

# WINDOWS REGISTRY (WINDOWS KAYIT DEFTERİ)



Efekan ACAR

# İçindekiler

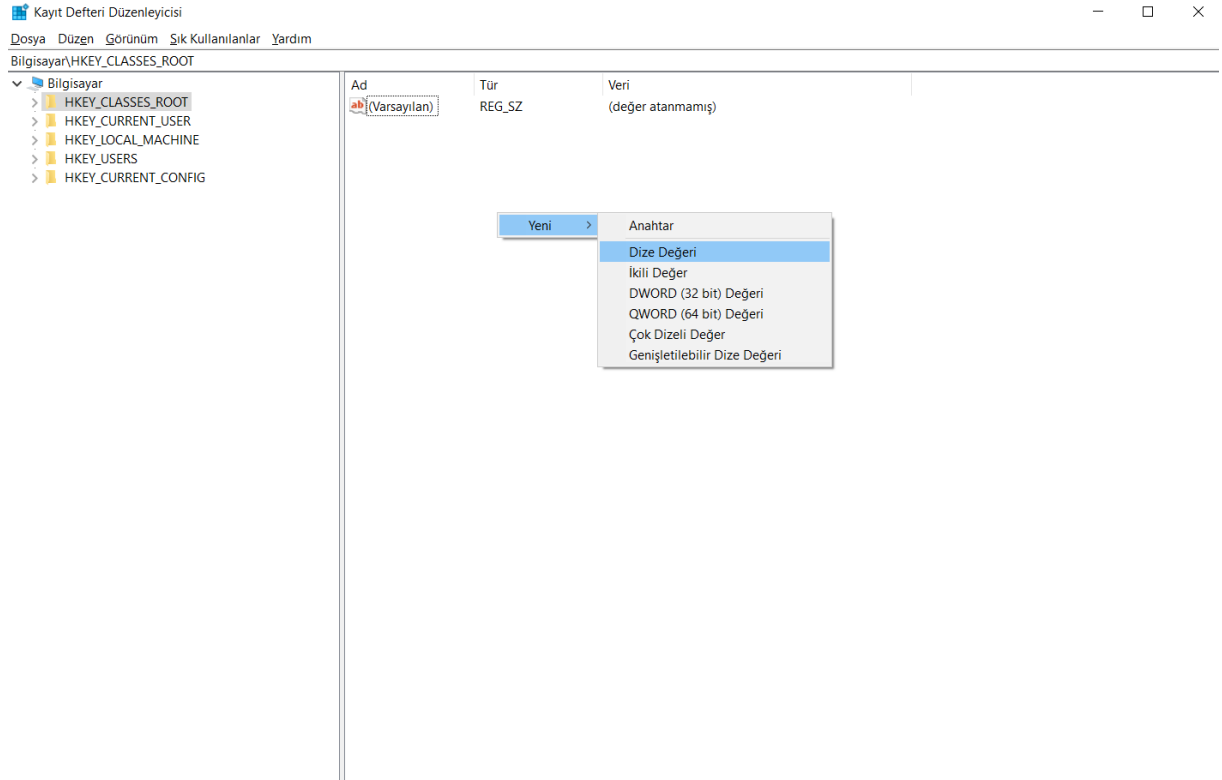
İçindekiler.....	2
Windows Registry.....	3
Kök Anahtarlar.....	4
Değerler .....	5
Üst Menü.....	6,7,8
HKEY CLASSES ROOT.....	8
HKEY CURRENT USER.....	8
HKEY LOCAL MACHINE.....	9
HKEY USERS.....	9
HKEY CURRENT CONFIG.....	9
WINDOWS REGISTRY ANALİZİ.....	10,11,12,13,14
KAYNAKLAR.....	15

# Windows Registry

Windows Registry(Windows Kayıt Defteri) işletim sistemi, yüklü programlar ve donanımlar hakkında bilgiler, ayarlar ve seçeneklerin bulunduğu bir veritabanıdır. Bütün Microsoft Windows işletim sistemlerinde ve bütün sürümlerinde bulunur. Windows'a yeni bir program yüklendiği zaman Kayıt Defterinde o program hakkındaki temel bilgi ve ayarları içeren bir alt anahtar oluşur. Kayıt Defterini görüntülemek veya üzerinde değişiklik yapmak için Kayıt Defteri Düzenleyicisi kullanılır.

## Windows Registry Editor

Registry Editor yani Kayıt Defteri Düzenleyicisine erişmek için öncelikle win+R tuşuna basarak çalıştır ekranına erişiyoruz, ardından regedit yazarak Tamam'a tıklıyoruz veya komut istemcisine regedit yazarak Enter diyoruz; yönetici izni verdikten sonra kayıt defteri düzenleyicisi açılmış oluyor. Registry Editor'e kısaca Regedit de denir.



Sol kısımda yer alan her bir klasöre KEY(ANAHTAR) denir, sağ kısımda bulunan dosyalara ise VALUE(DEĞER) denir. Sağ tıklayarak yeni bir anahtar veya değer oluşturabiliriz.

