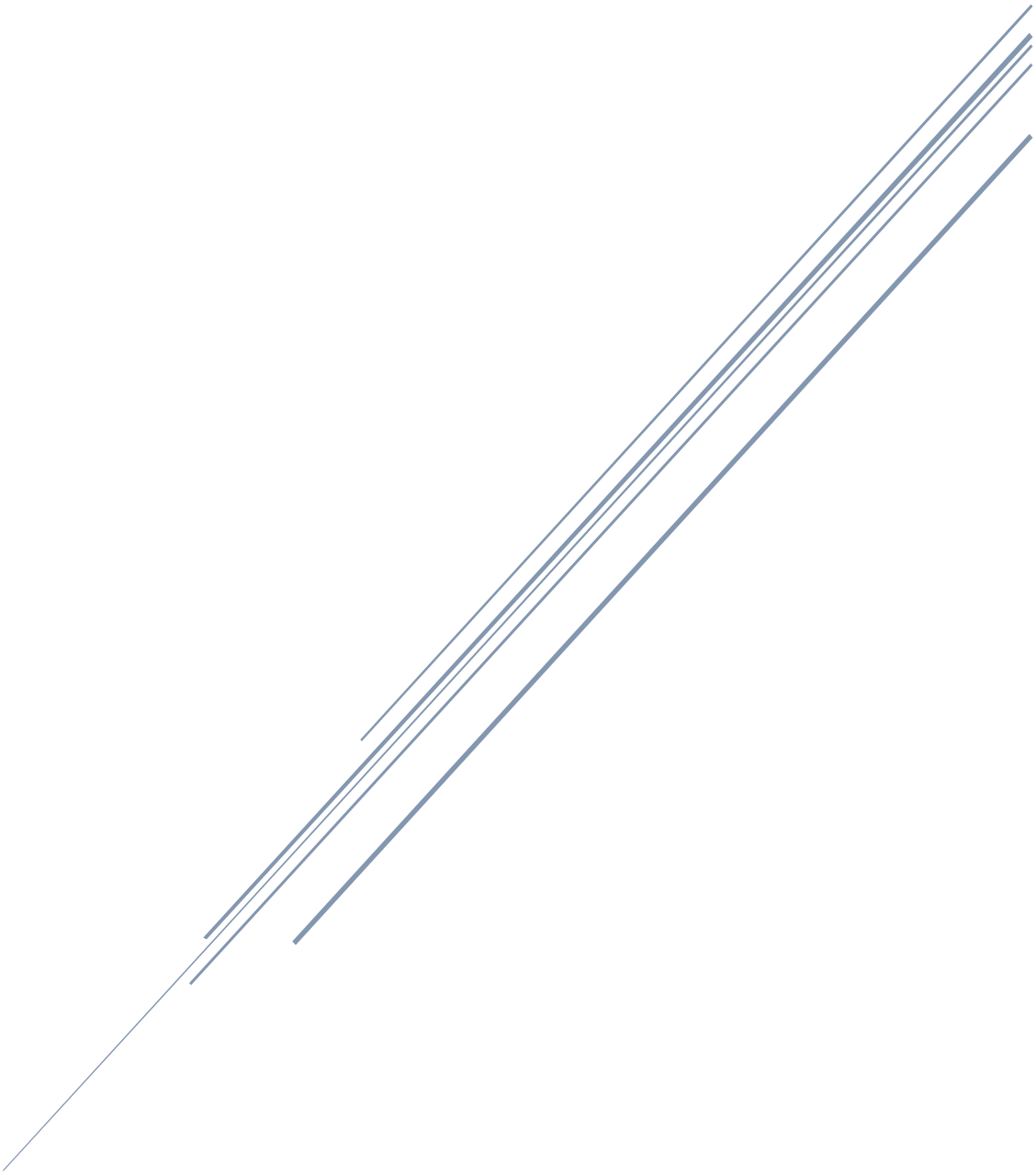
# WİNDOWS REGİSTRY ANALİZİ



Serdal Tarkan ALTUN

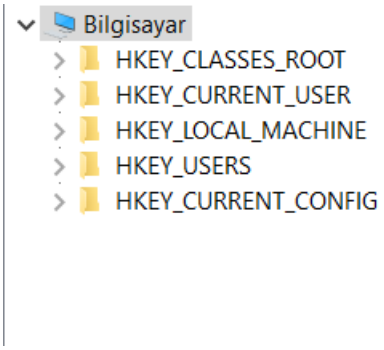
# İÇİNDEKİLER

# 1. REGİSTRY(Kayıt Defteri) Nedir?

Windows'ta çalışan uygulamalar ve hizmetler için kritik olan verileri içeren hiyerarşik bir veri tabanıdır. Bilgisayar sistemi hakkında ki genel bilgileri ile uygulamalara ait geçmiş kayıtların tutulduğu yer olan registry sistemin hızlı, tutarlı ve işlevsel olarak çalışması amacıyla otomatik olarak tutulan kayıtlardan oluşmaktadır.

## 1.1. Windows Registry Dosyaları Nelerdir ve Manuel Bilgi Nasıl Öğrenilir?

Windows Kayıt defteri olarak da bilinmektedir. Ve registry dosyaları 5 adet KEY(Anahtardan) oluşmaktadır. Dosyalar şunlardır;




- *HKEY_CLASSES_ROOT:*

Dosya uzantı bilgiler, hangi tip dosyanın hangi programla açılması gerektiği ve dosya tipleriyle ilgili tanımlamanın yapıldığı gruptur.

- *HKEY_CURRENT_USER*

O an oturum açmış kullanıcılar alakalı bilgiler içermektedir. Kullanıcılara özgü ayarlar saklanmaktadır. Ortam değişkenleri, masaüstü ayarları, kontrol panel ayarları ve uygulama yapılandırmaları buna örnek verilebilir.

- *HKEY_CURRENT_CONFİG*

Bilgisayardaki donanım profil hakkında saklanan veriler bu grupta bulunmaktadır.

- *HKEY_USERS*

Bilgisayarda hali hazırda açık olan kullanıcıların ayarları ve çalıştırdıkları uygulamalara özgü çeşitli verileri taşımaktadır.

- *HKEY_LOCAL_MACHİNE*

Bu grupta bilgisayara özgü yapılandırma bilgileri bulunmaktadır. Donanım, SAM, güvenlik, yazılım ve sistem olmak üzere 5 alt anahtar içermektedir.

### 1.1.1. SAM Dosyası Nedir?

SAM Güvenlik Hesap Yöneticisi olarak bilinmektedir. Bu dosya içerisin de kullanıcı hesapları, misafir hesaplar ve bunların şifrelerinin tutulduğu veri tabanı dosyasıdır.

### 1.1.2. SECURİTY Dosyası Nedir?

Sistemdeki güvenlik bilgilerini ve ilkelerini içerir. Security içerisinde hangi kullanıcıların sisteme erişmesine izin veriliyor, bu kullanıcılar sisteme hangi kanallardan erişiyor gibi soruların cevabı bu anahtar altında saklanıyor.

### 1.1.3. SOFWARE Dosyası Nedir?

Bu dosya da sistemde kurulu olan yazılımlara ve daha önce kurulmuş ve kaldırılmış olan yazılımların bilgilerine ulaşabiliyoruz.

### 1.1.4. HARDWARE Dosyası Nedir?

Bu dosya içerisinden bağlı olan giriş-çıkış(donanım) birimleri hakkında ki bilgilere ulaşabiliyoruz.

### 1.1.5. SYSTEM Dosyası Nedir?

Bu anahtar normalde yalnızca yerel sistemde yönetici ayrıcalıklarına sahip kullanıcılar tarafında yazılabilir. Windows sistem kurulumu hakkında bilgiler, dosya sistemi içeren şu an takılı aygıtların listesi ve sistem donanım sürücüleri hakkından bilgileri içerisinde tutan anahtardır.

sizlere biraz **NTUSER.DAT** dosyasından bahsetmek istiyorum.

### 1.1.6. NTUSER.DAT Dosyası Nedir?

Her kullanıcı profil içerisinde gizli olarak bulunmaktadır. Bu dosya içerisinde kullanıcı profil bilgilerin içerir. Aslında Windows kayıt defterinden depolanan kayıtların bir kopyasıdır.

