AccessData

FTK IMAGER

KULLANIM KILAVUZU

**İÇİNDEKİLER**

1.Giriş

2.FTK IMAGER NEDİR

3.FTK Imager Kurulumu

4.Yazılım Bölümleri

5.FTK Imager Kullanıcı Arayüz Sekmeleri

6.FTK Imager İle İmaj Alma

7.FTK Imager ile RAM imajı alma

8.FTK Imager ile Mount işlemi

9.FTK Imager yazılımı ile imaj inceleme süreci

1.Giriş

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

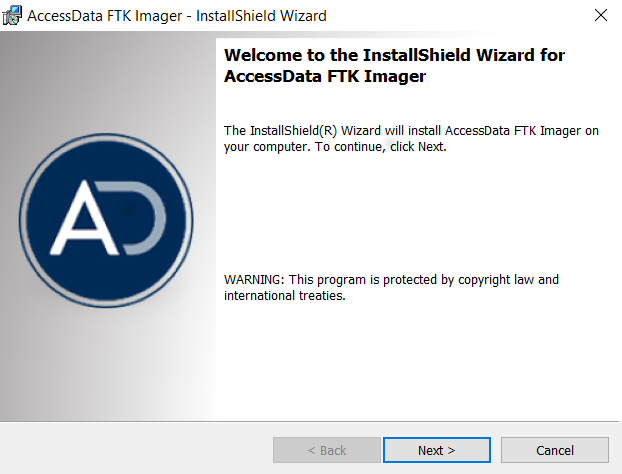
2.FTK IMAGER NEDİR

FTK Imager sabit disk, CD, DVD, klasor veya dosya imajı alabileceğimiz ve aldığımız imajı ön izleyebileceğimiz ücretsiz bir yazılımdır. FTK Imager ile dd, e01, ve AFF biçimlerinde imaj alınabilir, alınan imaja sonradan erişilebilir ve imaj dosyası disk sürücüsü gibi gösterilebilir.Ayrıca alınan bir imaj dosyasıda bu ücretsiz yazılım ile incelenebilir. Windows, Linux ve Mac'le uyumlu olan FTK Imager FAT, NTFS, ext2, ext3 gibi dosya formatlarını destekler.

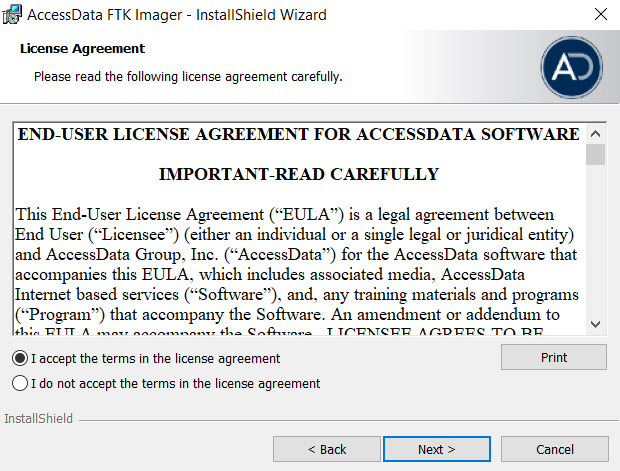
3.FTK Imager Kurulumu

FTK Imager yazılımını AccesData’nın web sitesi üzerinden ücretsiz olarak indirebilirsiniz.

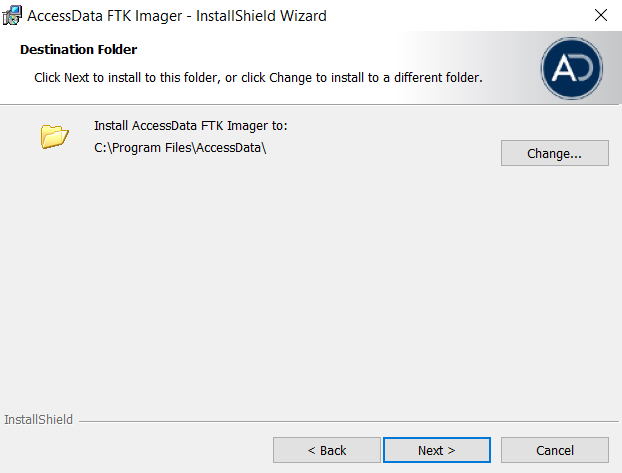
<http://accessdata.com/product-download>



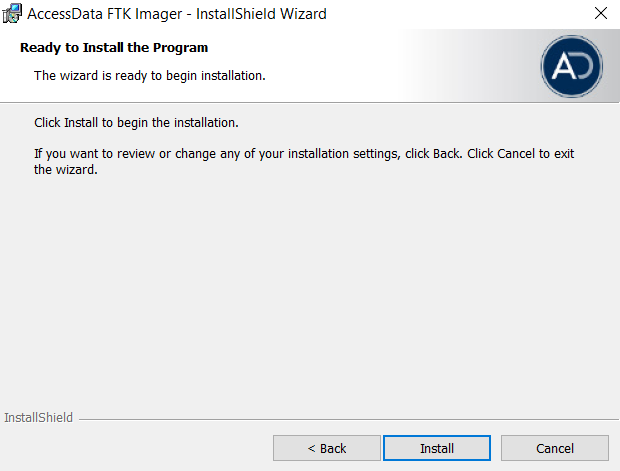
* Açılan pencerede Next butonuna tıklayın.



