



# YAZILIM, YAZILIM TÜRLEİ

Dr. Günay TEMÜR / KAYNAŞLI MESLEK YÜKSEKOKULU

# Bilgisayar

## Donanım

## Yazılım

### Harici (Dış) Donanımlar

### Dahili (İç) Donanımlar

### Sistem Yazılımları

### Uygulama Yazılımları

Klavye  
Mouse

WEB Cam  
Mikrofon

Anakart  
İşlemci  
Ram  
GPU

Sabit Disk  
Ethernet Kartı  
Ses Kartı

PC İşletim  
Sistemleri

Mobil İşletim  
Sistemleri

Oyunlar

Office  
Programları

Monitör  
Hoparlör

Yazıcı  
Tarayıcı

Güç Kaynağı  
Soğutucular

Kasa  
CD- DVD  
Sürücüler

Windows  
Mac OS  
Linux  
Pardus

Android  
IOS  
Windows Mobile

Virüs  
Programları

Web Programları

# YAZILIM

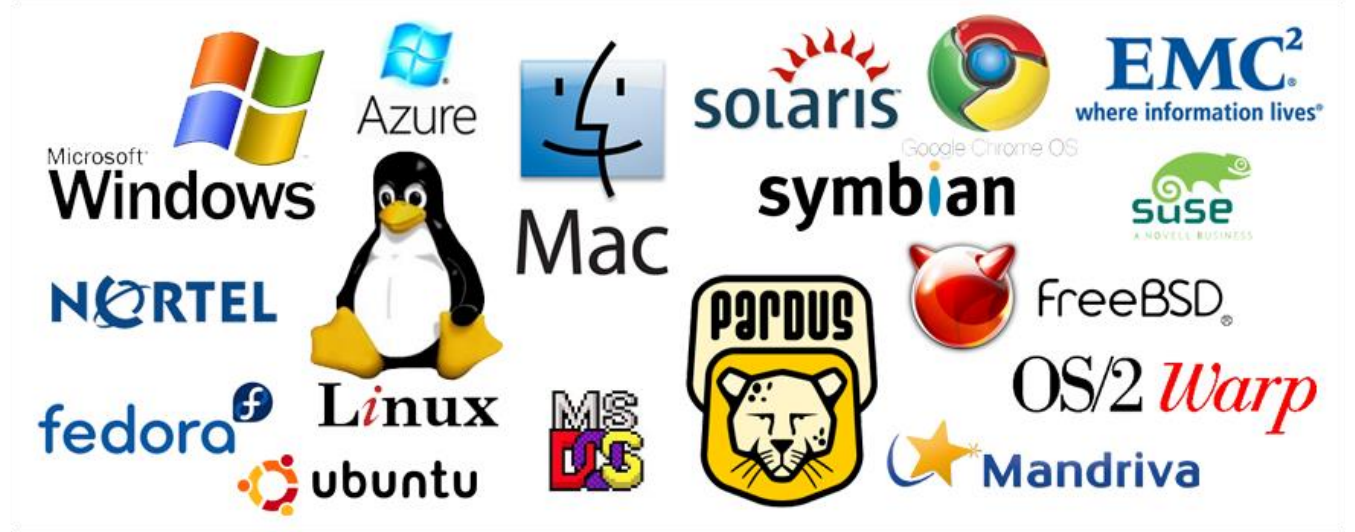
Bilgisayar donanımının istenilen amaçlar doğrultusunda çalıştırılmasını ve kullanıcının bilgisayarda istediđi işlemleri yapabilmesini sağlayan programlardır.

Örneđin; resim yapmamızı sağlayan “Paint”, internette gezinmemizi sağlayan Google Chrome, görüntülü konuşma yaptığımız Skype ve Whatsapp, virüsleri temizleyen Security gibi tüm programlar birer yazılımdır.

# YAZILIM ÇEŞİTLERİ

## Sistem Yazılımları

Sistem yazılımlarına İşletim Sistemleri de diyebiliriz. Bilgisayarımızın ya da akıllı telefonumuzun açıldığı andan kapandığı ana kadar kullanıldığı, tüm donanım ve diğer tüm yazılımların yönetimini sağlayan en temel yazılımlardır.



