

AUTOPSY TRKE KULLANIM KILAVUZU



İÇİNDEKİLER

1.KAPAK SAYFASI.....	1
2.İÇİNDEKİLER.....	2
3.AUTOPSY NEDİR?.....	3
3.ÖZELLİKLERİ.....	3
4.EKLENTİ MODÜLLERİ.....	4
4.AUTOPSY KURULUMU.....	5
4.1.KURULUM ADIMLARI.....	7
5.UYGULAMA ARAYÜZÜ.....	10
5.1.İLK GÖRÜNÜM.....	10
5.2.ÜST PANEL.....	11
5.2.1.CASE.....	12
5.2.2.VIEW.....	12
5.2.3.TOOLS.....	15
5.2.4.WINDOW.....	15
5.2.5.HELP	15
6.VAKA OLUŞTURMA	16
7.VAKA GÖRÜNÜM.....	19
7.1.ÜST GÖRÜNÜM.....	19
7.2.ALT GÖRÜNÜM.....	24
7.3.SOL GÖRÜNÜM.....	25
7.4.ORTA GÖRÜNÜM.....	27
7.5.SAĞ TIKLAMA	28

AUTOPSY NEDİR?

Autopsy, açık kaynaklı bir adli bilişim platformudur. İlk olarak 2000 yılında Basis Technology tarafından geliştirilmiştir. The Sleuth Kit® ve diğer dijital adli bilişim araçlarına yönelik grafik arayüzdür. Kullanımı kolay ve hızlıdır. Her türlü mobil cihazı ve dijital medyayı analiz edebilir. Kolluk kuvvetleri, ulusal güvenlik, dava desteği ve kurumsal soruşturma alanlarında kullanılır. Basis Technology, eğitim , ticari destek ve eklenti modülleri sağlar.



ÖZELLİKLER

- **LNK Dosya Analizi** : Kısayolları ve erişilen belgeleri tanımlar
- **E-posta Analizi** : Thunderbird gibi MBOX formatındaki mesajları ayrıştırır.
- **Çok Kullanıcılı Vakalar** : Büyük vakalarda diğer denetçilerle işbirliği yapın.
- **Zaman Çizelgesi Analizi** : Aktiviteyi tanımlamaya yardımcı olmak için sistem olaylarını grafiksel bir arayüzde görüntüler.
- **Anahtar Kelime Arama** : Metin çıkarma ve dizin arama modülleri, belirli terimlerden bahseden dosyaları bulmanızı ve düzenli ifade kalıplarını bulmanızı sağlar.
- **Dosya Türü Algılama** : İmzalara ve uzantı uyumsuzluğu algılamasına dayalı
- **İlginç Dosyalar Modülü**, dosya ve klasörleri ad ve yola göre işaretler.
- **Android Desteği** : SMS, arama kayıtları, kişiler, Tango, Arkadaşlarla Sözler ve daha fazlasından veri çıkarır.

- **Web Yapıları** : Kullanıcı etkinliğini tanımlamaya yardımcı olmak için yaygın tarayıcılardan web etkinliğini çıkarır.
- **Kayıt Analizi** : En son erişilen belgeleri ve USB aygıtlarını belirlemek için RegRipper'i kullanır.
- **EXIF** : JPEG dosyalarından coğrafi konum ve kamera bilgilerini çıkarır.
- Medya Oynatma ve Küçük Resim görüntüleyici.
- **Sağlam Dosya Sistemi Analizi** : NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, dahil olmak üzere yaygın dosya sistemleri için destek,
- **Unicode Dizeleri Çıkarma** : Birçok dilde ayrılmamış alandan ve bilinmeyen dosya türlerinden dizeleri çıkarır.

EKLENTİ MODÜLLERİ

VIDEO TRIYAJ

Autopsy Video Triyaj modülü bir video dosyasını rahat görüntüleyebilmek için küçük resimlere böler. Doğrudan Autopsy kullanıcı arayüzüne entegre olur. Kanun uygulayıcı, istihbarat analistleri ve müffetişler için video içeriği bakımından verimli bir modüldür.

KULLANIM DURUMLARI

- Bir içeriğin içerisinde gizlenmiş olan video dosyalarını hızlı bir şekilde tanımlamaya yarar.
- Videoyu izlemeden denk gelen bir videonun dosya içeriğinin özünü öğrenmemizi sağlar.
- Bir videoda daha fazla araştırma yapılması gereken bir durum olup olmadığını belirler.

PROJECT VIC

Mağdurları ve faailleri daha hızlı ve etkili şekilde tanımlamaya yarar. Görüntü ve verileri bir araya getirerek yerel ve uluslararası yasa uygulama kurumlarının verileri ile kıyaslama yapar. Çocuklara Karşı İnternet Suçları Görev Güçleri, federal kurumlar ve bağımsız kuruluşların desteğiyle yapılmıştır.

AUTOPSY KURULUMU

Autopsy, Kali Linux'ta kurulu olarak gelir, Windows 64bit veya 32bit işletim sistemi için de herhangi bir program gibi yükleyebiliriz. <https://www.autopsy.com/download/> adresinden Autopsy'i indirebilirsiniz.



AUTOPSY
DIGITAL FORENSICS

DOWNLOAD

ADC

Download Autopsy

VERSION 4.19.3 FOR WINDOWS

DOWNLOAD 64-BIT >

DOWNLOAD FOR LINUX AND OS X

Autopsy 4 will run on Linux and OS X. To do so:

- Download the Autopsy [ZIP file](#) (NOTE: This is not the latest version)
- Linux will need The Sleuth Kit [Java .deb Debian package](#)
- Follow the [instructions](#) to install other dependencies

3rd Party Modules

3rd party add-on modules can be found in the [Module github repository](#).

From this repository, you can download all modules or just the ones that you want.

Older Versions

You can find other versions of Autopsy at:

- Autopsy 4.4.0 and later: [GitHub](#)
- Autopsy 4.3.0 and earlier: [Source Forge](#)
- “DOWNLOAD 64-BIT” Bölümünden direk olarak 64bit Windows işletim sistemli cihazınıza son sürüm olan 4.19.3 ü indirebilirsiniz.

- “3. Party Modules” Bölümünden 3.parti modülleri indirebilirsiniz.
- “Older Versions” Bölümünden eski sürümleri indirebilirsiniz.

Advanced


Six files are made available with each release:

- autopsy-X.X.X-32bit.msi: A 32-bit Windows installer.
- autopsy-X.X.X-64bit.msi: A 64-bit Windows installer.
- autopsy-X.X.X.zip: Used for Linux and OS X installations and for module developers.
- One .asc file (GPG signature) for each of the above files.
- Source code at github.com
- Brian’s GPG Key: [local copy](#) or [MIT’s server](#)
- See the [Developer’s Guide](#) for details on the source code repository.

Bugs

See the [support](#) page for details on reporting bugs.

Announcements

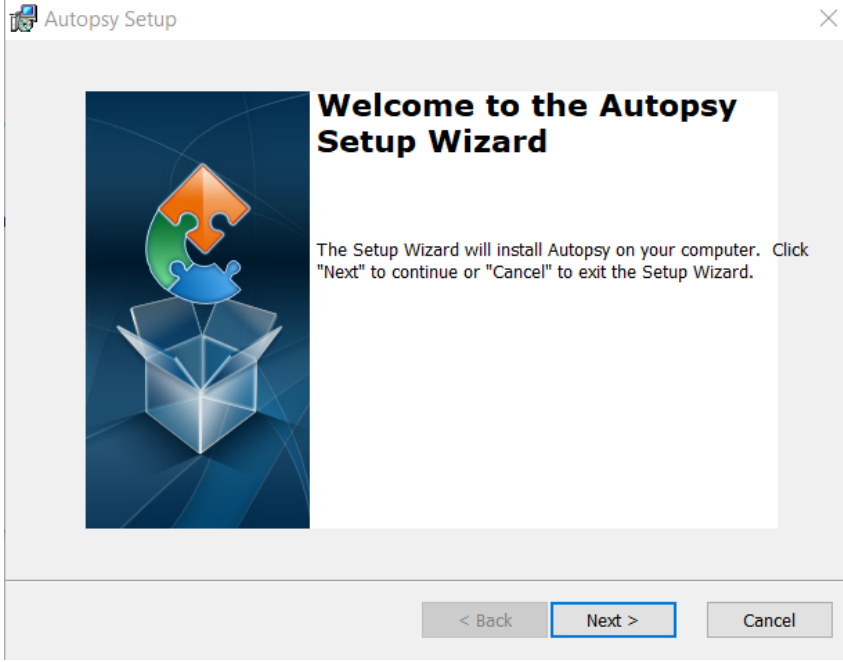
Announcements of new releases are tweeted from the [@sleuthkit](#) account, emailed to the [sleuthkit-announce](#) email list, and the RSS feed .

- “Advanced”(Gelişmiş) Bölümünden diğer yükleyici ve kaynak kodlarına ulaşabilirsiniz.
- “Bugs” Bölümünde Hataları bildirebilmek için destek sayfasına göz atabilirsiniz.