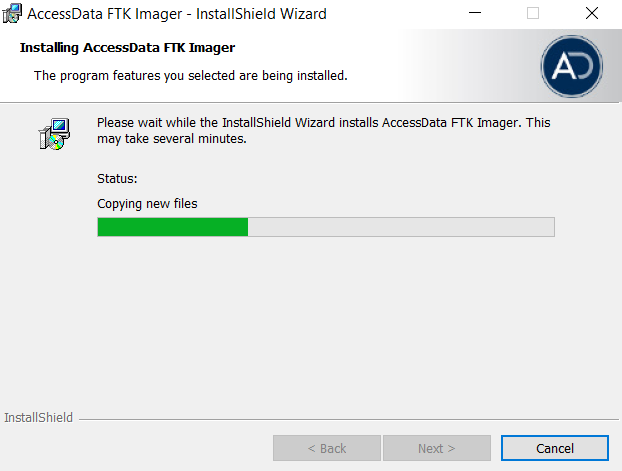
* Kurulumun devam etmesi için sözleşmeyi kabul edin ve Next butonuna tıklayın.



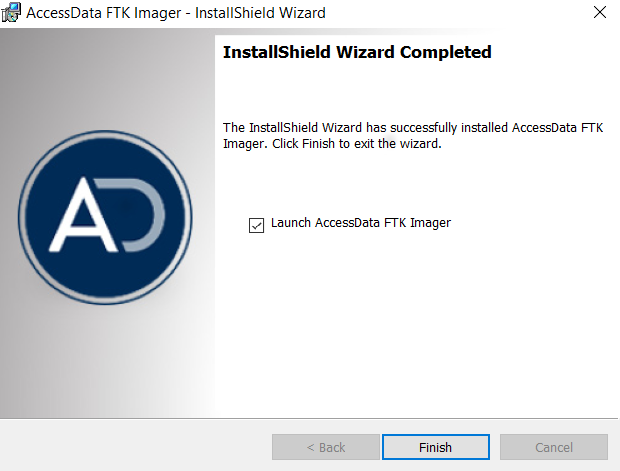
* FTK Imager programının kurulacağı dosya yolunu seçip ve Next butonuna tıklayın.



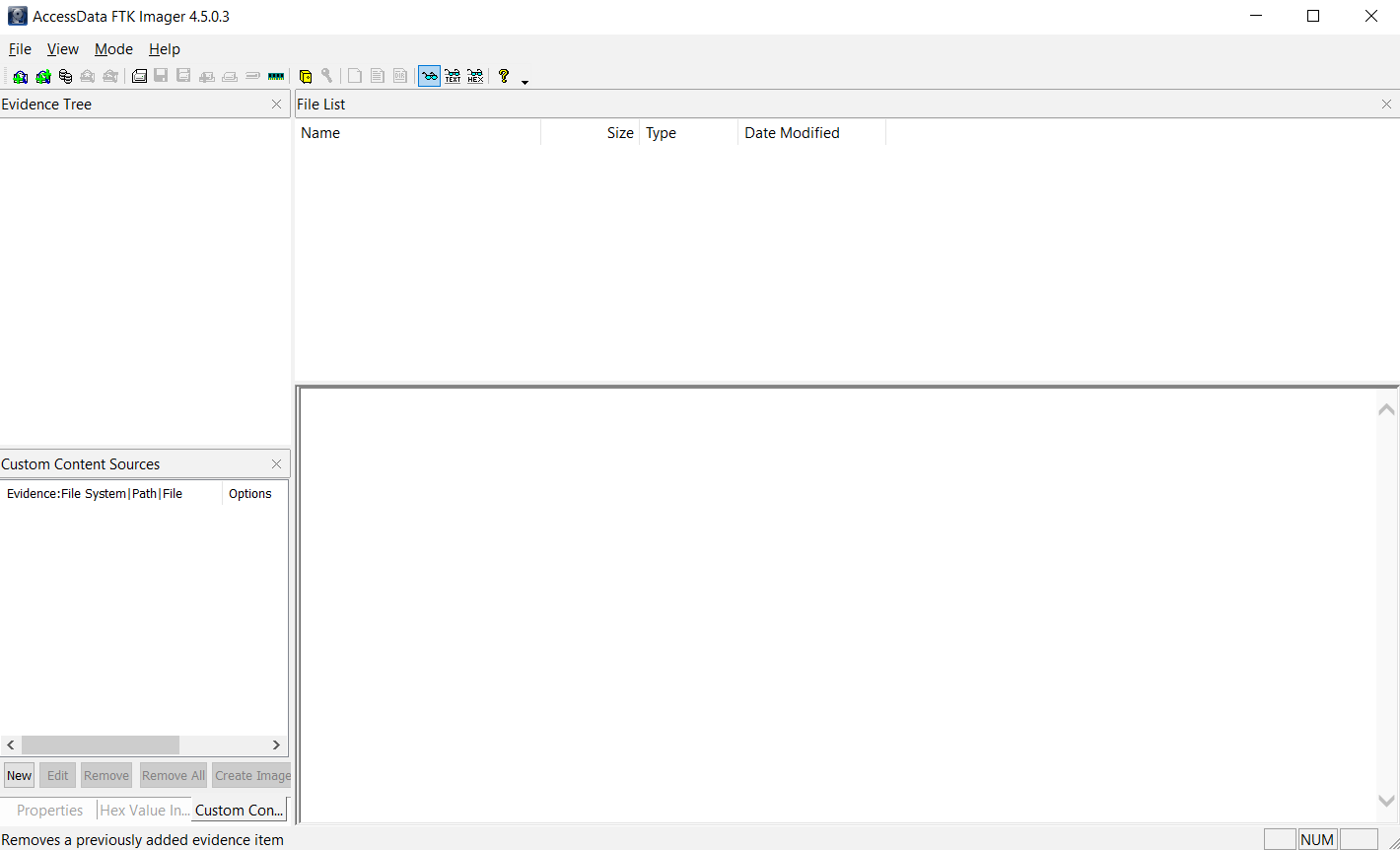
* Install butonuna tıklayıp kurulumu başlatın .



