



AccesData FTK IMAGER KULLANIM KILAVUZU

DÜZGÜN KÜÇÜK

1. FTK IMAGER HAKKINDA

FTK Imager, Acces Data firması tarafından üretilen ve tamamen ücretsiz olan bir adli bilişim yazılımıdır. Bu program ile elde edilen rapor ve verilerin delil niteliğinde olduğu tüm mahkemelerce kabul edilmiştir.

FTK Imager'in Özellikleri

- ✓ RAM imajları alabilir
- ✓ Depolama aygıtlarının imajlarını alabilir
- ✓ Disk şifreleyebilir
- ✓ Şifreli diskleri açabilir
- ✓ İmaj dosyalarını mount edebilir (imaj dosyalarını inceleme yapılan bilgisayarda yazma engelleme modunda açarak bir disk sürücüsüyümüş gibi görünme imkanı sağlar).
- ✓ Alınan imaj dosyalarını açarak görevliye ön inceleme imkanı sunabilir.

2. FTK IMAGER KURULUMU

FTK Imager, AccesData'nın web sitesinden ücretsiz olarak indirilebilir.

İndirme bağlantısı: <https://accessdata.com/product-download>

FTK® Imager 4.5

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.

WHAT'S NEW?

The release of 4.5 follows earlier releases of 4.3.0 and 4.3.1.1 which included significant speed improvements in image creation (we've seen imaging time cut in half) and additional evidence processing improvements including **XFS file system support**. Users can **parse XFS file systems** (versions 3, 4 & 5) when investigating and collecting from RHEL Linux environments. 4.5 brings with it improvements to the command line, disk imaging, evidence parsing and memory dump.

WHAT DOES FTK IMAGER ALLOW YOU TO DO?

- **Create forensic images** of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media.
- **Preview files and folders** on local hard drives, network drives, CDs and DVDs, thumb drives or other USB devices.
- **Preview the contents** of forensic images stored on the local machine or on a network drive.
- **Mount an image for a read-only view** that leverages Windows® Internet Explorer® to see the content of the image exactly as the user saw it on the original drive.
- **Export** files and folders from forensic images.
- See and **recover files that have been deleted** from the Recycle Bin, but have not yet been overwritten on the drive.
- **Create hashes of files** to check the integrity of the data by using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).
- **Generate hash reports** for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case evidence. When a full drive is imaged, a hash generated by FTK Imager can be used to verify that the image hash and the drive hash match after the image is created, and that the image has remained unchanged since acquisition.

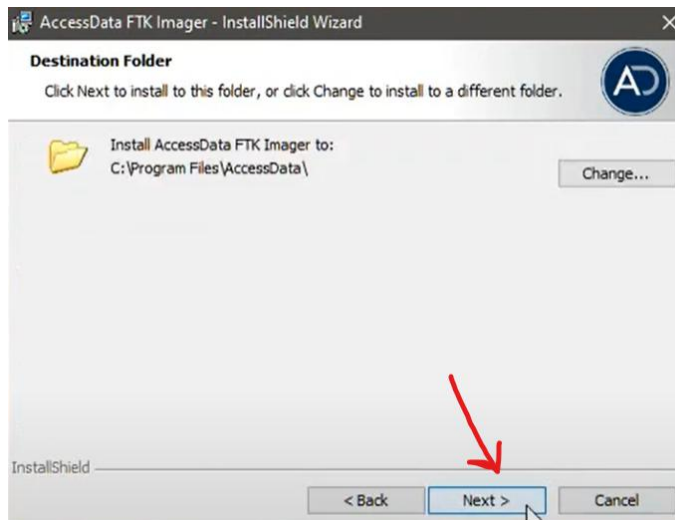
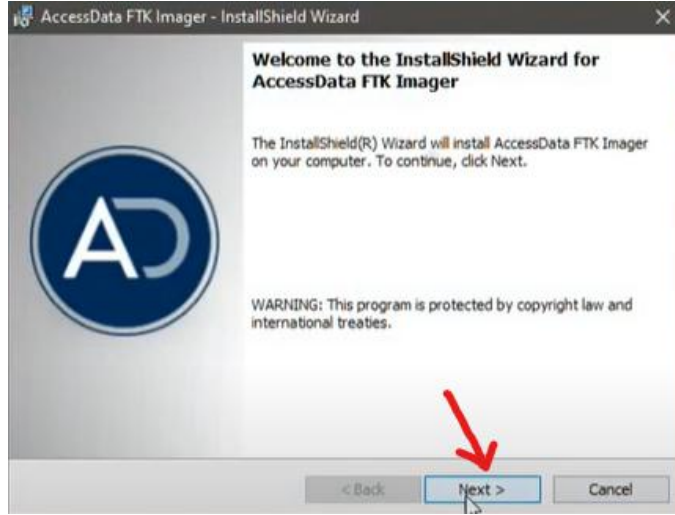
To download FTK Imager 4.5, please fill out the form below. The link to the download will be sent to the email address you enter:

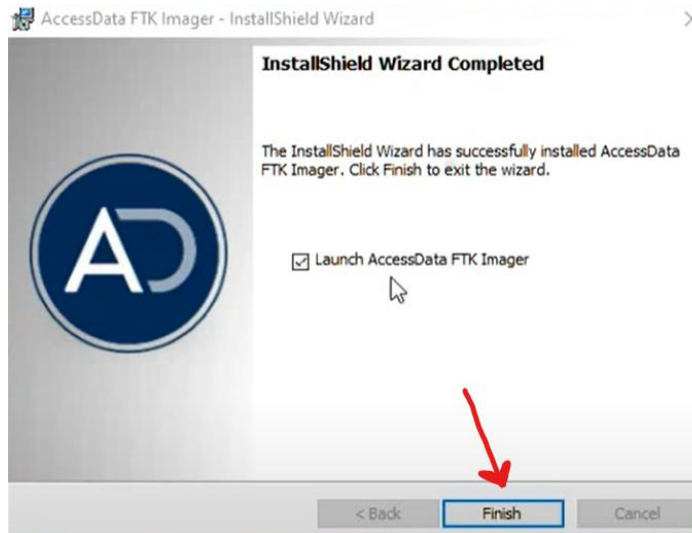
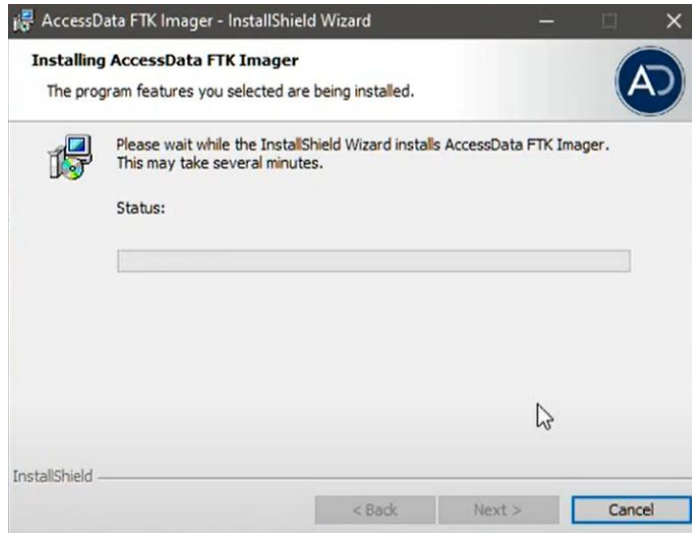
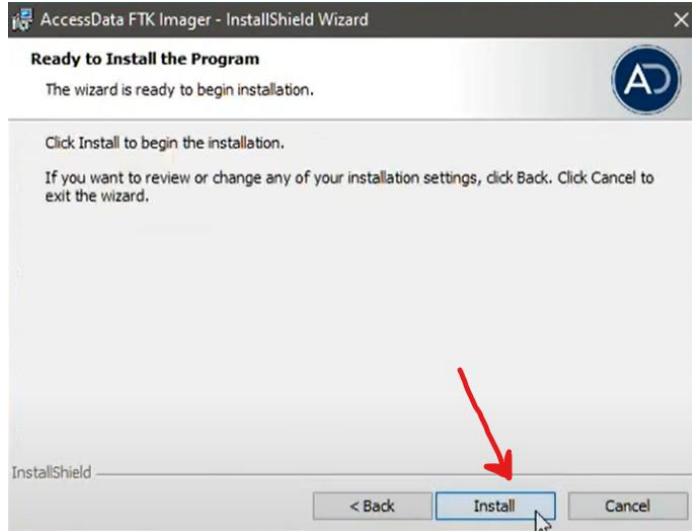
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email	<input type="text"/>
Phone	<input type="text"/>
Country	<input type="text"/>
Organization	<input type="text"/>
Job Title	<input type="text"/>
Job Function	<input type="text"/>
Organization Type	<input type="text"/>
My organization is currently using FTK	<input type="text"/>

Email Opt In

☐ Yes*

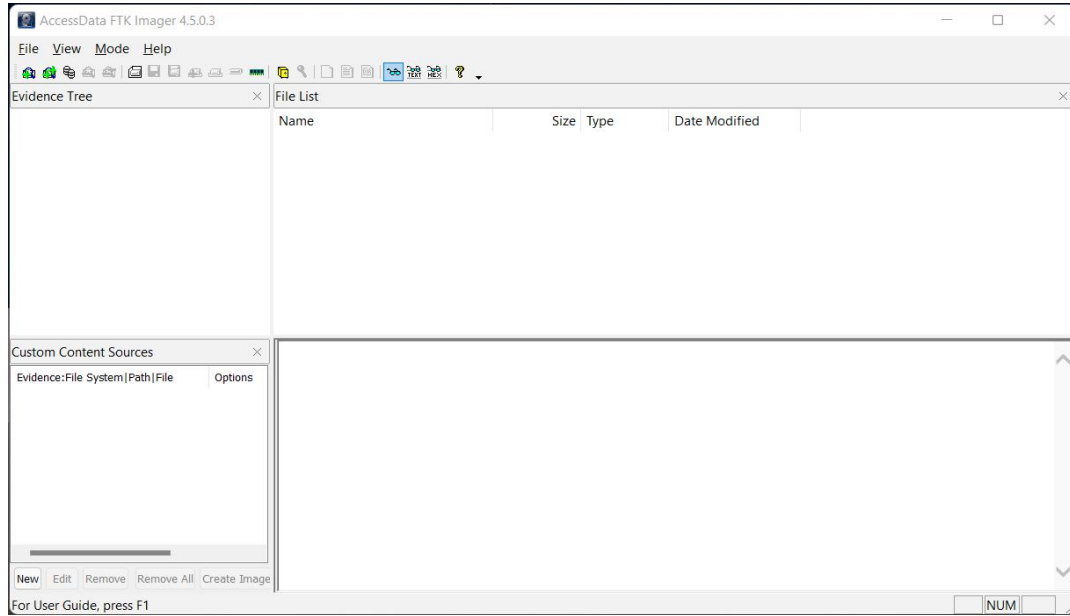
İndirme bağlantısına gittikten sonra üstte gösterilen form doldurulmalıdır. Form doldurulduktan sonra kurulum dosyasının bağlantısı, form içinde belirtilen e-posta adresine gönderilecektir. Kurulum dosyasını indirdikten sonra dosya açılmalı ve aşağıdaki adımlar izlenmelidir.