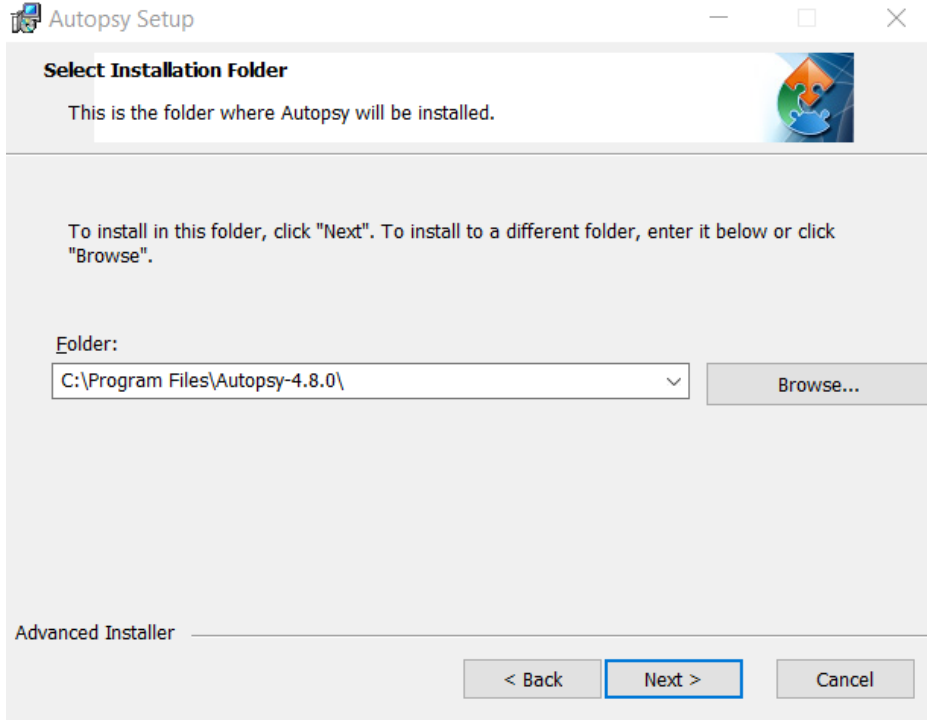
- “Announcements” Bölümünde duyurulardan haberdar olmak için sleuthkit twitter hesabına ve sleuthkit-announce e-posta hesabına ulaşabilirsiniz.

KURULUM ADIMLARI

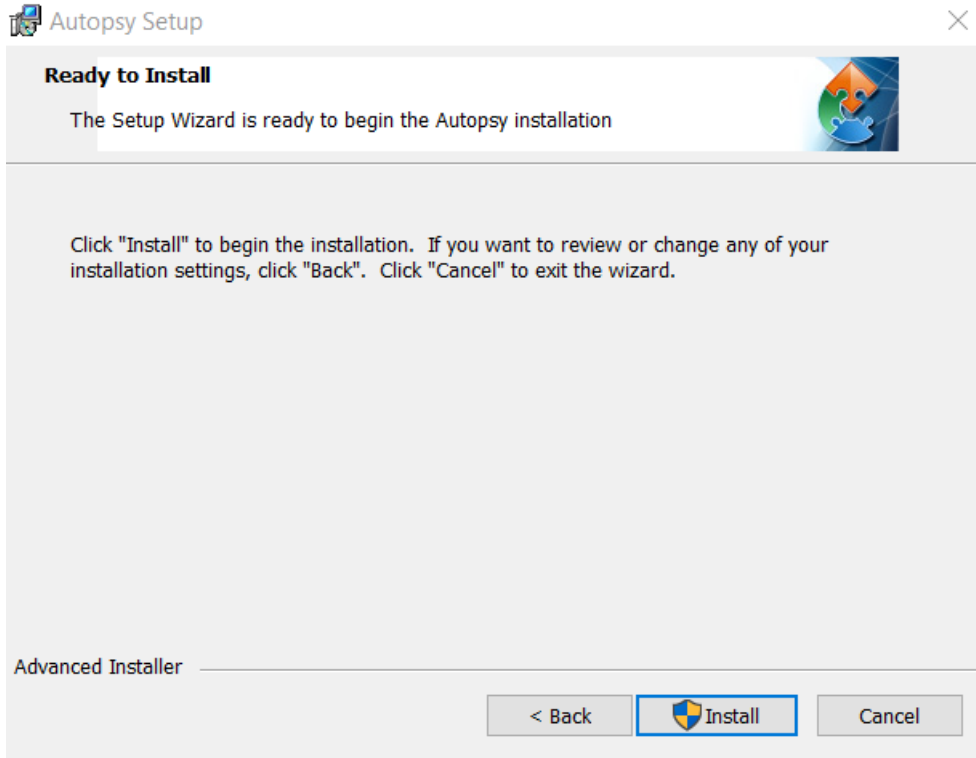
- 1- Autopsy programını yüklemek için “Next” butonuna basarak devam ediniz.



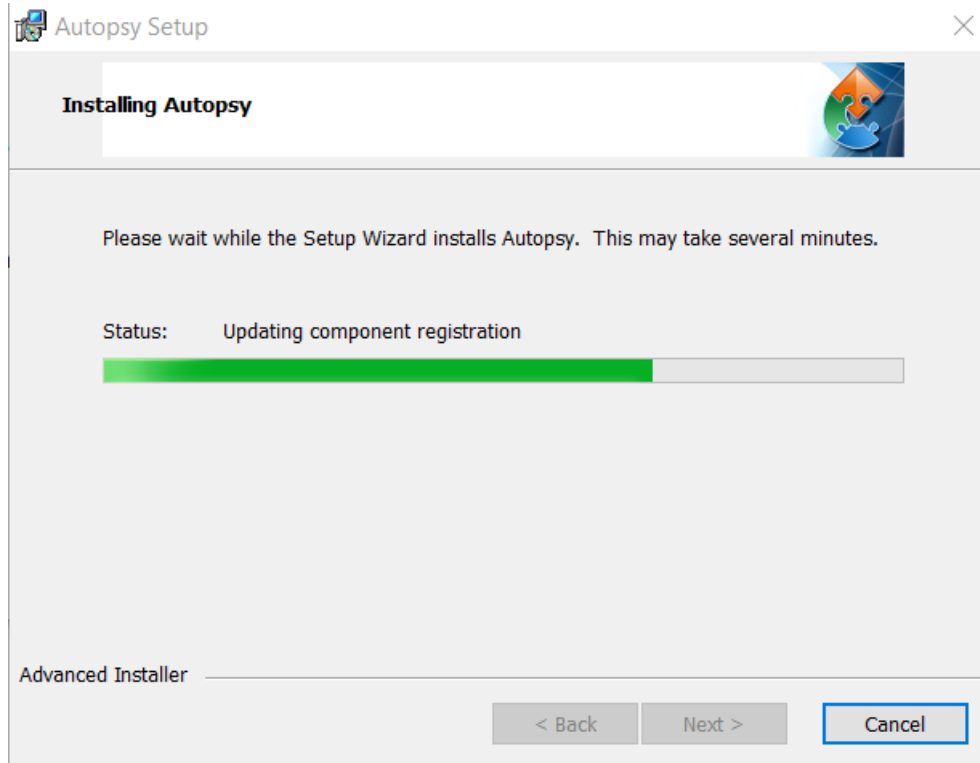
- 2- Programınızın kurulmasını istediğiniz dosya konumunu seçtikten sonra “Next” butonuna basarak devam ediniz.



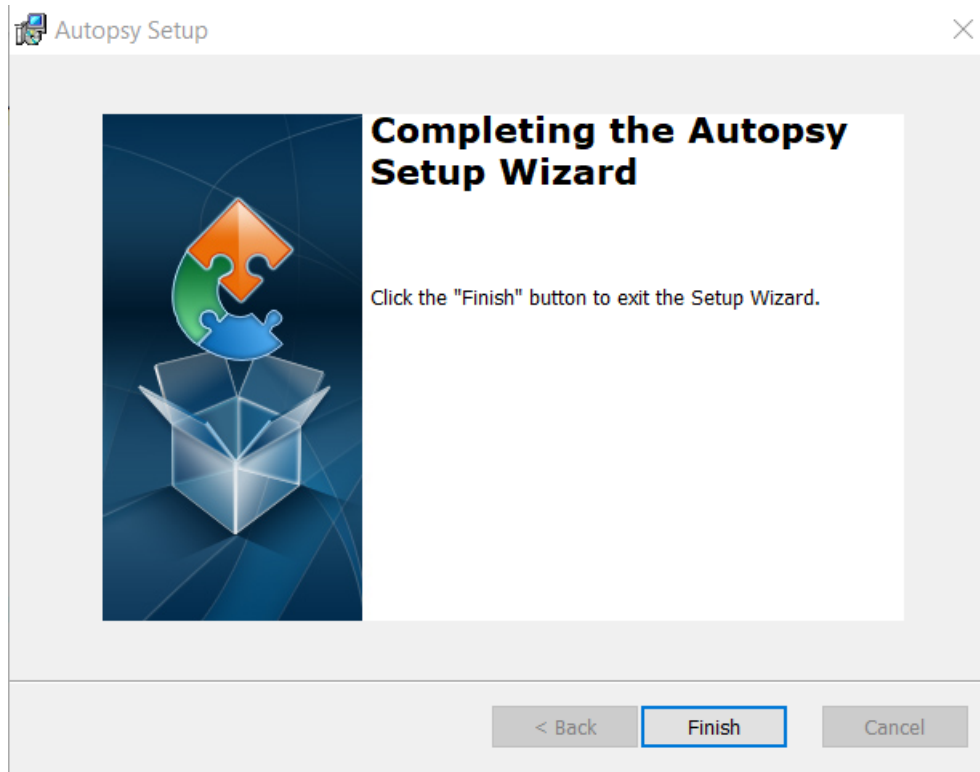
- 3- “Install” butonuna basarak devam ediniz. Bu işlem yönetici izni isteyecektir.



- 4- Yükleme işlemi birkaç dakika sürebilir, eğer daha uzun sürerse tekrar yükleme adımlarını gerçekleştirmeyi deneyebilirsiniz.



- 5- Yükleme işlemi tamamlandıktan sonra "Finish" Butonuna tıklayarak yükleyiciden çıkabilirsiniz.