* Kurulumun başladığını ve devam ettiğini görüyoruz.



* Kurulum bittikten sonra masaüstünde kısayolun oluşması için işaretleyin. Finish butonuna basın.

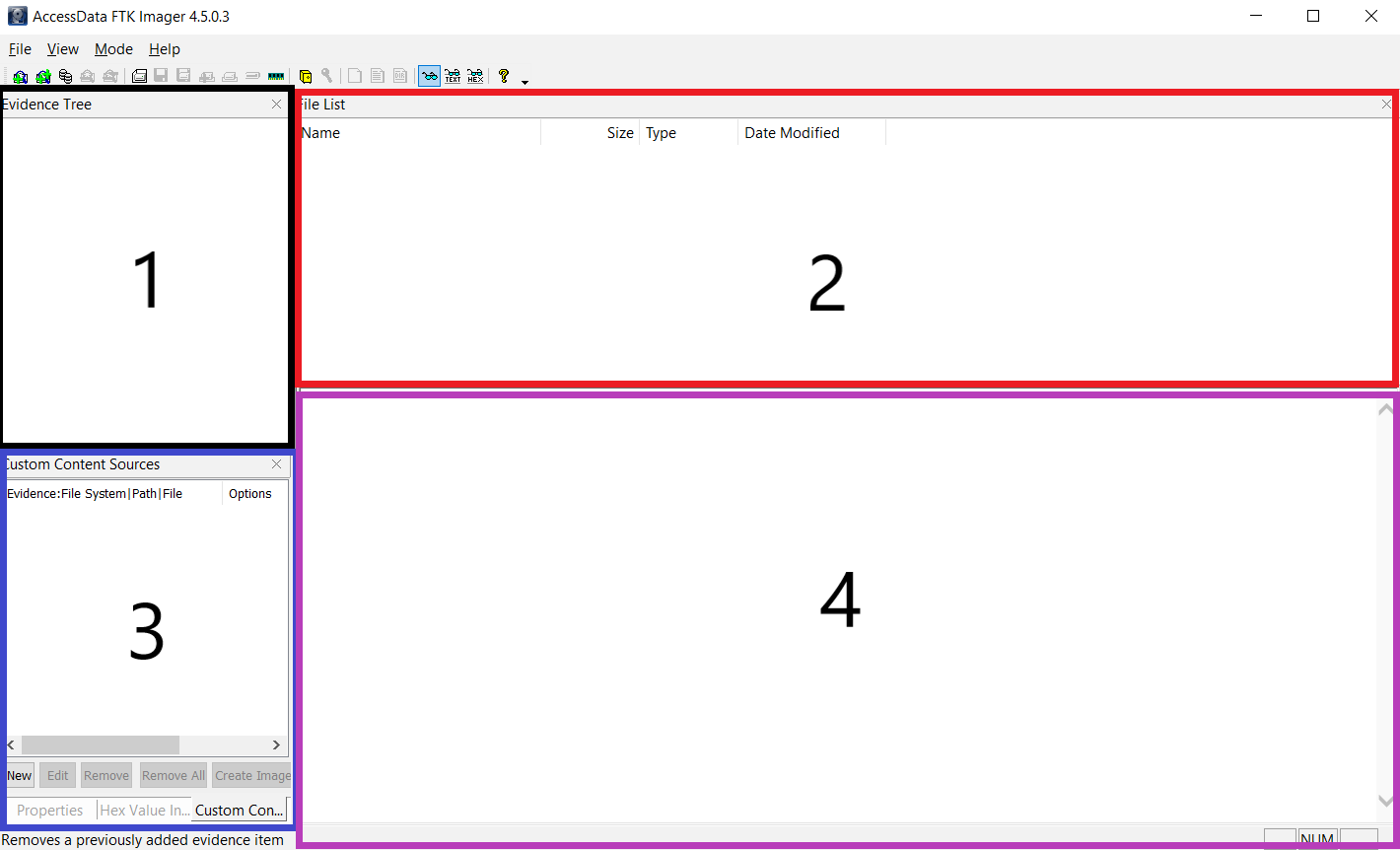


Masaüstünde kısayolu oluşan FTK Imager’a tıklayıp çalıştırabilirsiniz.

4.Yazılım Bölümleri

Imager yazılımı dört bölümden oluşur.Bunlar;

* Evidence Tree
* File List
* Hex Value Interpreter
* Costum Content Sources’dir.



Evidence Tree (1) : Bu bölümde eklenen imajın dizin ağaç yapısını görmekteyiz.

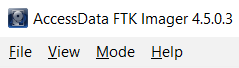
File List (2) : Bu bölümde seçilen dizin içerisinde yer alan dosyaları görmekteyiz.

Costum Content Sources (3) : Özel içerik alanlarını gösterir.Aynı zamanda seçilen alanda imaj alma, düzenleme gibi işlemlerini gerçekleştirebiliriz.

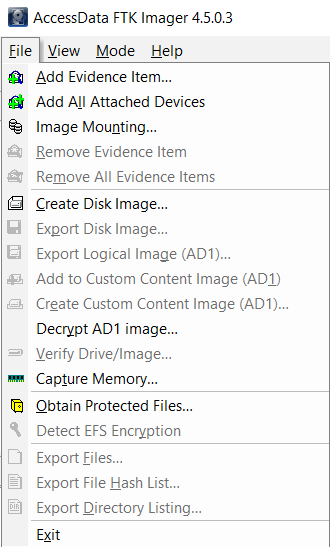
Hex Value (4): Seçilen dosya veya klasörlerin hexadecimal karşılıklarını gösterir.

5.FTK Imager Kullanıcı Arayüz Sekmeleri

Menüler sağ üst köşede bulunur.Aşağıdaki gibi görünür ;



