**FEX IMAGER KULLANIM KLAVUZU**

**İÇİNDEKİLER**

**1.Giriş**

**2.FEX Imager Nedir**

**3.FEX Imager Kurulumu**

**4.FEX Imager Bölümleri**

**5.FEX Imager Arayüz Sekmeleri**

**6.FEX Imager İle Physical İmaj Alma**

**7.FEX Imager İle Logical İmaj Alma**

**8.FEX Imager İle Klasör İmajı Alma İşlemi**

**9. FEX Imager İle İmajın İmajını Alma işlemi**

**10.FEX Imager İle Remote Bağlantı**

**11.Fex Imager İle Sadece Hash Hesaplatma**

**1.Giriş**

FEX Imager yazılımı, Adli Bilişim alanında önemli sayılan yazılımlar arasında yer alan ücretsiz bir yazılımdır.

Bu kullanım klavuzunda FEX imager nedir, FEX imager’ın kurulumu nasıl yapılır, FEX imager’da inceleme nasıl yapılır bunun gibi soruların cevabını bulabiliriz.

**2.FEX Imager Nedir**

FEX Imager GetData tarafından geliştirilmiş bir adli inceleme programıdır.

E01 ve DD (RAW) formatındaki imajları birbirleri arasında kolayca dönüştürme özelliğine sahip.

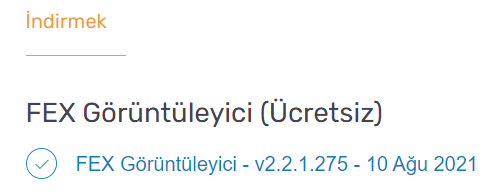
Orjinal medyanın tümü yerine istediğiniz aralıktaki sektörlerin imajını almayı olası kılıyor.

MD5, SHA1 ve SHA256 HASH değeri hesaplama ve her sektör için SHA256 HASH değeri hesaplama, imaj dosya büyüklüğü belirtme, imaj sırasında transfer hızı ve süre bilgisi gösterebilme, ayrıntılı kayıt (log) tutabilme, EnCase imajları için sıkıştırma ve vaka detayları girebilme. Program ayrıca her sektörün ayrı ayrı HASH değerini hesaplatabiliyor ve bu özelliği ile kısmen bozuk disklerdeki veri bütünlüğü kontrol edilebiliyor.

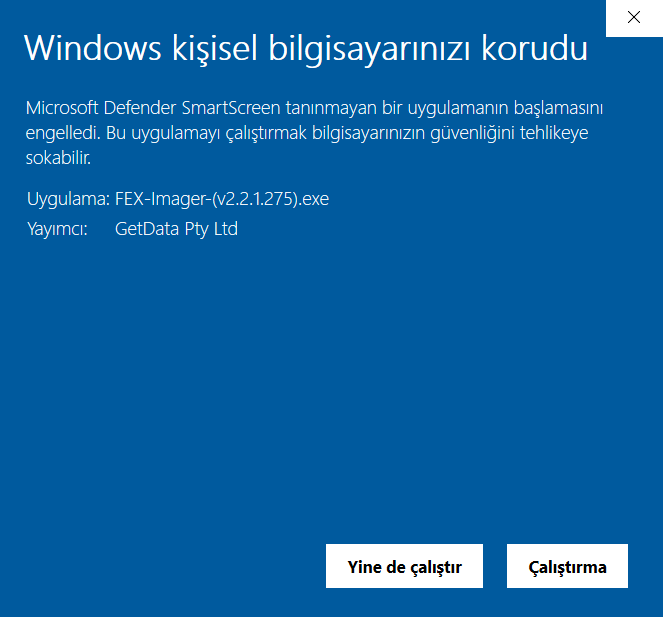
**3.FEX Imager Kurulum**

FEX imager yazılımını GetData’nın web sitesinden ücretsiz bir şekilde indirebilirsiniz.

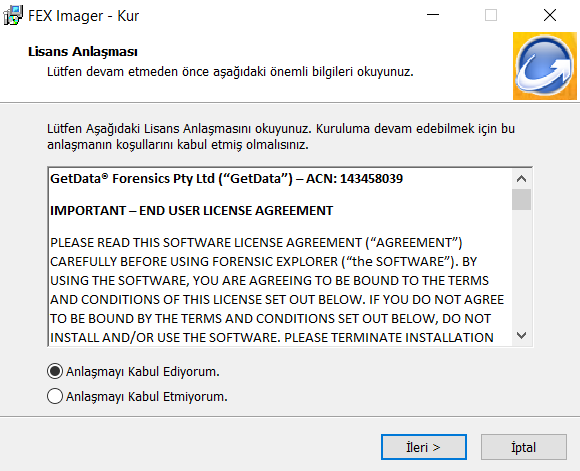
<https://getdataforensics.com/product/fex-imager/download/>



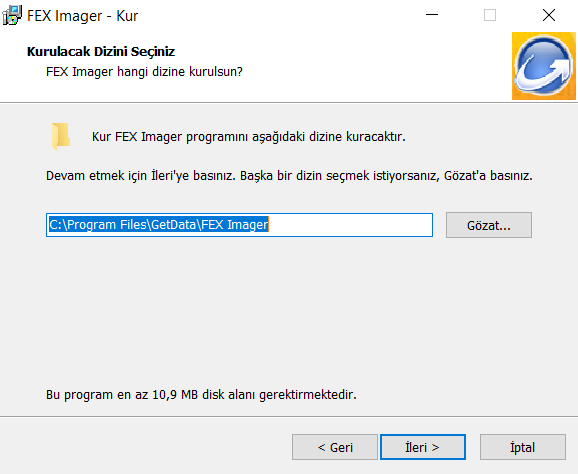
* İndirmek için tıklanır.



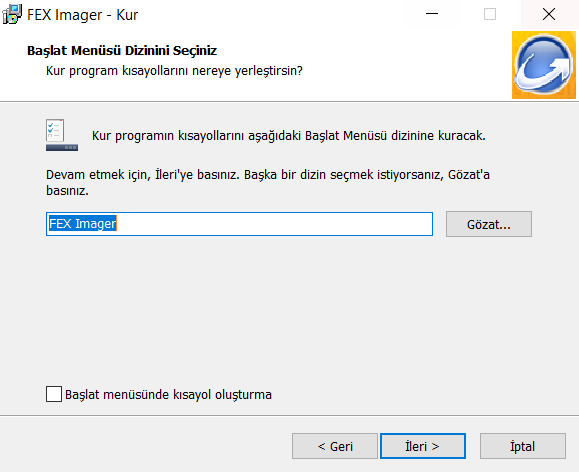
* Kurulumun yapabilmesi için Yine de çalıştır’a basılması gerekir.



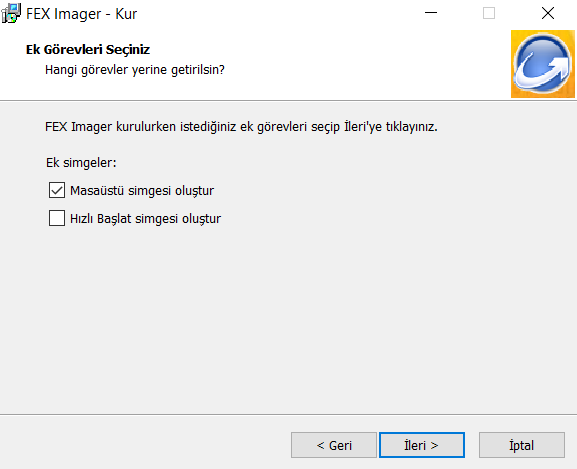
* Kurulumu gerçekleştirebilmek için Anlaşmayı Kabul Ediyorum’a tıklanması gerekir.Ardından ileri denir.



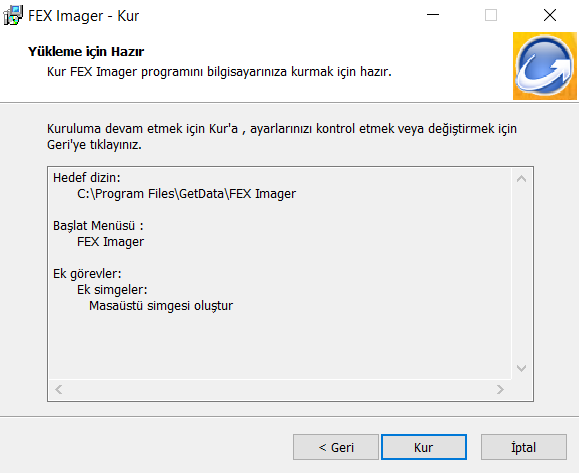
* FEX Imager programının kurulacağı dosya yolunu seçip İleri denir.



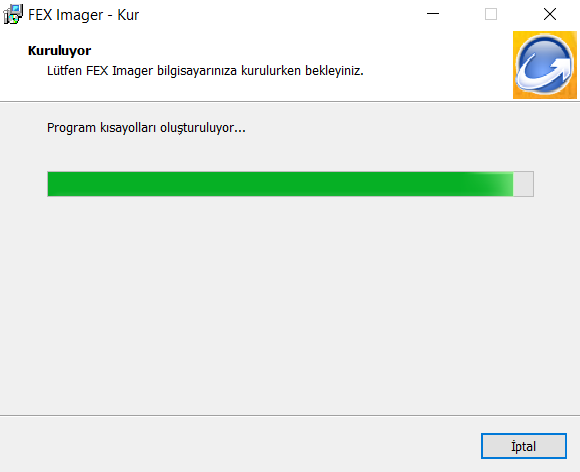
* FEX Imager programının masaüstündeki ismi belirlenir.



* Masaüstü kısayol oluşturmak için seçme yapılabilir.



* Seçimler yapıldıktan sonra Kur butonuna basılıp kurma işlemi başlatılır.



* Kurulumun başladığı ve devam ettiği görülür.



* Kurma işlemi tamamlandıktan sonra Son butonuna tıklanılır.



* Kısayol masaüstünde oluşturuldu.

**4.FEX Imager Bölümleri**

FEX imager 3 bölümden oluşur:



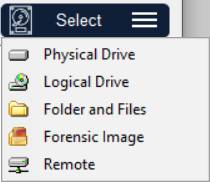
**Source**: Giriş bölümü burasıdır. Alacağımız imaj türünü seçme işlemini burda gerçekleştiririz.

**Destination:** Hedef ekranıdır, imaj dosyasının parametrelerinin bulunduğu yerdir set, tip, sıkıştırma, isim, yer vb bilgileri burdan ayarlayabiliriz.

**Progress: :** İlerleme ekranında kaynak bilgileri ve hedef bilgileri görüntülenir. İmaj alınırken geçen süre , ilerleme bilgisi, imaj bitimine kalan süre ve imaj alma hızı görüntülenir.

**5.FEX Imager Arayüz Sekmeleri**

**Select Bölümü:**



Select bölümünde alınabilen imaj türleri gösterilir.

Bu imaj türleri aşağıdaki gibidir:

**Physical Drive:** Fiziksel imaj alma işlemi gerçekleştirilir**.**

**Logical Drive:** Mantıksal bir bölümün imaj alma işlemi gerçekleştirilir**.**

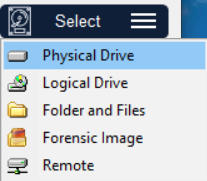
**Folder and Files:** Dosya ya da klasörün imajını alma işlemi gerçekleştirilir.

