Evidence Penceresi:

New Case -> Investigator -> New -> Investigator ID

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

New Case -> Case Notes

Bir vakayla ilgili bu vakayı kısa bir şekilde tanımlayacak,özetleyecek,açıklayacak özel bilgileri yazıyoruz.

New Case -> Case Time Zone Settings -> TimeZone

Gelen vakanın hangi ülkeden gelindiği belli değilse TimeZone alanı Local Time seçilir.Local Time'ı seçtikten sonra, daha sonraları vakamızın tarih ve saat ayarlamasını yapabiliriz.

Forensic Explorer -> Options -> General

Standart kaydetme yollarını değiştirebiliriz.Standart dizinleri belirliyoruz.

Forensic Explorer -> Options -> Case

Kaç dakikada bir vakanın kaydedileceği ve kaç kere yeni kaydın oluşturulmasını belirliyoruz.

Forensic Explorer -> About

Forensic Explorer'ın web adresini,destek alabileceğimiz adresi,versiyonu,son kullanma tarihini görebiliyoruz.

Tools -> Backup Settings

Backup yapacağımız alanları seçebiliyoruz.

Tools -> Backup Current Case

Mevcut durumu yedekledikten sonra eski backup'a dönebiliriz.

Verify Hash

Seçtiğimiz formatta Hash doğrulaması sağlayabiliriz.Başlattığımızda hash değerini hesaplıyor.Hesapladıktan sonra rapor dosyasındaki hash ile hesapladığı hash'i karşılaştırıyor.Aynı olduğunu ispatladıktan sonra vaka üzerinde çalışabiliriz.

Virtual Live Boot

Fiziksel bir imaj dosyasını canlandırmak için.

New Case -> OK -> Add device

Canlı olarak fiziksel imaj inceleyebiliriz.

Add RAID

RAID sistemi ekleyebiliyoruz.

Raid birden fazla diske veri kaydetme.

Raid bir verinin kaydedilme türüdür.

Remote ya da Network

Ağ üzerindeki bir bilgisayarın IP adresi ve port numarası biliniyorsa, buraya ağ üzerinden bir bilgisayarı bağlayıp ağ üzerinden bir bilgisayarın incelenmesini sağlarız.

Reflesh

Yenilemek.

- **Add device'de OK'a basarak inceleyeceğimiz diski belirtip Evidence Processor penceresi çıkar.Bu pencerede farklı imajlara farklı prosesler uygulayabiliriz.**

New Case -> OK -> Add image

New Case -> OK -> Add file

Sadece bir dosyayı incelemek istiyorsak.

New Case -> OK -> Add group

Aynı olayda farklı kişilerin incelemesi yapılacaksa.

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

Evidence Processor Penceresi:

FileSystem

Yapılacak proseslerin bütününü içerir.Seçmezsek proses penceresi aktif hale gelmez.

Verify Device Hashes

Ayarlarına tıkladığımız zaman imaj dosyasının hangi formatta istiyorsak o formatta hash değerini hesaplatabiliriz.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.

Search for FileSystems -> Signature Analysis

Dosya imza değerlerinin tutulmasını sağlıyor.Bu pencere bir dosyanın gerçek uzantısını bulmaya yarar.Bu pencerede tanınmış dosya uzantıları var.Sistemin ayrıntılı bir biçimde dosya imza analizi yapmasını sağlıyor.

Search for FileSystems -> Expand Compound Files

Tıkladığımızda tanıdığı sıkıştırılmış dosya uzantıları gözükür.Elimizdeki sıkıştırılmış dosya tek bir dosya olarak mı görülsün yoksa onun içerisindekileri gruplandırsın mı, seçtiğimiz uzantılara göre bunu belirleriz.

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

Search for FileSystems -> Process in Parallel -> Triage

Triage raporu oluşturmaya yarıyor.Bir imaj dosyasının belli standart alanlarını bize gösterir.İmaj dosyasıyla ilgili ön bilgi almayı sağlarız.

Search for FileSystems -> Process in Parallel -> Hash Files

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 istiyorsak.**

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

Search for FileSystems -> Process in Parallel -> Extract Metadata

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.**

Search for FileSystems -> Process in Parallel -> File Carve

Silinmiş dosyaları kurtarmak için dosya kazıma alanını kullanıyoruz.