**File:** Dosya menüsü araç çubuğunda kullanabileceğimiz tüm özelliklere erişimemizi sağlar.



**Add Evidence Item =** Tek delil ekleme işlemini yapar.

**Add All Attached Devices =** Bağlı olan tüm cihazların eklenmesi işlemini yapar.

**Image Mounting =** İmaj mount etme işlemini yapar.

**Remove Evidence Item =** Tek delil silme işlemini yapar.

**Remove All Evidence Items =** Tüm delillerin silinmesi işlemini yapar.

**Create Disk Image =** Disk imajı oluşturma işlemini yapar.

**Export Disk Image =** Disk imajını dışa aktarma işlemini yapar.

**Export Logical Image =** Lokal bir imajı dışa aktarma işlemini yapar.

**Add to Custom Content Image =** Özel imaj içeriği ekle işlemini yapar.

**Create Custom Content Image =** Özel imaj içeriği oluştur işlemini yapar.

**Decrypt AD1 image =** Lokal imajın şifresini çöz işlemini yapar.

**Verify Drive/Image =** Disk veya imaj doğrula işlemini yapar.

**Capture Memory =** Ram imajı yakala işlemini yapar.

**Obtain Protected Files =** Korunan dosyaları elde et işlemini yapar.

**Detect EFS Encryption =** EFS çözümlemeyi algılama işlemini yapar.

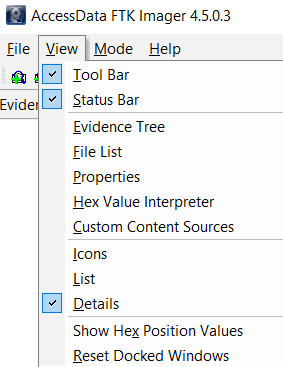
**Export Files =** Dosyayı dışa aktar işlemini yapar .