**Forensic Image:** İmajın imajını alma işlemi gerçekleştirilir.

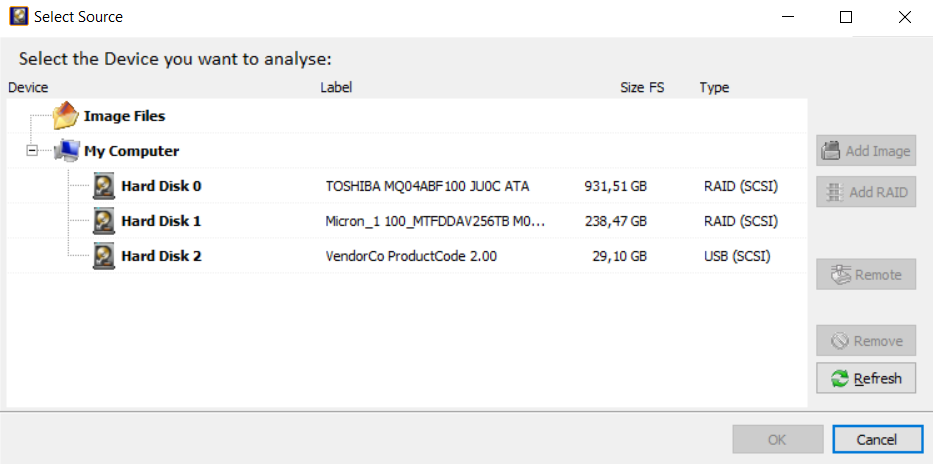
**Remote:** Uzaktan bağlantıyla imaj alma işlemi gerçekleştirilir.

**6.FEX Imager İle Physical İmaj Alma**

**-** Select bölümüne tıklandıktan sonra Physical Drive butonuna basılarak bilgisayarda var olan fiziksel aygıtlar görülür.



**-** İmajı alınacak USB depolama aygıtı seçilir.



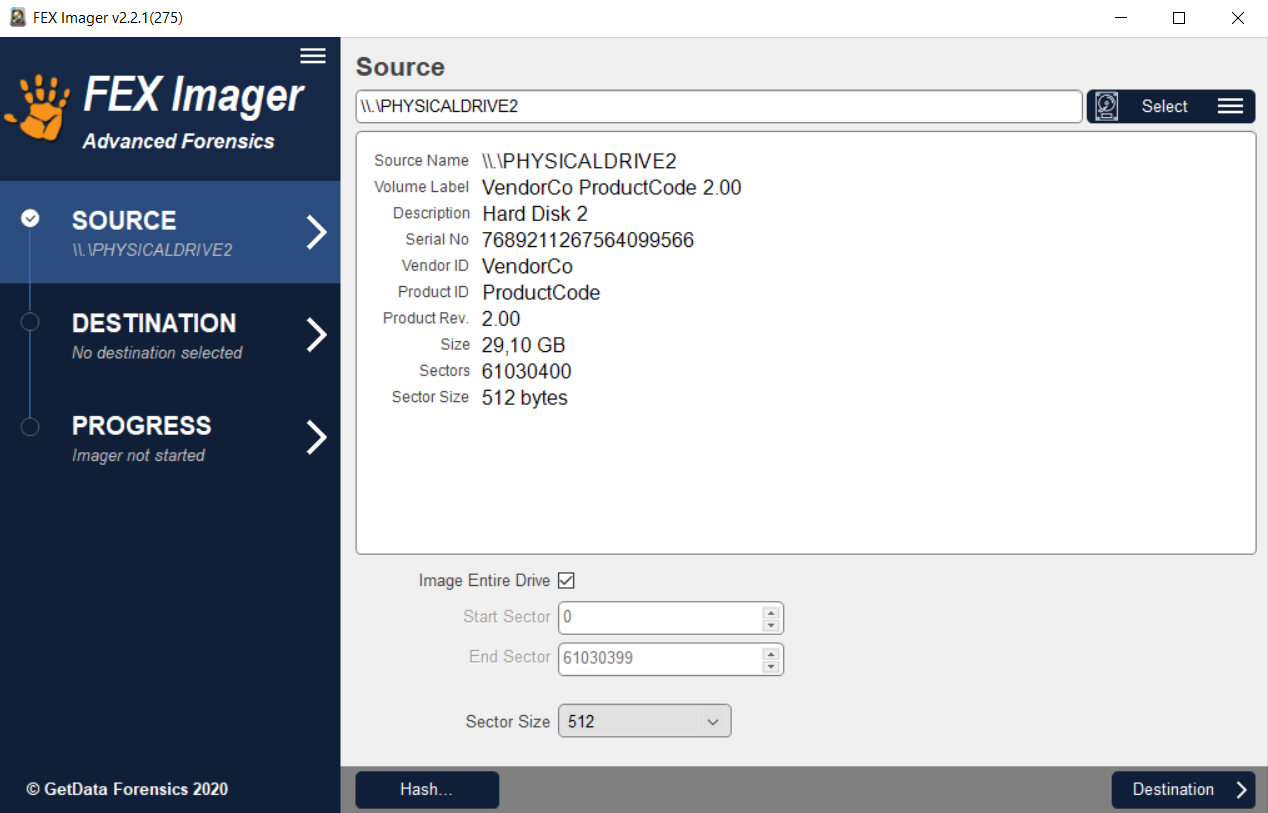
**Add RAID:** RAID sistemi ekleyebiliyoruz.Raid birden fazla diske veri kaydetme.Raid bir verinin kaydedilme türüdür.

**Remote:** Ağ üzerindeki bir bilgisayarın IP adresi ve port numarası biliniyorsa, buraya ağ üzerinden bir bilgisayarı bağlayıp ağ üzerinden bir bilgisayarın incelenmesini sağlanır.

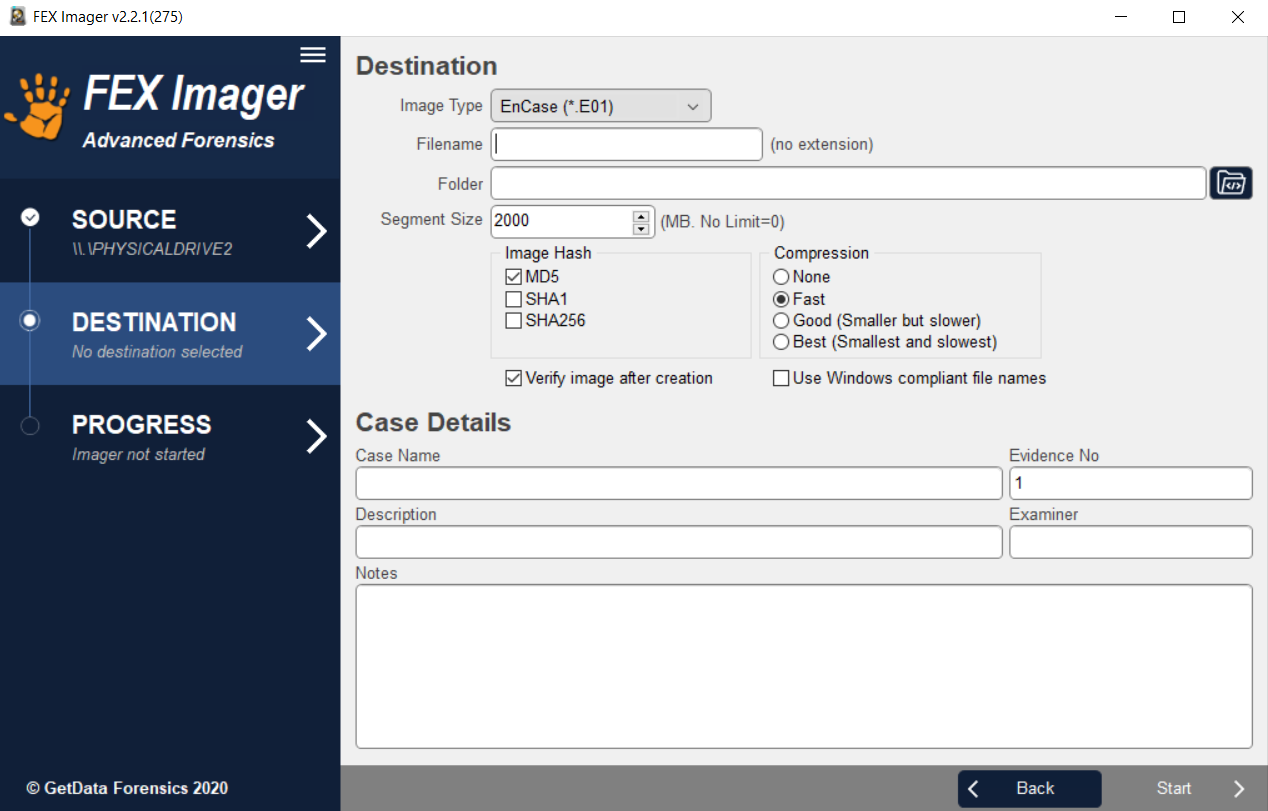
**Remove:** Kaldırmak için kullanılır.

**Reflesh:** Yenilemek için kullanılır.

**-**  Seçtikten sonra yeni pencerede seçtiğimiz fiziksel cihaz hakkında bilgiler gelir. Aynı pencerenin altında eğer takılan cihazın tümüyle imajı alınacaksa Image Entire Drive seçilir.Tüm imaj alınmayacaksa eğer imajı alınacak cihazın sektör başlangıcı ve bitişi girilir. Sector Size’a basıldığında sektör boyutu seçilir.



