Autopsy 4.22.1

AUTOPSY 4.22.1 İLE DİJİTAL ADLİ BİLİŞİM İNCELEMELERİ

Türkçe Kullanım Kılavuzu ve Uygulamalı Analiz Rehberi

Bu kitap, Autopsy 4.22.1 sürümünü Türkçe ve uygulama odaklı biçimde öğrenmek isteyen kullanıcılar için hazırlanmıştır.

RECEP ŞENEL
redzeptech@recepsenel.com

Website : www.recepsenel.com

İçindekiler

İthaf

Bu kitap; Dijital dünyada gerçeğin, yalnızca teknolojiyle değil; hukuk, etik ve vicdanla birlikte anlam kazandığına inananlara…

Bir log kaydının, bir zaman damgasının, bir silinmiş dosyanın sadece teknik veri değil;
bazen bir hakkın, bazen bir mağduriyetin, bazen de adaletin sessiz tanığı olduğunu bilenlere…

Bilişimi yalnızca sistem kurmak, kod yazmak, araç kullanmak olarak değil; sorumluluk,
disiplin ve doğru olanı koruma bilinciyle ele alanlara…

Hukukun üstünlüğünü, delil bütünlüğünü, insan haklarını ve mesleki etiği, teknik bilginin ayrılmaz parçası görenlere…

Sahada, masa başında, mahkeme salonunda ya da bir olayın sessiz izleri arasında;
gerçeğe sadık kalmaya çalışan tüm analistlere, bilişimcilere, hukukçulara ve adalet arayışına emek verenlere ithaf edilmiştir.

Çünkü dijital dünyada, en güçlü savunma; doğru yöntem, sağlam delil ve adalete bağlılıktır.

Önsöz

Dijitalleşen dünyada artık her adımımız, her kararımız ve hatta her niyetimiz dijital birer iz bırakıyor. Bir zamanlar "tozlu dosyalar" arasında aranan gerçekler, bugün milyarlarca satır log kaydının, silinmiş veri bloklarının ve karmaşık dosya sistemlerinin derinliklerinde gizli. Dijital adli bilişim (Digital Forensics), işte bu sessiz izleri konuşturma sanatıdır.

Bu kitap, sadece bir yazılımın kullanım kılavuzu değildir. Bu çalışma; yıllar süren saha deneyiminin, yüzlerce vaka incelemesinin ve "verinin dili"ne duyulan merakın bir sonucudur. Autopsy 4.22.1 gibi güçlü bir aracı merkezine alırken, asıl amacı analiste araçtan bağımsız bir bakış açısı kazandırmaktır. Çünkü dijital dünyada her işlem bir iz bırakır; ancak bu izi anlamlı bir kanıta dönüştüren şey, analistin metodolojik yaklaşımı ve teknik disiplinidir.

Kitap boyunca, Autopsy'nin teknik imkanlarını en uç noktaya kadar zorlayacağız. Kurulumdan başlayarak; bellek analizinin karanlık koridorlarından bulut artefaktlarının karmaşıklığına, anti-forensics teknikleriyle mücadeleden mahkemede sunulacak raporun titizliğine kadar geniş bir yelpazeyi ele alacağız.

Bu eseri hazırlarken temel motivasyonum, ülkemizdeki Türkçe kaynak eksikliğini bir nebze de olsa gidermek ve bu mesleğe gönül vermiş profesyonellere güvenilir bir rehber sunmaktır. Unutmayın; bir analist sadece log okuyan biri değil, verinin bıraktığı boşlukları da anlamlandıran bir dedektiftir.

Işığın sadece aydınlık yerlere değil, diskin en karanlık sektörlerine de ulaşması dileğiyle…

Recep Şenel

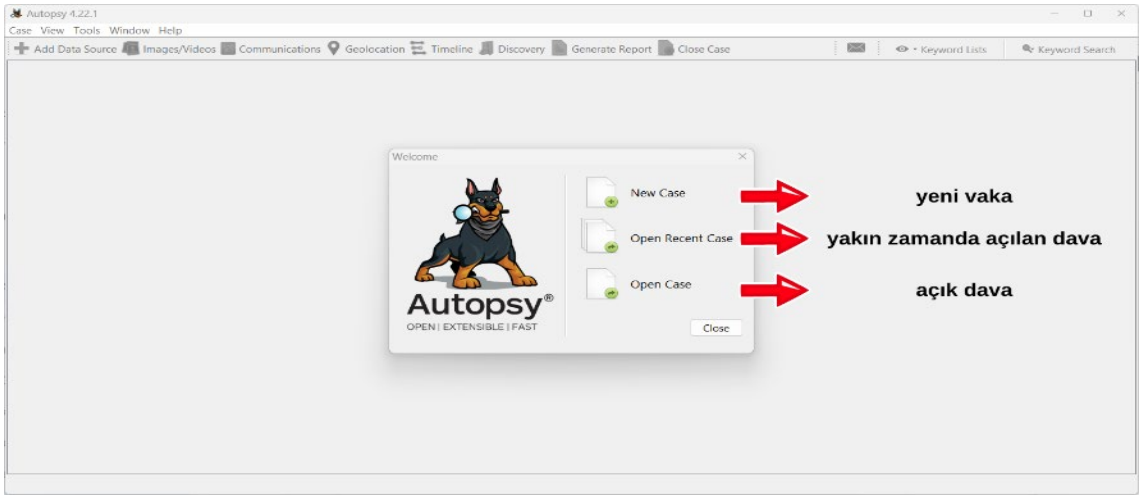
Bölüm 1: Autopsy'ye Giriş ve Ekosistem Analizi

1.1. Autopsy Nedir?

Autopsy, dijital adli bilişim süreçlerinde ham verilerin analiz edilmesi, kanıtların ayıklanması ve olay yeri incelemesinin dijital boyutta gerçekleştirilmesi için tasarlanmış, açık kaynaklı bir dijital inceleme platformudur. Temelde, arka planda çalışan Sleuth Kit (TSK) kütüphanelerinin grafik kullanıcı arayüzü (GUI) olarak işlev görse de, güncel versiyonları (özellikle 4.22.x serisi) ile tek başına kapsamlı bir analiz motoruna dönüşmüştür. Dünya çapında kolluk kuvvetleri, askeri birimler ve kurumsal olay müdahale (Incident Response) ekipleri tarafından güvenilirliği ve modüler yapısı nedeniyle standart bir araç olarak kabul edilir.Dijital dünyada yapılan her işlem, çoğu zaman görünmeyen ama silinmesi zor izler bırakır. Bir dosyanın açılması, silinmesi, taşınması; bir internet sitesine girilmesi; bir USB belleğin takılması; hatta sistem saatindeki küçük bir oynama bile bir olayın parçası olabilir.İşte bu noktada Autopsy, dijital delillerin sistematik biçimde incelenmesini sağlayan güçlü bir adli bilişim analiz platformudur.

Autopsy; disk imajları, klasör yapıları, silinmiş dosyalar, internet geçmişi, e-posta kayıtları, zaman çizelgeleri ve kullanıcı aktiviteleri gibi çok sayıda dijital artefaktı analiz ederek olayın teknik hikâyesini ortaya çıkarmaya yardımcı olur.

Bu araç yalnızca bir yazılım değil; aynı zamanda bir olayın izini sürmek için kullanılan metodolojik bir inceleme ortamıdır. Autopsy; disk imajlarının analizi, akıllı telefon incelemeleri ve siber olay müdahale süreçlerinde kullanılan, dünya çapında kabul görmüş, açık kaynaklı ve modüler bir dijital adli bilişim (digital forensics) platformudur. Temelini **The Sleuth Kit (TSK)** kütüphanesinden alan bu araç, karmaşık komut satırı işlemlerini kullanıcı dostu bir grafik arayüzle (GUI) birleştirir.



Tablo: Bir Bakışta Autopsy Operasyonel Profili

Özellik	Açıklama	Analist İçin Önemi
Lisans Modeli	Açık Kaynak (Open Source / Apache 2.0)	Ücretsiz kullanım ve topluluk desteği ile sürekli güncellenme.
Çekirdek Yapı	The Sleuth Kit (TSK) tabanlı	Güçlü ve güvenilir dosya sistemi analiz motoru.
Platform Desteği	Windows (Yerel), Linux/macOS (Sınırlı)	Windows üzerinde en stabil ve performanslı çalışma deneyimi.
Analiz Yöntemi	Otomatik Ingest Modülleri	Saatler süren manuel işlemleri dakikalar içinde otomatiğe bağlama.
Dosya Sistemi	NTFS, FAT, exFAT, HFS+, UFS, Ext2/3/4	Hemen hemen tüm depolama birimlerinden veri çekebilme yeteneği.
Geliştirilebilirlik	Python (Jython) ve Java API desteği	İhtiyaca özel yeni analiz modülleri tasarlayabilme esnekliği.

1.2. Temel Operasyonel Kabiliyetler

Autopsy'yi rakiplerinden ayıran ve profesyonel analizlerde tercih edilmesini sağlayan temel özellikler şunlardır:

- Çoklu Dosya Sistemi Desteği: NTFS, FAT, exFAT, HFS+, UFS ve Ext2/3/4 gibi geniş bir yelpazede dosya sistemi analizi gerçekleştirir.
- Modüler Analiz (Ingest Modules): Veri setleri sisteme dahil edildiği anda (ingest süreci); anahtar kelime arama, hash eşleştirme, EXIF verisi çıkarma ve web geçmişi analizi gibi işlemleri eşzamanlı olarak yürütür.
- Timeline (Zaman Çizelgesi) Analizi: Olayın kronolojik akışını görselleştirerek, şüpheli aktivitelerin birbiriyle olan korelasyonunu ortaya koyar.
- Artefakt Kurtarma: Silinmiş dosyaların geri getirilmesi, "unallocated space" (tahsis edilmemiş alan) taraması ve kayıt defteri (registry) analizi gibi kritik forensic işlemlerini otomatikleştirir.

Profesyonel Not: Autopsy, sadece bir "dosya görüntüleyici" değil; bir disk imajı içerisindeki milyarlarca baytlık veri yığını arasından anlamlı kanıtı (probative evidence) ayıklayan bir karar destek mekanizmasıdır.

1.3. Neden Autopsy 4.22.1

4.22.1 sürümü, bellek yönetimi ve büyük veri kümelerindeki (Big Data) indeksleme performansı açısından önceki sürümlere göre stabilize edilmiştir. Bu kitapta, bu sürümün sunduğu güncel veri işleme mimarisi üzerinden ilerleyeceğiz.

Autopsy'nin en büyük avantajı, karmaşık dijital delilleri anlaşılır hale getirmesidir.

Sağladığı temel faydalar

- Delil bütünlüğünü korur
- Hash doğrulama yapar
- Silinmiş dosyaları tespit eder
- Web geçmişini çıkarır
- Şüpheli kullanıcı hareketlerini analiz eder
- Zaman çizelgesi üretir
- Olay korelasyonu sağlar
- Mahkemeye uygun rapor üretimine destek verir

Autopsy'nin Tanımı

Autopsy, açık kaynak kodlu bir dijital adli bilişim (DFIR) platformudur.

Temel amacı:

- Dijital delilleri bozmadan incelemek
- Sistem üzerindeki kullanıcı aktivitelerini ortaya çıkarmak
- Silinmiş/veri kalıntılarını analiz etmek
- Olay zaman çizelgesi oluşturmak
- Delilleri raporlamak

Teknik altyapı

Autopsy şu temel bileşenler üzerine kuruludur:

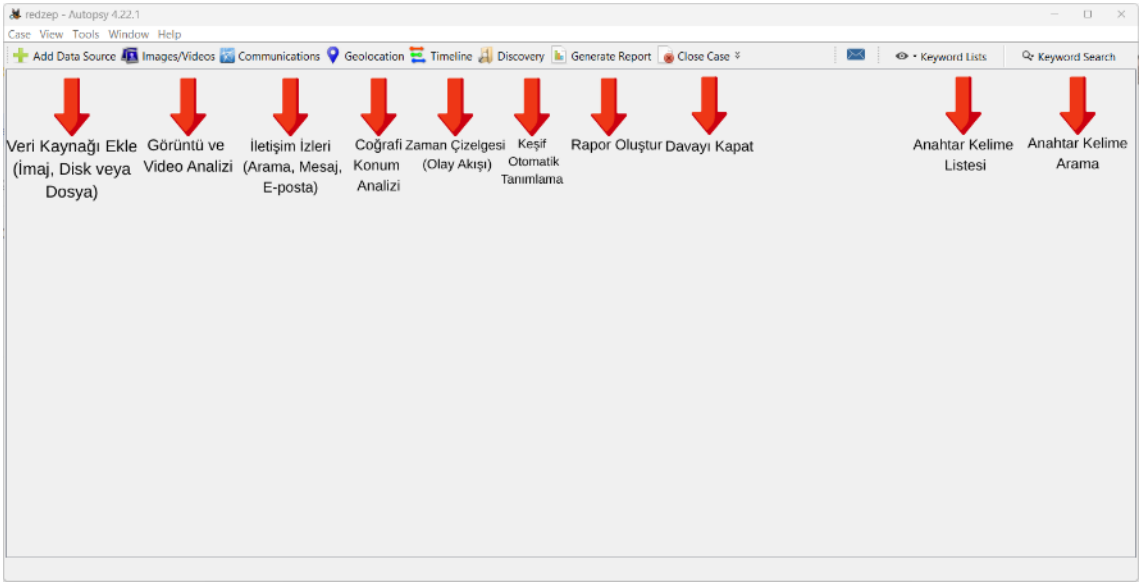
- Java tabanlı arayüz
- Sleuth Kit (TSK) analiz motoru
- SQLite / case database altyapısı
- Ingest modülleri (otomatik analiz bileşenleri)

Desteklediği başlıca veri kaynakları

- Fiziksel disk imajları (E01, dd, raw)
- Mantıksal klasörler
- USB / harici disk kopyaları

Bellek dump çıktıları (ek araçlarla)

- Mobil veri yedekleri
- Sanal diskler (VMDK, VHD vb.)