**Export File Hash List =** Hash listelerini dışa aktarma işlemini yapar.

**Export Directory Listing =** Klasör listelerini dışa aktarma işlemini yapar.

**Exit =** Çıkış işlemini yapar.

**View:** FTK Imager bölümlerinin görünümünü özelleştirme işlemini yapan seçenektir.



**Tool Bar =** Araç çubuğu

**Status Bar =** Durum çubuğu

**Evidence Tree =** Olay ağacı

**File List =** Dosya listesi

**Properties =** Seçenekler

**Hex Value Interpreter =** Hex değer yorumlayıcı

**Custom Content Sources =** Özel içerik kaynakları

**Icons =** İkon

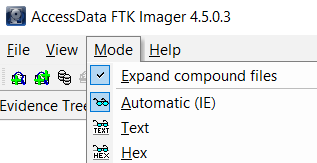
**List =** Liste

**Details =** Detaylar

**Show Hex Position Values =** Hex pozisyon değerini göster

**Reset Docked Windows =** Yerleşik Windowsu sıfırla

**Mode:** Mod menüsü görüntüleyici önizleme modunu seçmenizi sağlar.

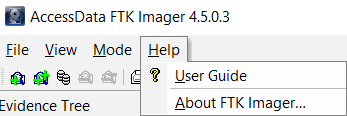


**Automatic =** Bileşik dosyayı genişlet

**Text =** İmaj hakkında text dosyası tutma işlemini yapar.

**Hex =** Hexadecimal rapor oluşturma işlemini yapar.

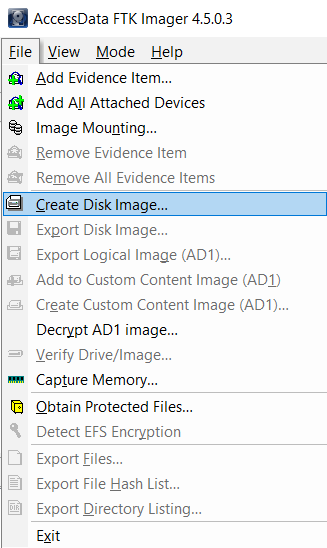
**Help:**FTK imager kullanımı hakkında bilgi alabileceğimiz alandır.



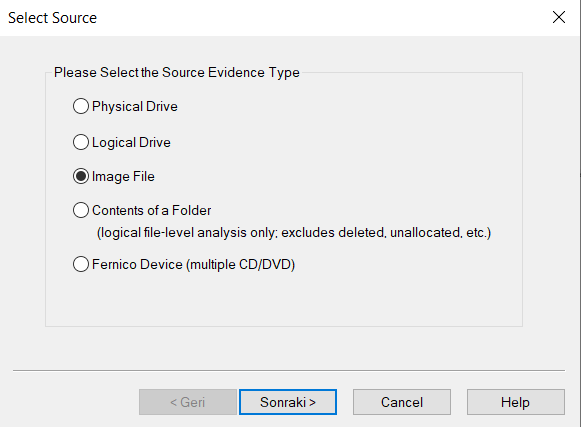
6.FTK Imager İle İmaj Alma

Aşağıdaki adımları takip ederek imaj işlemini gerçekleştirebiliriz.

**1:** File menüsünden Create Disk İmage seçeneğini aktif ederek imaj alma işleminin ilk adımını gerçekleştiririz.



**2:**Açılan pencereden alacağımız imaj türünü seçerek işleme devam ederiz.



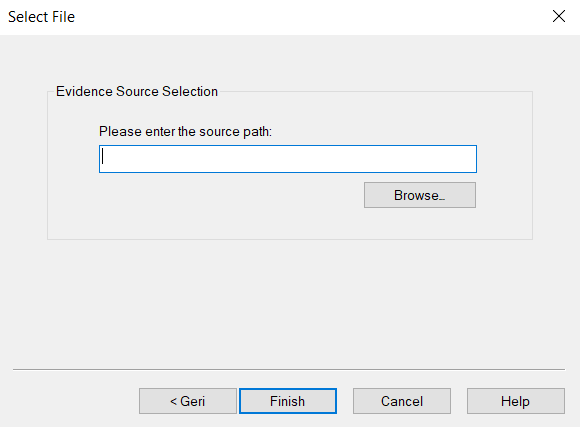
**Pyscial Drive:** Seçilen diski olduğu gibi imajını alıp aktarır.

**Logicial Drive:** Diskin belirli bir bölümünün imajını alır.(Örn:C,D,E sürüleri gibi)

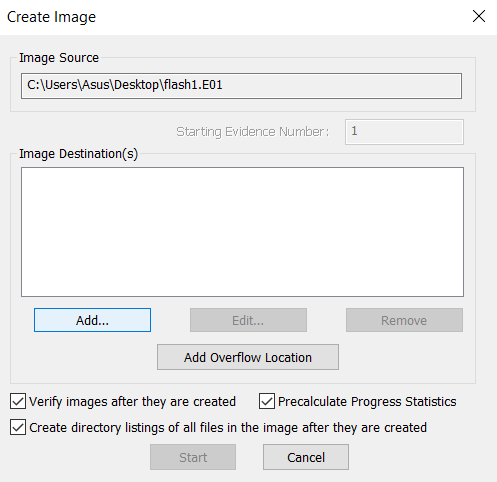
**Image File:** Bir imaj dosyasının imajını alır.

