FTK Imager ile Disk İmajı Alma Ve Görüntüleme

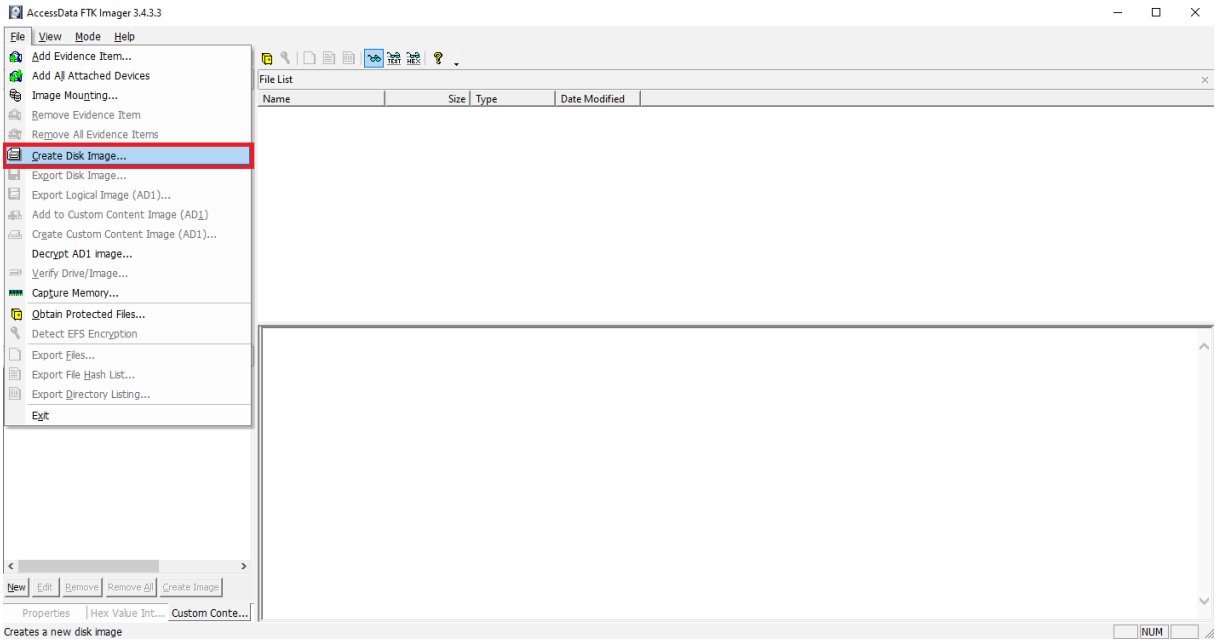
Bu yazımızda adli bilişim açısından önemli bir yere sahip olan FTK (Access Data Forensics Tool Kit) programında imaj almayı anlatacağım. Öncelikle birazcık FTK hakkında bilgi sahibi olalım.

FTK(Access Data Forensics Tool Kit) Adli bilişimde kullanılan Windows tabanlı en popüler ikinci yazılımdır. Kullanımı daha kolay olduğundan adli bilişim mühendisleri ve uzmanları tarafından tercih edilmektedir. Access Data Forensics Tool Kit'de adli bilişimin tüm aşamalarında (imaj alma, analiz ve raporlama) kullanılmaktadır.