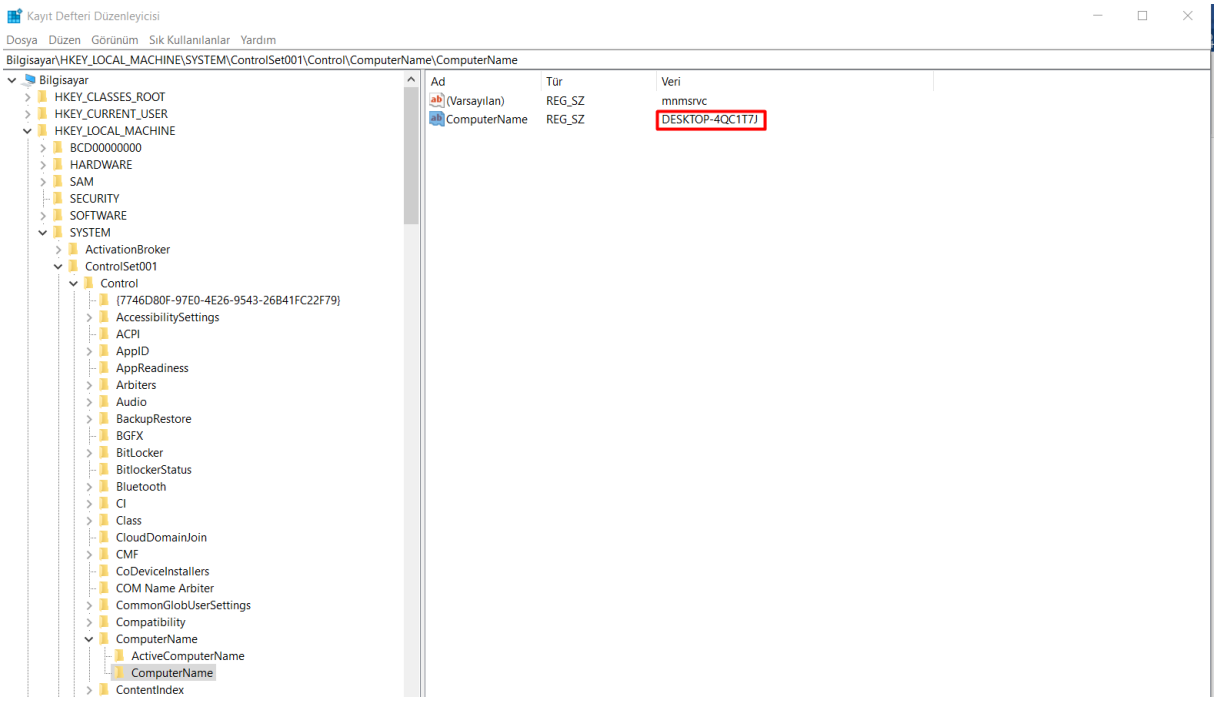
Şimdi ise manuel bir şekilde Windows kayıt defteri dosyalarından bilgiler elde etmeye çalışalım.

## 1.1. Kayıt Defterinden manuel olarak bilgi nasıl çekilir?

- *Bilgisayar Adı Nasıl Öğrenebiliriz?*

Windows kayıt defterimizde, verdiğim konuma giderek bilgisayar ismini öğrenebiliyoruz.

**HKLM \ SYSTEM \ ControlSet### \ Control \ ComputerName \ ComputerName**

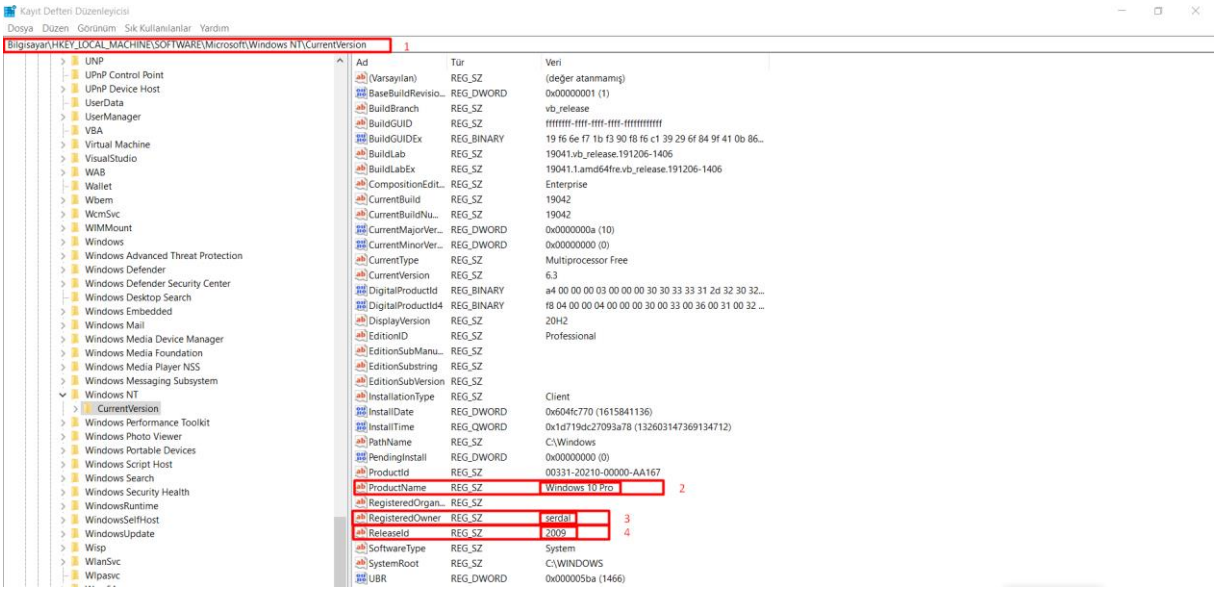



Şekilde ComputerName kısmında bilgisayar ismi gözükmektedir.

- *İşletim Sistemini, Sürümünü ve Kullanıcısını Nasıl Öğreniriz?*

Kayıt defterinden verdiğim konumu takip ederek işletim sistemi, sürümü ve kullanıcısı hakkında bilgi sahibi olabiliriz.

**HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion**



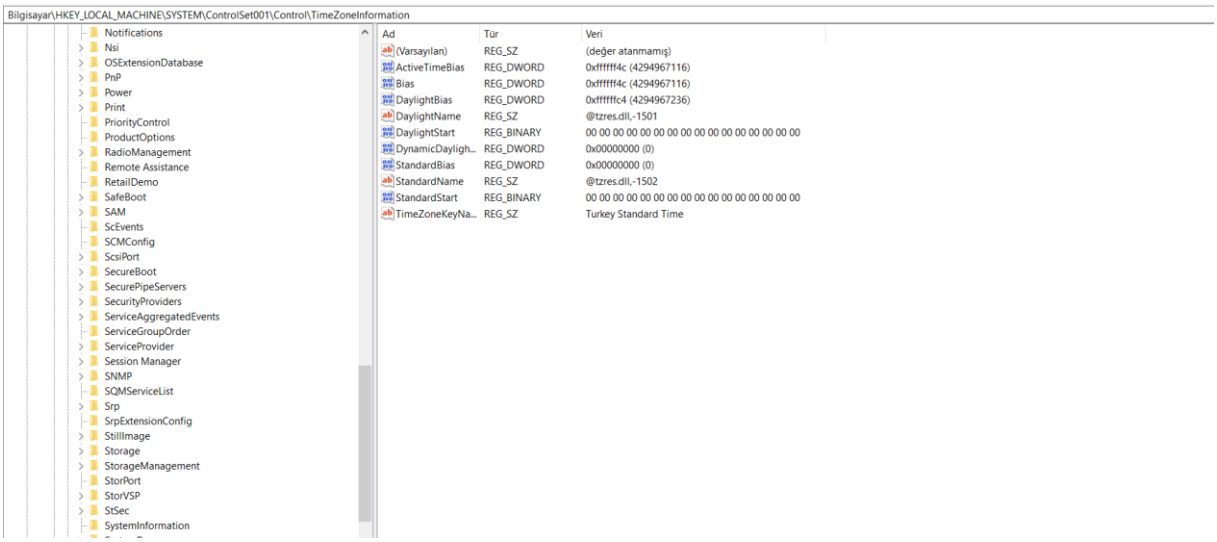

Verdiğim konuma gittiğimizde böyle bir görselle karşılaşıyoruz. Numaralandırma yaptığım kısımlardan veriler elde edebiliyoruz.

1. Bu kısım bulunduğumuz dosya konumunu göstermektedir.
2. Burada ise bize kullanılan işletim sistemini söylemektedir.
3. Kısımda ise kullanıcı adını görmekteyiz.

- *Saat Dilimi Bilgilerine Nasıl Ulaşabiliriz?*

Verdiğim konuma giderek Saat Dilimi Bilgilerine ulaşabilirsiniz.

**HKEY_LOCAL_MACHINE \ SYSTEM \ ControlSet001 \ Control \ TimeZoneInformation**




Buradan gördüğümüz üzere pek sonuç alamadık. Kayıt Defterinde anlamlandıramadığımız dosyaları yazılımlar kullanarak anlaşılabilir hale getirebiliyoruz.

Registry dosyalarından doğrudan bilgiler alabilmemiz mümkün değildir. Bu bilgiler alabilmemiz için bazı yazılımlar kullanmamız gerekmektedir. Sizlere şimdi Eric Zimmerman'ın github hesabından indirmiş olduğum Registry Explorer yazılımı ile Registry dosyalarının içerisinden nasıl bilgiler elde ediyoruz onları anlatacağım.

Registry dosyalarını inceleyebilmemiz için dosyanın orijinali kopyalayarak ya da almış olduğumuz imajlar üzerinden gerçekleştirebiliriz.

