

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 ile 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.

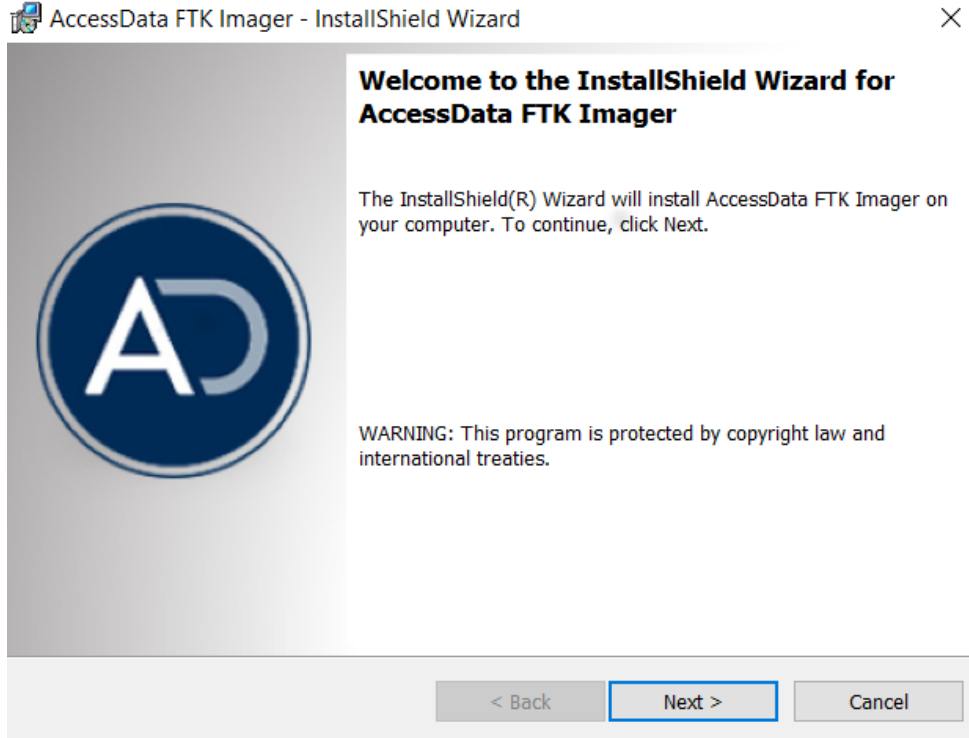
2.FTK IMAGER NEDİR

FTK Imager sabit disk, CD, DVD, klasör 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.

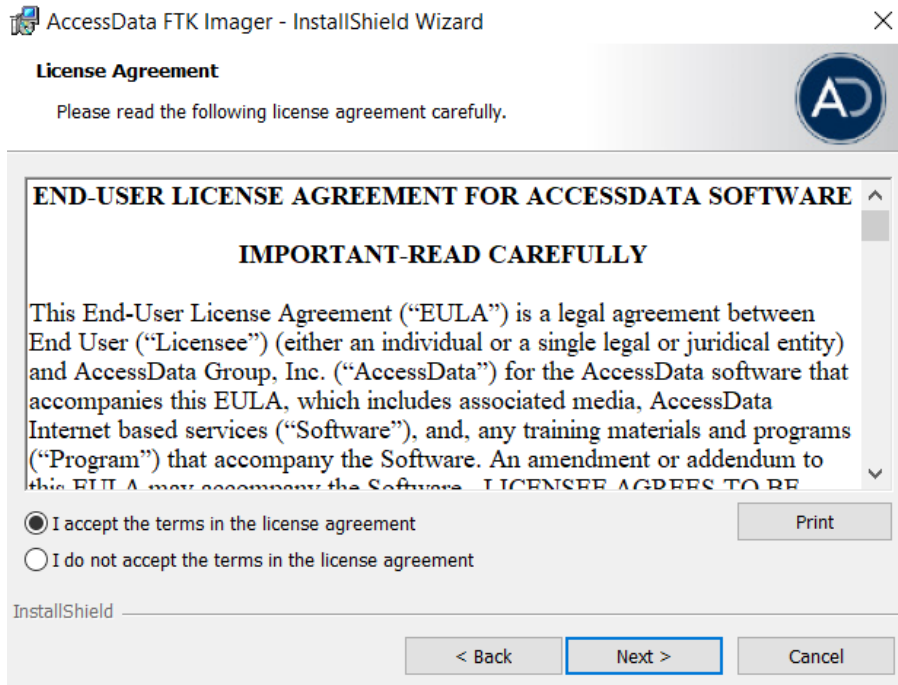
3.FTK Imager Kurulumu

FTK Imager yazılımını AccessData'nın web sitesi üzerinden ücretsiz olarak indirebilirsiniz.

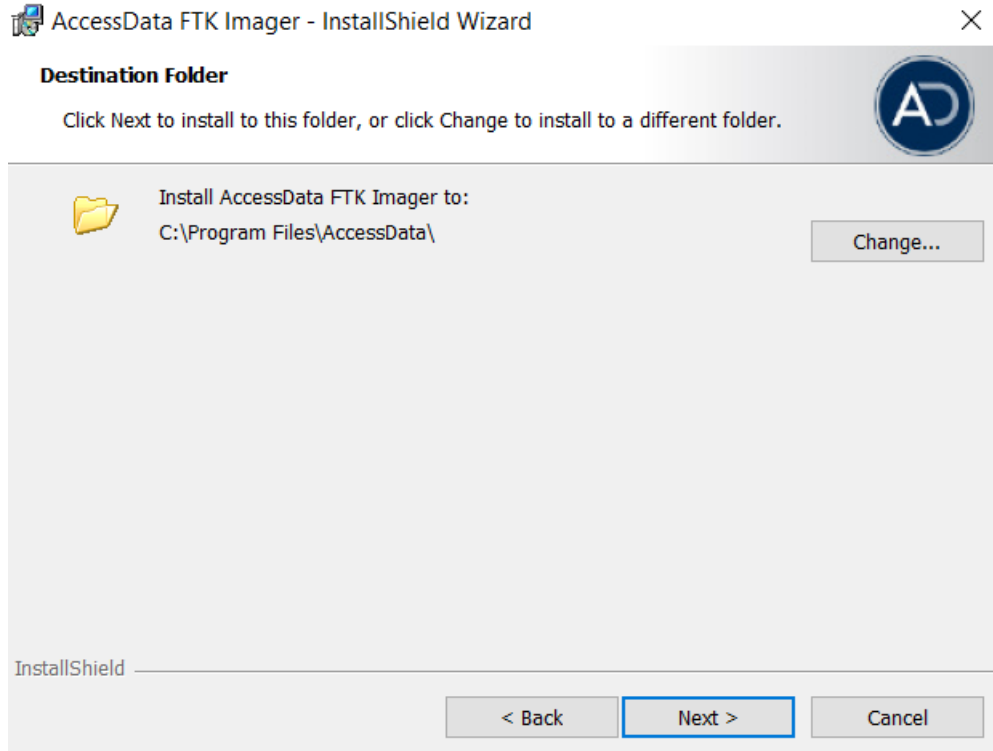
<http://accessdata.com/product-download>