Gerekli adımlar geçildikten sonra kurulum işlemi başarıyla tamamlanmış olacaktır.

FTK Imager'in doğru bir şekilde çalışması için programın “yönetici olarak çalıştır” çeklide çalıştırılması gerekir. Program açıldıktan sonra aşağıdaki arayüz ile karşılaşılacaktır.

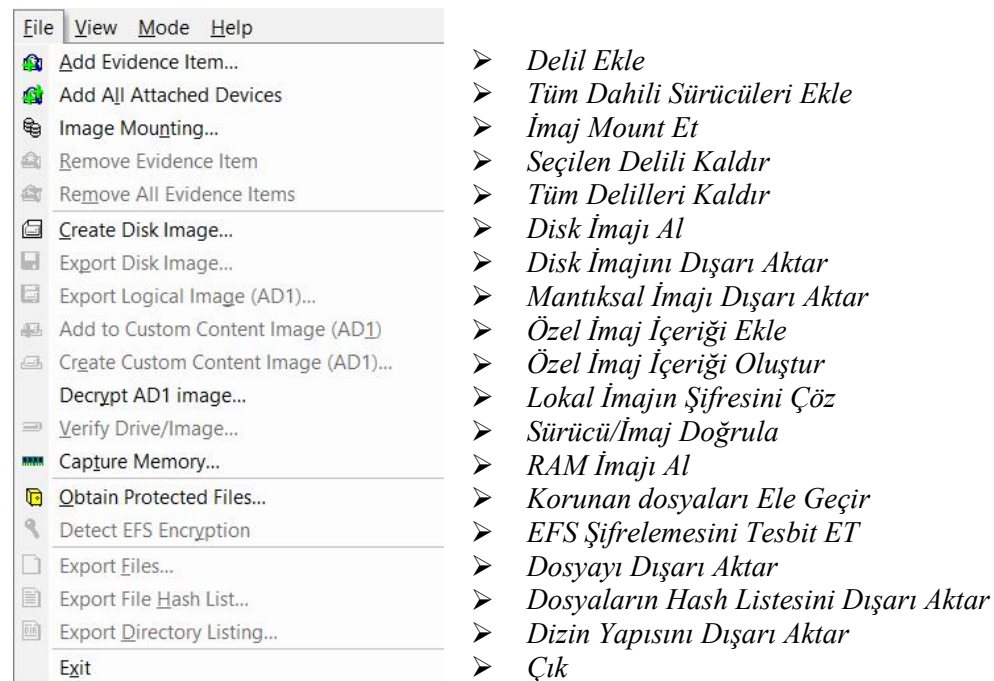


3. FTK Imager Menüleri

FTK Imager'in File, View, Mode ve Help olmak üzere 4 adet menüsü bulunmaktadır.

3.1. File Menüsü

File menüsünün içindeki seçenekler:



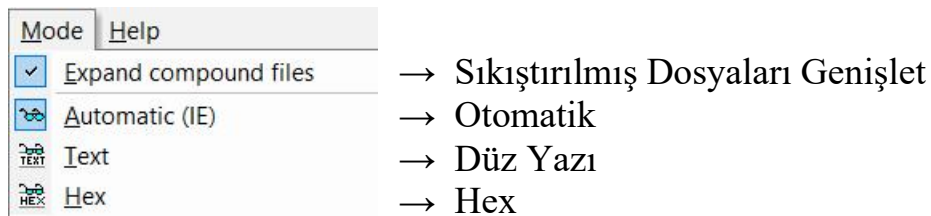
3.2. View Menüsü

View menüsü, programın arayüzü ile ilgili özelleştirmelerin yapılabileceği alandır.



3.3. Mode Menüsü

Mod menüsü, verilerin hangi türde okunacağını seçilmesini sağlar.

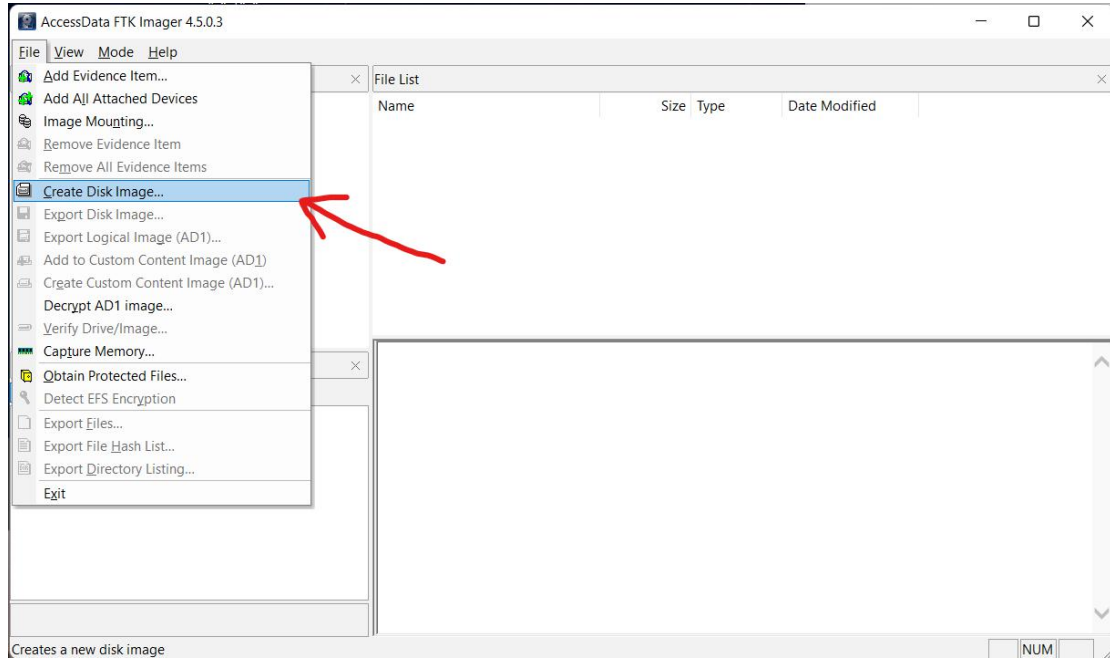


NOT: Menülerin altında araç çubuğu bulunmaktadır. Araç çubuğuna bir nevi kısa yol da denilebilir. Araç çubuğunda, menülerin içinde bulunan seçeneklerden en sık kullanılanlar yer almaktadır. Araç çubuğu, View menüsünden açılıp kapatılabilir.

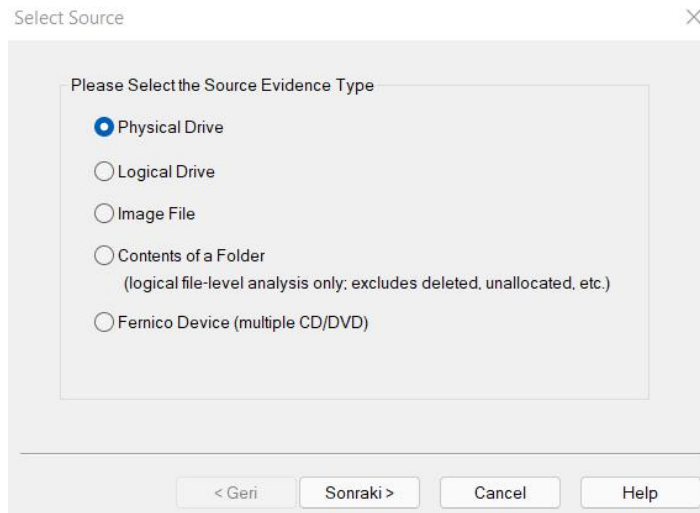


4. FTK Imager İle Disk İmajı Alma Adımları

- File menüsünde bulunan disk imajı al bölümüne tıklanmalı.



- Karşılaşılan ekranda imaj kaynağı ile ilgili bir seçim yapılmalıdır.



Üst görselde bulunan seçeneklerin açıklamaları:

Physical Drive: Bilgisayarda takılı olan fiziksel depolama aygıtlarının imajını almak için seçilmelidir.

Logical Drive: Bilgisayarda bulunan mantıksal depolama alanlarının imajını almak için seçilmelidir.

Image File: Var olan bir imajın imajını almak için seçilmelidir.

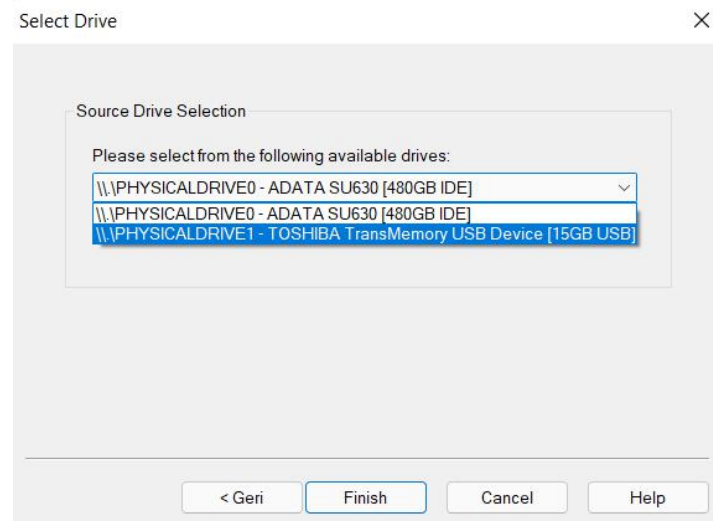
Contents of Folder: Mantıksal sürücü içinde bulunan dizinlerin imajını almak için seçilmelidir (dizin içerisinde bulunan silinmiş dosyalar ve tanımlanmamış disk bölümleri imaj içerisine dahil edilmez).

Fernico Device: Çoğaltılabilir olan cihazların (CD/DVD) imajlarını almak için seçilmelidir.

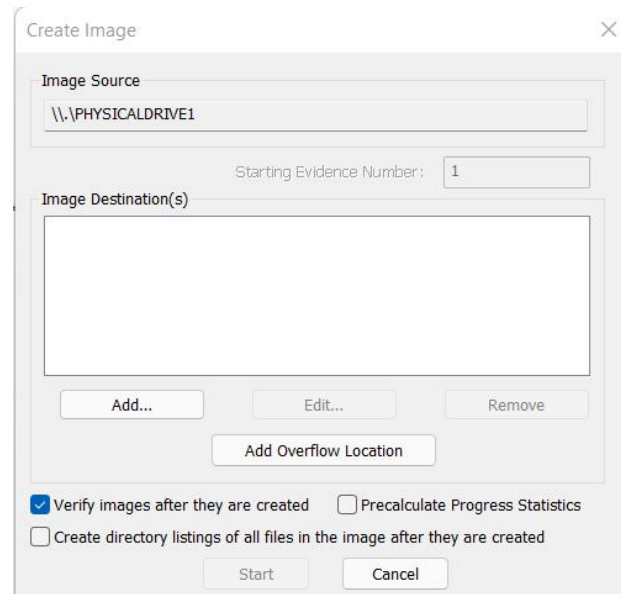
İmajı alınacak yapıya ait seçim yapıldıktan sonra “Sonraki” butonuna tıklanmalıdır.