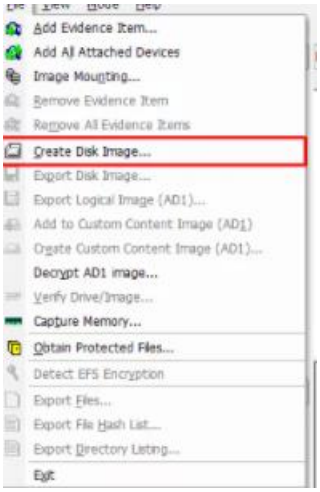
# 2. İMAJ ALMA

## 2.1. İmaj nedir?

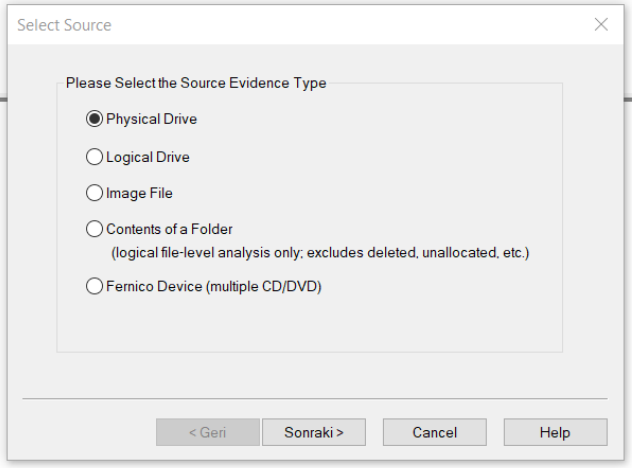
Bir cihazın veya depolama aygıtlarının o andaki verilerinin kopyasının alınmasına denir. Adli bilişim alanında direkt delil üzerinde incelemek yerine imaj yani verinin kopyası üzerinde çalışmamız olası bir veri kaybını ortadan kaldırır. Bir delilin istediğimiz kadar adli kopyasını alabiliriz. Kopya alma işlemi farklı yazılımlarla yapılabilmektedir. Ben sizlere FTK Imager üzerinden kopya alma işlemini göstereceğim.

## 2.2. İmaj nasıl alınır?

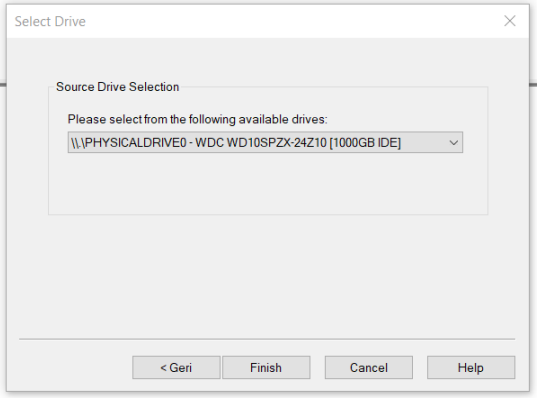
FTK imager yazılımında File sekmesinden Create disk Image seçeneğini seçelim.



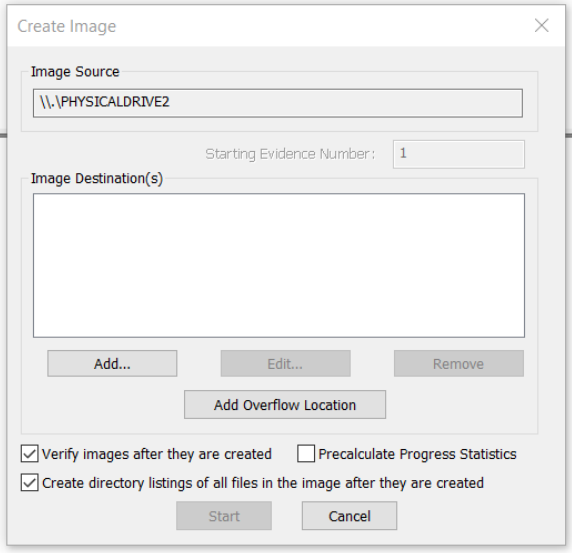

Physical Drive seçeneği ile devam edelim. Ve sonraki seçeneğine tıklayalım.




Burada imaj almak istediğimiz diski seçiyoruz. Seçtiğimiz işlemin ardından Finish diyoruz.

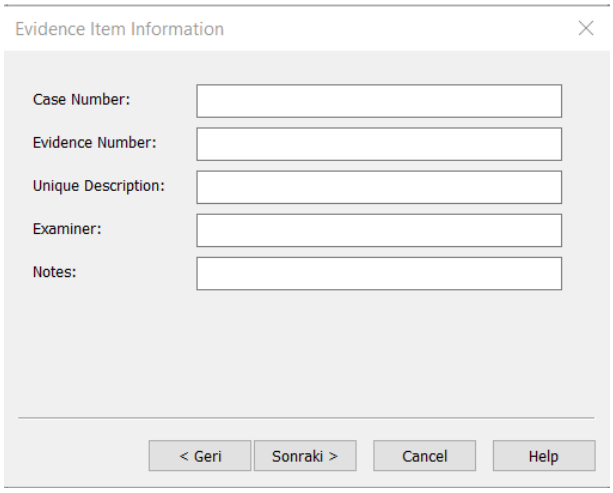



Şimdi ise bizi bu şekilde bir sayfa karşılıyor.



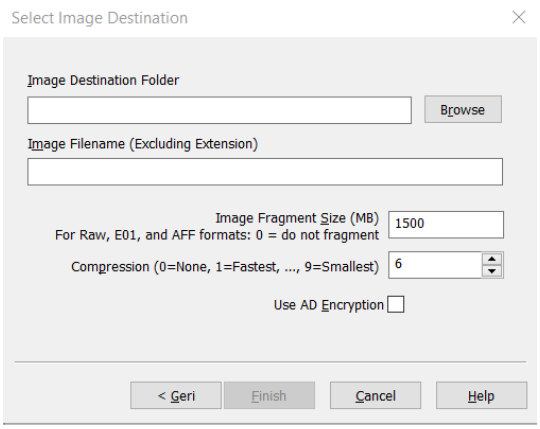
Add seçeneğinden imaj formatını seçiyoruz.

**DD formatı:** Bu formatta ki imajlar herhangi bir sıkıştırma uygulamadan birebir alınan imajlar olarak bilinirler ve sürücüler ile aynı boyutta olurlar.

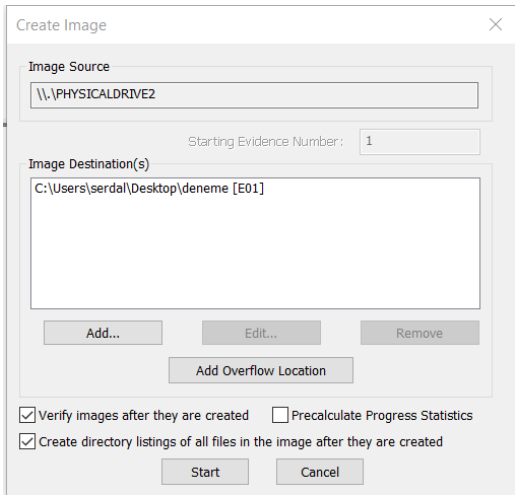



Bu açılan sayfada imaj ile alakalı verebileceğimiz bilgileri doldurmamızı istiyor. Bu kısım Adli Bilişim açısından önemlidir. Şimdilik ben hepsine 1 veriyorum ve sonraki seçeneğine tıklayarak devam ediyorum.

Şimdi ki açılan sayfada **Destination Folder** kısmından imajı nereye almak istiyorsak orayı seçiyoruz. **Filename** kısmından imaj dosyasına isim veriyoruz. **Fragment** kısmı imaj dosyasını 1500 mb dan sonra parçalara bölümleme işlemi yapmamızı sağlıyor. **Compression** kısmından ise bölümlendirme sayısını seçebiliyoruz. **Use AD Encryption** buradan ise dosyayı şifreleyebiliyoruz.



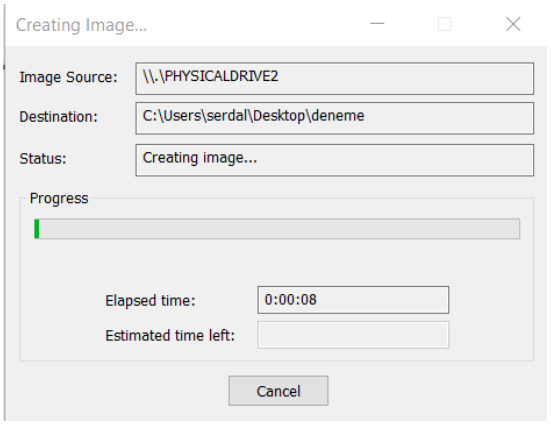

İşlemleri yapmamızın ardından Finish sekmesi açılacak. Tıklayarak devam edelim. Bizi tekrardan bu sayfaya gönderiyor.




Şimdi ise size sayfanın alt kısımda bulunan kutucuklar hakkında bilgi vereceğim.

-**Verify Images after they are created** kısmından diskin ilk hali ile imaj arasında doğrulama işlemi (hash doğrulaması) yapıyor.

Şimdi ise Start diyerek işlemi başlatmış oluyoruz. İşlemin devam ederken şu ekran karşımızda oluyor.

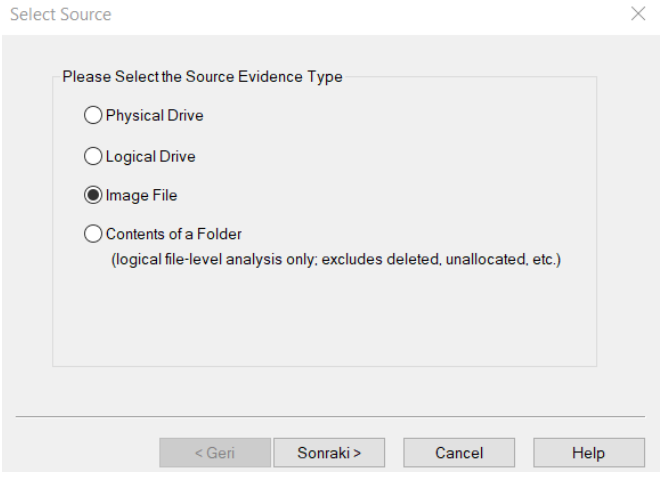



Bu işlem bittikten sonra imaj alma işlemini gerçekleştirmiş oluyoruz.