# YAZILIM ÇEŞİTLERİ

## Uygulama Yazılımları

Uygulama Yazılımları: Programcılar tarafından programlama dillerinden biri ile belirli konulardaki problemlerin çözümüne yönelik kullanıma sunulmuş yazılımlardır. Uygulama yazılımları hangi sistem yazılımına (İşletim Sistemine) uygun yazılmışlarsa o sistem yazılımı altında çalışırlar. Değişik amaçlara yönelik hazırlanmış binlerce uygulama yazılımı bulunmaktadır.



# KULLANIM HAKLARINA GÖRE YAZILIM ÇEŞİTLERİ

## Lisanslı Yazılım:

Kullanabilmek için lisans hakkının satın alınmasının gerektiği yazılımlardır.

Örnek: MS Office ,Windows 10 vs

## Demo Yazılımlar:

Tanıtım amacıyla bir süreliğine ücretsiz olarak kullanılabilen yazılımlardır. Bu yazılım türünde üretici 10 Gün veya 30 Gün gibi bir süre size yazılımı ücretsiz sunar. Bu süre dolduğunda yazılımı kullanmaya devam etmeniz için lisans haklarını satın almanız gerekmektedir.

Örnek: Çeşitli antivirüs yazılımları.

# KULLANIM HAKLARINA GÖRE YAZILIM ÇEŞİTLERİ

## Freeware (Ücretsiz) Yazılımlar:

Kullanıcıdan her hangi bir ücret talep etmeden CD, disket veya internet yoluyla dağıtılarak kullanıma sunulan yazılımlardır.

Örnek: VLC Media Player, Winrar vs.

## BETA Yazılımlar:

Üreticinin yazılımın eksikliklerinin test edilmesi amacıyla piyasaya sürdüğü yazılımlardır. Bu yazılımlar bir süre kullanıcılara sunulur içeriğindeki eksiklikler veya olumsuz yönler test edilir ve bu eksiklikler giderildiğinde asıl yazılım lisanslı, demo veya bedava olarak tekrar piyasaya sürülür.

# KAYNAĞINA GÖRE YAZILIM ÇEŞİTLERİ

## Avantajları

- Kullanıcı özgürdür.
- Güvenlidir.
- Hızlıdır.
- Beğenilmeyen kısımlar değiştirilebilir.
- Sağlamdır.
- Yazılım korsanlarının yaptıkları kolayca tespit edilebilir.
- Düşük maliyetlidir.

## Dezavantajları

- Serbestçe dağıtılıyor olması; insanlar üzerindeki güveni azaltmıştır.
- Teknik destek ve donanım açısından eksiklikleri vardır.
- Yazılımlar değiştirilebildiği için tutarlı sayılmazlar.
- Sistem hakkında belli bilgilere sahip olmayan kişilerin kullanmalarının zor olması.

## 1-Açık Kaynak Kodlu Yazılımlar (Open Source)

- Bu tür yazılımlar kaynak kodları ile birlikte dağıtılır .Bu da kullanıcıya bu kodları inceleyebilmesini, üzerinde değişiklikler yapabilmesini, geliştirebilmesini ve kendi projelerinde kullanabilmesini sağlar. Açık Kaynak Kodlu yazılımlara örnek olarak; 7 Zip, Open Office, Blender, File Zilla, Linux İşletim Sistemi, Firefox, Cam Studio gibi yazılımları verebiliriz.



# KAYNAĞINA GÖRE YAZILIM ÇEŞİTLERİ

## Avantajlar

- Öncelikle dağıtılmadığı için insanlar bunu güvenilir görmüşlerdir.
- Bu yazılımlar tutarlı yazılımlardır.
- Programlar ayrı ayrı kurulabilir.
- Kolay kurulumu vardır.
- Belli bilgi birikimine sahip olmayan biri dahi kullanabilir.