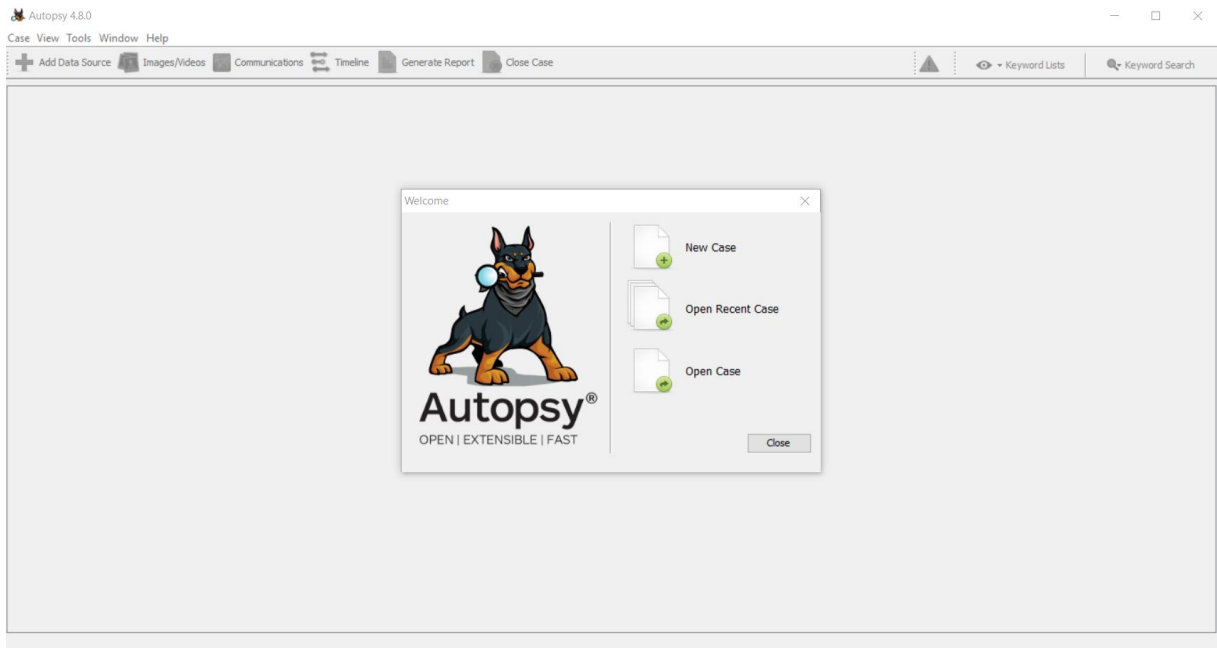


6- İlk açılışta modüller indirileceği için açılış biraz uzun sürebilir.



UYGULAMA ARAYÜZÜ

İLK GÖRÜNÜM



New Case = Yeni Dava

Open Recent Case = Son Davayı Aç

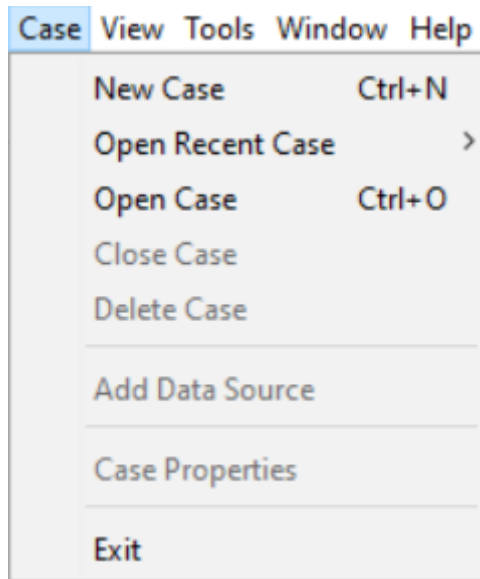
Open Case = Dava Aç

ÜST PANEL



Case View Tools Window Help

Case = Durum/Dava



New Case (Yeni Vaka) = Yeni vaka oluşturmak için kullanılır. Kısayol: Ctrl+N

Open Recent Case (Son Vakayı Aç) = Üzerine tıkladığınız zaman son vakaları ve son vakaları temizle butonunu gösterir. Vakaya tıklayarak açabilirsiniz.

Open Case (Dava Aç) = Hazırda bulunan bir davayı açmak için kullanılır.

Close Case (Davayı Kapat) = Açık olan davayı kapatır.

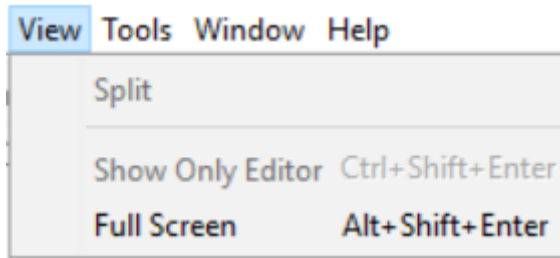
Delete Case (Davayı Sil) = Açık olan davayı siler.

Add Data Source (Veri kaynağı ekle) = Davaya veri kaynağı eklemek için kullanılır.

Case properties (Dava Özellikleri) = Açık olan davanın özelliklerini gösterir.

Exit (Çıkış) = Uygulamayı kapatır ve çıkar.

View = Görünüm

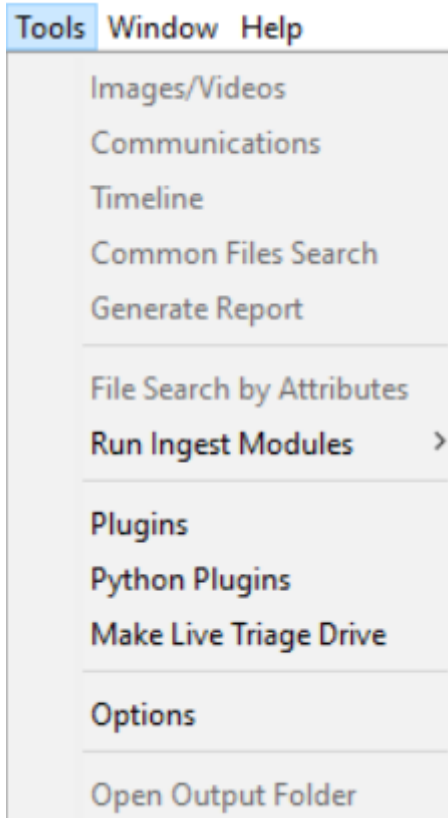


Split (Bölmek) = Ekranı kullanım alanına göre böler.

Show Only Editör (Yalnızca Düzenleyiciyi Göster) = Sadece düzenleyiciyi gösterir. Kısayol: Ctrl+Shift+Enter

Full Screen (Tam Ekran) = Tam ekran görünümüne geçer.

Tools = Araçlar



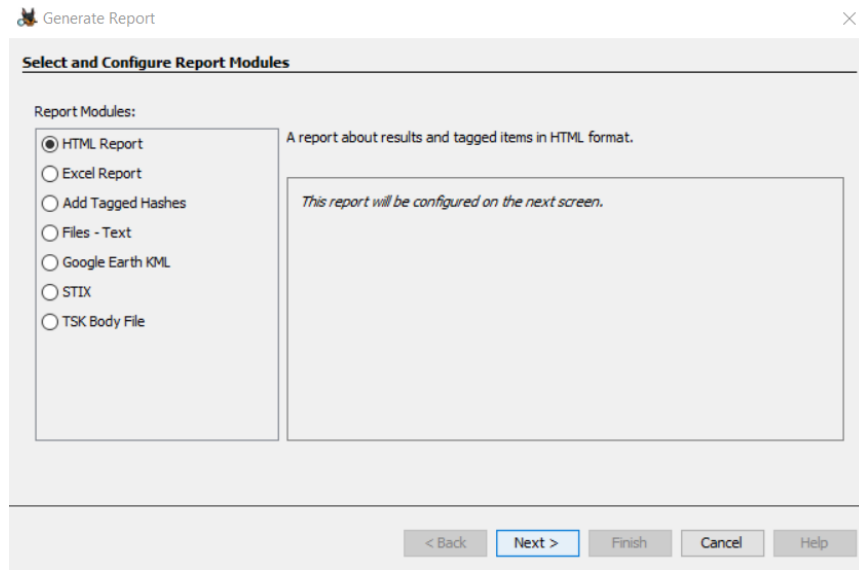
Images/Videos (Resimler/Videolar) = Resimleri veya videoları gösterir.

Communications (İletişim) =İletişim görselleştirme ve düzenleyiciyi açar.

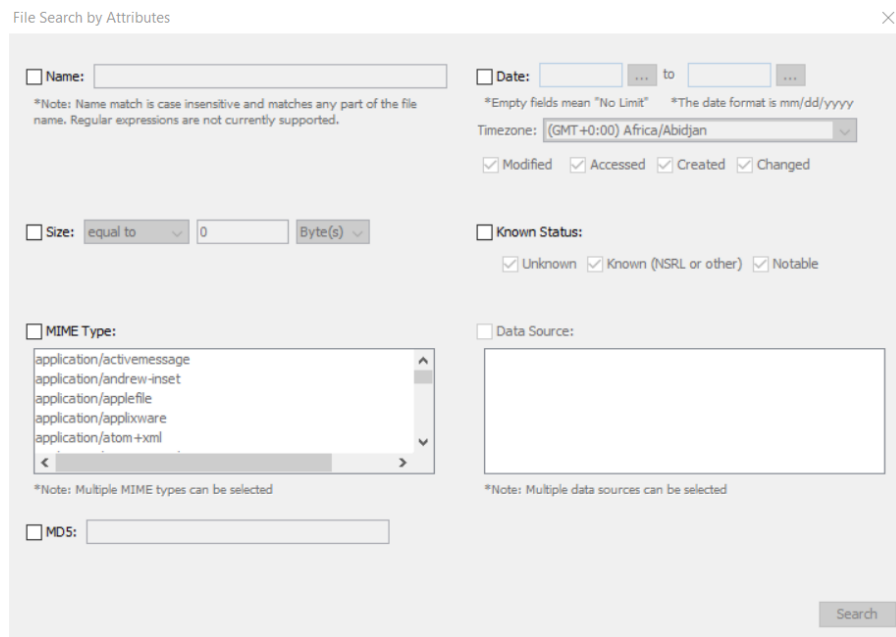
Timeline (Zaman Çizelgesi) = Oluşturulan zaman çizelgesini açar.

Common Files Search (Ortak Dosya Arama)

Generate Report (Rapor Oluştur) = Rapor oluşturma ekranını açar.