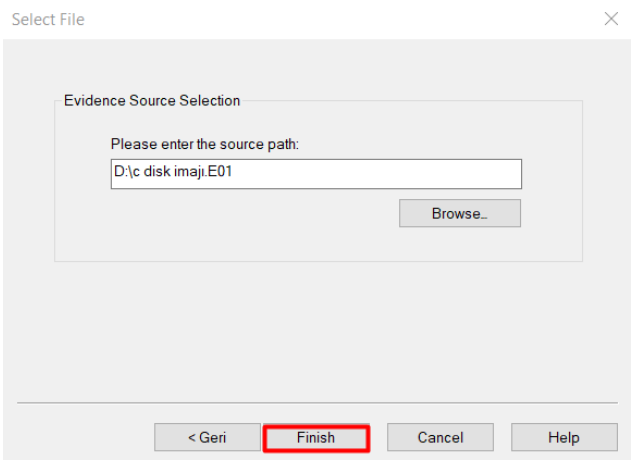
## 2.3. İmajı İçeri Aktarma Nasıl Yapılır?

İmaj alma işlemini gerçekleştirdikten sonra FTK Imager yazılımı üzerinden imajı içeri aktarıyoruz. **File > Add Evidence Items** seçeneğine tıklıyoruz.

Ardından açılan sekmede **Image File** butonunu aktif etmemizin ardından sonraki seçeneğine tıklıyoruz.




Burada ise imaj dosyasının konumunu gösterdikten sonra **Finish** seçeneğine tıklayarak imajı içeri aktarmış oluyoruz.




Imaj dosyasını başarılı bir şekilde içeri aktarmamızın ardından verdiğim dosya konumuna giderek **NTUSER.DAT** dosyasını export etme işlemini gerçekleştirebiliriz.

## 2.4. Dosyaları Export Etme İşlemi Nasıl Yapılır?

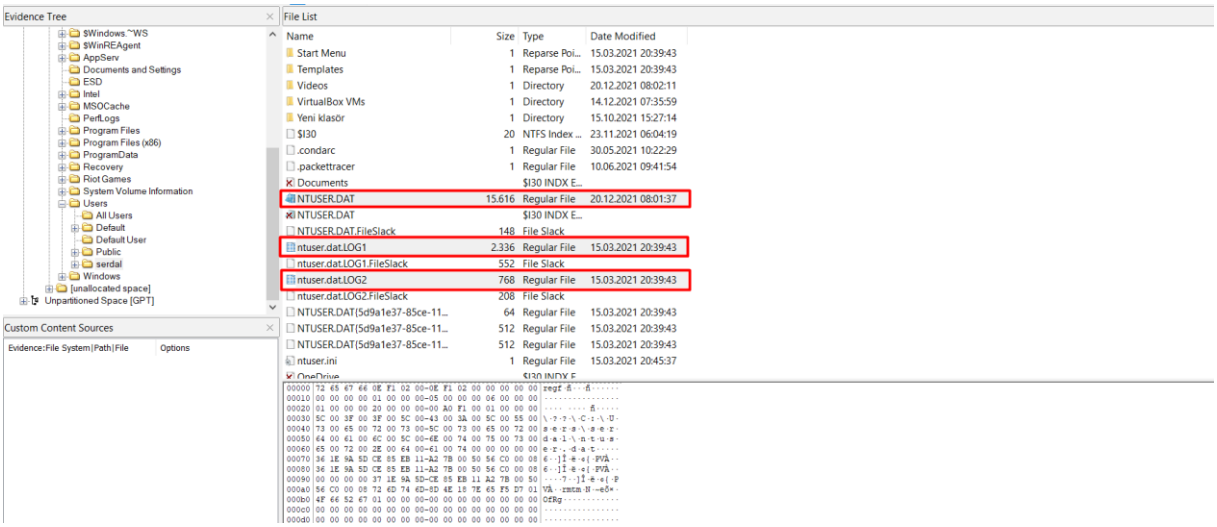
NTUSER.DAT dosyalarının bulunduğu konum;

**C:\ users \ kullanıciadi \ NTUSER.DAT**

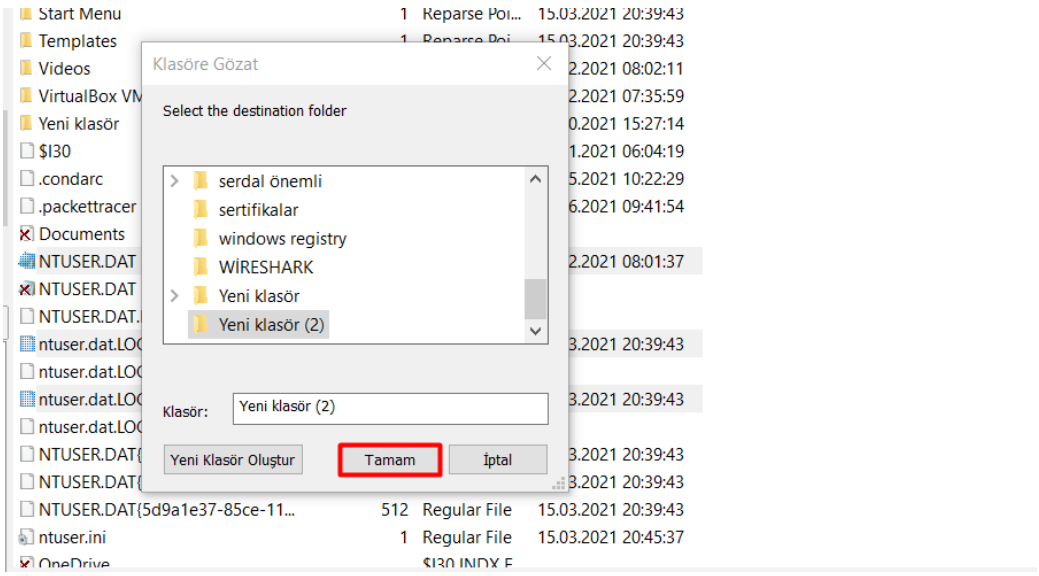
SAM, SECURİTY, SOFWARE ve SYSTEM dosyalarının bulunduğu konum;

**C \ Windows \ system32 \ config**

Dosyaları bulalım ve export edelim.




Dosyaları seçmemizin ardından sağ tık > Export File diyoruz.



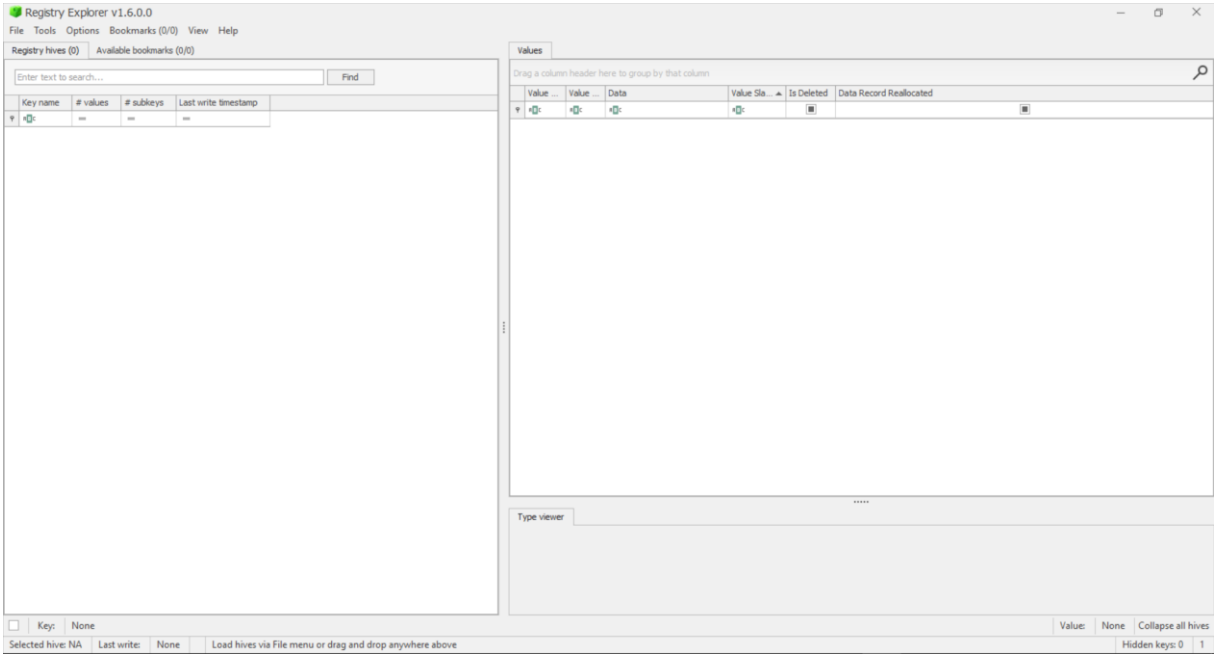

Açılan bu ekranda export edeceğimiz konumu seçtikten sonra tamam seçeneğine tıklayarak export etme işlemini tamamlamış oluyoruz. Bu işlemleri diğer registry dosyalarına da uyguluyoruz.