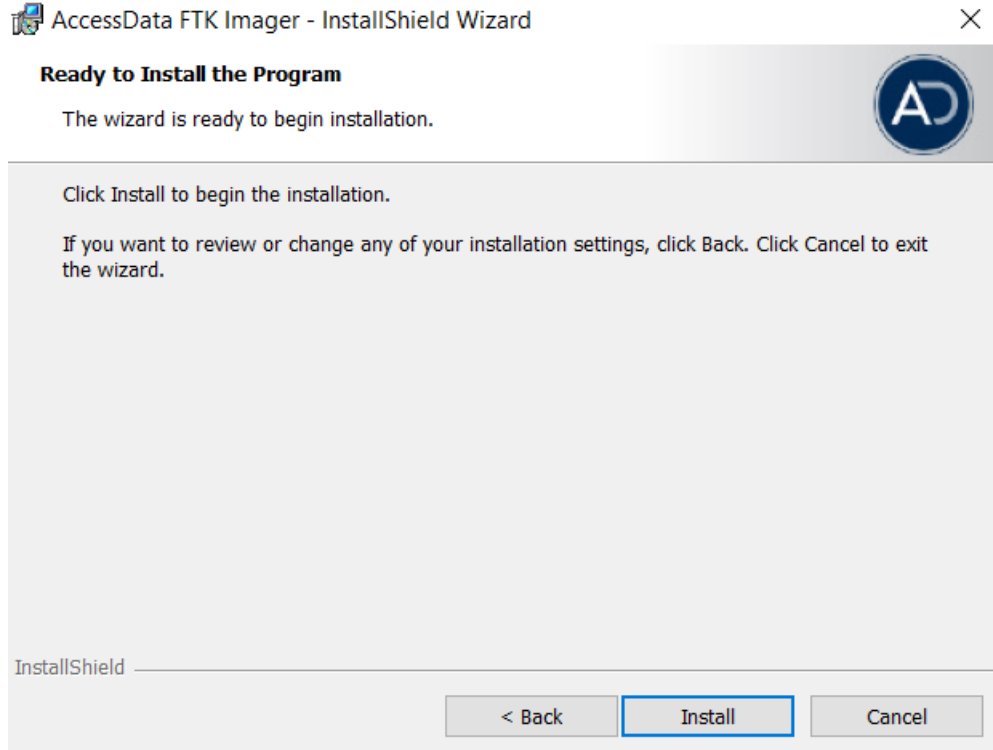
- Açılan pencerede Next butonuna tıklayın.



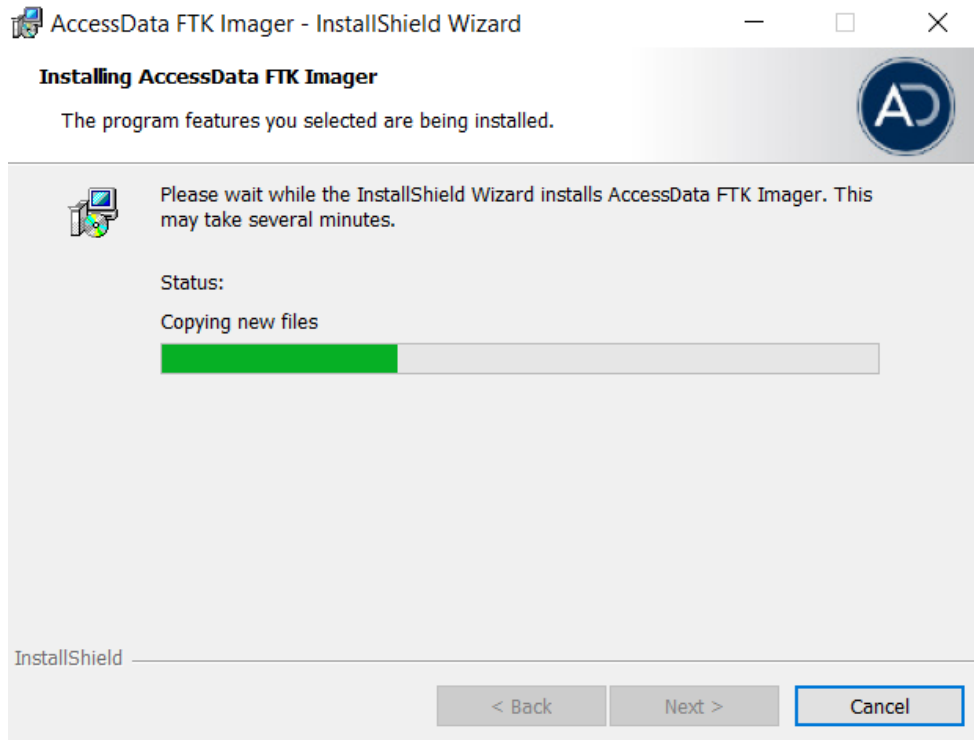
- Kurulumun devam etmesi için sözleşmeyi kabul edin ve Next butonuna tıklayın.