## Dezavantajlar

- Ücretlidir.
- Çok çabuk virüs bulaşır.
- Yazılımı değiştirme ve geliştirme imkanı yoktur.
- Güvenilir değildir.
- Hatalarını tanımlamak zordur.

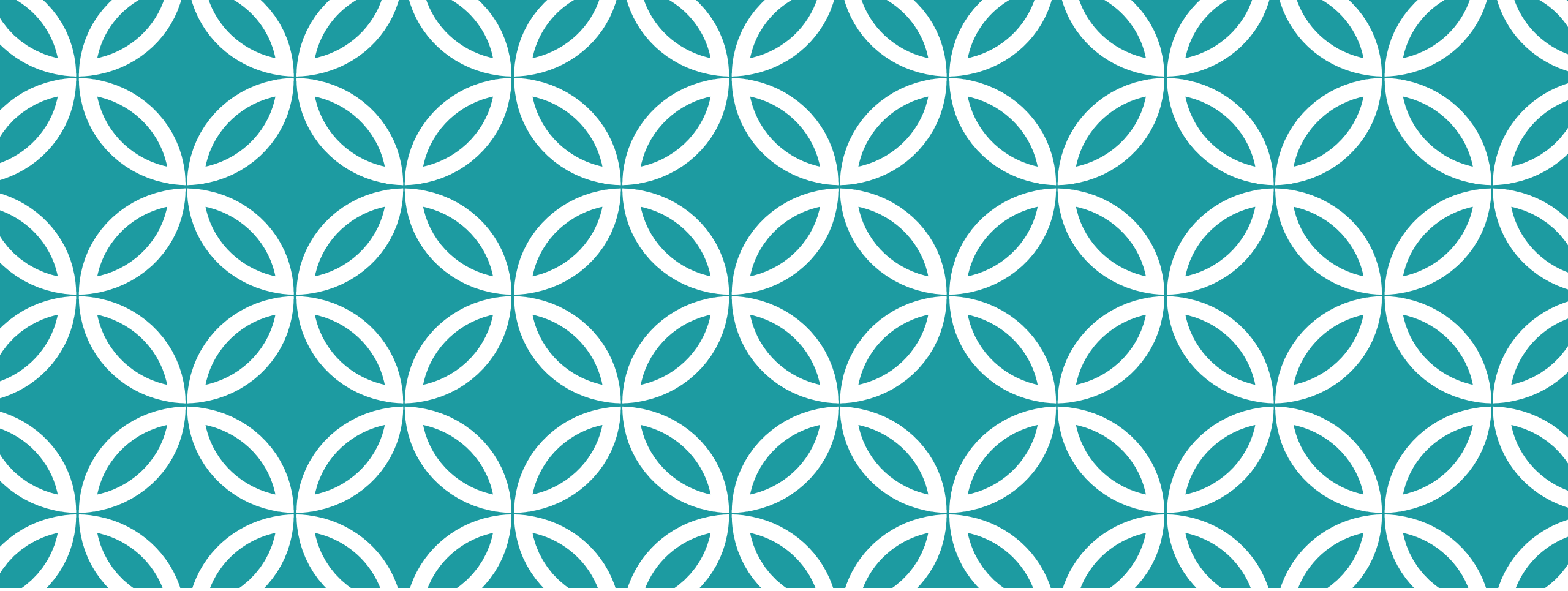
## 2- Kapalı Kaynak Kodlu Yazılımlar (Closed Source)

- Üreticinin ücretli olarak piyasaya sürdüğü, üzerinde üretici izni olmadan herhangi bir değişiklik yapılamayan lisanslı yazılımlardır. Geliştirme imkanı olmaması, hataların tanımlanmasının zor olması, güvenlik açısından sorunlar oluşturabilmesi gibi bir çok dezavantajı olmasına rağmen dünyanın en çok kullanılan yazılımları bunlardır. Kapalı Kaynak Kodlu yazılımlara örnek olarak;
- Windows İşletim Sistemi, Photoshop, MS Office, Media Player gibi yazılımları verebiliriz.