FileSystem -> Cache Thumbnails

Thumbnails dosyalarının incelenmesi için kullanılıyor.Verilen boyut aralığındaki thumbnails dosyalarını incele diyebiliriz.

Triage dosyasında neler görülür ?

Reports -> Triage -> Title Page

Kapak kısmı, başlık kısmı

Reports -> Triage -> Triage - Bookmark Folder

Dosyada neler olduğu

- **Hesabın oluşturulma tarihi**
- **Bilgisayarın kullanıcıları**
- **Zaman dilimi**
- **Bilgisayarın son kapatılma zamanı**
- **Bilgisayarın adını**
- **Emailler**
- **Driver'ların yüklendiği yazıcıları gösterir.**
- **Bilgisayarda kullanılan harici diskler, flash diskler**
- **Triage raporundaki her bir boyutun tek tek partition'ları, partition tipi, boyutu, bootable yapılmış mı, partition size'ları, allocated alan var mı, tüm alanları buradan görebiliyoruz.Gizli bir alan varsa buradan görürsek o alanı özellikle açıp inceleriz.**
- **Bilgisayarda olan browsers.**
- **Shadow Copy Files**
- **Kullanıcı Folder'larını gösterir.**

- **Bu bilgisayarda bir dosyanın kalıcı olarak yok edilmesini sağlayan programları gösterir.**

File System Penceresi

Kare = Seçme, seçerek üzerinde işlem yapılır.

Pentagram işareti = Gösterme, pentagramla belirlenen dosyalar ekranda gözükür.

Bir dosyaya sağ tıkladığımızda:

Add Bookmark

Dikkat etmemiz gereken dosyaları seçebiliyoruz.Notumuzu yazabiliyoruz.Delil dosyaları Bookmarks'a eklenir.

Open

Windowsta standart olarak seçtiğimiz dosyahangi programla açılıyorsa otomatik olarak açılır.

Open with

Hangi programla açmak istediğimizi sorar.

Determine file signature

Sadece belirlediğimiz dosya için dosya imza analizi yaptırır.

Expand compound file(s)

Toplu bir dosya varsa onun açılıp incelenmesi için kullanılır.

Export

Delimited rows ya da Export Rows = Seçtiğimiz dosyayı csv dosyasına ya da tab dosyasına aktarabiliriz.Aktardıktan sonra bu dosyayı görüp inceleyebiliriz.

Folders and files -> Source = **Seçtiğimiz dosyayı dışarıya aktarabiliriz.Check ettiğimiz dosyaları dışarıya aktarabiliriz.**

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

Folders and files -> Destination -> Keep file date/time = **Dosyanın metadata alanlarıyla beraber düzgün bir şekilde date'nin time'nın da muhafaza edilmesini istiyorsak.İmaj dosyasında o dosyanın oluşturulma zamanı, değiştirilme zamanı, bütün tarih zaman bilgilerinin muhafaza edilmesini istiyorsak bunu seçeriz.**

Folders and files -> Destination -> Split largefiles into = **Dosya boyutunu seçiyoruz.En fazla ne kadarsa kurtar.**

Folders and files -> Destination -> Destination Folder = **Verileri aktaracağımız yer.**

- **Bir dosyayı open diyip açtıktan sonra kaydettiğimizde tarih ve zamanını değiştiririz, metadata verilerini değiştirebiliriz.Farklı kaydet dediğimiz zaman bu dosyanın kendi oluşturulma değiştirilme zamanıyla beraber otomatik bir şekilde değişiyor.Ama export dediğimizde tarih, zamanı ve dosya konumunu muhafaza ederek ayrıntılı bir şekilde işlemlerimizi yapabiliriz.**

Send to module

Email = **Email dosyalarında aktif olur.Email ile seçilen dosya gelir.O dosyanın içeriğini ayrıntılı bir şekilde inceleyebiliriz.**

Registry =

Columns

Edit Columns = **Gösterilen sütunların yerini değiştirebiliriz.Yeni sütun ekleyip kaldıabiliriz.**

