

FORENSİC EXPLORER KULLANIM KLAVUZU

İÇİNDEKİLER

- 1.Giriş**
- 2.Forensic Explorer Nedir ?**
- 3.Forensic Explorer Kurulumu**
- 4. Evidence Penceresi**
- 5. File System Penceresi**
- 6. Keyword Search Penceresi**
- 7. Index Search Penceresi**
- 8. Email Penceresi**
- 9. Registry Penceresi**
- 10. Bookmarks Penceresi**
- 11. Reports Penceresi**
- 12. Scripts Penceresi**
- 13. Genel Kısım**

1.Giriş

Forensic Explorer yazılımı, Adli Bilişim alanında önemli sayılan yazılımlar arasında yer alan ücretli bir yazılımdır.

Bu kullanım klavuzunda Forensic explorer nedir, Forensic explorer'ın kurulumu nasıl yapılır, Forensic explorer'da inceleme nasıl yapılır bunun gibi soruların cevabını bulunabilir.

2.Forensic Explorer Nedir ?

Forensic Explorer GetData tarafından geliştirilmiş bir adli inceleme programıdır.

İmaj alma, hash hesaplama, detaylı inceleme yapmaya olanak sağlar. Bunların hepsi klavuzda detaylı olarak görülecektir.

3.Forensic Explorer Kurulum

Forensic explorer yazılımını GetData'nın web sitesinden indirebilirsiniz.

30 günlük değerlendirme sürüm anahtarı talep edilebilir. Talepten sonra aşağıdaki linkten indirme yapılır:

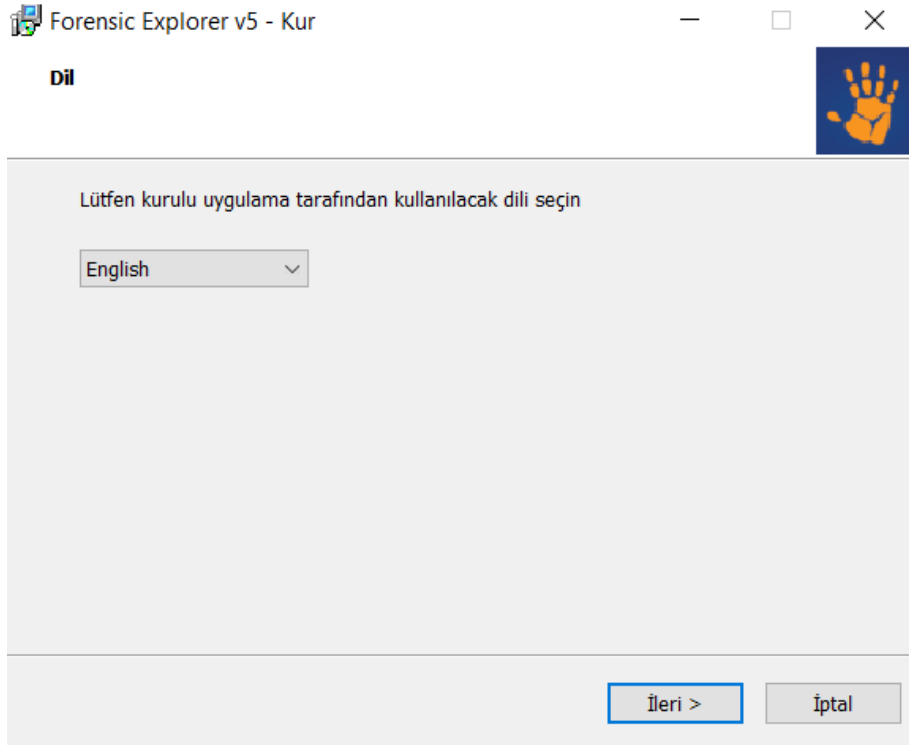
<https://getdataforensics.com/product/forensic-explorer-fex/download/>

Download

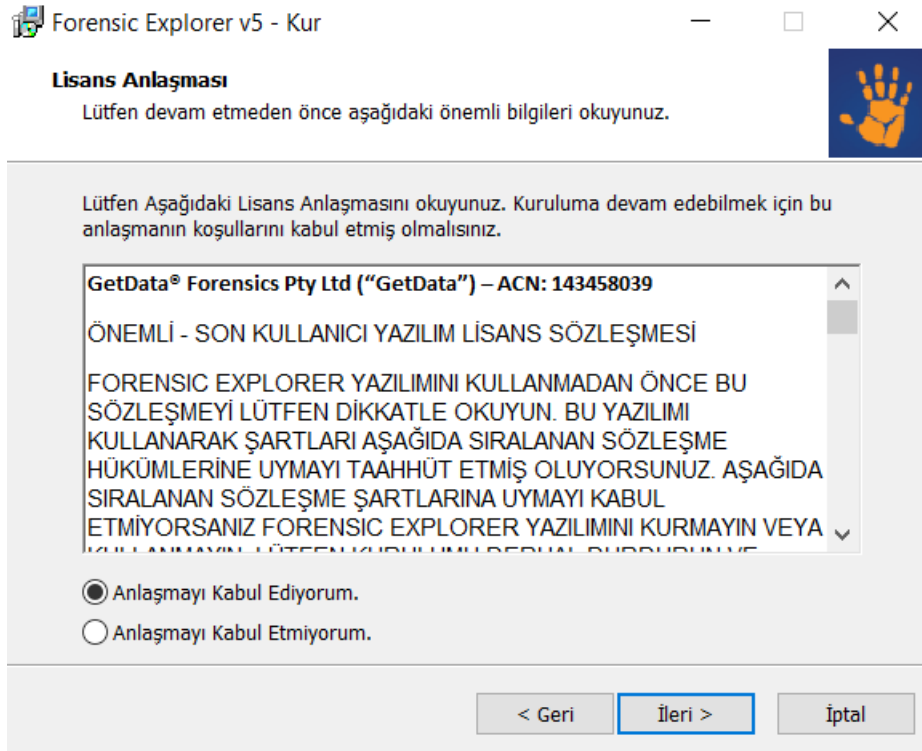
Forensic Explorer 64 bit

- ✓ Forensic Explorer - Full - v5.4.8.2320 - 26 Nov 2021
- ✓ Forensic Explorer - Evaluation - v5.4.8.2320 - 26 Nov 2021

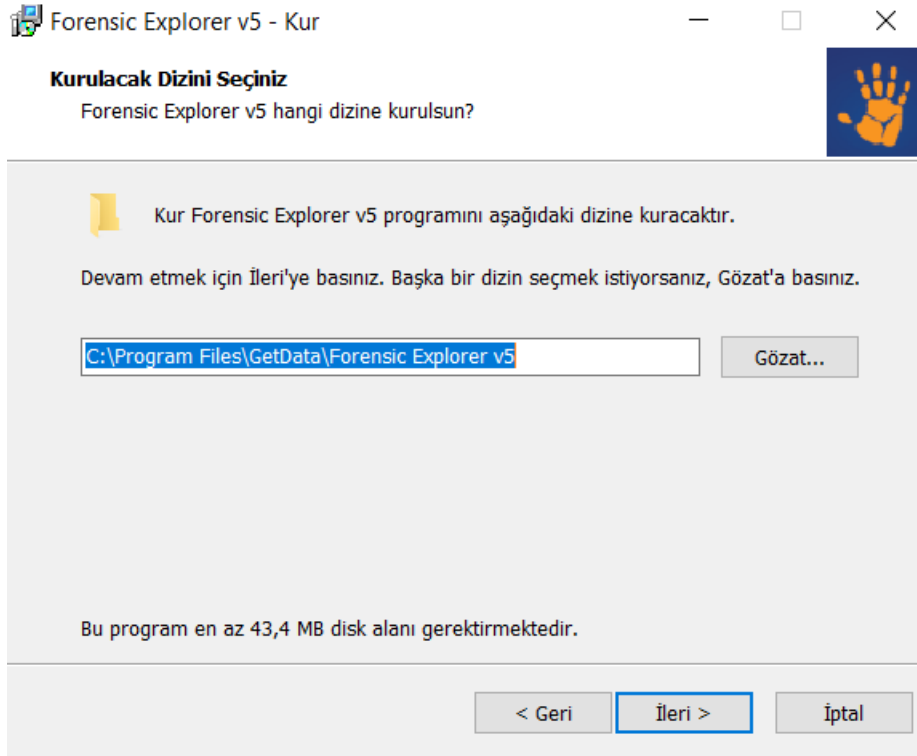
- İndirmek için tıklanır.



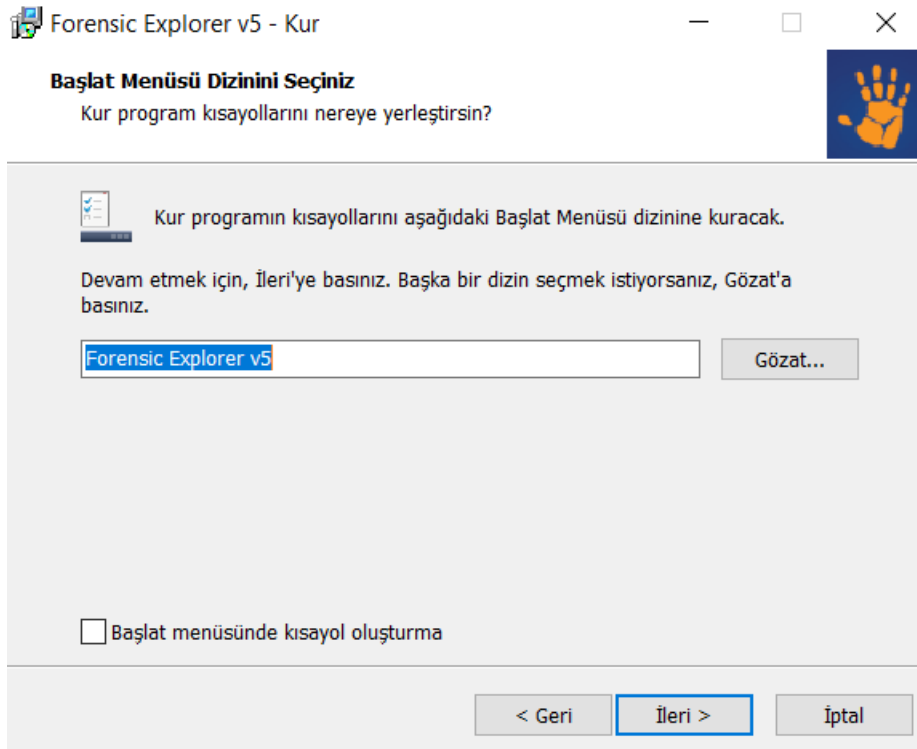
- Yönetici olarak çalıştırıldıktan sonra dil ayarlaması yapılır.



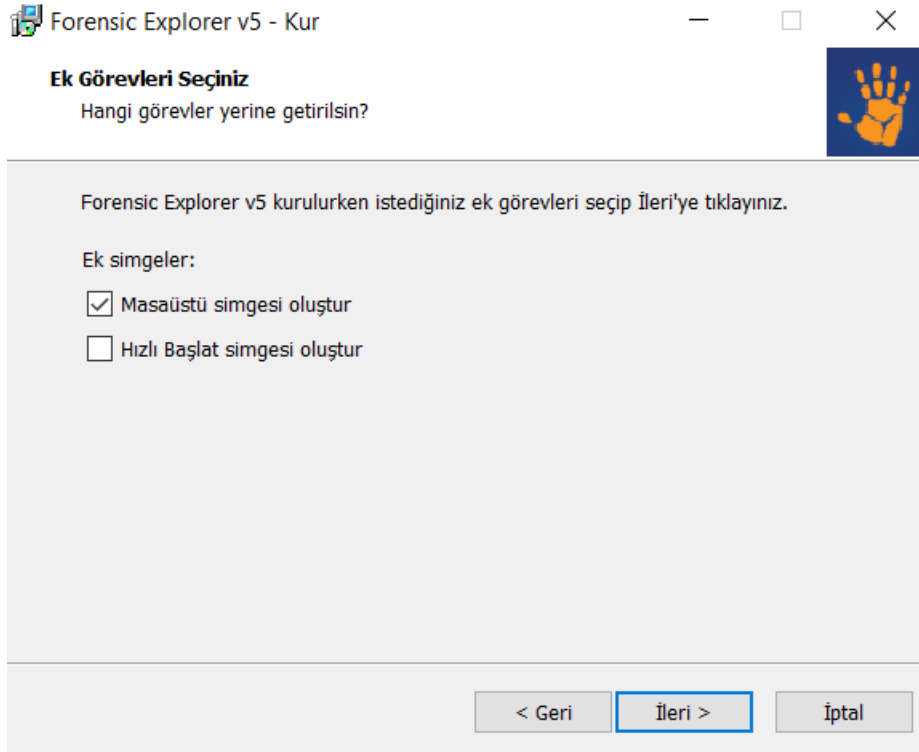
- Kurulumu gerçekleştirebilmek için Anlaşmayı Kabul Ediyorum'a tıklanması gerekir.Ardından ileri denir.



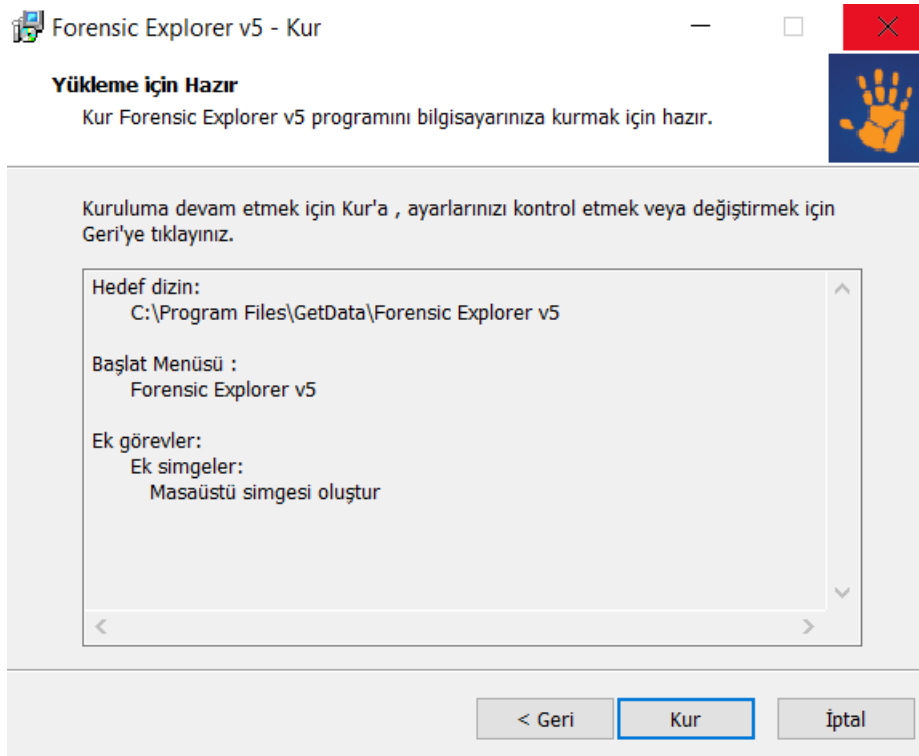
- Forensic Explorer programının kurulacağı dosya yolunu seçip İleri denir.



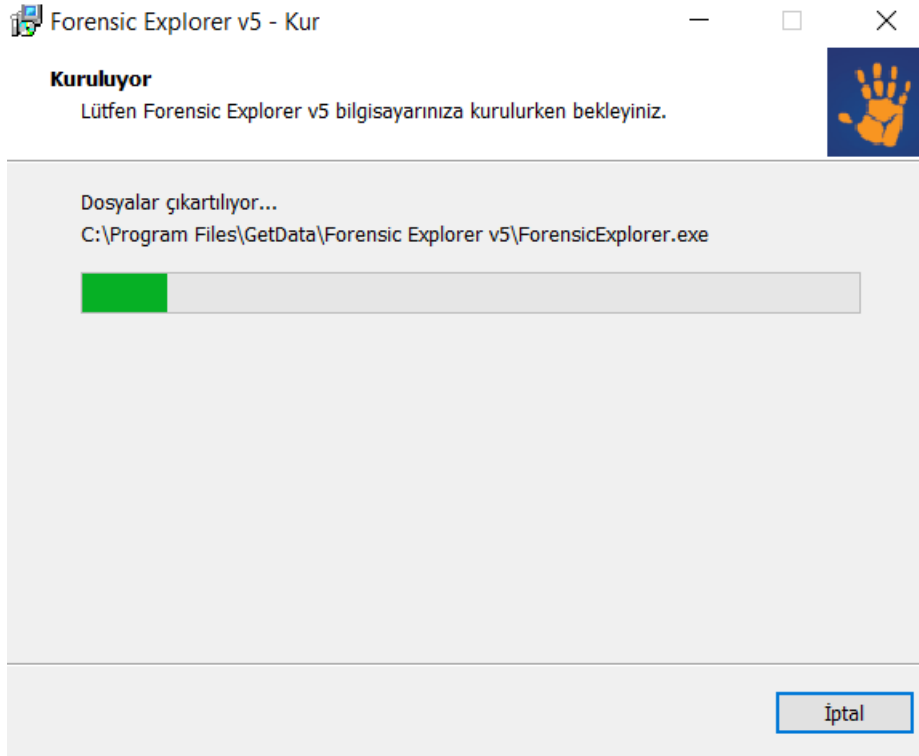
- Forensic Explorer programının masaüstündeki ismi belirlenir.