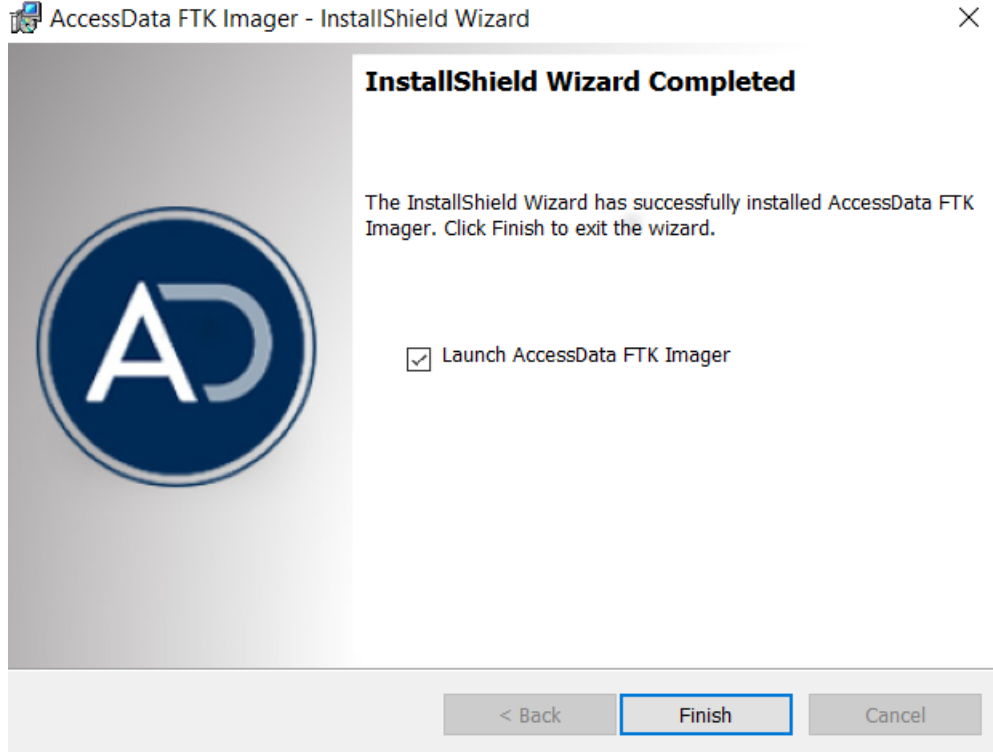
- FTK Imager programının kurulacağı dosya yolunu seçip ve Next butonuna tıklayın.



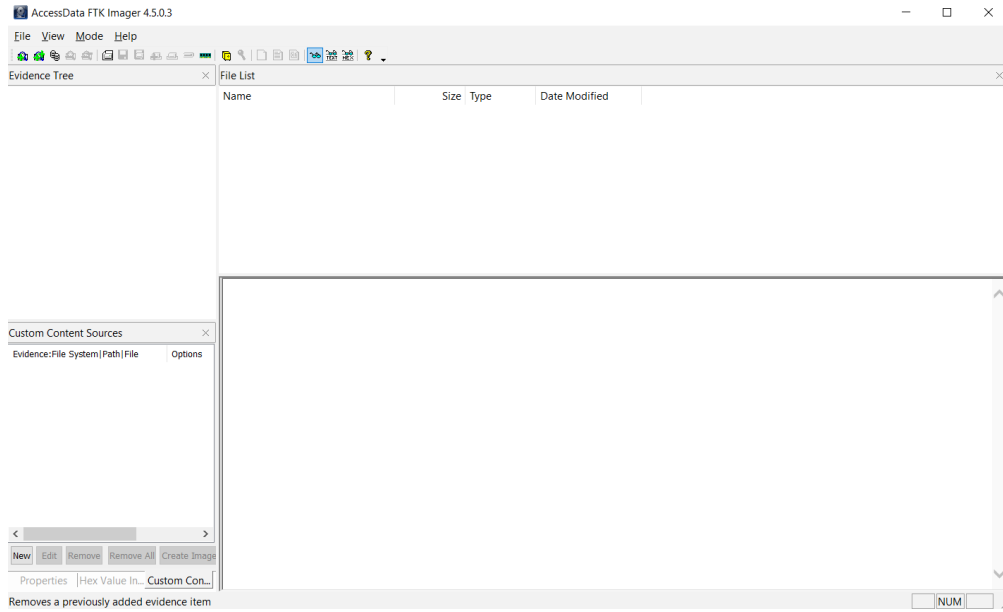
- Install butonuna tıklayıp kurulumu başlatın .



- Kurulumun başladığını ve devam ettiğini görüyoruz.