**-** Ayarlamalar yapıldıktan sonra sağ alt taraftaki Destinationbutonuna tıklanır.



* **Destination kısmı**

**Image Type:** İmaj tipi seçilir.Fex imager E01 ve DD imaj sıkıştırma formatlarını destekler.

**Filename:** Alınacak olan imajın ismi yazılır.

**Folder:** Alınacak olan imajın kaydedileceği dosya yolu belirlenir.

**Segment Size:** Kaç MB’lık bölümler olarak imajın kaydedileceği seçilir.Belirlediğimiz bir boyut seçilebilir.

**Image Hash**: İmajın hangi hash değerlerinde(MD5,SHA1,SHA256) hesaplanması isteniyorsa o hash değerleri seçilir.

**Compression :** Sıkıştırma işleminin hangi şekilde yapılacağı seçilir.

* **Case Details kısmı**

**Case Name:** Vakanın ismi yazılır.

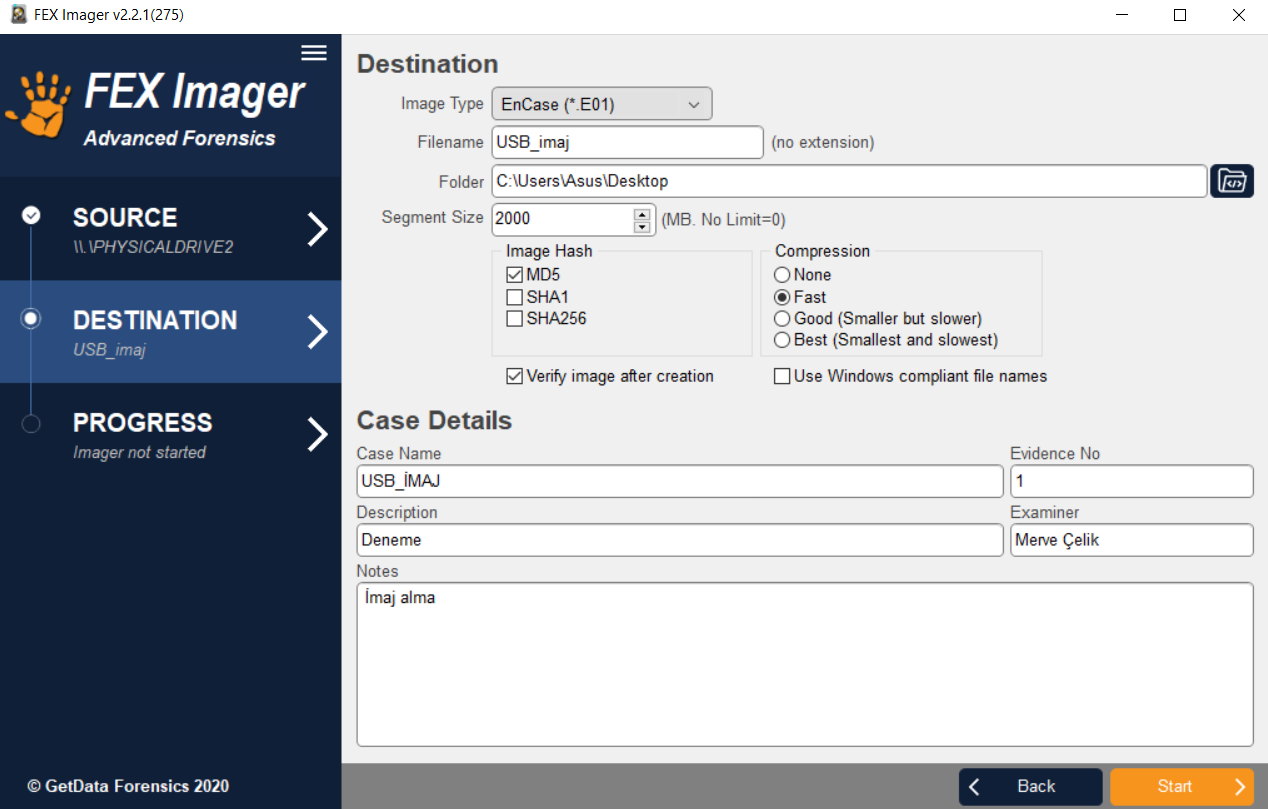
**Evidence No:** Kanıt numarası yazılır**.**

**Description:** İmajı bize tanımlayan özellik yazılır.

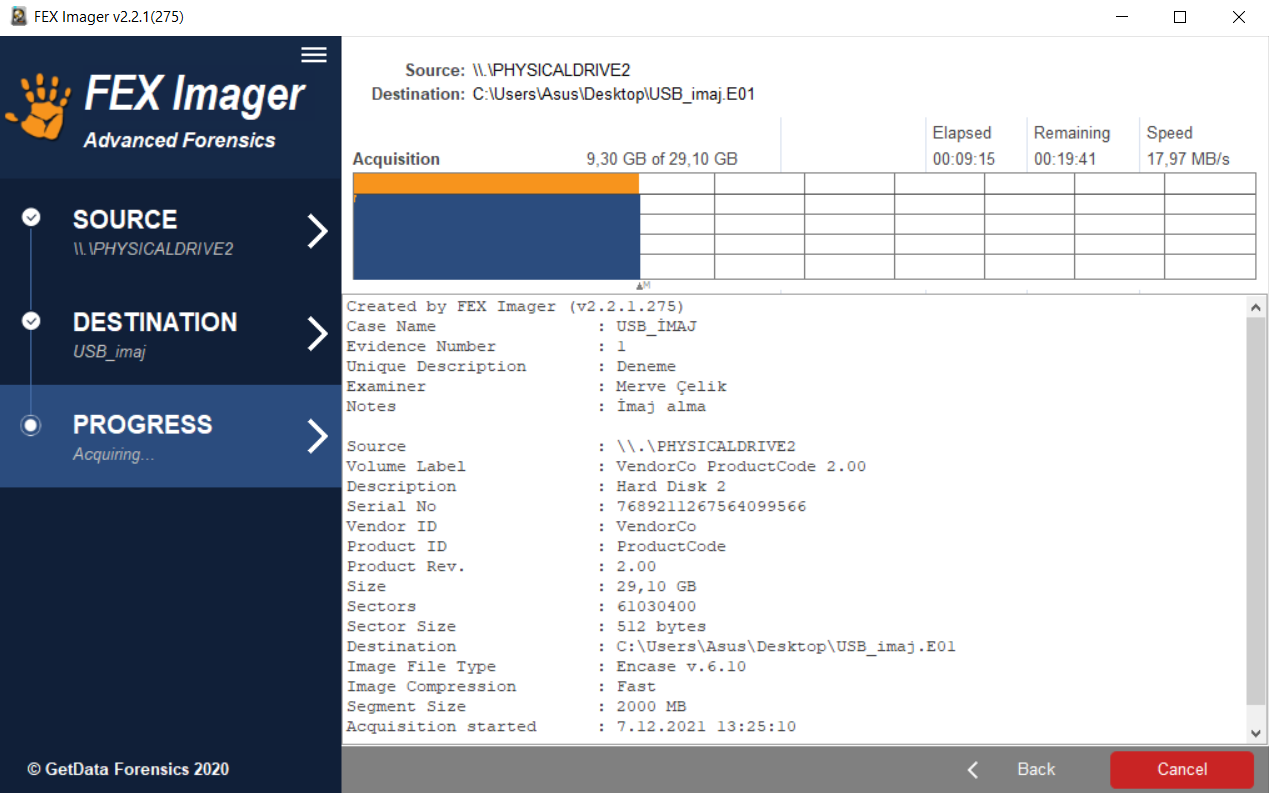
**Examiner:** İnceleme yapan kişinin ismi yazılır.

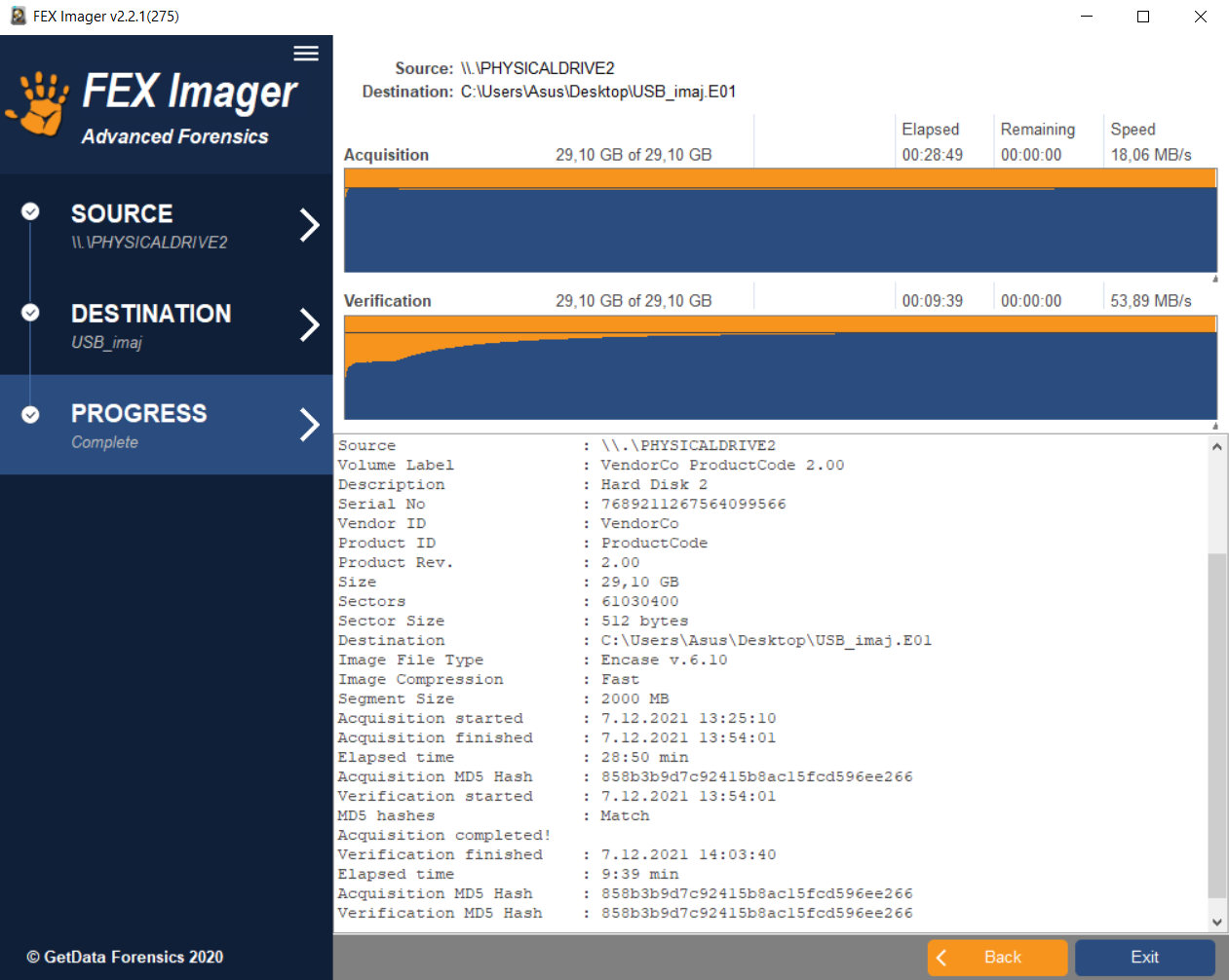
**Notes:** Vakayla ilgili bu vakayı kısa bir şekilde tanımlayacak,açıklayacak özel bilgiler yazılır.

**-** Ayarlar yapıldıktan sonra Start butonuna basılıp imaj alma işlemi başlatılır.

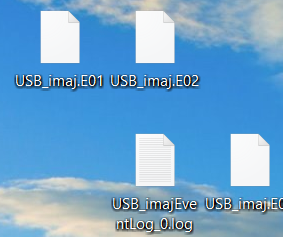


* İmaj işleminin başladığı görülür. İmaj hakkındaki bilgiler gözlemlenebilir.