1.4. Mimari Yapı ve The Sleuth Kit (TSK) İlişkisi

Autopsy, aslında iki ana bileşenden oluşan hibrit bir yapıya sahiptir. Bu ilişkiyi bir bina benzetmesiyle açıklarsak; The Sleuth Kit (TSK) binanın temeli ve taşıyıcı kolonlarıyken, Autopsy kullanıcıların etkileşime girdiği estetik ve fonksiyonel dış cephedir.

Katman	Bileşen	Görev ve İşlev
Arayüz (GUI)	**Autopsy**	Kullanıcı etkileşimi, verilerin görselleştirilmesi ve raporlama.
Analiz Katmanı	**Ingest Modules**	Hash analizi, kelime arama, metadata çıkarma gibi otomatik görevler.
Kütüphane Katmanı	**The Sleuth Kit**	Dosya sistemlerine erişim, silinmiş verileri kurtarma ve ham veri işleme (C/C++ tabanlı).
Veri Depolama	**SQLite / Solr**	Analiz sonuçlarının (Case veritabanı) ve metin indekslerinin saklanması.

Kritik Not: Autopsy, verileri doğrudan diskten okumaz. TSK kütüphanelerini kullanarak dosya sistemi yapılarını (Inodes, Block groups vb.) analiz eder ve bunları anlamlı bir klasör hiyerarşisine dönüştürerek size sunar.

Autopsy Arayüzünün Temel Mantığı

Autopsy arayüzü, analistin veriye yukarıdan bakmasını sağlayan, ancak ihtiyaç duyduğunda en derindeki tek bir bayta kadar inmesine izin veren bir hiyerarşiyle çalışır. Arayüzü dört temel panel üzerinden analiz etmek, kullanım disiplini açısından kritiktir:

1. Sol Panel: Veri Gezgini (Tree Viewer)

Burası vakanın "haritasıdır". Veriler hiyerarşik bir ağaç yapısında sunulur.

- **Data Sources:** Eklenen disk imajlarını ve içindeki dosya sistemini gösterir.
- **Views:** Dosyaları türlerine göre (Resimler, Videolar, Dokümanlar, Çalıştırılabilir dosyalar) otomatik gruplandırır.
- **Results:** Ingest modüllerinin (web geçmişi, e-postalar, yüklü programlar) çıkardığı analiz sonuçları burada listelenir.
- **Tags:** Analistin inceleme sırasında "delil" olarak işaretlediği kritik bulgular burada toplanır.

2. Orta Alan: Liste Paneli (Result Viewer)

Sol panelde seçilen klasörün veya analiz sonucunun içeriği burada listelenir.

- Bir klasöre tıkladığınızda içindeki dosyalar; isim, boyut, oluşturulma tarihi ve **MD5 Hash** değerleri gibi sütunlarla burada dökülür.
- **Tablo Görünümü:** Standart liste görünümüdür.
- **Thumbnail Görünümü:** Özellikle görsel kanıtların olduğu klasörlerde hızlı önizleme sağlar.

3. Alt Panel: İçerik Görüntüleyici (Content Viewer)

Arayüzün en teknik kısmıdır. Orta panelde seçilen tek bir dosyanın "içine" bakmanızı sağlar.

- **Hex:** Dosyanın ham halini 16'lık tabanda görmenizi sağlar (veri kazıma için kritik).
- **Strings:** Dosya içindeki okunabilir metin parçalarını ayıklar.
- **Application:** Resim, PDF veya Video gibi dosyaları doğrudan Autopsy içinde görüntüler.
- **Metadata:** Dosyanın sahiplik bilgileri, izinleri ve sistem kayıtlarını gösterir.

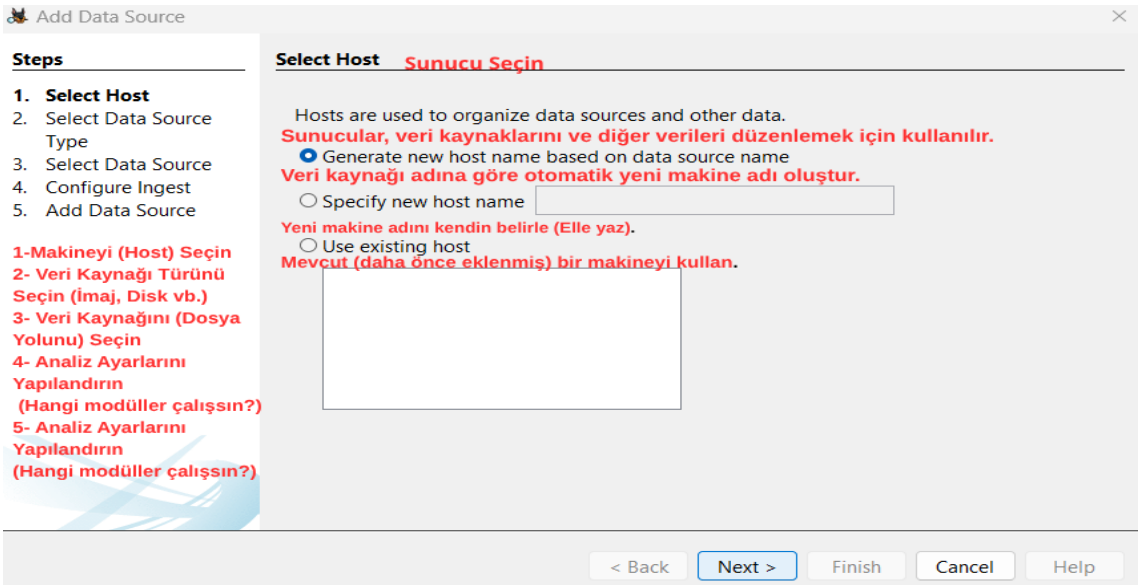
4. Sağ Alt Alan: Durum ve Bilgi Çubuğu

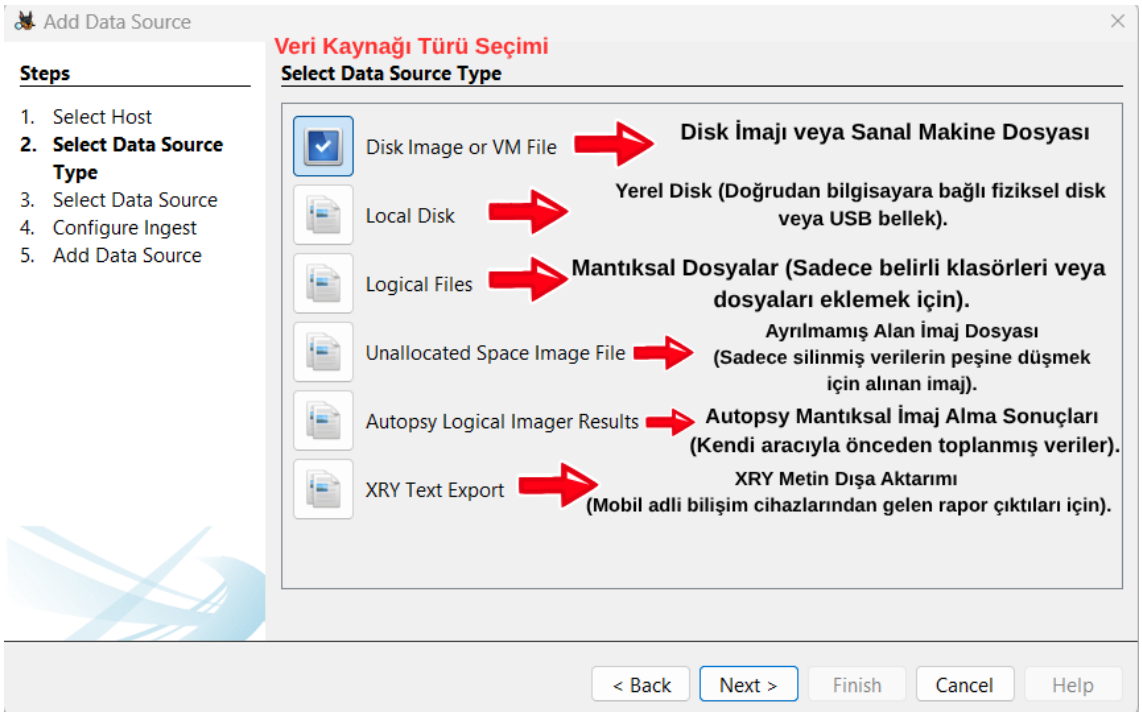
Analiz süreçlerinin (Ingest) ne durumda olduğunu gösterir.

- **Ingest Progress:** Arka planda çalışan analizlerin (indeksleme, hash eşleştirme vb.) yüzdesini takip edebilirsiniz.
- **Memory Usage:** Autopsy'nin o an ne kadar RAM tükettiğini gösterir; kilitlenmeleri önlemek için buradan takip yapılmalıdır.

Panel	Soru	Analist Aksiyonu
Sol Panel	"Nereye bakmalıyım?"	Kategoriyi veya veri kaynağını seçer.
Orta Panel	"Hangi dosya şüpheli?"	Dosyalar arasında filtreleme ve eleme yapar.
Alt Panel	"Bu dosyanın içinde ne var?"	Seçili dosyayı derinlemesine analiz eder ve doğrular.

Analist Notu: Autopsy arayüzünde en çok yapılan hata, alt paneldeki sekmeleri (Hex, Strings, Metadata) kontrol etmeden sadece görsel önizlemeye güvenmektir. Unutmayın, bir suçlu dosya uzantısını değiştirse bile **Hex** sekmesi asla yalan söylemez.




Add Data Source
Veri Kaynağı Türü Seçimi
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Disk İmajı veya Sanal Makine Dosyası
Local Disk
Yerel Disk (Doğrudan bilgisayara bağlı fiziksel disk veya USB bellek).
Logical Files
Mantıksal Dosyalar (Sadece belirli klasörleri veya dosyaları eklemek için).
Unallocated Space Image File
Ayrılmamış Alan İmaj Dosyası (Sadece silinmiş verilerin peşine düşmek için alınan imaj).
Autopsy Logical Imager Results
Autopsy Mantıksal İmaj Alma Sonuçları (Kendi aracıyla önceden toplanmış veriler).
XRY Text Export
XRY Metin Dışa Aktarımı (Mobil adli bilişim cihazlarından gelen rapor çıktıları için).
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Veri Kaynağını Seç
Path:
Dosya Yolu (İmaj dosyasının bulunduğu yer).
Browse
Göz At.
Ignore orphan files in FAT file systems
FAT dosya sistemlerindeki (bağlantısız) dosyaları yoksay.
Time zone:
Zaman Dilimi (Olayın gerçekleştiği yerel saat dilimi
(GMT+3:00) Europe/Istanbul
Sector size:
Sektör Boyutu (Genelde Otomatik Algıla bırakılır).
Auto Detect
Bitlocker Password (optional):
Bitlocker Parolası (Eğer disk şifreliyse, analizi açmak için buraya şifre girilir).
Hash Values (optional):
Hash Değerleri
MD5:
SHA-1:
SHA-256:
İmajın parmak izi (Bütünlük doğrulaması için).
NOTE: These values will not be validated when the data source is added.
Bu değerler veri kaynağı eklenirken doğrulanmayacaktır (Sadece kayıt altına alınır).
< Back
Next >
Finish
Cancel
Help

Bölüm 2: Kurulum ve Konfigürasyon

Profesyonel bir forensic çalışmasında kurulum, sadece "Next" butonuna basmaktan ibaret değildir. Veri bütünlüğünü korumak ve performans optimizasyonu yapmak esastır.