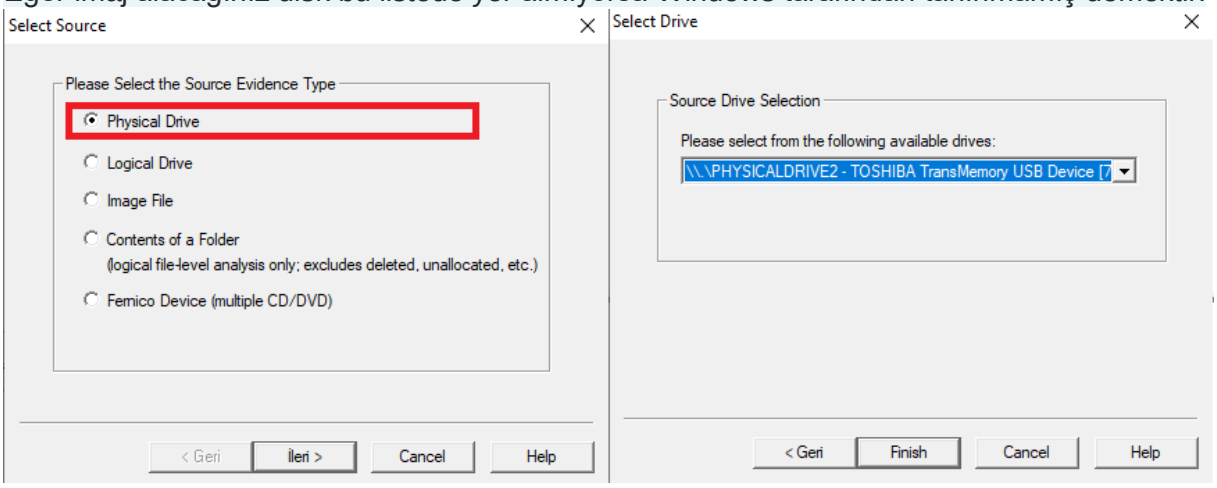
Bugün ise İmaj almak için FTK'nın ücretsiz dağıttığı FTK Imager'ı kullanacağız. FTK Imager USB, HDD ve CD-DVD gibi donanımsal aygıtlar üzerinde bulunan verilerin imajı alınabilmektedir. Aynı zamanda FTK Imager bu ortamlardaki dijital delillerin imajını almadan ön izlemesine imkan tanır.Programın en önemli özelliği adli kanıt barındıran dosyalar üzerinde MD5 ile SHA-1 denilen hash algoritmaları oluşturma özelliğine sahip olmasıdır. Adli suç unsuru barındıran dataların hepsinden Hash değerlerini oluşturma ve raporları çıkarabilmek özelliğine sahiptir. Bunun avantajı ise hedef datanın hash değerlerinin tutarlı olduğunu gösterebilmesdir.

Şimdi imaj alma kısmına geçebiliriz.

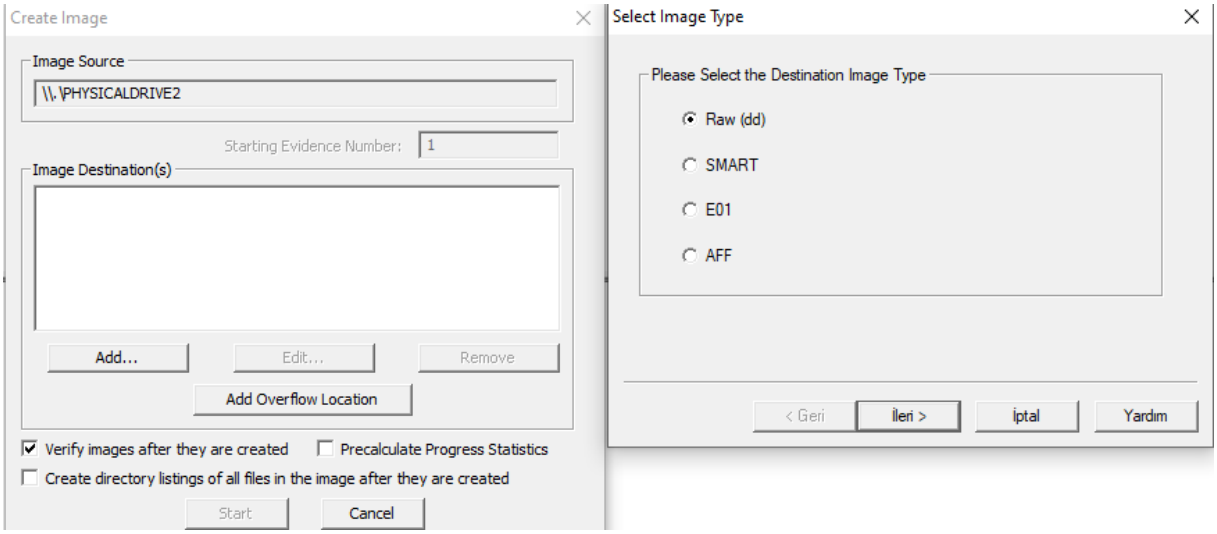
1- Programı indirip çalıştırdıktan sonra karşınıza çıkan ekrandaki File menüsünden Create Disk Image seçeneğini seçip disk imajı oluşturma aşamasına geçiyoruz.