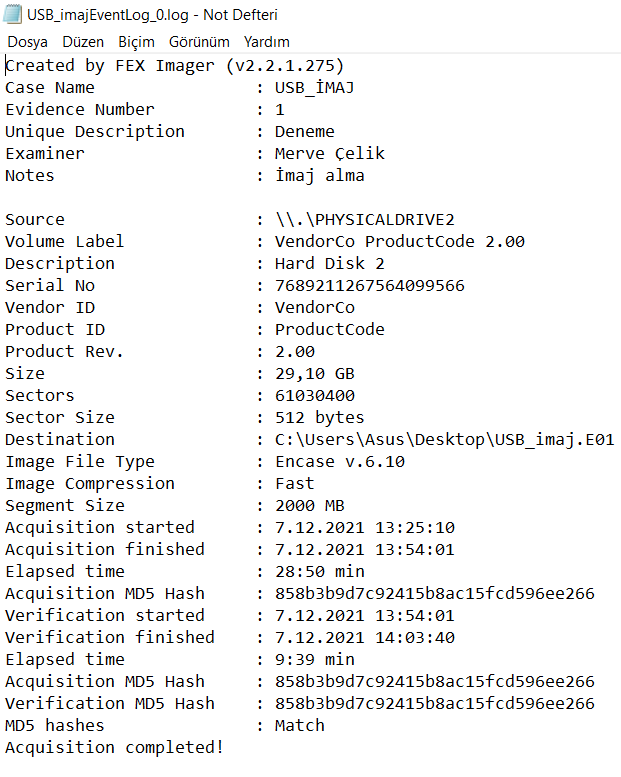




**-** İmaj işlemi bittikten sonra seçtiğimiz dosya yolunda imajlar görülür.

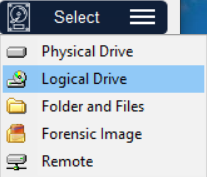


**-** Log dosyası içerisinde imaj hakkında bilgiler gözükür.

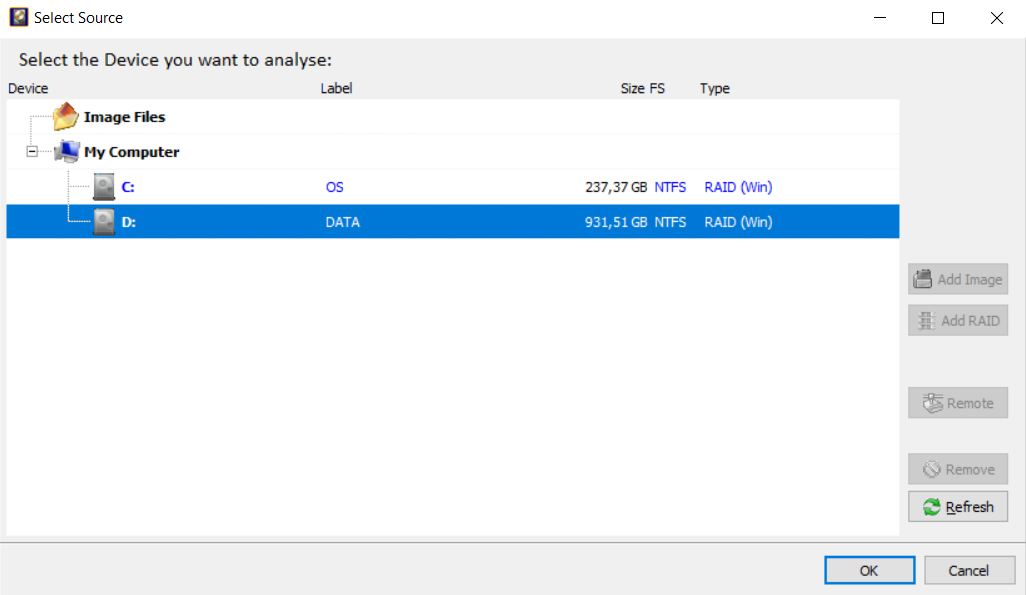


**7.FEX Imager İle Logical İmaj Alma**

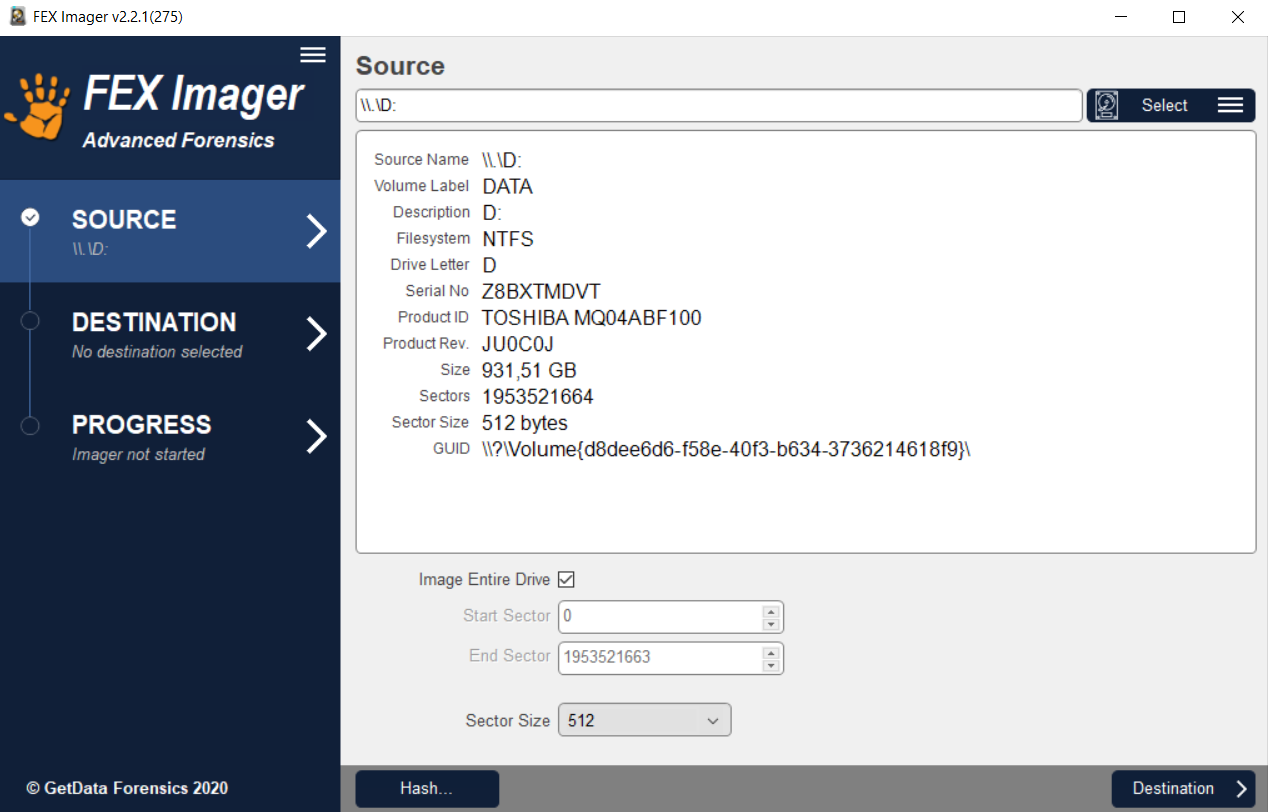
**-** Select bölümüne tıklandıktan sonra Logical Drive butonuna basılarak lokal imaj alma işlemi başlatılır.



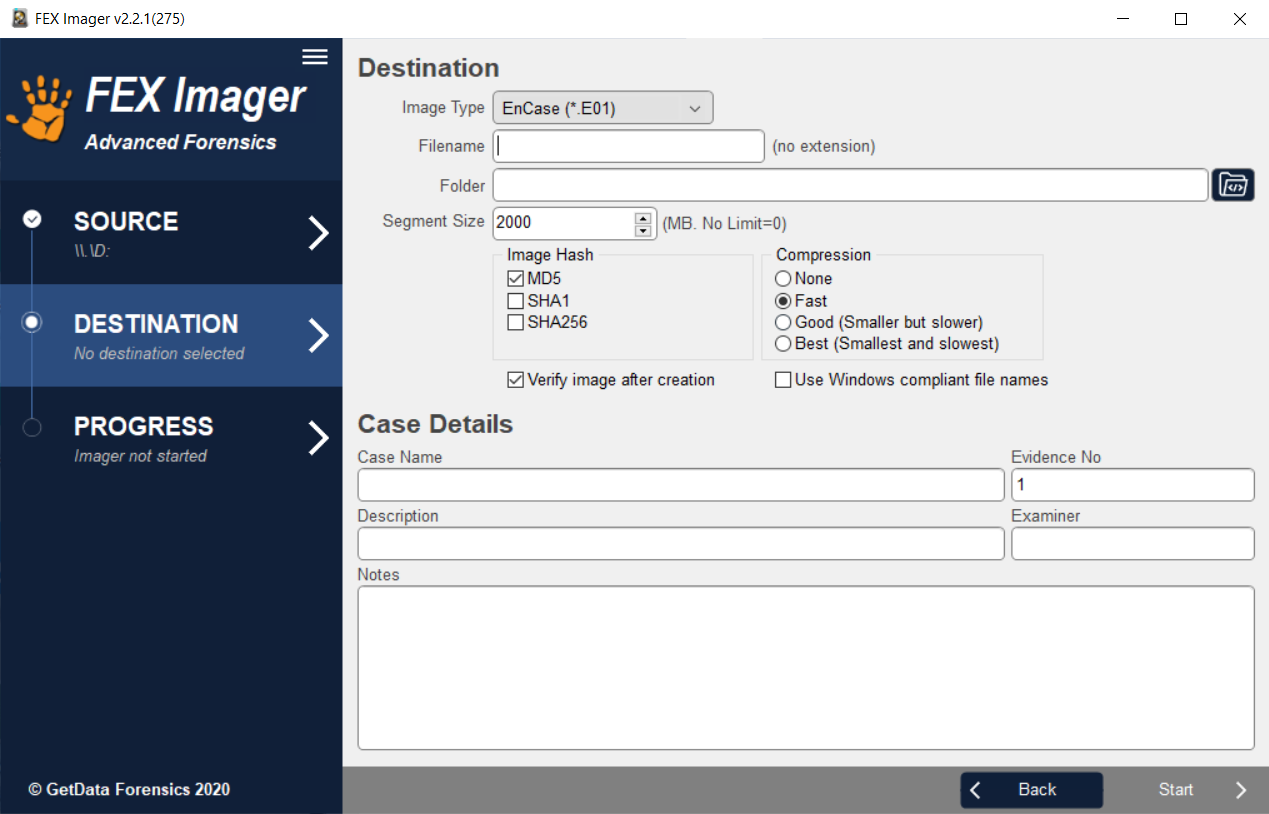
**-** İmajı alınacak bölüm seçilir sonra OK denir.