# Kök Anahtarlar

Registry menüsü 5 kök anahtardan oluşur. Bu kök anahtarlara kovan da denir.

## HKEY CLASSES ROOT

Dosya türlerinin, dosya uzantılarının ve ole bilgilerinin bulunduğu anahtardır. Dosyaların ilişkilendirilmesi ve menü ayarları da burada bulunur.

## HKEY CURRENT USER

Şu anda Windows'ta oturum açmış kullanıcı ile ilgili ayarların tümünü içerir. Buradaki ayarlardan sadece oturumu açık olan kullanıcı etkilenir. Masaüstü ayarları, görüntü ayarları, ağ ayarları, güvenlik hakları vb.

## HKEY LOCAL MACHINE

Bilgisayarın donanımına ait bilgileri içerir. Bütün sürücülerini görebilirsiniz. Başlangıç uygulamaları, güvenlik duvarları ve diğer hizmetler bu anahtarda yer alır. Tüm kullanıcıları etkileyecek bir değişiklik yaptığınız kayıtlar burada bulunur.

## HKEY USERS

Bilgisayarda yer alan kullanıcıların temel hesap bilgileri bu anahtarda bulunur.

## HKEY CURRENT CONFIG







Bu anahtarda ise mevcut donanımın konfigürasyonu ile ilgili ayrıntılar bulunur.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current kısayolunun görevini görür.

## HKEY DYN DATA

Bu anahtar yalnızca Windows 95, 98 ve NT sürümlerinde yer alıyordu. Aygıtlar hakkında bilgiler yer alır. Bilgisayara aygıt eklendikçe veya çıkarıldıkça bilgiler değişebilir. Diğer sürümlerde bu bilgiler HKEY LOCAL MACHINE içerisinde yer alır.

# Değerler

 Dize Değeri	REG_SZ	
 İkili Değer	REG_BINARY	(sıfır uzunlukta ikili değer)
 DWORD(32bit)Değeri	REG_DWORD	0x00000000 (0)
 QWORD(64bit)Değeri	REG_QWORD	0x00000000 (0)
 Çok Dizeli Değer	REG_MULTI_SZ	
 Genişletilebilir Dize Değeri	REG_EXPAND_SZ	

## Dize Değeri

Kayıt defterinde en çok kullanılan alt anahtardır. Değerin tek bir satırda tanımlanmasına imkan verir.

## İkili Değer

Özelliklerin 1 veya 0 olarak tanımlanmasına izin verir.

## DWORD(32bit)Değeri

Değerleri ondalık veya onaltılık olarak tanımlayabilir. İkili değere benzer ancak 32bitlik bir değer olarak saklanır.

## QWORD(64bit)Değeri

DWORD'e benzer ancak 64bitlik bir değer olarak saklanır.

## Çok Dizeli Değer

Değerin birden çok satırda tanımlanmasına imkan verir.

## Genişletilebilir Dize Değeri

Genişletilmesi gereken sistem değişkenlerini içerir. Farklı konumlarda aynı değer olarak bulunabilir.

# Üst Menü

## Kayıt Defteri Düzenleyicisi

Dosya Düzen Görünüm Sık Kullanılanlar Yardım

Bilgisayar\HKEY\_CLASSES\_ROOT

Burada bir Takım ayarları yapmanızı sağlayacak Dosya, Düzen, Görünüm, Sık Kullanılanlar ve Yardım bölümleri yer alıyor. Hemen altında ise bulunduğumuz konumu görmemizi sağlayan Adres Çubuğunu bulunuyor.

### Dosya

#### Kayıt Defteri Düzenleyicisi



Al diyerek daha önceden alınmış olan bir yedeği kendi kayıt defterimize yükleyebiliriz.

Ver diyerek de belirli bir anahtarın veya tüm kayıt defterinin yedeğini alabiliriz. Bu kısım önemli çünkü bir değerde yanlışlıkla yapmış olacağımız değişiklik işletim sisteminde aksaklıklara neden olabilir.

Yığın var ise buradan yükleyebilir veya kaldırabilirsiniz.

Ağ kaydında kayıtlı bir kayıt defteri var ise bağlanabilir veya bağlantıyı kesebilirsiniz.

Yazdır diyerek belirtmiş olduğunuz kısmı yazdırabilirsiniz.

Çık diyerek Kayıt Defteri Düzenleyicisini kapatabilirsiniz.

## Düzen

t Defteri Düzenleyicisi

Düzen	Görünüm	Sık Kullanılanlar	Yard
Değiştir...			
İkili Veriyi Değiştir...			
Yeni			>
İzinler...			
Sil		Del	
Yeniden Adlandır			
Anahtar Adını Kopyala			
Bul...		Ctrl+F	
Sonrakini Bul		F3	

Bu kısımda seçili değerin verisi üzerinde değişiklik yapabilirsiniz.

Yeni bir anahtar veya değer oluşturabiliriz. Geçerli anahtar için izinleri değiştirebiliriz.

Geçerli değeri silebilir veya yeniden adlandırabilirsiniz.