2.1. Sistem Gereksinimleri ve Optimizasyon

Autopsy 4.22.1, yoğun işlem gücü ve I/O (Giriş/Çıkış) hızı gerektirir.

- **Bellek (RAM):** Minimum 16 GB (Büyük imajlar için 32 GB+ önerilir).
- **Depolama:** Vaka (Case) dosyaları ve indeksler için hızlı bir **NVMe SSD** kullanımı, analiz süresini %40'a kadar kısaltır.
- **Java Runtime:** Autopsy, 64-bit Java Runtime Environment (JRE) gerektirir (Paket içeriğinde genellikle mevcuttur).

2.2. Adım Adım Kurulum Prosedürü

1. **İndirme ve Doğrulama:** Resmi web sitesinden (autopsy.com) 4.22.1 sürümünü indirin. İndirme sonrası dosya bütünlüğünü doğrulamak için **SHA-256 hash** değerini kontrol edin. Bu, profesyonel bir forensic alışkanlığıdır.
2. **Yönetici Yetkileri:** Kurulumu "Yönetici Olarak Çalıştır" (Run as Administrator) modunda başlatın. Bu, ham disk aygıtlarına erişim için gereklidir.
3. **Dizin Seçimi:** Program dosyalarını varsayılan dizine kurabilirsiniz ancak **Vaka Verilerini (Case Data)** işletim sisteminin bulunduğu diskten farklı, yüksek hızlı bir sürücüde depolamanız önerilir.

2.3. İlk Yapılandırma: Central Repository ve Solr

Kurulum sonrası yapılması gereken ilk profesyonel ayarlar şunlardır:

- **Central Repository:** Daha önceki vakalarda karşılaştığınız hash değerlerini ve yorumları merkezi bir veritabanında tutmanızı sağlar. Bu, tekrarlayan incelemelerde hız kazandırır.
- **Keyword Search (Solr):** Autopsy, metin arama işlemleri için Apache Solr kullanır. Bellek ayarları kısmından Solr için ayrılan RAM miktarını sistem kapasitenize göre optimize edin.

Bölüm 3: Vaka Yönetimi ve Veri Entegrasyonu

Autopsy'de bir inceleme başlatmak, yapılandırılmış bir veri tabanı ve klasör hiyerarşisi oluşturmak anlamına gelir. 4.22.1 sürümüyle gelen performans iyileştirmeleri, özellikle büyük imaj dosyalarının indekslenmesinde kritik rol oynar.

3.1. Yeni Bir Vaka Oluşturma (New Case Creation)

Yeni bir soruşturma başlatırken izlenmesi gereken standart prosedür şu şekildedir:

Vaka Bilgileri (Case Information): "New Case" butonuna tıkladığınızda karşınıza gelen ekranda, vakanın ismini ve depolanacağı ana dizini (Base Directory) seçin.

Profesyonel Tavsiye: Vaka isimlendirmesinde **YIL-AY-GUN_VAKA-NO** (Örn: **2024-05-20_001-Satis-Hirsizligi**) gibi standart bir protokol izlemek, arşiv yönetimini kolaylaştırır.

Vaka Tipi (Case Type): * **Single-user:** Yerel makinenizde tek başınıza çalışıyorsanız seçin.

Multi-user: Bir ekip ile aynı vaka üzerinde, merkezi bir PostgreSQL veritabanı kullanarak çalışacaksanız bu seçeneği kullanın.

Opsiyonel Bilgiler: Soruşturmacı adı (Examiner), vaka numarası ve notlar kısmı, raporlama aşamasında başlık verisi olarak kullanılacağı için titizlikle doldurulmalıdır.

3.2. Veri Kaynağı Ekleme (Add Data Source)

Vaka oluşturulduktan sonra, analiz edilecek dijital delilin sisteme tanıtılması gerekir:

- **Disk Image or VM File:** En yaygın yöntemdir. .E01, .raw, .vmdk gibi imaj dosyalarını destekler.
- **Local Disk:** Canlı bir sistemdeki fiziksel sürücüyü doğrudan analiz etmek için kullanılır (Yazma korumalı donanım -Write Blocker- kullanımı zorunludur).
- **Logical Files:** Sadece belirli klasörlerin veya dosyaların analizi için tercih edilir.

3.3. Veri İşleme Motoru: Ingest Modules

Veri Ekleme sürecinin en kritik aşaması, hangi modüllerin çalıştırılacağına karar vermektir. Her modülü seçmek süreci inanılmaz yavaşlatabilir; bu yüzden hedefe yönelik seçim yapılmalıdır.

Modül Adı	**İşlevi**	**Ne Zaman Kullanılmalı?**
Recent Activity	Web geçmişi, çerezler ve son açılan belgeleri ayıklar.	Kullanıcı davranış analizi gerekiyorsa.
Hash Lookup	Dosyaları bilinen iyi (NSRL) veya kötü hash listeleriyle karşılaştırır.	Zararlı yazılım veya standart dosya eleme için.
File Type Sig.	Dosya uzantısı ile gerçek içeriği (Magic Number) karşılaştırır.	Gizlenmiş dosyaları bulmak için (Örn: .jpg görünümlü .zip).
Keyword Search	İmaj içindeki tüm metinleri ve meta verileri indeksler.	Kelime bazlı arama yapılacaksa (Vazgeçilmezdir).
EXIF Parser	Fotoğraflardan GPS ve kamera verilerini çeker.	Konum bazlı kanıt aranıyorsa.

Önemli Uyarı: Ingest süreci devam ederken Autopsy arayüzünde bazı veriler görünmeye başlar, ancak tam analiz sonuçları (özellikle Keyword Search) modüller %100 tamamlanmadan kesinlik arz etmez. Sağ alt köşedeki ilerleme çubuğunu mutlaka takip edin.

Bölüm 4: Gelişmiş Analiz Teknikleri ve Zaman Çizelgesi (Timeline) Yönetimi

Veri işleme (Ingest) tamamlandıktan sonra, analistin görevi devasa veri yığınları arasında anlamlı korelasyonlar kurmaktır. Autopsy 4.22.1, bu süreçte veriyi yapılandırılmış bir biçimde sunarak "olay örgüsünü" kurmamıza yardımcı olur.

4.1. Zaman Çizelgesi (Timeline) Analizi

Dijital bir suçun veya siber olayın "ne zaman" gerçekleştiğini belirlemek, şüphelinin o anki aktivitelerini kanıtlamak için kritiktir.

- **Count View (Yoğunluk Görünümü):** Belirli bir tarih aralığında sistemde gerçekleşen dosya oluşturma, değiştirme veya erişim (MAC times) trafiğini çubuk grafiklerle gösterir. Olağandışı trafik artışları (spike), veri sızıntısı veya zararlı yazılım faaliyetine işaret edebilir.
- **Details View (Detay Görünümü):** Her bir olay kaydının (event) içeriğini gösterir. Örneğin; bir USB belleğin takılması ile bir belgenin kopyalanması arasındaki saniyelik farkı buradan yakalayabilirsiniz.
- **L2 (Level 2) İnceleme:** Timeline üzerinden doğrudan ilgili dosyaya sağ tıklayıp "View in Directory" diyerek dosyanın sistemdeki konumuna gitmek, bağlamsal analiz (contextual analysis) için hayati önem taşır.

Dijital bir suçun veya siber olayın "ne zaman" gerçekleştiğini belirlemek, şüphelinin o anki aktivitelerini kanıtlamak için kritiktir. Autopsy Timeline aracı, sistemdeki her dosya hareketini, internet geçmişini ve olay günlüklerini (Event Logs) tek bir kronolojik akışta birleştirir.

Kritik Uyarı: Timeline analizi yaparken sistem saatinin (System Clock) doğruluğunu mutlaka kontrol edin. Eğer cihazın saati hatalıysa, tüm kronolojik kanıtlar sarsılabilir; bu durumda "Offset" hesaplaması yapılarak düzeltme uygulanmalıdır.

Timeline modülü veriyi üç farklı perspektifle sunar:

Görünüm Modu	Teknik İşlevi	Analist Ne Zaman Kullanmalı?
Count View (Sayım Görünümü)	Belirli bir tarih aralığındaki dosya trafiğini çubuk grafiklerle (spike) gösterir.	Sistemdeki olağandışı aktivite artışlarını (veri sızıntısı, toplu silme) tespit etmek için.
Details View (Detay Görünümü)	Her bir olay kaydının (event) içeriğini, dosya yolunu ve olay tipini liste olarak sunur.	Bir USB belleğin takılması ile bir belgenin kopyalanması arasındaki saniyelik farkı yakalamak için.
List View (Liste Görünümü)	Klasik tablo formatında, filtrelenmiş olayları döküm olarak verir.	Raporlama öncesi kanıtları seçmek ve son kontrolleri yapmak için.

Timeline Analizinde "Kritik İzler" (MAC Times)

Autopsy, dosya sistemindeki dört temel zaman damgasını (Timestamp) analiz eder:

- **Modified (M):** Dosya içeriğinin en son ne zaman değiştirildiği.
- **Accessed (A):** Dosyaya en son ne zaman erişildiği (Bazı sistemlerde kapalı olabilir).
- **Created (C):** Dosyanın bu medya (disk) üzerinde ilk kez oluşturulduğu tarih.
- **Changed (B):** NTFS sistemlerinde dosyanın metadata (izinler, isim vb.) bilgilerinin değiştiği an.

Profesyonel Strateji: "L2 İnceleme" (Bağlamsal Analiz)

- Timeline üzerinden şüpheli bir ana rastladığınızda, ilgili olaya sağ tıklayıp **"View in Directory"** diyerek dosyanın sistemdeki fiziksel konumuna gitmek hayati önem taşır. Bu sayede dosyanın hangi klasörde olduğu ve çevresinde başka hangi şüpheli verilerin bulunduğu "bağlamsal" olarak anlaşılabilir.

4.2. Anahtar Kelime Arama (Keyword Search) ve Filtreleme

Milyonlarca dosya arasında manuel arama yapmak imkansızdır. Profesyonel bir analist, **Regular Expressions (Regex)** kullanarak daha akıllı aramalar yapar.

- **Standart Aramalar:** İsim, soyisim veya proje kod adları.
- **Regex Aramaları:** Kredi kartı numaraları, e-posta adresleri veya belirli bir IP bloğu gibi desen tabanlı aramalar.
    - ***Örnek:*** **\b\d{4}-\d{4}-\d{4}-\d{4}\b** (Kredi kartı formatı için).
- **Filtreleme:** Analiz yükünü azaltmak için "Known Files" (NSRL) filtresi kullanılarak işletim sistemine ait binlerce "temiz" dosya görünümden gizlenmelidir.

4.3. Veri Görselleştirme ve İletişim Grafiği

Autopsy'nin gelişmiş sürümlerinde yer alan **Communications** sekmesi, sosyal bir ağ haritası çıkarır.

- **Korelasyon:** Şüpheli şahsın kimlerle, hangi platform (E-posta, Mesajlaşma) üzerinden ve ne sıklıkla iletişim kurduğunu bir ağ grafiği olarak sunar.
- **Metadata Analizi:** Dosyaların içindeki gizli veriler (EXIF, Author bilgisi vb.) üzerinden, bir belgenin asıl kaynağını veya bir fotoğrafın çekildiği coğrafi koordinatları tespit edebilirsiniz.

4.4. İşletim Sistemi Artefaktları (Artifacts)

Profesyonel bir raporda mutlaka yer alması gereken kritik artefaktlar:

1. **Web Artifacts:** Tarayıcı geçmişi, indirmeler ve form verileri.
2. **Recent Documents:** Kullanıcının en son eriştiği dokümanların (LNK dosyaları) analizi.
3. **Installed Programs:** Sistemde bulunan ancak silinmiş olabilecek izinsiz yazılımlar.

Analist Notu: Timeline analizi yaparken sistem saatinin (System Clock) doğruluğu mutlaka kontrol edilmelidir. Eğer imajı alınan cihazın saati hatalıysa, tüm kronolojik kanıtlar sarsılabilir. Bu tür durumlarda "Offset" (Zaman farkı) hesaplaması yapılarak düzeltme uygulanmalıdır.

Bölüm 5: Gizli Verilerin Tespiti (Steganografi ve Parola Kırma)

Dijital incelemelerde karşılaşılan en büyük zorluk, şüphelinin veriyi kasıtlı olarak gizlemesi veya şifrelemesidir. Profesyonel standartlar, bu tür engellerin sistematik bir şekilde raporlanmasını ve mümkünse aşılmasını gerektirir.

5.1. Steganografi Analizi (Veri Gizleme)

Steganografi, bilginin başka bir dosyanın (genellikle görsel veya ses) içine, dikkat çekmeyecek şekilde gömülmesidir. Autopsy içinde bu durumu tespit etmek için **"Image Analyzer"** ve belirli eklentiler kullanılır.