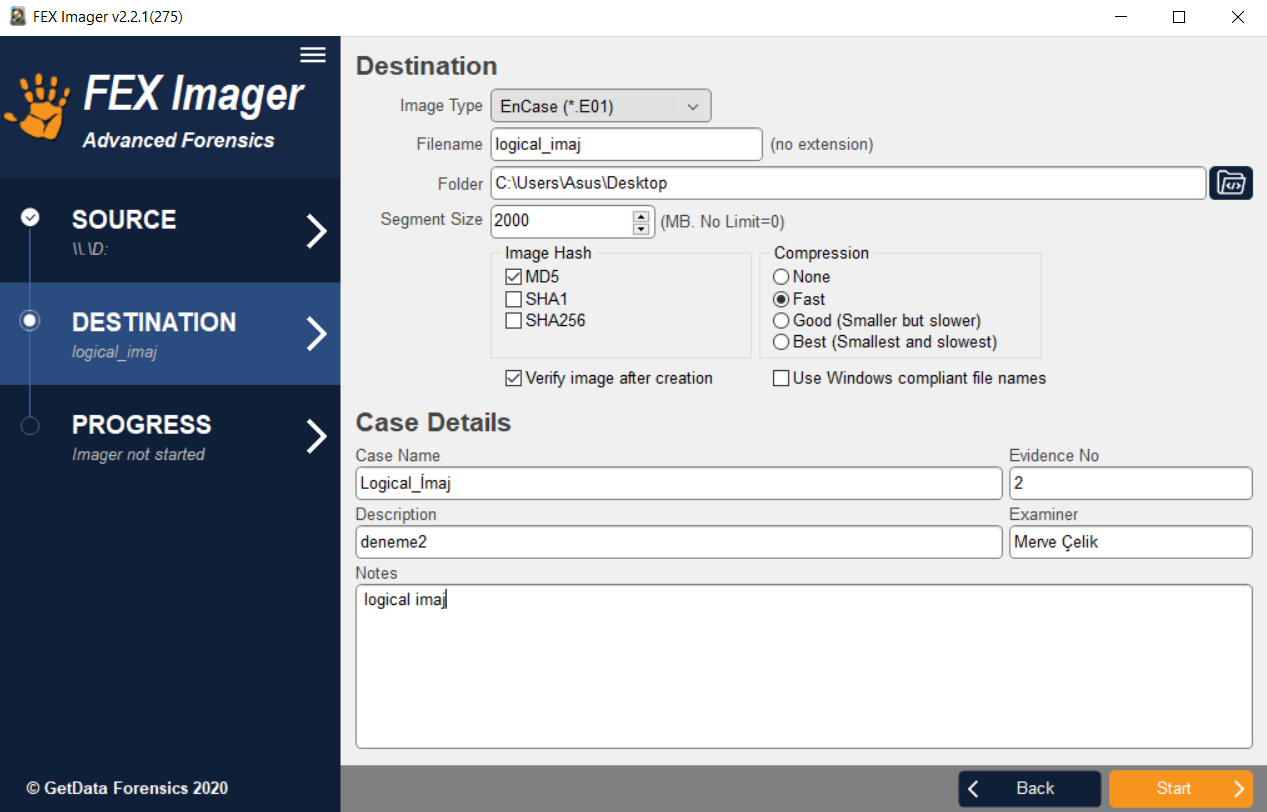


**-** OK denildikten sonra Source penceresinde seçilen bölüm hakkında bilgiler yer alır.

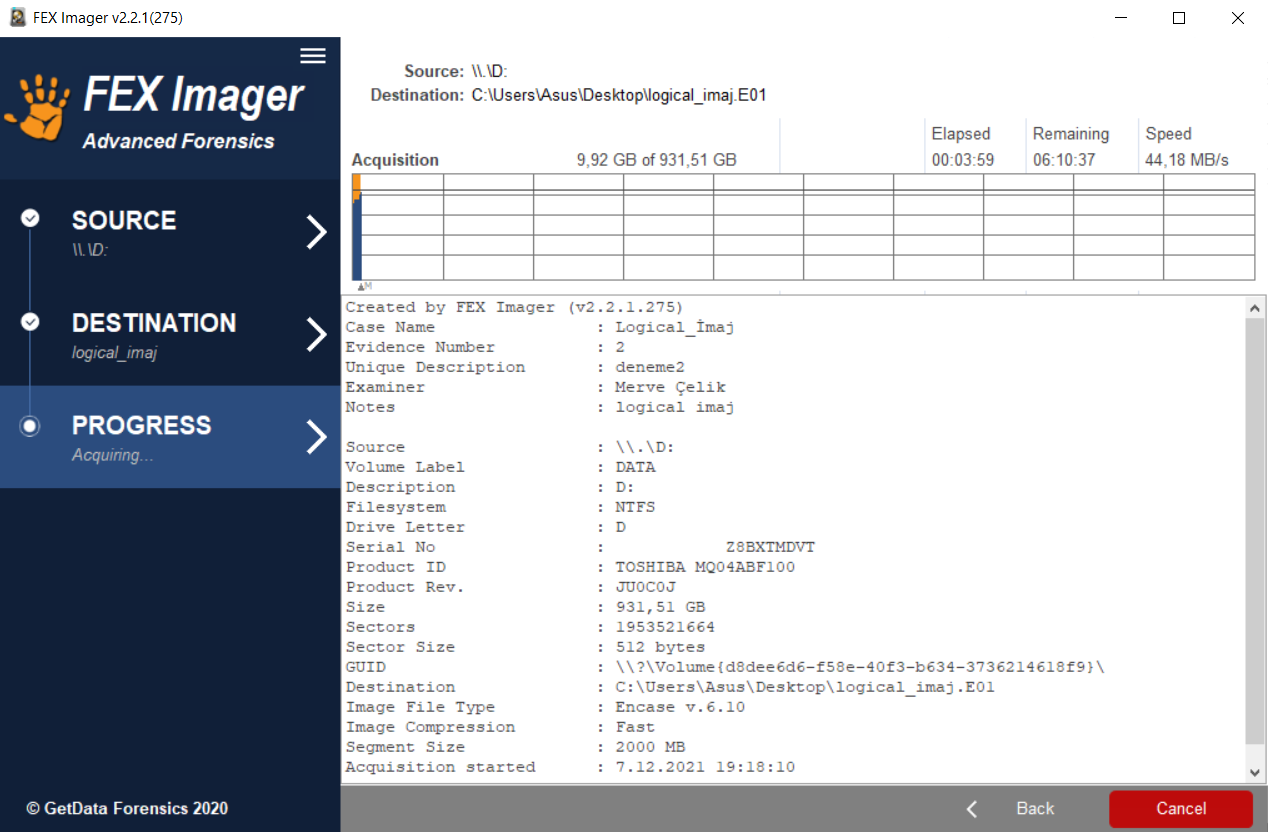


**-** Destination bölümünde imaj hakkında ayarlar yapılır. Start diyerek imaj alma işlemi başlatılır.

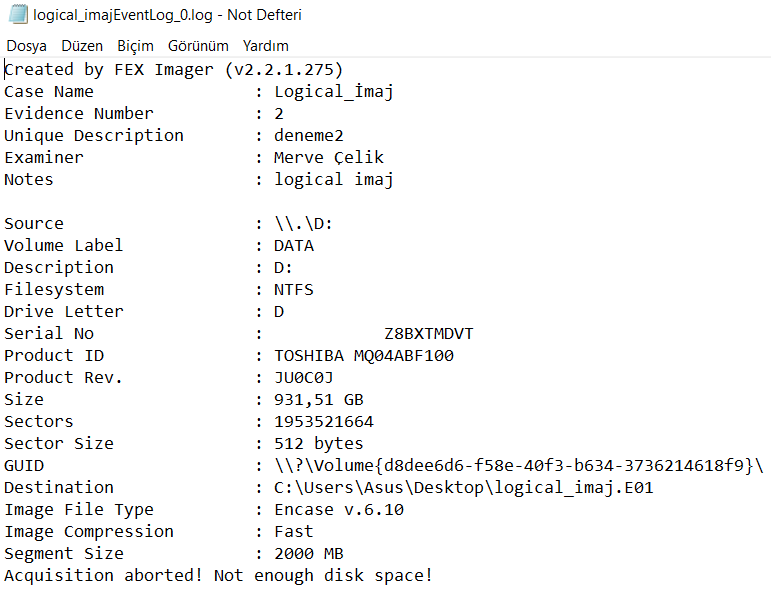




* İmaj işleminin başladığı görülür. İmaj hakkındaki bilgiler gözlemlenebilir.



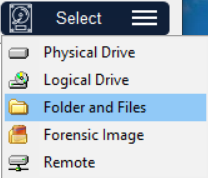
**-** İmaj işlemi bittikten sonra seçtiğimiz dosya yolunda imajlar görülür. Log dosyası içerisinde imaj hakkında bilgiler gözükür.



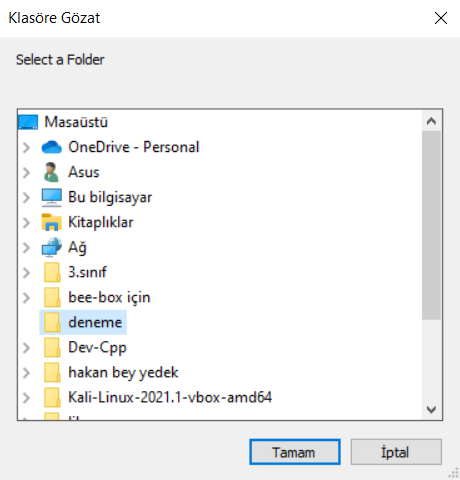
**8.FEX Imager İle Klasör İmajı Alma İşlemi**

Dosya ya da klasör imajı alma işlemi yapılır.

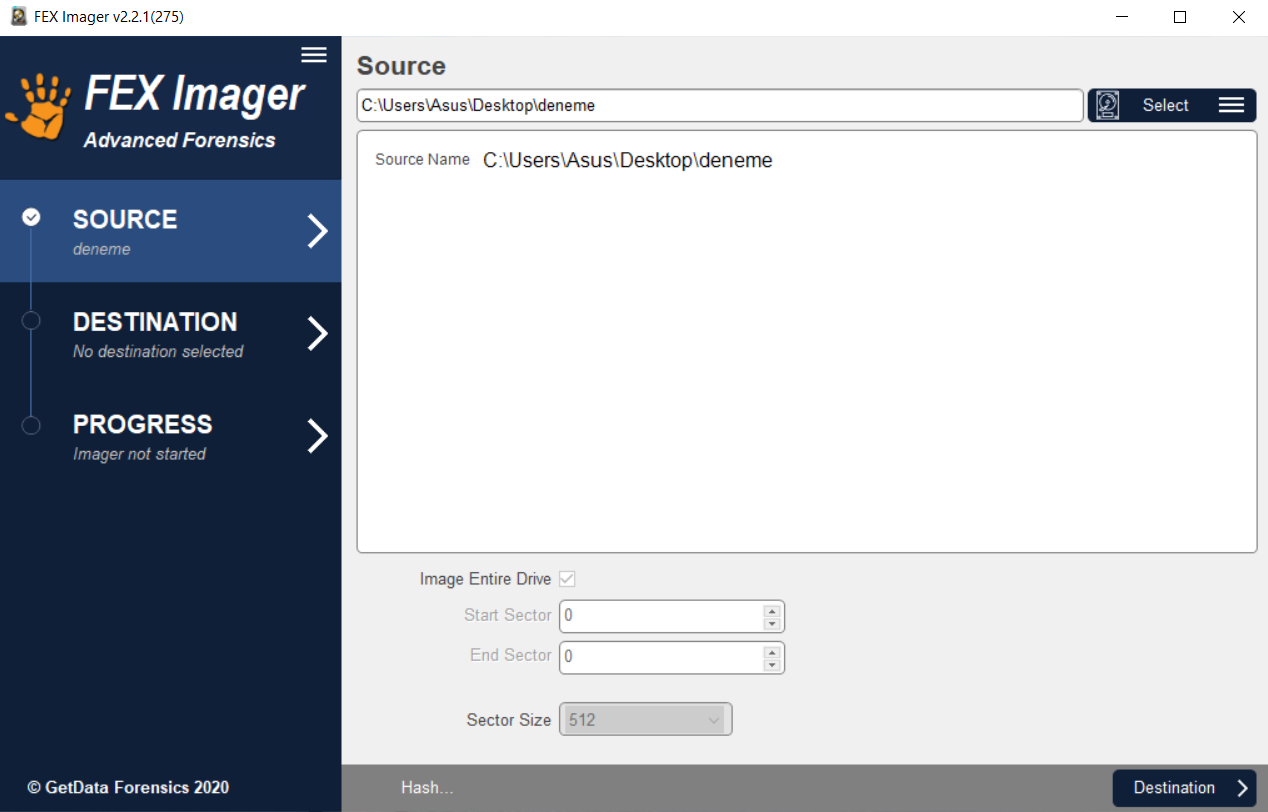
**-** Select bölümüne tıklandıktan sonra Folder and Files butonuna basılarak imaj alma işlemi başlatılır.



