FEX IMAGER KULLANIM KILAVUZU

DÜZGÜN KÜÇÜK

1. FEX IMAGER HAKKINDA

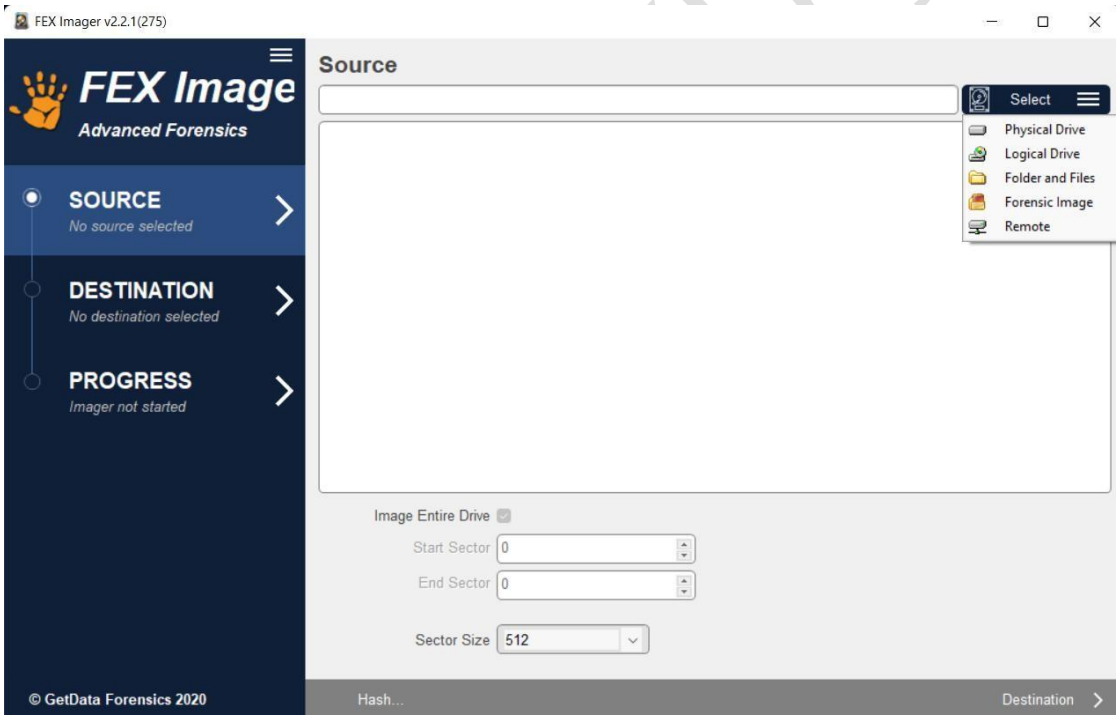
FEX Imager, GetData Forensics Firması tarafından oluşturulan bir adli kopya alma yazılımıdır.

FEX Imager programının Özellikleri

- Dizin, fiziksel sürücü, mantıksal sürücü, imaj dosyası ve GetData Forensics sunucusunu kullanarak uzak cihazlarda bulunan verilerin imajlarını alabilir.
- İmaj aldıktan sonra imajı alınan kaynak ile oluşturulan imajın hash doğrulama işlemini yapabilmektedir.
- E01 ve Raw imaj formatlarını desteklemektedir.
- Sha256, Sha1 ve MD5 hash formatlarını desteklemektedir.
- İmaj alırken imajın başlayacağı ve biteceği sektör numaraları manuel olarak ayarlanabilir.

