVD kaydediciniz varsa **Recordable CD/DVD**'yi seçip **İleri** tıklanır. Dosya olarak tutulacaksa **File** seçilebilir.



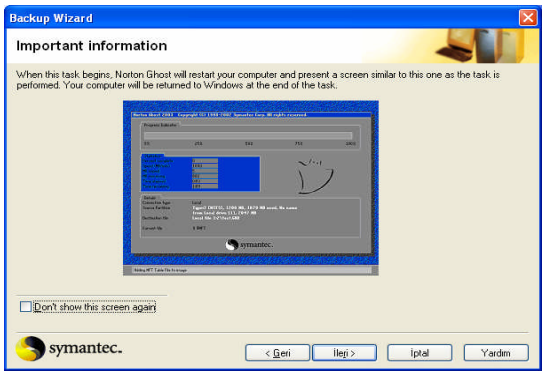
Adım 3- CDR00001.GHO ismi otomatik olarak atılmıştır. **Image description** penceresine hatırlamanızı sağlayacak açıklama yazabilirsiniz.



Adım 4- Herhangi bir değişiklik yapmadan **Ok** ile pencere geçilir.

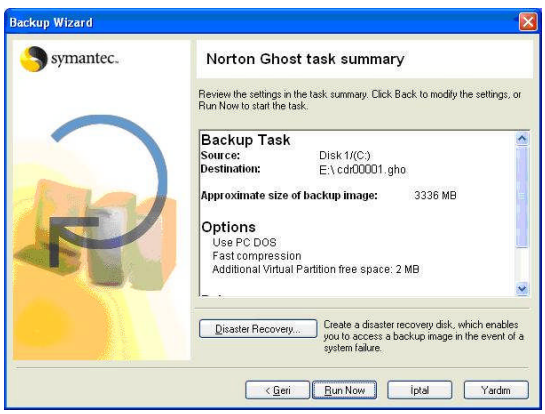


Adım 5- Gelişmiş ayarlara girmeden **İleri** ile devam edilir.

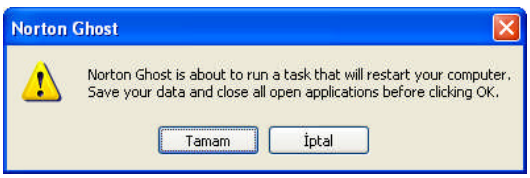


Adım 6- Yedek işleminin başlayacağı ve kutucuk işaretlenmezse ekrandaki pencerenin DOS yükleme sırasında görüntülenmesini sağlar. **İleri** ile devam edilir.

Adım 5- DOS ile açılış yapılarak yükleme yapılabileceği ifade ediliyor. **Continue** ile devam edilir.



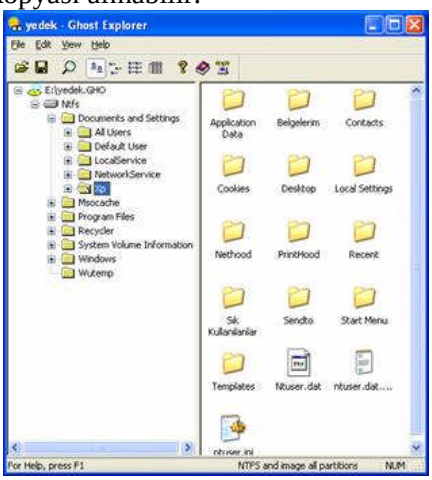
Adım 6- Yapacağı işlemlerin raporu listelenmiştir. **Run Now** seçilir.