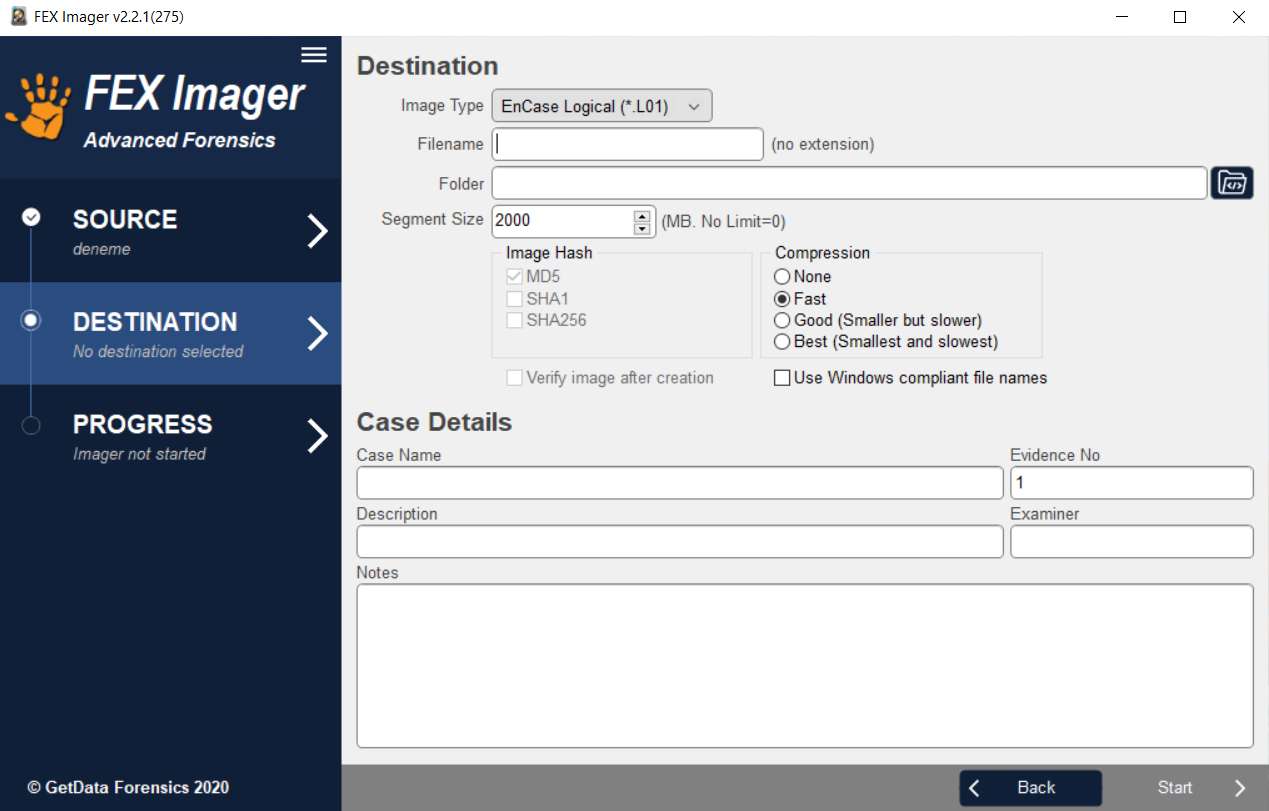
**-** Karşımıza çıkan pencerede imaj alacağımız dosyayı seçip devam ediyoruz.

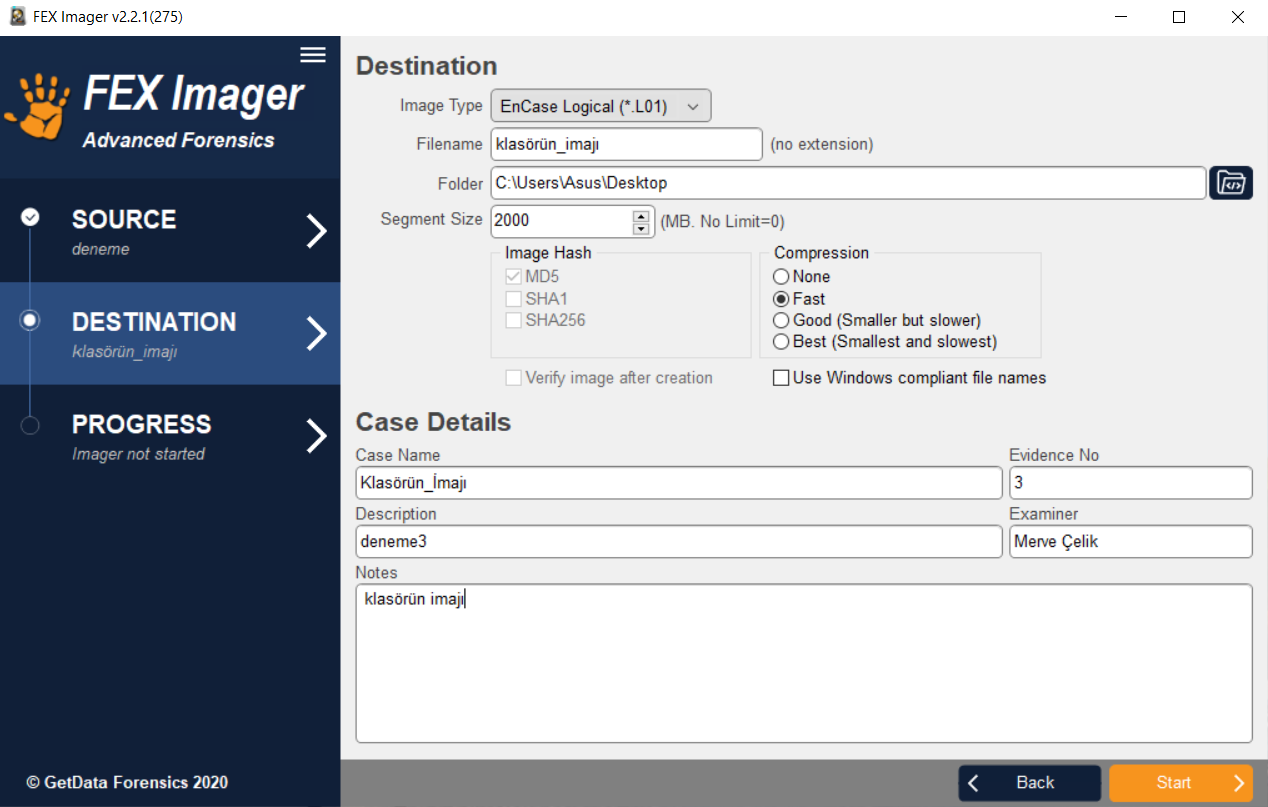


**-** Destination kısmına gidilir.

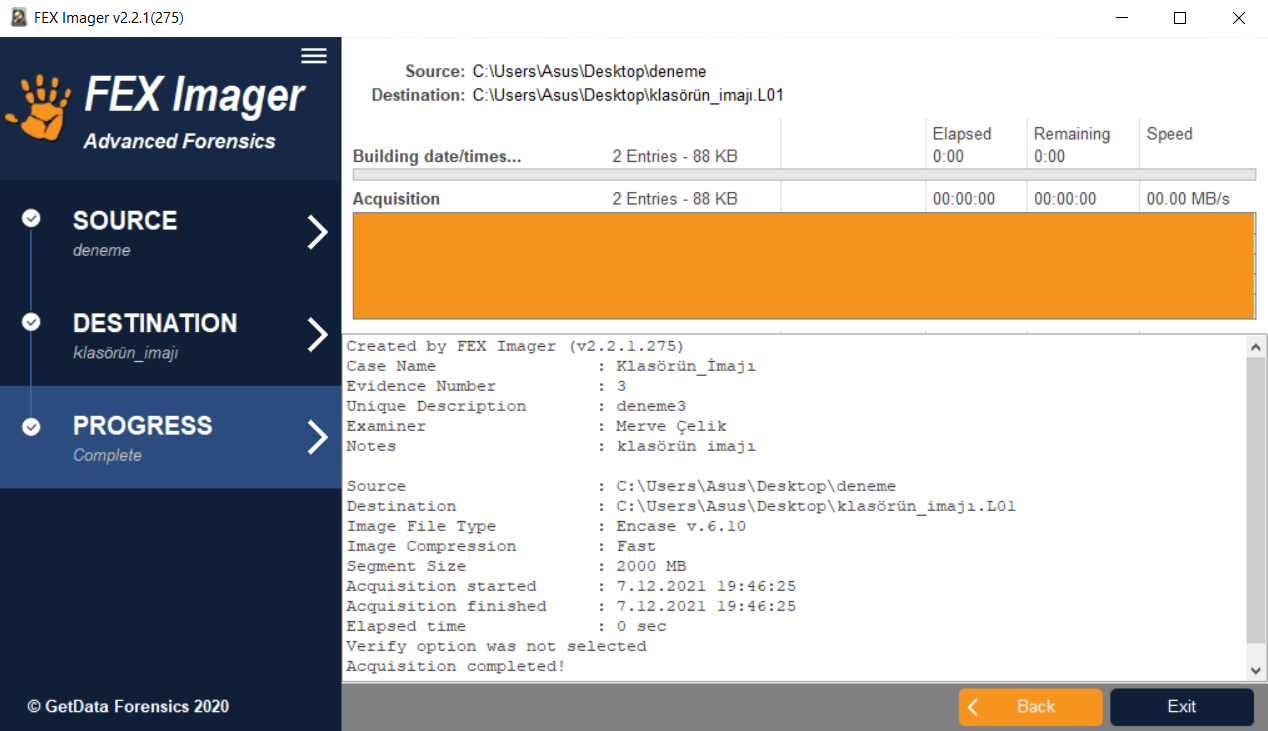


**-** Destination bölümünde imaj hakkında ayarlar yapılır. Start diyerek imaj alma işlemi başlatılır.

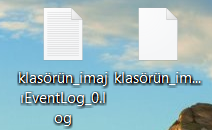




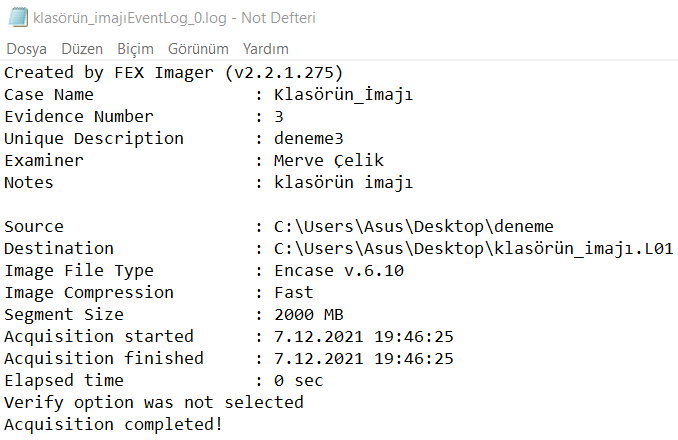
* İmaj işleminin başladığı görülür. İmaj hakkındaki bilgiler gözlemlenebilir.