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

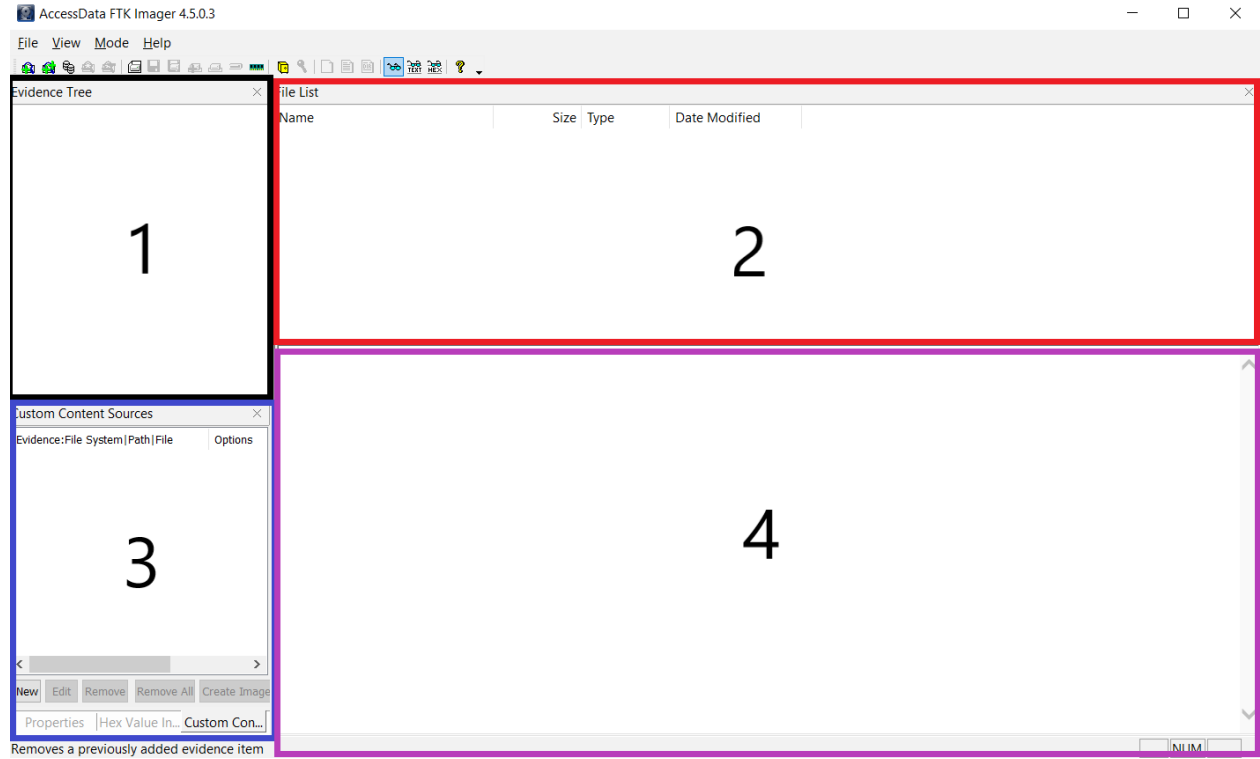


Masaüstünde kısayolu oluşan FTK Imager'a tıklayıp çalıştırabilirsiniz.

4.Yazılım Bölümleri

Imager yazılımını 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

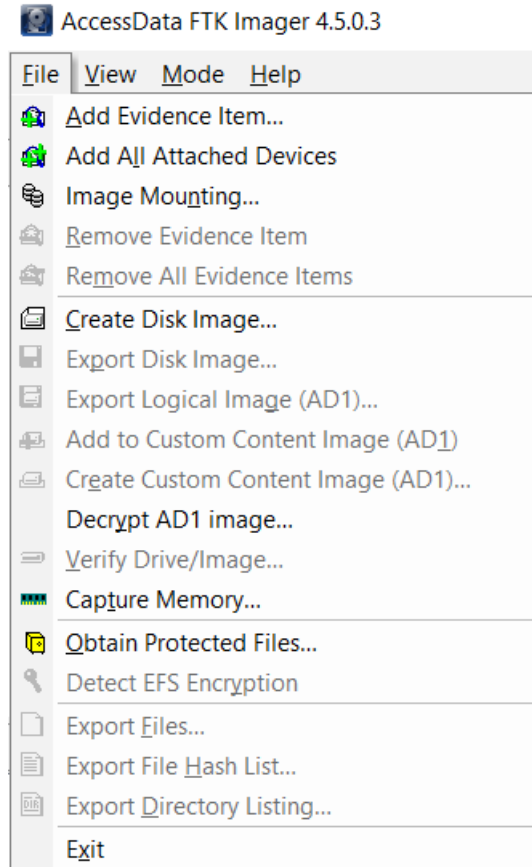
Menüler sağ üst köşede bulunur.Aşağıdaki gibi görünür ;



AccessData FTK Imager 4.5.0.3

File View Mode Help

File: Dosya menüsü araç çubuğunda kullanabileceğimiz tüm özelliklere erişimimizi 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.

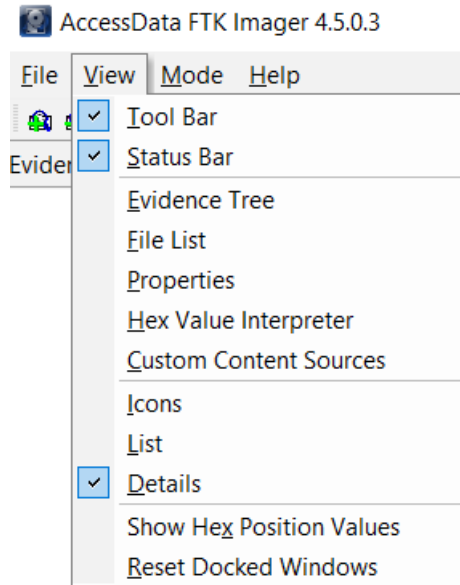
Export Files = Dosyayı dışa aktar işlemini yapar .

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

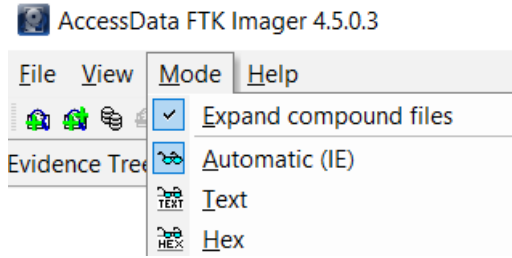
List = Liste

Details = Detaylar

Show Hex Position Values = Hex pozisyon değerini göster

Reset Docked Windows = Yerleşik Windowsu sıfırla

Mode: Mod menüsü görüntüleyici önizleme modunu seçmenizi sağlar.

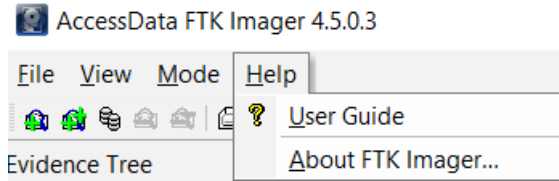


Automatic = Bileşik dosyayı genişlet

Text = İmaj hakkında text dosyası tutma işlemini yapar.

Hex = Hexadecimal rapor oluşturma işlemini yapar.

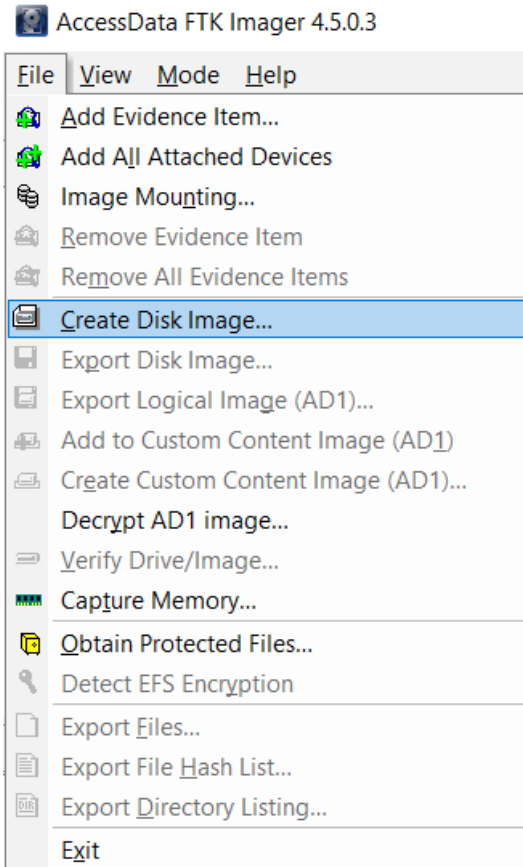
Help:FTK imager kullanımı hakkında bilgi alabileceğimiz alandır.