- Masaüstü kısayol oluşturmak için seçme yapılabilir.



- Seçimler yapıldıktan sonra Kur butonuna basılıp kurma işlemi başlatılır.



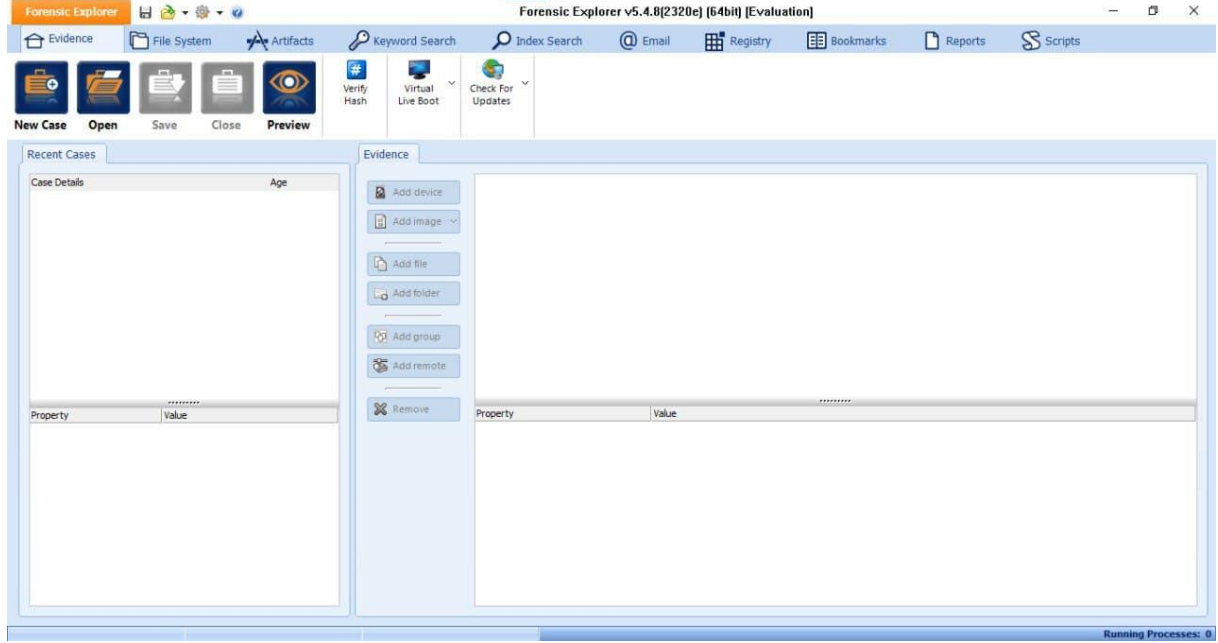
- Kurulumun başladığı ve devam ettiği görülür.



- Kurma işlemi tamamlandıktan sonra Son butonuna tıklanılır.

4.Evidence Penceresi


- Aşağıda Evidence penceresi gösterilmiştir.



New Case




- Aşağıda New Case penceresi gösterilmiştir. Yukarıdaki New Case butonuna tıklanıldığında yeni bir dava oluşturulur.

 New Case

Case Name:

Investigator:

Cases Folder: 

Case Notes:

Case Number:

Case Time Zone Settings

TimeZone:

TimeZone Name:

Daylight Savings:

STD/DLS Bias: / minutes

Case Created:

Case Name: Vakanın ismi yazılır.

Investigator: İnceleme yapan kişinin ismi yazılır.

Cases Folder: Vakanın kaydedileceği yol seçilir.

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

Case Number: Kanıt numarası yazılır.

TimeZone: Gelen vakanın hangi ülkeden geldiği belli değilse TimeZone alanı Local Time seçilir. Local Time'ı seçtikten sonra, daha sonraları vakanın tarih ve saat ayarlaması yapılabilir.

- New butonuna tıklarsak aşağıdaki pencere açılır.

Update Investigator ×

Investigator ID: {DEE974BA-8D53-43B5-925D-45052FCE34DC}

Full Name:

Title/Position:

Organization:

Department:

Contact ☒ Address ☐

Phone:

Fax:

Cell/Mobile:

Email:

URL:

Investigator ID: Bu ID eşsiz bir ID'dir. Her insanda herkeste farklıdır.

Full Name: İnceleyecinin ismi yazılır.

Ve inceliyici hakkında yazılan diğer bilgiler yazılır.

Open

- Aşağıdaki Open butonuna tıklanıldığında istenilen kayıtlı dava açılır .



Save

- Aşağıdaki Save butonuna tıklanıldığında oluşturulan dava kaydedilir .



Close

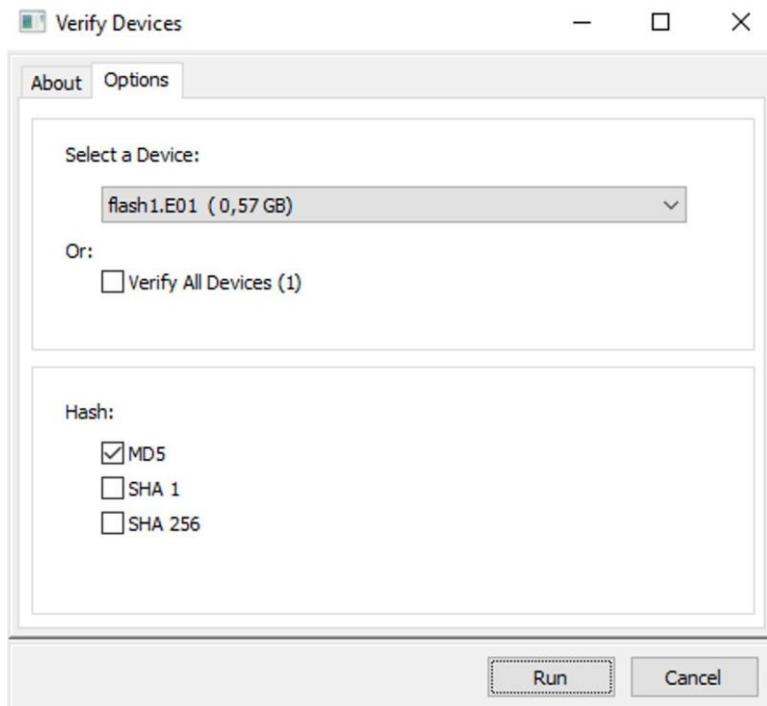
- Aşağıdaki Close butonuna tıklanıldığında açık olan dava kapatılır. .



Verify Hash



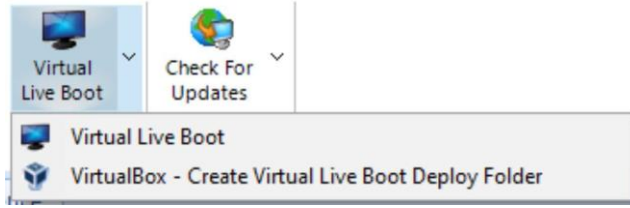
- Seçilen formatta(MD5,SHA1,SHA256) Hash doğrulaması sağlanabilir.Başlatıldığında hash değerini hesaplar. Hesapladıktan sonra rapor dosyasındaki hash ile hesapladığı hash'i karşılaştırır. Aynı olduğunu ispatladıktan sonra vaka üzerinde çalışılabilir.



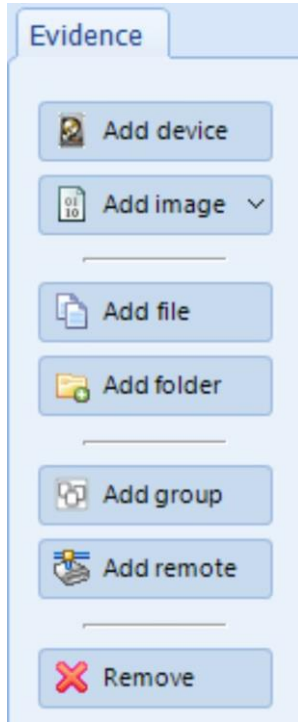
Virtual Live Boot



- Fiziksel bir imaj dosyasını canlandırmak için kullanılır.

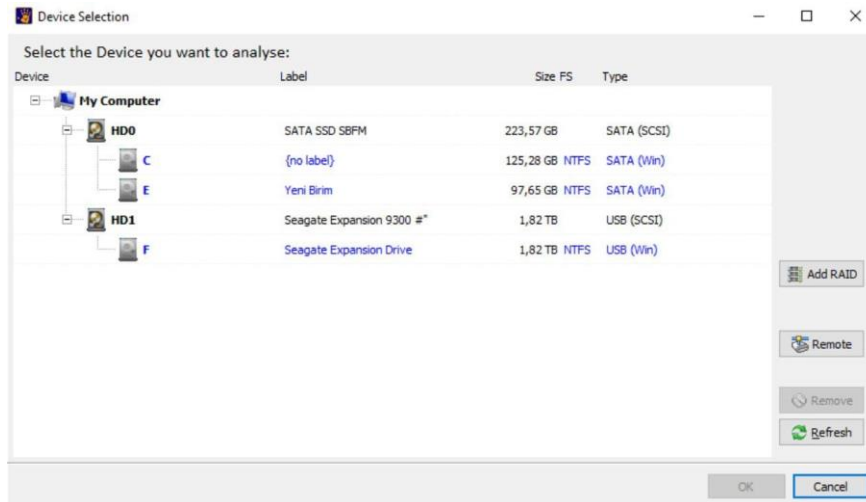


İmajı açma kısımları:



Add device

Canlı olarak fiziksel imaj incelenir.



Add RAID: RAID sistemi eklenebilir. Raid birden fazla diske veri kaydetmedir. 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 sağlar.

Refresh: Yenilemek.

Add image

İstenilen imaj dosyası seçilir.

Add file

Sadece bir dosya incelenmek isteniyorsa seçilir.

Add group

Aynı olayda farklı kişilerin incelemesi yapılacaksa seçilir.


Seçtikten sonra prosesler ve saat dilimi ayarlarını yap çıkar. Vakanın zaman dilimini seçtikten sonra aynı şekilde öğrendikten sonra vakanın incelenecek zaman dilimini seçilir.

















Evidence Processor Penceresi:

İncelenecek imaj seçilip OK'a basıldıktan sonra Evidence Processor penceresi çıkar. Bu pencerede farklı imajlara farklı prosesler uygulanabilir.

Evidence Processor

Evidence Name:

(DEFAULT) 

Tasks	Enabled
FileSystem	 <input checked="" type="checkbox"/>
Process in Parallel	 <input checked="" type="checkbox"/>
Verify Device Hash	 <input type="checkbox"/>
Search for ISO Tracks (CD/DVD)	 <input type="checkbox"/>
Search for MBRs	 <input checked="" type="checkbox"/>
Search for FileSystems	 <input checked="" type="checkbox"/>
Signature Analysis	 <input type="checkbox"/>
Expand Compound Files	 <input type="checkbox"/>
Process in Parallel	 <input checked="" type="checkbox"/>
Triage	 <input type="checkbox"/>
Hash Files	 <input type="checkbox"/>
Extract Metadata	 <input type="checkbox"/>
File Carve	 <input type="checkbox"/>
New Index	 <input type="checkbox"/>
Cache Thumbnails	 <input type="checkbox"/>
Cache Video Thumbnails	 <input type="checkbox"/>

Adjust Time Zone Settings

TimeZone:

TimeZone Name:

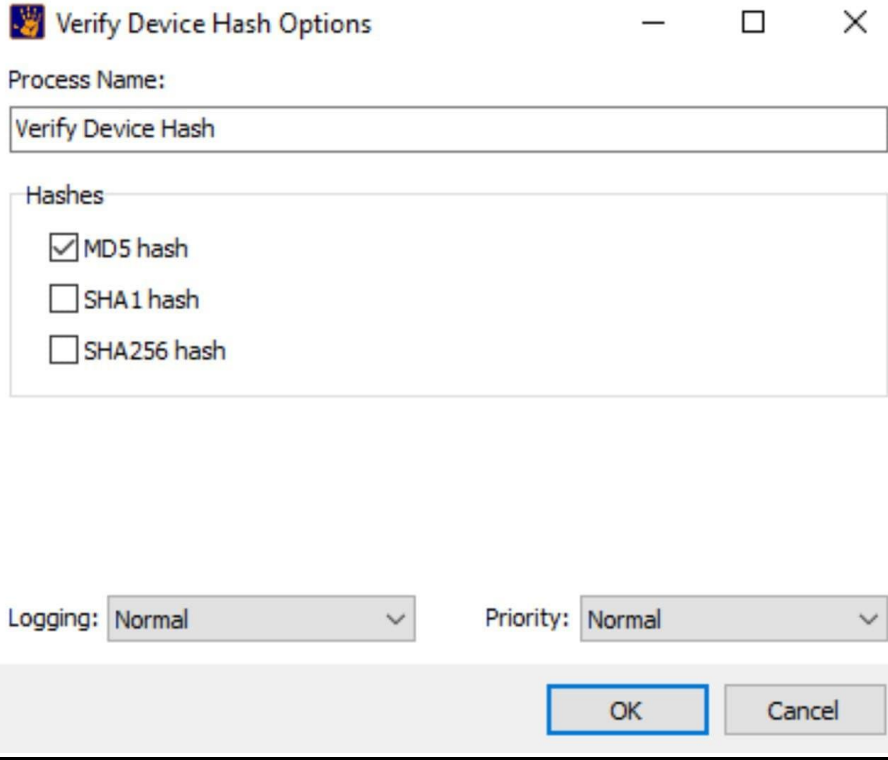
Daylight Savings:

STD/DLS Bias: / minutes

FileSystem

Yapılacak proseslerin bütünüdür. Seçmezsek proses penceresi aktif hale gelmez.

Verify Device Hashes



The image shows a Windows-style dialog box titled "Verify Device Hash Options". It has a standard title bar with minimize, maximize, and close buttons. The dialog contains a "Process Name:" label followed by a text input field containing "Verify Device Hash". Below this is a section labeled "Hashes" containing three checkboxes: "MD5 hash" (checked), "SHA1 hash" (unchecked), and "SHA256 hash" (unchecked). At the bottom, there are two dropdown menus: "Logging:" set to "Normal" and "Priority:" set to "Normal". The bottom right corner features "OK" and "Cancel" buttons.

Ayarlarına tıkladığımız zaman imaj dosyasının hangi formatta istiyorsak o formatta hash değerini hesaplayabiliriz.İmaj dosyasının bütününün hash'ini hesaplar.

Logging = Log tutma düzeyini belirliyoruz.


Priority = Bu proses için sistem kaynaklarını hangi özellikte kullanacağı seçilir.

Search for MBRs

Bilinmeyen MBR dosyalarının aranması için kullanılıyor.Disk bölümlerinin yönetilmesinde bilinen bilinmeyen dosyaların aranması taranması için kullanılır.

MBR, disk bölümlerini yönetiyor.

Signature Analysis

 Signature Analysis Options

Process Name:

Signature Analysis

Filetypes to determine:

- ☒ Archives
- ☒ Artifacts
- ☒ Camera
- ☒ Databases and Financials
- ☒ Documents
- ☒ Email
- ☒ Graphics
- ☒ Internet
- ☒ Microsoft Office
- ☒ Multimedia
- ☒ Music
- ☒ Text (WARNING: Slows Search)
- ☒ Video
- ☒ Apple OS
- ☒ Windows
- ☒ Operating System

Find:

Options

☐ Force determination

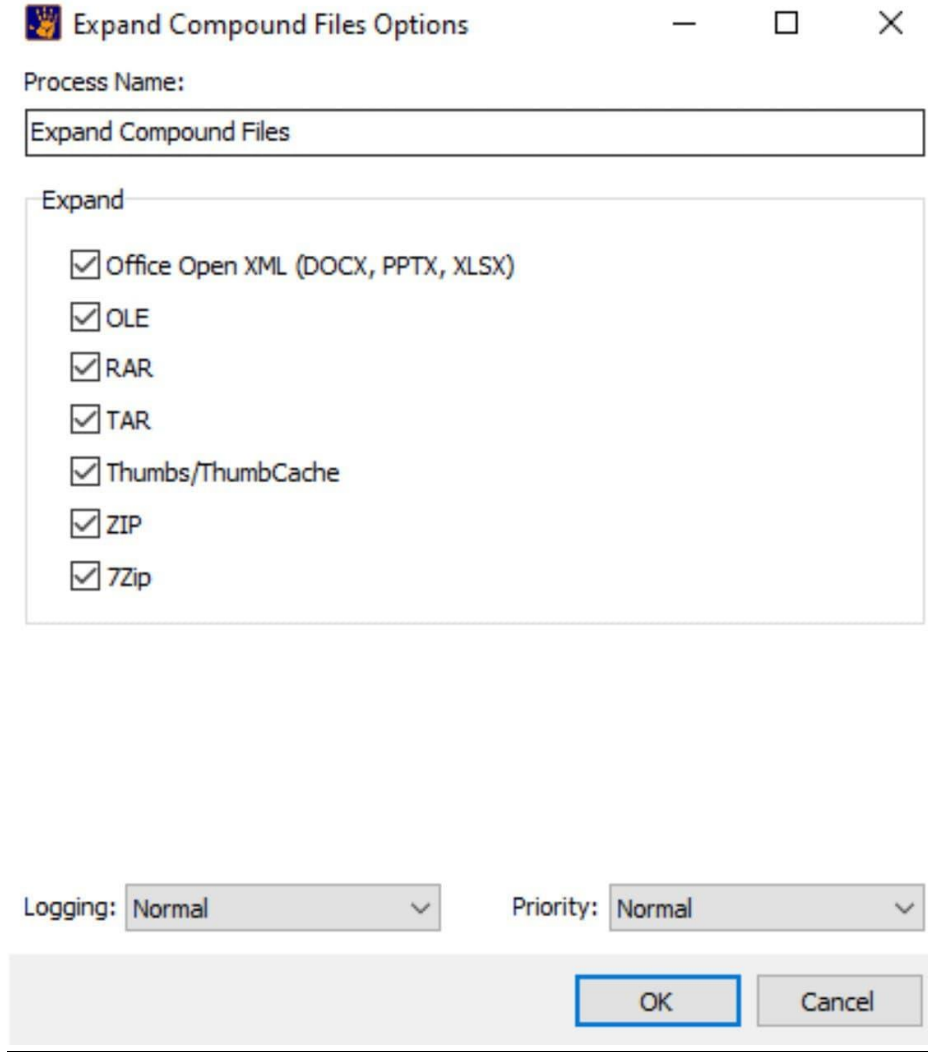
Insert new columns at position:

Logging:

Priority:

Dosya imza deęerlerinin tutulmasını saęlar.Bu pencere bir dosyanın geręek uzantısını bulmaya yarar.Bu pencerede tanınmıř dosya uzantıları var.Sistemin ayrıntılı bir bięimde dosya imza analizi yapmasını saęlar.