**-** İmaj işlemi bittikten sonra seçtiğimiz dosya yolunda imajlar görülür.

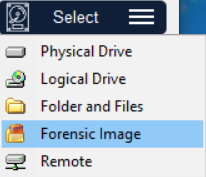


**-** Log dosyası içerisinde imaj hakkında bilgiler gözükür.

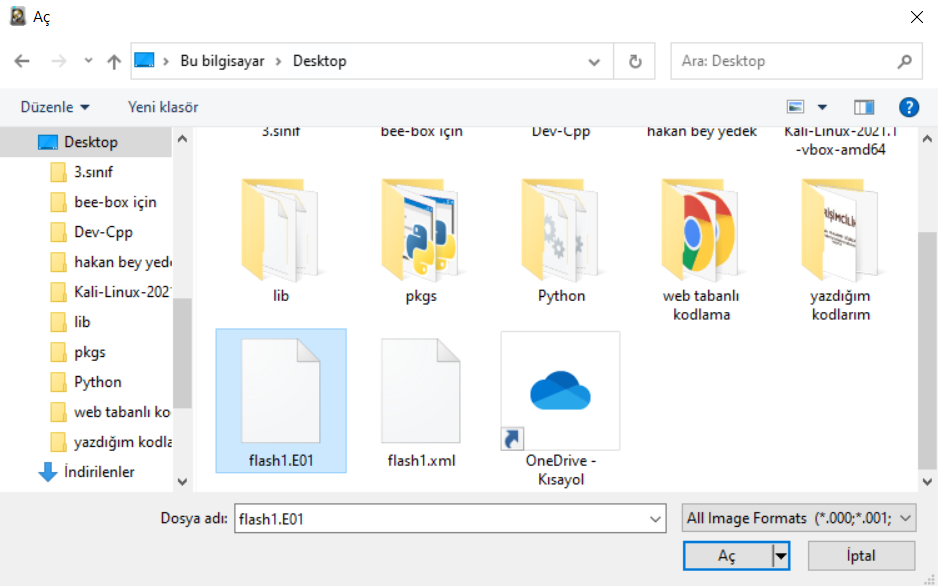


**9. FEX Imager İle İmajın İmajını Alma İşlemi**

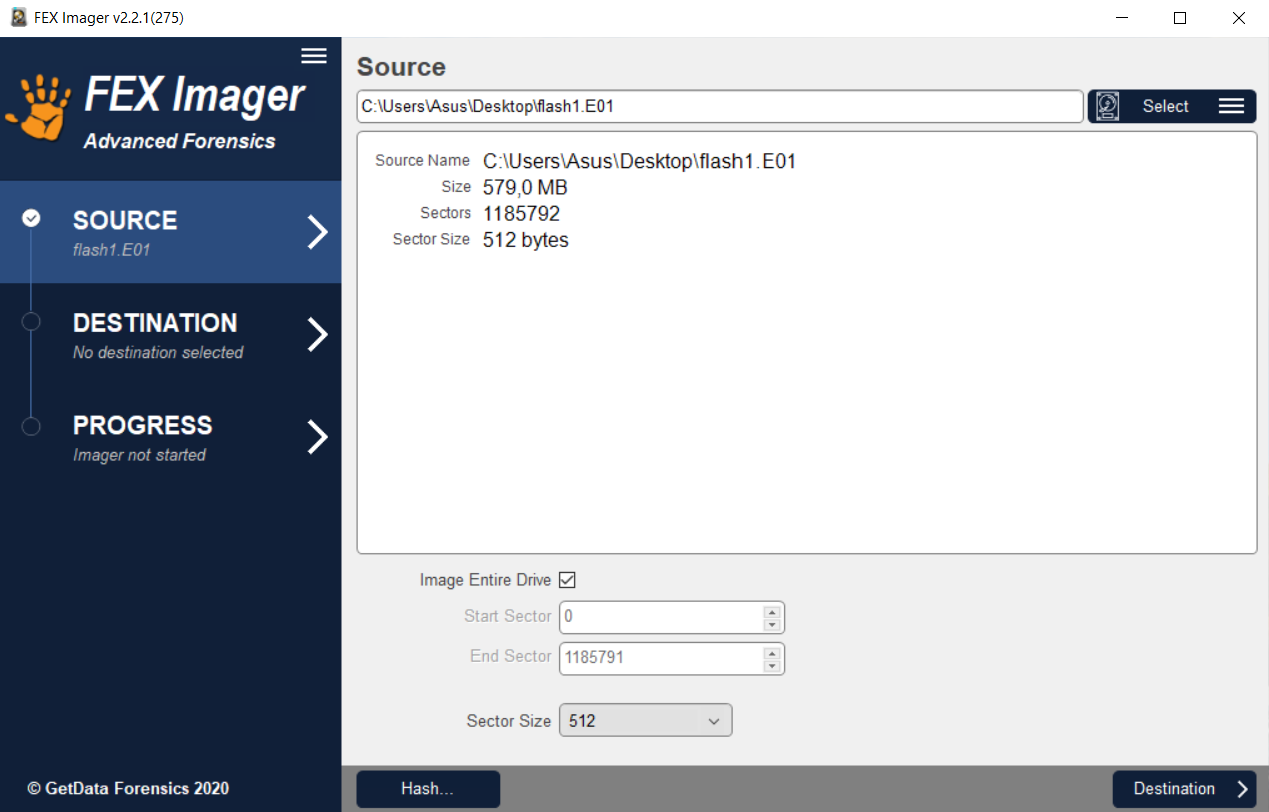
**-** Select bölümüne tıklandıktan sonra Forensic Image butonuna basılarak imajı alınmış bir dosyanın imaj alma işlemi gerçekleşir.

****

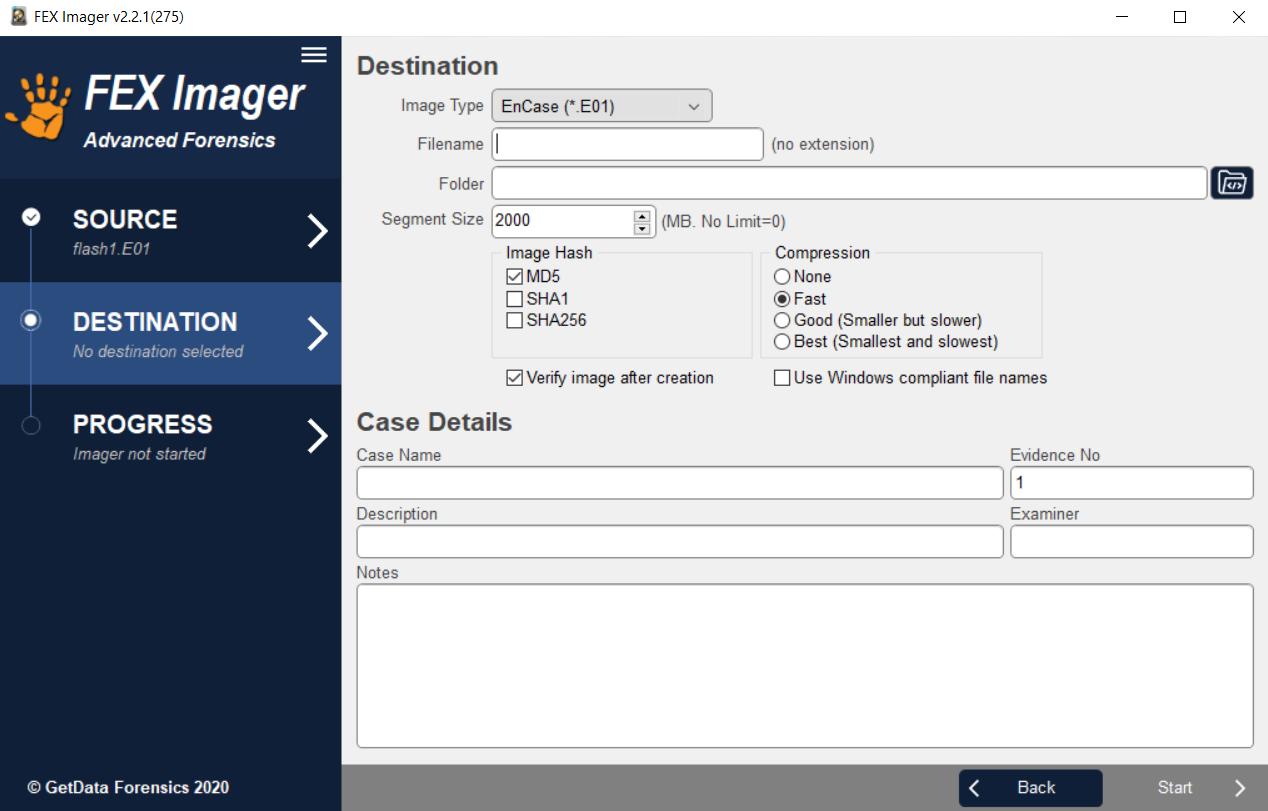
**-** Karşımıza çıkan pencerede imaj alacağımız dosyayı seçip devam ediyoruz.