Anahtar Adını kopyalayabilirsiniz.

Bul kısmına tıklayarak veya Ctrl+F3 kombinasyonlarını yaparak arama yapabilirsiniz, F3'e basmaya devam ederek de arama sonuçlarını görebilirsiniz.

## Görünüm

Düzenleyicisi

Görünüm	Sık Kullanılanlar	Yardım
✓ Adres Çubuğu		
Böl		
İkili Veriyi Görüntüle...		
Yenile		F5
Yazı Tipi		

Görünüm ile ilgili özelleştirmeleri buradan yapabilirsiniz.

Adres çubuğunu aktif veya deaktif edebilirsiniz.

Sayfayı yenileyebilir ve yazı tipini değiştirebilirsiniz.

## Sık Kullanılanlar

Buradan sık kullanılanlara ekleme veya çıkarma işlemlerini yapabilirsiniz.

## Yardım

Bu kısımda Kayıt Defteri Düzenleyicisi hakkında yardım alabilirsiniz.

# HKEY CLASSES ROOT

Bu anahtarda dosya uzantılarının yer aldığını öğrenmiştik. Dosya Gezgininde bu uzantıya sahip bir dosyayı açmak istediğinizde hangi program ile açılacağı bilgisi burada yer alır. Dosya uzantılarının yanı sıra programların bazı teknik yönleri ile ilgili olan CLSID, ProgID ve IID anahtarları da burada bulunur. Bu kovan HKEY\_CURRENT\_USER\Software\Classes ve HKEY\_LOCAL\_MACHINE\Software\Classes konumlarında bulunan verilerin birleştirilmiş halidir.

# HKEY CURRENT USER

Denetim masasında farklı uygulamalarda yapılandığınız ayarların çoğu bu anahtarda yer alır. Çeşitli kayıt defteri değerleri, kurulu yazıcılar, masaüstü kişiselleştirmeleri, ortam değişkenleri, ağ sürücüler vb. burada bulunur.

Bu anahtarın bazı yaygın alt anahtarları şunlardır: AppEvents, Console, Control Panel, Environment, EUDC, Identities, Keyboard Layout, Network, Printers, Software, System ve Volatile Environment

Windows sürümleri arasında bu alt anahtarlar değişiklik gösterebilir.

AppEvents\EventLabels anahtarı içerisinde bildirim sesleri, Windows ve diğer uygulamalardaki açıklama, ses gibi işlevler bulunur.

Control Panel alt anahtarında klavye, Mouse gibi araçların işlev hızları bulunur.

Environment yani Ortam anahtarında ise Path ve Temp gibi ortam değişkenleri yer alır.

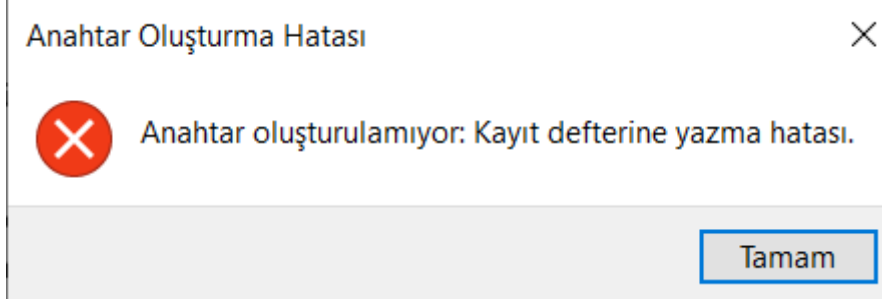
Software alt anahtarında ise özel yazılımlar yer alır.



# HKEY LOCAL MACHINE

Geçerli donanım ve aygıt sürücüler hakkında bir çok bilgi yer alır.

Bu anahtar altında başka bir anahtar açılmaz.



Alt anahtarları: BCD00000000, Hardware, Sam, Security, Software, System

Software bu anahtarda en çok erişilen alt anahtardır. Her program kayıt defterinin bu alt anahtarına veri yazar. Program her başladığında yeniden yapılandırma yapmadan açılmasını sağlar.

Hardware alt anahtarı içerisinde BIOS, işlemciler ve diğer donanım aygıtları hakkında veriler bulunur.

HKEY LOCAL MACHINE anahtarı içerisindeki Sam ve Security alt anahtarları gizli anahtardır, diğer anahtarlar gibi içeriğine bakılamaz.

## SAM

Güvenlik Hesapları Yöneticisi veritabanlarıyla ilgili bilgileri bulundurur. Kullanıcılar, misafir hesaplar ve yönetici hesapları hakkındaki oturum bilgileri ve parolaların kriptografik hash değerleri yer alır.

## SECURITY

Bu alt anahtarda geçerli kullanıcının güvenlik ilkeleri bulunur. Kullanıcıların erişim izinleri ve erişim bilgileri yer alır.

Yönetici izinlerine sahip bir kullanıcı bile bu anahtarlara erişemez, sadece sistem hesabı kullanılarak açılabilir.