Expand Compound Files



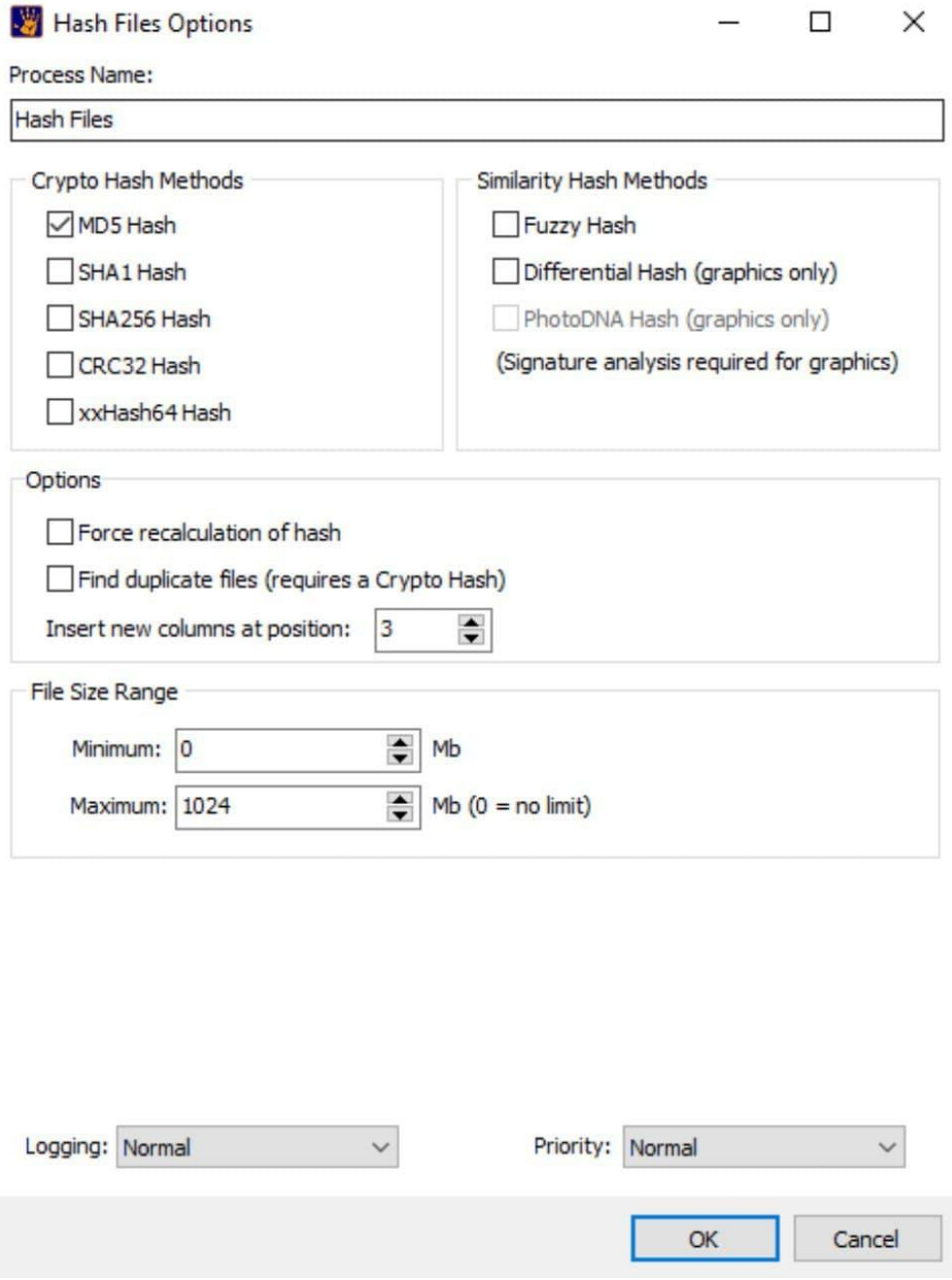
Tıklanıldığında tanıdığı sıkıştırılmış dosya uzantıları gözükür. Elimizdeki sıkıştırılmış dosya tek bir dosya olarak mı görülsün yoksa onun içerisindekileri gruptandırın mı, seçilen uzantılara göre bu belirlenir.

Thumbs/ThumbCache = Gruplara ayrılmış bir şekilde ön izleme yapılmasını sağlayan dosyalardır.

Triage

Triage raporu oluşturmaya yarar. Bir imaj dosyasının belli standart alanlarını gösterir. İmaj dosyasıyla ilgili ön bilgi alma sağlanır.

Hash Files

The image shows a Windows-style dialog box titled "Hash Files Options". It has a standard title bar with a minimize button, a maximize button (disabled), and a close button. The dialog is divided into several sections. At the top, there is a "Process Name:" label followed by a text box containing "Hash Files". Below this, there are two columns of hash methods. The left column, "Crypto Hash Methods", includes checkboxes for MD5 Hash (checked), SHA1 Hash, SHA256 Hash, CRC32 Hash, and xxHash64 Hash. The right column, "Similarity Hash Methods", includes checkboxes for Fuzzy Hash, Differential Hash (graphics only), and PhotoDNA Hash (graphics only), with a note "(Signature analysis required for graphics)" below. Below these columns is an "Options" section with checkboxes for "Force recalculation of hash" and "Find duplicate files (requires a Crypto Hash)", and a label "Insert new columns at position:" followed by a spinner box set to "3". Below the options is a "File Size Range" section with "Minimum:" and "Maximum:" labels, each followed by a spinner box and a unit label. The minimum is set to "0" Mb, and the maximum is set to "1024" Mb, with a note "(0 = no limit)". At the bottom, there are two dropdown menus for "Logging:" (set to "Normal") and "Priority:" (set to "Normal"). At the very bottom right, there are "OK" and "Cancel" buttons.

Hash Files Options

Process Name:

Hash Files

Crypto Hash Methods

- ☒ MD5 Hash
- ☐ SHA1 Hash
- ☐ SHA256 Hash
- ☐ CRC32 Hash
- ☐ xxHash64 Hash

Similarity Hash Methods

- ☐ Fuzzy Hash
- ☐ Differential Hash (graphics only)
- ☐ PhotoDNA Hash (graphics only)

(Signature analysis required for graphics)

Options

- ☐ Force recalculation of hash
- ☐ Find duplicate files (requires a Crypto Hash)

Insert new columns at position: 3

File Size Range

Minimum: 0 Mb

Maximum: 1024 Mb (0 = no limit)

Logging: Normal

Priority: Normal

OK Cancel

İmaj içerisindeki her bir dosyanın ayrı ayrı hash'ini hesaplamak için kullanılır.

Options -> Force recalculation of hash = Bir dosyanın hash değerinin hesaplatılmadan geçmesini istemiyorsak seçeriz.Hash'in yeniden hesaplatılmasını zorla.

Options -> Find duplicate files = Yenilenen dosyaları bul.

Options -> Insert new columns at position = FileSystem alanına bilgilerin kaç sütun halinde gelmesini istenirse.

File Size Range = Verilen boyut aralığı dışında olan dosyaların hash değerini hesaplama.

Extract Metadata

Extract Metadata Options

Process Name:

Extract

- ☒ Digital Cameras (Make/Model)
- ☒ DOC, XLS, PPT by Author
- ☒ DOC, XLS, PPT by Date Printed
- ☒ GPS Photos
- ☒ LNK by Target Volume
- ☒ MS Jump List
- ☒ PDF by Author

Bookmark

- ☐ Digital Cameras (Make/Model)
- ☐ DOC, XLS, PPT by Author
- ☐ DOC, XLS, PPT by Date Printed
- ☐ GPS Photos
- ☐ LNK by Target Volume
- ☐ MS Jump List
- ☐ PDF by Author

Logging: Priority:

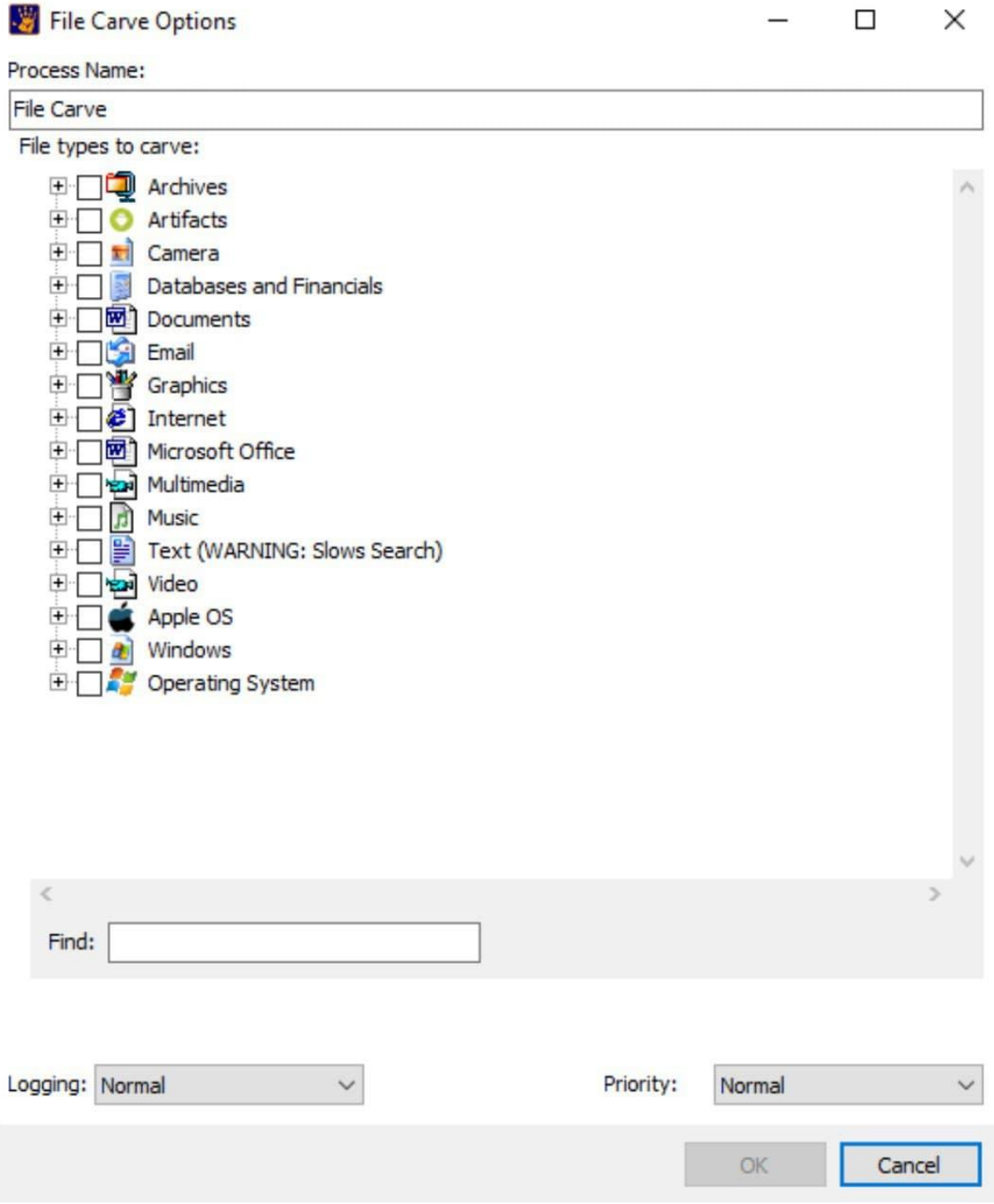
Bir dosyanın içerisinde metadata alanları varsa, ayrıntılı bir şekilde metadata alanlarının çıkarılması için kullanılan alandır.

Mesela bir dosyanın oluşturulma tarihi, bir dosyanın değiştirilme tarihi, bir dosyanın konum bilgisi, bir dosyanın yazar bilgisi.

Bir dosyanın üst verilerini çıkarmak, elde etmek.


Bookmark = Delil demek. Delil olarak ekleme seçenekleri var.

File Carve



Silinmiş dosyaları kurtarmak için dosya kazıma alanı kullanılır.

Cache Thumbnails

 Cache Thumbnails Options

Process Name:

Cache Thumbnails


File Size Range

Minimum: 0 Mb

Maximum: 0 Mb (0 = no limit)

Logging: Normal Priority: Normal

OK Cancel

 Cache Video Thumbnails Options

Process Name:

Cache Video Thumbnails

File Size Range

Minimum: 0 Mb

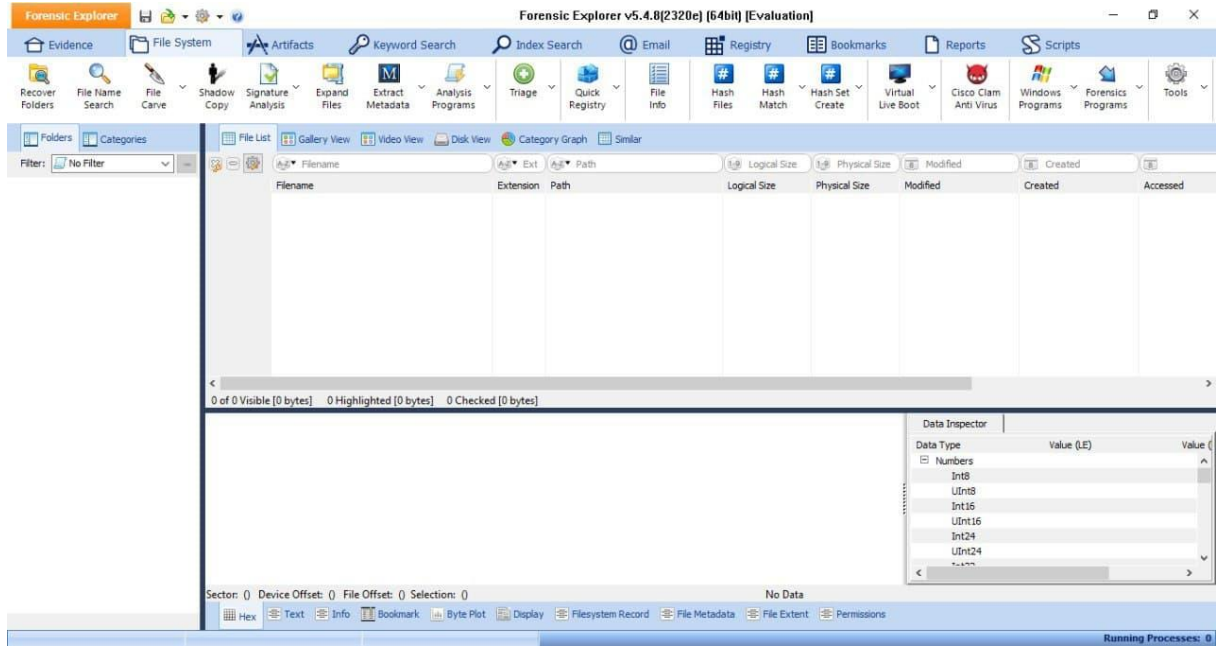
Maximum: 0 Mb (0 = no limit)

Logging: Normal Priority: Normal

OK Cancel

Thumbnails dosyalarının incelenmesi için kullanılır. Verilen boyut aralığındaki thumbnails dosyalarını incele denilebilir.

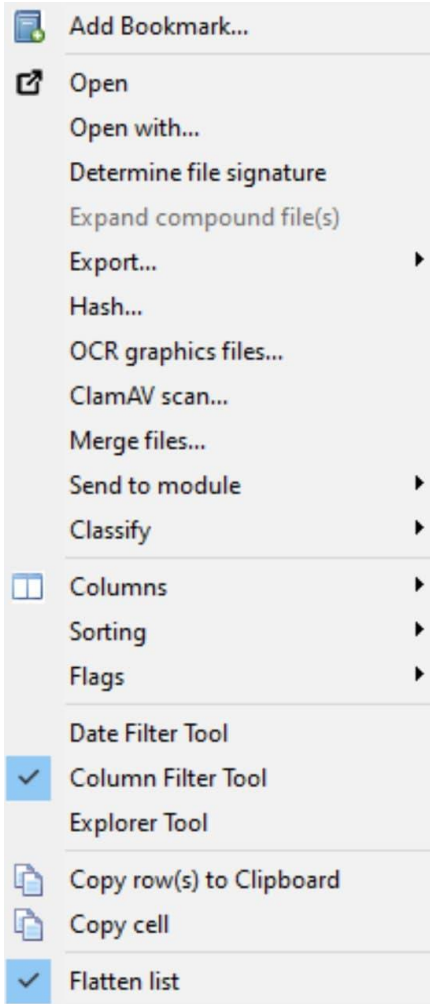
5.File System Penceresi



Kare = Seçme, seçerek üzerinde işlem yapılır.