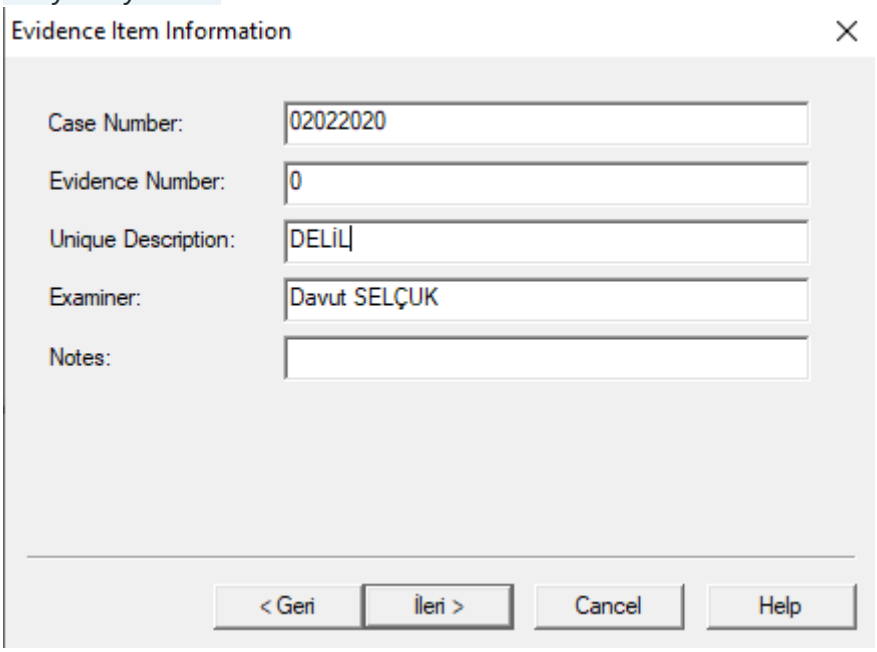
2- Create Disk İmage dedikten sonra bizde hangi donanım üzerinden imaj almak istediğimizi sormakta. Biz örnek bir USB üzerinden imaj alacağımızdan ve bu usb fiziksel bir donanım olduğundan ilk seçeneği seçerek listedeki hedef donanımı tanımlıyoruz ve Finish diyoruz. Eğer imaj alacağınız disk bu listede yer almıyorsa Windows tarafından tanınmamış demektir.



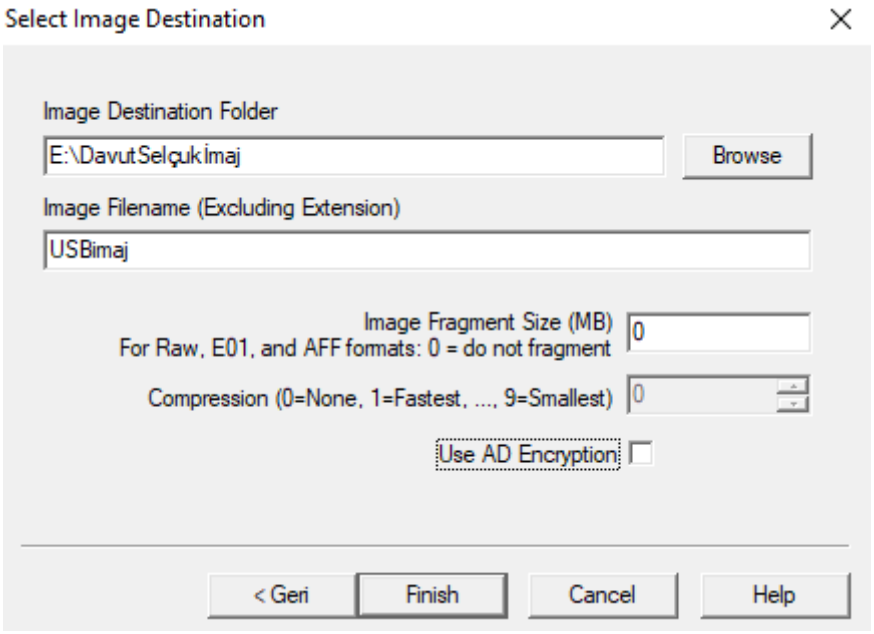
3- İmaj alacağımız diski seçtikten sonra karşımıza nereye kaydedeceğimizi soran ekran gelir.
Verify images after they are created seçeneğini seçersek imaj alma işleminden sonra doğrulama yapacaktır ve bu işlem imaj alma işlemini iki katına çıkaracaktır.
Precalculate Progress Statistics seçeneği seçilirse imaj alma işleminin ne kakar süreceğini gösterir.
Create directory listings of all files in the image after they are created imaj alınacak diskin içindeki dosyaların detayları imajın kaydedileceği yere yazılır.
Buradan Add butonuna tıklayarak incelenecek diskin hedef kısmını seçiyoruz.Karşımıza imaj tipinin ne olacağını soruyor.İlk seçeneği seçerek devam ediyoruz.