Adım 7- Yapdığınız çalışmalarınız var ise kaydedin. Bilgisayarınız kapanıp açılacak. **Tamam** ile devam edin

Artık imaj dosyanız CD yada DVD'ye yazıldı. Aynı işlemi **Adım 2**'de File seçeneği ile gerçekleştirerek devam edersek yazacağınız isim, belirteceğiniz disk içindeki bir klasörün içine (örneğin d:\yedek\martyed.gho) bir imaj dosyasıda oluşturabilirsiniz. Bu imaj dosyası içinde C: sürücüsündeki tüm dosyalar paketlenmiş durumdadır. Windows, herhangi bir nedenden açılamaz hale geldiğinde DOS yada CD ile açılış yapıp geri yükleme (restore) gerçekleştirilebilinir.

Paketli bu gho uzantılı dosyanın içerisinde birçok dosya vardır. Bu dosyaların bazılarına yeniden kurulum yapmadan kullanma ihtiyacınız doğabilir. Bu imaj dosyası içinden herhangi bir dosyaya ulaşmanız gerektiğinde Ghost programının kurulduğu klasörün içinde (C:\Program Files\Symantec\Norton Ghost 2003) **GhostExp.exe** isimli bir dosya vardır. **Ghost Explorer** olarak isimlendirilen bu program çalıştırılıp, **File → Open** seçeneği kullanılarak daha önceden yedek alınan dasyanın içeriği tıpkı **Windows Gezgini** ile bakar gibi görülebilir, dosyaların kopyası alınabilir.



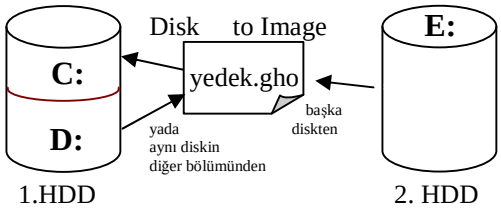
Resim 2.10: yedek.gho dosyasının GhostExplorer ile içerisinin görüntülenmesi

2.3.4. İmajı Geri Yüklemek

Sistemimize kurulu olan Ghost 2003 programının Restore komutu ile görsel geri alma işlemi yapılabilir. Genellikle bu işlem WINDOWS'sunuzun açılamaz duruma geldiği hallerde gerçekleştirildiği ve virüsün tehdit ettiği durumlarda yapıldığına göre temiz bir DOS açılışı ile yapılması daha uygun olacaktır.

DOS Geri yükleme sırasında 2 yöntem vardır. Bunlar;

- Disk olarak alınmış imaj dosyasından geri yükleme , (disk to from image (1)).
- Partition olarak alınmış imaj dosyasından geri yükleme , (partition to from image (2)).



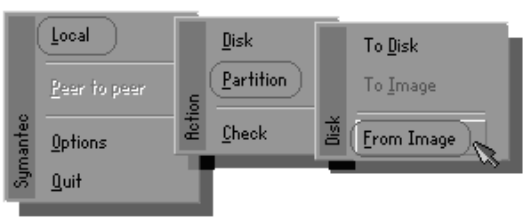
Resim 2.9: Aynı diskin D: bölümündeki ya da başka disk-disket-CD'deki imaj dosyası C: ye geri yüklenebilir

Bu işleme başlamak için;PC'nizi bir açılış disketi yada açılış CD'si ile açın. (CD den yada disketten ilk açılış için BIOS boot ayarlarını önceden yapmış olmanız gereklidir. Bazı BIOS'larda F12 ile boot menüsü ekranıda getirilebilir)

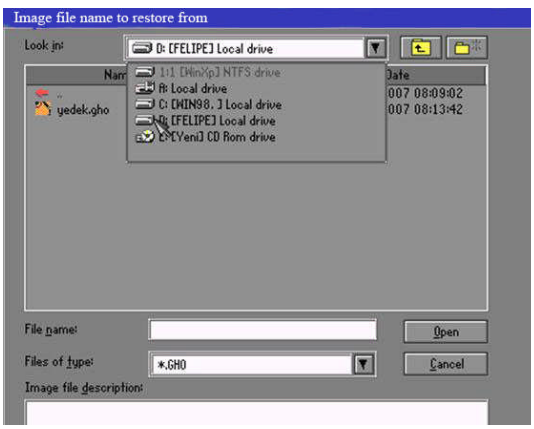
A:\> GHOST ↵

yazarak programı çalıştıralım.