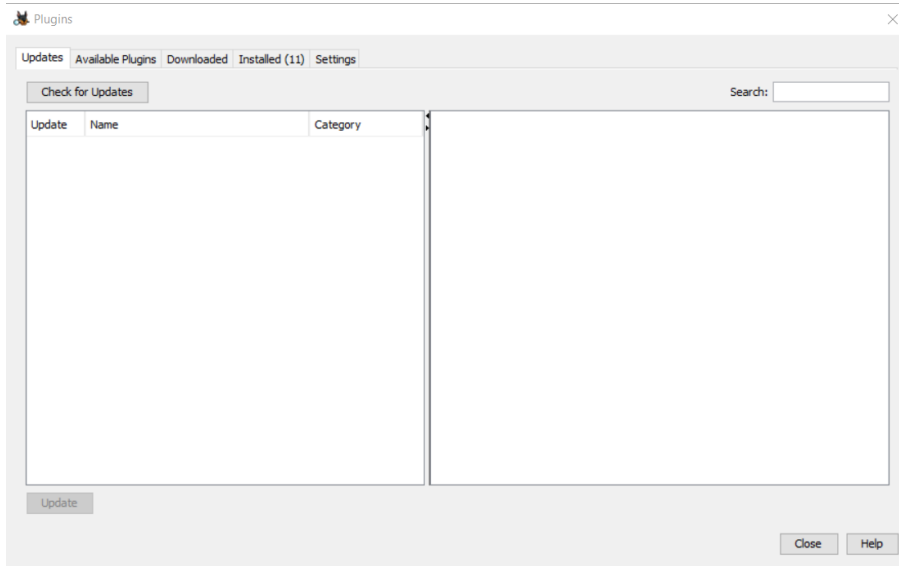


File Search by Attributes (Niteliklere Göre Dosya Arama) = İsim, boyut, tarih, MIME türü veya MD5 değerine göre arama yapılabilir.



Run Ingest Modules (Alınan Modülleri Çalıştırın) = Sahip olunan modülleri gösterir ve çalıştırır.

Plugins (Eklentiler) = Eklentiler ekranını açar bu ekrandan Güncellemeleri, mevcut eklentileri, indirilenleri, yüklenenleri ve ayarlar bölümlerini görebilirsiniz. Installed(Yüklenenler) ekranından modülleri aktif veya deaktif edebilirsiniz. Seçtiğiniz modülleri silebilir veya yükleyebilirsiniz.

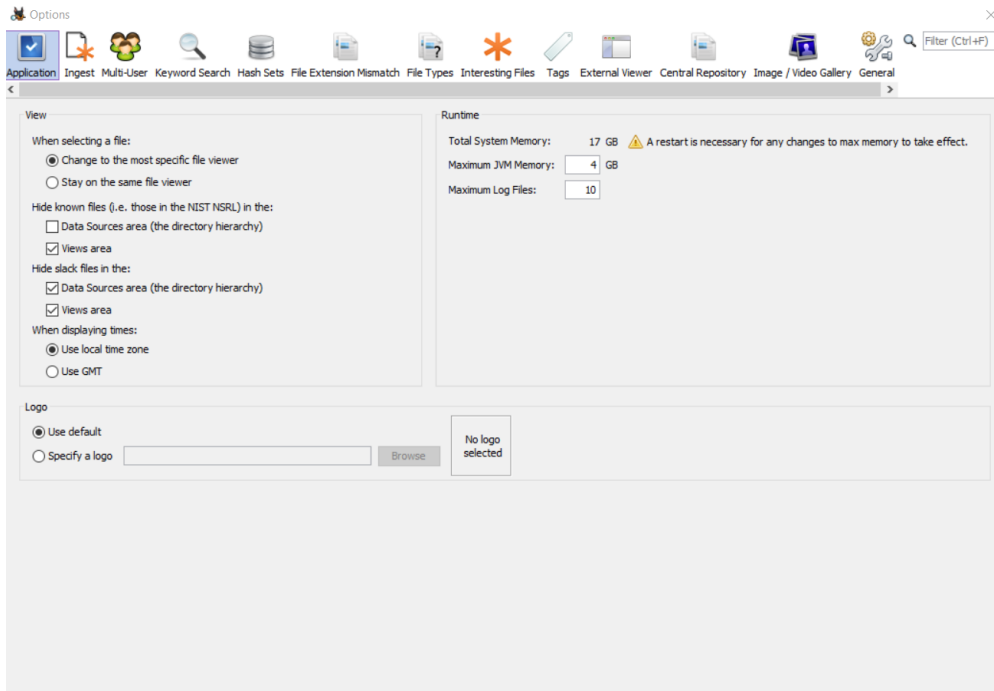


Python Plugins (Python Eklentileri) = Python eklentileri dosya dizinini açar.

Make Live Triage Drive (Canlı Triyaj Sürücüsü Yapın) = Bu özellik, uygulamayı ve toplu iş dosyasını bir sürücüye kopyalar. Yazılımı yüklemeyi analiz etmeye ve görüntülemeye izin verir.

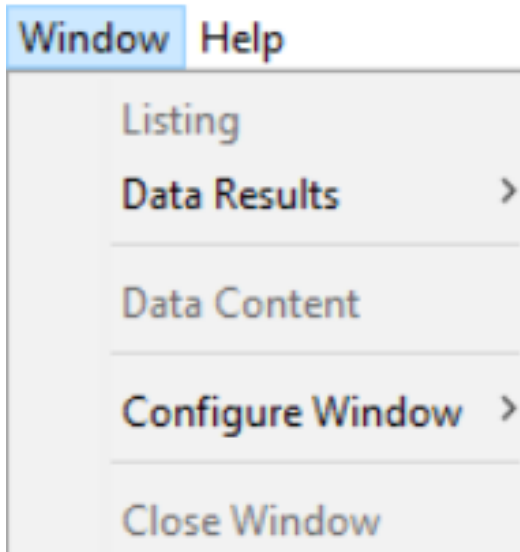
Bu sistemi analiz etmek için sürücüyü takın ve “RunFromUSB.bat” ı yönetici olarak çalıştırın. Ardından “Add Data Source” kısmından “Local Disk” i seçin.

Options (Seçenekler) = Burada bulunan seçenekler: Uygulama, İçeri Aktar, Çoklu Kullanıcı, Anahtar Kelime Araması, Hash Setleri, Dosya Uzantısı Uyuşmazlığı, Dosya Türleri, İlginç Dosyalar, Etiketler, Harici Görüntüleyici, Merkezi Bellek, Resim/Video Galerisi, Genel



Open Output Folder (Çıktı Klasörünü Aç) = Dava klasörünü açar.

Window = Pencere



Listing (Liste)

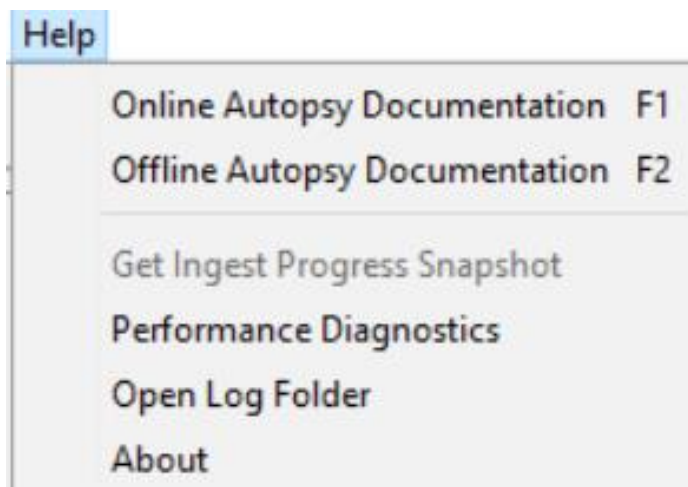
Data Results (Veri Sonuçları)

Data Content (Veri İçeriği)

Configure Window (Pencereyi Yapılandır) = Maksimize etmek, float, float grubu, küçültmek, grubu küçültmek, dock, dock grubu, klon belgesi, belgeyi böl, yeni belge sekme grubu, belge sekme grubunu daralt

Close Window (Pencereyi Kapat)

Help = Yardım



Online Autopsy Documentation (Çevrimiçi Otopsi Belgeleri)

Offline Autopsy Documentation (Çevrimdışı Otopsi Belgeleri)

Get Ingest Progress Snapshot (İlerleme Anlık Görüntülerini Alın)

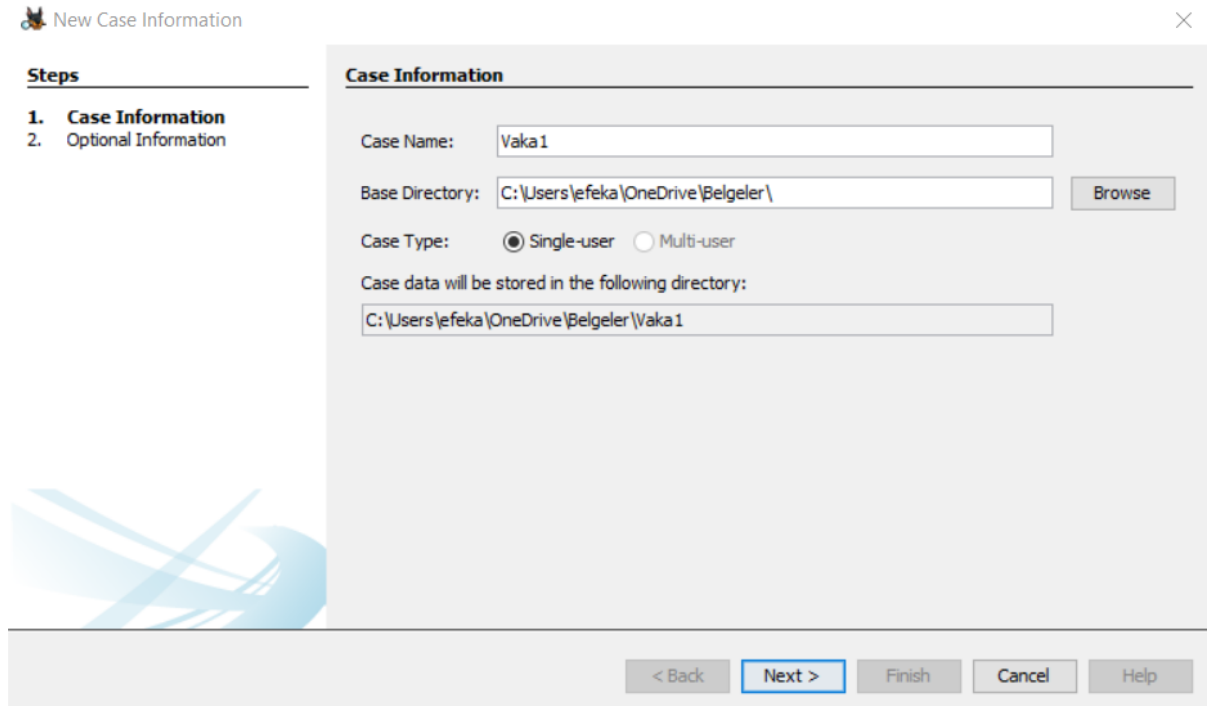
Performance Diagnostics (Performans Teşhisi)

Open Log Folder(Günlük Klasörünü Aç)

About (Hakkında)

VAKA OLUŞTURMA

Vaka oluşturmak için başlangıçta açılan pencereden “new case” yazan kısma tıklayabilirsiniz. Eğer pencere kapandıysa veya açılmadıysa Sol üstteki Case bölümünden “new case” yazan kısma tıklayabilirsiniz. Kısayolu Ctrl+N



New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: Vaka1

Base Directory: C:\Users\efeka\OneDrive\Belgeler\ Browse

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

C:\Users\efeka\OneDrive\Belgeler\Vaka 1

< Back **Next >** Finish Cancel Help

Bu kısımda Vaka ismini yazıyoruz ve Vakanın kaydedilmesini istediğimiz dizini belirtiyoruz.