Not: Bu kılavuzda alınan imaj fiziksel bir sürücünün imajıdır. Hangi imaj tipi seçilirse seçilsin bundan sonra uygulanacak adımlar genel olarak aynıdır.

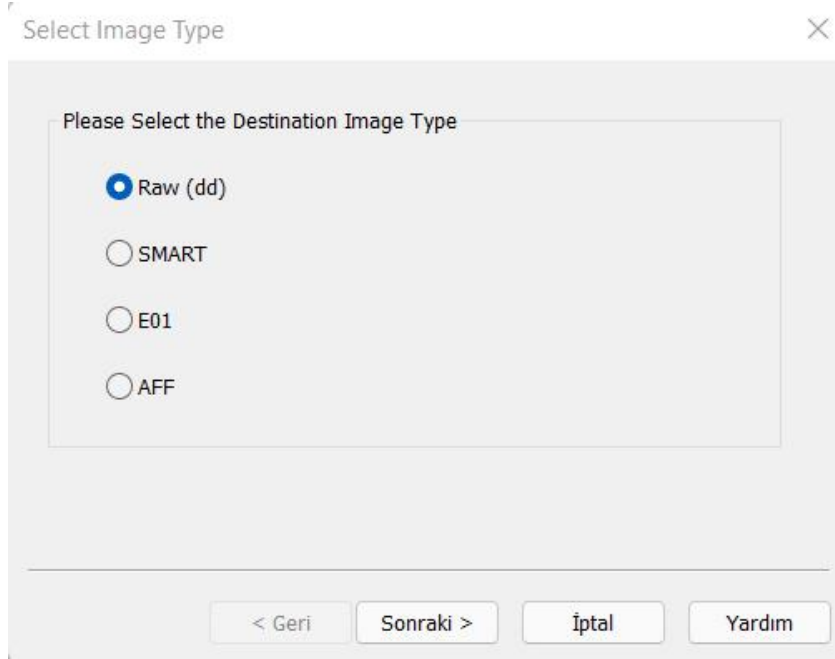
- İmaj kaynağının tipini seçtikten sonra kaynak disk seçilmelidir.



- Disk seçildikten sonra oluşturulacak imaj dosyasına ait konfigürasyonların yapılması gerekmektedir. Bunun için yeni karşılaşılan ekranda bulunan “Add...” butonuna tıklayarak bir sonraki aşamaya geçilmelidir.



- “Add...” butonuna tıkladıktan sonra aşağıdaki pencere açılacaktır ve bu pencerede imaj formatının seçilmesi istenilmektedir.



Üst görselde bulunan imaj formatlarının açıklamaları:

Raw (dd): 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.

SMART: Linux için geliştirilen SMART uygulamasının dosya formatıdır. İmaj dosyasının içerisinde veriler ham verilerdir. Metadata ve doğrulama değerlerini de içermektedir.

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

AFF: Gelişmiş bir dosya formatıdır. Veri ve metadata bilgilerinin aynı dosyada veya ayrı bir dosya içerisinde saklanması olanak sağlar. Sıkıştırılmış veya sıkıştırılmamış olarak imaj alma imkanı sunmaktadır. Sıkıştırılmamış imaj dosyaları sonradan sıkıştırılabilmektedir.

- İmaj tipi seçildikten sonra delile ait özel bilgiler girilmelidir.

Evidence Item Information

Dava Numarası → Case Number: 2021-009

Delil Numarası → Evidence Number: 006

Delile ait açıklama → Unique Description: Beyaz Renkli Flash Bellek (Toshiba)

Müfettiş → Examiner: Düzgün Küçük

Notlar → Notes:

< Geri Sonraki > Cancel Help

- Gerekli bilgiler girilip geçildikten sonra aşağıdaki pencere açılacaktır.

Select Image Destination

Image Destination Folder: C:\İnceleme Browse

Image Filename (Excluding Extension): Beyaz Flash Bellek

Image Fragment Size (MB): 1500
For Raw, E01, and AFF formats: 0 = do not fragment

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

Use AD Encryption ☐

< Geri Finish Cancel Help

Açılan pencerede bulunan seçenekler:

Image Destination Folder: Bu bölüm, alınan imaj dosyasının nereye kaydedileceğinin seçilmesini sağlar.

Image Filename: İmaj dosyasına verilecek isim.

Image Fragment Size: İmaj dosyasının kaç MB'lık parçala ayrılacağına ayarlandığı bölümdür. Raw, E01 ve AFF formatları için değer 0 olarak ayarlanırsa parçalama işlemi yapılmadan imaj tek parça halinde oluşturulur.

Compression: Eğer seçilen imaj formatı sıkıştırmayı destekliyorsa sıkıştırma katsayısı buradan ayarlanmalıdır. Sıkıştırma katsayısı en küçük 1, en büyük 9 olarak ayarlanabilir. Atanan katsayı ile doğru orantılı olacak şekilde imaj alma süresi de artmaktadır. Eğer katsayı değeri 0 olarak girilirse herhangi bir sıkıştırma uygulanmadan imaj alınır.

Use AD Encryption: Bu seçenek seçilirse oluşturulacak imaj dosyasını AD ile şifreler.

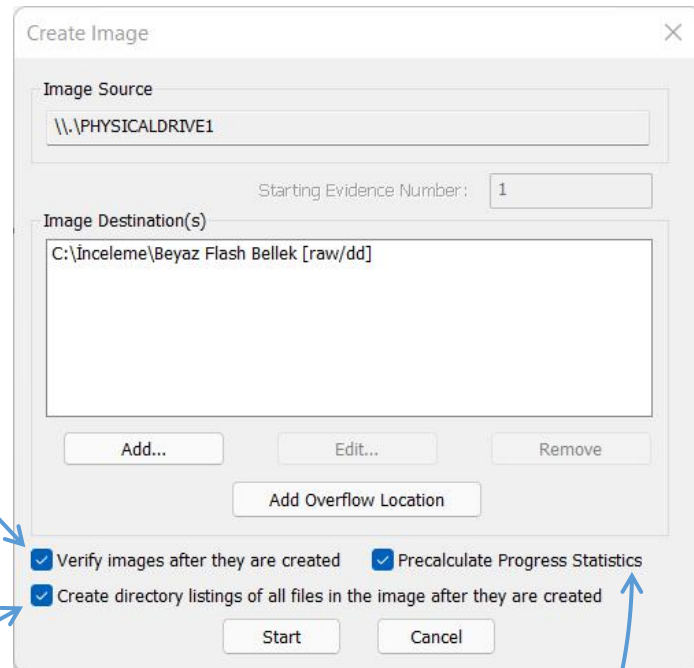
Kullanıcının elinde bir şifreleme sertifikası varsa bu bölüm üzerinden programa aktararak şifreleme işlemi gerçekleştirilebilir.



The dialog box is titled "AD Encryption Credentials". It has a close button (X) in the top right corner. The main heading is "Enter Credentials To Encrypt". There are two radio buttons: "Password:" (selected) and "Certificate (.pfx, .p12, .pem)". The "Password:" option has two text input fields labeled "Password:" and "Re-enter:". To the right of the "Re-enter:" field is a checkbox labeled "Show password". The "Certificate" option has a text input field and a "Browse" button to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

- İmaj için gerekli konfigürasyonlar yapıldıktan sonra adım 2.4 penceresine geri dönülmektedir. Bu pencerenin alt kısmından bulunan üç seçenek bulunmaktadır.

Alınan imajın ve imaj kaynağının hash değerlerini hesaplayarak iki hash değerinin de aynı olup olmadığını karşılaştırır

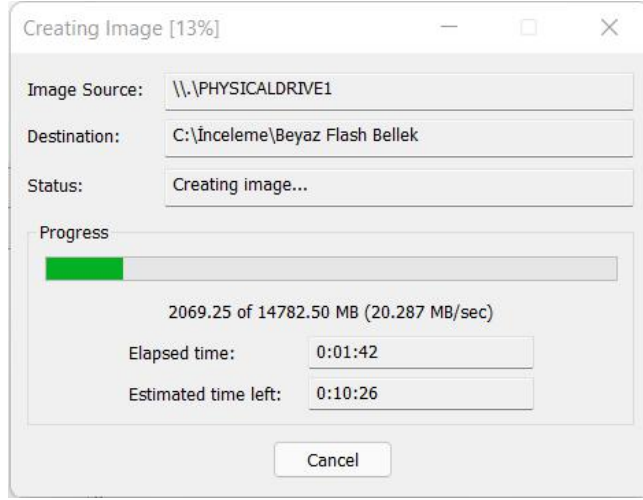


The dialog box is titled "Create Image". It has a close button (X) in the top right corner. The "Image Source" field contains "\\.\PHYSICALDRIVE1". Below it is a "Starting Evidence Number:" field with the value "1". The "Image Destination(s)" field contains "C:\İnceleme\Beyaz Flash Bellek [raw/dd]". Below this field are three buttons: "Add...", "Edit...", and "Remove". Below these is an "Add Overflow Location" button. At the bottom, there are three checked checkboxes: "Verify images after they are created", "Precalculate Progress Statistics", and "Create directory listings of all files in the image after they are created". At the very bottom are "Start" and "Cancel" buttons.

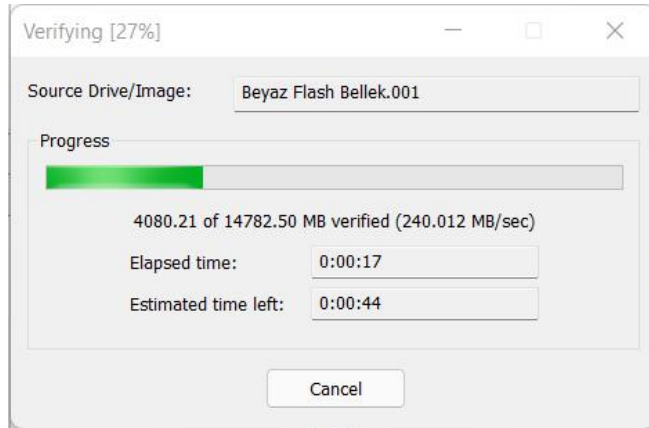
İmaj içindeki tüm dosyaların dizin listesini oluşturarak csv formatındaki dosyaya yazar ve bu dosyayı imajın kaydedileceği dizinin içerisine kaydeder.

İmaj alma işlemi sırasında tahmini kalan süre ve tamamlanma yüzdesi gibi istatistikleri gösterir.