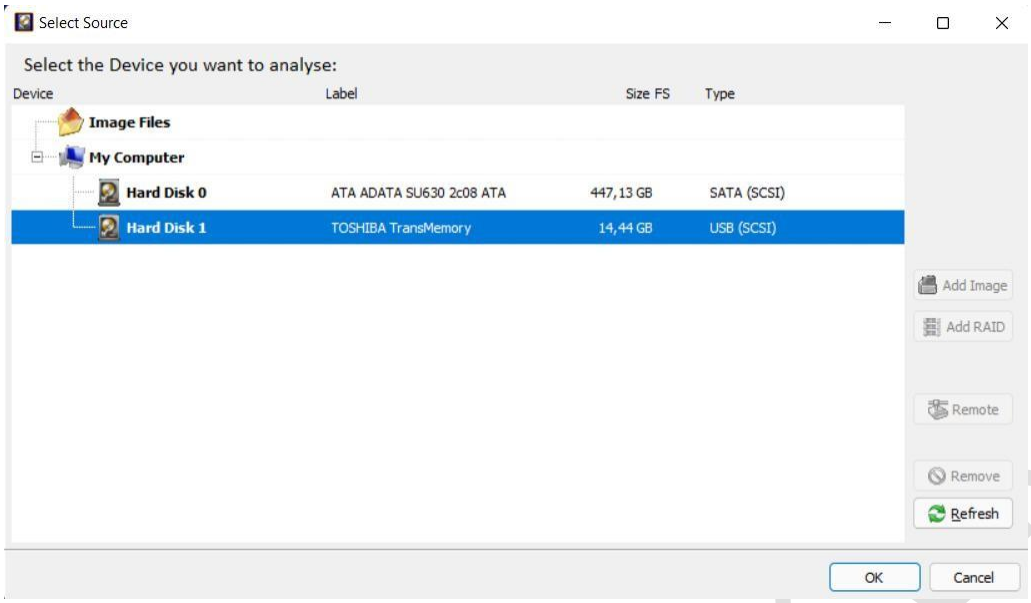
2. FEX IMAGER İLE İMAJ ALMA İŞLEMİ

Programın gayet sade ve basit bir arayüzü bulunmaktadır. Programın açılış ekranı alt görselde yer almaktadır.