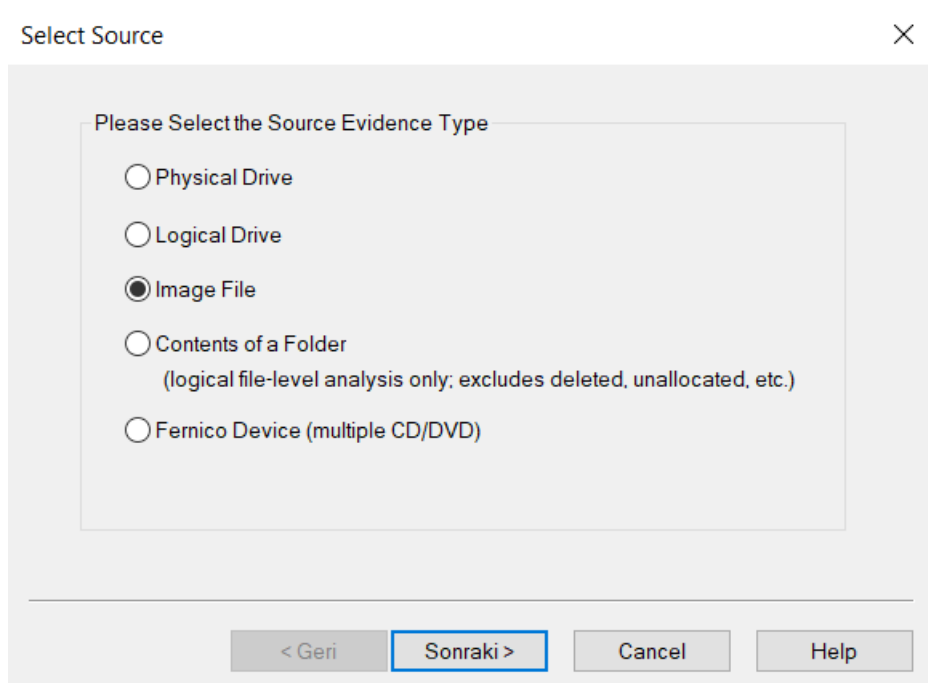
6.FTK Imager İle İmaj Alma

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.



Pysical 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.

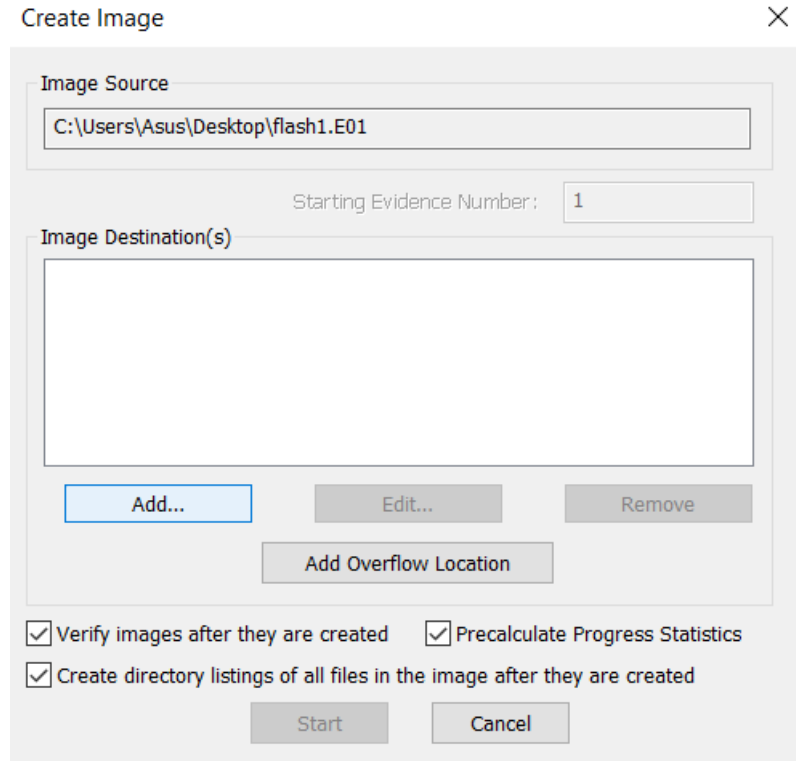
Fernico Device: Çoğaltılabilir CD , DVD tarzı disklerin imajını alır.

Select File ×

Evidence Source Selection

Please enter the source path:

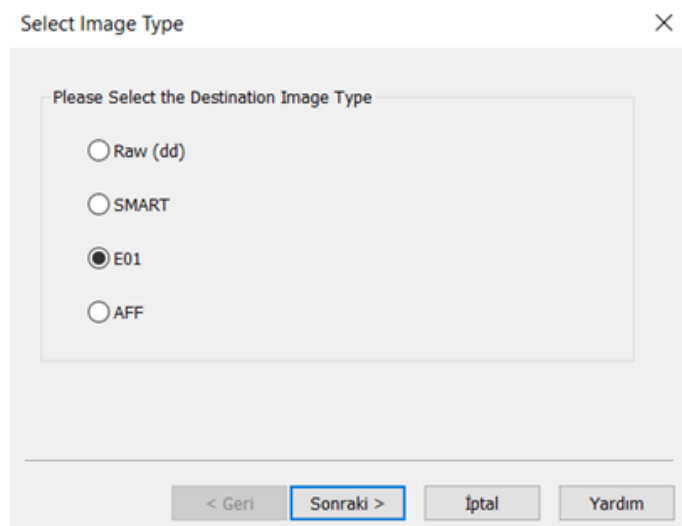
3 : Image dosyasının kaydolacağı yeri Browse diyerek seçiyorum ve işlemlerime devam ediyorum.