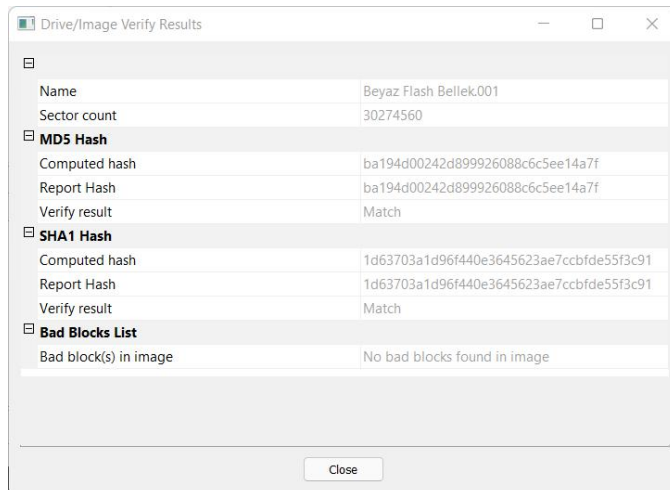
- Tüm adımlar gerçekleştirildikten sonra imaj alma işlemi başlatılabilir.
- İmajın alınması işlemi.



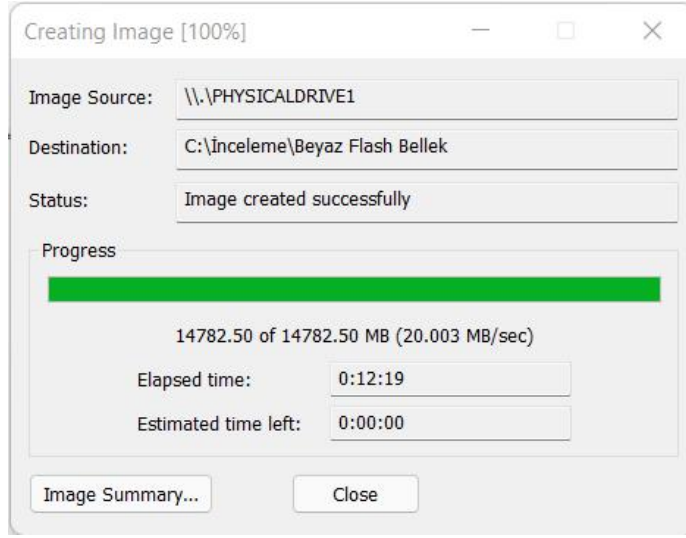
- Alınan imaj ile diske ait hash değerlerinin hesaplanıp karşılaştırılması işlemi.



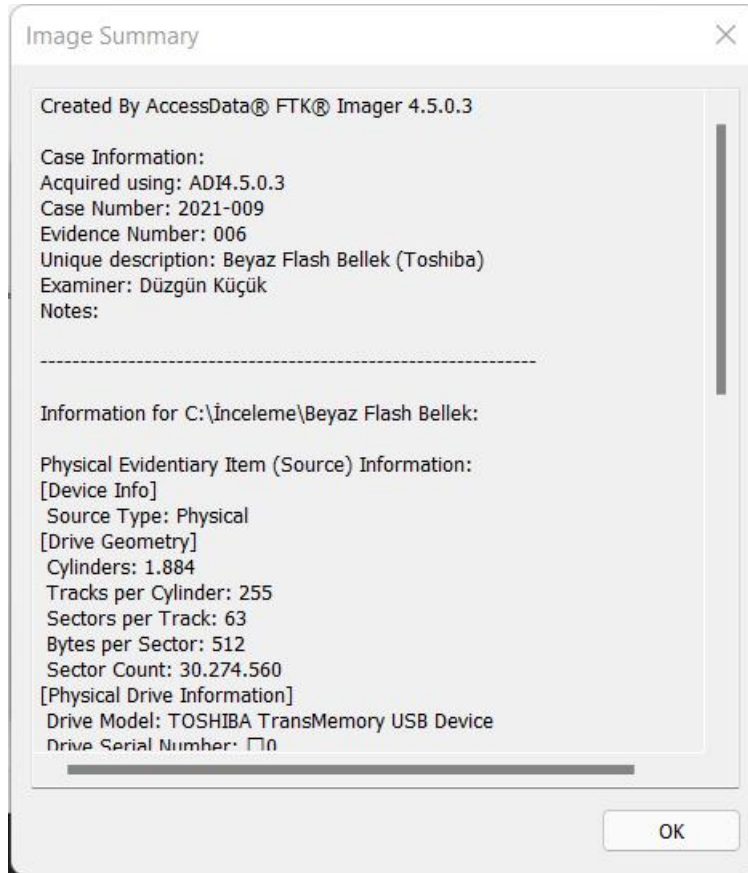
- Karşılaştırılan hash değerlerinin doğrulama işleminin sonucu.



- Tüm işlemlerin başarıyla sonlanırsa aşağıdaki ekran ile karşılaşılacaktır.



Üst görselde bulunan pencerenin “Image Summary...” butonuna tıklanıldığında oluşturulan imaj dosyasına ait bilgiler alttaki görselde görünmektedir.



Bu bilgiler imajın kaydedildiği dizinde “txt” uzantılı bir dosyanın içinde de bulunmaktadır.

Bu bilgisayar > Yerel Disk (C:) > İnceleme				
Ad	Değiştirme tarihi	Tür	Boyut	
Beyaz Flash Bellek.001	21.11.2021 12:09	WinRAR arşivi	1.536.000 ...	
Beyaz Flash Bellek.001.csv	21.11.2021 12:20	Comma Separated...	60 KB	
Beyaz Flash Bellek.001.txt	21.11.2021 12:21	Metin Belgesi	2 KB	
Beyaz Flash Bellek.002	21.11.2021 12:10	002 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.003	21.11.2021 12:12	003 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.004	21.11.2021 12:13	004 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.005	21.11.2021 12:14	005 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.006	21.11.2021 12:15	006 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.007	21.11.2021 12:17	007 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.008	21.11.2021 12:18	008 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.009	21.11.2021 12:19	009 Dosyası	1.536.000 ...	
Beyaz Flash Bellek.010	21.11.2021 12:20	010 Dosyası	1.313.280 ...	
Beyaz Flash Bellek.240832	21.11.2021 12:05	240832 Dosyası	0 KB	

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Acquired using: ADI4.5.0.3

Case Number: 2021-009

Evidence Number: 006

Unique description: Beyaz Flash Bellek (Toshiba)

Examiner: Düzgün Küçük

Notes:

Information for C:\İnceleme\Beyaz Flash Bellek:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 1.884

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 30,274,560

[Physical Drive Information]

Drive Model: TOSHIBA TransMemory USB Device

Drive Serial Number: 00

Drive Interface Type: USB

Removable drive: True

Source data size: 14782 MB

Sector count: 30274560

[Computed Hashes]

MD5 checksum: ba194d00242d899926088c6c5ee14a7f

SHA1 checksum: 1d63703a1d96f440e3645623ae7ccbfde55f3c91

Image Information:

Acquisition started: Sun Nov 21 12:08:08 2021

Acquisition finished: Sun Nov 21 12:20:27 2021

Segment list:

C:\İnceleme\Beyaz Flash Bellek.001

C:\İnceleme\Beyaz Flash Bellek.002

C:\İnceleme\Beyaz Flash Bellek.003

C:\İnceleme\Beyaz Flash Bellek.004

C:\İnceleme\Beyaz Flash Bellek.005

C:\İnceleme\Beyaz Flash Bellek.006

C:\İnceleme\Beyaz Flash Bellek.007

C:\İnceleme\Beyaz Flash Bellek.008

C:\İnceleme\Beyaz Flash Bellek.009

C:\İnceleme\Beyaz Flash Bellek.010

Image Verification Results:

Verification started: Sun Nov 21 12:20:28 2021

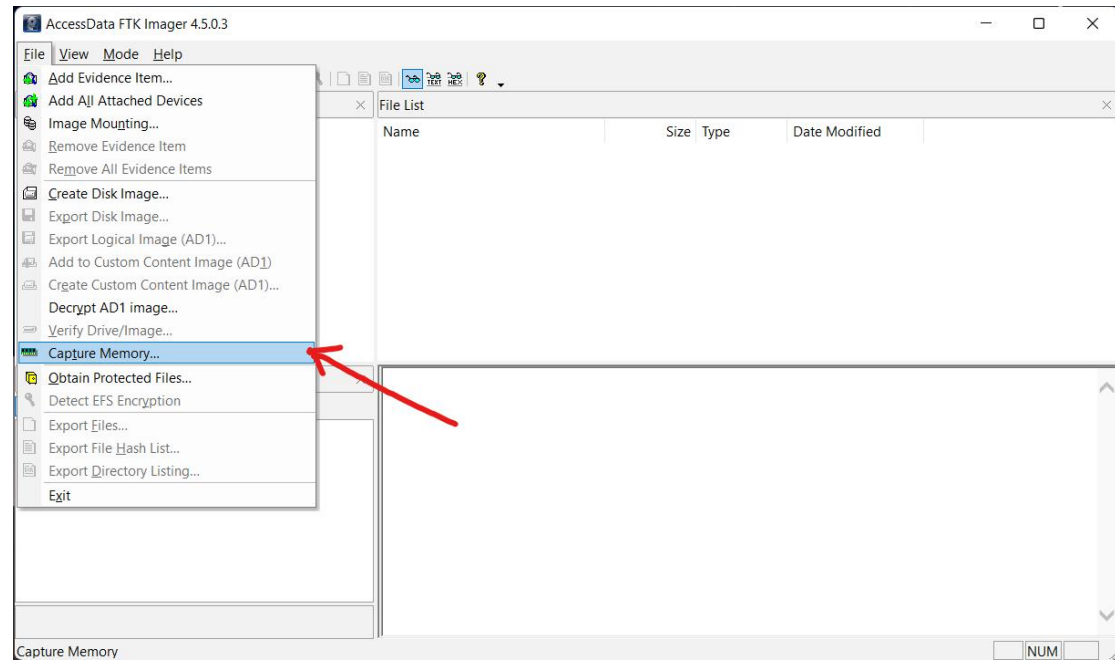
Verification finished: Sun Nov 21 12:21:26 2021

MD5 checksum: ba194d00242d899926088c6c5ee14a7f : verified

SHA1 checksum: 1d63703a1d96f440e3645623ae7ccbfde55f3c91 : verified

5. FTK Imager İle RAM İmajı Alma Adımları

- File menüsü altında bulunan “bellek yakala” seçeneği seçilmelidir.



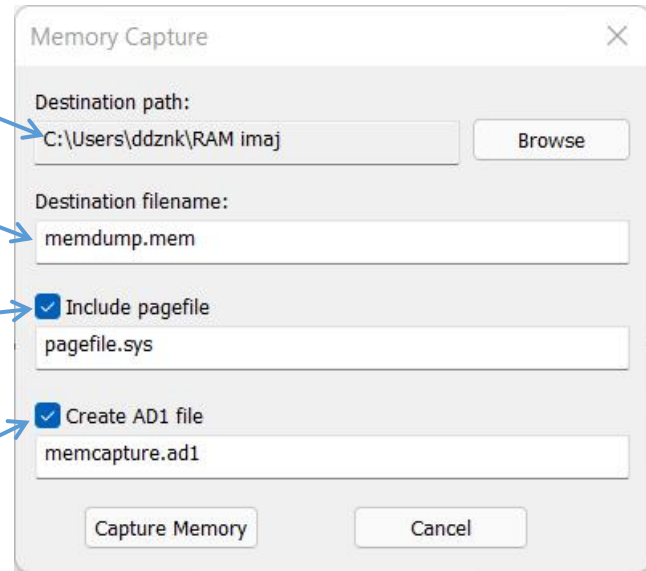
- Açılan pencerede imaj alma işlemine dair seçenekler bulunmaktadır.