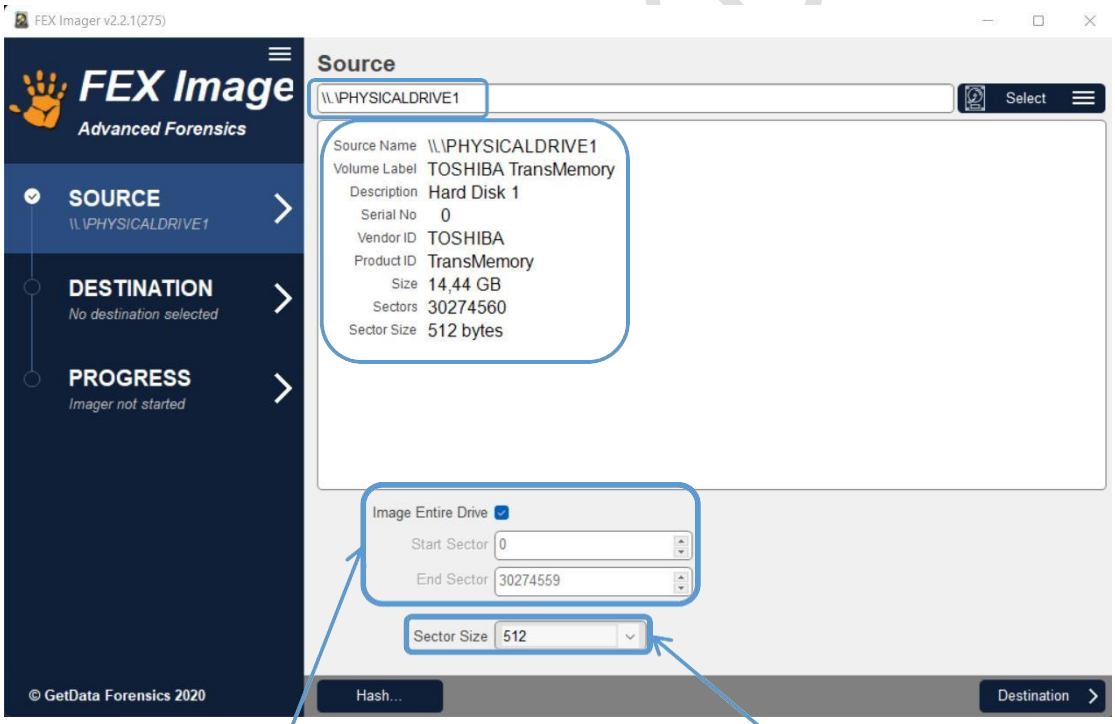


İmaj alma işlemi için ilk olarak programın sağ üst köşesinde bulunan "Select" butonuna tıklanmalı ve imajın alınacağı kaynağın tipi seçilmelidir.

İmaj tipini seçtikten sonra yeni açılan ekrandan imajı alınacak kaynağın konu seçilmelidir.



Kaynağın konumu seçildikten sonra programın önceden boş olan bölümlerine kaynağa ait bilgiler gelecektir.



Tik işareti kaldrırıldığında imaj alma işleminin diskin hangi sektöründe başlayım hangi sektöründe biteceği manuel olarak ayarlanabilir. İşaret kaldırılmadığında diskin tamamının imajı alınmaktadır.

Diskteki sektörlerin boyutunu seçmek için 512, 2048 ve 4096 olmak üzere üç seçenek bulunmaktadır.

Gerekli ayarlamalar yapıldıktan sonra imaj alma işleminin diğer adımına geçmek için sağ alt tarafta bulunan "Destination" butonuna tıklanmalıdır. Yeni açılan ekran, altta bulunan ekran alıntısında gösterilmiştir.

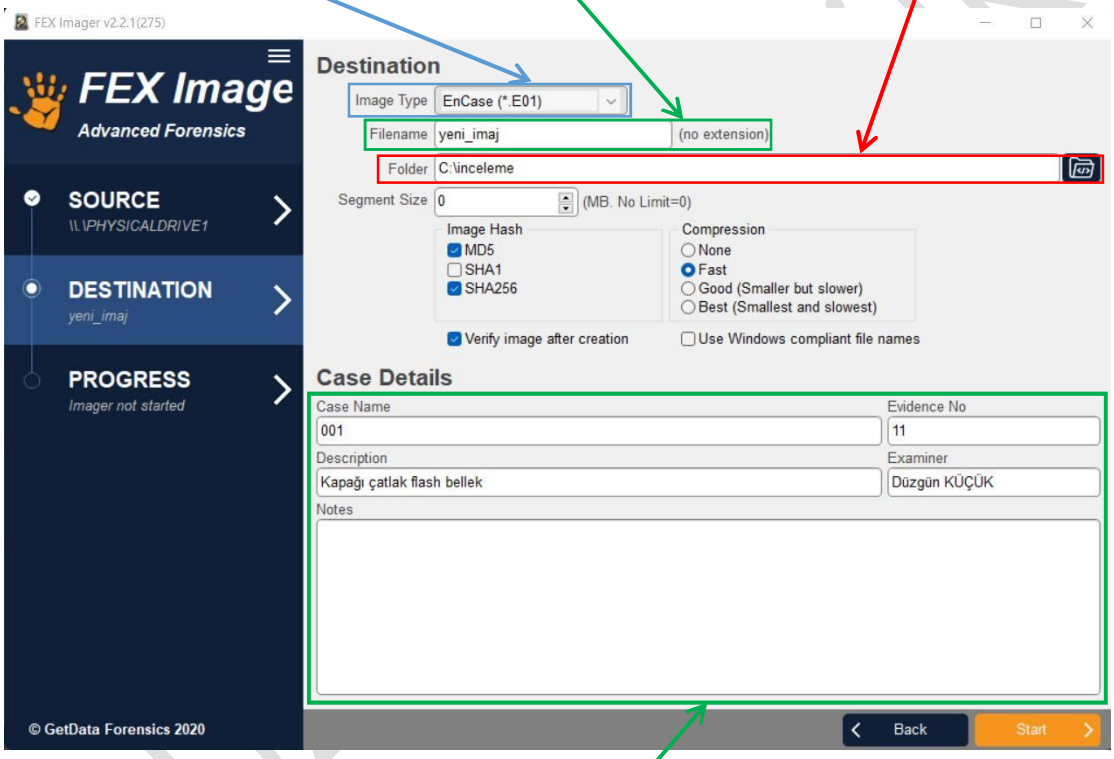
İmaj Tipinin Seçileceği Bölüm
Program, Raw ve E01 olmak üzere iki tane imaj tipini desteklemektedir.