Pentagram işareti = Gösterme, pentagramla belirlenen dosyalar ekranda gözükür.

Bir dosyaya sağ tıkladığımızda:



Add Bookmark

Dikkat edilmesi gereken dosyalar seçilebilir. Not yazılır. Delil dosyaları Bookmarks'a eklenir.

Open

Windowsta standart olarak seçtiğimiz dosya hangi programla açılıyorsa otomatik olarak açılır.

Open with

Hangi programla açmak istenildiğini sorar.

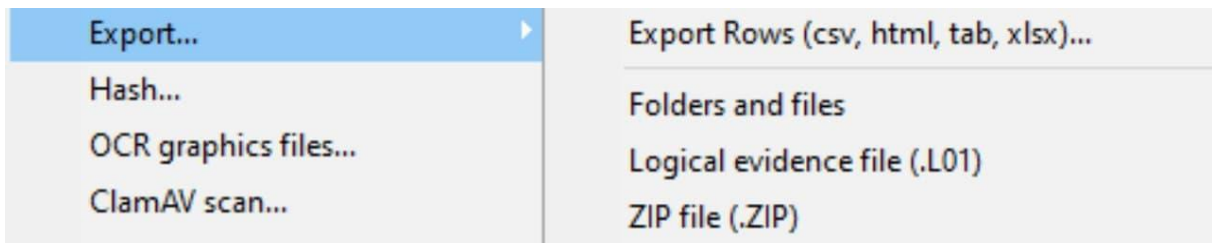
Determine file signature

Sadece belirlenen dosya için dosya imza analizi yaptırır.

Expand compound file(s)

Toplu bir dosya varsa onun açılıp incelenmesi için kullanılır.

Export



Export Rows = Seçilen dosya csv dosyasına ya da tab dosyasına aktarılabilir. Aktardıktan sonra bu dosyayı görüp inceleyebiliriz.

Folders and files -> Source = Seçilen dosya dışarıya aktarılabilir.

Folders and files -> Destination -> Keep folder structer = Seçilen dosyanın bu imaj dosyası içerisinde bulunduğu dizin yapısını da aktarır.

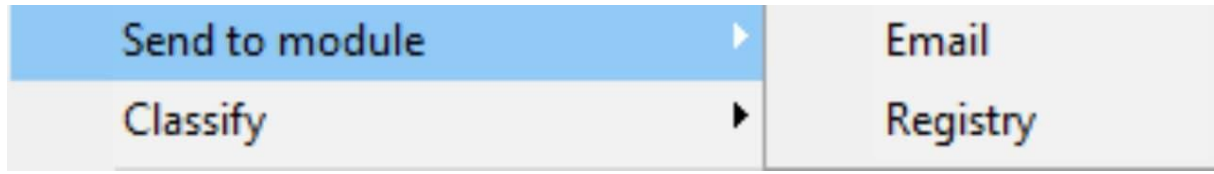
Folders and files -> Destination -> Keep file date/time = Dosyanın

metadata alanlarıyla beraber düzgün bir şekilde date'nin time'nın da muhafaza edilmesi isteniyorsa. İmaj dosyasında o dosyanın oluşturulma zamanı, değiştirilme zamanı, bütün tarih zaman bilgilerinin muhafaza edilmesi isteniyorsa bu seçilir.

Folders and files -> Destination -> Split largefiles into = Dosya boyutu seçilir. En fazla ne kadarsa kurtar.

Folders and files -> Destination -> Destination Folder = Verilerin aktarılacağı yer.

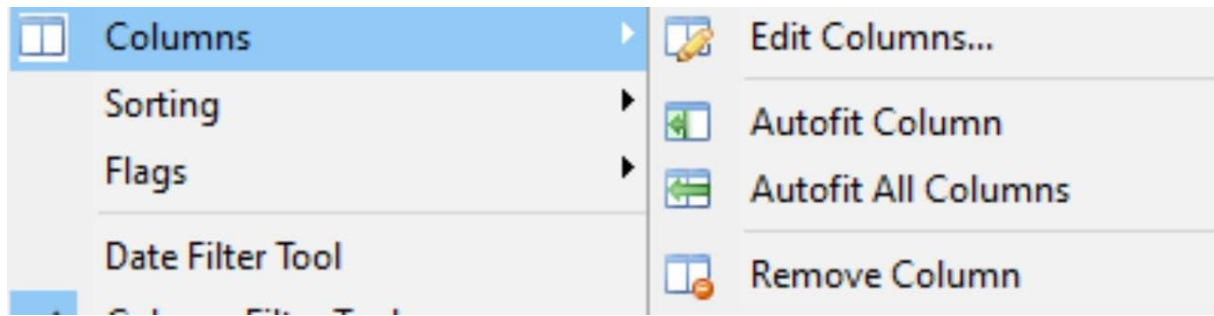
Send to module



Email = Email dosyalarında aktif olur. Email ile seçilen dosya gelir. O dosyanın içeriği ayrıntılı bir şekilde incelenebilir.

Registry = Registry dosyalarında aktif olur. Registry ile seçilen dosya gelir. O dosyanın içeriği ayrıntılı bir şekilde incelenebilir.

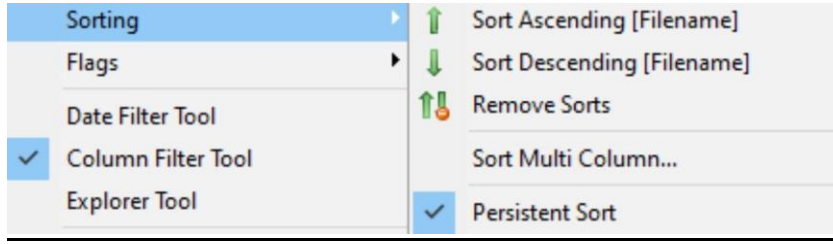
Columns



Edit Columns = Gösterilen sütunların yeri değiştirilebilir. Yeni sütun eklenip kaldırılabilir.

Autofit Column = Otomatik sığdırır.

Sorting

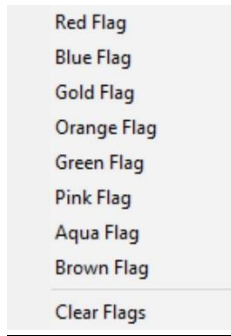


Sort Ascending = Artan sırayla sıralar.

Sort Descending = Azalan sırayla sıralar.

Sort Multi Column = Birden fazla alanda sıralama yapılır.

Flags



Renkler 1'den başlayarak devam eder. Belirlenen özelliklere göre dosyalara renk verilir. Bir dosyaya farklı renklerle o dosyalar üzerinde farklı işlemler yapmak isteniyorsa derecelendirilebilir.

Date Filter Tool

Tarihi ve zamanı belirlenen dosyalar görülür.

Text Filter Tool ya da Column Filter Tool

Seçildiğinde filtreleme yapan bölüm çıkar.

Explorer Tool

Dosya içi arama için kullanılır.

Copy row(s) to Clipboard

Bütün satır alanını kopyalar.

Copy cell

Bir hücreyi kopyalamak için kullanılır.

Görüntüleme seçenekleri:



Gallery View

Ön görüntüyü sağlar.

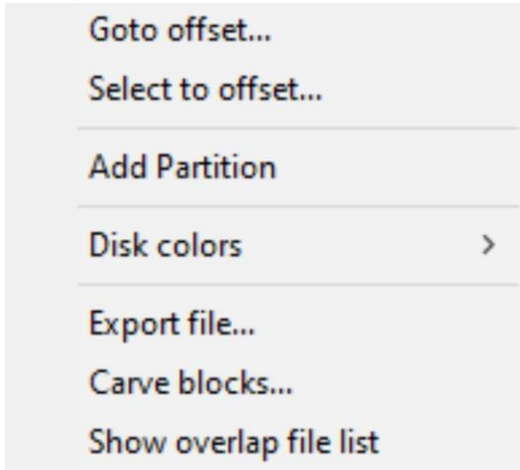
- Thumbnails dosyalar küçük dosyalardır.Ön görüntü dosyalarıdır.Tırnak dosya olarak adlandırılır.Büyütüldüğünde çözünürlüğü çok iyi değildir.Ancak küçük haliyle bulunduğu yer ile ilgili önemli bilgiler verir.

Disk View

Sektörlerin renkleri biri tarafından derecelendirilmez.

Diskin sektörel boyutta ayrıntılı bir şekilde belli sektörler üzerinde inceleme yapılmasını sağlar. Dosyalar hangi sektördeyse hangi byte'taysa görülür.

Sağa tıklayıp:



Goto Sector = Gitmek istenilen sektör girip gidilir.

Disk colors = Renklerin temsil ettiklerini gösterir.

Export blacks = Buranın kapsadığı alanlar export edilir.

Carve blocks = Belirlediğimiz sektörü carve edebiliriz.Bookmark olarak ekliyebiliriz.

Show ovelop file list = Diskin alanını ayrıntılı bir şekilde anlatır.

Category Graph

Ne tür dosyalar olduğunu gösteriyor.

Bir dosyaya tıkladığımızda:



Hex = Hexadecimal alanı görülür.

Text = Text alanı görülür.

Info = Dosyayla ilgili ayrıntılı bilgi edinmek için. Dosya bookmark dosyası mı, size'ı nedir, Extension'ı nedir, uzantısı nedir, uzantısı eşleşiyor mu, File Category'si nedir, File Signature'si nedir gibi.

Bookmark = Bookmarkla ilgili bir şey var mı.

Byte Plot = Bir resmin düzensizliğini gösterir. Entropy değeri ne kadar yüksek olursa o resim içerisinde değişiklik yapıldığını gösterir. Entropy değerinin yüksek olmasına bağlı olarak resmin düzensizliğinin ölçüsünü gösterir.

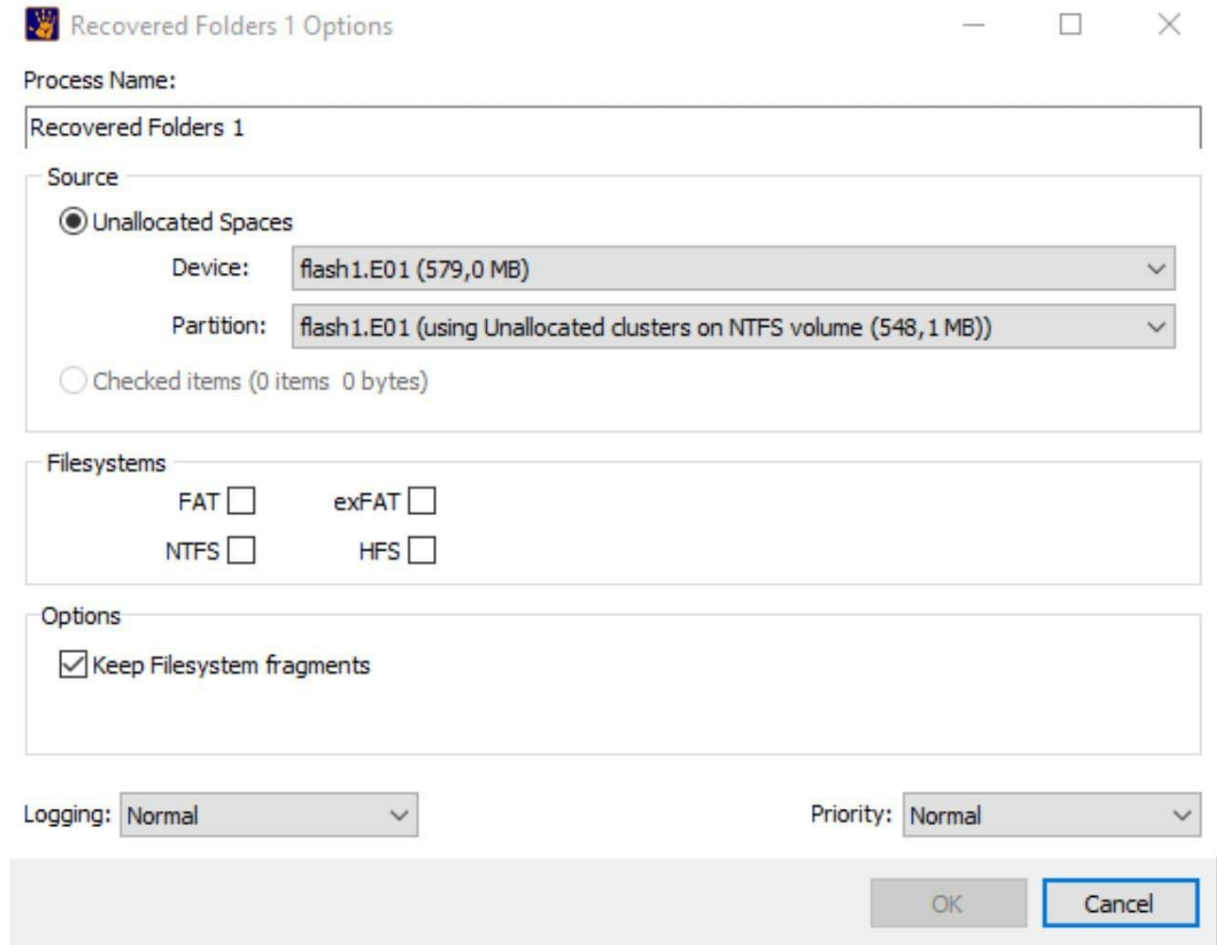
Display = Seçilen dosyanın görüntülenme ekranıdır.

Filesystem Record = Dosyanın record edildiğindeki süreçleri gösterir.

File Metadata = Metadata alanında neler olduğu görülür.

File Extent = Dosya kendi bulunduğu diskinde hangi sektörde, hangi sektör başlangıcında, hangi byte'da, hangi cluster'da tek tek görülür. Bir dosyanın ayrıntılı bir şekilde nerde olduğu sektör bazında, byte bazında, cluster bazında görülür.

Recover Folders



Recovered Folders 1 Options

Process Name:

Recovered Folders 1

Source

☒ Unallocated Spaces

Device: flash1.E01 (579,0 MB)

Partition: flash1.E01 (using Unallocated clusters on NTFS volume (548,1 MB))

☐ Checked items (0 items 0 bytes)

Filesystems

FAT ☐ exFAT ☐

NTFS ☐ HFS ☐

Options

☒ Keep Filesystem fragments

Logging: Normal


Priority: Normal

OK Cancel

FAT formatında, NTFS formatında, exFAT formatında, HFS formatında dizinlerin kurtarılmasını sağlar.

File Carve alanı MFT'ye bakar. Ana dosya tablosudur. MFT tablosu sabit diskte bulunan tüm dosyaların ve klasörlerin sabit diskin hangi noktasında bulunduğunu ve ne kadarlık yer kapladığını gösterir. File Carve işleminde MFT'ye bakılır, sahipsiz dosyaların bilgisini de getirir. Ancak Recover Folders'da metadatasına bakmaz sadece dosyayı sahipsiz bir şekilde kurtarır.

File Carve

 File Carve 02 Options

Process Name:
File Carve 02

Source
☒ Unallocated space (3 items 548,2 MB)
☐ Checked items (0 items 0 bytes)
☐ Include Raw Devices, Partitions and Files

Search Mode: Sector Byte Offset: 0

File types to carve:

- ☐ Archives
- ☐ Artifacts
- ☐ Camera
- ☐ Databases and Financials
- ☐ Documents
- ☐ Email
- ☐ Graphics
- ☐ Internet
- ☐ Microsoft Office
- ☐ Multimedia
- ☐ Music
- ☐ Text (WARNING: Slows Search)
- ☐ Video
- ☐ Apple OS
- ☐ Windows
- ☐ Operating System

Find:

Logging: Normal Priority: Normal

OK Cancel

File Carve alanındayken bir dosyayı seçip o dosyanın File Extent alanına bakıldığında, sektör başlangıcı ve sektör bitiş alanı var. İki dosyanın başlangıç sektörü ve bitiş sektörü aynıysa ya da bulunduğu byte alanı birbirleriyle aynıysa bu dosyalar birbirinin aynıdır.

Shadow Mount



Gölge kopyalardır.Shadow dosyalar, bazı işletim sistemlerinin geriye dönüş dosyaları var. Bilgisayarın bir önceki çalışır formattaki formu olarak adlandırılabilir.

Orijinal imaj var. Bir de onun volume shadow alanı var. Volume shadow alanındaki alanda orijinal dosyayla farklı olan dosyalar ekrana getirilirse sadece o dosyalar incelenirse o dosyadaki paralolar, geçerlilik süreleri net bir şekilde görüntülenir. Bunun için farklı alanlar ya da tüm dosyalar denirse volume shadow color alanında bu dosyalar ayrıntılı bir şekilde incelenebilir.

Mount method -> All files

Tüm dosyaları getir.


Mount method -> Only files that are different

Gerçek dosyayla yedeği arasında shadow copy arasındaki sadece farklı dosyaları gösterir.