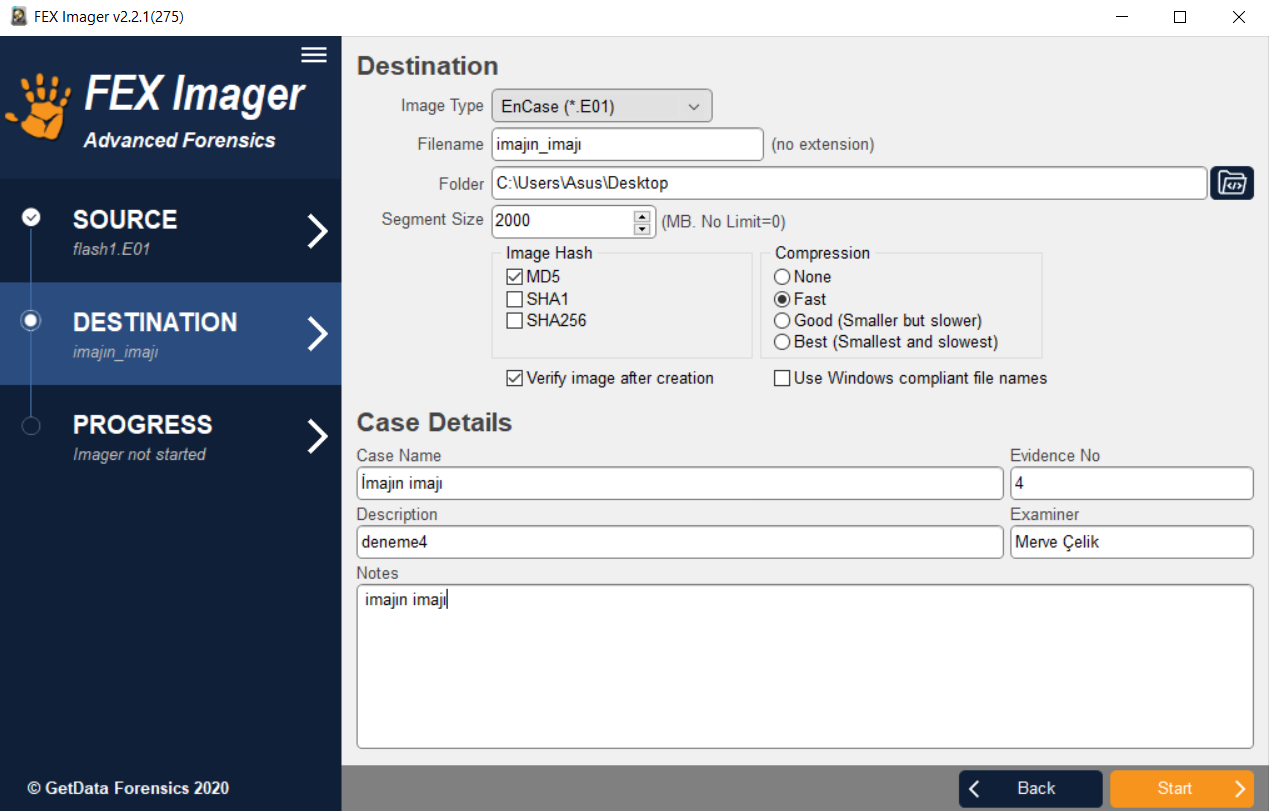


**-** Destination kısmına gidilir.

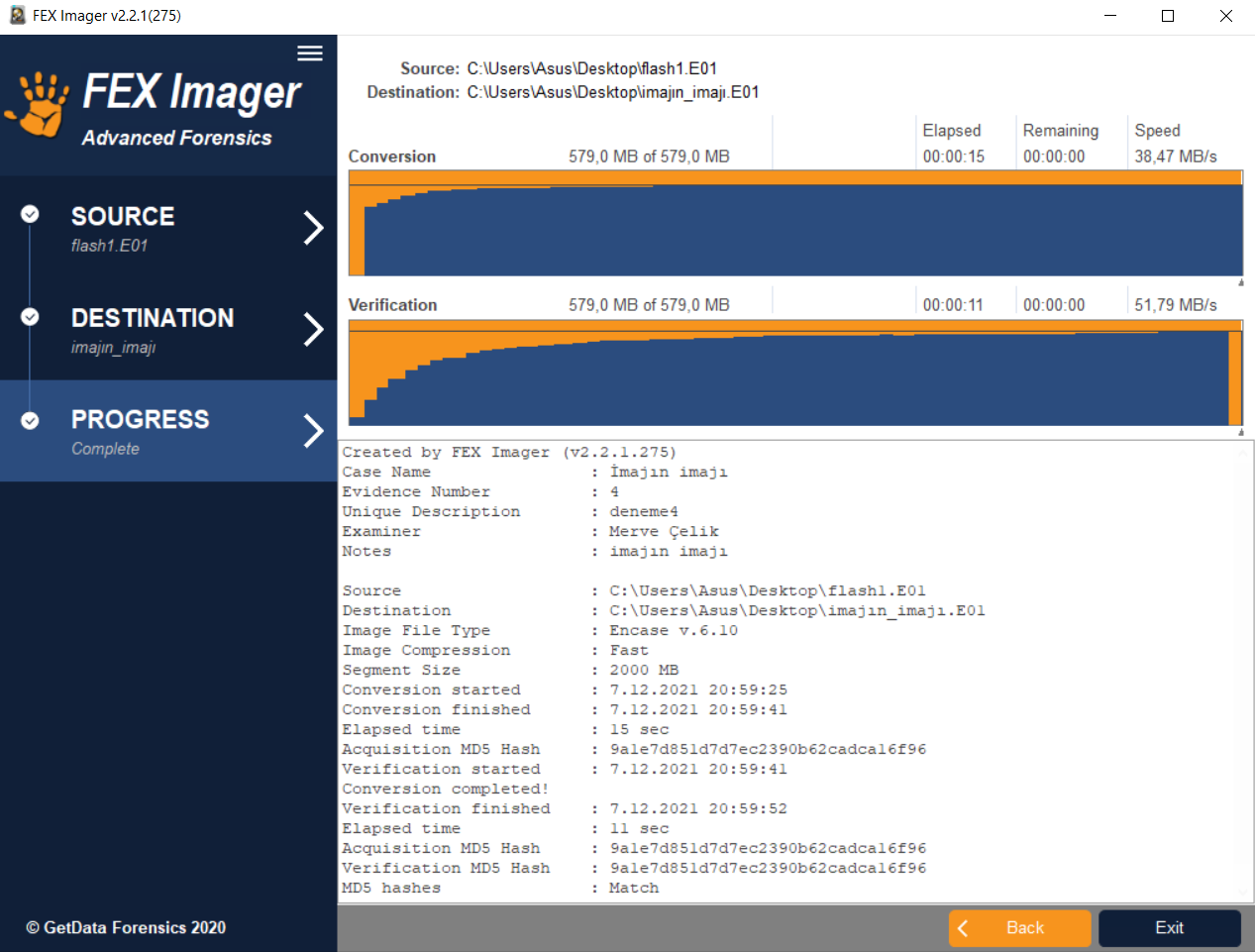
****

**-** Destination bölümünde imaj hakkında ayarlar yapılır. Start diyerek imaj alma işlemi başlatılır.

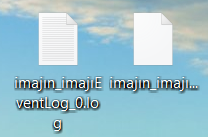
****

****

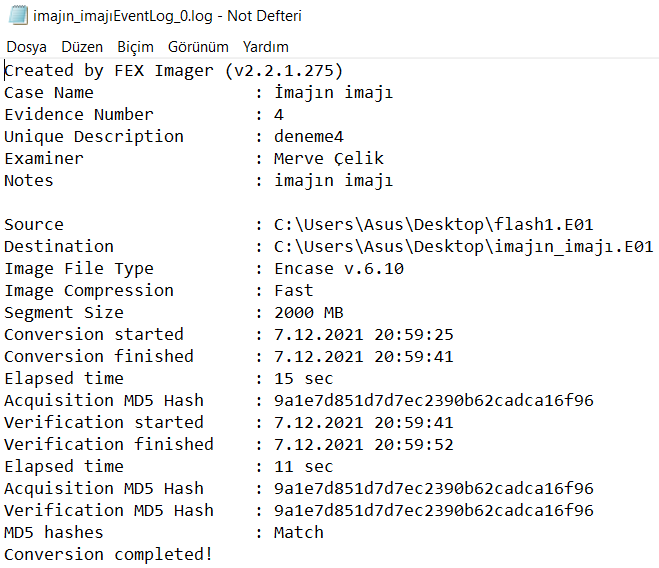
* İmaj işleminin başladığı görülür. İmaj hakkındaki bilgiler gözlemlenebilir.

****

**-** İmaj işlemi bittikten sonra seçtiğimiz dosya yolunda imajlar görülür.

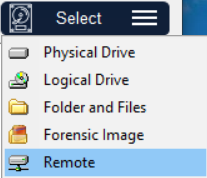
****

**-** Log dosyası içerisinde imaj hakkında bilgiler gözükür.



**10.FEX Imager İle Remote Bağlantı**

**-** Select bölümüne tıklandıktan sonra Remote butonuna basılarak uzaktan bağlantıyla imaj alma işlemi bu bölümde gerçekleştirilir.



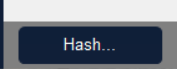
Fex imager, UDP protokolünü kullanarak aynı ağ üzerindeki cihaza uzaktan erişmemize olanak sağlar. Bu işlemi gerçekleştirmemiz için öncelikle GetDataNetworkServer.exe’yi çalıştırarak IP adresimizi görüntülemeliyiz ve dağıtma işlemini gerçekleştirmeliyiz. GetDataNetworkServer.exe dosyası FEX imager yükleme klasöründe bulunur. Bu seçenek aktifleştirildikten sonra uzaktan bağlantı yapılacak cihazın IP adresi girilir, port ve paket ayarları yapıldıktan sonra paket yakalama işlemi başlar.

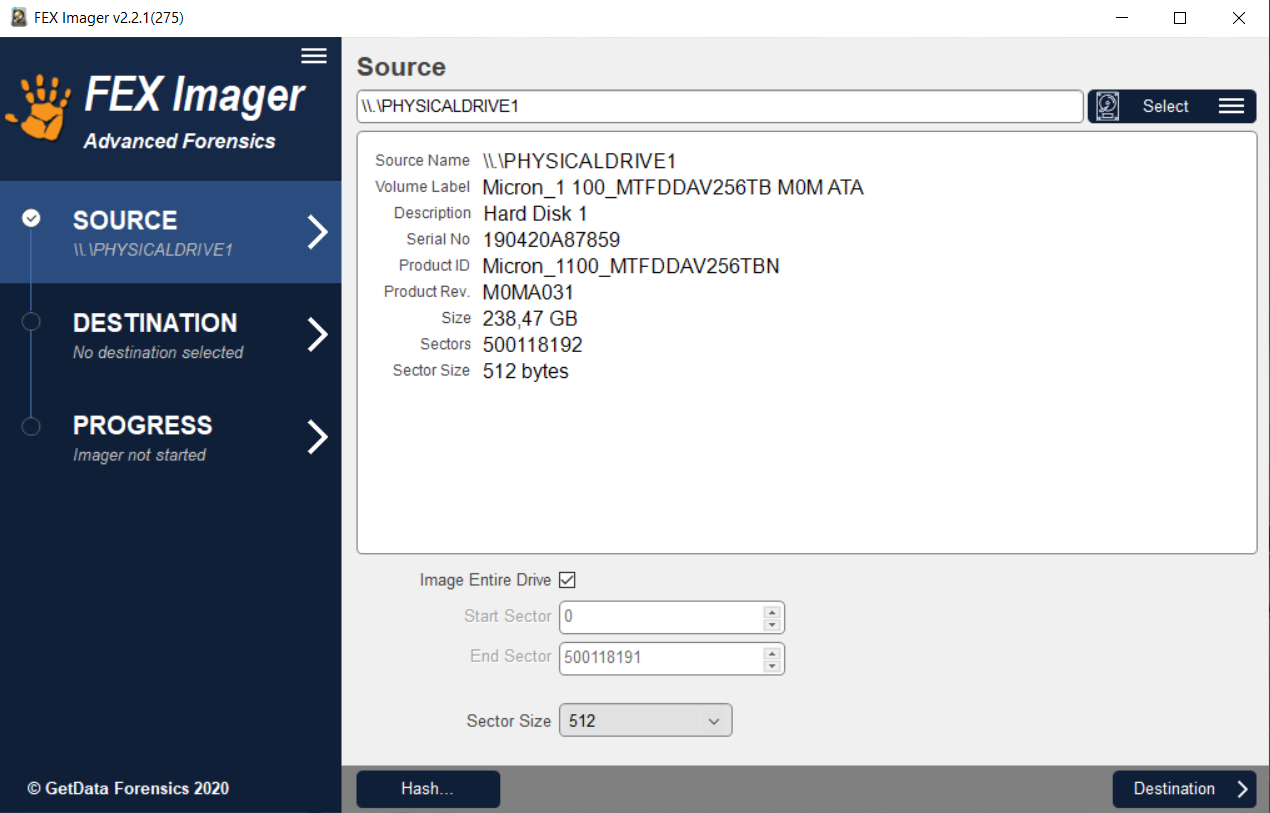
**11.Fex Imager İle Sadece Hash Hesaplatma**

FEX imager dosyaların, klasörlerin, disklerin ve imaj aldığımız her türde sadece hash hesaplatması yapmamıza olanak sağlar.

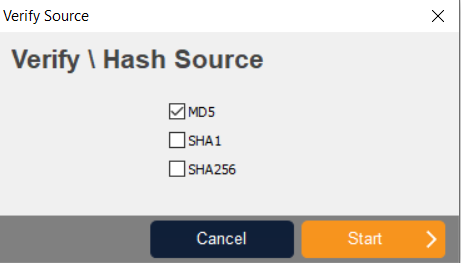
Bu özellik adli incelemelerde oldukça önemlidir.

**-** Hashini almak istediğimiz imajı seçip sol alt köşedeki Hash kısmına tıklanır.





**-** Hangi hash formatlarıyla hash alınması isteniyorsa seçilir.



**-** Hash alma işleminin başladığı görülür.