- **Lsb (Least Significant Bit) Analizi:** Dijital fotoğrafların piksellerindeki en önemsiz bitlerin değiştirilip değiştirilmediği incelenir. Autopsy üzerinde bir görselin meta verilerinde veya dosya boyutunda tutarsızlık fark edildiğinde bu durum "Şüpheli" olarak işaretlenmelidir.
- **Dosya Uzantısı ve İmza Uyumsuzluğu:** Bir dosyanın başlık bilgisi (File Header) .jpg diyor ancak içerik analizi dosyanın içinde gizli bir .zip veya .txt olduğunu söylüyorsa, Autopsy bunu **"Extension Mismatch"** hatasıyla raporlar. Bu, steganografik bir faaliyetin en temel belirtisidir.

Tablo: Steganografi Belirtileri ve Analist Stratejisi

Belirti / Anomali	**Teknik Anlamı**	**Autopsy'de Uygulanacak Adım**
Extension Mismatch	Dosya uzantısı ile gerçek içerik (Magic Number) uyuşmuyor.	"Results -> Analysis Results" altındaki uyarıları inceleyin.
High Entropy	Dosyanın belirli bölgelerinde çok yüksek veri karmaşıklığı var.	**Hex Viewer** sekmesinde dosyanın rastgelelik oranına bakın.
EXIF Bozulması	Görselin meta verilerinde tutarsızlık veya eksiklik.	"Content Viewer -> Metadata" sekmesini kontrol edin.
Thumbnail Farkı	Dosyanın küçük resmi (thumbnail) ile asıl içeriği farklı.	**Image Analyzer** modülünde görselleri yan yana kıyaslayın.

5.2. Parola Kırma ve Şifreli Dosya Analizi (Password Cracking)

Autopsy, kendi başına bir kaba kuvvet (brute-force) saldırı aracı değildir; ancak şifreli dosyaları tespit eder ve analiz için dış araçlara (external tools) veri hazırlar.

5.2.1. Şifreli Dosyaların Tespiti

Ingest süreci sırasında Autopsy, **Encryption Detection** modülü sayesinde şunları raporlar:

- **Parola Korumalı Office Belgeleri:** Word, Excel veya PDF dosyalarındaki kısıtlamalar.
- **Arşiv Dosyaları:** Şifreli .zip veya .rar içerikleri.
- **Disk Şifreleme:** BitLocker, TrueCrypt veya VeraCrypt ile korunan bölümler (Partitions).

5.2.2. Çözüm Stratejileri

Şifreli bir dosya tespit edildiğinde profesyonel iş akışı şu şekildedir:

1. **Wordlist (Sözlük) Oluşturma:** Şüphelinin diskindeki diğer dosyalardan (notlar, tarayıcı geçmişi, kullanıcı adları) elde edilen kelimelerle kişiselleştirilmiş bir sözlük oluşturulur.
2. **Dış Araç Entegrasyonu:** Autopsy'den dışa aktarılan (Export) şifreli dosyalar, **Hashcat** veya **John the Ripper** gibi yüksek performanslı araçlara aktarılır.
3. **GPU Yardımlı Kırma:** Karmaşık şifrelerin çözümü için işlemci (CPU) yerine ekran kartlarının (GPU) paralel işlem gücünden yararlanılır.

Adım	İşlem	Teknik Detay / Araç
1. Tespit	Autopsy ile şifreli dosyanın tespiti ve işaretlenmesi.	**Encryption Detection** Modülü.
2. Hazırlık	Şifreli dosyanın (veya hash değerinin) dışa aktarılması.	**Export** fonksiyonu.
3. Sözlük Oluşturma	Şüphelinin diskindeki verilerden kişiselleştirilmiş kelime listesi hazırlama.	Tarayıcı geçmişi, kullanıcı adları ve notlar.
4. Kırma İşlemi	Yüksek performanslı dış araçlarla saldırı başlatma.	**Hashcat** veya **John the Ripper**.
5. GPU Desteği	Hız kazanmak için ekran kartlarının işlem gücünü kullanma.	Paralel işlem mimarisi.

5.3. Bellek (RAM) Üzerinden Şifre Kazanımı

Bazı durumlarda şifreyi kırmak yerine, bilgisayar açıkken alınan bellek imajı (RAM dump) üzerinden şifreleme anahtarlarını "temiz metin" (plain text) olarak çekmek çok daha hızlı bir yöntemdir. Autopsy'ye entegre edilebilen **Volatility** aracı ile RAM analizi yapılarak açık olan BitLocker sürücüsünün "Master Key" verisi elde edilebilir.**Memory Forensics:** Eğer şüpheli bilgisayar açıkken imaj alındıysa, Autopsy'ye entegre edilebilen veya haricen kullanılan **Volatility** aracı ile RAM analizi yapılır.

- **Kazanım:** Şifreleme anahtarları, açık olan BitLocker sürücüsünün "Master Key" verisi veya tarayıcıda o an açık olan oturumların parolaları bellekten temiz metin (plain text) olarak çekilebilir.

Etik ve Hukuki Uyarı: Parola kırma işlemleri, davanın yasal kapsamı ve arama kararı (search warrant) dahilinde yapılmalıdır; aksi takdirde elde edilen kanıtlar mahkemede reddedilebilir.

Bellek (RAM) Analizi ve Volatility Entegrasyonu

- Dijital bir incelemede disk verileri "geçmişi", bellek verileri ise "şimdiyi" temsil eder. Birçok zararlı yazılım (fileless malware) diskte iz bırakmaz, sadece bellekte yaşar. Autopsy 4.22.1, açık kaynaklı bellek analizi standardı olan **Volatility Framework** ile entegre çalışarak bu uçucu verileri kalıcı kanıtlara dönüştürür.

Neden Bellek Analizi?

Bazı kritik kanıtlar sadece sistem açıkken RAM üzerinde bulunur ve bilgisayar kapandığı an yok olur:

Şifreleme Anahtarları: BitLocker, VeraCrypt gibi yazılımların açık olan sürücülerine ait anahtarlar.

Ağ Bağlantıları: O an uzak sunucuyla iletişim kuran bir RAT (Remote Access Trojan) izleri.

Uçucu Mesajlaşmalar: Tarayıcıda açık kalan ve henüz diske yazılmamış chat kayıtları.

Çalışan Süreçler (Processes): Kendi adını gizleyen veya sistem dosyası gibi görünen zararlı yazılımlar.

Autopsy İçinde Volatility Kullanımı

Autopsy, bellek dump dosyalarını (.raw, .mem, .dmp) bir veri kaynağı olarak kabul eder.

Analiz İş Akışı:

Veri Kaynağı Ekleme: "Add Data Source" kısmından bellek imajınızı seçin.

Volatility Modülünü Yapılandırma: Ingest Modülleri listesinden Volatility'yi seçin.

Profil Seçimi: RAM imajının alındığı işletim sistemi sürümünü (Örn: Win10x64) belirtin. Yanlış profil seçimi, analiz sonuçlarının hatalı veya boş dönmesine neden olur.

Kritik Volatility Artefaktları Tablosu

Analiz bittiğinde, Autopsy'nin sol panelindeki **"Results"** sekmesi altında şu kritik başlıkları incelemelisiniz:

Artefakt Adı (Plugin)	Analistin Bakış Açısı	Önem Derecesi
PsList / PsScan	Sistemde o an çalışan tüm gizli veya açık süreçleri listeler.	★★★
NetScan	Aktif ağ bağlantılarını, IP adreslerini ve portları gösterir.	★★★
CmdLine	Bir sürecin terminalden hangi parametrelerle çalıştırıldığını gösterir.	★★
Malfind	Belleğe enjekte edilmiş zararlı kod parçacıklarını tespit eder.	★★★
Hivescan / Printkey	Kayıt defterinin (Registry) RAM'deki o anki halini sorgular.	★★

Bellekten Şifre Kazanımı (Plaintext Passwords)

Bellek analizinin en "mucizevi" yanlarından biri, hash kırma süreciyle uğraşmadan parolaları temiz metin olarak elde etmektir.

- **Mimikatz Entegrasyonu:** Volatility üzerinden çalışan Mimikatz eklentisi, Windows oturum açma bilgilerini (LSASS süreci üzerinden) RAM'den çekebilir.
- **Yara Taraması:** Bellek içinde belirli Regex kalıplarıyla (kredi kartı, e-posta, şifre) arama yaparak, uygulamaların RAM'de açık bıraktığı hassas verileri yakalayabilirsiniz.

Profesyonel İpucu: Bellek imajı alırken sistemdeki RAM miktarı kadar (veya biraz fazlası) boş alanınız olduğundan emin olun. 16 GB RAM'i olan bir makinenin imajı tam 16 GB yer kaplayacaktır. Bu dosya daha sonra Autopsy içinde indekslenirken disk I/O hızınız analizin süresini doğrudan etkiler.

Etik ve Hukuki Not: Parola kırma işlemleri, vakanın yasal kapsamı (search warrant) dahilinde yapılmalıdır. Aksi takdirde, elde edilen kanıtlar "yasaklı meyve" doktrini gereği mahkemede reddedilebilir.

Bölüm 6: Kanıt Zinciri (Chain of Custody)

Kanıt zinciri, dijital delilin (hard disk, USB, telefon vb.) ele geçirilmesinden mahkemeye sunulmasına kadar geçen süreci belgeleyen kronolojik bir kayıt defteridir.

Profesyonel bir kanıt zinciri belgesi şunları içermelidir:

- **Tanımlama:** Cihazın seri numarası, marka/modeli ve fiziksel durumu.
- **Zaman Damgası:** El koyma, teslim etme ve analiz başlangıç saatleri.
- **Gözetim Kaydı:** Delile kimin, ne zaman ve hangi amaçla eriştiğinin (analiz, kopyalama, depolama) imzalı dökümü.
- **Hash Doğrulaması:** İmajın alındığı andaki Hash değeri ile analiz bittiğindeki Hash değerinin aynı olduğunun (veri bütünlüğünün) kanıtı.

6.1. Autopsy Raporlama Modülü

Autopsy, manuel rapor yazma yükünü hafifleten ancak özelleştirmeye açık güçlü bir raporlama motoruna sahiptir. Analiz bittiğinde "Generate Report" butonu ile süreç başlatılır.

Rapor Formatları ve Kullanım Alanları:

1. **HTML Report:** En yaygın formattır. Tarayıcı üzerinden açılır ve tüm bulgular (dosyalar, görseller, timeline) arasında linkler yardımıyla hızlı geçiş sağlar.
2. **Excel/CSV:** Çok sayıda veri (Örn: 10.000 adet arama kaydı) üzerinde istatistiksel analiz yapmak veya başka bir veritabanına aktarmak için idealdir.
3. **VICS (Video Image Classification Standard):** Çocuk istismarı gibi özel vakalarda, görsel verilerin kolluk kuvvetleri standartlarında sınıflandırılması için kullanılır.

6.2. Profesyonel Bir Raporun Anatomisi

İyi bir forensic raporu hem teknik bir uzmanın hem de teknik bilgisi olmayan bir hakimin anlayabileceği seviyede olmalıdır:

1. **Yönetici Özeti (Executive Summary):** Teknik detaylara boğulmadan, vakanın sonucunu (Örn: "Şüphelinin bilgisayarında X tarihinde veri sızıntısı yapıldığı tespit edilmiştir") belirten kısımdır.
2. **Yöntem ve Araçlar:** Analizde hangi yazılımların (Autopsy 4.22.1, Hashcat vb.) ve hangi donanım yazma koruyucuların (Write Blocker) kullanıldığı belirtilir.
3. **Bulgular ve Analiz:** Kanıtların (Artifacts) ekran görüntüleri ve hash değerleri ile sunulduğu ana bölümdür.
4. **Sonuç (Conclusion):** Elde edilen bulguların vaka ile olan illiyet bağı net bir şekilde ortaya konur.

6.3. Veri Bütünlüğü ve Hash Hesaplamaları

Analiz sonunda, orijinal imajın ve çalışma dosyasının bozulmadığını kanıtlamak için matematiksel doğrulama yapılır.

$$H(data) = Hash\_Value$$

Eğer veride tek bir bit dahi değişirse, sonuçtaki hash değeri tamamen farklı çıkacaktır. Raporunuzda başlangıç ve bitiş hash değerlerinin eşleştiğini belirtmek, savunma makamının "verilerle oynandı" iddiasını çürüten en büyük silahtır.

Son Söz: Dijital adli bilişim bir araç kullanma becerisi değil, bir **dürüstlük ve metodoloji** disiplinidir. Autopsy 4.22.1 bu disiplini uygulamanız için size yolu gösterir, ancak adaleti sağlayan sizin tarafsız analizinizdir.