The 'Create Image' dialog box is shown with a close button (X) in the top right corner. It contains the following elements:

- Image Source:** A text box containing the path 'C:\Users\Asus\Desktop\flash1.E01'.
- Starting Evidence Number:** A text box containing the number '1'.
- Image Destination(s):** A large empty rectangular box for listing destinations.
- Buttons:** Below the destination box are three buttons: 'Add...' (highlighted in blue), 'Edit...', and 'Remove'. Below these is a button labeled 'Add Overflow Location'.
- Checkboxes:** Three checkboxes are present, all of which are checked:
 - ☒ Verify images after they are created
 - ☒ Precalculate Progress Statistics
 - ☒ Create directory listings of all files in the image after they are created
- Action Buttons:** At the bottom are two buttons: 'Start' and 'Cancel'.

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



The 'Select Image Type' dialog box is shown with a close button (X) in the top right corner. It contains the following elements:

- Title:** 'Please Select the Destination Image Type'.
- Radio Buttons:** Four radio buttons are listed:
 - ☐ Raw (dd)
 - ☐ SMART
 - ☒ E01
 - ☐ AFF
- Navigation Buttons:** At the bottom are four buttons: '< Geri' (disabled), 'Sonraki >' (highlighted in blue), 'İptal' (disabled), and 'Yardım' (disabled).

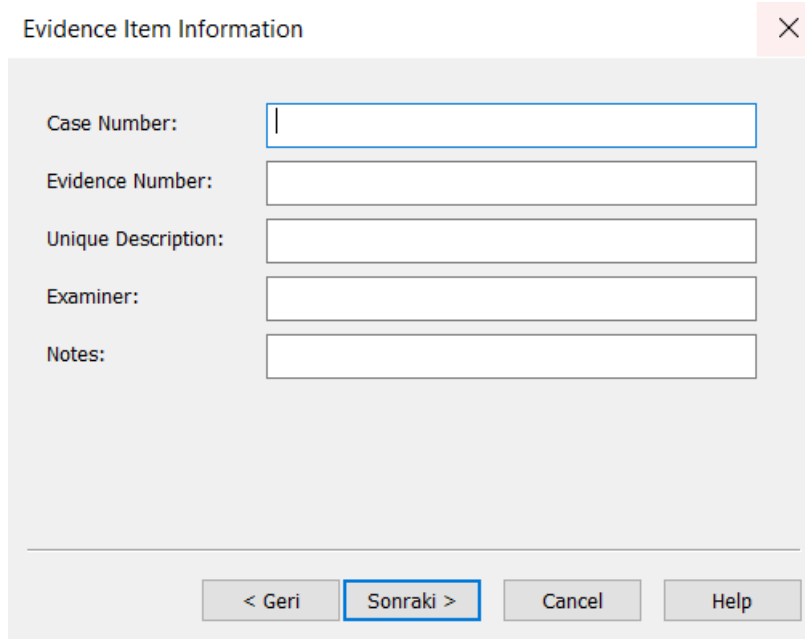
DD: İmaj alma işlemi esnasında herhangi bir sıkıştırma uygulanmaz, elde edilecek imaj dosyası kaynak ile aynı boyuttadır. Ayrıca imaj dosyası içerisinde yalnızca hamveri bulunur, herhangi bir metadata verisi yer almaz.

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.

A screenshot of a software dialog box titled "Evidence Item Information". The dialog has a close button (X) in the top right corner. It contains five text input fields: "Case Number:", "Evidence Number:", "Unique Description:", "Examiner:", and "Notes:". The "Case Number" field is currently active, showing a cursor. At the bottom of the dialog, there are four buttons: "< Geri", "Sonraki >", "Cancel", and "Help". The "Sonraki >" button is highlighted with a blue border.

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 işlemi başlatıyoruz.

Image Fragment Size: İmaj dosyasını kaç MB'lık parçalar şeklinde tutmak istediğinizi belirliyorsunuz.

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

Use AD Encryption: İmajı şifreli olarak alma işlemini gerçekleştirir.

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

Select Image Destination ×

Image Destination Folder

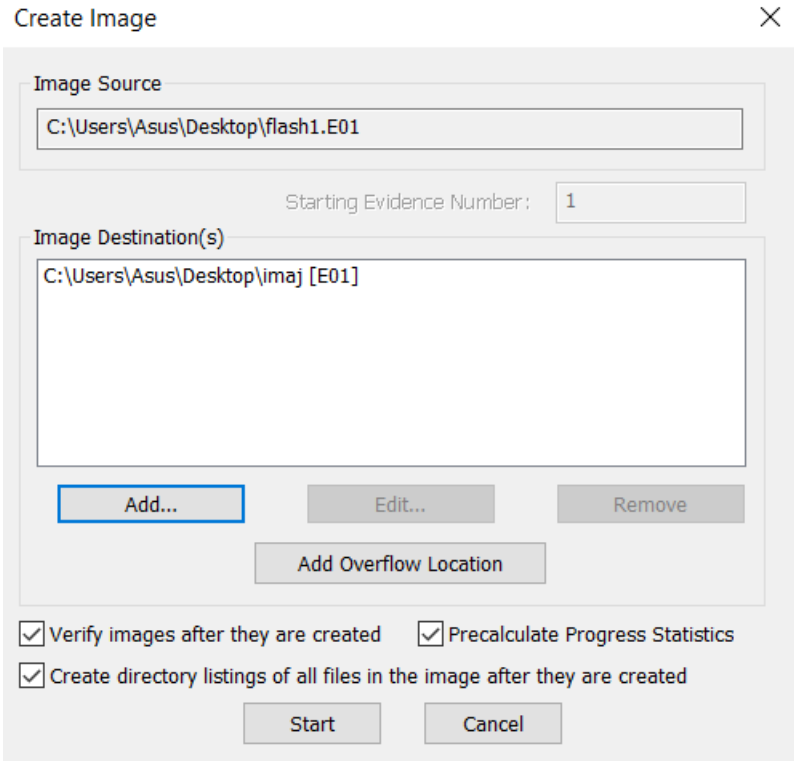
Image Filename (Excluding Extension)