Color

Renk eklenir. Dosyanın shadow copy'den gelen dosya olduğunu mu yoksa orijinal dosya mı olduğunu anlaşılsın diye renk verilir. Renkler VSS color'da gözüktür.

Signature Analysis

 Signature Analysis Options

Process Name:

Signature Analysis

Source

☒ Searchable items (24144 items 200,57 GB)

☐ Unallocated space

☐ Checked items (0 items 0 bytes)

☐ Include Raw Devices, Partitions and Files

Filetypes to determine:

- ☒ Archives
- ☒ Artifacts
- ☒ Camera
- ☒ Databases and Financials
- ☒ Documents
- ☒ Email
- ☒ Graphics
- ☒ Internet
- ☒ Microsoft Office
- ☒ Multimedia
- ☒ Music
- ☒ Text (WARNING: Slows Search)
- ☒ Video
- ☒ Apple OS
- ☒ Windows
- ☒ Operating System

Find:

Options

☐ Force determination

Insert new columns at position: 3

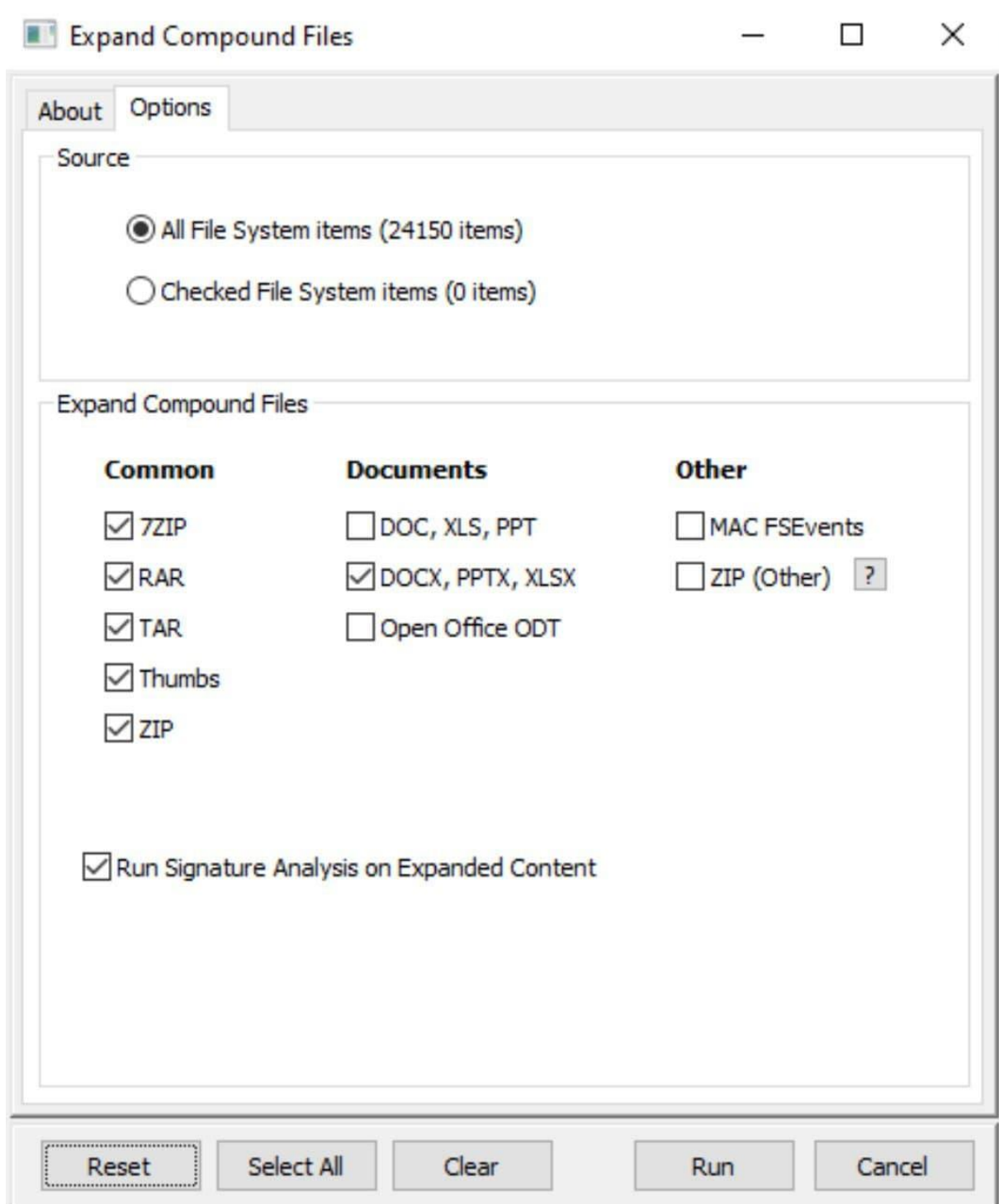
Logging: Normal

Priority: Normal

OK Cancel

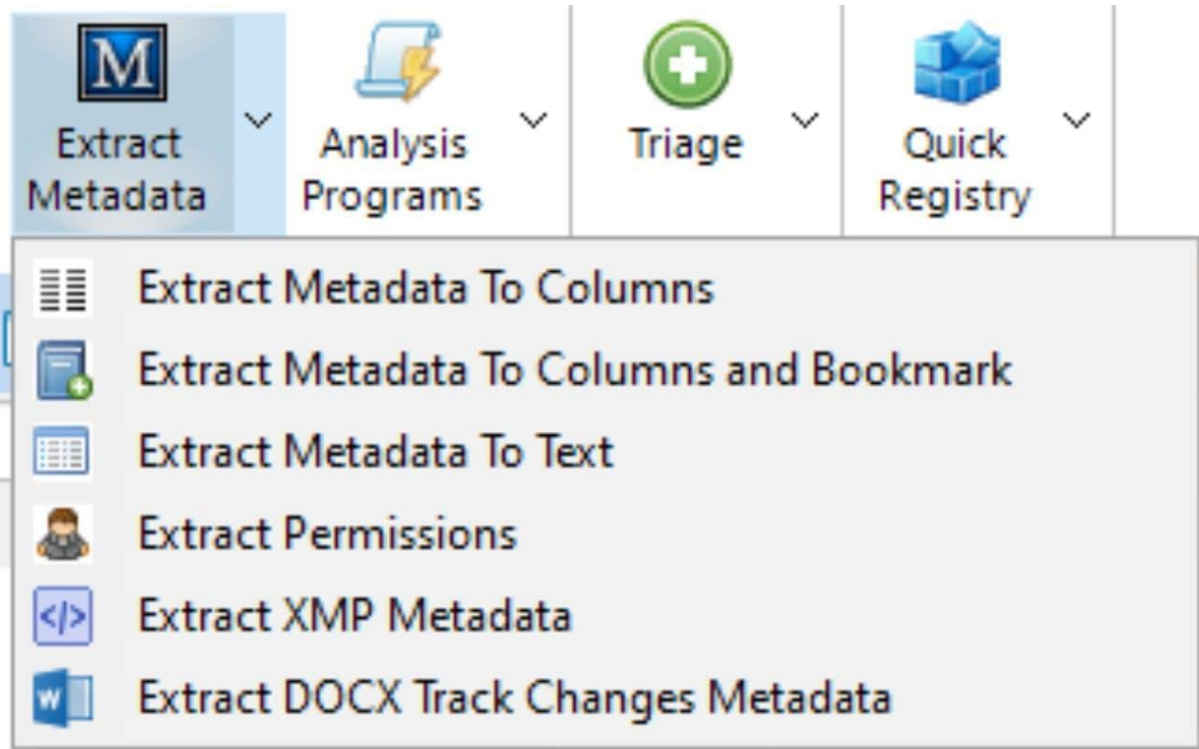
Dosyaların uzantısının gerçekten o uzantıya sahip olup olmadığını veya bir dosyanın uzantısı yoksa bile hangi uzantıya sahip olduğunu çözmesini sağlar.

Expand Files



Sıkıştırılmış dosyaların açılmasını sağlar. Sıkıştırılmış dosyaları tek bir dosya olarak değil de farklı dosyalar halinde gözükmesini sağlar.

Extract Metadata



Bookmark Cameras by Make/Model

Bir kameranın marka modeli kamera dosyalarının içerisinde bilgi ihtiva eden kamera dosyalarının metadatalarını veya exif bilgilerini çıkarır.

Bookmark GPS Photos by Make/Model

GPS içeren verileri çek. Metadata alanlar varsa bu alanların inceleyicinin gözünün önüne serilmesi için kullanılan alandır. Metadata alanında çıkarılan veriler Bookmarks'ta Script Output'ta ayrıntılı bir şekilde görüntülenebilir. Report'ta New deyip Samples'e tıklayıp örnek dosyaları görebiliriz.

Analysis Programs

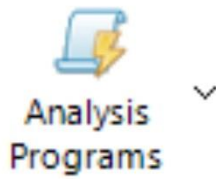
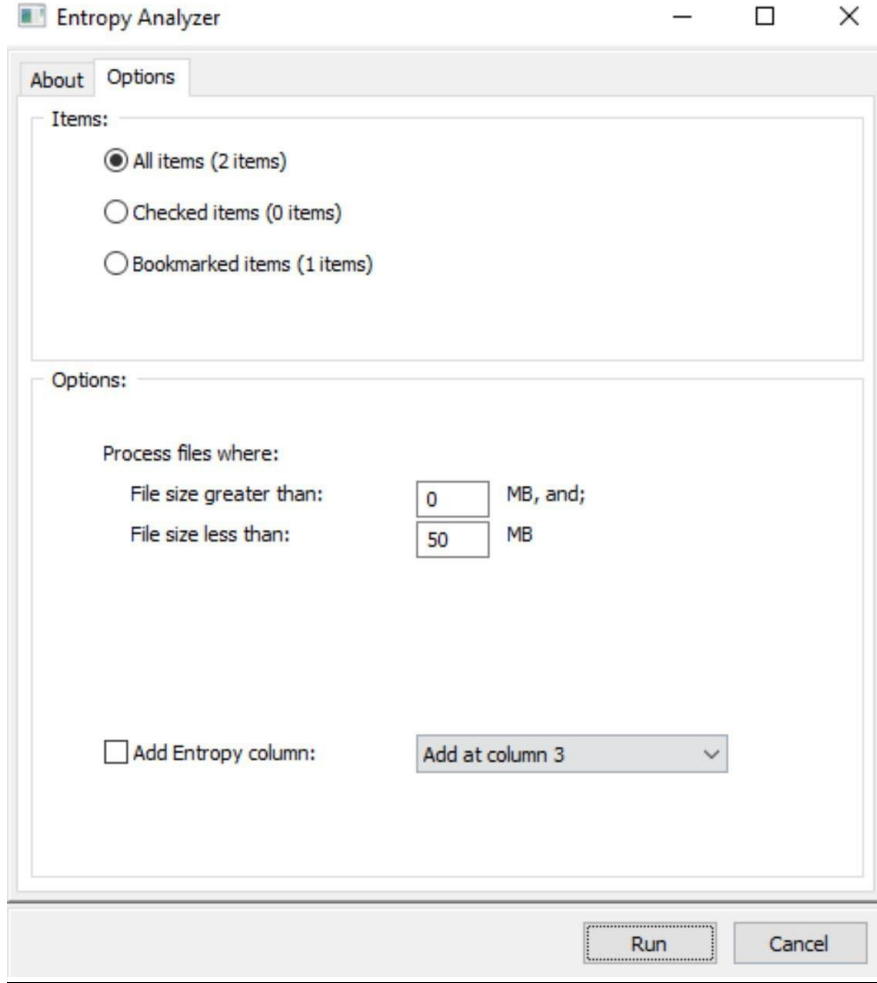


	Chart File Types
	Chart Partitions
	Chart Sub-folder Sizes
	Chart Time Line
	Count Files
	Count Zero Sectors
	Encrypted Files
	Entropy Analysis
	ESE - Parse to CSV
	Export File Types
	File Name Search
	Regex Keyword Search
	Folder Size Column Add
	GPS - Distance From Coordinates
	GPS - GoogleEarth KML Create
	Highlighted File Information
	iTunes Backup - Identify and Bookmark
	Journal Parser (\$UsnJrnl~\$J - v2)
	Recycle Bin - Match \$I with \$R
	Recycle Bin - Parse INFO2 (Win XP)
	Skin Tone Analysis
	Timeline to CSV
	Video - Extract Thumbnail Key Frames
	Video - Detect MKV Multiplexing
	Volume ID and Partition Information
	Win7 Thumbcache - Parse Windows.edb
	ZIP - Internal File Names

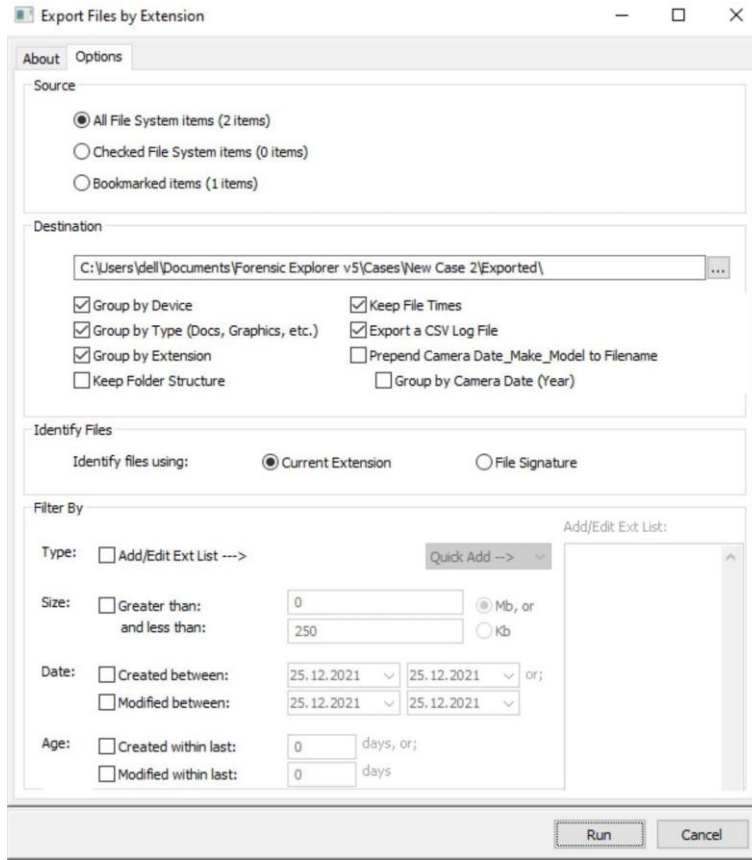
Entropy Analysis



Entropy Analizi yapmak için. Entropy'ler tek tek hesaplanacak sonra her dosyanın Entropy değeri File List alanına sütun olarak gelir.

Entropy analizi bir dosyanın düzensizliğinin ölçüsüdür. Entropy değeri ne kadar yüksekse o dosyanın düzensizliğinin o kadar fazla olduğunu gösterir. Entropy analizi bir dosyanın sıkıştırılmış, şifrelenmiş veya parolalı olduğunu gösterir. Entropy'nin görselleştirilmiş hali Byte Plot alanında gözüktür. Mavi kısım yazdırılamayan karakterler özel alanlar, kırmızı kısım 0 ile 9 arasındaki rakamlar, sarı kısım ise a'dan z'ye kadar olan yazdırılabilir karakterler. Bunlar bir dosyanın Entropy analizidir.

Export File Types



Dosya imza analizi yaparak ya da mevcut dosyaları tanımlayarak dosyaları export eder.

Destination

- Device'a göre gruplandır.
- Uzantıya göre gruplandır.
- Kendi mevcut konumlarını saklı tut.
- Özniteliklerini saklı tut.
- CSV dosyalarını da export et.

Identify Files

File signature yapılmış haliyle mi dosyaları export etsin yoksa mevcut haliyle mi dosyaları export etsin, seçilir.

Filter By

- Tanımlanmış dosyalar.Tipe göre export et denirse seçim yapılır.(Documents dosyaları)
- Dosyaların boyutuna göre export edilebilir.
- Dosyaların oluşturulma değiştirilme tarihine göre export edilebilir.
- Dosyaların yaşına göre dosyalar export edilebilir.

Export edilen veriler kendi otomatik bulunduğu uzantıya göre gruplandırılabilir.

Distance From Coordinates

Distance From Coordinates

About Options

Source

☒ All File System items (2 items)

☐ Checked File System items (0 items)

Starting Coordinates

Select Location New York

Edit Location New York - Statue of Liberty

Edit Latitude 40,6902416

Edit Longitude -74,0455407

☐ Use currently Highlighted file (File System)

File Name flash1.E01

File Latitude no latitude found

File Longitude no longitude found

Distance

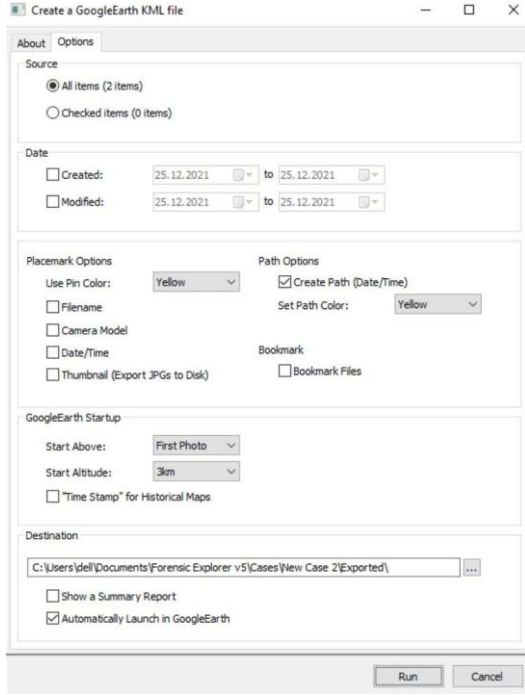
Interval Distance 2 ☒ Miles ☐ Km

Intervals 50

Run Cancel

Seçilen ile göre koordinat dosyaları varsa bu dosyaların bulunup çıkarılmasını sağlar.