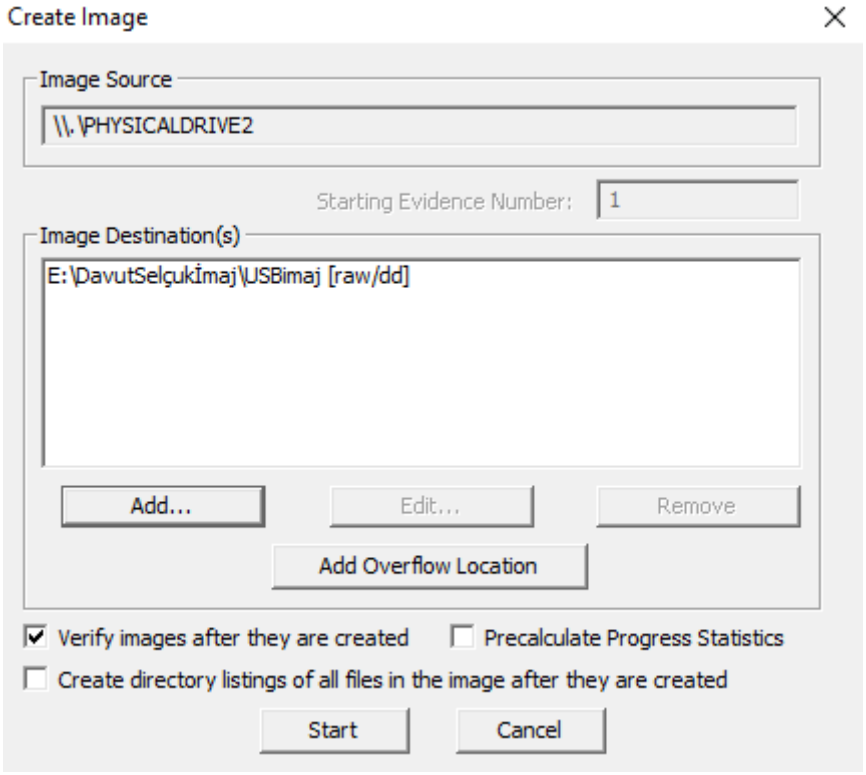
4- Bu kısımda vaka numarasını,açıklamalar,not kısmını kendi isteğiniz gibi doldura biliyorsunuz. Adli bilişim standartlarına göre doldurmanız birden fazla data analizi yapacaksanız düzenli şekilde bulunmasını sağlar. Bu bilgiler imaj dosyasının oluşturulduğu dosyada yer alır.



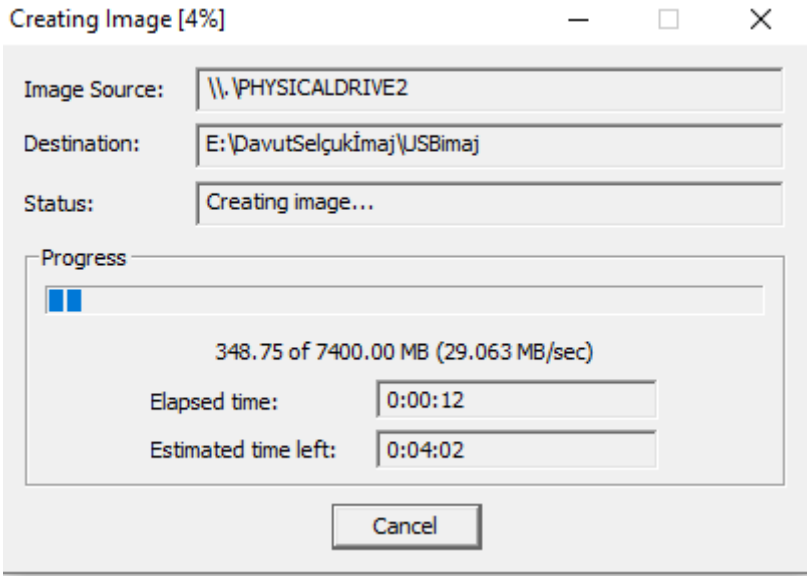
5- Bu kısımda ise imaj dosyasının nerede tutulacağını belirtiyoruz.**"Image Fragment Size (MB)"** kısmına 0(sıfır) yazılmalıdır. Hemen altında bulunan **"Compression"** seçeneği ise sadece imaj sıkıştırma desteği sunan formatlardan birisinin seçilmesi durumunda aktif olur. En alttaki seçenek ise alacağınız formattaki verinin şifreli olmasını durumda **"Use AD Encryption"** seçeneği seçilmelidir. Ve ardından Finish butonuna basılır.