Raw: İmaj alırken herhangi bir sıkıştırma işlemi uygulanmaz, imaj dosyasının içerisinde sadece ham veriler bulunur, imaj dosyası kaynak ile aynı boyuttadır ve imaj dosyasının içerisinde metadata bulunmamaktadır.

E01: EnCase tarafından geliştirilen, sıkıştırılmış imaj formatıdır. Veriler yazılırken parçalara ayrılır ve her parçanın içerisinde metadatalar ve doğrulama değerleri bulunmaktadır.

İmaj Dosyasının İsinin Belirlendiği Bölüm

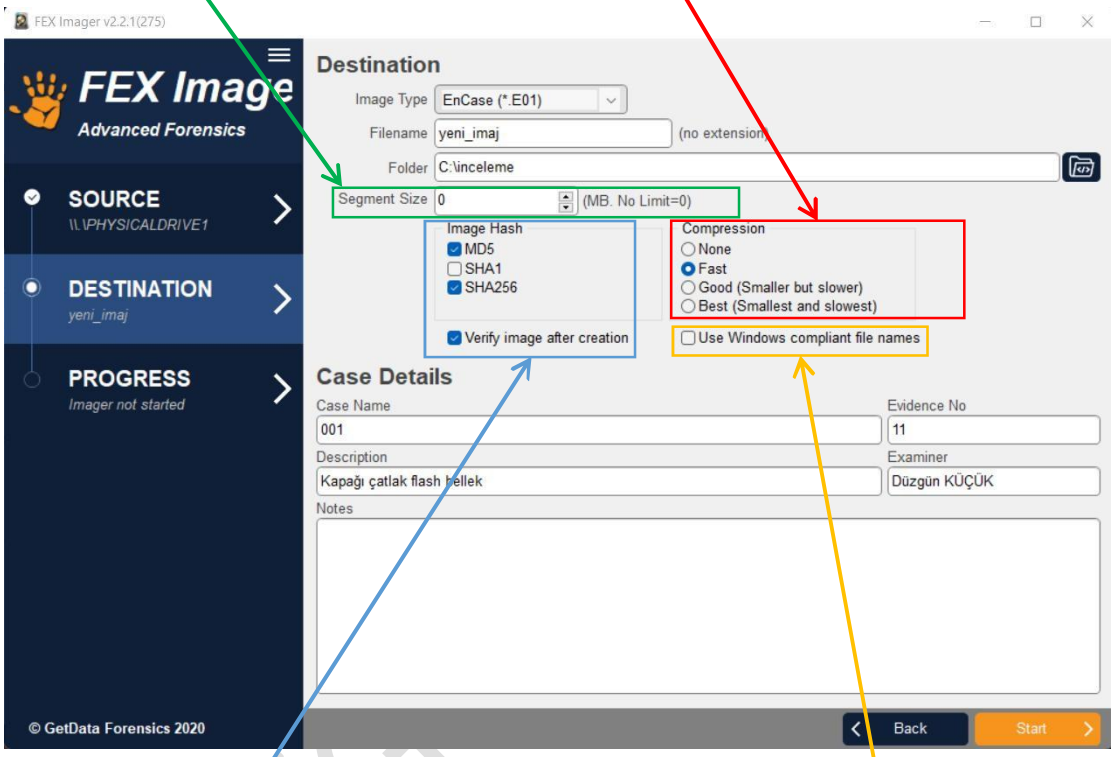
İmaj Dosyasının Yazılacağı Konum



Davaya Ait Detayların Girileceği Bölümdür

<u>İmaj Dosyasının Kaç MB'lik Parçala Ayrılacağının Ayarlandığı Bölüm</u>
Eğer değer 0 olarak ayarlanırsa parçalama işlemi yapılmadan imaj tek parça halinde oluşturulur.