İmajın kaydedileceği alanın seçilmesini sağlar.

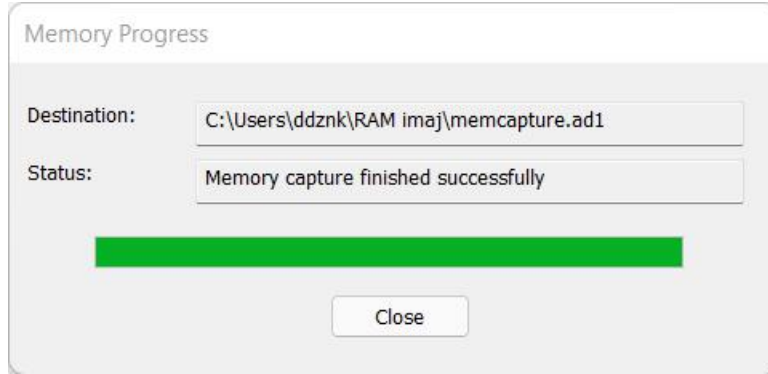
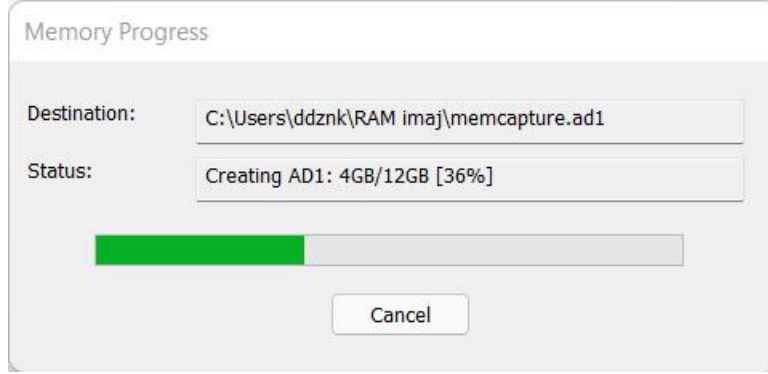
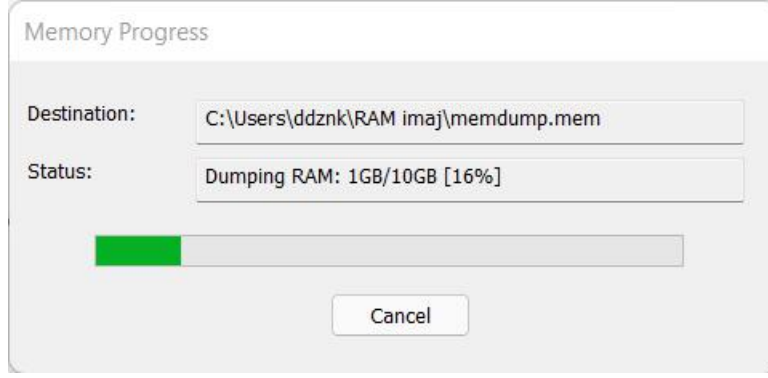
İmaj dosyasına verilecek isim

Windows işletim sisteminin sanal bellek olarak kullandığı dosyaları imaj alma işlemine dail eder

Hem RAM hem pegefile dosyasını birleştirip tek bir imaj olarak yazar.



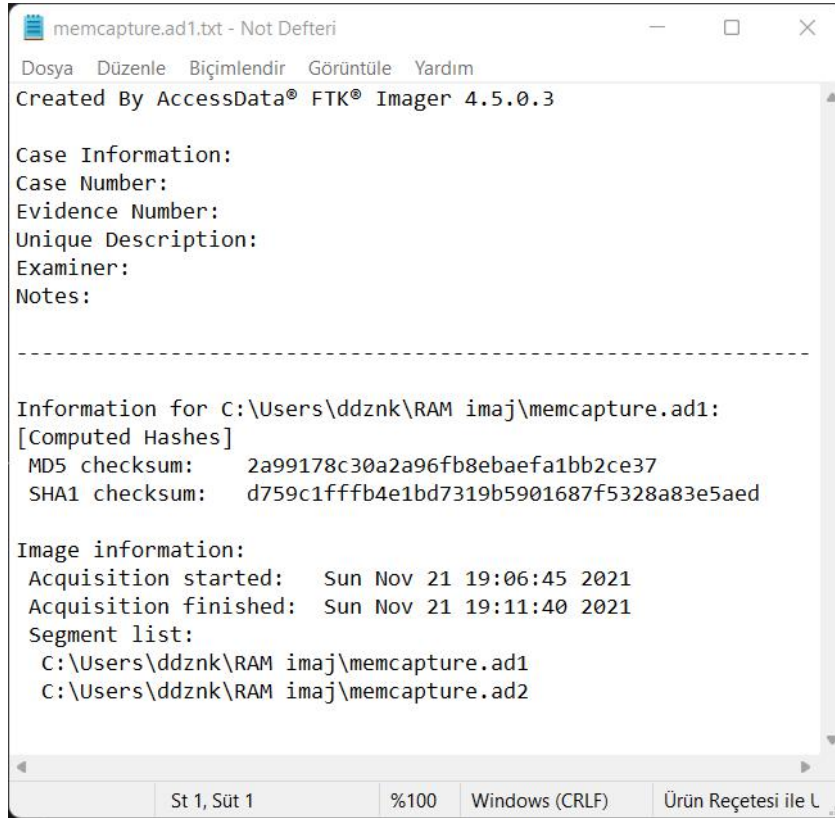
- Gerekli Ayarlamalar yapıldıktan sonra imaj alma işleminin bitmesi beklenmelidir.



- Tüm İşlemler bittikten sonra oluşturulan dosyalar alttaki görünmektedir.

Düzgün Küçük > RAM imaj				
Ad	Değiştirme tarihi	Tür	Boyut	
memcapture.ad1	21.11.2021 19:11	AD1 Dosyası	1.953.125 ...	
memcapture.ad1.txt	21.11.2021 19:11	Metin Belgesi	1 KB	
memcapture.ad2	21.11.2021 19:11	AD2 Dosyası	658.988 KB	
memdump.mem	21.11.2021 19:05	MEM Dosyası	9.936.896 ...	
pagefile.sys	21.11.2021 19:06	Sistem dosyası	1.966.080 ...	

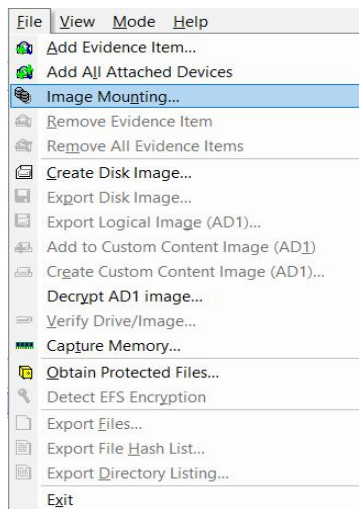
- txt uzantılı dosyasının içeriği aşağıda bulunan görseldeki gibidir.



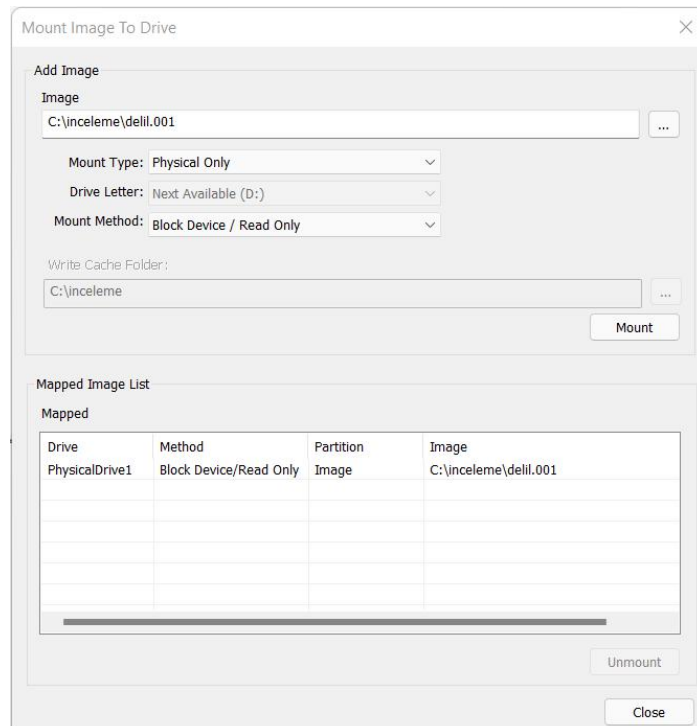
6. FTK Imager İle İmajların Mount İşlemi

İmajların, inceleme yapılacak bilgisayar içine mantıksal bir diskmiş gibi aktarılması işlemine mount etmek denir. Mount işlemi yapıldığında imaj sadece okunabilir şekilde açılmaktadır. Busayede delile herhangi bir zarar gelmesi önlenmektedir.

- Mount işlemi için ilk olarak File menüsü altında bulunan “Image Mounting...” seçeneği seçilmelidir.