GoogleEarth KML Create



Bir dosyanın içerisinde konum verileri varsa konum verilerine göre GoogleEarth üzerinden tek tek o dosyaları konumsal olarak göstermek için kullanılır.

Highlighted File Properties

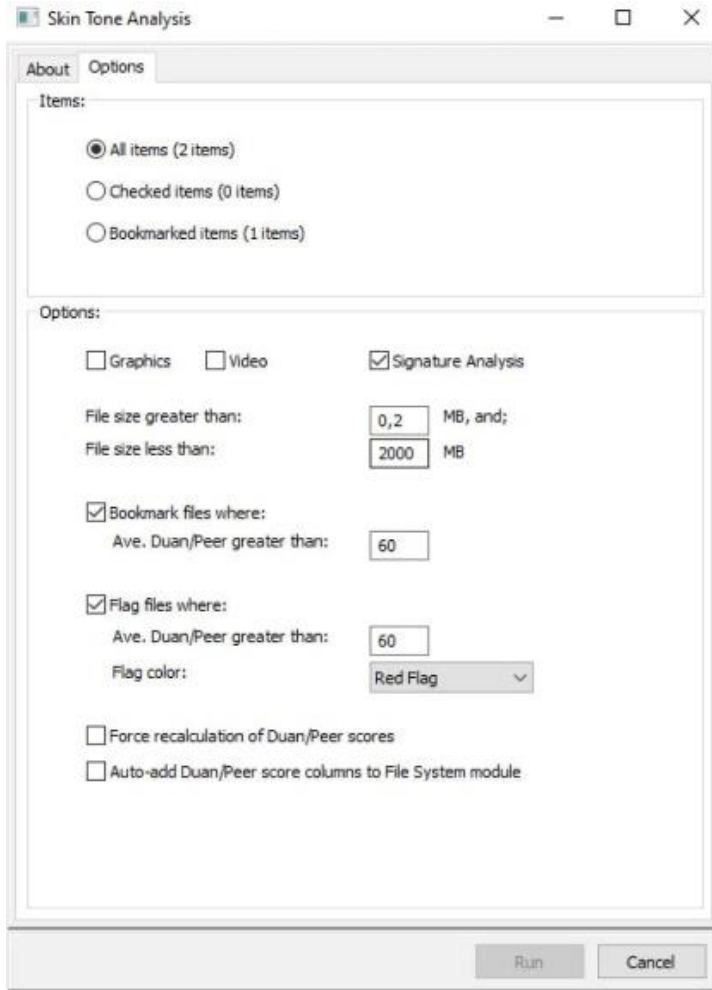
Seçilen dosyayla ilgili bilgi getiriyor.

iTunes Backup - Identify and Bookmark

iTunes Backup - Analyze and Bookmark

iTunes yedeğiyle ilgili analiz yapmayı sağlar.

Skin Tone Analysis



Ten rengine uygun resimleri ekranda görüntülemek için kullanılır.

- Hangi tür dosyalarda
- Kaç mb arasında olanları
- Duan oranı
- Peer oranı
- Flag ekleme
- Bookmarks'a ekleme

Timeline To CSV



Export edilen Extract Metadata alanındaki,

Extract Metadata alanını çalıştır.

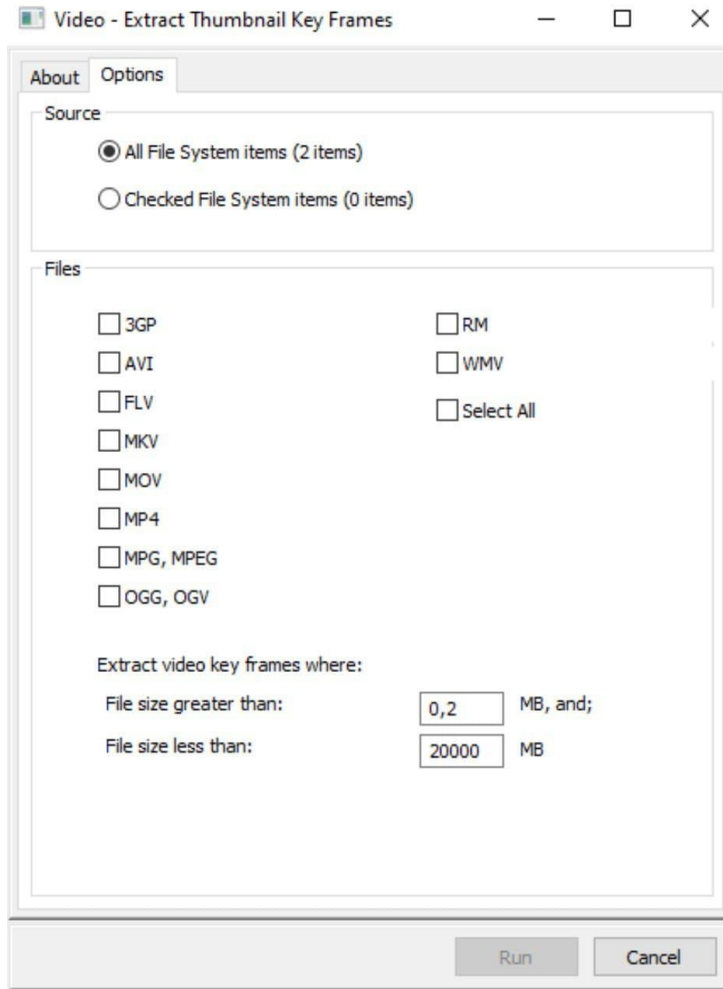
Email modülüne gönder.

Expand compand files yap.

Ondan sonra işlemleri gerçekleştir.

- Created Modified ya da Email Registry dosyalarını
- Belli aralıktaki dosyaların Timeline alanında gözükmesini sağlar.

Video – Thumbnail Key Frames



Multimedya dosyalarının uygun formatta frame frame görüntülenmesini ve sadece belli frame'ler üzerinde işlem yapılmasını sağlamak için kullanılır.

Triage



Triage raporunu File System Registry alanında Bookmarks'a ekler.

File System

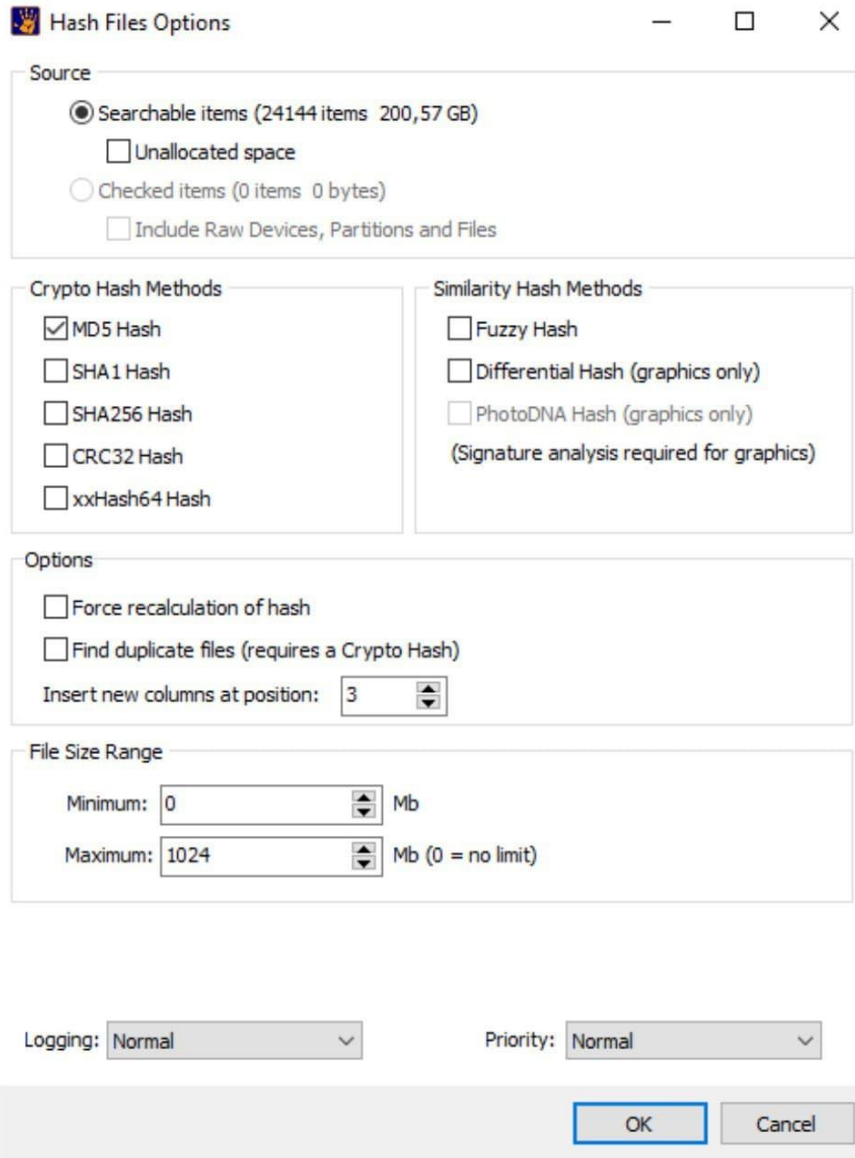
FileSystem alanında seçilen bilgilerin kurtarılıp getirilmesi için.

USB Storage Devices

Windows User Accounts

SAM dosyalarının çıkarılmasını, Triage raporunda bunların gözükmesini sağlar.

Hash Files

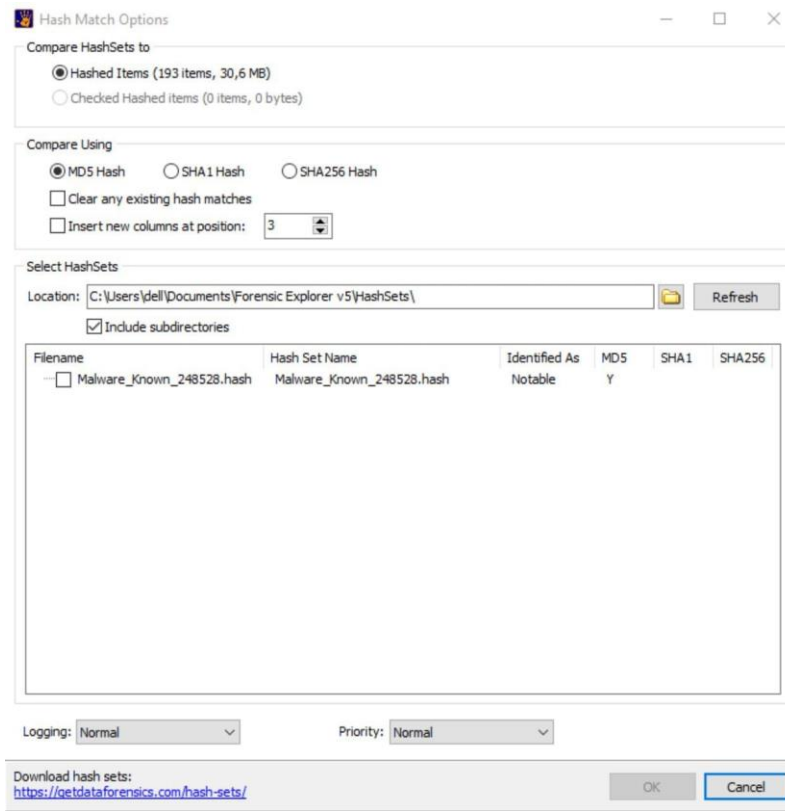
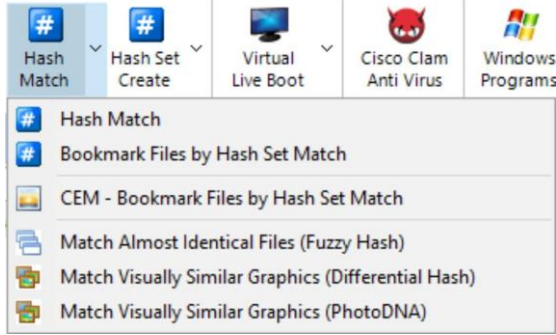


The image shows a Windows-style dialog box titled "Hash Files Options". It contains several sections for configuring file hashing:

- Source:** Includes radio buttons for "Searchable items (24144 items 200,57 GB)" (selected), "Unallocated space", and "Checked items (0 items 0 bytes)". There is also a checkbox for "Include Raw Devices, Partitions and Files".
- Crypto Hash Methods:** A list of checkboxes for "MD5 Hash" (checked), "SHA1 Hash", "SHA256 Hash", "CRC32 Hash", and "xxHash64 Hash".
- Similarity Hash Methods:** A list of checkboxes for "Fuzzy Hash", "Differential Hash (graphics only)", and "PhotoDNA Hash (graphics only)". A note below states "(Signature analysis required for graphics)".
- Options:** Includes checkboxes for "Force recalculation of hash" and "Find duplicate files (requires a Crypto Hash)". Below these is a label "Insert new columns at position:" followed by a text box containing "3" and a small up/down arrow.
- File Size Range:** Includes two rows: "Minimum: 0 Mb" and "Maximum: 1024 Mb (0 = no limit)". Each has a text box and a small up/down arrow.
- Logging:** A dropdown menu currently showing "Normal".
- Priority:** A dropdown menu currently showing "Normal".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Seçili dosyaların hash'ini hesaplamak için kullanılır.

Hash Match



Bir hash setinin, imajda seçilen dosyaların hash'ile eşleşmesini sağlar.

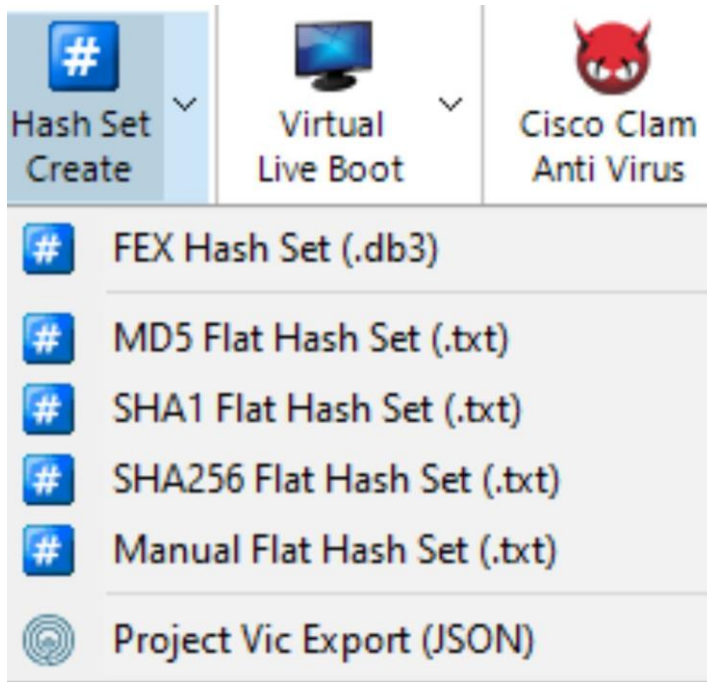
Hash setinin 1. amacı:

Daha öncesinde oluşturulmuş malware gibi terör gibi pornografi gibi standart dosyaların hash değerleri hesaplanır. Sonra hash seti oluşturulur. Sonra o dosyaların birbirleriyle hashlerinin eşleşmesi sağlanır.

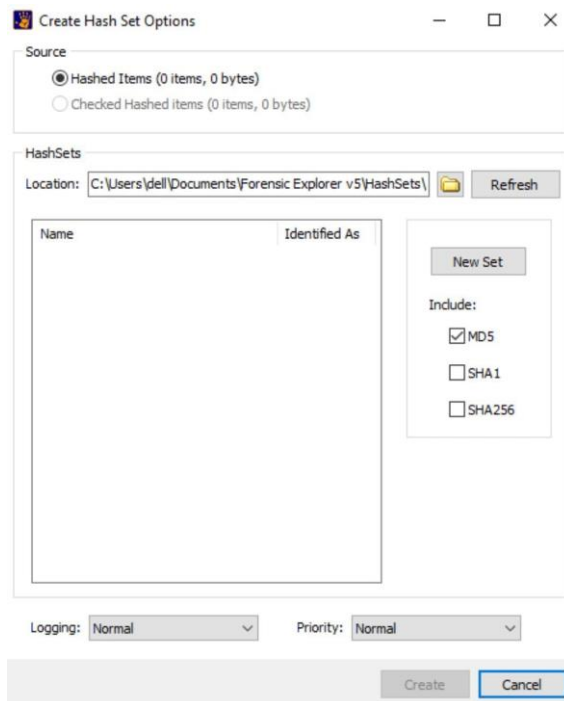
Hash setinin 2. amacı:

Şüpheli bilgisayarın hash değerleri alınır, hash seti oluşturulur. Diğer bilgisayarlarla eşleştirilir.