**Content of Folder:** Silinen,tanımlanmamış vs bölümlerin imajını alır.

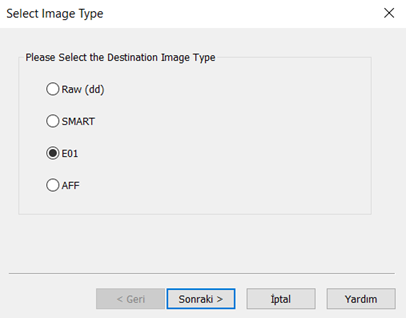
**Fernico Device:** Çoğaltılabilir CD , DVD tarzı disklerin imajını alır.



**3 :** Image dosyasının kaydolacağı yeri Browse diyerek seçiyorum ve işlemlerime devam ediyorum.



**4:** Karşımıza imaj sıkıştırma formatını seçmemiz için bir pencere çıkmakta bu pencereden add butonuna tıklayıp imaj formatımızı seçiyoruz.



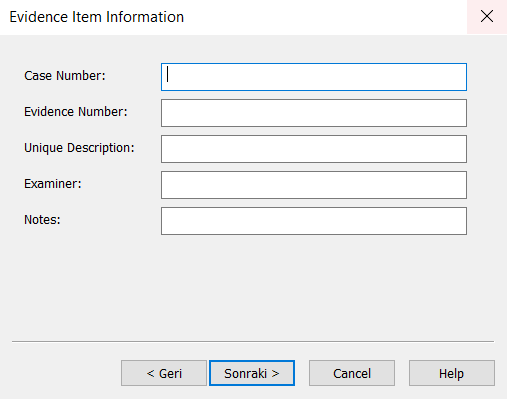
**DD**:Imaj alma işlemi esnasında herhangi bir sıkıştırma uygulanmaz, elde edilecek imaj dosyası kaynak ile aynı boyuttadır. Ayrıca imaj dosyası içerisinde yalnızca hamveri bulunur, herhangi bir metadata verisi yer almaz.

**SMART**: Linux işletim sistemi için geliştirilmiş SMART uygulamasının, ham verinin yanında metadata ve doğrulama değerlerini de içeren dosya formatıdır.

**E01:** EnCase imaj formatıdır, veri dosyaya yazılırken bloklara bölünür ve her bloğa ait hesaplanan checksum değeri verinin arkasına yazılır. Dolayısıyla imaj dosyası yalnızca veriyi değil, metadata ve doğrulama kodlarını da içerir.

**AFF:** Gelişmiş Dosya Formatıdır(Advanced File Format), veri ile metadata bilgileri birleştirilerek aynı dosya içerisinde saklanır.

**5 :** E01 imaj sıkıştırma formatını seçip imaj alma işlemine devam ediyoruz.



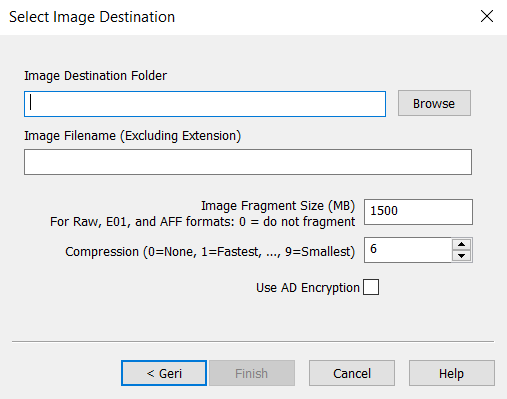
**6 :** Yukarıdaki bilgileri doldurmamız Adli inceleme süreci için oldukça önemlidir. Bilgiler eksiksiz bir şekilde doldurulduktan sonra ileri diyerek açılan pencerede oluşacak olan imaj dosyasının nereye kaydedileceğini seçiyoruz ve ardından start butonuna basarak imaj alma işlemini başlatıyoruz.

**Image Fragment Size:** Imaj dosyasını kaç MB’lık parçalar şeklinde tutmak istediğinizi belirliyorsunuz.

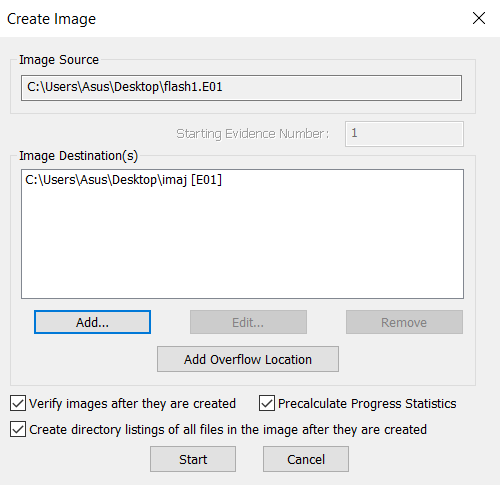
**Compression:** 0-9 arasındaki sayılarla sıkıştırma ölçüsünü belirliyosunuz. Sayı arttıkça sıkıştırmada artacağından imaj alma süresi de uzayacaktır.