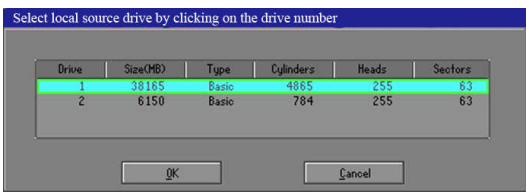
Alıştırma: DOS açılış haline getirilimiş ve CD'ye atılmış imaj dosyasını C: bölümüne geri yükleme işlemini yapalım.



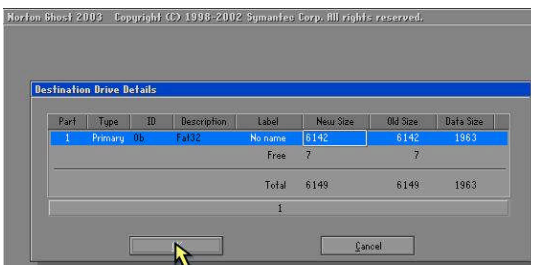
Adım 1- Local →Partition→Frome Image



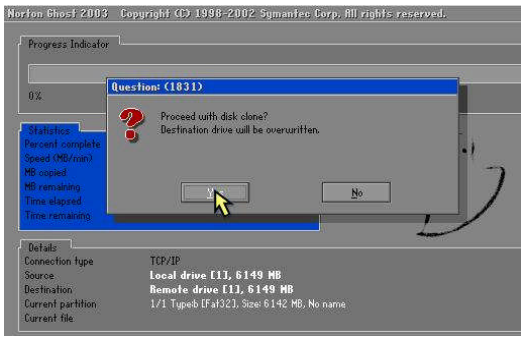
Adım 2- Daha önceden alınan imaj dosyası seçilip **Open** tıklanır



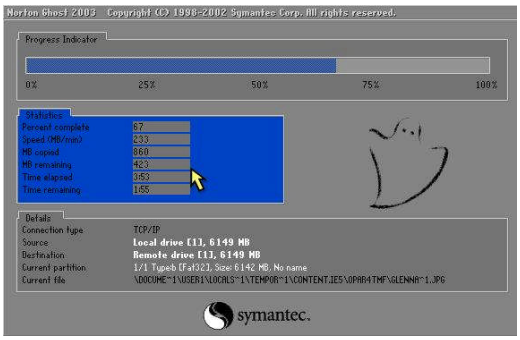
Adım 2- Yüklemenin yapılacağı partitiona ait disk seçilip **OK** tıklanır



Adım 3- Yüklemesi yapılacak partition seçilip **OK** tıklanır



Adım 4- Partition içindeki tüm programların silinip üzerine yeniden yazılacağını belirten uyarı gelir.



Adım 5- Dosyalar yüklenmeye başlar. %100 oluncaya kadar devam eder.

Adım 6- Yüklemenin başarıyla tamamlandığını belirten açıklamadan sonra **Reset Computer** ile açılış yeniden başlatılır.