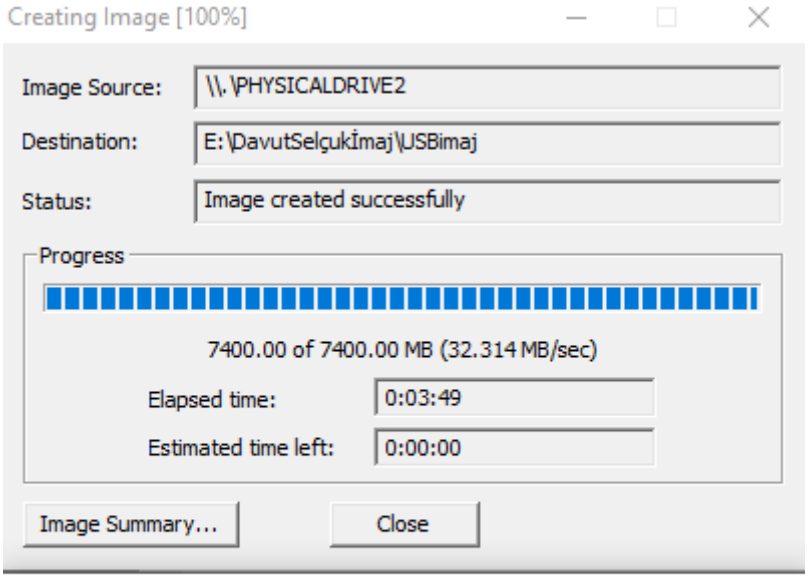
6- Yaptığımız ayarlamalardan sonra Start butonuna basarak imaj alma işlemine başlıyoruz.

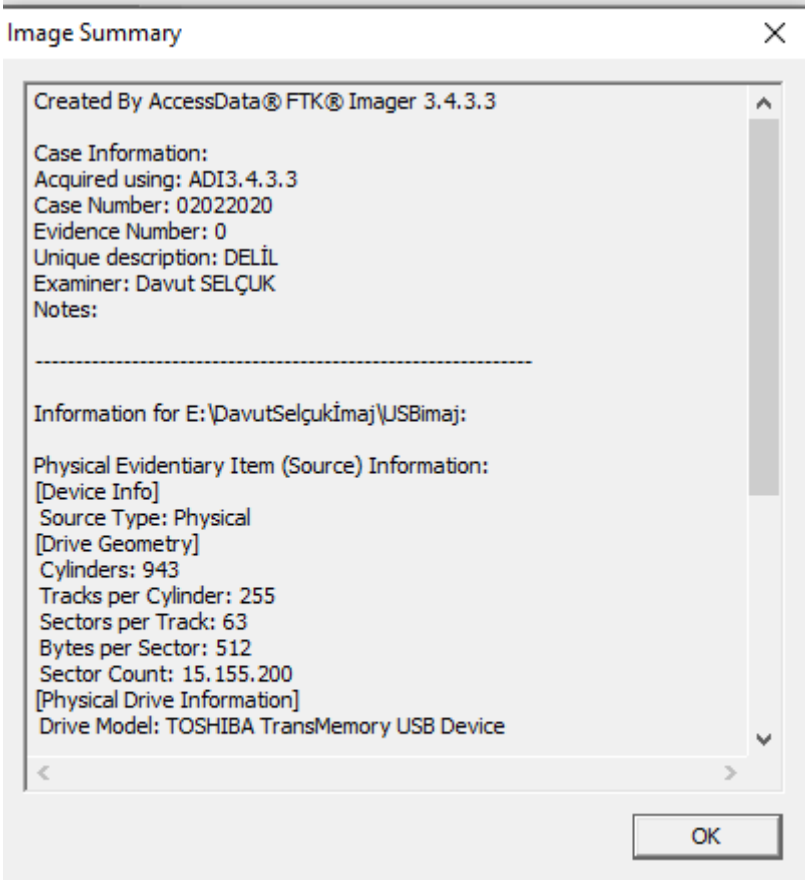


7- İmaj alma işlemimiz başlamıştır. İmaj alma işlemi diskin boyutuna göre 5 dakika ile 2-3 saat arasında sürebilir.