**Use AD Encryption:** İmajı şifreli olarak alma işlemini gerçekleştirir.

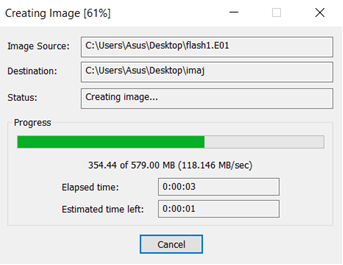
**Verify:** Imaj sonrası imaj ile orjinal disk arasında doğrulama işlemi yapar.

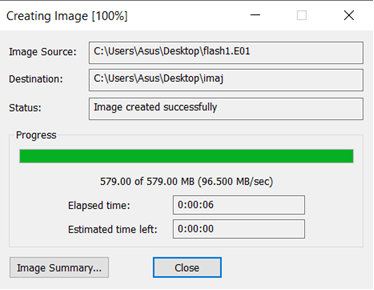


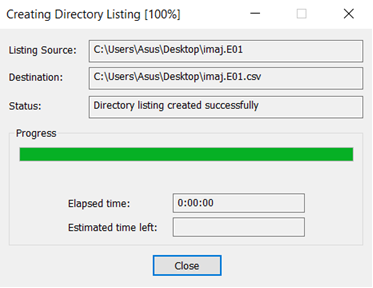
* İmaja dosyasını isimlendirip kaydedileceği dizini belirleyerek işleme devam ediyoruz.

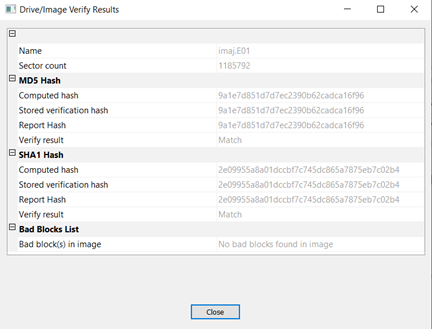


* Start diyip imaj alma işlemini başlatıyoruz.









Imaj bitiminde ekranda imaj dosyasının hash değerleri,sektör sayısı ve hatalı sektör sayısı gibi birçok bilgi gösterilir.

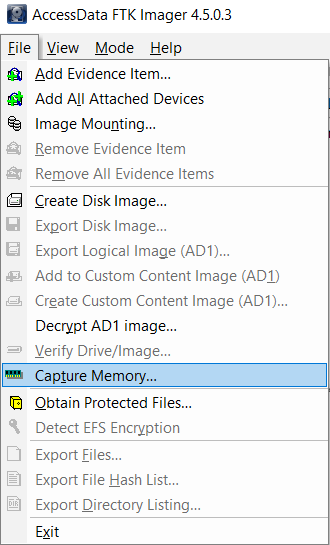
İmaj bitiminde belirtilen yere imaj dosyası ve text uzantılı bir log dosyası kaydolur.Bu text dosyasında imajın hash değerleri,alınma saati,vakanın ismi,inceleyenkişinin ismi gibi birçok önemli bilgi tutulur.

7.FTK Imager ile RAM imajı alma

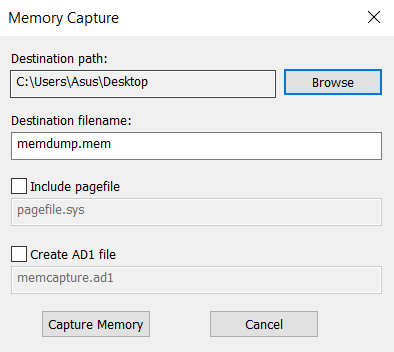
Açık olan bilgisayarın güncel durumdaki ram imajını almak için kullanırız.

RAM imajı alma işlemleri sırayla ;

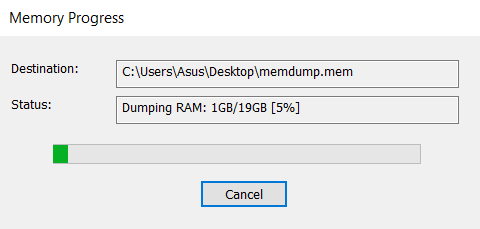
**1:** File menüsünden veya araç çubuğundan Capture Memory seçeneğine tıklanır.



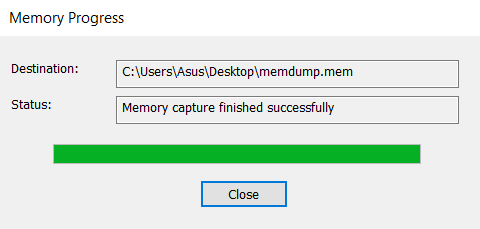
**2:** Açılan yeni pencerede imajın kaydolacağı yer ve imaj dosyasınınisimlendirme işlemlerini yapıp işleme devam etmeliyiz.