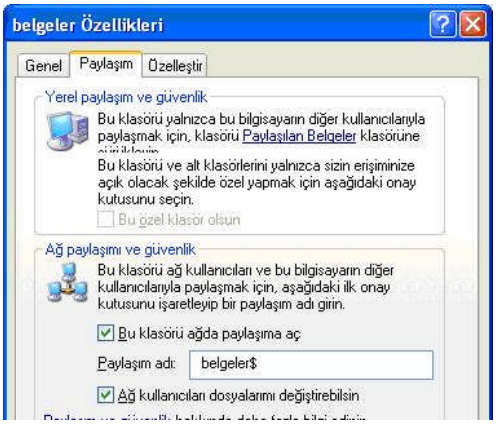
2.4. Ağ Üzerinden Yedekleme

2.4.1 Ağ Komşularından Bilgisayara Ulaşmak

Diskinizde yeterli yer olmadığı zaman yedeğinizi almak için taşınabilir depolama cihazları kullanmakta bir çözüm olarak düşünülebilir. Fakat bunun için ekonomik ihtiyaçlar gerektirmektedir. Bir laboratuvar ortamında ağ yapılandırması var ise ağ içinde bulunan bilgisayarların herhangi birinde bulunan program yada dosya diğer bilgisayarlar tarafından da kullanılabilir. Laboratuvarda bulunan tüm bilgisayarlar, dosyalarını belirtilen paylaşımlı klasörde kayıt altına alabilir. Bunun için ağ üzerinde kayıt yapılacak klasörün tam paylaşımlı halde hizmete açılmış olması gerekir.

Ağ üzerindeki AEML isimli bilgisayarda belgeler isimli bir paylaşım açalım**.**

Adım 1- Belgeler isimli bir klasör oluşturun.
Adım 2- Klasör üzerinde sağ tıklayın
Adım 3- Paylaşım ve Güvenliki tıklayın
(*XP Home içinde şifre ile paylaştırma yoktur. Paylaşımı detaylandırmak için basit paylaşım özelliği seçilmemelidir*.)



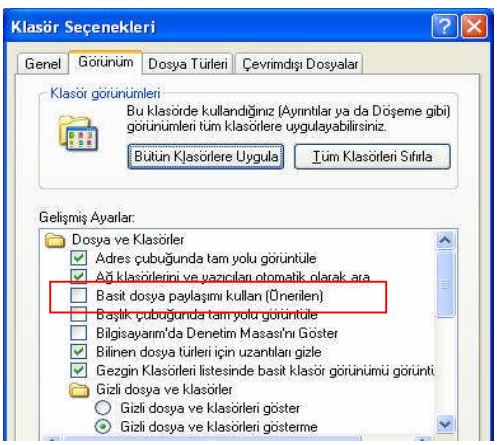
Adım 4- Basit paylaşımda ;

Bu klasörü ağda paylaşıma aç seçilirse, ağ üzerinden okunup, açılabilir.

Paylaşım adı bölümüne, ağda görülecek ismi yazılır.

Ağ kullanıcıları dosyalarımı değiştirebilsin seçilirse, ağ üzerindekilerin okuyup açmanın yanı sıra yazma, değiştirme hatta silme yetkisi verilmiş olur. Tabiî ki bu durum dışarıdan virüs girişi ve hertürlü tehlike anlamına gelmektedir.

(**Eğer ağda bulunan PC lerin paylaşım adını görmesini istemiyorsanız, paylaşım adının sonuna **$** işareti koyunuz - **belgeler$** gibi*



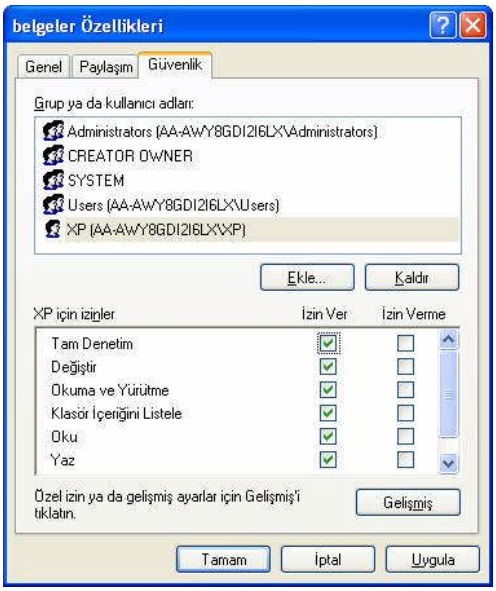
yada paylaşımın kullanıcıya özel verilmesi istenilirse;

1- Belgelerim penceresi (veya başka pencere) açılır,

2- Araçlar - Klasör Seçenekleri seçilir,

3- **Basit dosya paylaşımını kullan** seçeneğinin onayı kaldırılır.