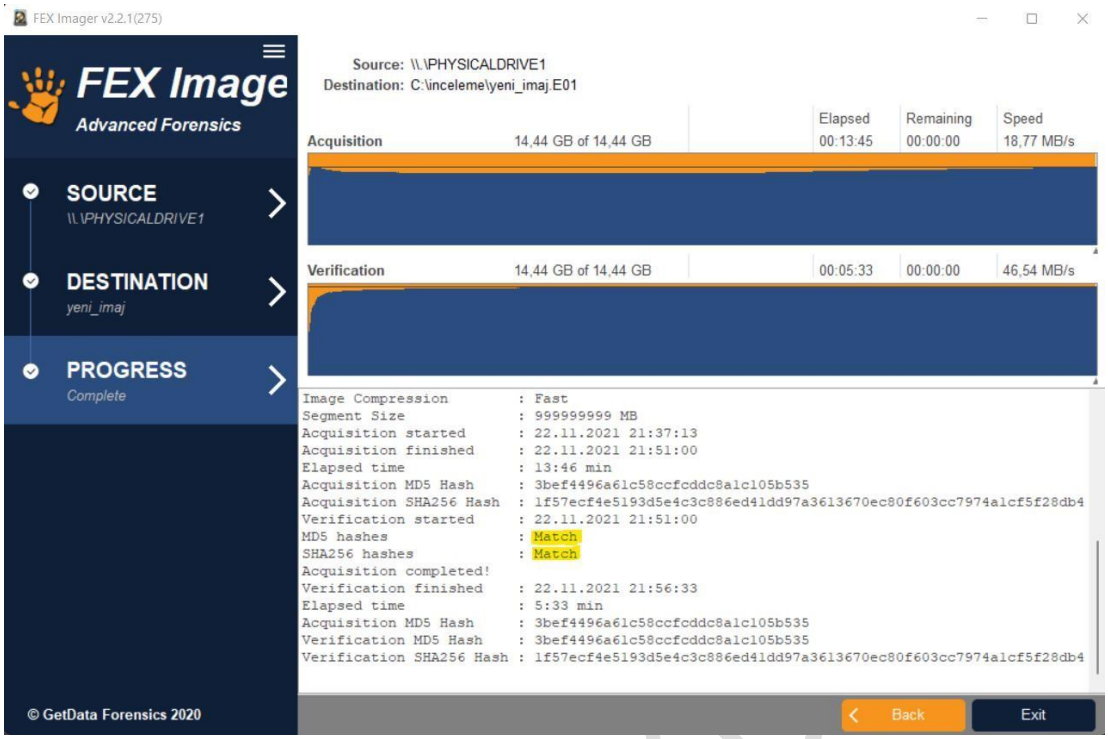
<u>Sıkıştırma Oranını Göstermektedir</u>
İmaj alma formatı E01 olarak seçilirse bu bölüm aktifleşecektir. Sıkıştırma oranı ne kadar artarsa doğru orantılı bir şekilde imaj alma süresi de o kadar artacaktır.



<u>Hash Seçenekleri</u>
Eğer "Verify image alter creation" seçeneği seçiliyse disk ve imaj dosyasını seçilen hash değerleriyle doğrulama işlemine sokar. Bu seçenek seçilmediyse alınacak imaj dosyasının sadece seçilen hash değerlerini hesaplar.