Bölüm 7: Arayüz Anatomisi ve Navigasyon Stratejileri

Autopsy arayüzü, rastgele yerleştirilmiş pencerelerden ibaret değildir; standart bir adli bilişim iş akışını (Workflow) takip eder. Bir analistin başarısı, hangi verinin nerede olduğunu bilmesinden çok, o veriye en hızlı nasıl "navigasyon" yapacağını bilmesine bağlıdır.

7.1. Tree Viewer (Sol Panel): Hiyerarşik Kontrol

Bu panel, vakanın "iskeletidir". Veriler burada kategorize edilir:

- **Data Sources:** İmajın fiziksel yapısını (bölümler, klasörler) gösterir.
- **Views:** Dosyaları tipine göre (Mime Type) ayırır. Örneğin; tüm videoları tek bir klasörde görmek için burası kullanılır.
- **Results:** Ingest modüllerinin bulduğu "ilginç" her şey (çerezler, EXIF, silinmiş dosyalar) burada listelenir.
- **Tags:** Sizin tarafınızdan "kritik" olarak işaretlenen kanıtlar.

7.2. Result Viewer (Sağ Üst Panel): Liste ve Tablo Görünümü

Seçilen klasörün içeriği burada dökülür. Profesyonel analizde şu sütunlara dikkat edilmelidir:

- **S (Score):** Autopsy'nin dosya hakkındaki şüphe puanı.
- **C (Comment):** Dosyaya eklenen analist notları.
- **Modified/Accessed/Created (MAC) Times:** Dosyanın zaman damgaları.

7.3. Content Viewer (Sağ Alt Panel): Derinlemesine İnceleme

Bir dosyanın üzerine tıkladığınızda, o dosyanın "ruhunu" burada görürsünüz:

- **Hex:** Dosyanın ham (binary) verisi. Gizli imzaları yakalamak için kullanılır.
- **Text:** Dosya içindeki okunabilir metinler.
- **Application:** Dosyayı (resim, PDF, Office) orijinal haliyle görüntüler.
- **Metadata:** Dosyanın sahiplik, boyut ve sistem bilgileri.

Bölüm 8: Veri Kaynağı Türlerinde Uzmanlaşma

Autopsy sadece bir sabit disk analiz aracı değildir. Farklı veri kaynaklarına göre yaklaşım değişmelidir:

8.1. Mantıksal Kanıt Dosyaları (L01)

Dosya bazlı alınmış imajlardır. Eğer tüm diski değil de sadece kullanıcı klasörünü analiz ediyorsanız, Autopsy'nin dosya sistemi tablolarına (MFT gibi) erişemeyeceğini, sadece mevcut dosyaları işleyebileceğini unutmamalısınız.

8.2. Sanal Makine İmajları (VMDK, VHD)

Sanal makineler, içinde başka bir dosya sistemi barındıran "matruşka" yapılardır. Autopsy, bir .vmdk dosyasını sanki fiziksel bir diskmiş gibi mount ederek içindeki işletim sistemini analiz edebilir.

8.3. Unallocated Space (Tahsis Edilmemiş Alan) Analizi

Silinen dosyalar aslında diskten hemen silinmez; sadece "üzerine yazılabilir" olarak işaretlenirler.

- **Carving İşlemi:** Autopsy, dosya sistemi kayıtları silinmiş olsa bile, dosya imzalarını (header/footer) takip ederek veriyi "oyup çıkarma" (carving) yapar. Bu, adli bilişimin en "mucizevi" anlarından biridir.

Bölüm 9: Autopsy Modülleri (Ingest) - Derin Dalış

Kullanıcıların en çok atladığı ama en çok veri kaçırdığı yer burasıdır. Modülleri detaylandıralım:

9.1. Android Analyzer (ALEAPP Entegrasyonu)

Eğer bir telefon imajı (Physical Dump) inceliyorsanız, bu modül devreye girer:

- **Mesajlar ve Aramalar:** SQLite veritabanlarından WhatsApp, SMS ve arama kayıtlarını çeker.
- **Konum Geçişleri:** Cihazın bağlandığı Wi-Fi noktaları üzerinden konum geçmişi çıkarır.

9.2. Email Parser

- Outlook (PST/OST) ve Thunderbird (MBOX) dosyalarını analiz eder.
- E-posta eklerini (attachments) otomatik olarak ayıklayıp ayrı bir klasöre koyar ve içeriklerini indeksler.

9.3. PhotoRec Carver

Bu, açık kaynaklı efsanevi PhotoRec aracının Autopsy içine gömülmüş halidir. Standart yöntemlerle kurtarılamayan medya dosyalarını (fotoğraf, video) sektör sektör tarayarak geri getirir.

Bölüm 10: Hash Setleri ve Veri Eleme Sanatı (NSRL)

Dijital bir imajda yüz binlerce dosya bulunur ve bunların %90'ı işletim sistemine veya standart yazılımlara ait, davanın konusu olmayan "temiz" (known-good) dosyalardır. Profesyonel bir analist, bu verileri elemek için **Hash Set** mekanizmasını kullanır.

10.1. NSRL (National Software Reference Library) Nedir?

NSRL, bilinen tüm ticari yazılımların hash değerlerini (MD5, SHA-1) içeren devasa bir veritabanıdır.

- **Eleme (Filtering):** Autopsy'ye NSRL setini tanıttığınızda, sistem dosyaları "Known" (Bilinen) olarak işaretlenir ve analizin dışında tutulur. Bu, inceleme yükünü %70-80 oranında azaltır.

10.2. Özel Hash Setleri (Known Bad)

Eğer elinizde daha önceki vakalardan kalma çocuk istismarı görselleri veya zararlı yazılım (malware) hash listeleri varsa, bunları Autopsy'ye **"Notable"** (Dikkat Çekici) olarak ekleyebilirsiniz.

- **Otomatik Alarm:** Ingest sırasında bu listeyle eşleşen bir dosya bulunursa, Autopsy kırmızı bir bayrakla sizi anında uyarır.

Bölüm 11: "Interesting Items" ve Otomatik Tespit

Autopsy, belirli kriterlere uyan dosyaları "İlginç Öğeler" (Interesting Items) klasöründe toplamanıza olanak tanır. Bu, manuel arama yapmadan önce sistemin size sunduğu bir öncelik listesidir.

11.1. Kural Tabanlı Tespit

Bu modül, dosya adı, uzantısı veya yoluna (path) göre otomatik yakalama yapar. Profesyonel bir incelemede şu kurallar mutlaka aktifleştirilmelidir:

- **Kripto Varlıklar:** Cüzdan dosyaları (wallet.dat), anahtar kelimeler (Bitcoin, Ethereum, mnemonic).
- **Bulut Depolama:** Dropbox, OneDrive veya Google Drive senkronizasyon klasörleri.
- **Encryption Tools:** TrueCrypt, VeraCrypt veya BitLocker yapılandırma dosyaları.

11.2. Bulut Artefaktları

Modern vakaların çoğu bulutta biter. Autopsy, sistemde yüklü bulut uygulamalarının metadata verilerini analiz ederek, yerelde olmayan ancak bulutta senkronize edilmiş dosyaların listesini çıkarabilir.

Bulut Servislerinin Yerel İzleri (Sync Logs)

Bulut servisleri, verimlilik adına yerel bilgisayarda veritabanları (genellikle SQLite) ve günlük dosyaları tutar. Autopsy'nin yerleşik **SQLite Viewer** aracı, bu veritabanlarını manuel olarak incelemenize olanak tanır.

İncelenmesi Gereken Kritik Dosyalar:

- **OneDrive:** %LocalAppData%\Microsoft\OneDrive\settings\Personal dizinindeki .dat ve .ini dosyaları.

Google Drive: %LocalAppData%\Google\DriveFS dizinindeki veritabanları.

Dropbox: %AppData%\Dropbox\info.json ve config.db dosyaları.

Bölüm 11.3: Dark Web ve Kripto Varlık İz Analizi

Geleneksel tarayıcılar ve bankacılık sistemleri izlenebilirken, Dark Web (Tor) ve Kripto paralar anonimlik katmanları ekler. Ancak hiçbir sistem tamamen izsiz değildir. Analist, bu gizli dünyaların yerel disk üzerindeki ayak izlerini yakalamalıdır.

11.3.1. Dark Web (Tor Browser) İzleri

Tor Browser, gizlilik odaklı olduğu için verileri RAM üzerinde tutmaya çalışır ancak kurulum ve kullanım sırasında diskte silinmesi zor artefaktlar bırakır.

- **Kurulum İzleri:** Şüphelinin diskinde Tor Browser klasörünün varlığı veya Prefetch dosyalarında tor.exe, firefox.exe (Tor versiyonu) izleri davanın yönünü değiştirir.
- **State Dosyası:** Tor klasörü içindeki Data/Tor/state dosyası, köprülere ve giriş düğümlerine dair teknik bilgiler içerir.
- **Tor Logs:** %AppData%\Tor dizininde bulunan günlükler, bağlantı zaman damgalarını (Timestamp) yakalamanızı sağlar.

11.3.2. Kripto Varlıklar ve Cüzdan Analizi

Kripto paralar diskte "Cüzdan" (Wallet) dosyaları veya "Mnemonic" (12-24 kelimelik kurtarma kodları) olarak iz bırakır.

Tablo: Kripto Varlık Artefaktları ve Tespit Yöntemleri

Varlık Türü	Dosya Adı / Uzantısı	Autopsy Arama Stratejisi
Core Cüzdanlar	wallet.dat	**File Signature** taraması ile gizlenmiş cüzdanları bulma.
Borsa Kayıtları	Tarayıcı Önbelleği (Cache)	binance.com, btcturk.com gibi URL filtreleme.
Kurtarma Kodları	.txt, .pdf, .jpg	**Keyword Search** ile 12/24 kelimelik dizin taraması.
Yazılım Cüzdanları	Electrum, Exodus	**Installed Programs** modülü ile cüzdan yazılımı tespiti.

11.3.3. "Interesting Items" İçin İleri Seviye Regex Kalıpları

Kripto adresleri belirli matematiksel kalıplara sahiptir. Autopsy'nin **Keyword Search** modülüne şu Regex'leri ekleyerek diskteki tüm cüzdan adreslerini saniyeler içinde dökebilirsiniz:

- **Bitcoin (Legacy):** ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$.
- **Ethereum:** ^0x[a-fA-F0-9]{40}$.
- **Mnemonic Anahtar Kelimeler:** Autopsy üzerinde "Notable" bir liste oluşturun: seed, recovery, phrase, mnemonic, private key.

11.3.4. Dark Web Pazar Yeri Kalıntıları

Şüphelinin Dark Web üzerinden yaptığı alışverişler, tarayıcının "Thumbnail" (Küçük resim) önbelleğine düşebilir.

- **Image Analyzer:** Autopsy'nin bu modülünü kullanarak, Tor klasörü içindeki şifrelenmiş görünen ancak aslında küçük resim kalıntısı olan images.db gibi dosyaları görselleştirin.
- **Kullanıcı Adı Korelasyonu:** Dark Web forumlarında kullanılan takma isimleri (Alias), diskteki diğer dökümanlar veya e-posta kayıtlarıyla eşleştirin.

Analist Notu: Kripto varlık takibi yaparken, bulunan bir cüzdan adresinin "Public Key" (Kamuya açık) mi yoksa "Private Key" (Özel anahtar) mi olduğunu ayırt etmek kritiktir. Private Key veya Seed Phrase bulmak, varlıkların kontrolünün şüphelide olduğunun en güçlü kanıtıdır.

Bölüm 11.4: Anti-Forensics Teknikleriyle Mücadele

Dijital adli bilişim dünyasında "Anti-Forensics", bir analistin kanıt bulmasını engellemek, veriyi tahrif etmek veya analizi yavaşlatmak amacıyla yapılan her türlü bilinçli eylemi ifade eder. Profesyonel bir analist, sadece mevcut veriyi okumaz; eksik olan verinin neden eksik olduğunun da peşine düşer.

11.4.1. Temizlik Araçlarının (Wiper) Tespiti

Şüpheliler genellikle CCleaner, BleachBit veya benzeri "privacy" araçlarını kullanarak tarayıcı geçmişini ve geçici dosyaları silmeye çalışırlar.

- **Prefetch ve Superfetch Analizi:** Autopsy'nin sunduğu bu izler sayesinde, şüphelinin analizden hemen önce bir temizlik aracı çalıştırıp çalıştırmadığı "kabak gibi" ortaya çıkar.

- **Registry İzleri:** Temizlik araçları kurulduğunda veya çalıştırıldığında Windows Kayıt Defteri'nde (Registry) mutlaka bir "Run" veya "Recent" anahtarı bırakırlar.
- **Sonuç:** Eğer sistemde bir wiper yazılımı tespit edilirse, raporda "kasıtlı veri yok etme girişimi" olarak belirtilmelidir.