# PEKİ TÜM YAZILIMLAR FAYDALI MIDİR?

Tabi ki piyasada bulunan tüm yazılımlar faydalı değildir. Bilgisayar, tablet veya akıllı telefonumuzun bilgi güvenliğini tehdit edecek bir çok zararlı yazılım da mevcuttur.

Bu zararlı yazılımların neler olduğunu ve bunlardan nasıl korunmamız veya kurtulacağımızı Bilgi Güvenliği konumuzda detaylı olarak anlatacağız.



ZARARLI YAZILIMLAR

VİRÜSLER

# VİRÜSLER

Bilgisayar ortamına kullanıcının istemi, onayı dışında aktarılmış (trojans, worms) mevcut kullanıcı dosyalarını, bilgisayardaki yazılım ve/veya işletim sisteminin bütünlüğünü, erişilebilirliğini, gizliliğini tehdit eden yetkisiz kod parçaları ve küçük yazılımlar genel olarak virüs olarak adlandırılırlar. Bilgisayar virüsleri, bir bilgisayardan bir diğerine yayılmak ve bilgisayar sisteminin çalışmasına müdahale etmek amacıyla tasarlanmış program kodlarıdır.

# VİRÜSLER

Bilinen ilk bilgisayar virüsü, 1971 yılında BBN Technologies'de mühendis olan Robert Thomas tarafından geliştirilmiştir. "Creeper" virüsü olarak bilinen Thomas'ın deneysel programı, ARPANET'te ana bilgisayarları etkileyerek ve "I'm the creeper: Catch me if you can." teletype mesajını görüntüleyerek işlevini gerçekleştirdi.

İnternette tamamen eğlence amacıyla gezinirken veya oyun oynarken ya da başka bir bilgisayardan sadece küçük bir fotoğrafı USB belleğinize aktarırken kötü amaçlı yazılımlara (malware) maruz kalabilirsiniz. Bu zararlı yazılımlar, dosyalarınızı imha edebilir ,kötü niyetli kişilere hakkınızdaki her türlü kişisel bilgiyi verebilir, fotoğraflarınızı çekebilir ve hatta cihazınızın kontrolünü ele geçirebilirler.

# PHISHING (OLTALAMA):

Phishing, dolandırıcıların rastgele kullanıcı hesaplarına güvenilir kaynakların veya kullandığınız hizmetlerin taklit adresleri ve kopya içerikleri ile e-mail gönderdikleri bir çevrimiçi saldırı türüdür. Güvenilir bir firma veya kişinin kimliğine bürünüldüğü bir tür sosyal mühendislik saldırısıdır. Password (Şifre) ve Fishing (balık avı) kelimelerinin birleşimi ile ortaya konan bu saldırı atağında amaç Username ve Password bilgisi başta olmak üzere Bitcoin Cüzdanı, Kredi Kartı bilgilerinden tutun tüm abonelik verileriniz, program/oyun keyleriniz dahil çok kapsamlı şekilde bilgi elde etmeye yönelik olabilir.

# WORMS (SOLUCAN):

Bilgisayarınızda bulunan ağ bağlantısı sayesinde herhangi bir yerleşik dosyaya gizlenmek zorunda kalmayan solucan, her bilgisayara ağ bağlantısı üzerinden bulaşabilir. En büyük farkı, kopyalanıp çoğalması için herhangi bir insan eylemine ihtiyaç duymamasıdır. Ağların yaygın olarak kullanılmasından önce, bilgisayar solucanları bir sisteme monte edildiklerinde, kurban sistemine bağlı olan diğer depolama aygıtlarına bulaşarak, depolama ortamları üzerinden yayılmıştır. USB sürücüler hala bilgisayar solucanları için ortak bir vektördür.

# TROJAN HORSES (TRUVA ATI):

Bir program ile bilgisayarınıza yüklenen bu virüs arka planda gizli olarak çalışır. Mesela en sinsi Truva Atı türlerinden biri, bilgisayarınızı virüslerden kurtardığını iddia eden ancak bunun yerine bilgisayarınıza Truva Atı bulaştıran bir programdır. Genellikle, Truva atı, masum görünümlü bir e-posta ekinde veya ücretsiz indirmede gizlenir. Kullanıcı e-posta ekini tıkladığında veya ücretsiz programı indirdiğinde, içine gizlenmiş olan kötü amaçlı yazılım kullanıcının bilgisayar aygıtına aktarılır, içeri girdikten sonra, kötü niyetli kod , saldırganın gerçekleştirmesi için tasarladığı görevi ne olursa olsun yürütebilir.