# 3. Registry Explorer Yazılımı İle Dosyalar Nasıl İncelenir?

## 3.1. Dosyalar İçeri Nasıl Aktarılır?

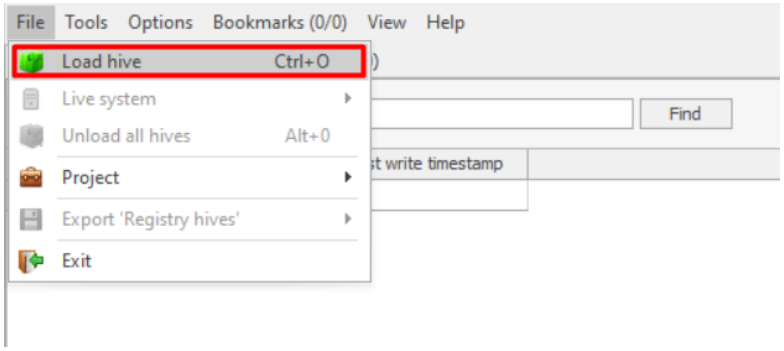
Bu işlemin ardından Eric Zimmerman Github hesabından indirmiş olduğum Registry Explorer yazılımını açıyoruz.

**Eric Zimmerman Github hesabı**: http://ericzimmerman.github.io/#!index.md

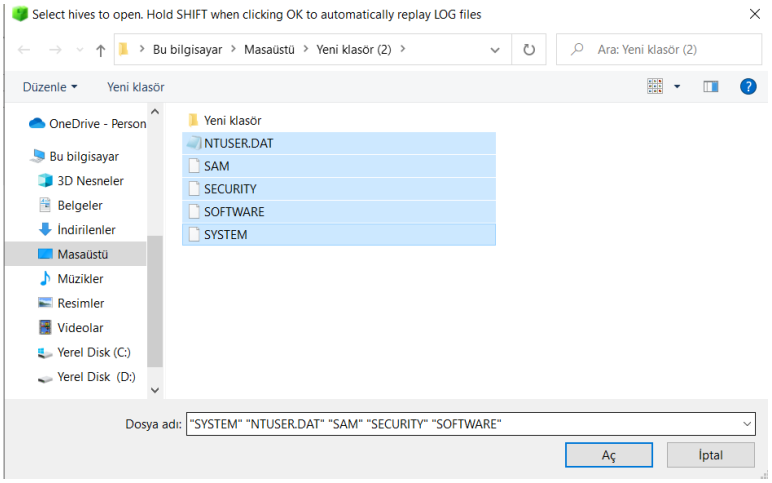


Yazılımı açtıktan sonra bu ekran bizi karşılıyor. Şimdi ise export etmiş olduğumuz NTUSER.DAT dosyasını burada açıp inceleyeceğiz.

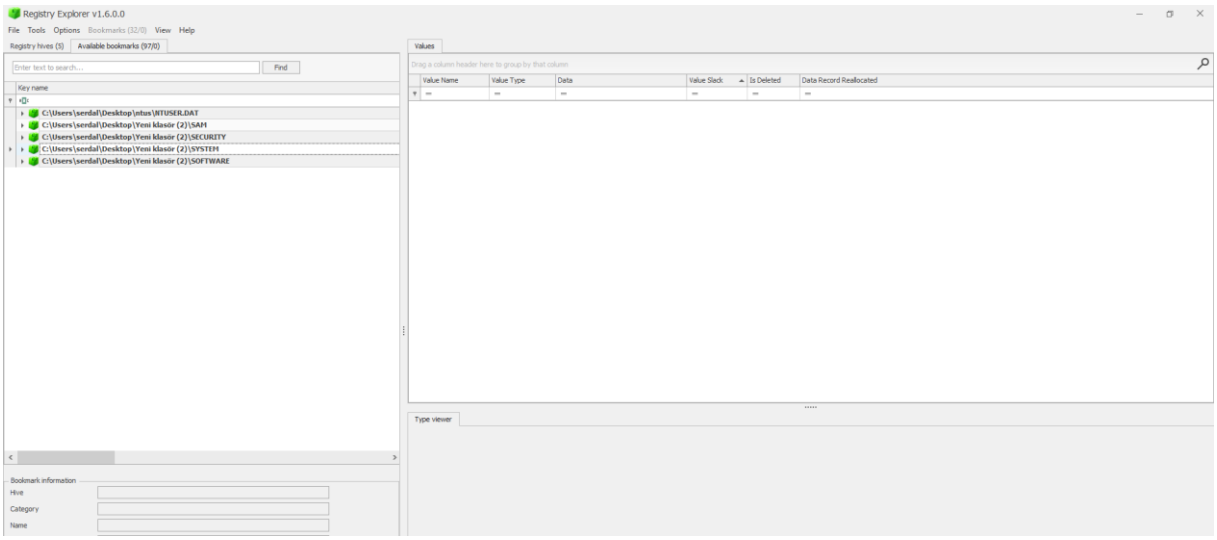
Burada **File > Load Hive** seçeneği ile devam ediyoruz.




Bu seçenekten sonra açılan sayfadan dosyaları seçiyoruz ve Aç seçeneğine tıklıyoruz.



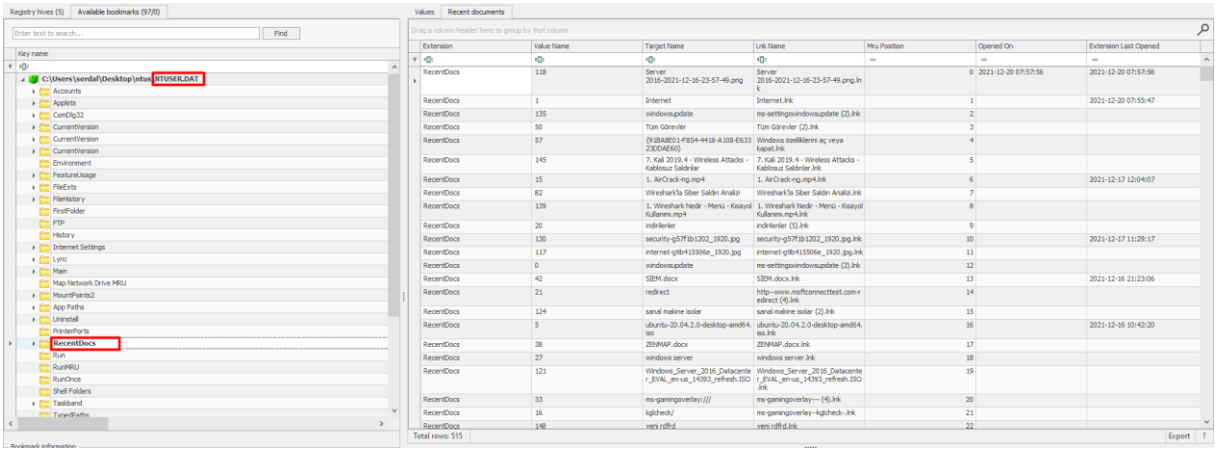

Dosyayı açma işlemini gerçekleştirmiş oluyoruz.



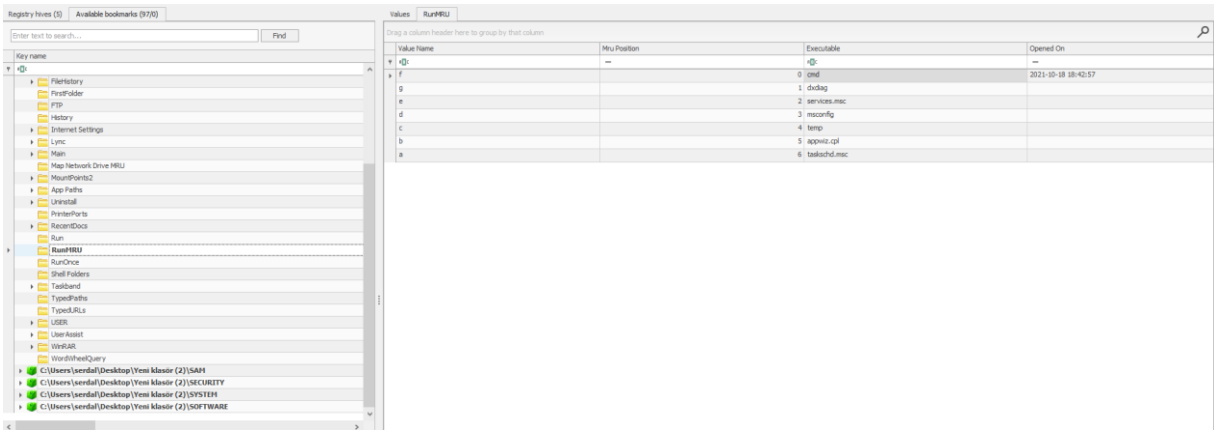
## 3.2. Veriler Nasıl Analiz Edilir?