# HKEY USERS

Bilgisayardaki tüm aktif kullanıcıların yapılandırma bilgileri bu anahtarda bulunur. Kullanıcıya özel denetim ayarları bulunur, kullanıcı ilk oturum açtığında yüklenir. O kullanıcının güvenlik tanımlayıcısı veya SID'si ile adlandırılır.

.Default, S-1-5-18, S-1-5-19 ve S-1-5-20 yerleşik sistem hesaplarıdır.

# HKEY CURRENT CONFIG

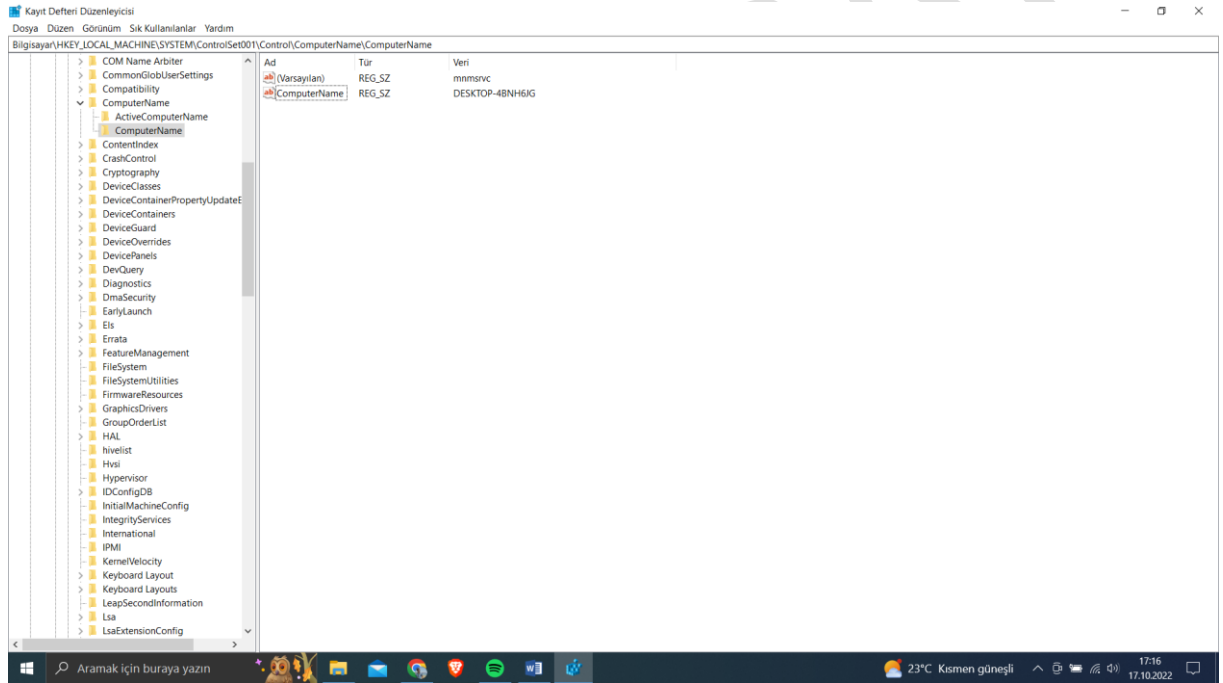
\SYSTEM\Current\ControlSet\Hardware Profiles\Current\ asıl konumudur. Software ve System olmak üzere 2 alt anahtarı vardır. Donanım profili hakkındaki bilgileri içerisinde bulundurur.

# WINDOWS REGISTRY ANALİZİ

Registry analizi için elimizde canlı bir sistem veya bir imaj olabilir. Ancak Regeditte kısıtlı erişim olduğu için KAPA, Autopsy veya FTK imager araçlarından birisi kullanılabilir. Canlı analiz için ise Registry Viewer, Zimmerman's Registry Explorer veya Reg Ripper kullanılabilir. Ancak gerçek bir adli suç aramıyorsak kendi registry'mizden de bir çok bilgi edinebiliriz.