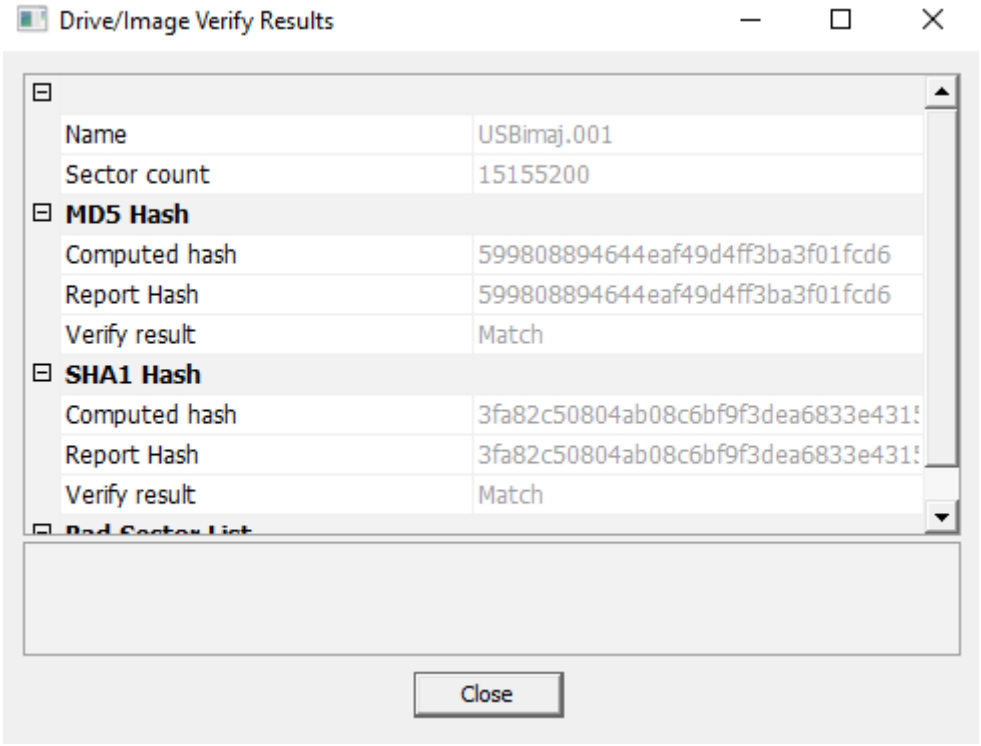


8- İmaj alma işlemimiz bitmiştir. Image Summary butonuna basarak alınan dosya imajının genel bilgileri mevcut durumdadır.