Artık istediğiniz kullanıcıya paylaşım verebilirsiniz.



Bu durumda **Paylaşım ve Güvenlik** seçildiğinde yandaki pencere karşınıza gelecektir.

Sisteminize tanımladığınız kullanıcı isimleri sizin belirlediğiniz yetkilere uygun kullanır.

Bunlar;
-**Oku :** Sadece okunabilir,
-**Okuma ve Yürütme :**Okunur ve çalıştırılır,
-**Yaz :** İçerisine bilgi eklenebilir.
-**Değiştir :** Açılıp içerik değiştirilebilir.
-**Tam denetim:** Tüm işlemler yapılabilir.

Bunlar; okuma, çalıştırma, yazma, silme, değiştirme işlemleridir.

Ağ üzerinde paylaşıma açılan klasör içindeki bilgiler sadece okunacak ise Bu klasörü ağda paylaşıma aç yada basit paylaşımda değil ise Oku aktif yapılarak paylaşıma açılmış olması yeterlidir. Ağ üzerendeki paylaşıma açılmış klasöre erişmek için;

- Masaüstünden **Ağ Bağlatılarım** çift tıklanır.
- Gelen pencereden Çalışma grubu bilgisayarlarını göster tıklanır.
- Veri alacağınız PC bu çalışma grubunda görünüyor ise çift tıklayarak içerisindeki paylaşıma açılmış olan paylaşım isimlerine ulaşılır. PC başka bir çalışma grubu içinde ise pencerenin araç çubuğunda bulunan **Yukarı** düğmesi ile ağ üzerindeki çalışma grupları listelenir. Girilecek grup ismi çift tıklanıp paylaşımın bulunduğu bilgisayar ismide çift tıklanarak paylaşım isimlerine ulaşılır.
- Girilecek paylaşım ismide çift tıklanarak içerisindeki dosyalar görüntülenir. Gerekiyorsa duruma göre kopyası alınır.

Tam paylaşıma açılan klasör içine dışarıdan kopyalanacak bir program parçacığının bilgisayarınızda verebileceği zararları grup halinde tartışın.Tam paylaşıma açılan bu klasör C: sürücüsü ise dışarıdan bu bilgisayara neler yapılabir?

Ağ üzerindeki **aeml** isimli bilgisayarda **belgeler** isimli bir paylaşıma ulaştığımızı düşündüğümüze göre Paylaşım içine girdiğinizde pencerenizin adres çubuğunda yazan komut satırı ise aşağıdaki gibi olması gerekir.

Bu komut satırındaki ifadeleri şöyle açıklayabiliriz;

\\ aeml \ belgeler

Ağda bilgisayar adını **paylaşım adını**

Ağ komşularındaki aeml isimli PC"nin içindeki belgeler klasörüne girilir.

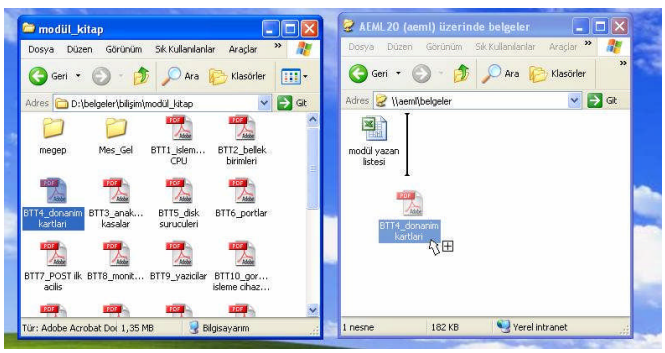
Resim 2.1: Ağdaki aeml bilgisayarındaki paylaşıma açılmış belgeler penceresi

Bilgisayarım yada Belgelerim penceresini açık adres çubuğuna **\\aeml\belgeler** yazıp Enter tuşuna basarak hızlıca giriş yapılabilir.