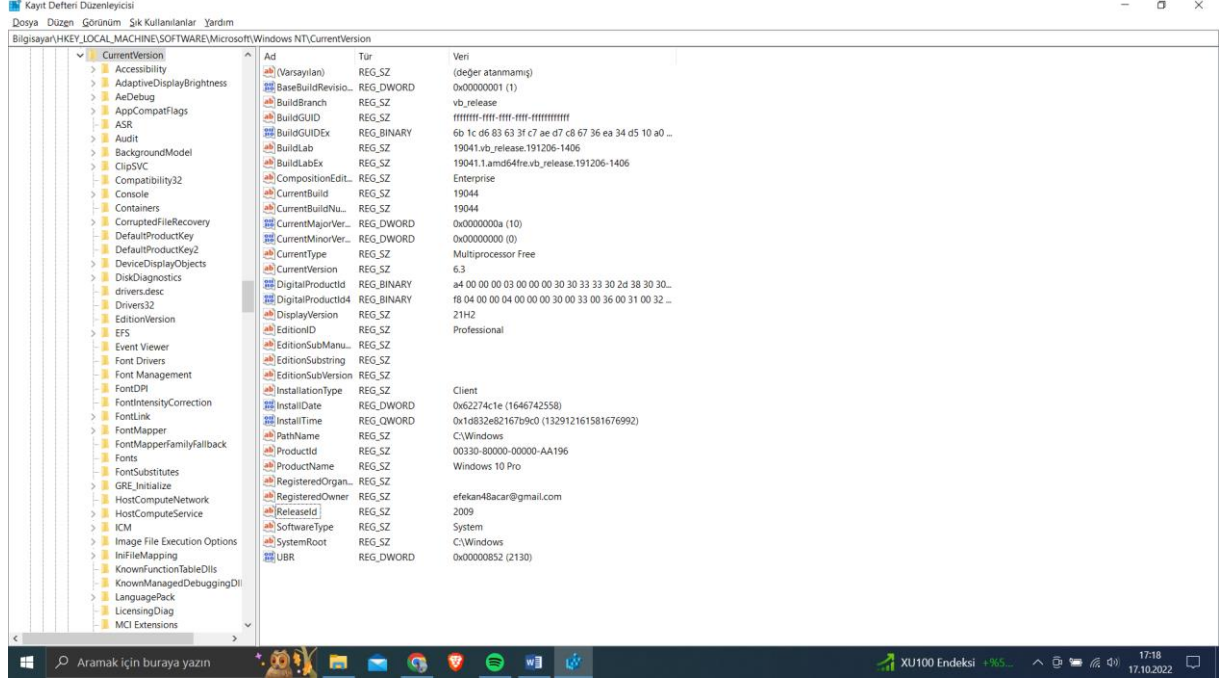
Bilgisayar\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Bu konumdan bilgisayar adını öğrenebilirsiniz.



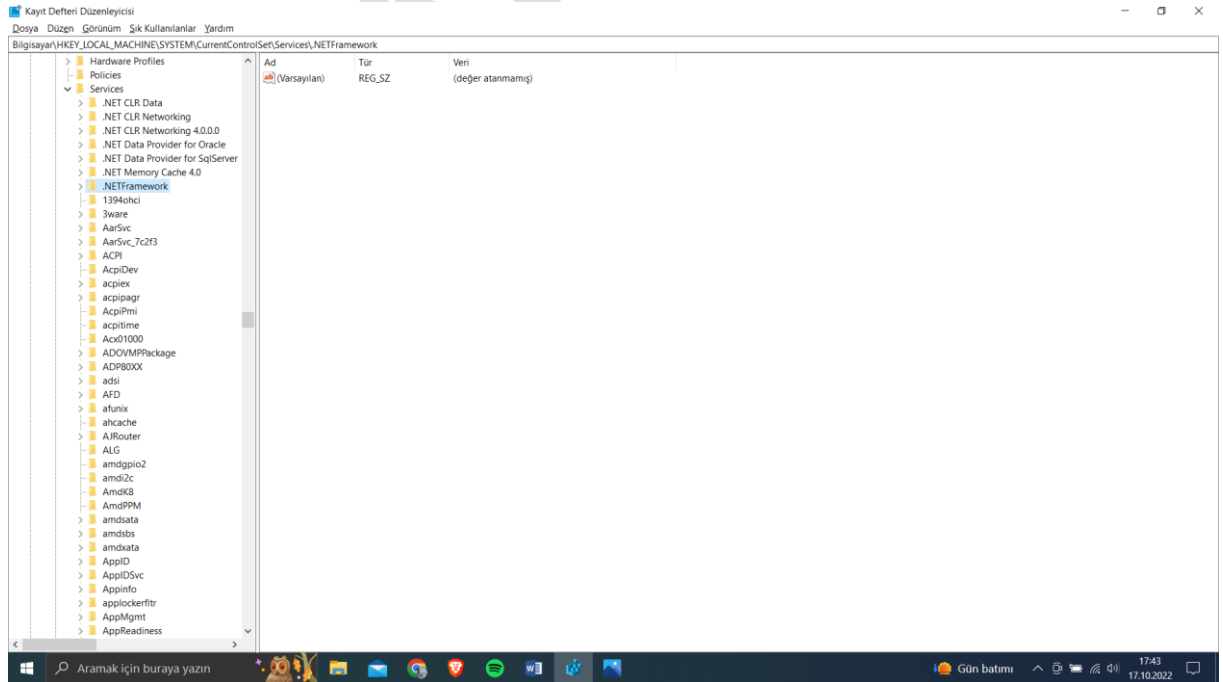
## Bilgisayar\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Bu konumdan bir çok bilgiye ulaşabilirsiniz. İşletim sistemi sürümü, geçerli kullanıcının eposta adresi, bilgisayarın piyasaya sürülme yılı vb.