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment

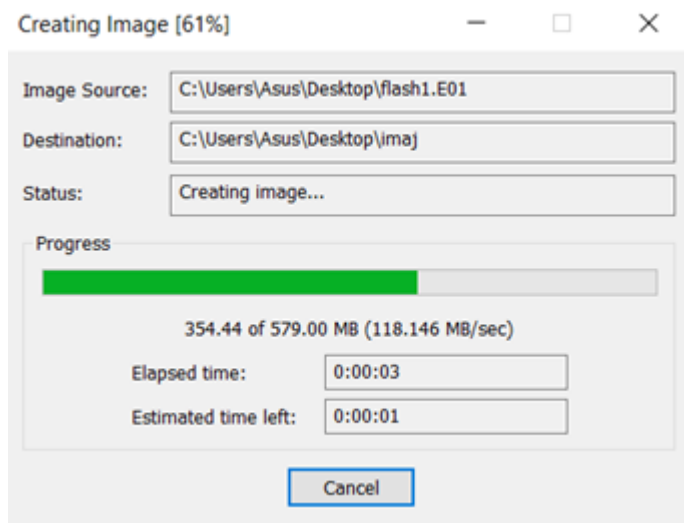
Compression (0=None, 1=Fastest, ..., 9=Smallest)

Use AD Encryption ☐

- İmaja dosyasını isimlendirip kaydedileceği dizini belirleyerek işleme devam ediyoruz.



- Start diyip imaj alma işlemini başlatıyoruz.



Creating Image [100%] — □ ×

Image Source: C:\Users\Asus\Desktop\flash1.E01

Destination: C:\Users\Asus\Desktop\imaj

Status: Image created successfully

Progress

579.00 of 579.00 MB (96.500 MB/sec)

Elapsed time: 0:00:06

Estimated time left: 0:00:00

Image Summary... Close

Creating Directory Listing [100%] — □ ×

Listing Source: C:\Users\Asus\Desktop\imaj.E01

Destination: C:\Users\Asus\Desktop\imaj.E01.csv

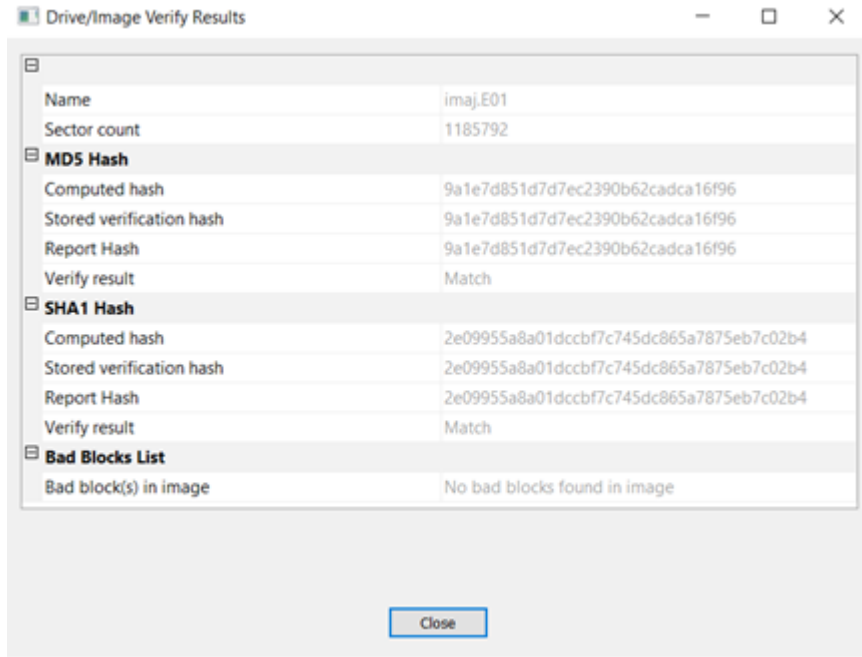
Status: Directory listing created successfully

Progress

Elapsed time: 0:00:00

Estimated time left:

Close



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

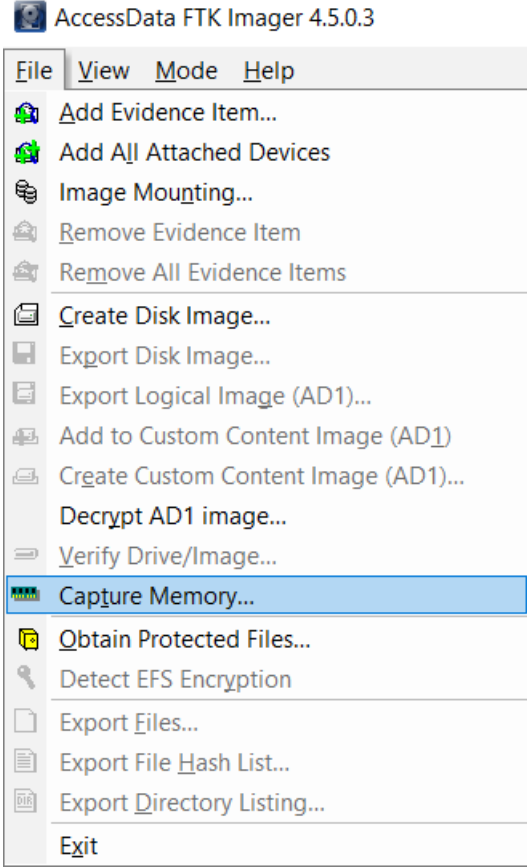
İmaj bitiminde belirtilen yere imaj dosyası ve text uzantılı bir log dosyası kaydolur.Bu text dosyasında imajın hash değerleri,alınma saati,vakanın ismi,inceleyenkişinin ismi gibi birçok önemli bilgi tutulur.

7.FTK Imager ile RAM imajı alma

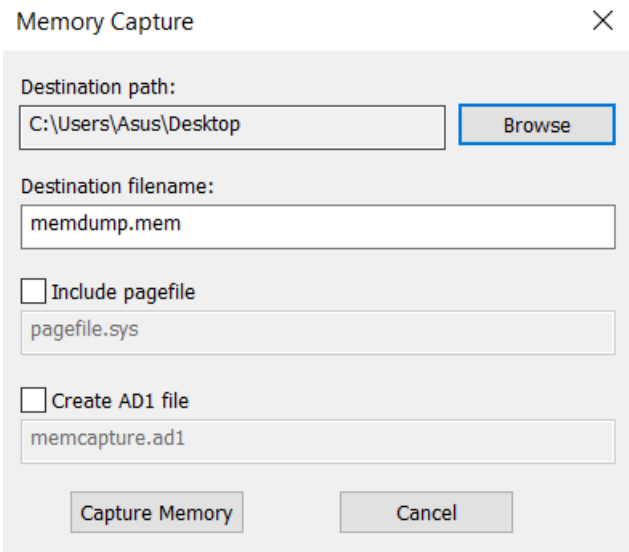
Açık olan bilgisayarın güncel durumdaki ram imajını almak için kullanırız.