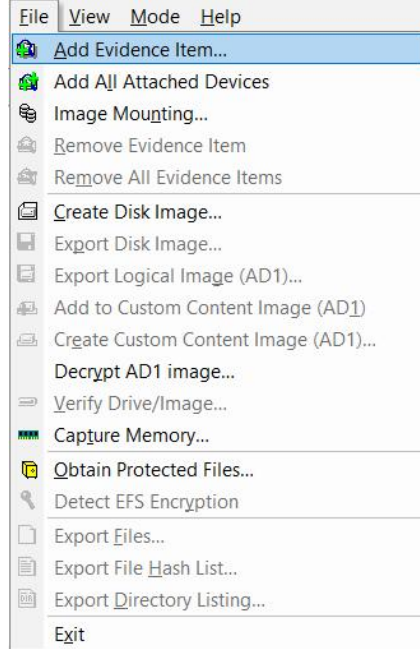


- “Blok Cihazı / Sadece Oku, Blok Cihazı / Yazılabilir, FAT32 / Sadece Oku” seçenekleri bulunmaktadır*

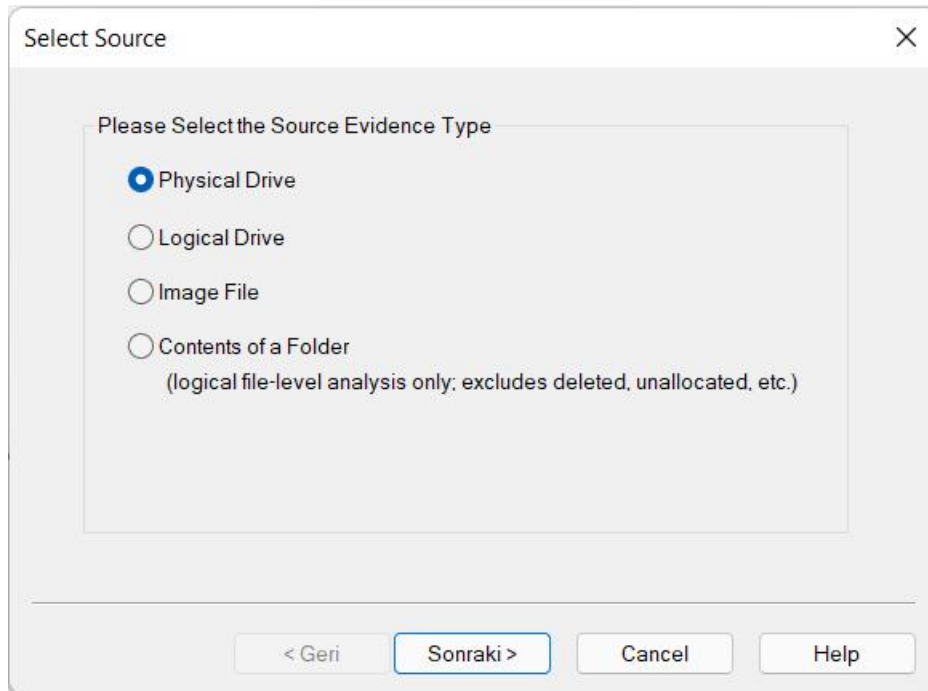


7. FTK Imager İle İmaj Analizi

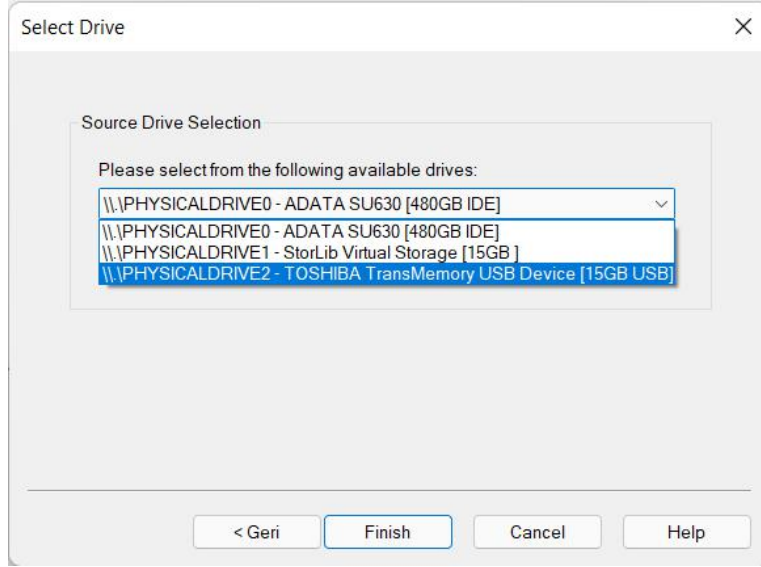
- İlk olarak File menüsü altında bulunan “Add Evidence Item...” butonuna tıklanmalı.



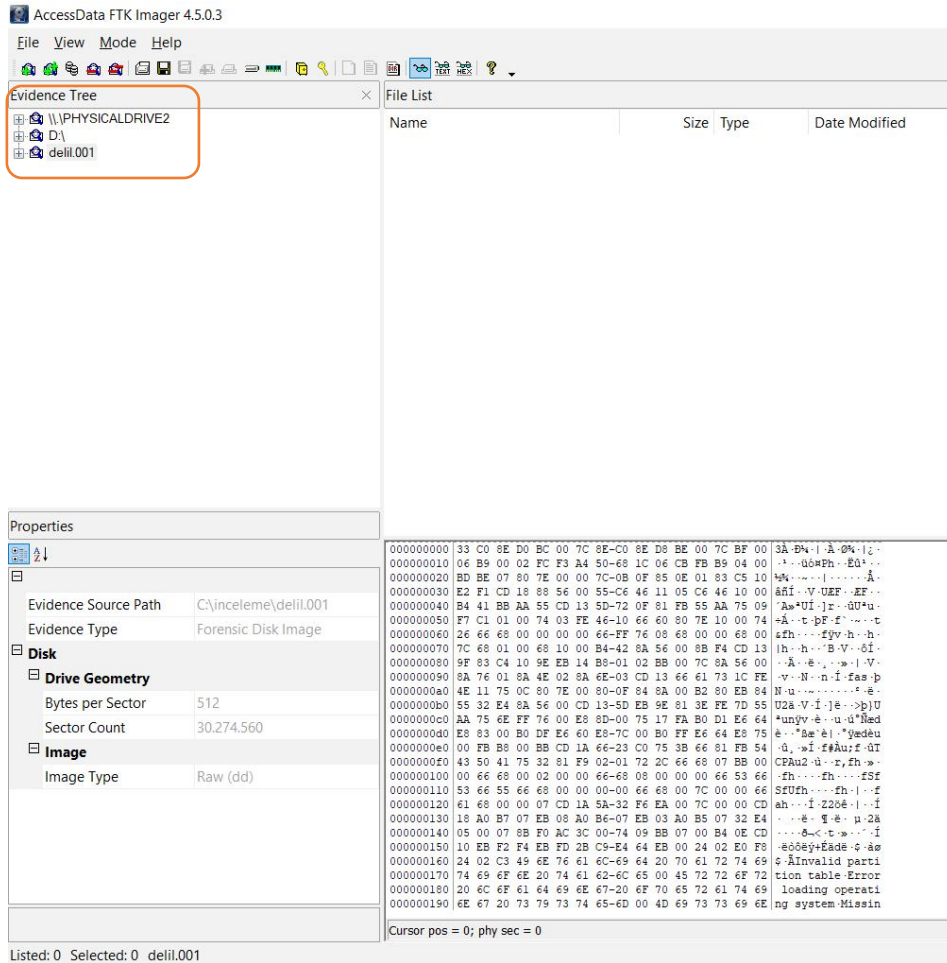
- Açılan sekmede inceleme yapılacak kaynağın tipi seçilmelidir.



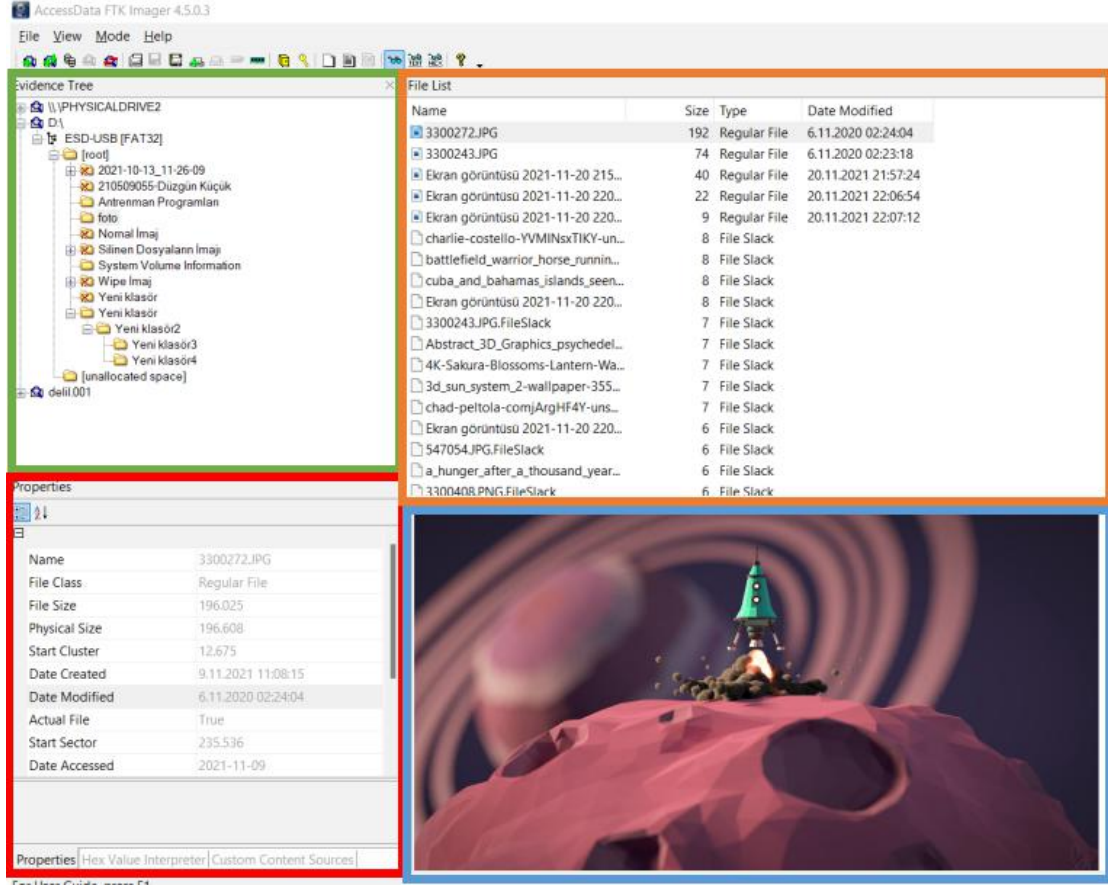
- Kaynağın tipi seçildikten sonra cihaz içerisinde bulunan kaynağın yolu seçilmelidir.



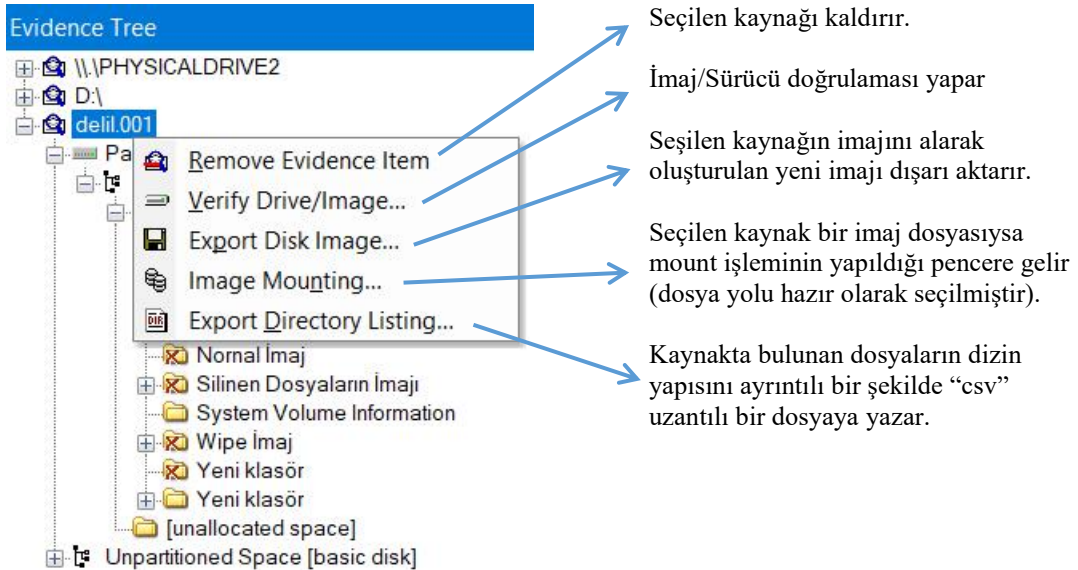
- Not: İstenildiği takdirde bu adımlar tekrardan uygulanıp birden fazla inceleme kaynağı için aynı anda inceleme yapılabilir.