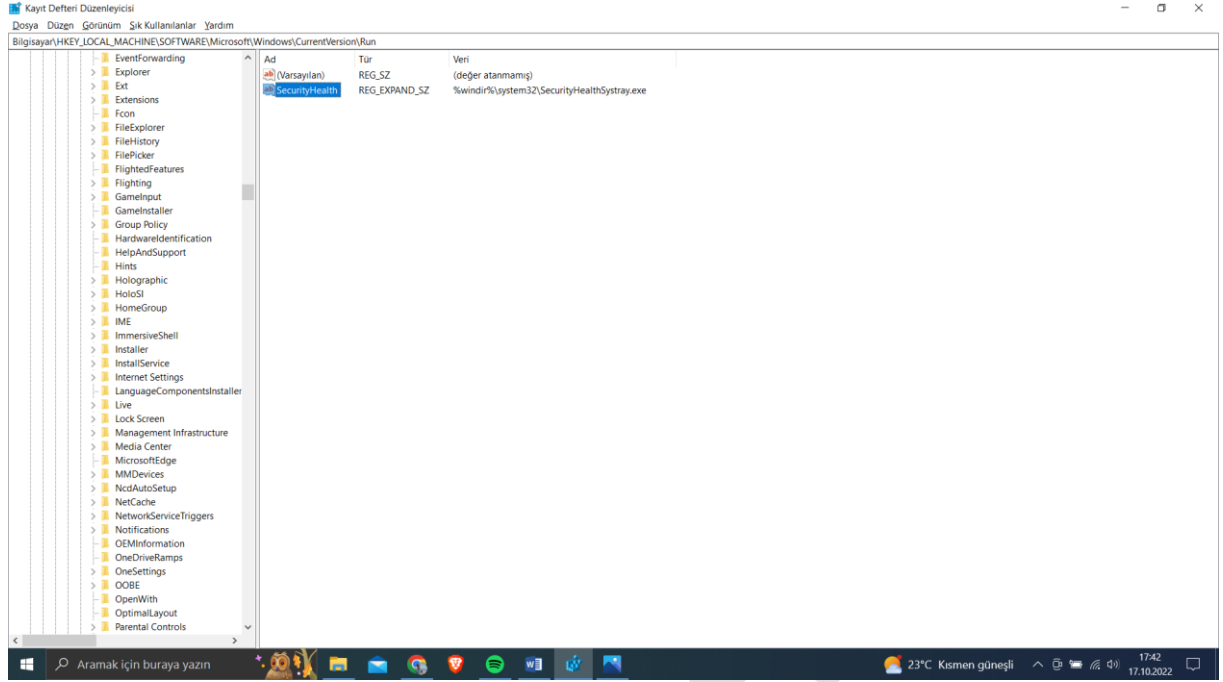
## Bilgisayar\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Service

Bu konuma gittiğimiz zaman bilgisayardaki hizmetlerin tümünü görüntüleyebilirsiniz.



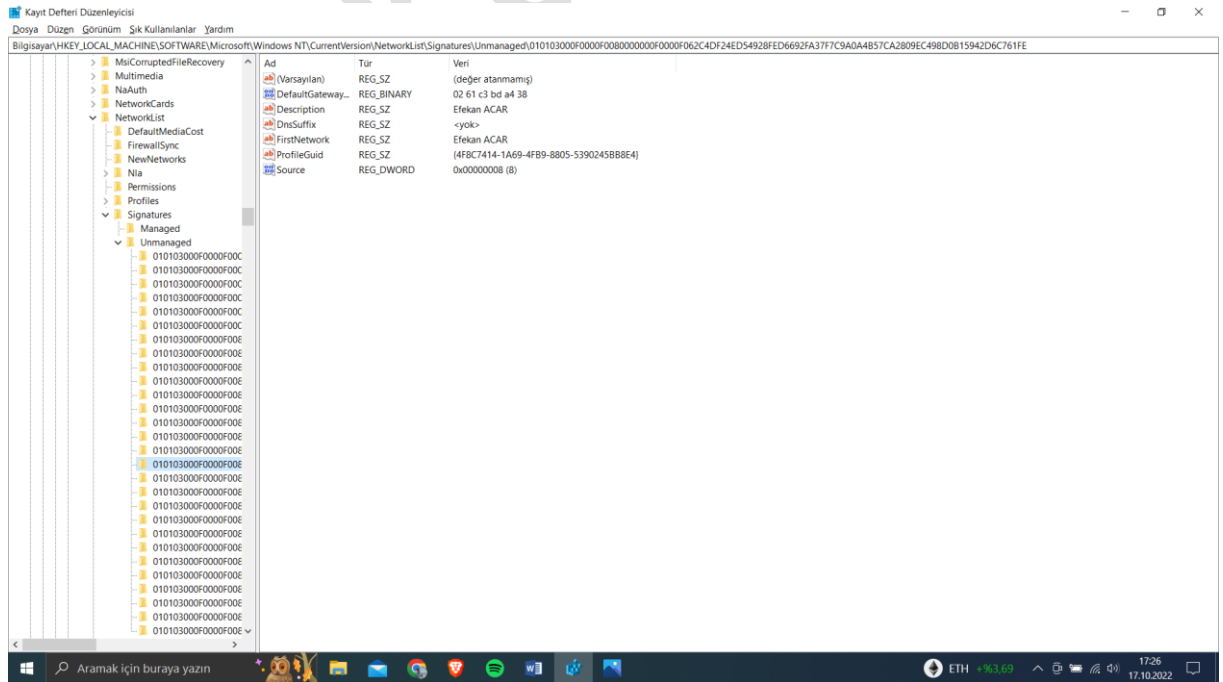
## Bilgisayar\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Bu konumda bir kullanıcı oturum açtığı zaman çalışan program ve komutları görebilirsiniz.