2.4.2. Verileri Diğer Bilgisayara Kopyalamak

Ağ üzerinde bulunan **aeml** bilgisayarındaki **belgeler** isim ile yazılabilir şekilde paylaşıma açılmış klasöre, bilgisayarımızdaki verilerimizi kopyala yapıştır yada sürükle bırak ile kopyalayabiliriz.

Paylaşıma ulaşmak için **Ağ Bağlantılarım** çift tıklanarak kayıt yapılacak bilgisayara ulaşılabileceği gibi ilgili pencerenin adres çubuğuna **\\aeml\belgeler** yazıp Enter tuşuna basılarak da gerçekleştirilebilir . Verilerinizi kopyalayacağınız pencere açılmış olacaktır. Artık kendi bilgisayarınızda bir pencere açmış gibi kopyalama işlemlerini uygulayabilirsiniz.



Resim 2.2: Windows güvenlik merkezi ile sisteminizi güncel tutun

2.4.3. Kopyalanan Verileri CD ye Yazmak

Ağ üzerinde veri aktarım hızı, ağ üzerindeki veri trafik yoğunluğuna bağlı olarak değişkenlik gösterir. CD ye yazma işlemi sırasında, CD ye yazılacak veri ağdaki bir PC den direkt olarak CD içine yazılmak istenirse ağ trafiği kesintilere neden olabilir ve yazım hızını da oldukça düşürür. Bu tip sorunlarla karşılaşmamak için öncelikle CD ye yazacağınız verileri kendi bilgisayarınızda bir klasör içine kopyalamalısınız.

Bu işlemi gerçekleştirdikten sonra, daha önce **Klasörü CD ye yazmak** başlıklı 2.1.2. konusundaki adımları kullanılarak CD'ye yazabilirsiniz.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ "Sisteminizdeki verilerin yedeğini oluşturduğunuz yeni bir klasöre alınız.	➢ XCOPY
➢ Oluşturduğunuz bu klasörü CDye yazdırınız.	
➢ Yedekleme işlemini Windows Yedekleme/Geri Yükleme Sihirbazı ile gerçekleştiriniz.	➢ Donatılar → Sistem Araçları
➢ Bilgisayar sisteminizin imajını başka bir disk üzerine alınız	➢ Disk to disk
➢ Sisteminizi ağ üzerinden yedekleyiniz.	

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıdaki sorulardan; sonunda parantez olanlar doğru yanlış sorularıdır. Verilen ifadeye göre parantez içine doğru ise "D" , yanlış ise "Y" yazınız. Şıklı sorularda doğru şıkkı işaretleyiniz. (*Doğru-Yanlışlar 5puan, çoktan seçmeli sorular 10 puandır*)

1. Sabit diskin parçalanmış her bir parçasına partition denir ? .....D( ) Y( )

2. Yedek alınmış dosyaları geri yüklemek için Backup işlemi yapılır. .....D( ) Y( )

3. Yedekleme, XP Home İşletim Sistemine sonradan kurulur. .....D( ) Y( )

4. CD den CD ye kopya almak için Nero programı kullanılır. .....D( ) Y( )

5. Disk to Disk hem fdisk hemde format işlemini gerçekleştirir. .....D( ) Y( )

6. Bir diskin imajı dosya halinde alınırken, dosya aynı disk içine alınabilir. .....D( ) Y( )

7. Aşağıdakilerden hangisi imaj programı değildir?
A) Acronis B) Restore C) ImageReady D) Ghost

8. Diskin tümünün yedeğini, dosya olarak almak için hangi sıra takip edilir?
A) Local→Partition→to Image B) Local→Disk→from Image
C) Local→Disk→to Image D) Local→Partition→to Partition