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: 001

Examiner

Name: efekan

Phone: 0

Email: 0

Notes:

Organization

Organization analysis is being done for: Manage Organizations

< Back Next > Finish Cancel Help

Bu kısım eğer gerçek bir vaka incelemiyorsanız fazla önemli değildir. Vaka numarası; sorgulayan kişinin ismi, telefon numarası, e-mail adresi ve eklemek istediği notları bölümleri vardır.

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☒ Disk Image or VM File

☐ Local Disk

☐ Logical Files

☐ Unallocated Space Image File

< Back Next > Finish Cancel Help

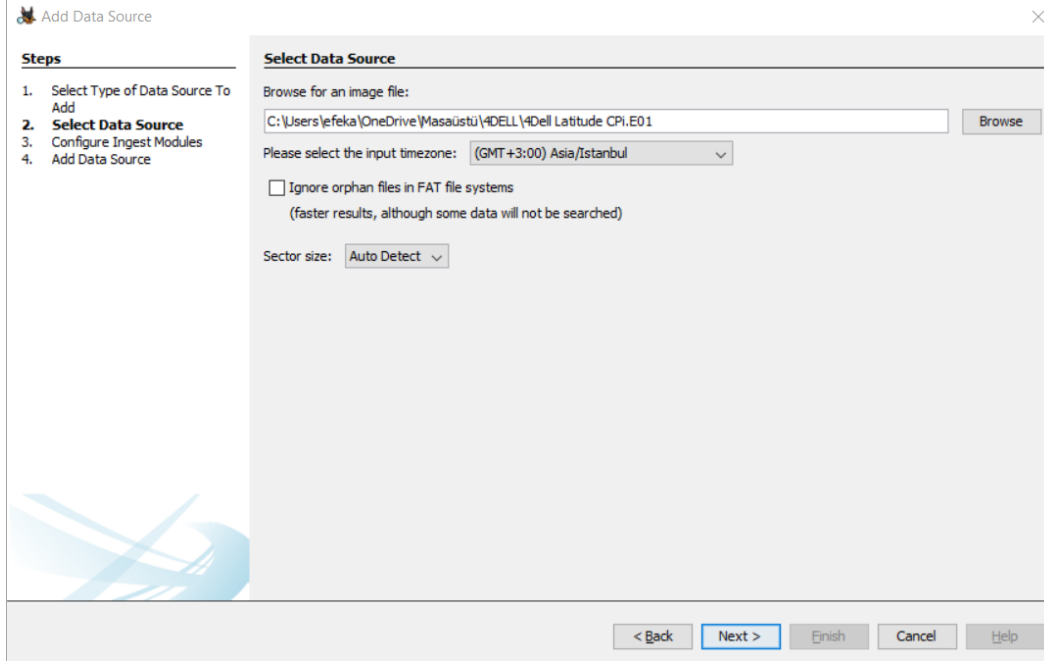
Bu kısımda eklenecek veri kaynağı türünü seçmeniz isteniyor:

Disk İmajı veya WM dosyası = Bir diskin birimlerinin içeriğini ve yapısını içeren dosyalara verilen isimdir. WM dosyası ise Windows media biçimlerinden biri için kısaltılmış sürümdür.

Yerel Disk Dosyalar = Doğrudan ana bilgisayara yüklenen bir bilgisayar sürücü dosyalarıdır.

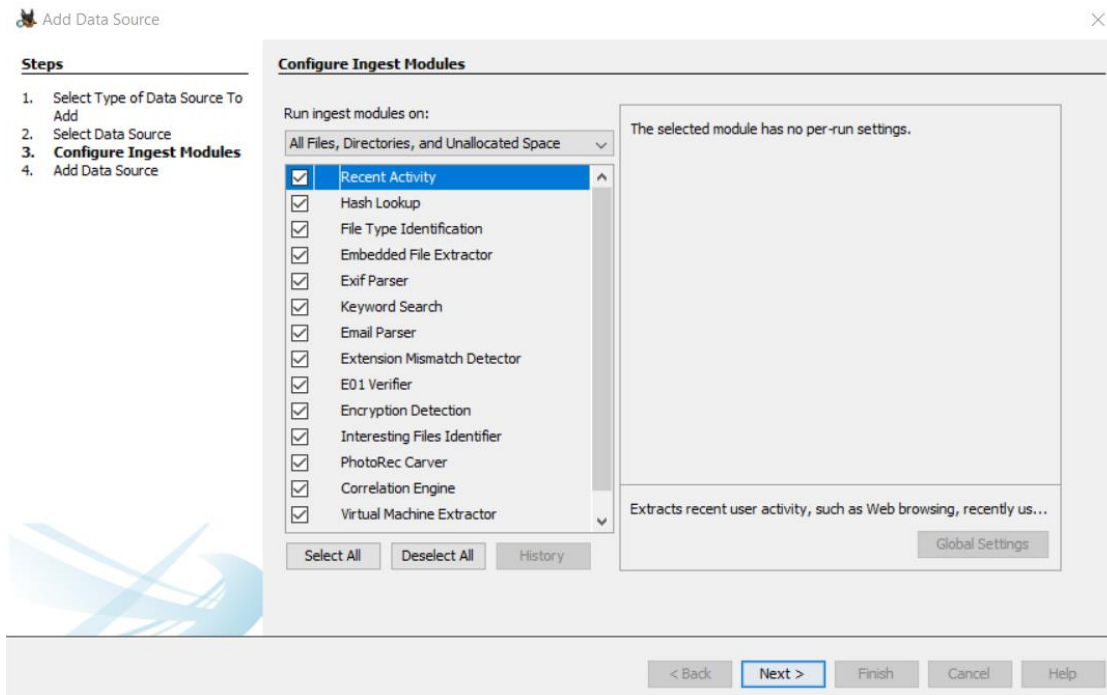
Mantıksal Dosyalar = Geleneksel bir şekilde yapılandırılmış dosya sistemlerini ilişkisel bir veri tabanı arayüzü ile birleştirilmesidir.

Ayrılmamış Alan İmajı Dosyası = Herhangi bir bölüme ayrılmamış disk alanının imaj dosyasıdır.



Bu kısımda seçtiğimiz veri kaynağı dosyasını belirtiyoruz, saat dilimini seçiyoruz ve sektör büyüklüğünü ayarlıyoruz.

Sektör büyüklüğü sabit disk sürücü gibi bir depolama ortamının özel olarak boyutlandırılmış bir bölümüdür.

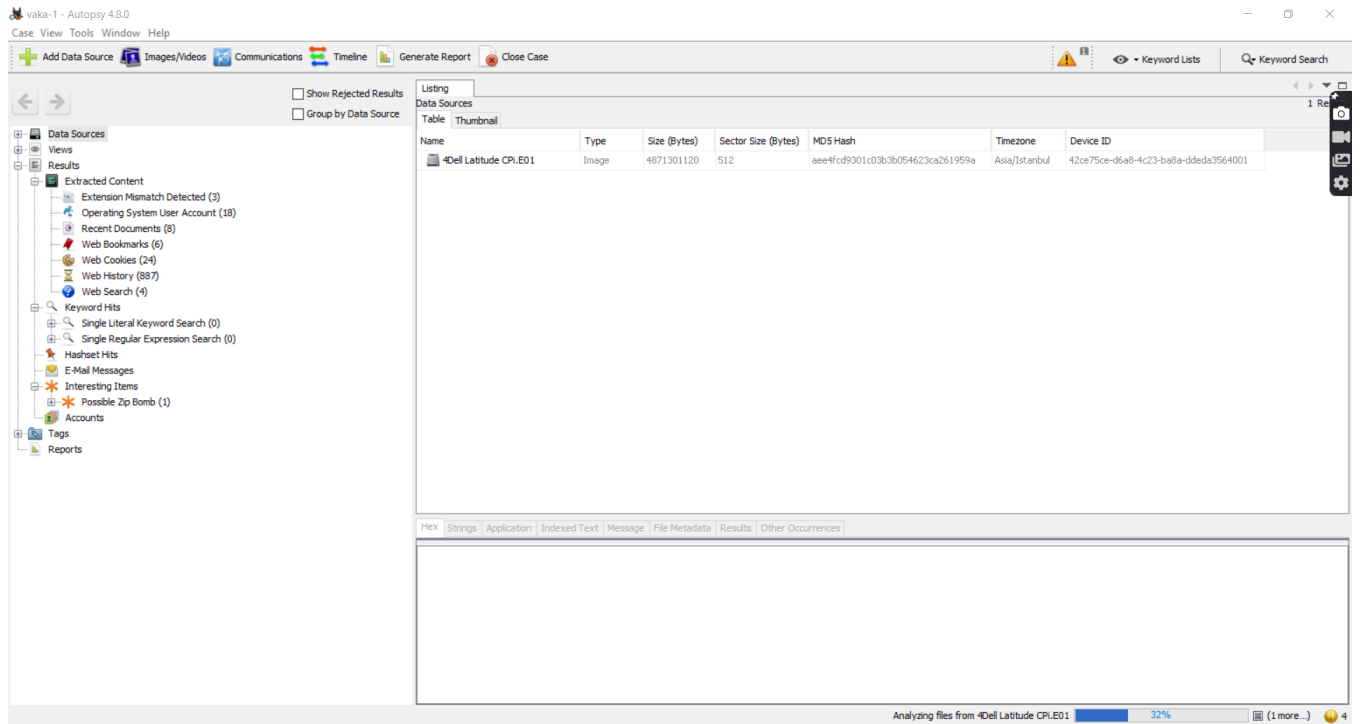


Bu kısımda alınan modülleri yapılandırabilirsiniz. Hash arama, Dosya türü tanımlayıcı, anahtar kelime araması, şifreleme algılaması vb. Bu modülleri seçebilir, seçimi kaldırabilir veya modül ayarları ekleyebilirsiniz.