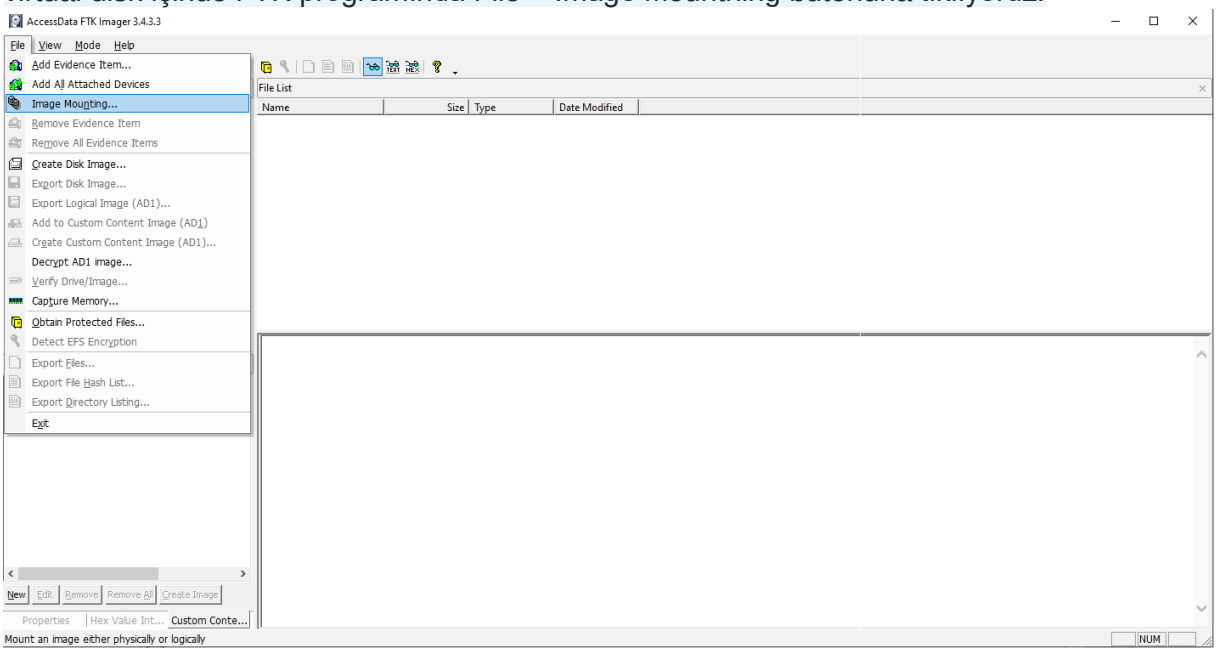




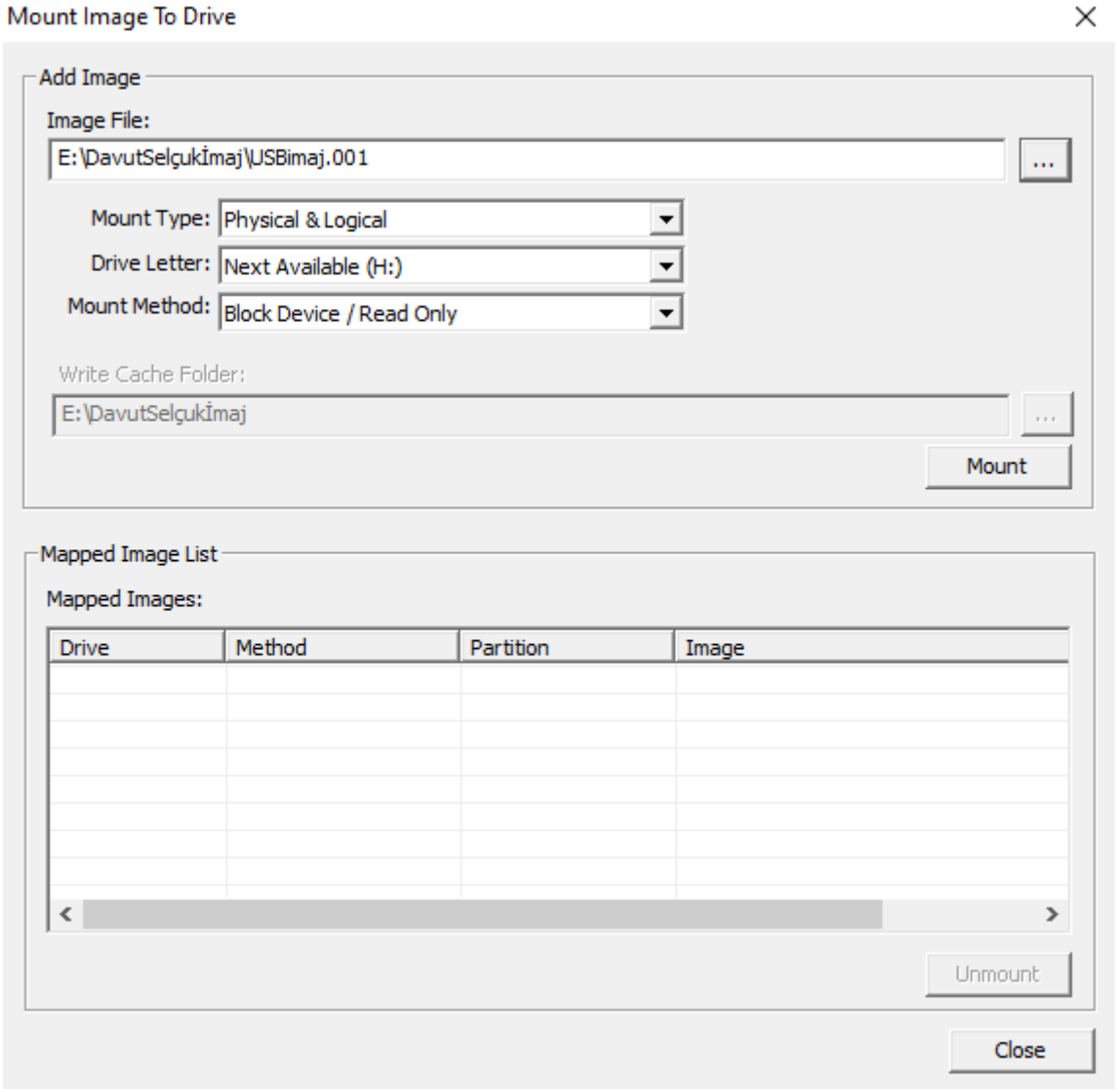
9- Karşımıza çıkan son ekranda ise diskin hash değerleri bulunur.