9. Ağ üzerinde paylaşım isminizin görüntülenmesini istemiyorsanız başına hangi işareti koyarız?
A) & B) $ C) @ D) #

10. \\ işareti neyi temsil eder?
A) Sürücü B) Partition C) Ağ D) Klasör

11. Ghost programında geri yükleme yapılırken imaj dosyanızın geri yükleneceği yer için hangi ifade kullanılır?
A) Local B) Drive C) Source D) Destination

12. Hangisi DOS altında imaj alındıktan sonra geri yükleme işlemidir?
A) disk to image B) partition to partition C) disk from image D) disk to disk

13. Birden fazla komutu çalıştıran toplu işlem dosyasına ne denir?
A) Ghost.exe B) Autoexec.bat C) Nero StartSmart D) Backup.exe

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 geri dönerek tekrar inceleyiniz

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

Modül ile kazandığınız yeterliği aşağıdaki kıstaslara göre değerlendiriniz.

	DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayır
1	Virüs, trojan, spy'ın zarar verme şekillerini anlatabildiniz mi?		
2	Antivirüs programını kurup ayarlarını yapabildiniz mi?		
3	Antivirüs programınızı güncelleyebildiniz mi?		
4	Sistemi virüs testinden geçirebildiniz mi?		
5	Verileri bir sürücüden başka bir sürücüye kopyalayabildiniz mi?		
6	Verileri CD ye yazabildiniz mi?		
7	Windows Yedeklemeyi kullanarak yedekleme yapabildi niz mi?		
8	Yedekleme ayarlarını öğretildiği şekilde uygulayabildi niz mi?		
9	Image Programını kurabildi niz mi?		
10	Disk veya bölümün (partitionun) imajının alabildi niz mi?		
11	Ağ kullanarak verilerini kullanıma açabildi niz mi?		
12	Verilerini ağdaki başka bir bilgisayara kopyalayabildi niz mi?		
13	Geri yükleme noktası oluşturabildiniz mi?		
14	Oluşturduğu geri yükleme noktasına dönebildiniz mi?		

DEĞERLENDİRME

Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

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

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

1	**Y**
2	**D**
3	**D**
4	**Y**
5	**D**
6	**Y**
7	**B**
8	**B**
9	**A**
10	**C**
11	**C**
12	**A**
13	**D**

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

1	**D**
2	**Y**
3	**D**
4	**D**
5	**D**
6	**Y**
7	**C**
8	**C**
9	**B**
10	**C**
11	**D**
12	**C**
13	**B**

ÖNERİLEN KAYNAKLAR

- www.antivirus.odtu.edu.tr
- www.bid.ankara.edu.tr/yardim.html
- www.bilgisayardershanesi.com
- www.bilisimlisesi.com
- www.bim.gazi.edu.tr
- www.chip.com.tr
- www.kaspersky.com
- www.mcafee.com
- www.microsoft.com/turkiye
- www.olympos.org
- www.pandasoftware.com
- www.pcworld.com.tr
- http://security.symantec.com
- www.wikipedia.org
- www.yenidownload.com/yardimmerkezi.asp

KAYNAKÇA

- http://agguvenligi.hakkindabilgi.com
- www.antivirus.odtu.edu.tr
- www.bid.ankara.edu.tr/yardim.html
- www.bilgisayardershanesi.com
- www.bim.gazi.edu.tr/virüsler.htm
- www.chip.com.tr
- www.cisecurity.org
- http://csirt.ulakbim.gov.tr/dokumanlar/
- www.kaspersky.com
- www.mcafee.com
- www.microsoft.com/turkiye/athome/security/default.mspx
- www.olympos.org
- www.pandasoftware.com
- http://pcpratik.blogspot.com
- www.pcworld.com.tr
- http://security.symantec.com
- www.wikipedia.org
- www.yenidownload.com/yardimmerkezi.asp