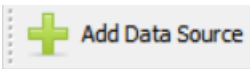
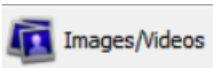
Daha sonra veri kaynağı veri tabanına eklenecek ve dosya analiz edilecek.

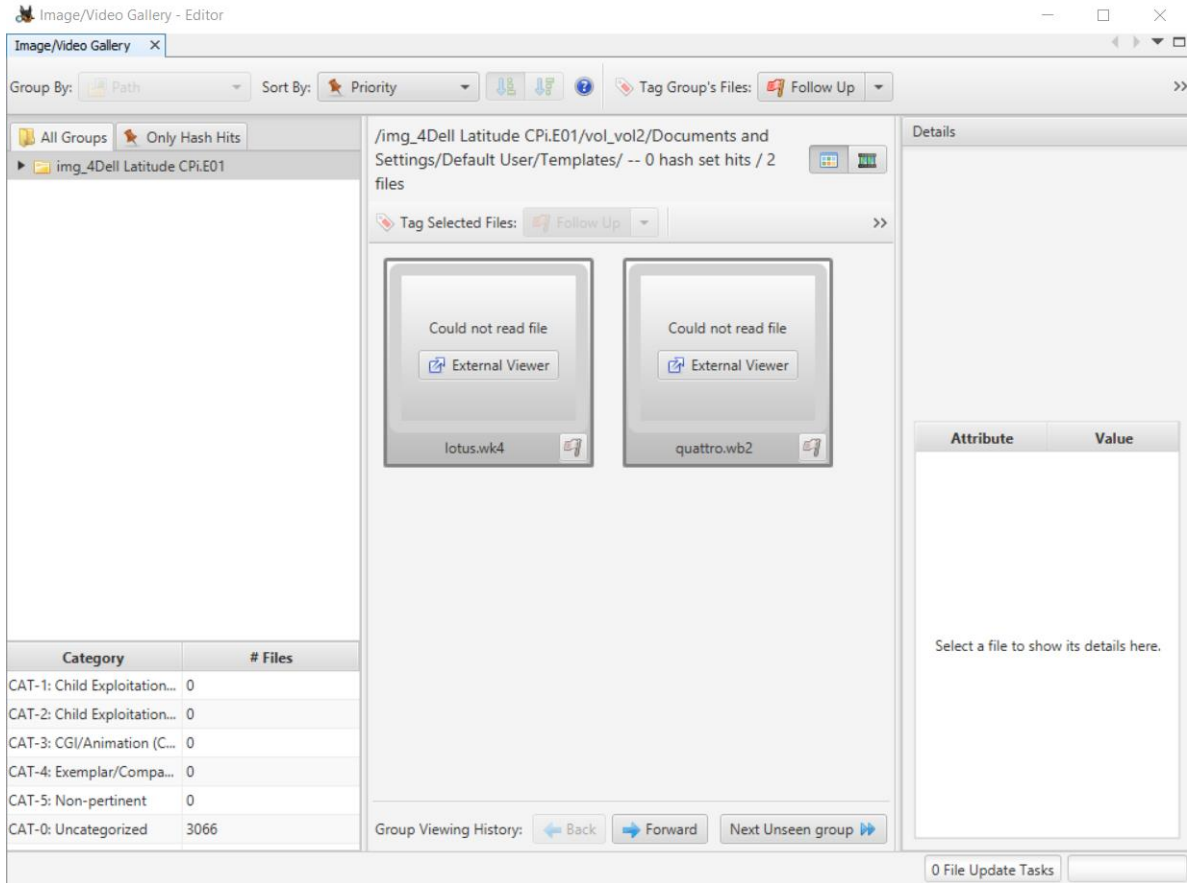
VAKA GÖRÜNÜMÜ

Vaka görünümü aşağıdaki şekildedir.



ÜST GÖRÜNÜM

-  Buraya tıklayarak veri kaynağı ekleyebilirsiniz.
-  Bu bölümde fotoğraflar ve videoları detaylı bir şekilde görebileceğiniz bir pencere açılır.



Bu kısımda fotoğrafları “Group By” bölümünden dosyaya, hashsete, kategoriye, taga, kamera marka veya modeline göre gruplayabilirsiniz. “Sort By” bölümünden önceliğe, isime veya boyuta göre sıralayabilirsiniz. “Tag Group’S Files” kısmından işaretli olanları takip edebilir yıldızlayabilir veya işaretli olmayanları görebilirsiniz.

Sol kısımda bütün gruplar veya sadece hash seçimlerini görebilirsiniz.

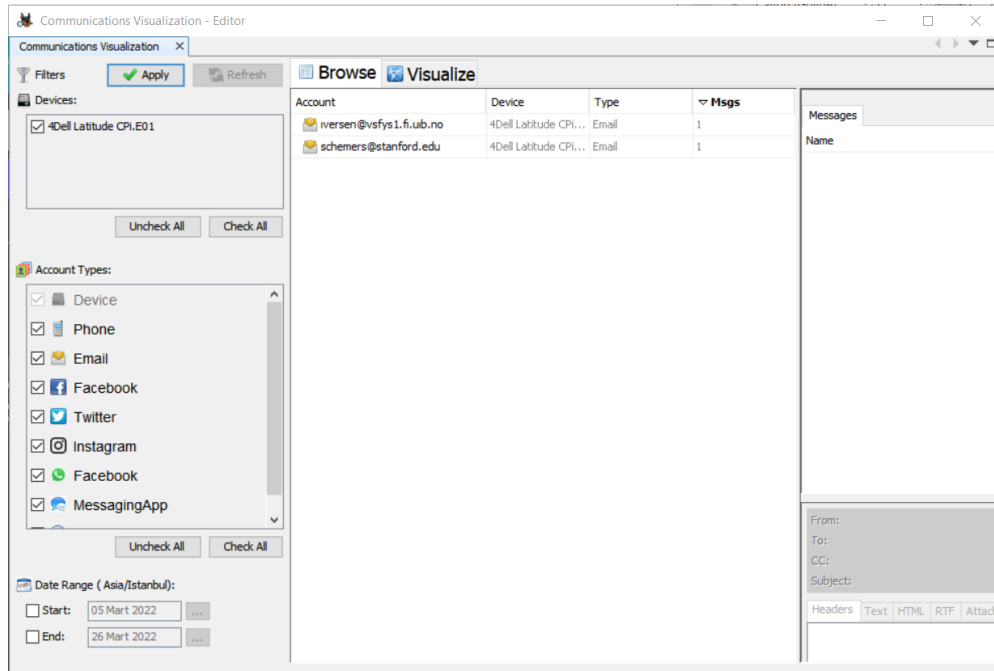
Sol alttaki kısımdan çocuk istismarı, animasyon, kopya veya ilgisiz kategorilerinde kaç adet dosya olduğunu görebilirsiniz.

Altta kısımdan grup görüntüleme geçmişini geri alabilir veya sonraki gruba geçebilirsiniz.

Attribute	Value
Name	Rhododendron.bmp
Analyzed	true
Category	CAT-0: Uncategorized
Tags	
Path	/img_4Dell Latitude CPi.E01/vol_vol2/W INDOWS/
Created Time	2004-08-20 01:24:22 EEST
Modified Time	2001-08-23 21:00:00 EEST
MD5 Hash	927a66bd587e31c b12d3ab25381658 dc
Hashset	
Camera Make	
Camera Mo...	

Sağ kısımda ise dosyayla ilgili detaylı bilgilere erişebiliyoruz. Dosya ismi, analizi, kategorisi, etiketi, yolu, oluşturma zamanı, değiştirilme zamanı, md5 formatında hash değeri, kamera marka ve modeli gibi.

-  İletişim görselleştirme ve düzenleyicisi penceresini açar.



Sol taraftaki “Devices” bölümünden cihazları işaretleyip kontrol edebilirsiniz.

Yine sol taraftaki “Account Types” bölümünden hesap türlerini seçebilirsiniz. Telefon, e-posta, facebook, twitter, instagram, whatsapp vb.

Sol alt kısımdan tarih aralığını gün, ay, yıl olarak belirleyebilirsiniz.

Ortadaki kısımdan verileri araştırabilir veya görselleştirebilirsiniz.