11.4.2. Zaman Damgası Manipülasyonu (Timestomping)

Analizi yanıltmak için dosya tarihlerinin (MAC times) değiştirilmesi işlemine "Timestomping" denir.

Tablo: Timestomping Belirtileri ve Analist Hamlesi

Belirti	Teknik Anlamı	Analistin Karşı Hamlesi
Hassasiyet Kaybı	Dosya tarihinin milisaniye kısmının ".000" olması.	NTFS $MFT kayıtlarını ve $I30 indekslerini Autopsy ile derinlemesine inceleyin.
Mantıksız Sıralama	Dosya oluşturma tarihinin, değiştirme tarihinden sonra olması.	**Timeline** modülünü kullanarak sistem olaylarıyla (Event Logs) dosya tarihlerini karşılaştırın.
Kayıt Defteri Tutarsızlığı	Registry'deki son kullanım tarihi ile dosya tarihinin uyuşmaması.	Shell Bags ve Jump Lists artefaktlarını kontrol ederek dosyanın gerçek erişim zamanını bulun.

11.4.3. Uzantı Değiştirme ve Veri Gizleme

Veriyi saklamanın en basit yolu, bir .zip dosyasının uzantısını .jpg yapmaktır.

- **Extension Mismatch (Uzantı Uyumsuzluğu):** Autopsy, dosyanın başlık bilgisi (Header/Magic Number) ile uzantısı uyuşmadığında otomatik olarak "Extension Mismatch" uyarısı verir.
- **MIME Type Analizi:** Analist, dosyanın sadece ismine değil, Autopsy'nin belirlediği gerçek içerik türüne (MIME Type) odaklanmalıdır.
- **Data Carving:** Dosya sistemi tabloları silinmiş olsa bile, Autopsy dosya imzalarını takip ederek "tahsis edilmemiş alan"dan veriyi oyup çıkarabilir.

11.4.4. Gizli Bölümler ve Konteynerler

Şüpheliler disk içinde görünmez alanlar oluşturabilir.

- **Host Protected Area (HPA):** Diskin donanımsal olarak gizlenmiş bölümleri. Autopsy ile disk imajı eklenirken sektör sayısındaki tutarsızlıklar bu durumu ele verir.
- **VeraCrypt / BitLocker Konteynerleri:** Diskteki devasa boyutlu, rastgele veri yığını gibi görünen dosyalar genellikle şifreli birer konteynerdir.
- **Analist Stratejisi:** Bu dosyaların "Entropy" (Karmaşıklık) değerine bakın; çok yüksekse içinde şifreli veri saklanıyor demektir.

Analist Notu: Anti-forensics çabası başlı başına bir şüpheli davranış kanıtıdır. Şüphelinin "hiçbir şey yapmadım" beyanını, sistemde çalışan bir veri silme aracının izleri saniyeler içinde çürütebilir.

Bulut Servisi	Kritik Yerel Artefakt	Analist Stratejisi
OneDrive	SyncEngine-*.odl (Günlükler)	Dosya transfer geçmişi ve silinen dosyaların tespiti.
Google Drive	metadata_sqlite_db	Bulut üzerinde mevcut olan ama yerelden silinmiş dosya listesi.
Dropbox	filecache.dbx	Senkronize edilen dosyaların orijinal yolları ve hash değerleri.
iCloud	client_state.plist	Apple cihazlar arası senkronize edilen veriler ve hesap bilgileri.

Bulut "Token" ve Kimlik Doğrulama Analizi

Şüpheli, analizden önce dosyalarını buluttan silmiş olsa bile, sistemde kalan "Auth Token" (kimlik doğrulama anahtarları) sayesinde yasal izinler dahilinde bulut hesabına erişim sağlanabilir. Autopsy, bu anahtarların saklandığı konumlardaki verileri ayıklayarak analistin dış araçlarla (örn. rclone veya özel scriptler) buluta erişmesine kapı açar.

İleri Seviye Arama (Regex) ile Bulut İzleri Takibi

Bulut servislerine ait bağlantı URL'lerini ve kullanıcı kimliklerini bulmak için **Keyword Search** modülünde şu kalıplar kullanılabilir:

Paylaşım Linkleri Yakalama:
(drive\.google\.com|dropbox\.com|onedrive\.live\.com)\/s\/[A-Za-z0-9]+

Paylaşım Linkleri Yakalama:
(drive\.google\.com|dropbox\.com|onedrive\.live\.com)\/s\/[A-Za-z0-9]+

Bölüm 12: Etiketleme (Tags) ve Açıklama (Annotations)

Analiz sırasında bir dosyanın "kanıt" niteliği taşıdığına karar verdiğinizde, onu sadece hatırlamak yetmez; raporlanabilir bir formata sokmanız gerekir.

12.1. Etiketleme Metodolojisi

Her bulguya rastgele etiket basmak yerine, hiyerarşik bir sistem kurun:

- **Tag: "Follow Up":** Daha detaylı incelenmesi gereken, şüpheli ama kesinleşmemiş dosyalar.
- **Tag: "Evidence - High":** Doğrudan suçla ilişkilendirilen, rapora girmesi kesin olan dosyalar.
- **Tag: "Privileged":** Avukat-müvekkil gizliliği gibi yasal nedenlerle rapordan muaf tutulması gereken veriler.

12.2. Analist Notları (Comments)

Bir dosyayı etiketlerken mutlaka "Neden" etiketlediğinizi belirten kısa, teknik ve objektif bir not ekleyin.

Örnek Not: "Dosya içeriğinde şüphelinin silmeye çalıştığı X_projesi_planlari.pdf belgesine ait metadata izleri saptanmıştır."

Bölüm 13: Gelişmiş Filtreleme (Content Filters)

Autopsy'nin merkezindeki "Views" sekmesini profesyonelce kullanmak, samanlıkta iğne aramayı bitirir.

Filtre Türü	Kullanım Amacı	Analist Stratejisi
File Size	Büyük boyutlu dosyaları bulma.	Genellikle video imajları veya disk şifreleme konteynerleri (container) büyük boyutludur.
MIME Type	İçerik türüne göre ayırma.	Uzantısı değiştirilmiş dosyaları (Örn: .txt görünümlü .exe) yakalamak için en etkili yoldur.
Past Week	Zaman bazlı kısıtlama.	Olayın gerçekleştiği kritik zaman dilimine odaklanarak diğer milyonlarca dosyayı gizler.

Bölüm 14: İşletim Sistemi ve Kullanıcı Analizi (OS Accounts)

Bir sistemde ne yapıldığından ziyade, bunu **kimin** yaptığını ispatlamak adli bilişimin temelidir. Autopsy, Windows ve Linux kayıt defterlerini (Registry) otomatik analiz ederek kullanıcı profillerini çıkarır.

14.1. Kullanıcı Profilleri ve Yetki Analizi

- **Kullanıcı Hesapları (OS Accounts):** Sistemdeki aktif, pasif veya gizlenmiş tüm yerel ve domain hesapları listelenir.
- **Login Denemeleri:** Şüphelinin sisteme en son ne zaman giriş yaptığı (Last Login) ve kaç başarısız deneme olduğu gibi veriler, "brute-force" saldırısı veya yetkisiz erişim teşebbüslerini kanıtlar.
- **SID (Security Identifier):** Her kullanıcının benzersiz kimlik numarasıdır. Silinmiş bir dosyanın sahipliğini (Owner) belirlemek için Autopsy üzerinden bu ID eşleştirmesi yapılır.

14.2. Run Programs ve Prefetch Analizi

Autopsy'nin en sevdiğimiz özelliklerinden biri; sistemde hangi programın, kaç kez ve en son ne zaman çalıştırıldığını göstermesidir.

- **Prefetch & Superfetch:** Bir uygulama çalıştırıldığında Windows'un oluşturduğu izlerdir. Şüpheli, analizden önce bir "Cleaning" (Temizlik) aracı çalıştırdıysa, burada o aracın izi kabak gibi görünür.

Bölüm 15: Mobil Cihaz Analizi (Android & iOS)

Autopsy 4.22.1, mobil cihaz imajlarını (Physical veya File System dump) işleyebilen güçlü modüllere sahiptir. Genellikle **ALEAPP (Android)** ve **iLEAPP (iOS)** kütüphanelerini kullanarak verileri anlamlandırır.

15.1. İletişim ve Sosyal Medya Artefaktları

- **Çağrı Kayıtları (Call Logs):** Gelen, giden ve cevapsız aramalar; süre ve kişi bilgisiyle dökülür.
- **Mesajlaşma (SMS/MMS/Chat):** SQLite veritabanları otomatik olarak çözülür. WhatsApp, Signal veya Telegram gibi uygulamaların yerel yedekleri (şifresiz ise) okunabilir hale getirilir.
- **Kişi Listesi:** Rehberdeki isimler ve bunlarla ilişkili e-posta veya sosyal medya hesapları.

15.2. Konum ve Hareket Verileri (Geolocations)

Mobil cihazlar birer "takip cihazı" gibidir. Autopsy şunları ayıklar:

- **Wi-Fi Geçmişi:** Cihazın bağlandığı SSİD'ler ve konumları.
- **GPS Etiketleri:** Fotoğrafların içine gömülü koordinatlar veya harita uygulamalarının önbellek verileri.

Bölüm 16: VICS Data Source (Görsel Kanıt Standartları)

Özellikle hassas vakalarda (İstismar, Narkotik vb.), binlerce görseli manuel incelemek analist üzerinde hem psikolojik baskı yaratır hem de zaman kaybına neden olur. **VICS (Video Image Classification Standard)** burada devreye girer.

Büyük hacimli görsel verileri (on binlerce fotoğraf ve video) manuel olarak incelemek hem zaman kaybıdır hem de analist üzerinde ağır psikolojik baskı yaratır. Autopsy 4.22.1, uluslararası standart olan **VICS (Video Image Classification Standard)** protokolünü destekleyerek bu süreci sistematik hale getirir.

16.1. Görsel Sınıflandırma

Autopsy, görselleri "Hash" değerlerine göre uluslararası veritabanlarıyla (Project Vic gibi) karşılaştırır ve otomatik olarak şu kategorilere ayırır:

- **Category 1-5:** Suçun ciddiyetine göre uluslararası standart etiketleme.
- **Görsel Kümeleme:** Birbirine benzeyen fotoğrafları gruplayarak (PhotoDNA benzeri teknolojilerle), aynı mekanda çekilmiş kareleri hızlıca analiz etmenizi sağlar.

PhotoDNA ve Hash Tabanlı Görsel Eşleştirme

Geleneksel MD5 veya SHA-256 hash değerleri, bir görseldeki tek bir piksel değiştiğinde tamamen farklı bir sonuç verir. Ancak **PhotoDNA** gibi teknolojiler, görselin "parmak izini" içeriğe göre çıkarır.

- **Görsel Kümeleme:** Autopsy, birbirine benzeyen (örneğin aynı mekanda çekilmiş veya sadece üzerinde oynanmış) fotoğrafları gruplandırarak hızlı analiz yapmanızı sağlar.
- **Hash Veritabanı Karşılaştırması:** Görseller, uluslararası suç veritabanlarındaki (Project Vic vb.) bilinen suç içerikli hash değerleriyle otomatik olarak karşılaştırılır.

VICS Kategorizasyon Standartları

- Analiz sırasında bulunan görseller, hukuki süreçlerin standartlaşması için belirli kategorilere ayrılır.

Kategori	Tanım	Analist Aksiyonu
Category 1	Çok Yüksek Riskli / Doğrudan Suç İçeriği	Anında "Notable" (Dikkat Çekici) olarak etiketle ve rapora ekle.
Category 2-4	Şüpheli / Aracı İçerik	Bağlamsal analiz için diğer artefaktlarla (web geçmişi vb.) eşleştir.
Category 5	Alakasız / Temiz İçerik	Analiz yükünü azaltmak için görünümden gizle.

Video Triage (Hızlı Video Önizleme)

Büyük video dosyalarını sonuna kadar izlemek imkansızdır. Autopsy eklentileri sayesinde **Video Triage** yöntemi uygulanır.

- **Thumbnail Çıkarımı:** Videonun belirli saniyelerinden (örneğin her 10 saniyede bir) otomatik olarak ekran görüntüsü alınır.
- **İçerik Analizi:** Analist, videoyu açmadan sadece bu küçük resimlere bakarak videonun kanıt niteliği taşıyıp taşımadığına karar verebilir.

Bölüm 17: Extractor Modülleri (Data Raw Analysis)

Bazı veriler dosya sisteminde değil, diskin en karanlık köşelerinde (Unallocated Space) gizlidir.