### 3.2.1. NTUSER.DAT

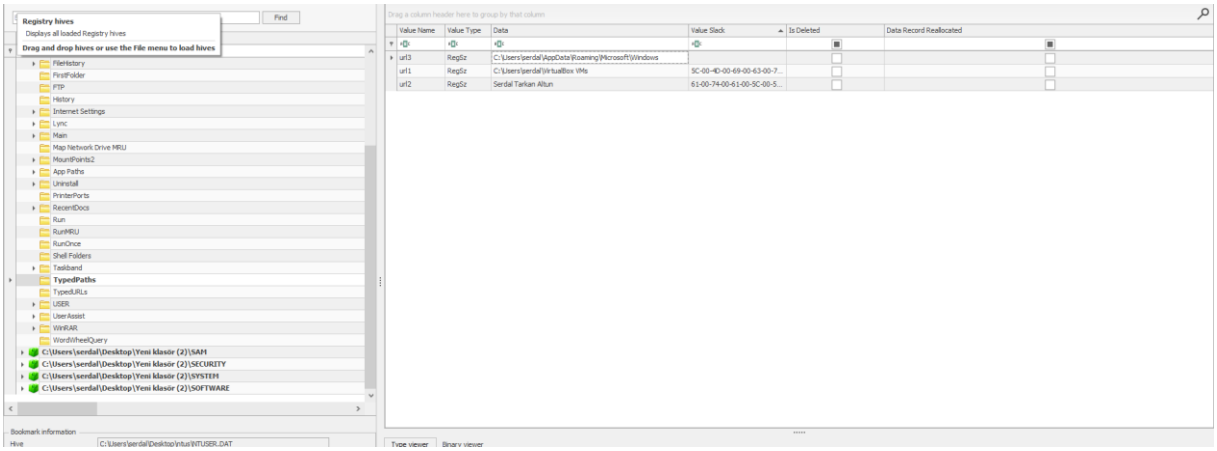
NTUSER.DAT altındaki **RecentDocx** dosyasına giderek son açılan dosyaları görebiliriz.



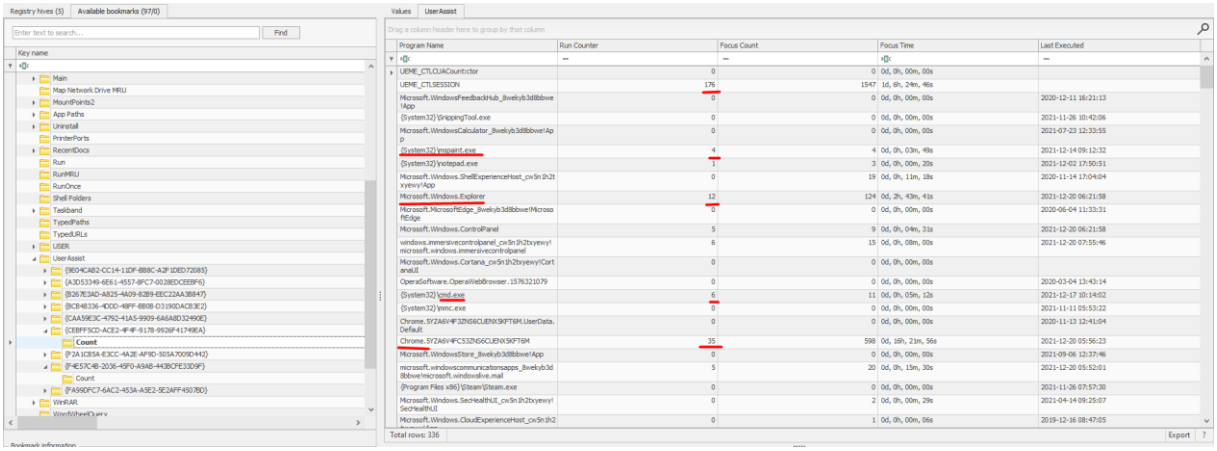
**RunMRU** dosyasından çalıştır uygulaması(Windows tuşu + R) ile aranan ve çalıştırılan uygulamaları göstermektedir.



**TypedPaths** dosyasından Windows gezginde hızlı erişim kısmında dosya konumunu vererek yaptığımız aramaları bizler göstermektedir.

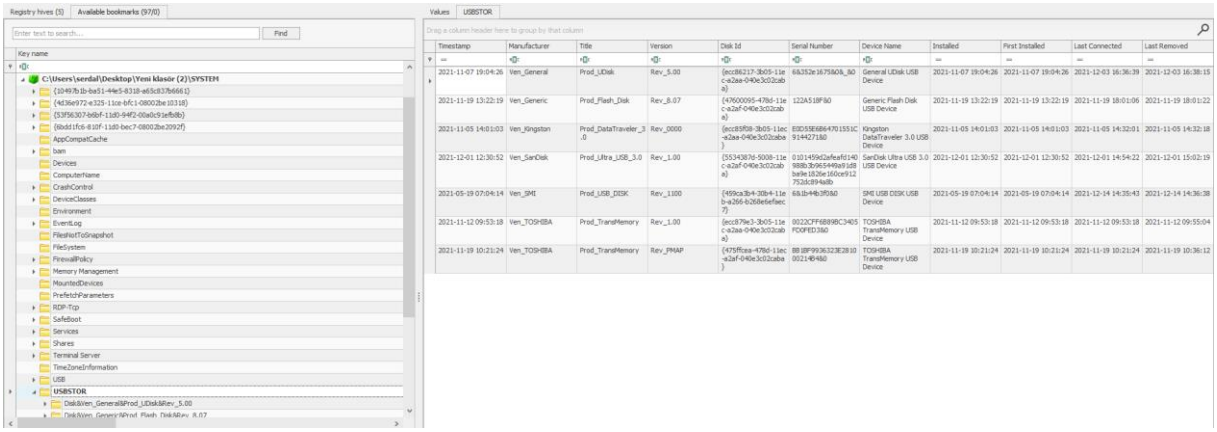


**UserAssist** dosyasından ise hangi uygulamanın ne zaman, kaç kez yürütüldüğünü göstermektedir.

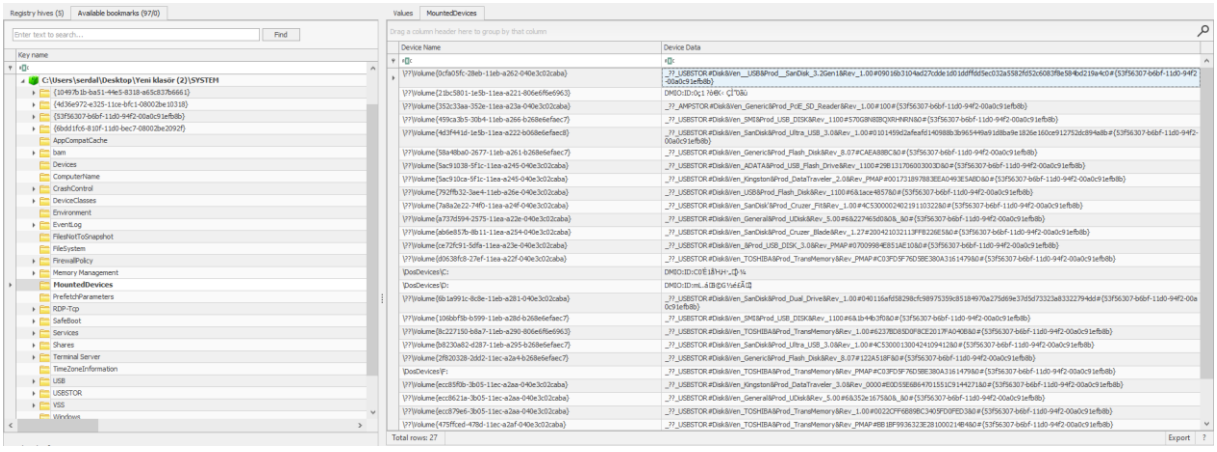


### 3.2.2. SYSTEM

**USBTOR** dosyası altına giderek takılan usb aygıtların üreticilerini, seri numaralarını ve zamanlarını detaylı bir şekilde görebilmekteyiz.



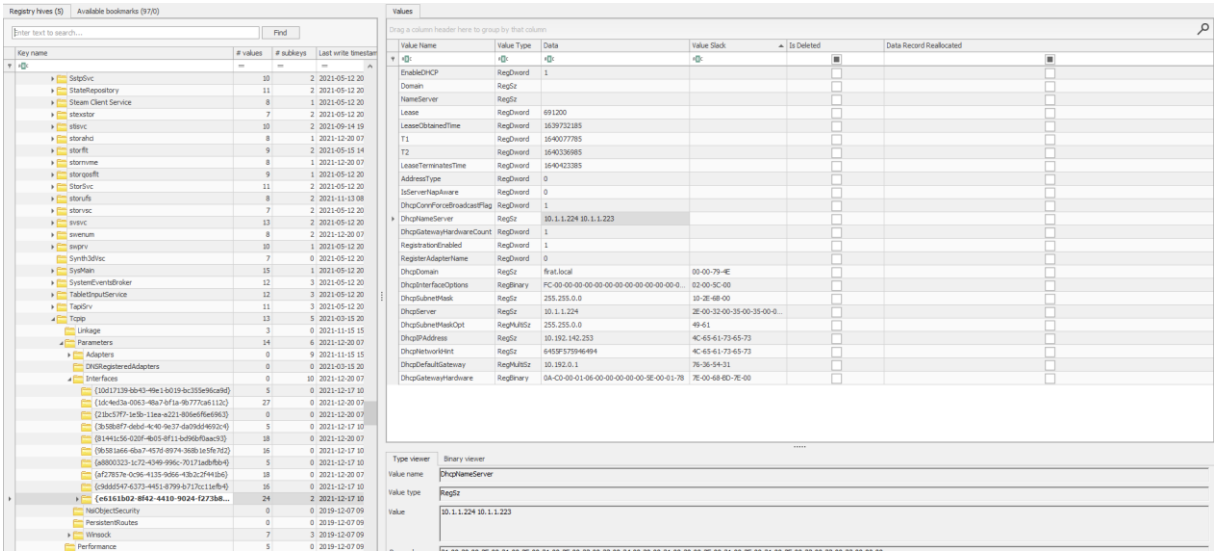
**MountedDevices** mount edilmiş cihazları göstermektedir.