The screenshot shows an email client interface. At the top, there's a search bar with the text "iversen@vsfys1.fi.uib.no" and a "1 Results" indicator. Below this is a table of messages with columns: type, From, To, Date, Subject, Attms, and Tags. The first message is an "E-Mail" from "IVERSEN@VSFYS1.FI.UIB.NO" to "schemers@Stanford.EDU" dated "1992-07-27 18:54:17 EEST" with subject "FPING under VMS" and 0 attachments. Below the table, there's a detailed view of the selected email. It shows the same header information. Below the header, there are tabs for "Headers", "Text", "HTML", "RTF", and "Attachments (0)". The "Text" tab is selected, showing the email body. The body starts with "-----HEADERS-----" followed by a detailed header block containing received information, date, and sender details.

type	From	To	Date	Subject	Attms	Tags
E-Mail	IVERSEN@VSFYS1.FI.UIB.NO	schemers@Stanford.EDU	1992-07-27 18:54:17 EEST	FPING under VMS	0	

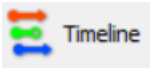
From: IVERSEN@VSFYS1.FI.UIB.NO; 1992-07-27 18:54:17 EEST
To: schemers@Stanford.EDU;
CC:
Subject: FPING under VMS

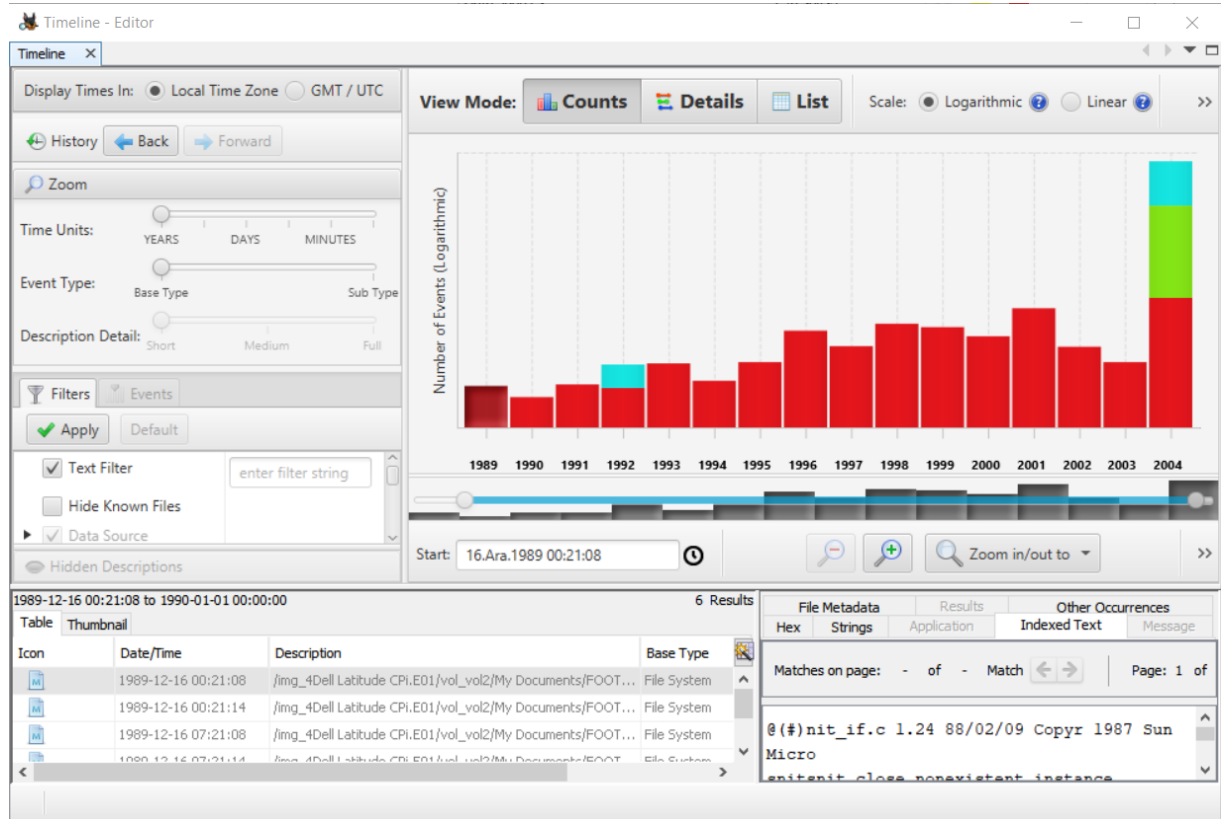
Headers Text HTML RTF Attachments (0)

-----HEADERS-----
Received: from Argus.Stanford.EDU by jessica.stanford.edu (5.59/25-eef) id AA28695; Mon, 27 Jul 92 08:54:22 PDT
Received: from vsfys1.fi.uib.no by Argus.Stanford.EDU (5.65/Inc-1.0) id AA28942; Mon, 27 Jul 92 08:54:19 -0700
Date: Mon, 27 Jul 1992 17:54:17 +0200
From: IVERSEN@VSFYS1.FI.UIB.NO (Per Steinar Iversen, Dept. of Physics, Univ. of Bergen, Norway, phone +47-5-212770)
Message-Id: <920727175417.21e004ce@VSFYS1.FI.UIB.NO>
Subject: FPING under VMS
To: schemers@Stanford.EDU
X-Vmsmail-To: SMTP%"schemers@Stanford.EDU"

Sağ üstteki kısımdan mesajları türüne, gönderene, gönderilene ve tarihe göre detaylı şekilde görebilirsiniz.

Sağ alttaki kısımda başlıkları ve metni görebilirsiniz.

-  Bu bölümde zaman çizelgesi penceresi açılacaktır.



Sol tarafta “Display Times In” bölümünden saat dilimini seçebilirsiniz.

Zaman birimini yıl, gün, dakika olarak ayarlayabilirsiniz. Etkinlik tipini belirleyebilirsiniz.

Metin filtresi, bilinen dosyaları gizle, web aktiviteleri gibi özellikleri filtreleyip uygulayabilirsiniz.

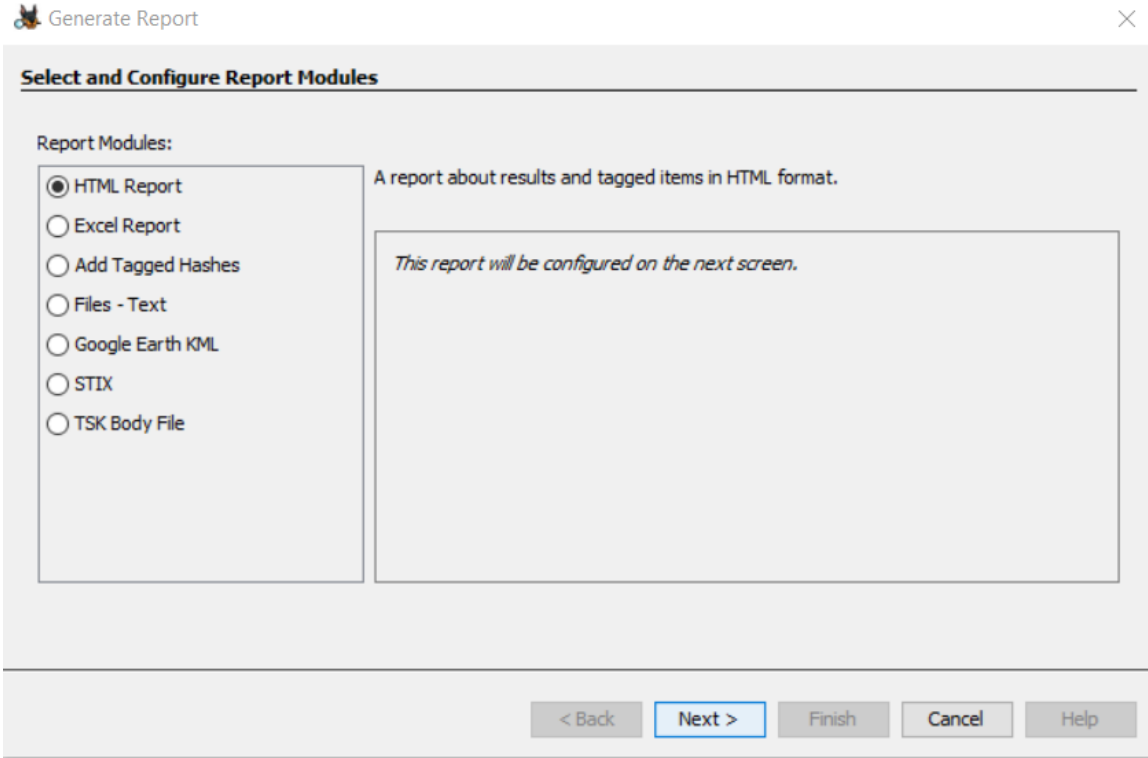
“View Mode” kısmında görünüm modunu sayılar, detaylar veya liste olarak seçebilirsiniz. “Scale” kısmında ölçeği logaritmik veya lineer olarak belirleyebilirsiniz. “Snapshot Report” ile anlık görüntü raporu alabilirsiniz. “Refresh View” ile görünümü yenileyebilir, “Update DB” ile veri tabanını güncelleyebilirsiniz.

Orta kısımda olaylar logaritmik olay sayısı zaman grafiğini görebilirsiniz.

Alt kısımda verileri tablo veya küçük resim olarak listeleyebilirsiniz. Bu tabloda simge, tarih, sat ve tanım bilgileri yer almaktadır.

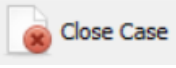
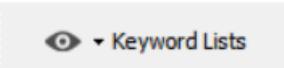
Sağ alt kısımda detaylı eşleşmeleri görebilirsiniz.

-  Bu kısımdan rapor oluştur penceresine erişebilirsiniz.



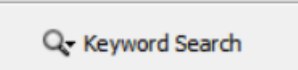
HTML ve excel raporu oluşturabilirsiniz. Etiketli hash ekleyebilir ve vb. modülleri seçebilirsiniz.

Raporu yapılandırabilir hangi veriler hakkında rapor oluşturmak istediğinizi seçebilirsiniz.

-  Close Case Buraya tıklayarak vakayı kapatabilirsiniz.
-  Keyword Lists Anahtar kelime listesini gösterir.

Telefon numaraları, e-posta adresleri, URI'ler, kredi kartı numaraları verilerini isim ve anahtar kelime bilgileri ile sıralar.

Aramayı seçili veri kaynaklarıyla sınırlayabilirsiniz.

-  Keyword Search Buraya tıklayarak anahtar kelime araması yapabilirsiniz.

Aramayı tam eşleşme, alt dizi eşleşme veya normal ifade şeklinde özelleştirebilirsiniz.

Aramayı seçilen veri kaynağı ile sınırlayabilirsiniz.