- **Keyword Search Extractor:** Diskteki her bir sektörü tarayarak e-posta adresleri, IP adresleri ve URL'leri ayıklar.
- **Archive Extractor:** .zip, .7z, .tar gibi sıkıştırılmış dosyaları tek tek açıp içindeki dosyaları sanki normal birer dosyaymış gibi ana analize dahil eder.

Profesyonel İpucu: Mobil analiz yaparken Autopsy'nin bulamadığı veriler olursa, "Application" sekmesinden doğrudan SQLite veritabanına (.db veya .sqlite) manuel olarak bakın. Autopsy size yerleşik bir **SQLite Viewer** sunar; bazen modüllerin kaçırdığı bir tablo satırı, davanın anahtar kanıtı olabilir.

Bölüm 18: Kayıt Defteri (Registry) ve Dijital İz Analizi

Windows işletim sisteminde atılan her adımın Registry üzerinde bir izi vardır. Autopsy bu karmaşık yapıyı (Hives) bizim için anlamlandırır.

18.1. USB ve Harici Donanım Geçmişi

Şüphelinin "Ben bu USB belleği hiç takmadım" savunmasını çürüten yer burasıdır.

- **USBSTOR:** Sisteme takılan her USB cihazın marka, model ve seri numarası kayıt altına alınır.
- **MountPoints2:** Hangi cihazın hangi harf (Örn: E:\, G:\) ile bağlandığını gösterir.
- **First/Last Connected:** Cihazın sisteme ilk ve son takılma zaman damgaları, olay örgüsü (timeline) için kritiktir.

18.2. Ağ Bağlantıları (Network History)

- **Wireless Profiles:** Cihazın daha önce bağlandığı tüm Wi-Fi ağlarının isimleri (SSID) ve şifreleme türleri burada saklanır. Bu, şüphelinin olay anında hangi konumda olduğuna dair güçlü bir kanıttır.

Bölüm 19: Apache Solr ve Arama Optimizasyonu

Autopsy, milyonlarca dosya içindeki kelimeleri anında bulmak için arka planda **Apache Solr** indeksleme motorunu kullanır. Ancak bu motoru verimli kullanmak bir sanattır.

19.1. İndeksleme Stratejisi

Veriyi ilk eklediğinizde (Ingest), "Keyword Search" modülü tüm metinleri bir kütüphaneye yazar.

- **Avantajı:** Analiz bittikten sonra "kredi kartı" diye arattığınızda, Autopsy 1 terabaytlık diski saniyeler içinde tarayıp sonucu getirir.
- **Dezavantajı:** İndeksleme işlemi CPU ve disk ömrünü (IOPS) çok yorar. Bu yüzden sadece gerekli dilleri ve dosya türlerini seçmek profesyonel bir yaklaşımdır.

19.2. Regular Expressions (Regex) - İleri Seviye Arama

Profesyonel bir analist, sadece kelime aratmaz; "kalıp" aratır. Autopsy içinde yerleşik gelen bazı Regex kalıpları şunlardır:

- **IP Adresleri:** (\d{1,3}\.){3}\d{1,3}
- **E-posta Adresleri:** [A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a-z]{2,}
- **Telefon Numaraları:** Belirli bir bölge koduna göre özelleştirilmiş kalıplar.

19.3: Performans Sorunları ve Çözüm Stratejileri

- Autopsy 4.22.1 güçlüdür ancak büyük veriler altında (Big Data) sistem kaynaklarını zorlayabilir. Analizin ortasında kilitlenen bir sistem, en büyük kabusunuzdur.

Sık Karşılaşılan Sorunlar ve Çözümleri

Sorun	Olası Neden	Çözüm Stratejisi
Arayüz Kilitlenmesi	Yetersiz RAM veya Solr Bellek Taşması	Araçlar -> Seçenekler kısmından Solr için ayrılan RAM miktarını artırın.
Yavaş İndeksleme	Çok fazla modülün aynı anda çalışması	Sadece hedefe yönelik Ingest Modüllerini seçin (Örn: Sadece Fotoğraflar).
Disk Dolu Hatası	Vaka dizininin dolması	Vaka dizini için imaj boyutunun en az iki katı boş alana sahip bir SSD kullanın.
Keyword Search Hatası	Solr indeksinin bozulması	Indexing Status kontrol edin; gerekirse indeksi silip sadece kritik kelimelerle yeniden başlatın.

Profesyonel Optimizasyon İpuçları

- **NSRL Filtreleme:** Analiz yükünü %70-80 azaltmak için bilinen sistem dosyalarını mutlaka eleyin.
- **Önceliklendirme (Triage):** Tüm diski taramadan önce, kullanıcının Desktop ve Documents klasörlerine öncelik veren özel dosya filtreleri oluşturun

Bölüm 20: Analizi Derinleştiren Eklentiler (Third-Party Plugins)

Autopsy'nin en büyük gücü, açık kaynak topluluğu tarafından geliştirilen eklentilerdir. "Tools -> Plugins" menüsünden erişebileceğiniz bu eklentiler, standart sürümde olmayan yetenekler kazandırır.

Profesyonel Analiz İçin Olmazsa Olmaz Eklentiler:

- **Browsing History View:** Chrome, Firefox ve Edge geçmişini tek bir birleşik tabloda sunarak kullanıcı aktivitelerini korele eder.
- **Skype/Discord Analyzer:** Standart modüllerin parse edemediği yeni nesil mesajlaşma veritabanlarını çözümler.
- **C4All (Cloud for All):** Bulut depolama servislerinin (Google Drive, OneDrive) yerel kalıntılarını daha derinlemesine analiz eder.

Analist Notu: Görsel analiz yaparken Autopsy'nin sağ alt panelindeki **"Application"** sekmesini kullanın. Bu sekme, görselleri işletim sisteminin kendi aracıyla açıyormuş gibi orijinal haliyle gösterirken, dosyanın metadata (EXIF) bilgilerini de yan panelde hazır tutar.

- **Video Triage:** Büyük video dosyalarının içinden belirli aralıklarla "thumbnail" (küçük resim) alarak, videonun tamamını izlemeden içeriği hakkında fikir sahibi olmanızı sağlar.
- **Skype/Discord Analyzer:** Standart modüllerin kaçırabileceği yeni nesil mesajlaşma uygulamalarının veritabanlarını parse eder.
- **Browsing History View:** Chrome, Firefox ve Edge geçmişini daha gelişmiş bir tabloda birleştirerek sunar.

Bölüm 21: Mahkeme İçin Rapor Sunum Teknikleri

Analiz bitti, kanıtlar bulundu; ancak iş burada bitmiyor. Dijital adli bilişim raporu, sadece bir teknik belge değil, bir "hukuki tercüme"dir. Teknik terim bilmeyen bir hakime veya savcıya, karmaşık bir siber olayı basitçe anlatabilmeniz gerekir.**Kanıtların Görselleştirilmesi:** Sadece dosya yolu (path) vermek yerine, Autopsy'den aldığınız ekran görüntülerini (screenshot) rapora ekleyin.

İyi bir rapor, teknik uzmanlığı tarafsızlıkla birleştirmelidir:

- **Yönetici Özeti (Executive Summary):** En başta, teknik detaylara girmeden olayın sonucunu (Örn: "X dosyasının Y tarihinde silindiği saptanmıştır") net bir şekilde belirtin.
- **Yöntem ve Donanım:** Analizde kullanılan Autopsy 4.22.1 versiyonu ve **Write Blocker** gibi donanımları listeleyin.
- **İlliyet Bağı:** Kanıt ile şüpheli arasındaki bağı (Örn: SID eşleştirmesi) somut verilerle kurun.

Mahkemede İfade Verme (Testifying)

Mahkemede bilirkişi olarak bulunduğunuzda şu altın kuralları uygulayın:

- **Jargonu Basitleştirin:** "Unallocated space" yerine "diskten silinmiş ama henüz üzerine veri yazılmamış alan" tanımını kullanın.
- **Hash Değerlerine Dayanın:** Sorulara "sanırım" yerine "Hash değerleri verinin değişmediğini kanıtlamaktadır" gibi kesin cevaplar verin

1. **Teknik Olmayan Özet:** Raporun en başına, teknik terim bilmeyen birinin bile anlayabileceği 1 sayfalık "Özet" koyun.
2. **Hash Onayı:** Raporun sonuna mutlaka "Bu analiz sırasında orijinal veri üzerinde hiçbir değişiklik yapılmamıştır" ibaresini ve hash değerlerini ekleyerek profesyonel imzanızı atın.

Önemli Not: Autopsy 4.22.1 kullanırken vaka dosyanızın bulunduğu disk dolarsa, veritabanı bozulabilir. Analize başlamadan önce her zaman vaka diskinizde (Case Directory) en az imaj boyutu kadar boş alan olduğundan emin olun.

Bölüm 22: Teknik Kod Yapıları ve Sorgu Dilleri

Autopsy içerisinde veriyi manipüle etmek ve özel aramalar yapmak için üç temel yapı kullanılır: **SQLite**, **RegEx** ve **Solr/Lucene**.

22.1. SQLite Sorguları (Veritabanı Analizi)

Autopsy, tüm uygulama verilerini, mesaj geçmişlerini ve sistem kayıtlarını .db veya .sqlite formatında saklar. Yerleşik "SQLite Viewer" üzerinde kendi sorgularını yazarak modüllerin bulamadığı verileri çekebilirsin.

Örnek Senaryo: Bir mesajlaşma veritabanından sadece belirli bir tarihten sonraki ve "silinmiş" olarak işaretlenmiş mesajları çekmek:

```
SELECT message_date, sender, text_body
FROM messages
WHERE is_deleted = 1 AND message_date > '2024-01-01'
ORDER BY message_date DESC;
```

Bu tür bir sorgu, analistin binlerce satır arasında kaybolmasını engeller.

22.2. Regular Expressions (RegEx - Düzenli İfadeler)

"Keyword Search" kısmında standart kelimeler yerine "kalıplar" aratmak için kullanılır. Autopsy'de en çok kullanılan kod yapıları şunlardır:

- **E-posta Yakalama:** [A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a-z]{2,}
- **Kredi Kartı (Visa) Yakalama:** ^4[0-9]{12}(?:[0-9]{3})?$
- **IPv4 Adresi Yakalama:** \b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b
- **MAC Adresi Yakalama:** ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$

22.3. Solr / Lucene Sorgu Dili

Autopsy'nin arama motoru olan Apache Solr, gelişmiş arama parametrelerini destekler. Arama çubuğuna yazabileceğin mantıksal operatörler şunlardır:

- **Boolean Operatörleri:** sifre AND gizli (Her iki kelimenin geçtiği dosyaları bulur).
- **Veya Operatörleri:** iphone OR android (İkisinden birinin geçtiği dosyaları bulur).
- **Gruplama:** (istifa OR yolsuzluk) AND "gizli belge" (Belirli bir kombinasyonu arar).
- **Wildcard (Joker):** forens* (Forensics, forensic, forensically gibi tüm kelimeleri kapsar).

22.4. Python ve Java ile Modül Geliştirme (Scripting)

Autopsy açık kaynaklı olduğu için kendi "Ingest Module"lerini yazabilirsin.

- **Jython (Python on Java):** Autopsy, Python scriptlerini kabul eder. Eğer piyasada olmayan yeni bir sohbet uygulamasının verilerini parse etmek istersen, Python ile bir IngestModule yazıp Autopsy'ye entegre edebilirsin.

Basit Bir Modül Yapısı Örneği (Mantıksal Akış):

```
class MySampleIngestModule:
    def process(self, dataSource, progressBar):
        # 1. Veri kaynağına bağlan
        # 2. Belirli dosyaları (örneğin .log) tara
        # 3. Dosya içindeki veriyi oku
        # 4. Sonuçları Autopsy "Blackboard"una (sonuç paneli) gönder
        return IngestModule.OK
```

22.5. TSK (The Sleuth Kit) Komut Satırı Araçları

Autopsy'nin arka planındaki "The Sleuth Kit" komut satırından da yönetilebilir. Profesyoneller bazen çok büyük disk imajlarını önceden taramak için terminal (CMD/Bash) üzerinden şu kodları kullanır:

fls -r image.e01: İmaj içindeki tüm dosyaları listeler.

icat -o offset image.e01 inode_no: Belirli bir inode numarasındaki dosyayı dışarı çıkartır.

img_stat image.e01: İmajın teknik detaylarını (sektör boyutu, disk yapısı vb.) verir.

Bölüm 23: Autopsy İçin Python (Jython) Eklentisi Geliştirme

Autopsy, Python kodlarını Java sanal makinesi üzerinde çalıştıran **Jython** altyapısını kullanır. Bu sayede hem Python'ın yazım kolaylığından faydalanabilir hem de Autopsy'nin tüm Java API'lerine erişebilirsiniz.