# SPYWARE (CASUS):

İnternette dolaşırken, ziyaret edilen siteleri, bu sitelerin içeriklerini sık kullanılan programları internet üzerinden üreticisine gönderir. internette dolaşırken tuzak pencerelere tıkladığında bilgisayara kurulur

# ADWARE (REKLAM):

Sadece kullanıcı ile ilgili bilgileri kullanmazlar aynı zamanda browser ayarlarını değiştirirler. Eğer anlam veremediğiniz reklamlar karşınıza çıkıyorsa ve browserınızın ana sayfası sizin istemediğiniz bir sayfa olarak ayarlanmışsa adware virüsü bulaşmış demektir.

# KEYLOGGER (TUŞ-KAYIT):

Keylogger, uzak bilgisayara kendi kurulumunu gerçekleştirdikten sonra genellikle kendini hiç belli etmeden çalışmaya başlar ve kaydettiği verileri programlandığı zaman aralıklarında hacker 'a iletir. Genellikle tüm klavye hareketlerini ara hafızasına alır ve transfer eder. Keylogger basitçe sizin klavyeden yaptığınız her vuruşu kaydeden ve bu kayıtları kişisel bilgilerinizi çalmak isteyen kişilere gönderen programlardır. Bu yolla sizin e-mail şifreniz, kredi kartı numaranız gibi hayati önem taşıyan bilgileriniz çalınabilir.

# SCREENLOGGER (EKKRAN-KAYIT):

Keylogger ile aynı temel mantığa dayanır. Fare ile ekranda bir noktaya tıklamanız ile beraber aynı anda screen logger, adeta ekranın tamamının ya da küçük bir bölümünün (genellikle fare merkezli olarak küçük bir dörtgenin) o anki resmini çekerek bunları internet ortamında sabit bir adrese iletir.

# SPAM (YIĞIN MESAJ):

Spam, e-posta, telefon, faks gibi elektronik ortamlarda çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletiler. En yaygın spam türleri reklamlar ve ilanlardır. Elektronik posta (e-posta), internet'in en eski ve halen en vazgeçilmez iletişim araçlarından birisidir. E-posta, fiziksel, alışıla gelmiş posta alımı ya da gönderiminin elektronik olanıdır ve internet üzerinden gerçekleştirilen, düşük maliyetli ve hızlı iletilen bir yapı olduğundan; güvenlik, kimlik denetimi gibi gereklilikler göz önünde bulundurulmamıştır ve bu yüzden e-posta altyapısı günümüzde internet'in en büyük problemlerine sebep teşkil etmektedir. Yiğın ileti sadece e-posta ile sınırlı değildir. Diğer şekillerde de kullanıcının karşısına çıkabilmektedir; Hızlı mesajlaşma servislerinde, haber gruplarında, Web arama motorlarında, Web günlüklerinde (bloglarda), Cep telefonlarında

# ZARARLI YAZILIMLARDAN KORUNMA YÖNTEMLERİ

Kötü amaçlı yazılımların bilgisayar, tablet ve akıllı telefon gibi cihazlarınıza girmesini önlemenin en yaygın yolu, bir anti malware ya da antivirüs programı yüklemektir.

Çoğu işletim sistemi yerleşik antivirüs yazılımı ile birlikte gelir. Örneğin; Bilgisayarınızda “Windows İşletim Sistemini” kullanıyorsanız içerisinde **Windows Defender** isimli güvenlik yazılımı ile birlikte yüklenmiştir. Ancak bazı durumlarda bu da yeterli olmayacaktır ve daha iyi, ücretsiz veya ücretli üçüncü taraf seçenekleri de yüklemek faydanıza olabilir.