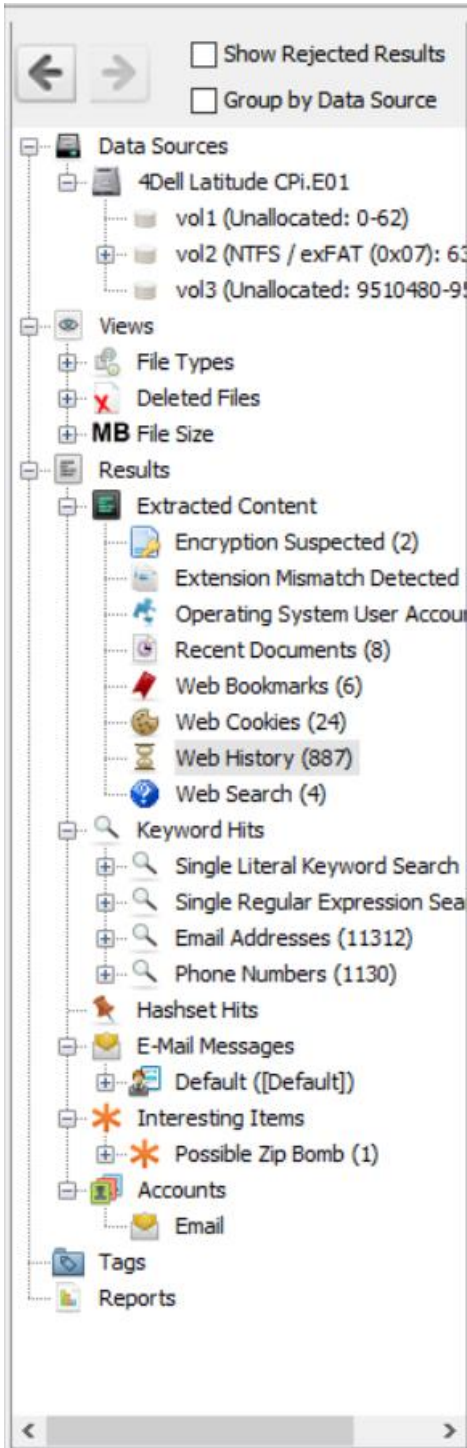
ALT GÖRÜNÜM



Seçilen veri kaynağından analiz edilen dosyaların yüzde cinsinden oranını görebilirsiniz.

Engel işaretli kısımdan ise oluşan hataları görebilirsiniz.

SOL GÖRÜNÜM



Burada seçtiğimiz veri kaynağındaki bütün verilere ulaşabiliriz.

“Show Rejected Results” butonu ile reddedilen sonuçları görebilirsiniz.

“Group by Data Source” butonu ile Veri kaynağına göre gruplama yapabilirsiniz.

AŞAĞIDAKİ KIRMIZI İLE YAZILAN BÖLÜMLERİN AÇIKLAMALARI YER ALMAKTADIR:

Data Sources Bu bölümde veri kaynakları listelenir

Veri kaynağının vol1, vol2 ve vol3 biçiminde dosya sistemleri yer alır. Vol2 NTFS dosya sistemidir.

Views Bu kısımdan dosya görünümünü File Types Deleted Files ve File Size olarak gruplayabilirsiniz.

File Types Dosya türleri

Deleted Files Silinen dosyalar

File Size Dosya boyutu

Results Sonuçlar bölümünde Extracted Content, Keyword Hits, E-mail Messages, Interesting Items ve Accounts bölümleri yer almaktadır.

Extracted Content Çıkarılan içerikler bölümü. Bu bölümde Encryption Suspected, Extension Mismatch Detected, Operating System User Account, Recent Documents, Web Bookmarks, Web Cookies, Web History ve Web Search yer almaktadır.

Encryption Suspected Şifreleme şüphesi bulunanlar

Extension Mismatch Detected Uzantı değişimi algılananlar

Operating System User Account İşletim sistemi kullanıcı hesabı

Recent Documents Son belgeler

Web Bookmarks Web yer imleri

Web Cookies Web çerezleri

Web History Web geçmişi

Web Search Web aramaları

Keyword Hits Anahtar kelime isabetleri burada gruplanır.

Single Lieral Keyword Search Tek değişmez anahtar kelime arama

Single Regular Expression Search Tek normal ifade arama

Email Addresses E posta adresleri

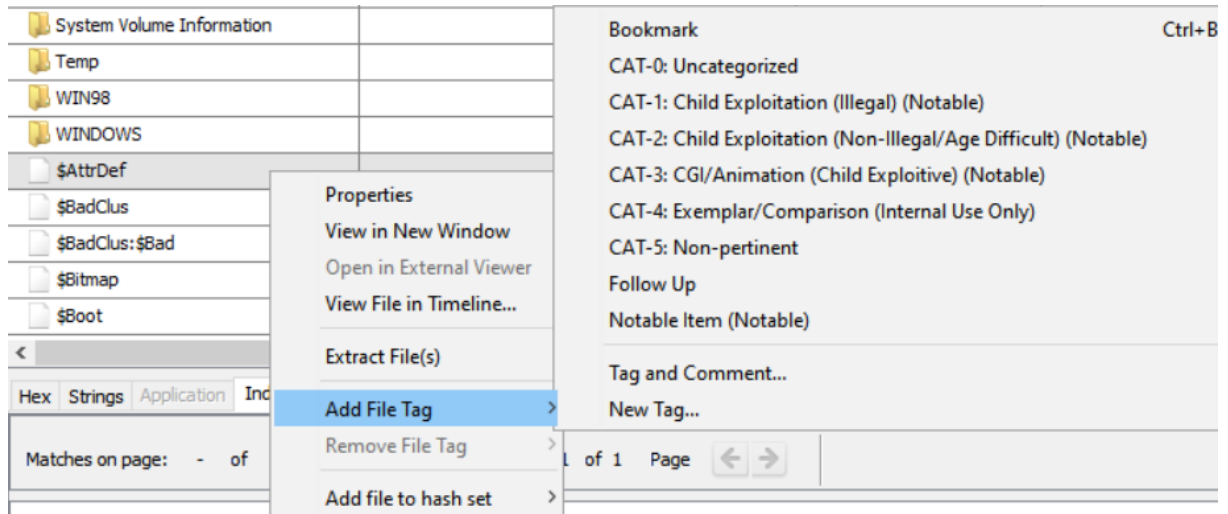
Phone Numbers Telefon numaraları

Hashset Hits Hashset Hitleri

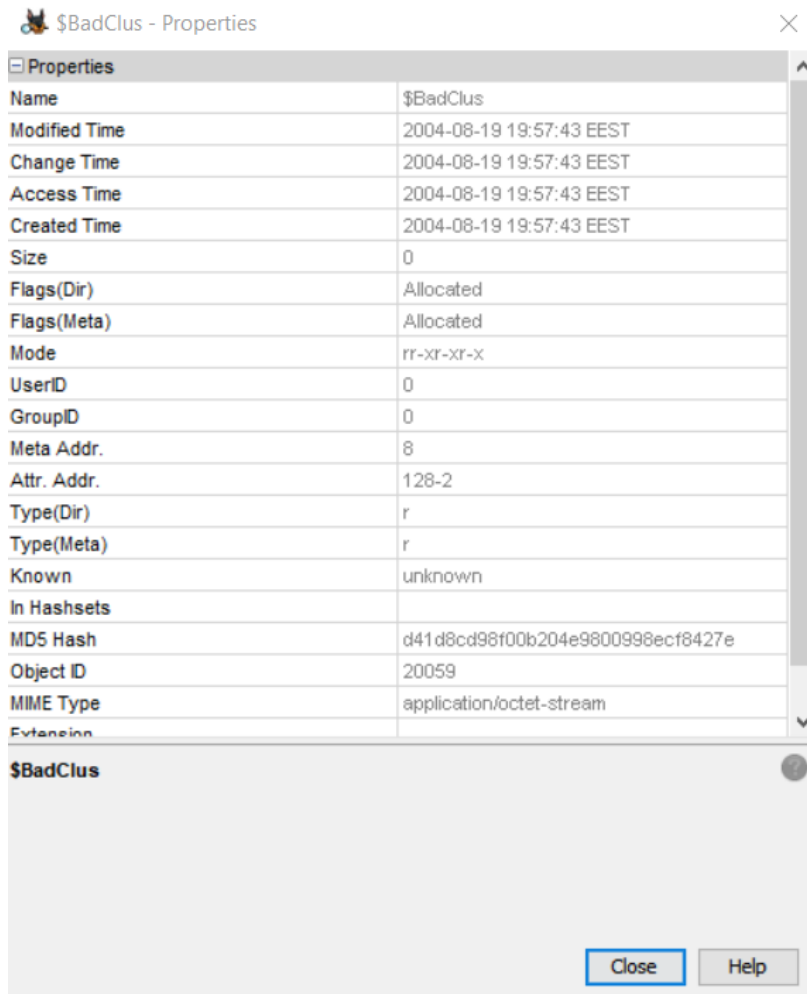
E-mail Messages E posta mesajları burada yer alır.

Alt kısımda ise hex, string, uygulama index metni, mesaj, dosya metadatası ve sonuç gibi veriler yer alır.

SAĞ TIKLAMA



Properties bölümünde dosya hakkındaki özellikleri gösterir.



Bu kısımda dosyanın ismi, konumu, oluşturulma zamanı, değiştirilme zamanı, boyutu, yetkileri, kullanıcı bilgileri, grup bilgileri, meta adresi hash değerleri gibi bilgiler yer alır.

View in New Window 'e tıklayarak yeni pencerede açabilirsiniz.

Open in External Viewer Dosyayı External'de açar

View File in Timeline Zaman çizelgesinde görüntüle

Extract File(s) Dosyayı bilgisayarınıza indirmek için buraya tıklayabilirsiniz.

Add File Tag Dosyaya etiket eklemek için kullanılır.

Remove File Tag Etiketi kaldırır.

Add file to hash set Hash setine dosya ekler.

Add File Tag butonu ile yer imlerine veya yasadışı olaylar bölümüne ekleyebilirsiniz. Yeni tag oluşturabilir, takip edebilir veya etiketleyip yorumlayabilirsiniz.