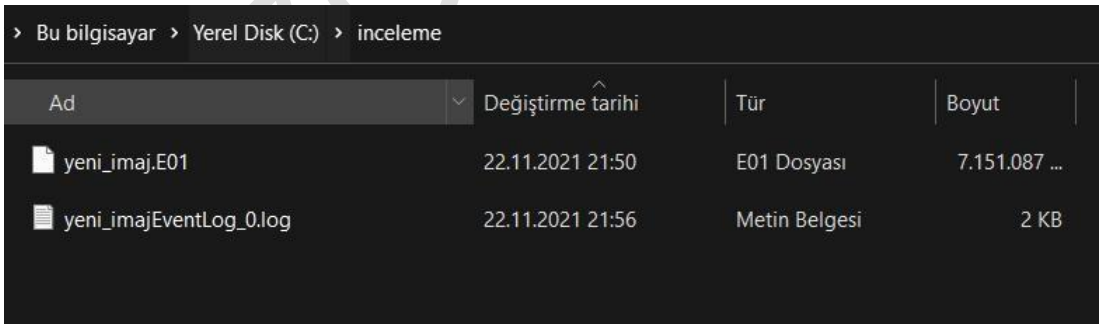
<u>Windows Uyumlu Dosya Adlarının Kullanılmasına Zorlama Seçeneği</u>

Tüm ayarlamalar yapıldıktan sonra “Start” butonuna basarak imaj alma işlemi başlatılabilir.



Üstteki görüntüde hash doğrulaması seçeneği seçili olduğu için hem imaj alma işlemi hem de hash doğrulaması işlemi yapılmaktadır. Tüm işlemlerin tamamlanmasıyla birlikte oluşturulan log kayıtları program tarafından kullanıcıya sunulmaktadır.

İmaj dosyasının kaydedildiği dizine giderek oluşturulan imaj dosyası ve log kaydına bakılabilir.

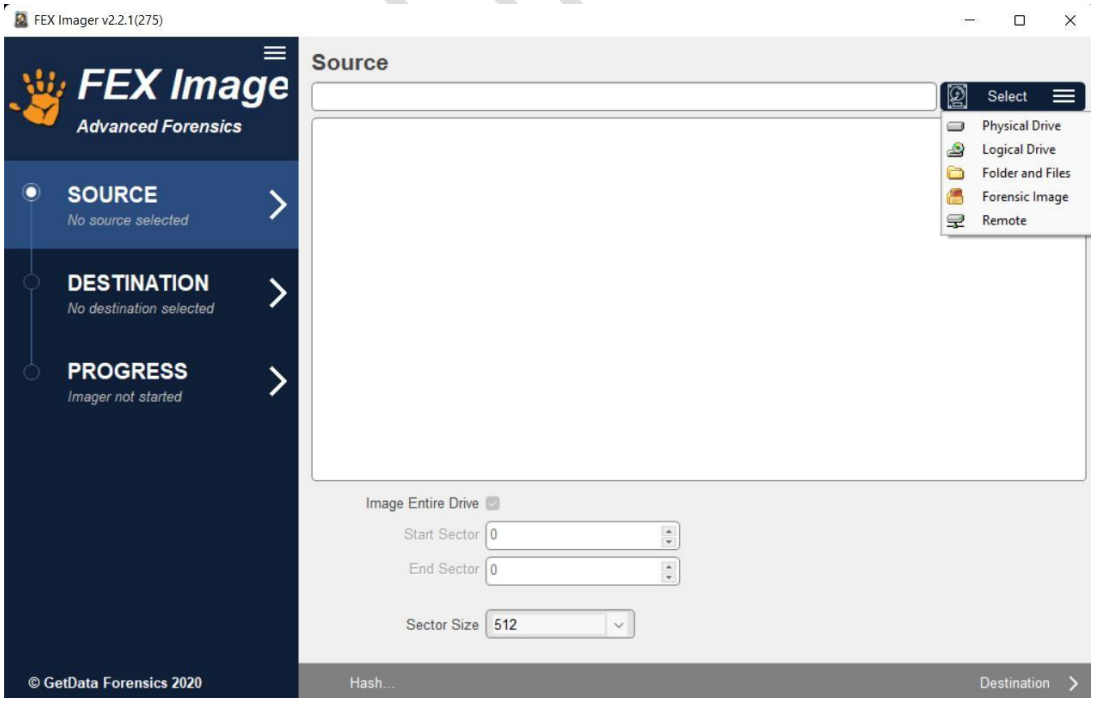


```
Created by FEX Imager (v2.2.1.275)
Case Name                : 001
Evidence Number          : 11
Unique Description       : Kapağı çatlak flash bellek
Examiner                 : Düzgün KÜÇÜK
Notes                    :
Source                   : \\.\PHYSICALDRIVE1
Volume Label             : TOSHIBA TransMemory
Description              : Hard Disk 1
Serial No                : 0
Vendor ID                : TOSHIBA
Product ID               : TransMemory
Size                     : 14,44 GB
Sectors                  : 30274560
Sector Size              : 512 bytes
Destination              : C:\inceleme\yeni_imaj.E01
Image File Type          : Encase v.6.10
Image Compression        : Fast
Segment Size             : 999999999 MB
Acquisition started      : 22.11.2021 21:37:13
Acquisition finished     : 22.11.2021 21:51:00
Elapsed time             : 13:46 min
Acquisition MD5 Hash     : 3bef4496a61c58ccfcddc8a1c105b535
Acquisition SHA256 Hash  : 1f57ecf4e5193d5e4c3c886ed41dd97a3613670ec80f603cc7974a1cf5f28db4
Verification started     : 22.11.2021 21:51:00
Verification finished    : 22.11.2021 21:56:33
Elapsed time             : 5:33 min
Acquisition MD5 Hash     : 3bef4496a61c58ccfcddc8a1c105b535
Verification MD5 Hash    : 3bef4496a61c58ccfcddc8a1c105b535
Verification SHA256 Hash : 1f57ecf4e5193d5e4c3c886ed41dd97a3613670ec80f603cc7974a1cf5f28db4
MD5 hashes               : Match
SHA256 hashes            : Match
Acquisition completed!
```