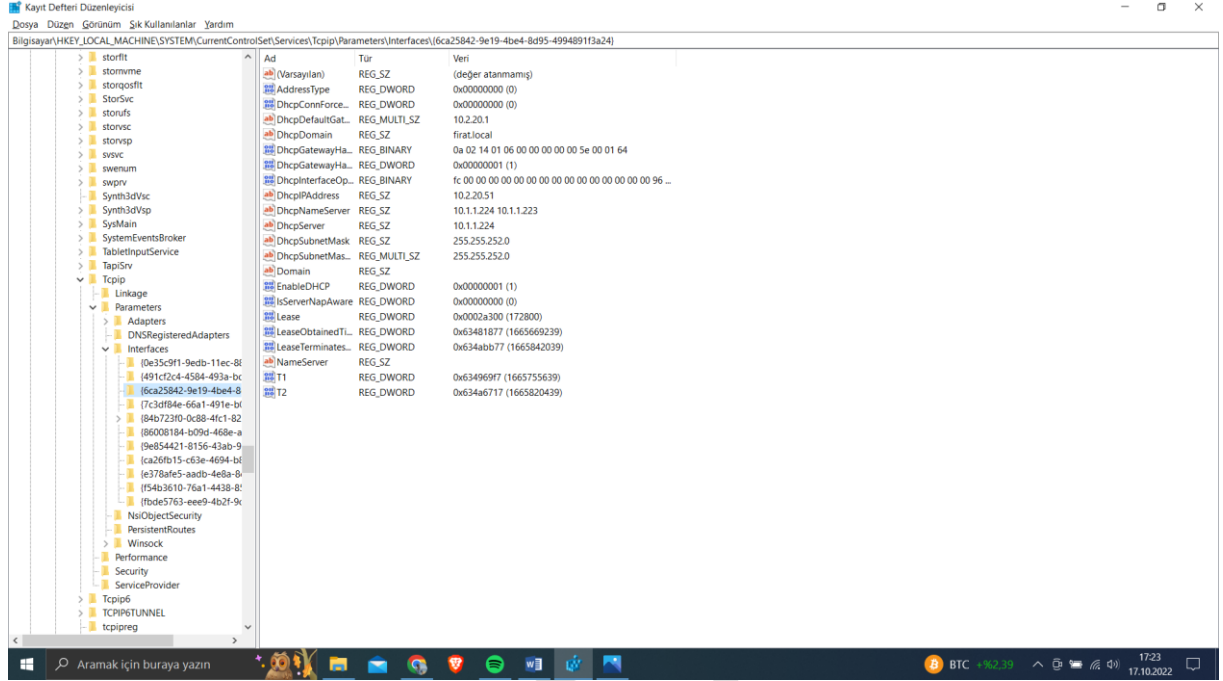
## Bilgisayar\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

Bu konumda bilgisayarın bağlı olduğu bütün geçmiş ağları görüntüleyebilirsiniz.



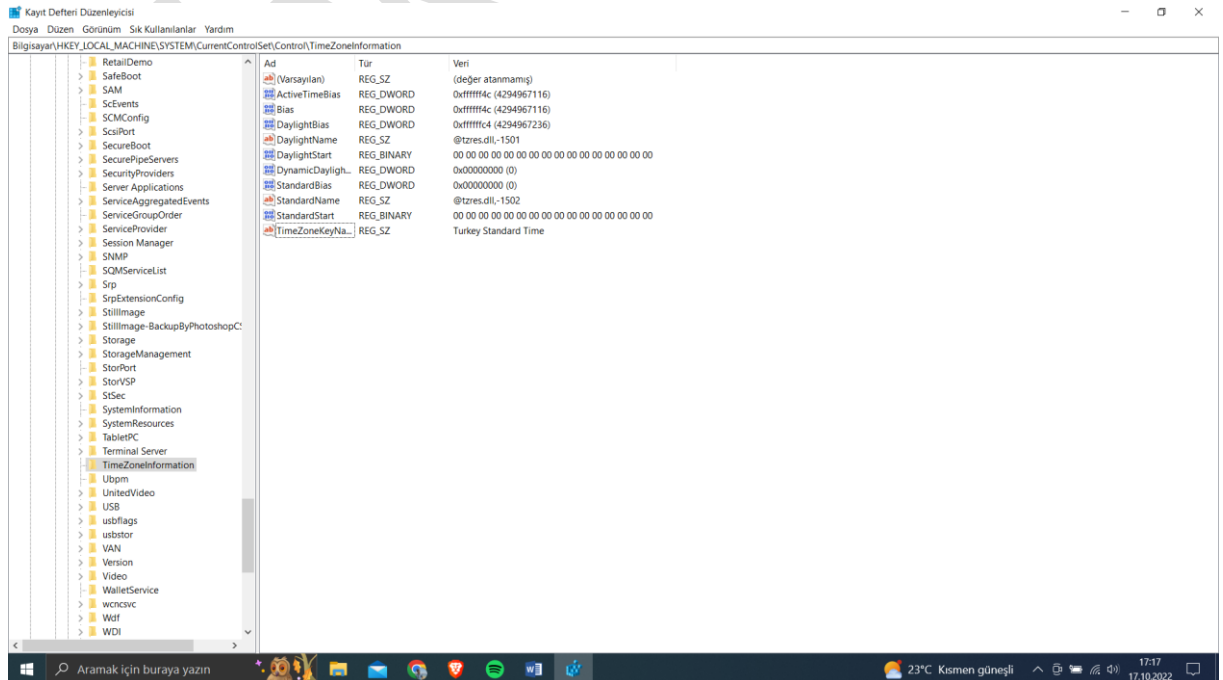
## Bilgisayar\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Service s\Tcpip\Parameters\Interfaces