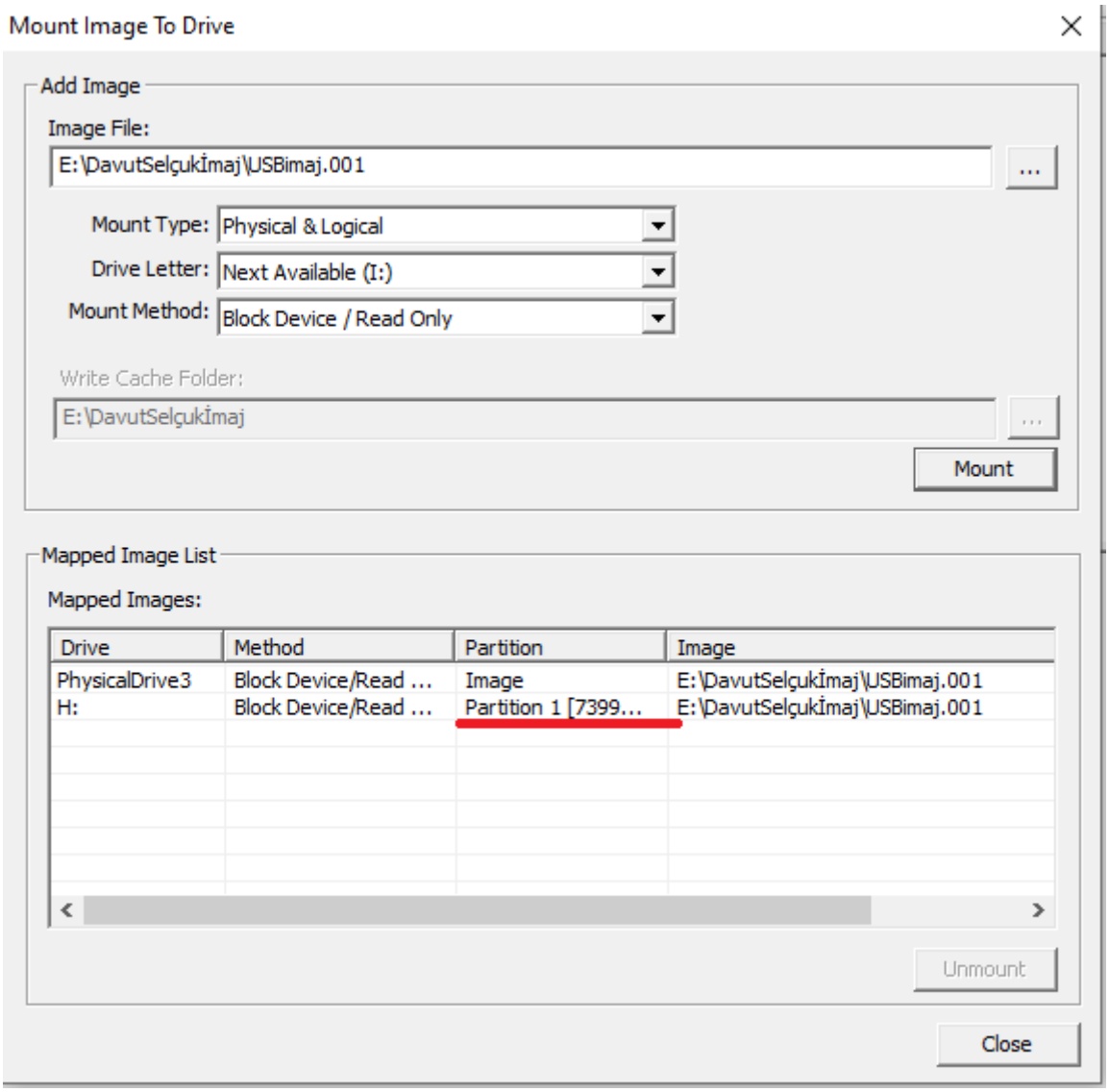
10- Peki imajı aldık ama bu imaj ile ne yapabiliriz ve nasıl inceleyebiliriz? Bunun cevabı yine program da saklı. İmaj aldıktan sonra yeni virtual disk oluşturup orada inceleme yapacağız. virtual disk içinde FTK programında File > İmage Mounthing butonuna tıklıyoruz.



11- Oluşturduğumuz imajı seçiyoruz ve ardından mount butonuna basarak sanal disk oluşturuyoruz.



12- Görüldüğü üzere program aldığımız imajın kopyası için virtual disk oluşturarak dosyaların orjinalinden farklı ama hash değerleri aynı olan dosyaları açarak verilerin orjinalliğini bozmadan çalışma ortamı sunmakta.



Yazımızın sonuna geldik vakit ayırdığınız için teşekkür ederim..