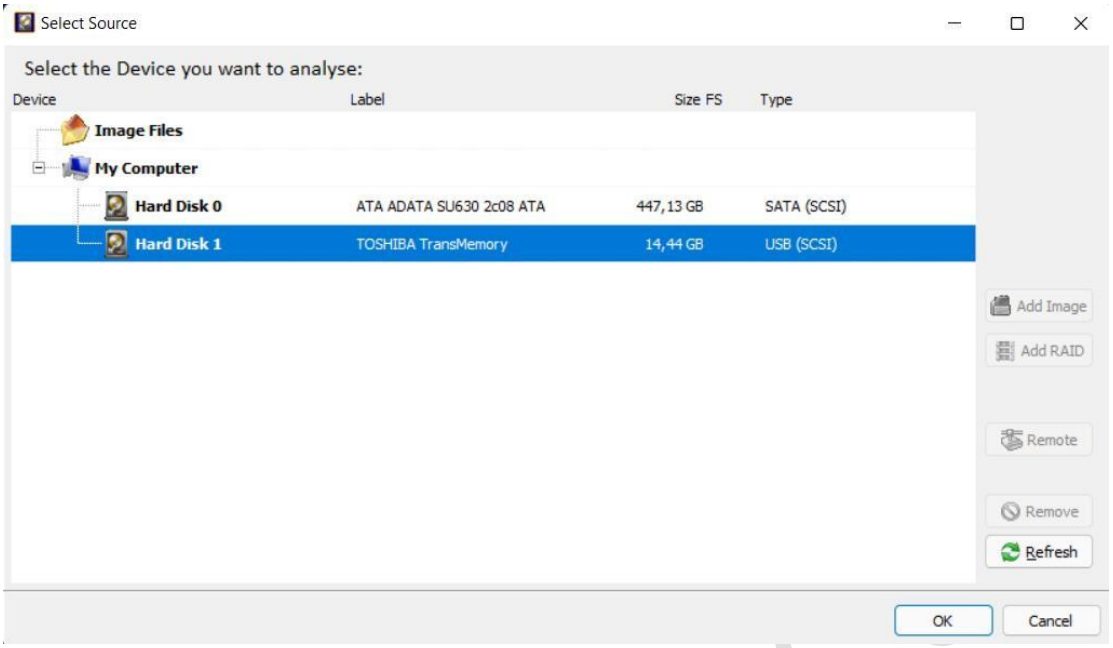
3. FEX IMAGER İLE HASH HESAPLANMASI İŞLEMİ