**3:** Tamam seçeneğine tıklayıp imaj alma işlemini başlatıyoruz.



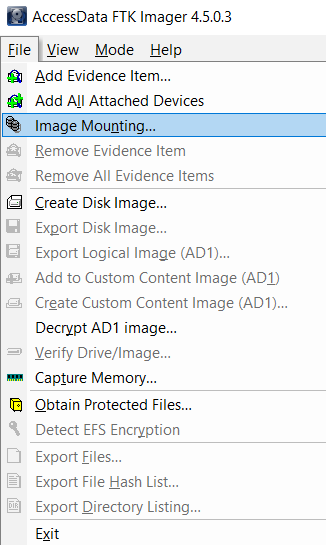
**4:** İmaj alma işlemi bitince imaj dosyasını belirleyen hedefe kaydolur.



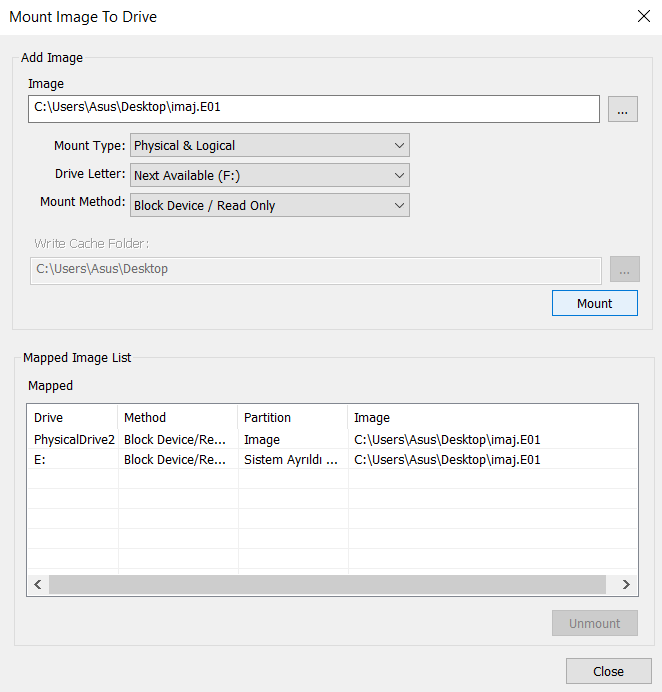
8.FTK Imager ile Mount işlemi

Mount işlemi imaj dosyasının sanal bir sürücüymüş gibi görünmesi işlemini yapar. Mount işlemi aşağıdaki gibi yapılmaktadır;

**1:** File menüsünde bulunan Image Mounting seçeneğine tıklanır.

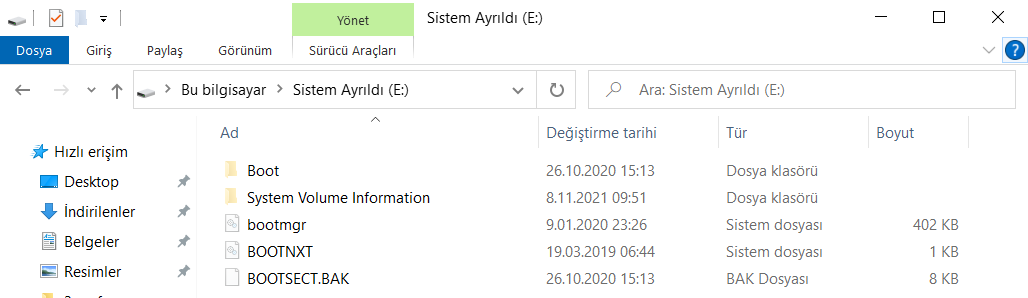


**2:** Açılan yeni pencerede imaj dosyasının bulunduğu dosya yolunu seçip mount seçeneğine tıklanır.



**3**: Mount seçeneğine tıklandıktan sonra Drive alanına yeni bir sürücü eklenecektir.

İstersek bu mount ettiğimiz dosyayı unmount diyerek kaldırabiliriz.



9.FTK Imager yazılımı ile imaj inceleme süreci

FTK imager yazılımı ile medyalar içerisinde bulunan verilerin ve birebir kopyası alınmış olan medyaların kopyalarının ön izlemesi yapılabilir. Alınmış olan imaj dosyaları sadece okuma modunda görüntülenebilir. İmaj içerisindeki veriler dışarı Windows ortamına aktarabilir. Silinmiş dosyalar görüntülenebilir. Hash değerleri üretilebilir.İncelemedeki verilerin kaynağı direk olarak elimizdeki donanım veya önceden alınmış bir image dosyası olabilir. Bunun dışında farklı yazılımlar ile alınan imajlar veya özel imajlar FTK imager ile analiz edilebilir. İnceleme yaparken bizim isteğimize göre verileri text ya da hexadecimal şekilde okuyabiliriz.