Autofit Column = **Otomatik sığdırır.**

Sorting

Sort Ascending = **Artan sırayla sıralar.**

Sort Descending = **Azalan sırayla sıralar.**

Sort Multi Column = **Birden fazla alanda sıralama yapabiliriz.**

Flags

Renkler 1'den başlayarak devam eder.Bizim renklendirdiğimiz alanlar.Kendi belirlediğimiz özelliklere göre dosyalara renk verebiliyoruz.Bir dosyaya farklı renklerle o dosyalar üzerinde farklı işlemler yapmak istiyorsak derecelendirebiliriz.

Date Filter Tool

Tarihini ve zamanını belirlediğimiz dosyaları görebiliyoruz.

Text Filter Tool ya da Column Filter Tool

Seçtiğimizde filtreleme yapan bölüm çıkıyor.

Explorer Tool

Dosya içi arama için kullanılır.

Copy row(s) to Clipboard

Bütün satır alanını kopyalar.

Copy cell

Bir hücreyi kopyalamak için kullanılır.

File System -> Gallery View

Ön görüntüyü sağlar.

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

File System -> Disk View

Sektörlerin renklerini biz derecelendirmiyoruz.

Diskin sektörel boyutta ayrıntılı bir şekilde belli sektörler üzerinde inceleme yapmamızı sağlar.Dosyaları hangi sektördeyse hangi byte'taysa görebiliriz.

Sağa tıklayıp:

Goto Sector = Gitmek istediğimiz sektörü girip gidiyoruz.

Disk colors = Renklerin temsil ettiklerini gösterir.

Export blacks = Buranın kapsadığı alanları export edebiliyoruz.

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

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

File System -> Category Graph

Ne tür dosyalar olduğunu gösteriyor.

Bir dosyaya tıkladığımızda:

Hex = Hexadecimal alanını görebiliriz.

Text = Text alanını görebiliriz.

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 olduğunu görebiliriz.

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

Filtre seçenekleri:

- **Folderdan hazırlanmış filtreleri seçebiliriz.**
- **Column Filter Tool'dan filtre uygulayabiliriz.**
- **Edit Columns'dan filtre uygulayabiliriz.**
- **Catagories görünümünde bilgisayarın kendi otomatik tanımladığı dosyamız var.Otomatik tanımlanan; dosya uzantısına göre, oluşturulma değiştirilme tarihine göre, flag'a göre dosyalarımız var.**

Recover Folders

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

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 alanındayken bir dosyayı seçip o dosyanın File Extent alanına baktığımızda, 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 aynısıdır.Adli makamlarda bu dosyalardan iki mükerrer buldum denir.**

Shadow Mount

Gölge kopyalar

Shadow dosyalar = Bazı işletim sistemlerinin geriye dönüş dosyaları var.Bilgisayarın bir önceki çalışır formattaki formu olarak adlandırılabilir.

Geri dönüşüm noktası belirliyoruz.O geri dönüşüm noktasında mesela bugünki tam çalışır haliyle formuyla bilgisayarı saklıyoruz.Sakladığımız hali tekrar geri getirmek için işlemler yapıyoruz.Shadow copylerde bunun gibi kopya dosyalardır.

Bilgisayarın çalışabilir formdaki son prosesi olarak adlandırılabilir.

Elimizde orijinal verimiz orijinal imajımız var.Bir de onun volume shadow alanı var.Volume shadow alanındaki alanda orijinal dosyayla farklı olan dosyaları ekrana getirirsek sadece o dosyaları incelersek o dosyadaki paraloları, geçerlilik sürelerini net bir şekilde görebiliriz.Bunun için farklı alanlar ya da tüm dosyalar dersek volume shadow color alanında bu dosyaları ayrıntılı bir şekilde inceleyebiliriz.

Mount method -> All files

Tüm dosyaları getir.

Mount method -> Only files that are different

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

Color

Renk ekliyoruz.Dosyanın shadow copy'den gelen dosya olduğunu mu yoksa orijinal dosya mı olduğunu anlayalım diye renk veriyoruz.Renkler VSS color'da gözükür.