**İnterface bilgileri:**

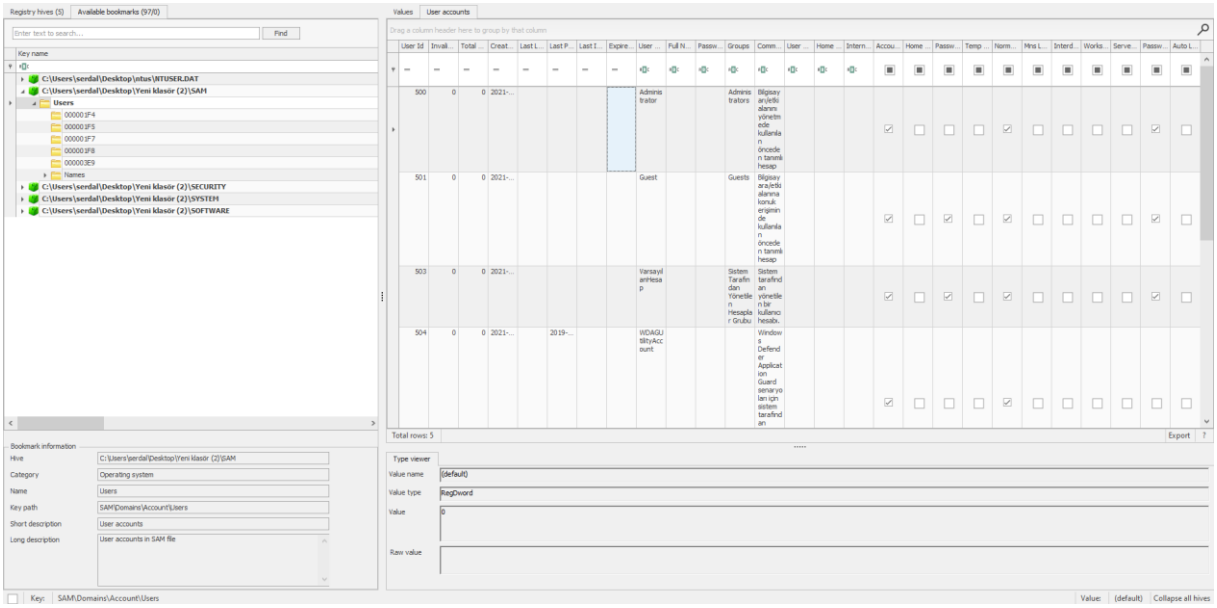
```
ControlSet001\Services\Tcpip\Parameters\Interfaces\{e6161b02-8f42-4410-9024-f273b87f3f70}
```

Konumuna giderek interfaclerimiz hakkından önemli bilgileri detaylı bir şekilde vermektedir.



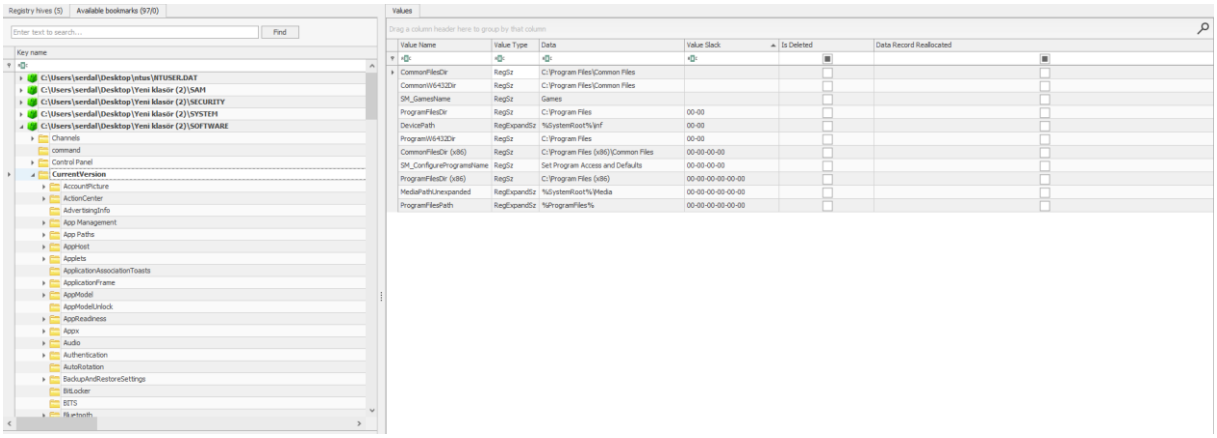
### 3.2.3. SAM

SAM dosyası altında sadece kullanıcıların son giriş tarihi, parola ipucu ve parola değiştirme tarihlerine ulaşabiliyoruz.

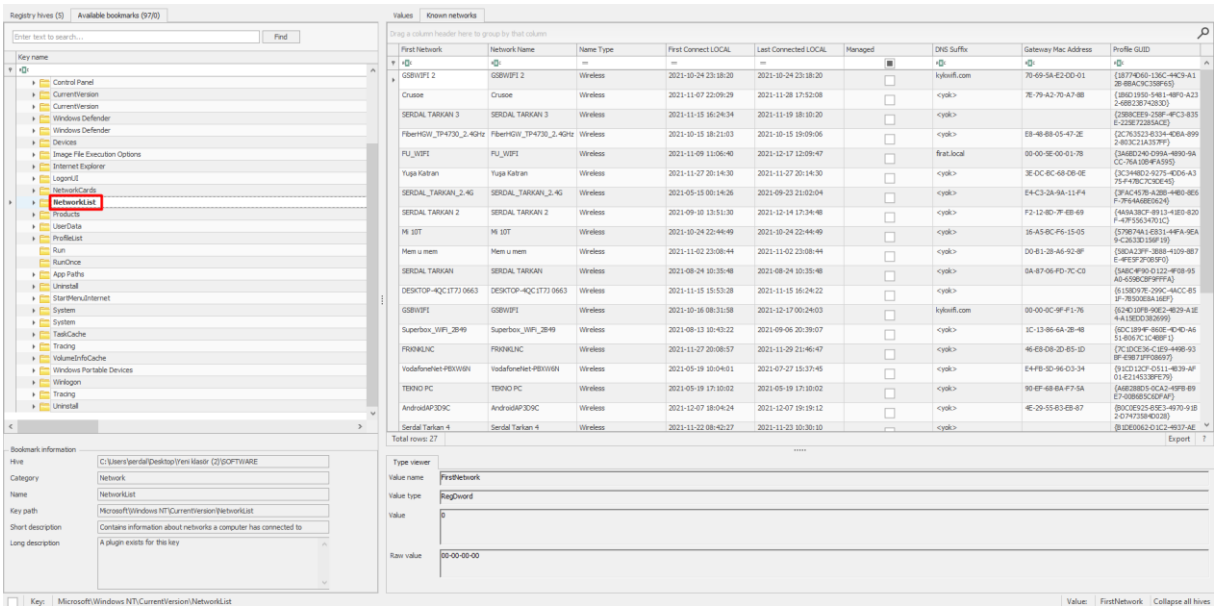


### 3.2.4. SOFWARE

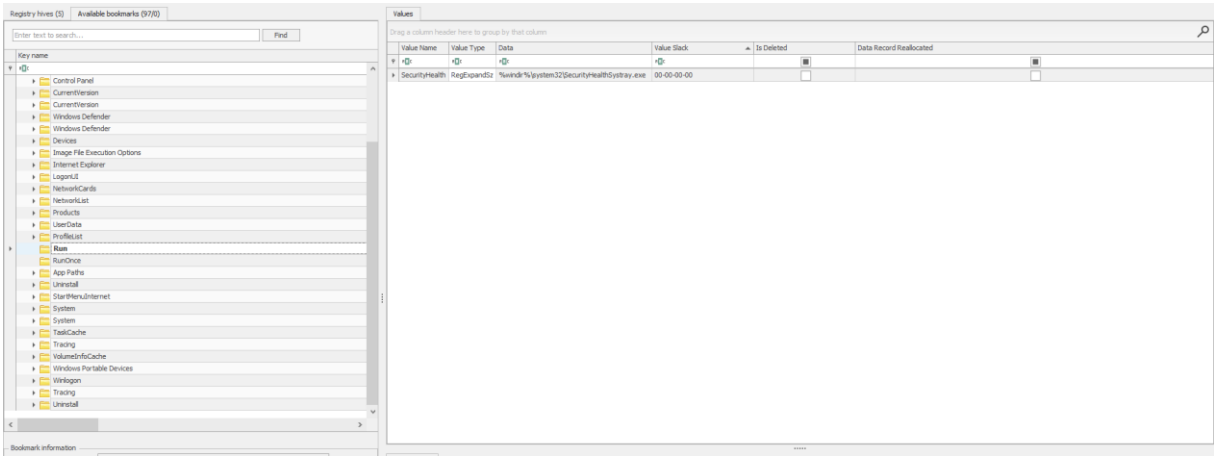
**CurrentVersion** işletim sistemi hakkında bilgi vermektedir.