- FTK Imager’de inceleme yapılırken inceleme yapan kişinin genel olarak yararlandığı 4 ana bölüm bulunmaktadır. Bu bölümler dizin hiyerarşisinin gösterildiği bölüm, dosyaların gösterildiği bölüm, dosyalara ait özizlemenin yapıldığı bölüm ve dosyalara ait metadataların bulunduğu bölümlerdir.



- İçeri aktarılan delil kaynaklarının üzerine fare ile sağ tıklanıldığında 5 farklı seçenek çıkmaktadır.



- Csv dosyası örneği.

1	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
2	[root]	Partition 1\ESD-USB [FAT32]\[root]\	8192				no
3	VBR Partition 1\ESD-USB [FAT32]\VBR	512					no
4	reserved sectors	Partition 1\ESD-USB [FAT32]\reserved sectors	1656120				no
5	[unallocated space]	Partition 1\ESD-USB [FAT32]\[unallocated space]\	0				no
6	FAT1	Partition 1\ESD-USB [FAT32]\FAT1	7560192				no
7	FAT2	Partition 1\ESD-USB [FAT32]\FAT2	7560192				no
8	System Volume Information	Partition 1\ESD-USB [FAT32]\[root]\System Volume Information\	8192	2021-Jun-11 20:24:34.360000	2021-Jun-11 20:24:36		no
9	Silinen Dosyaların İmajı	Partition 1\ESD-USB [FAT32]\[root]\Silinen Dosyaların İmajı\	8192	2021-Oct-28 10:53:18	2021-Oct-28 10:53:18		yes
10	2021-10-13_11-26-09	Partition 1\ESD-USB [FAT32]\[root]\2021-10-13_11-26-09\	8192	2021-Oct-28 11:32:27	2021-Oct-28 11:32:27		yes
11	Kali-linux-20	Partition 1\ESD-USB [FAT32]\[root]\Kali-linux-20	3814272000	2021-Jun-11 20:23:100.680000	2021-May-06 18:35:34		yes
12	Wipe image.log	Partition 1\ESD-USB [FAT32]\[root]\Wipe image.log	1443	2021-Oct-28 10:05:52.850000	2021-Oct-25 15:04:32		yes
13	Ganache-2.5.4-win-x64.appx	Partition 1\ESD-USB [FAT32]\[root]\Ganache-2.5.4-win-x64.appx	195574435	2021-Oct-28 10:05:57.180000	2021-Oct-19 18:07:04		yes
14	Yeni Microsoft Word Macro-Enabled Document.docm	Partition 1\ESD-USB [FAT32]\[root]\Yeni Microsoft Word Macro-Enabled Document.docm	0	2021-Oct-28 10:11:58.370000	2021-Oct-28 10:11:58.370000		yes
15	Yeni Metin Belgesi.txt	Partition 1\ESD-USB [FAT32]\[root]\Yeni Metin Belgesi.txt	22	2021-Oct-28 10:12:10.960000	2021-Oct-28 10:12:18		yes
16	Kayıt.m4a	Partition 1\ESD-USB [FAT32]\[root]\Kayıt.m4a	266355	2021-Oct-28 10:13:12.720000	2021-Oct-28 10:12:58		yes
17	Yeni PPTX Presentation.pptx	Partition 1\ESD-USB [FAT32]\[root]\Yeni PPTX Presentation.pptx	0	2021-Oct-28 10:13:54.060000	2021-Oct-28 10:13:56		yes
18	Normal İmaj	Partition 1\ESD-USB [FAT32]\[root]\Normal İmaj\	8192	2021-Oct-28 10:40:38	2021-Oct-28 10:40:38		yes
19	Wipe İmaj	Partition 1\ESD-USB [FAT32]\[root]\Wipe İmaj\	8192	2021-Oct-28 11:32:27	2021-Oct-28 11:32:26		yes
20	cuba and bahamas islands seen from space wallpaper-3554x1999.jpg	Partition 1\ESD-USB [FAT32]\[root]\cuba and bahamas islands seen from space wallpaper-3554x1999.jpg	18				
21	3d sun system 2 wallpaper-3554x1999.jpg	Partition 1\ESD-USB [FAT32]\[root]\3d sun system 2 wallpaper-3554x1999.jpg	681856	2021-Nov-09 11:08:13.490000	2021-Jun-05 05:18:		
22	4K-Patterns-Fractal-Twisted-Multicolored-Wallpaper-3840x2160.jpg	Partition 1\ESD-USB [FAT32]\[root]\4K-Patterns-Fractal-Twisted-Multicolored-Wallpaper-3840x2160.jpg	25				
23	4K-Sakura-Blossoms-Lantern-Wallpaper-3840x2160.jpg	Partition 1\ESD-USB [FAT32]\[root]\4K-Sakura-Blossoms-Lantern-Wallpaper-3840x2160.jpg	2770536	2021-Nov-09 11:08:13.7			
24	156899.JPG	Partition 1\ESD-USB [FAT32]\[root]\156899.JPG	767722	2021-Nov-09 11:08:14.020000	2021-Nov-07 11:52:36		yes
25	147054.JPG	Partition 1\ESD-USB [FAT32]\[root]\147054.JPG	1550811	2021-Nov-09 11:08:14.110000	2021-Nov-07 11:50:28		yes
26	1111675.PNG	Partition 1\ESD-USB [FAT32]\[root]\1111675.PNG	19664559	2021-Nov-09 11:08:14.270000	2021-Nov-07 11:53:48		yes
27	1300243.JPG	Partition 1\ESD-USB [FAT32]\[root]\1300243.JPG	74777	2021-Nov-09 11:08:15.810000	2020-Nov-06 02:23:18		yes
28	1300272.JPG	Partition 1\ESD-USB [FAT32]\[root]\1300272.JPG	196025	2021-Nov-09 11:08:15.850000	2020-Nov-06 02:24:04		yes
29	1300408.PNG	Partition 1\ESD-USB [FAT32]\[root]\1300408.PNG	1526725	2021-Nov-09 11:08:15.900000	2020-Nov-06 02:25:20		yes

- Dizinlerin üzerine fare ile sağ tıklanıldığında 5 farklı seçenek çıkmaktadır.

Seçilen klasörü içinde bulunan dizin ve dosyalarla beraber dışarı aktarır.

Seçilen klasörün içindeki dosyaların dosya yollarını, md5 ve sha1 hash değerlerini “csv” uzantılı bir dosyaya yazar.

Seçilen klasörün imajını alarak dışarı aktarır.

Seçilen dosya yada klasörün programın sola alt penceresinde bulunan bölüme eklemesini sağlar (seçilen dosya yada klasörler birleştirilip imajları alınabilir).

● Dışarı aktarılan hash listesi örneği.

```
C:\> inceleme > hash_list_foto.csv
1 MD5_SHA1_FileNames
2 "d0b8dec8bcb79a0241b52c8598270566", "c93c37577e8278da35a4b8643b733ce39516fe71", "D:\ESD-USB [FAT32]\[root]\foto3d_sun_system_2-wallpaper-3554x1999.jpg"
3 "4e7fc5d5964dc8731a001f0e034132c", "c9978dd1937440db691499860c1cb11935bc32", "D:\ESD-USB [FAT32]\[root]\foto4K_Patterns-Fractal-Twisted-Multicolored-Wallpaper-3840x2160.jpg"
4 "83a19b1a30530bee4f92eb2778e05786", "2bc982cf85648a04075b0dd778d4f1ac376dd266", "D:\ESD-USB [FAT32]\[root]\foto4K_Sakura- Blossoms-Lantern-Wallpaper-3840x2160.jpg"
5 "d576c3f56717f2d1b3dd127adea2ef1", "4f5cbf4b411bb322c3da1ab3724edfbdab3df1a1", "D:\ESD-USB [FAT32]\[root]\foto156899.JPG"
6 "5f682fazc5b4de6dcb188e024e38d8c", "30a3bd98b4ef9ac9472d451ee176f8b67019853c", "D:\ESD-USB [FAT32]\[root]\foto547054.JPG"
7 "8c5983d38694593ddfbcc4dcfcb8bd59d", "9ddc394532bf1e2d209b9d795534aedb31dc8c7", "D:\ESD-USB [FAT32]\[root]\foto1111675.PNG"
8 "0274b0a0e963472e49e742b5fd11c44", "e4d5cc3191b3292c54392055899c0ca1cfcfae9", "D:\ESD-USB [FAT32]\[root]\foto3380243.JPG"
9 "a138b120d16a2671f4dc5f5e327b29a", "e9a803a7b64227211b40f924d0f6637439c1f0c9b", "D:\ESD-USB [FAT32]\[root]\foto3380272.JPG"
10 "ef4892e3b6e98209d46ab9b3e1ca7", "58501bc756f21800a0232d09a064f534237da", "D:\ESD-USB [FAT32]\[root]\foto3380408.PNG"
11 "1420f4061a656da93879c3453eff1ed7", "742a6a1be2d9e7cced904f65237c0246df8cbaf2", "D:\ESD-USB [FAT32]\[root]\fotoa_hunger_after_a_thousand_year_nap-wallpaper-2560x1440.jpg"
12 "7974e37e17c9f4de0457b473ad3840", "07e4b7448f1af15f8ded1fea90331b4842f7dd4", "D:\ESD-USB [FAT32]\[root]\fotoAbstract_3D_Graphics_psychedelic_nebula_space_6000x4000.jpg"
13 "6a520f8b78fbc32ed7cbe0e21858ef", "c32836607f9cbb1c7b1f3baacd3b465b5a126aef", "D:\ESD-USB [FAT32]\[root]\fotoadolof_bock_painting-wallpaper-2560x1440.jpg"
14 "02874d227c6ede9a3881c631c213921", "283c6ccf001a670e0f7a3429cc95998e4a829b9b", "D:\ESD-USB [FAT32]\[root]\fotoalex_robert_sbwuopIUPI_unsplash.jpg"
15 "463db7fb81fca9a90500667a621acbb20", "2c1620240e4683a422f37a865584f79d05c30575", "D:\ESD-USB [FAT32]\[root]\fotoaurora_borealis_3-wallpaper-1920x1080.jpg"
16 "b23d2a2dc2cd4aeaf716c1af28338da", "354c67c24b0e9db142e75f68731f5424315ea22", "D:\ESD-USB [FAT32]\[root]\fotoautumn_stroll-wallpaper-2560x1440.jpg"
17 "b76be525d37fae4b0842966a361c642b", "ee79b1045b5a5f00a5885b545ab718bd116381e28", "D:\ESD-USB [FAT32]\[root]\foto_b76be525d37fae4b0842966a361c642b.jpg"
18 "3b56a59ca3d8011162437c7e4856220", "ccca41c0ec41835902c4e57dbdb40815eb7757", "D:\ESD-USB [FAT32]\[root]\fotobattlefield_warrior_horse_running_smoke_illustration-wallpa"
19 "a15c5bc3c83166a0bce923b8269fef", "044cb2e9feb3d1eb46fc78cd687992d9843bd559", "D:\ESD-USB [FAT32]\[root]\fotobrown_snowy_mountain-1054201.jpg"
20 "c6160d35d073354eae5d1ec9ae4cf", "a30498e70d4ba09ab415930dded42d2e93f10972b", "D:\ESD-USB [FAT32]\[root]\fotocaptain-wallpaper-2560x1440.jpg"
21 "b789e204f9f39044d07bf8b82e96e41ad", "c2995a6fa62c8e387117ceebb3ea19c6da2760e", "D:\ESD-USB [FAT32]\[root]\fotochad_peltola-comjArgH4Y_unsplash.jpg"
22 "3a3d4e113431d0e6cc3a24b69becfa6c", "a87c606267f580072c702fa37dc5674b640f01e", "D:\ESD-USB [FAT32]\[root]\fotocharlie_costello-VYMNsxTKY_unsplash.jpg"
23 "1f6d421d4c9af8bcc5d29f9c4c2a4db", "71d6f3271abee9396fdab6a7fa1f8deb595f38", "D:\ESD-USB [FAT32]\[root]\fotochinese_fisherman_painting-wallpaper-2560x1440.jpg"
24 "d10727953298c57f92ddef094643c65", "07d6c266c9ca1b9d11d6de1d73a98b837d4e98080", "D:\ESD-USB [FAT32]\[root]\fotocounter_strike_global_offensive_12-wallpaper-3840x2160.jpg"
25 "90cbe9ba80ec3d515ca386258c19b20d", "448a4baa7a1305f3d83d6530d610f480d96ab7aa", "D:\ESD-USB [FAT32]\[root]\foto_cuba_and_bahamas_islands_seen_from_space-wallpaper-3554x1999"
26 "b497fc79b914df2b8678499ae96fe98", "5b0c1d4b8772409bf89eb93686477a0c3a50b4068", "D:\ESD-USB [FAT32]\[root]\fotoEkran_görüntüsü_2021-11-20_215728.png"
27 "d4de9709d084f951051c61bc3a2dbb09", "d0e1a21a6706353a3da3883136a0ff6f570927a6", "D:\ESD-USB [FAT32]\[root]\fotoEkran_görüntüsü_2021-11-20_220650.png"
28 "61931777def34281572c482522f85e00", "54ed0170508435d42580f795c5d2a50992d805c", "D:\ESD-USB [FAT32]\[root]\fotoEkran_görüntüsü_2021-11-20_220709.png"
29 "a0e594ad78df8849196ah982fec1de7a", "50c18f6471a5a97b4a3224c5a6f9a8e869be48401", "D:\ESD-USB [FAT32]\[root]\fotoEkran_görüntüsü_2021-11-20_220732.png"
30 "5643b2d8467209935de4279749ac5a", "9bae244094e912d195d24a4f84cdcf8674455bce1a", "D:\ESD-USB [FAT32]\[root]\fotoEkran_görüntüsü_2021-11-20_220753.png"
```