Signature Analysis

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 sağlıyor.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 çıkarıyor.

Bookmark GPS Photos by Make/Model

GPS içeren verileri çek.

Metadata, dosyaların üst verileridir ve bu verilerin içerisinde marka,model,yazar,erişim tarihi,oluşum tarihi gibi alanlar varsa bu alanların inceleyicinin gözünün önüne serilmesi için kullanılan alandır.

Bu marka modelleri Bookmarks'ta Script Output'ta görebiliriz.

Metadata alanında çıkardığımız verileri Bookmarks'ta Script Output'ta ayrıntılı bir şekilde görüntüleyebiliriz.

Report'ta New deyip Samples'e tıklayıp örnek dosyaları görebiliriz.

Analysis Programs

Entropy Analysis

Entropy Analizi yapmak için, File List alanına Entropy alanıyla ilgili veriler gelsin istiyoruz.Her dosyanın Entropy analizinin yapılmasını istiyoruz.

Entropy analizi bir dosyanın düzensizliğinin ölçüsüdür.Entropy analizi bir dosyanın sıkıştırılmış, şifrelenmiş veya parolalı olduğunu gösterir.Entropy'nin görselleştirilmiş hali Byte Plot alanında gözükür.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.

Byte plot alanına baktığımızda Entropy analizinin yapılmasıyla beraber bir dosyanın Entropy değeri ne kadar yüksekse o dosyanın düzensizliğinin o kadar fazla olduğunu gösterir, o dosya içerisinde sıkıştırılmış işlemler,şifrelenmiş işlemler ya da parolalanmış işlemler gözükür.

Entropy'ler tek tek hesaplanacak sonra her dosyanın Entropy değeri File List alanında sütun olarak karşımıza gelir.

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, seçiyoruz.

Filter By

- **Tanımlanmış dosyalar.Tipe göre export et dersek seçim yaparız.(Documents dosyaları)**

- **Dosyaların boyutuna göre export edebiliyoruz.**
- **Dosyaların oluşturulma değiştirilme tarihine göre export edebiliyoruz.**
- **Dosyaların yaşına göre dosyaları export edebiliyoruz.**

Export edilen veriler kendi otomatik bulunduğu uzantıya göre gruplandırılabiliyor.

Distance From Coordinates

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 sağlıyor.

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 yapmamızı sağlamak için kullanılır.

Triage

Triage raporunu File System Registry alanında Bookmarks'a ekler.

File System

FileSystem alanında seçtiğimiz bilgilerin kurtarılıp getirilmesi için.

USB Storage Devices

Windows User Accounts

SAM dosyalarının çıkarılmasını, Triage raporunda bunların gözükmesini sağlıyoruz.

Hash Files

Seçili dosyaların hash'ini hesaplamak için kullanılıyor.

Hash Match

Bir hash setinin, imajımızdaki seçtiğimiz dosyaların hash'iyle eşleşmesini sağlıyor.

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 dediğimizde 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 sağlanacak.

- **Bu bilgisayarda en son kullanılan pencereleri görebiliriz.**
- **Denetim masasında bu bilgisayarda yapılan sistem ayarlarını, hangi programların yüklü olduğunu görebiliriz.**
- **Internet Explorer'da, Google Chrome'da kapanmış sayfaları geri yükleyebiliriz, geçmişi inceleyebiliriz.Kayıtlı şifreleri görebiliriz.**

Bu bilgisayarı kendi bilgisayarımızmış gibi ayrıntılı bir şekilde incelemek için Live Boot seçeneği kullanılır.

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.

Live Boot seçeneği elimizdeki imaj dosyasının düzgün bir şekilde kendi bilgisayarımızmış gibi ayrıntılı bir şekilde incelenmesini sağlar.

Tools

Backup Current Case

Mevcut Backup'ların ekranda gözükmesini sağlayabiliriz.

Backup settings

Backup setting'lerini tanımlayıp hangi dosyaların Backup'ının alınacağını tanımlayabiliriz.

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.

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.

Keyword Search Penceresi:

File System'de hangi dosyalarda inceleme yapacağımızla alakalı süreçler tamamlandıktan sonra sonra

Keyword Search bütün alanlarda işlem yapar.