Hash Set Create

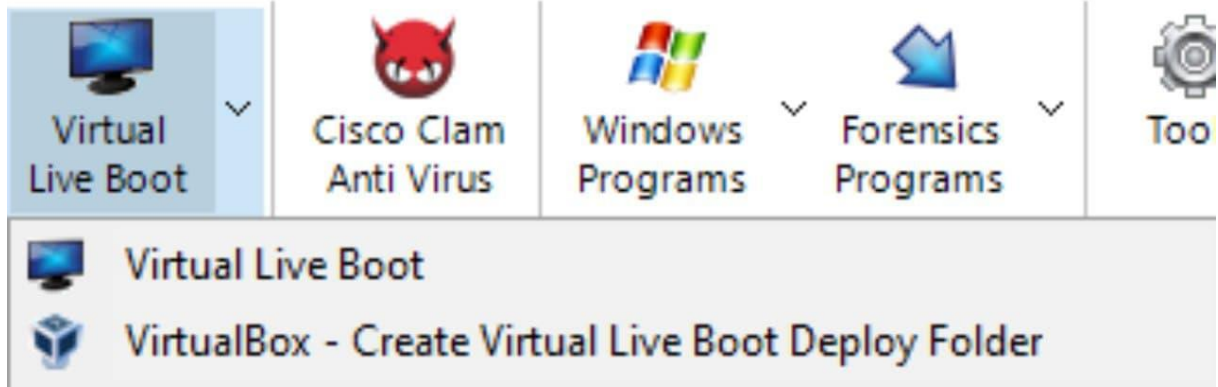


FEX Hash Set



Hash seti oluşturmak için. New Set denildiğinde bu new setin MD5 formatında, SHA1 formatında veya SHA256 formatında yeni bir hash değerinin oluşturulmasını içerisine tek tek dosyaların atılmasını ve böylelikle bir hash seti dosyasının oluşturulması sağlanabilir.

Live Boot



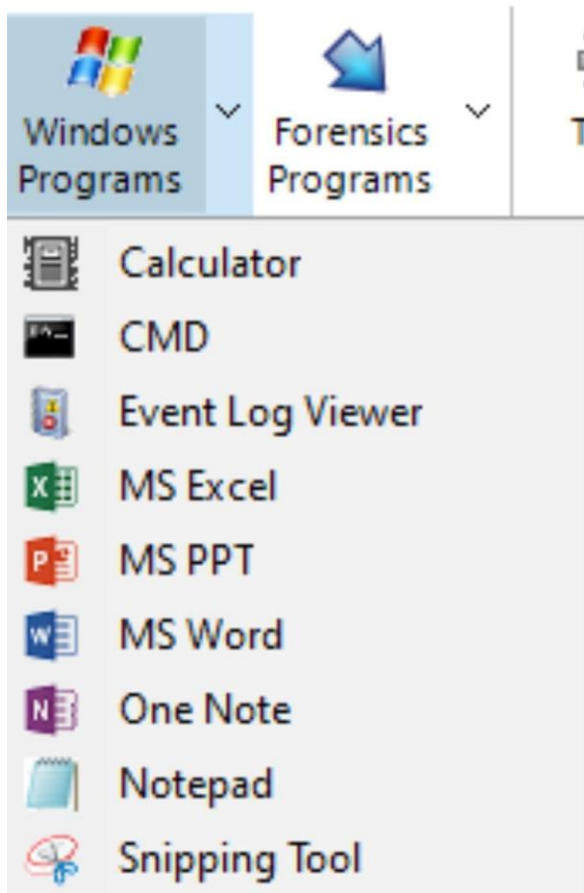
Özelliği kullanabilmek için Virtual Box, VMware Workstation, VMware Player'dan birinin ve Mount Image Pro'nun yüklü olması gerekir.

İmaj dosyasının bilgisayar ekranında açılıyormuş gibi açılması sağlanır. Live Boot seçeneği imaj dosyasının düzgün bir şekilde kendi bilgisayarımızmış gibi ayrıntılı bir şekilde incelenmesini sağlar.

- Bu bilgisayarda en son kullanılan pencereler görülebilir.
- Denetim masasında bu bilgisayarda yapılan sistem ayarları, hangi programların yüklü olduğu görülebilir.
- Internet Explorer'da, Google Chrome'da kapanmış sayfalar geri yüklenebilir, geçmiş incelenebilir. Kayıtlı şifreler görülebilir.

Bir bilgisayarın fiziksel bir şekilde çalışmasını sağlayan formatta çalışmamız gerekir.Yani donanımsal olarak imajının donanımsal olarak nasıl çalıştığının düzenlendiği özel formatta imaj almak gerekiyor ki bu bilgisayarın düzgün bir şekilde çalışması sağlanabilsin.

Windows Programs



Mevcut windows programlarının açılmasını sağlar.

- Hesap makinesi
- CMD ekranı
- Ekran alıntı aracı

Forensics Programs



FEX Imager

FTK imager'ın benzer programıdır.

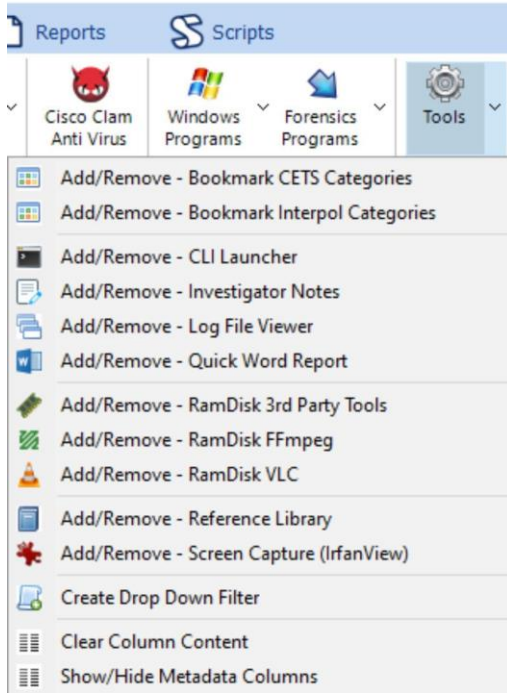
License Manager

Lisans dosyasının süresinin bu bilgisayarda ne zamana kadar geçerli olduğunu gösterir.

MIP v6

Mount Image Pro dosyasının çalışmasını sağlar.

Tools



Backup Current Case

Mevcut Backup'ların ekranda gözükmesi sağlanabilir.

Backup settings

Backup setting'leri tanımlanıp hangi dosyaların Backup'ının alınacağı tanımlanabilir.

Clear All File System Module Flags

Tüm flag dosyalarının clear olmasını sağlar.

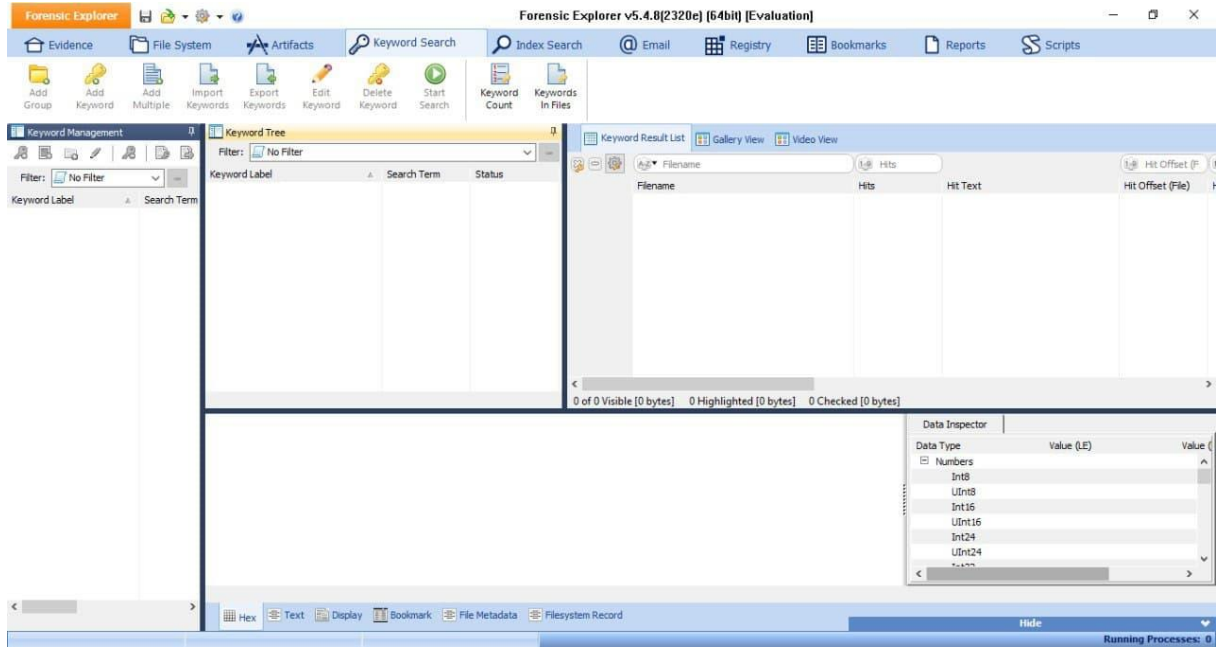
Clear Hash and Duplicate Count Columns

Mükerrer olan hash dosyalarının düzgün bir şekilde temizlenmesini sağlar.

Hide All Metadata Columns

Metadata columns'larının gizlenmesini sağlar.

6. Keyword Search Penceresi



File System’de hangi dosyalarda inceleme yapacağımızla alakalı süreçler tamamlandıktan sonra.

Keyword Search bütün alanlarda işlem yapar.

- Keyword’e isim verilir.
- Aramak istenilen kelime yazılır.
- Case Sensitive, büyük harf küçük harf duyarlılığı yapar.
- Hangi dillerde bulunacağı seçilir.
- Başlatılan pencerede hangi dosyada arama yapılacağı belirlenir.

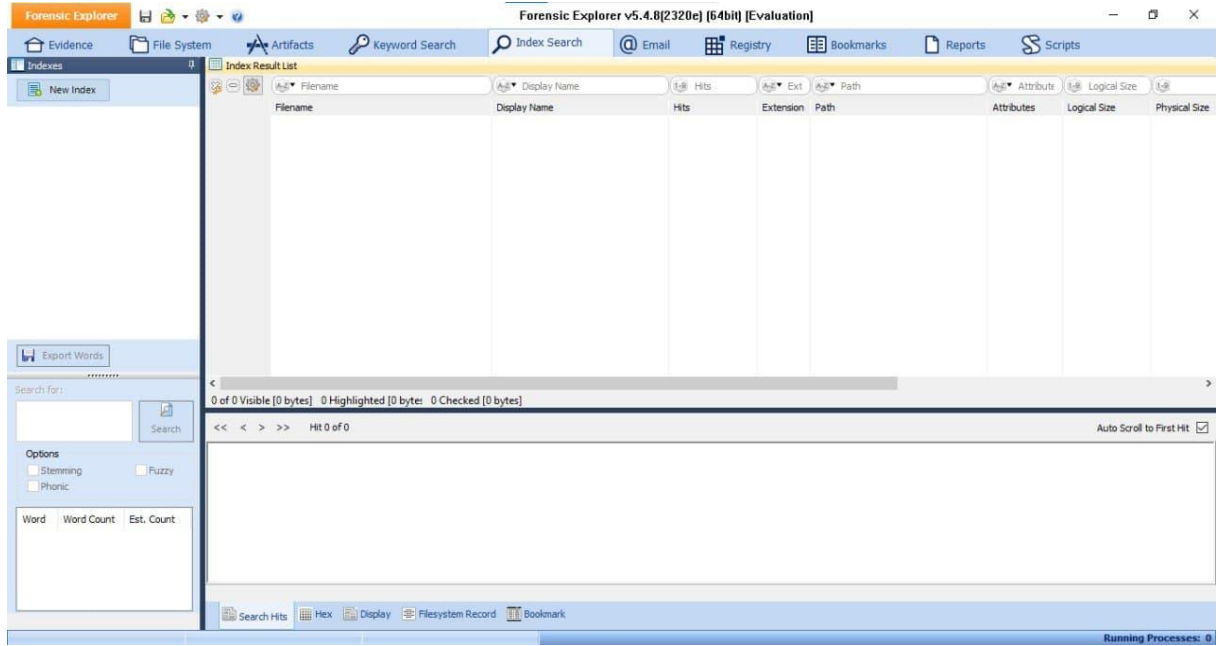
Add Multiple Keywords

Keyword’ler eklenir. Direkt yazılabilir. Önceki yapılan dosyalar Load from file’den buraya Load edilebilir. Yeni yazılanlar Save to file’den save edilebilir.

Edit Keyword

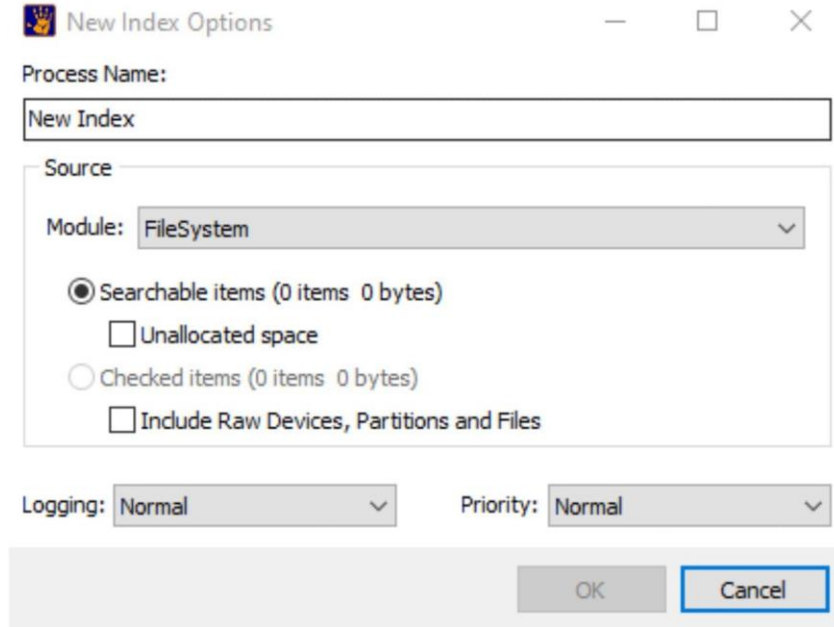
Üzerlerine tıklayıp içerisine girip düzenleme yapılabilir. Keyword’ün adı gibi. Arama yaptırılacak alan gibi(Hexadecimal).

7. Index Search Penceresi



New index denilip hangi alanlarda arama yapılması isteniyorsa seçilir.

New index denilip sadece Email,Registry,FileSystem'de bu dosyanın indexlenmesi sağlanabilir.



Indexleme uzun sürer.

Bir bilgisayarda neden kaç tane geçmiş bunlar ayrıntılı bir şekilde görülebilir.

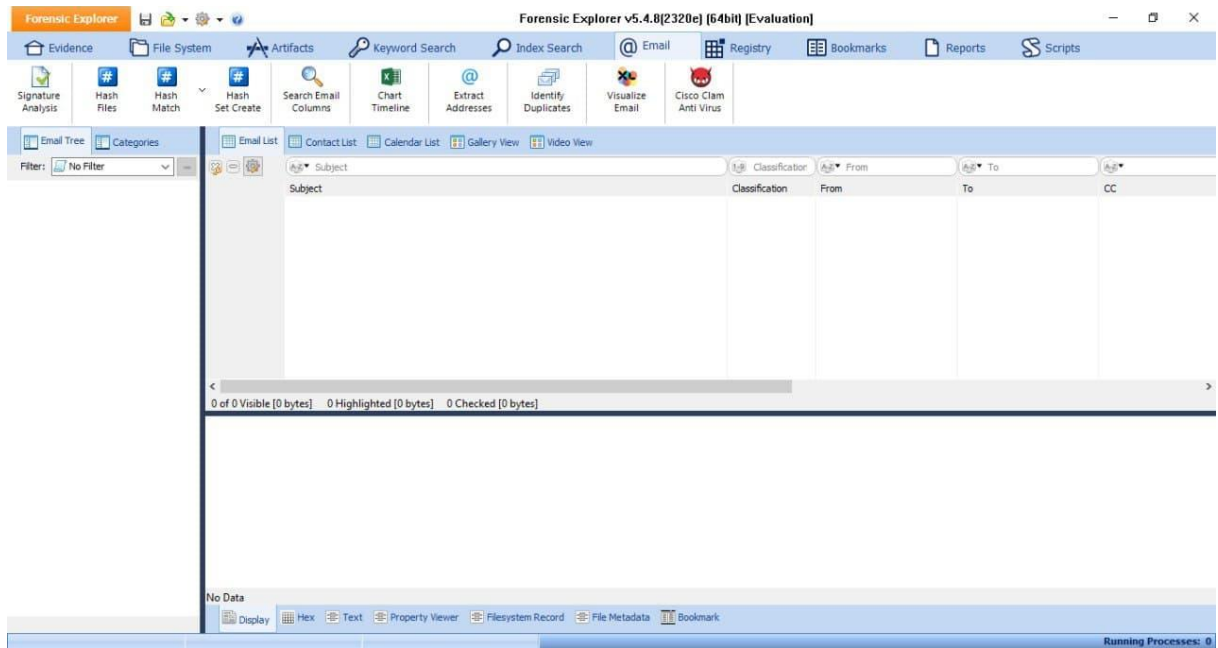
noise.dat dosyası dışında geçen kelimeleri buldurur. İngilizce kelimeler için bu noise.dat dosyası kullanılır.

Index taramasında noise.dat dosyasındaki kelimeler kullanılmaz. Çünkü bunlar çok kullanılan kelimelerdir ya da eklerdir.