Bu konumda bilgisayardaki kayıtlı ağ arabirimleri hakkında detaylı bir liste yer alır. Bu ağlar hakkında IP adresi, alt ağ maskesi vb. bilgiler yer alır.



## Bilgisayar\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

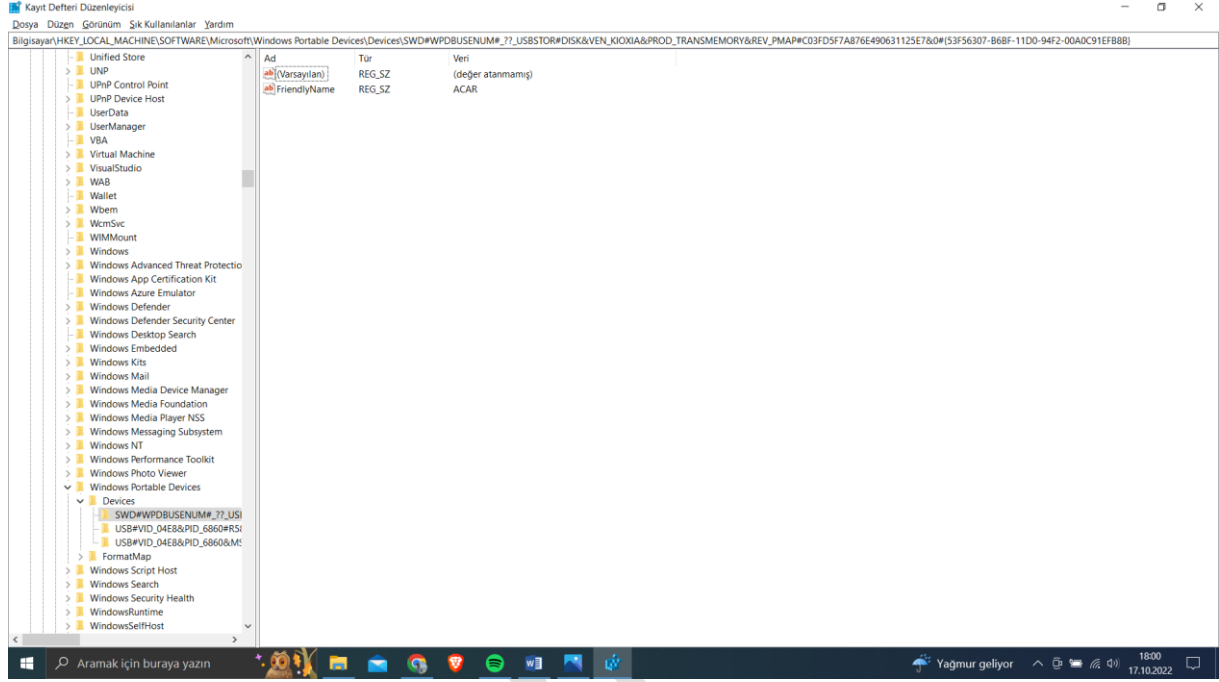
Bu konumda bilgisayarın hangi saat dilimini kullandığı bilgisi yer alır.



## Bilgisayar\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices\Devices

Bu konumda bağılı sürücülerin aygıt isimleri bulunur.

Bilgisayar\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USB konumunda ise bağılı USB aygıtları hakkında sürümü, satıcı kimliği ve ürün kimliği gibi bilgiler yer alır.



KAYNAKLAR:

[https://tr.wikipedia.org/wiki/Windows\\_Kay%C4%B1t\\_Deferi](https://tr.wikipedia.org/wiki/Windows_Kay%C4%B1t_Deferi)

<https://www.computerhope.com/jargon/r/registry.htm>

<https://www.lifewire.com/>

<https://tryhackme.com/room/windowsforensics1>

EfeKan ACAR