Fex Imager programı ile imaj alma işlemi dışında, imaj alınmadan da hash hesaplanması yapılabilir.

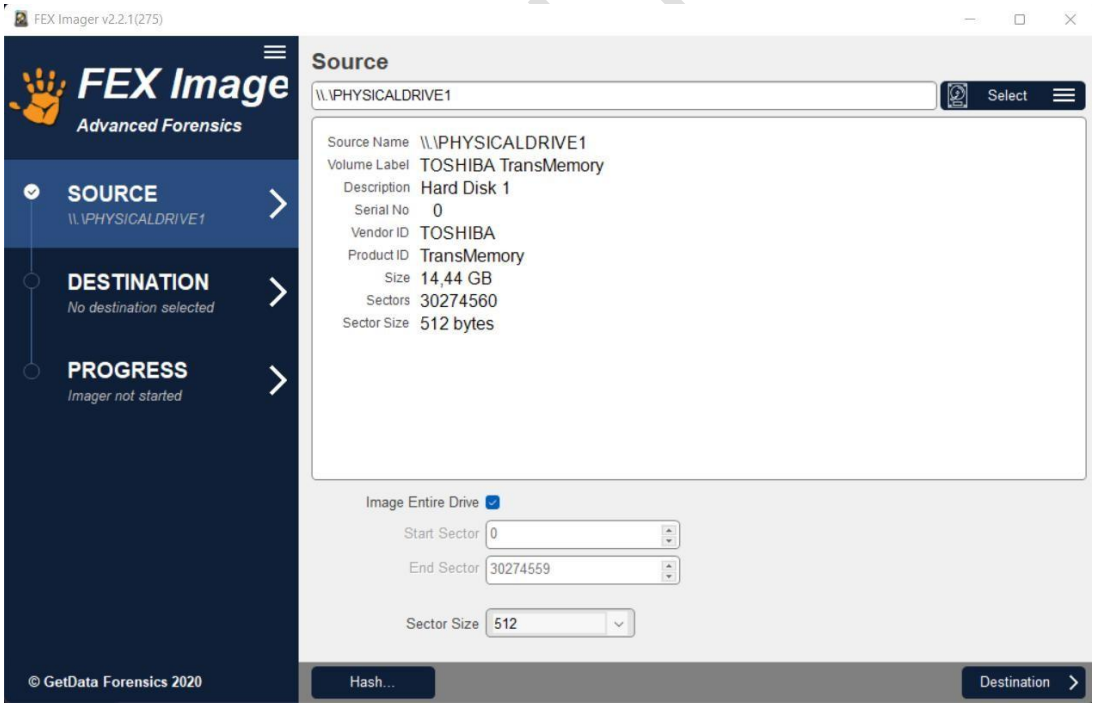
İlk olarak “Select” butonuna tıklayarak hash değerini hesaplamak istenilen kaynağın tipi seçilmelidir.



Kaynağın tipi seçildikten sonra kaynağın yolunun seçilmesi gerekir.



Kaynak seçildikten sonra programın sol alt tarafında bulunan “Hash...” butonuna tıklanmalıdır.



Açılan ekranda, kaynağa ait hangi hash değerlerinin hesaplanacağı seçilmeli ve “Start” butonuna tıklanmalıdır.

Tüm işlemler bittikten sonra seçilen hash değerleri hesaplanır ve program üzerinden kullanıcıya gösterilir.