Keyword sadece belirlenen kelimelerin aranmasını sağlar. Indexleme bir imajın felistinin çıkarılması. Bir kelime kaç kere geçmiş görülebilir.

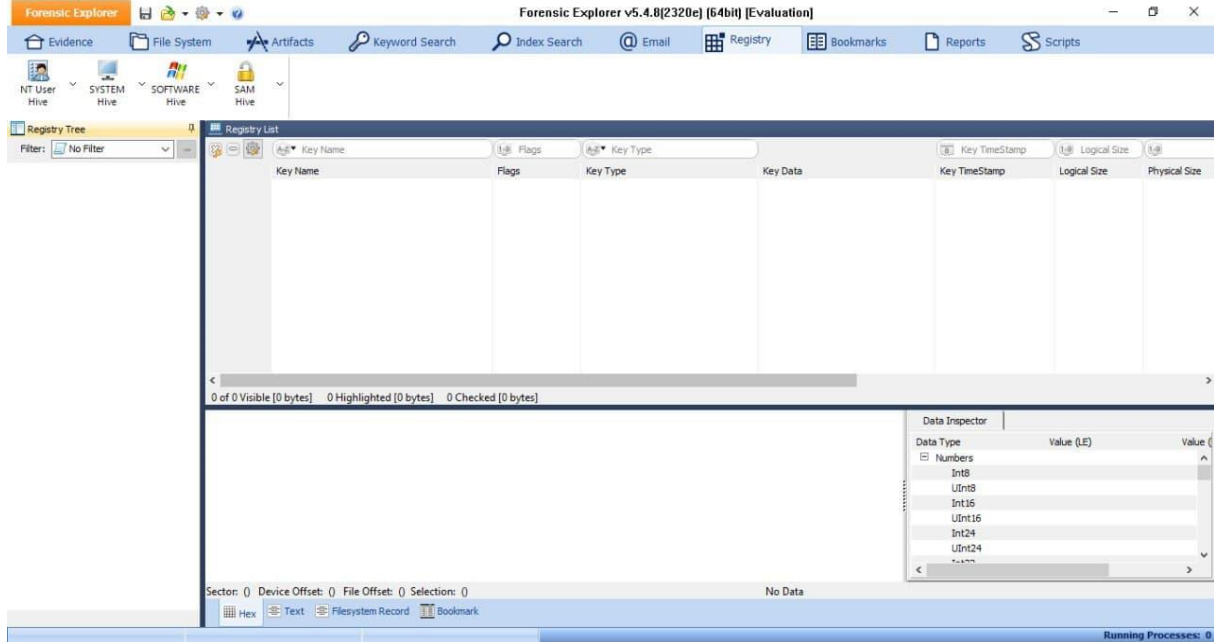
Index bütün imajın index'ini çıkarır. Keyword sadece aranan kelimenin kaçar tane bulunduğunu çıkarır.

8. Email Penceresi



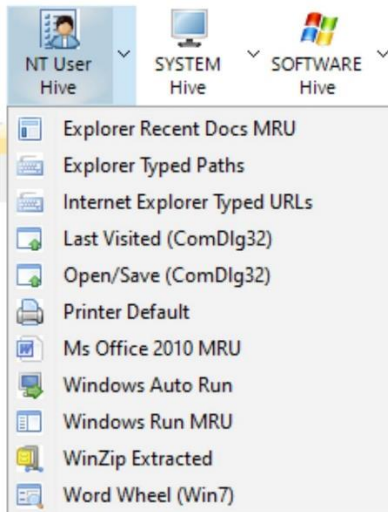
Bir dosyaya sağ tıklanıp sent to Module'den Email seçilip Email modülüne gönderilir. Email sekmesinde o dosya incelenebilir.

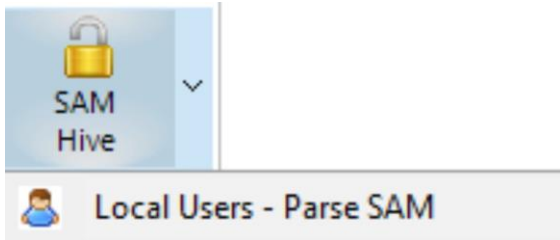
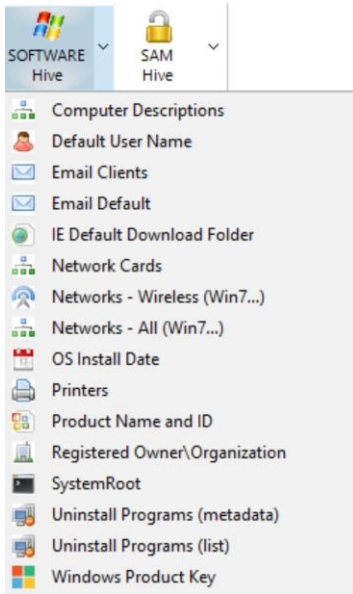
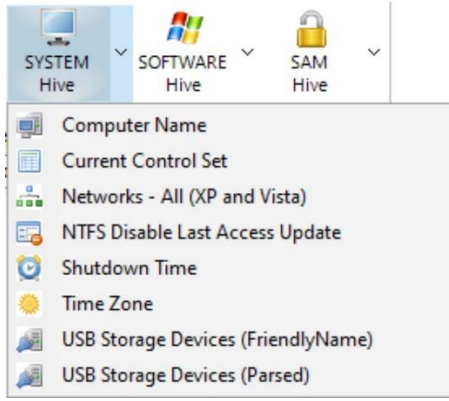
9. Registry Penceresi



File System'de Registry dosyaları seçilir.

Registry dosyalarından 4 tane var:



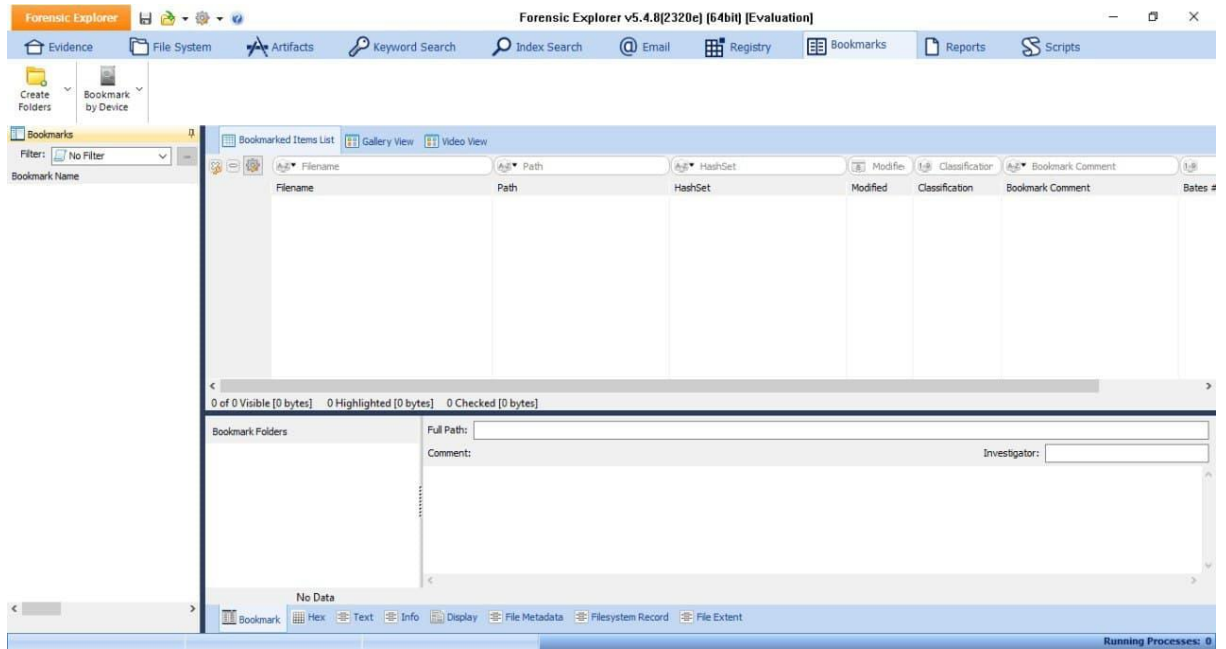


1. NT User dat dosyası
2. SYSTEM dosyası
3. SOFTWARE dosyası
4. SAM dosyası

Seçilen dosyaların Logical Size kısmı büyükten küçüğe sıralanır. En büyük olan ve Volume Shadow alanları renksiz olan esas dosyalardır. Büyük olan genellikle içerisindeki bilgi fazla olan dosyadır. Bu dosyaya sağ tıklanıp Send to module'e tıklanıp Registry'e tıklandığında Registry dosyasına hangi saat diliminde incelenecekse seçilip start denir. Bu Registry alanına gelir.

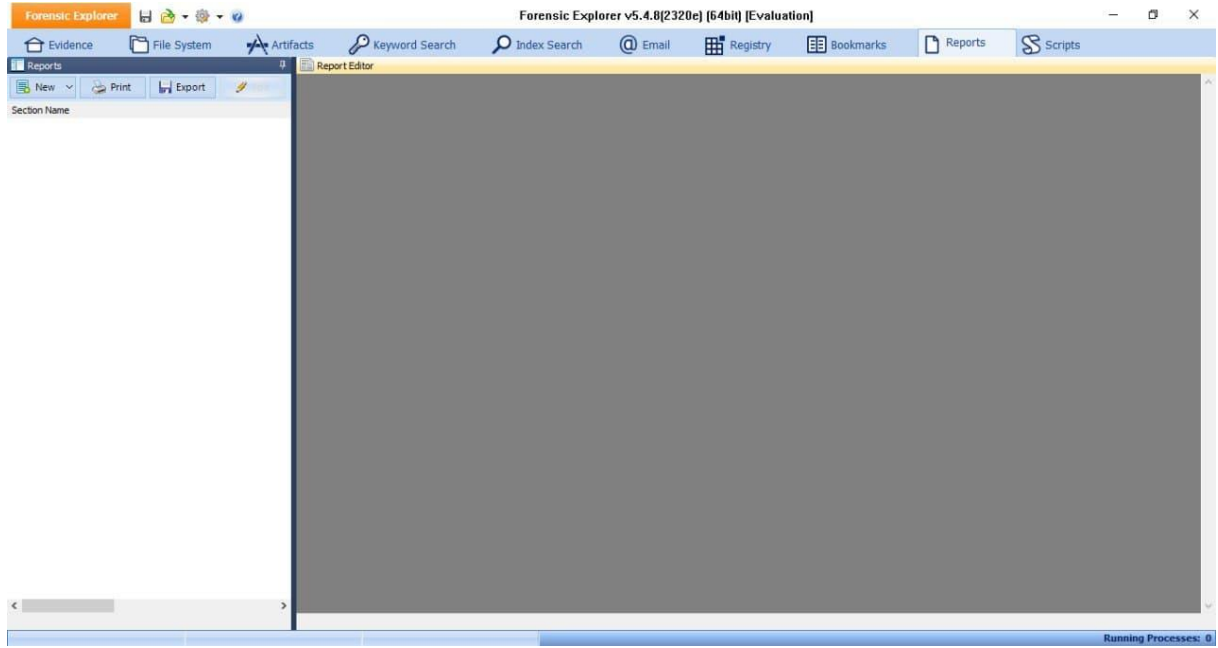
Registry alanında NT User'dan çıkarılacak alanlar, SYSTEM dosyasından çıkarılacak alanlar, SOFTWARE dosyasından çıkarılacak alanlar, SAM dosyasından çıkarılacak alanlar görülebilir.

10. Bookmarks Penceresi



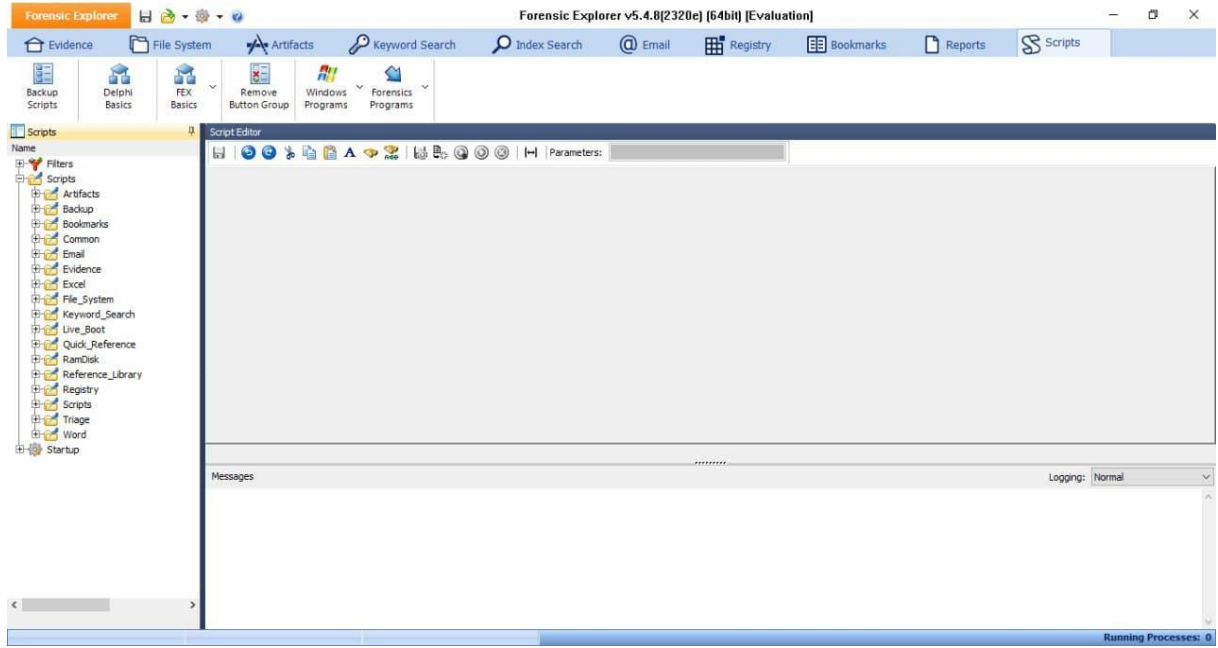
Delil olarak tanımlanan bütün dosyalar Bookmarks dosyaları içerisinde yer alır.

11. Reports Penceresi



Bookmarks'a eklenen her dosya burda otomatik bir şekilde gözükür. Otomatik bir şekilde görmek için New'den Samples'ı seçilebilir. Veya New'den Blank Report'u seçip boş bir rapor oluşturup Editleyip işlemler yapılabilir. Daha sonra bu Exportlanıp dışarıya aktarılabilir.

12. Scripts Penceresi



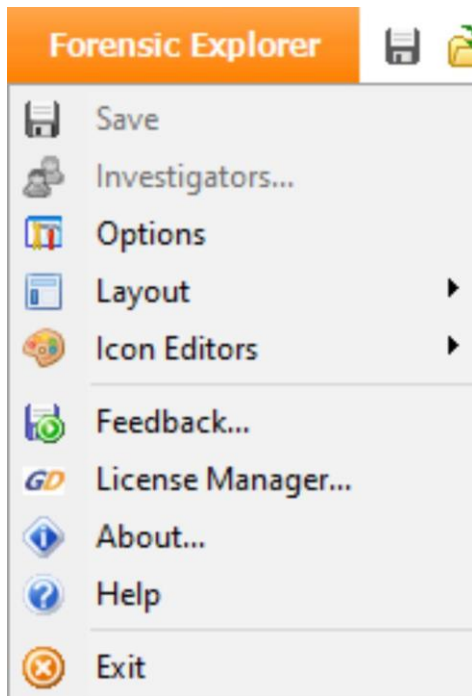
Backup’da ya da Delphi’de kod yazılabilir. Yazılan kodlar kaydedilip Apps’ta, Apps - Process All.pas’ı Create denildiğinde Apps’ler gelir. Process Apps’da örneğin Skype’a tıklanınca Skype ile ilgili processler yazışmalar görülebilir.

Apps’te, Process Apps’de Apps – Process ALL’a tıklandığı zaman tüm processleri işler.

Scripts’e gelinip Triage’a gelinip Triage.pas’a gelinip Triage raporunun oluşturulmasında neler hangi alandan çekilecek tek tek görülebilir.

Phone gelip, Phone Module Create.pas denilip çalıştırıldığında Phone sekmesi gelir. Bu sekmede iPhone ile ilgili yazışmalar, GoogleEarth ile ilgili yazışmalar ayrıntılı bir şekilde görülebilir.

13. Genel Kısım



Options -> General

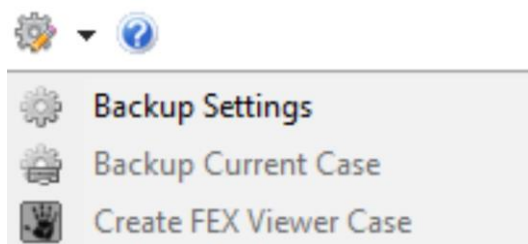
Standart kaydetme yolları değiştirilebilir. Standart dizinler belirlenir.

Options -> Case

Kaç dakikada bir vakanın kaydedileceği ve kaç kere yeni kaydın oluşturulması belirlenir.

About

Forensic Explorer'ın web adresini, destek alınabilecek adresi, versiyonu, son kullanma tarihi gözükür.



Tools -> Backup Settings

Backup yapılacak alanlar seçilebilir.

Tools -> Backup Current Case

Mevcut durum yedeklendikten sonra eski backup'a dönülebilir.

YouTube Linki: <https://youtu.be/ndhs0WJPxY4>