RAM imajı alma işlemleri sırayla ;

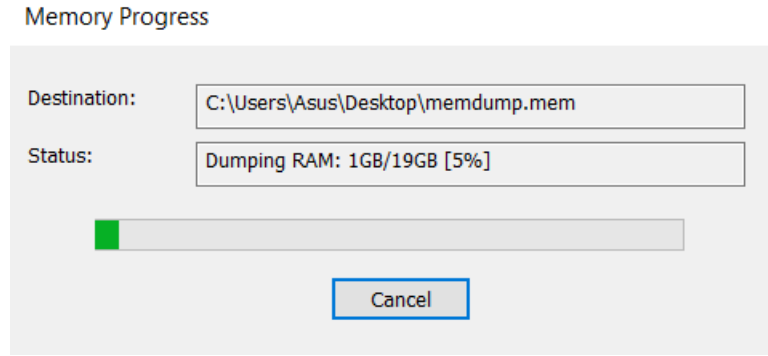
1: File menüsünden veya araç çubuğundan Capture Memory seçeneğine tıklanır.



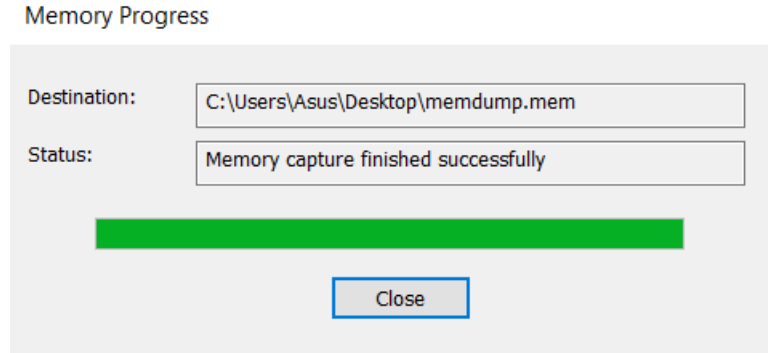
2: Açılan yeni pencerede imajın kaydolacağı yer ve imaj dosyasının isimlendirme işlemlerini yapıp işleme devam etmeliyiz.



3: Tamam seçeneğine tıklayıp imaj alma işlemini başlatıyoruz.



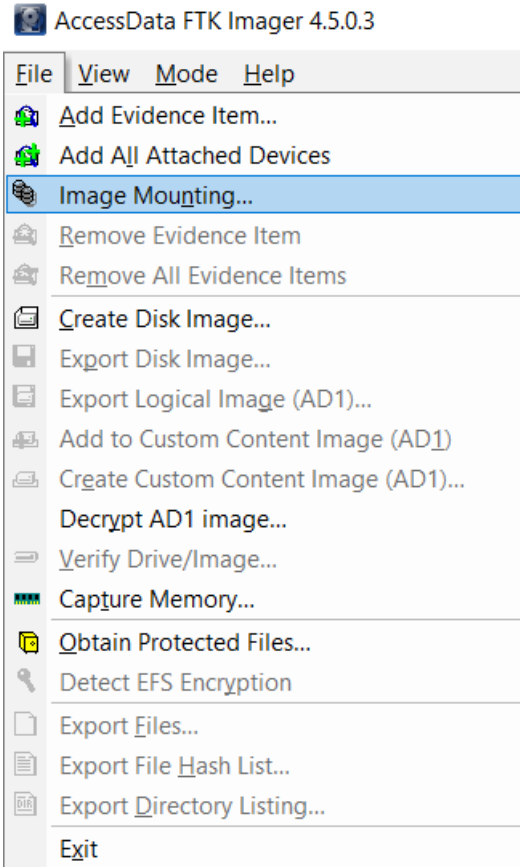
4: İmaj alma işlemi bitince imaj dosyasını belirleyen hedefe kaydolur.



8.FTK Imager ile Mount işlemi

Mount işlemi imaj dosyasının sanal bir sürücüyümüş 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.

Mount Image To Drive

×

Add Image

Image

C:\Users\Asus\Desktop\imaj.E01

...

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder:

C:\Users\Asus\Desktop

...

Mount

Mapped Image List

Mapped

Drive	Method	Partition	Image
PhysicalDrive2	Block Device/Re...	Image	C:\Users\Asus\Desktop\imaj.E01
E:	Block Device/Re...	Sistem Ayrıldı ...	C:\Users\Asus\Desktop\imaj.E01

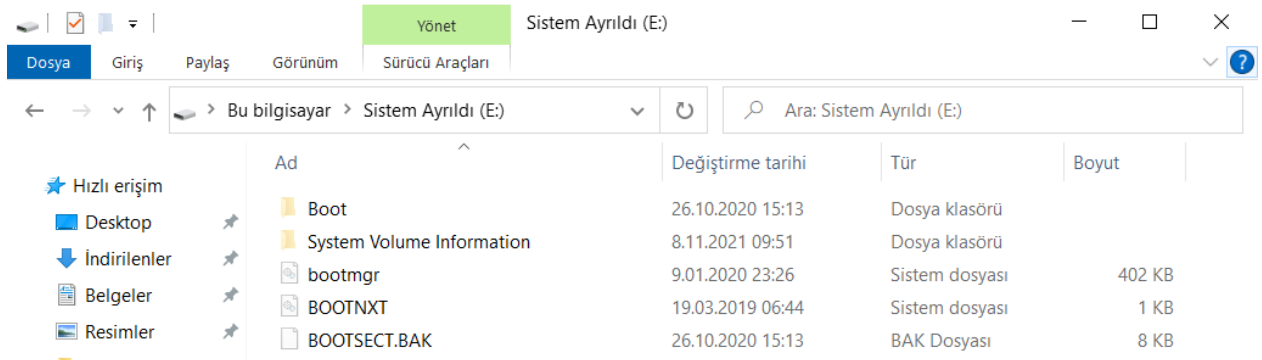
< >

Unmount

Close

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.