● “Costum Content Image” bölümü.

Custom Content Sources

Evidence:File System Path File	Options
D:\:ESD-USB [FAT32] \[root]\foto *	Wildcard,Consider Case,Include Su...
D:\:ESD-USB [FAT32] \[root]\foto_cuba_and_bahamas...	Exact
D:\:ESD-USB [FAT32] \[root]\Yeni klasör\Yeni klasör2 ...	Wildcard,Consider Case,Include Su...
D:\:ESD-USB [FAT32] \[root]\Normal İmaj *	Wildcard,Consider Case,Include Su...

New

Edit

Remove

Remove All

Create Image

Properties

Hex Value Interpreter

Custom Content Sources

Seçilen dosya ve klasörlerin imjını alma, listeden kaldırma ve listeye yeni eleman ekleme işlemleri bu pencereden yapılabilir.

- Costum Content Image alanında bulunan “Crate Image” butonuna tıklayarak seçilen dosyaların imajları alınabilir.

Bu bilgisayar > Yerel Disk (C:) > inceleme				Ara: inceleme
Ad	Değiştirme tarihi	Tür	Boyut	
aa.ad1	22.11.2021 14:01	AD1 Dosyası	59.114 KB	
aa.ad1.csv	22.11.2021 14:01	Comma Separated...	31 KB	
aa.ad1.txt	22.11.2021 14:01	Metin Belgesi	1 KB	

Üstteki görsel, “Costum Content Imag” kısmındaki dosya ve klasörlerin imajının alınması işlemiyle elde edilen dosyaları göstermektedir.

- “txt” uzantılı dosya içerisinde, imajın içine eklenen dosya ve klasörlerin ayrıntılı bilgileri bulunmaktadır.

```
aa.ad1.txt - Not Defteri
Dosya Düzenle Biçimlendir Görüntüle Yardım
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:









-----

Information for C:\inceleme\aa.ad1:
[Custom Content Sources]
D:\ESD-USB [FAT32][root]|foto|*(Wildcard,Consider Case,Include Subdirectories)
D:\ESD-USB [FAT32][root]|foto|cuba_and_bahamas_islands_seen_from_space-wallpaper-3554x1999.jpg(Exact)
D:\ESD-USB [FAT32][root]|Yeni klasör|Yeni klasör2|Yeni klasör4|*(Wildcard,Consider Case,Include Subdirectories)
D:\ESD-USB [FAT32][root]|Nornal İmaj|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum: 56a1158085adf8164141b8c6a7e3bc3c
SHA1 checksum: 7ce4f865d0c61a87481b641c63b8af769236954c

Image information:
Acquisition started: Mon Nov 22 14:01:11 2021
Acquisition finished: Mon Nov 22 14:01:16 2021
Segment list:
C:\inceleme\aa.ad1

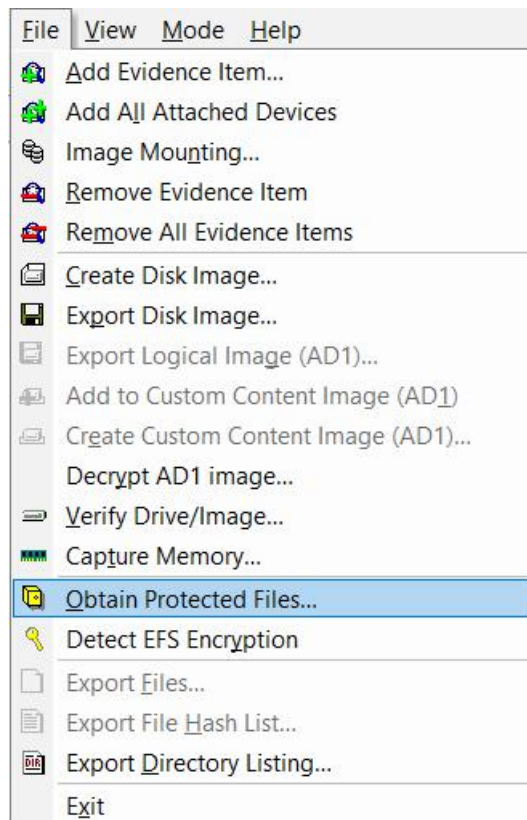
St 1, Süt 1 %100 Windows (CRLF) Ürün Reçetesi ile L
```

- Dosyaların üzerine fare ile sağ tıklanıldığında 3 farklı seçenek çıkmaktadır.

File List			
Name	Size	Type	Date Modified
 GURAY's HYPHERTROPHY no.1.pdf	111	Regular File	9.02.2021 22:18:42
 Balkaya Texas Method.xlsx	24	Regular File	22.03.2021 17:04:38
 DUZGUN_HYPHERTROPHY 3+1.x...	13	Regular File	10.10.2021 11:43:28
 DUZGUN_HYPHERTROPHY 3+1.x...	13	Regular File	26.09.2021 14:31:34
 DUZGUN_HYPHERTROPHY 3+1.x...		File Slack	
 DUZGUN_HYPHERTROPHY 3+1.x...		File Slack	
 DUZGUN_HYPHERTROPHY 3+1.x...		File Slack	
 DUZGUN_HYPHERTROPHY 3+1.x...		File Slack	

1. FTK Imager ile Korunan Kayıt Defteri Dosyalarına Ulaşma

- Bu işlem için File menüsünden “Obtain Protected Files...” seçeneğine tıklanmalı.

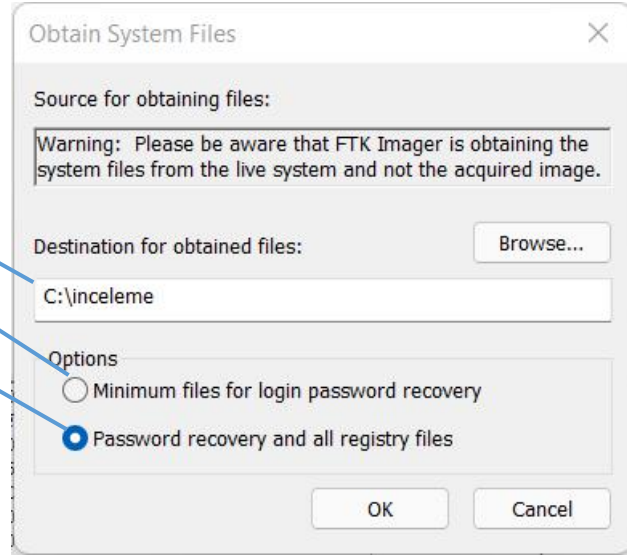


- Açılan pencerede dosya yolunun seçtikten sonra programın hangi dosyaları getireceği de seçilmelidir.

Dosyaların kaydedileceği yer

Sadece parola dosyalarını getirir

Tüm korumalı dosyaları getirir



- Çıkarılan Korumalı Dosyalar.

Bu bilgisayar > Yerel Disk (C:) > inceleme				Ara: inceleme	
Ad	Değiştirme tarihi	Tür	Boyut		
Users	22.11.2021 15:09	Dosya klasörü			
userdiff	18.11.2021 17:46	Dosya	8 KB		
default	22.11.2021 00:02	Dosya	512 KB		
SAM	22.11.2021 00:02	Dosya	128 KB		
SECURITY	22.11.2021 00:02	Dosya	32 KB		
software	22.11.2021 00:02	Dosya	91.392 KB		
system	22.11.2021 00:02	Dosya	16.384 KB		

- Tüm işlemler bittikten sonra File menüsü altında bulunan “Remove All Evidence Items” seçeneği ile içeri aktarılan tük kaynaklar kapatılabilir.