- **Keyword'e isim veriyoruz.**
- **Aramak istediğimiz kelime yazılır.**

- **Case Sensitive, büyük harf küçük harf duyarlılığı yapar.**
- **Hangi dillerde bulacağını seçiyoruz.**
- **Başlattığımız pencerede hangi dosyada arama yapılacağını belirliyoruz.**

Add Multiple Keywords

Keyword'lerimizi ekliyoruz.Direkt yazabiliyoruz.Önceki yaptığımız dosyaları Load from file'dan buraya Load edebiliriz.Yeni yazdıklarımızı Save to file'dan save edebiliriz.

Edit Keyword

Üzerlerine tıklayıp içerisine girip düzenleme yapabiliyoruz.Keyword'ün adı gibi.Arama yaptıracağımız alan gibi(Hexadecimal).

Index Search Penceresi:

New index diyip hangi alanlarda arama yapılmasını istiyorsak seçiyoruz.

New index diyip sadece Email,Registry,FileSystem'de bu dosyanın indexlenmesini sağlayabiliriz.

Indexleme uzun sürer.

Bir bilgisayarda neden kaç tane geçmiş bunları ayrıntılı bir şekilde görebiliriz.

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 belirlediğimiz kelimelerin aranmasını sağlar.Indexleme bir imajın felistinin çıkarılması.Bir kelime kaç kere geçmiş görebiliriz.

Index bütün imajın index'ini çıkarır.Keyword sadece aradığımız kelimenin kaçar tane bulduğunu çıkarır.

Email Penceresi:

Bir dosyaya sağ tıklayıp sent to Module'den Email'i seçip Email modülüne gönderiyoruz.Email sekmesinde o dosyayı ineleyebiliyoruz.

Registry Penceresi:

File System'de Registry dosylarını seçiyoruz.

Elimizde Registry dosyalarından 4 tane var:

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

Seçtiğimiz dosyaların Logical Size kısmını büyükten küçüğe sıralıyoruz.En büyük olan ve Volume Shadow alanları renksiz olan bizim esas dosyamızdır.Büyük olan genellikle içerisindeki bilgi fazla olan dosyadır.Bu dosyaya sağ tıklayıp Send to module'e tıklayıp Registry'e tıkladığımızda Registry dosyasına hangi saat diliminde incelenecekse seçip start diyoruz.Bu Registry alanına geliyor.

Registry alanında NT User'dan çıkarılacak alanlar, SYSTEM dosyasından çıkarılacak alanlar, SOFTWARE dosyasındaan çıkarılacak alanlar, SAM dosyasından çıkarılacak alanları görebiliriz.

Bookmarks Penceresi:

Delil olarak tanımladığımız bütün dosyalar Bookmarks dosyaları içerisinde yer alır.

Reports Penceresi:

Bookmarks'a eklediğimiz her dosya burda otomatik bir şekilde gözükür.Otomatik bir şekilde görmek için New'den Samples'ı seçebiliriz.Veya New'den Blank Report'u seçip boş bir rapor oluşturup kendimiz Editleyip işlemlerimizi yapabiliriz.Daha sonra bunu Exportlayıp dışarıya aktarabiliriz.

Scripts Penceresi:

Backup'da ya da Delphi'de kod yazabiliriz.Yazdığımız kodları kaydedip Apps'ta, Apps - Process All.pas'ı Create dediğimizde Apps'ler gelir.Process Apps'da örneğin Skype'a tıklayınca Skype ile ilgili processleri yazışmaları görebiliyoruz.

Apps'te, Process Apps'de Apps – Process ALL'a tıkladığımız zaman tüm processleri işler.

Scripts'e gelip Triage'a gelip Triage.pas'a gelip Triage raporunun oluşturulmasında neler hangi alandan çekilecek tek tek görebiliriz.

Phone gelip, Phone Module Create.pas diyip çalıştırdığımızda Phone sekmesi gelir.Bu sekmede iPhone ile ilgili yazışmaları, GoogleEarth ile ilgili yazışmaları ayrıntılı bir şekilde görebiliriz inceleyebiliriz.