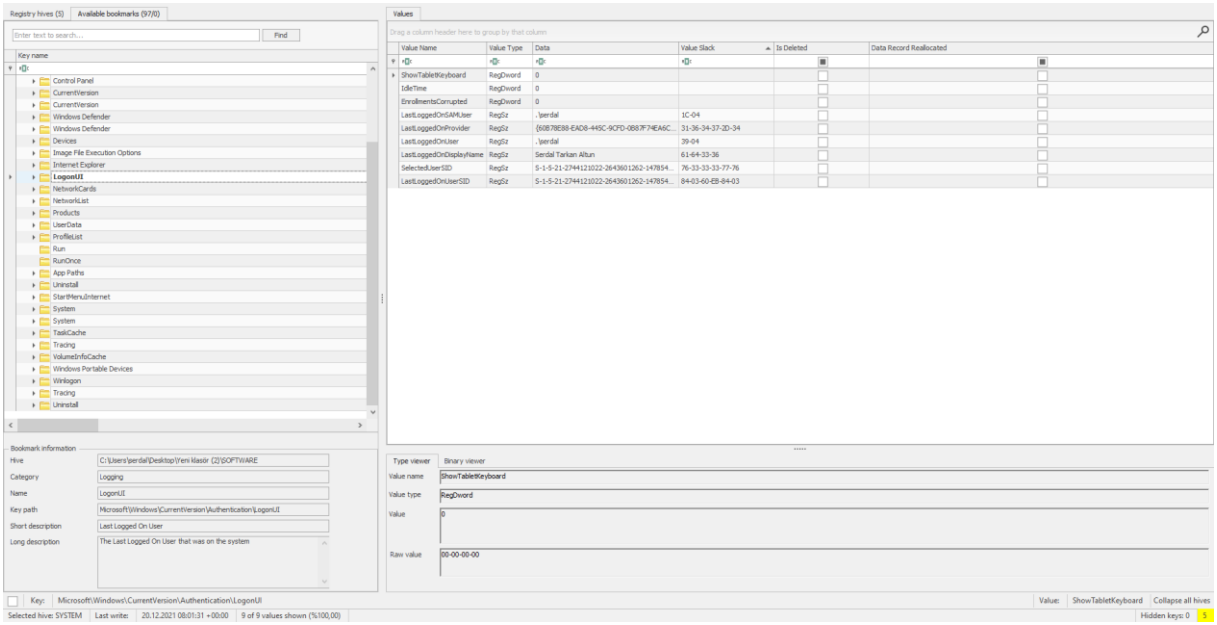
**NetworkList** kısmından bağlanılan kablosuz ağlarla ilgili ağ ismi, bağlanma tarihi, ayrılma tarihi vb. bilgilere ulaşabiliyoruz.



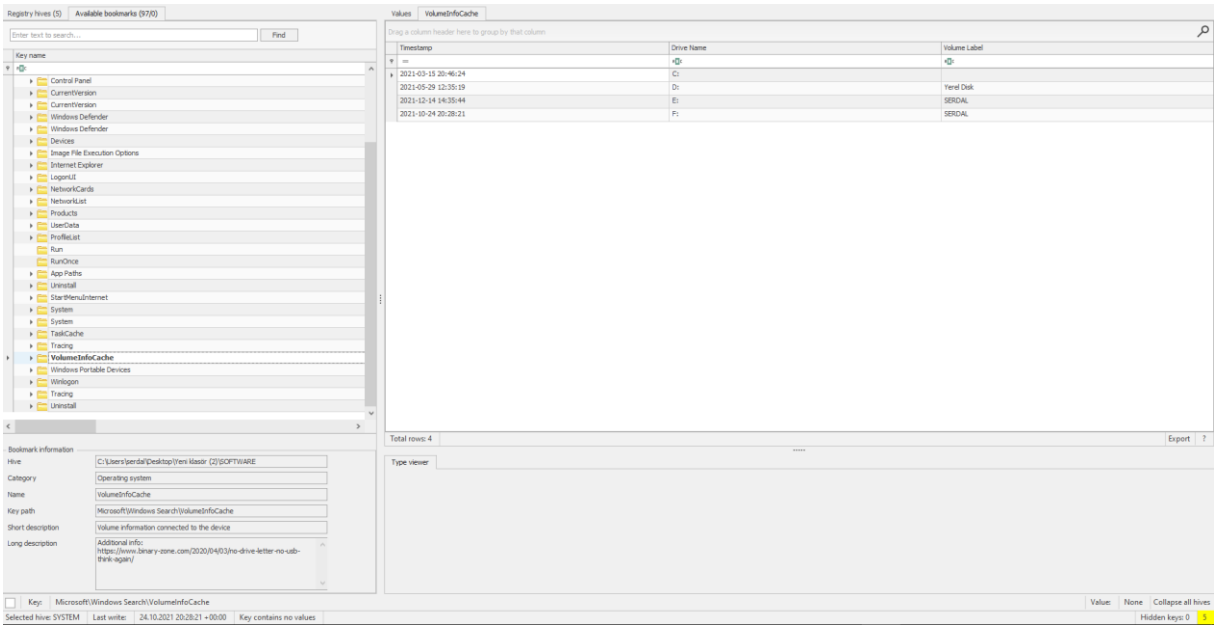
**Run** dosyası içerisinden ise başlangıç programlarını göstermektedir.



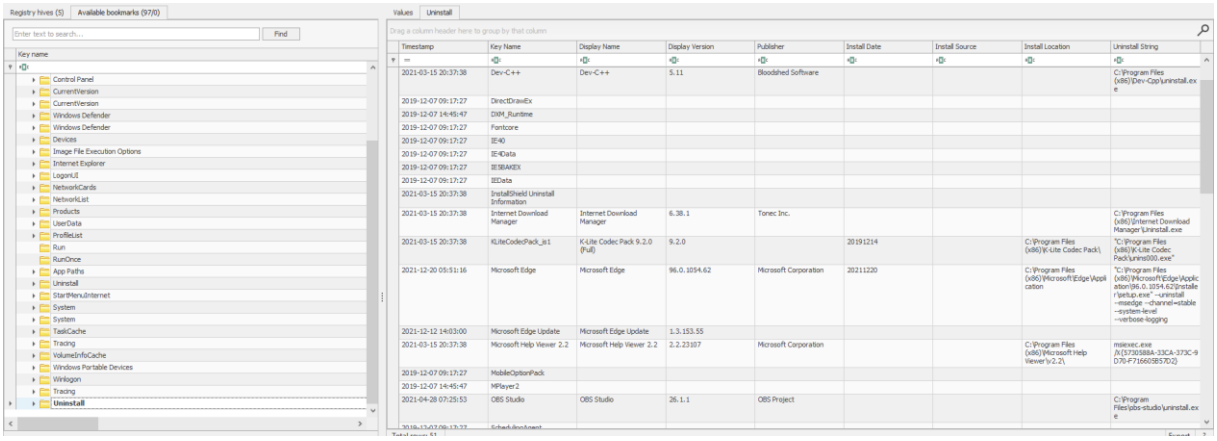
**LogonUI** dosyasında ise en son giriş yapan kullanıcı bilgileri bulunmaktadır.



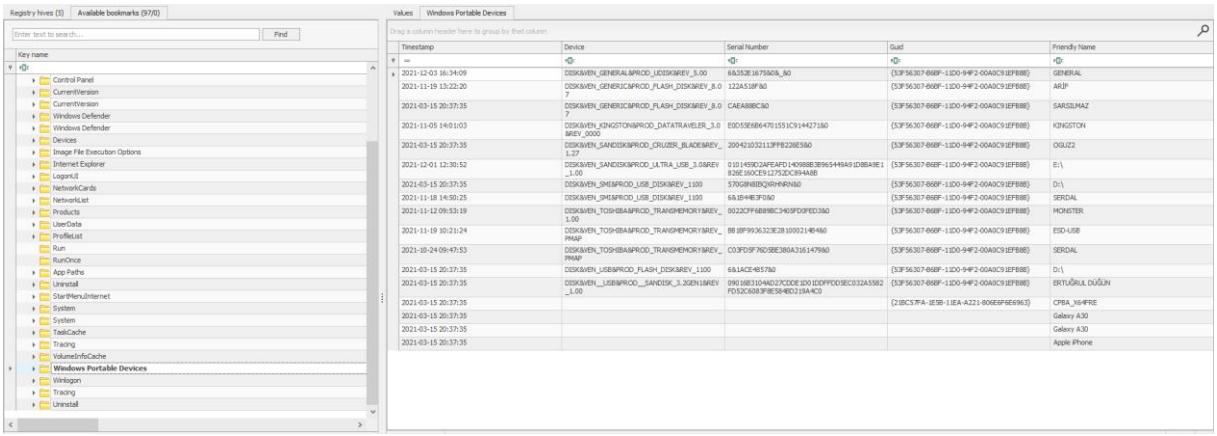
**VolumeInfoCache** dosyası altında disk bölümlerini görmekteyiz.



**Uninstall** burada ise kaldırılan uygulamalar hakkında bili verilmektedir.



**WindowsPortableDevice** dosya altında ise bağlanmış olan cihazlar hakkında bilgiler bulunmaktadır.



Anlatacaklarım buraya kadardı. Umarım faydalı olabilmişimdir. Hatalarım konusunda benimle iletişime geçebilirsiniz. 😊

# 4. KAYNAKÇA

http://www.blockcyforen.com/2021/01/windows-registry-nedir-windows.html

https://www.youtube.com/watch?v=xekpJkf2ItE

https://www.youtube.com/watch?v=VYROU-ZwZX8