23.1. Eklenti Türleri

Eklenti yazmaya başlamadan önce hangi türde bir modül yazacağınıza karar vermelisiniz:

1. **Ingest Modules:** Veri kaynağı eklenirken çalışan ve veriyi otomatik işleyen modüller (En yaygın olanı).
2. **Report Modules:** Analiz bittikten sonra özel formatta raporlar oluşturan modüller.
3. **Content Viewer Modules:** Sağ alt panelde dosyaları farklı bir gözle (Örn: özel bir şifreleme formatını çözerek) görmenizi sağlayan modüller.

23.2. Bir Ingest Modülünün Anatomisi

Bir Python eklentisi temel olarak üç ana sınıftan (class) oluşur. Bu yapı standarttır ve Autopsy'nin modülü tanıyabilmesi için şarttır:

1. **Factory Class:** Modülün adını, versiyonunu ve hangi türde (File-level veya Data-source level) çalışacağını sisteme bildirir.
2. **Settings Class:** Kullanıcı modülü çalıştırırken bir arayüz görsün mü? Hangi ayarları seçebilsin? (Opsiyoneldir).
3. **Process Class: İşin mutfağı burasıdır.** Her bir dosya veya veri kaynağı için çalışacak asıl Python kodları burada yazılır.

23.3. Örnek Senaryo: "Zararlı Dosya Uzantısı Yakalayıcı"

Diyelim ki sistemde **.exe** olup da kendini **.jpg** gibi gösteren dosyaları yakalayan bir eklenti yazmak istiyoruz. İşte temel mantık çerçevesi:

```
# Autopsy API kütüphanelerini içe aktar
from java.util.logging import Level
from org.sleuthkit.autopsy.casemodule import Case
from org.sleuthkit.autopsy.ingest import IngestModule
from org.sleuthkit.datamodel import TskData

class MyExtensionModule(IngestModule):
    def process(self, file):
        # 1. Dosyanın gerçek imzasını (MIME Type) kontrol et
        actual_type = file.getMIMEType()

        # 2. Dosya uzantısını al
        extension = file.getNameExtension()

        # 3. Mantıksal karşılaştırma yap
        if actual_type == "application/x-msdownload" and extension == "jpg":
            # 4. Eğer bir uyumsuzluk varsa, bunu "Blackboard" (Sonuçlar) kısmına gönder
            art = file.newArtifact(TskData.ArtifactType.TSK_INTERESTING_FILE_HIT)
            print("Şüpheli dosya yakalandı: " + file.getName())

        return IngestModule.ProcessResult.OK
```

23.4. Geliştirme ve Test Süreci

Eklentinizi yazdıktan sonra Autopsy'ye tanıtmak oldukça basittir:

1. **Dizin:** Autopsy içinden Tools -> Python Plugins seçeneğine tıklayın. Açılan klasöre yazdığınız .py dosyasını atın.
2. **Yeniden Başlatma:** Autopsy'yi kapatıp açtığınızda, "Ingest Modules" listesinde kendi modülünüzü göreceksiniz.
3. **Hata Ayıklama (Debugging):** Python kodunuzda bir hata varsa, Autopsy'nin log dosyasını (app.log) inceleyerek hatanın hangi satırda olduğunu görebilirsiniz.

23.5. Blackboard Kavramı (Veri Paylaşımı)

Autopsy'de bir modülün bulduğu sonucu kullanıcıya göstermesinin yolu **Blackboard** (Yazı Tahtası) sistemidir.

- Yazdığınız kod bir kanıt bulduğunda, bunu "Blackboard" üzerine bir **Artifact** (Bulgu) olarak yazar.
- Bu sayede bulgularınız, Autopsy'nin sol panelindeki "Results" kısmında diğer standart bulgularla birlikte listelenir.

Geliştirici Notu: Eklenti yazarken Autopsy'nin sunduğu SampleIngestModule.py şablonunu kullanmak hayat kurtarır. Bu şablon, gerekli tüm "boilerplate" (hazır kalıp) kodları içerir; size sadece process fonksiyonunun içini doldurmak kalır.

Bölüm 24: Uygulamalı Vaka Örnekleri (Case Studies)

Teorik bilgiyi pekiştirmek için Autopsy ile çözülebilecek iki temel senaryoyu inceleyelim.

Senaryo 1: Şirket İçi Veri Sızıntısı (Data Exfiltration)

Olay: Bir çalışan, istifa etmeden önce şirkete ait gizli projeleri kişisel USB belleğine kopyalamakla suçlanıyor.

- **Analiz Adımları:**
    1. **USBSTOR Analizi:** Kayıt defterinden şüphelinin bilgisayarına takılan USB cihazların seri numaraları belirlendi.
    2. **LNK Files & Jump Lists:** Şüphelinin en son açtığı dosyalar incelendi; gizli projelerin USB takılıyken açıldığı görüldü.
    3. **Shell Bags:** Şüphelinin USB içerisindeki hangi klasörlerde gezindiği tespit edildi.
    4. **Sonuç:** USB'nin seri numarası ile dosya erişim zamanları eşleştirilerek kanıtlandı.

Senaryo 2: Zararlı Yazılım ve Uzaktan Erişim (RAT)

Olay: Bir yöneticinin bilgisayarına yetkisiz erişim sağlandığı ve web kamerasının izlendiği şüphesi var.

- **Analiz Adımları:**
    1. **Network Connections:** Established durumdaki şüpheli dış IP adresleri yakalandı.
    2. **Prefetch Analizi:** Sistemde daha önce hiç kurulmamış olan bir "RAT.exe" dosyasının çalışma izleri bulundu.
    3. **Web History:** Şüphelinin bir oltalama (phishing) linkine tıkladığı ve zararlı yazılımı indirdiği URL tespit edildi.
    4. **Sonuç:** Zararlı yazılımın sisteme girdiği an ve hangi verileri dışarı sızdırdığı raporlandı.

Bölüm 25: Dijital Adli Bilişim Terimler Sözlüğü (Glossary)

Sektörde ve Autopsy arayüzünde en çok karşılaşacağın İngilizce terimlerin Türkçe karşılıkları ve teknik anlamları:

Terim	Türkçe Karşılığı	Açıklama
Artifact	Artefakt / Kanıt İzi	Bir dijital aktivite sonrası sistemde kalan veri kırıntısı.
Admissibility	Kabul Edilebilirlik	Kanıtın mahkemede yasal olarak geçerli sayılması durumu.
Chain of Custody	Kanıt Zinciri	Kanıtın ele geçirilmesinden mahkemeye kadar olan süreçteki kayıt formu.
Data Carving	Veri Kazıma	Dosya sistemi bozuk olsa bile dosya imzalarından veri kurtarma işlemi.
Hash Value	Özet Değer	Verinin dijital parmak izi (MD5, SHA-1, SHA-256).
Ingest	Veri İşleme / İçeri Alma	Ham verinin analiz modülleri tarafından taranması süreci.
Live Forensics	Canlı Adli Bilişim	Çalışan bir sistemin RAM ve ağ verilerinin anlık analizi.
Mount	Bağlamak	Bir disk imajını sanki fiziksel bir sürücüymüş gibi sisteme tanıtmak.
Unallocated Space	Tahsis Edilmemiş Alan	Dosya sistemi tarafından boş görünen ama silinmiş veri içerebilen alan.

Terim	Türkçe Karşılığı	Açıklama
Write Blocker	Yazma Koruyucu	Orijinal kanıtın üzerine veri yazılmasını engelleyen donanım/yazılım.
Triage	Önceliklendirme	Çok büyük veri yığınları arasında kritik kanıtların hızlıca tespiti.
MIME Type	Dosya İçerik Türü	Uzantıdan bağımsız olarak dosyanın gerçek türünü belirten etiket.

Bölüm 26: Analist Hataları, Hukuki Sorumluluk ve Raporlama

Dijital adli bilişimde hata payı sıfıra yakın olmalıdır. Çünkü dijital delil, "kırılgan" (fragile) bir yapıya sahiptir; tek bir yanlış tıklama, verinin hash değerini değiştirerek onu mahkeme gözünde "geçersiz" kılabilir.

26.1. Analistlerin Sıkça Yaptığı Kritik Hatalar

Profesyonel bir süreçte şu hatalar "ölümcül" kabul edilir:

1. **Yazma Korumasız İnceleme:** Orijinal delile donanımsal veya yazılımsal **Write Blocker** (Yazma Engelleyici) kullanmadan erişmek. (En ufak bir metadata değişimi kanıtı bozar).
2. **Dosya Uzantısına Güvenmek:** Bir dosyanın sadece .jpg veya .txt olmasına bakarak karar vermek. (Gelişmiş analizde her zaman MIME tipi kontrol edilmelidir).
3. **Hash Doğrulamasını Atlamak:** İmaj alırken ve analiz bitiminde hash değerlerini karşılaştırmamak.
4. **Önyargılı Analiz (Confirmation Bias):** Sadece şüpheliyi suçlayacak delillere odaklanıp, onu aklayabilecek (exculpatory) delilleri görmezden gelmek.

26.2. Delil Zinciri (Chain of Custody) Protokolü

Delil zinciri, delilin "kimin elinden geçtiğini" belgeleyen kutsal bir dokümandır. Bu zincirde bir saniyelik kopukluk bile savunma avukatının kanıtı çürütmesine yeter.

Zincirin Bozulmaması İçin Gerekenler:

- **Unique Identifier:** Her delile benzersiz bir vaka/delil numarası verilmeli.
- **Secure Storage:** Analiz dışındaki zamanlarda deliller, statik elektriği engelleyen torbalarda ve kilitli dolaplarda (Faraday kafesi özellikli) saklanmalı.
- **Activity Logs:** "Analiz başladı", "Analiz durduruldu", "Delil kasaya kaldırıldı" gibi her adım saat/dakika bazlı imzalanmalı.

26.3. Hukuki Sorumluluk ve Etik

Bir adli bilişim uzmanı mahkemede **"Bilirkişi" (Expert Witness)** sıfatıyla bulunur.

- **Tarafsızlık:** Analist, savcının veya savunmanın tarafı değildir; o sadece "verinin" tarafıdır.
- **Yalan Beyan:** Mahkemeye sunulan raporun yanlış veya yanıltıcı olması, "Yargıyı yanıltma" suçuna girer ve analistin hapis cezası almasına yol açabilir.
- **Gizlilik:** Vaka verilerinin (şirket sırları, özel hayat vb.) üçüncü şahıslarla paylaşılması KVKK (Türkiye için) ve GDPR kapsamında ağır suçtur.

26.4. Mahkemeye Sunulacak Raporun Standartları

Mahkeme raporu, Autopsy'den çıkan ham çıktı değildir; o verilerin **hukuki ve teknik yorumudur.**

Bölüm	İçerik ve Dikkat Edilmesi Gerekenler
Giriş (Introduction)	Vakanın özeti, görevlendiren makam ve inceleme amacı.
Yöntem (Methodology)	Kullanılan donanım (Write Blocker) ve yazılım (Autopsy 4.22.1) versiyonları.
Teknik Analiz	Bulunan dosyaların **Hash değerleri**, sistemdeki yolları (Path) ve ekran görüntüleri.
Bulguların Yorumu	"X dosyası bulundu" yerine; "X dosyası Y tarihinde Z kullanıcısı tarafından oluşturulmuş ve silinmiştir" tespiti.
Sonuç (Opinion)	Kesin ve net yargılar. "Olabilir, sanırım" gibi ifadelerden kaçınılmalıdır.

26.5. Mahkemede İfade Verme (Testifying)

Analist, raporunu sunduktan sonra mahkemeye çağrılabilir.

- **Jargon Kullanımı:** Hakim veya savcı "inode" veya "unallocated space" terimlerini bilmeyebilir. Analist, teknik kavramları "bir çocuğun anlayabileceği" kadar basitleştirerek anlatmalıdır.
- **Eminlik:** Sorulan sorulara "Evet/Hayır" veya "Veriler bunu gösteriyor" şeklinde, hash değerlerine dayanarak cevap verilmelidir.

Bölüm 27: Adli Bilişim Analiz Kontrol Listesi (Checklist)

Bir vaka üzerinde çalışırken hata yapmamak için şu maddelerin üzerini tek tek çizin:

1. Hazırlık ve El Koyma Aşaması

- [ ] **Yasal İzin:** Arama ve el koyma kararı (vaka emri) dosyanızda mı?
- [ ] **Donanım Kontrolü:** Yazma Koruyucu (Write Blocker) çalışıyor mu ve güncel mi?
- [ ] **Steril Ortam:** Analiz makineniz internetten yalıtılmış ve önceki vakalardan temizlenmiş mi?
- [ ] **Kanıt Zinciri:** "Chain of Custody" formu oluşturuldu ve ilk imza atıldı mı?

2. İmaj Alma ve Doğrulama

- [ ] **Fiziksel İmaj:** Diskin ham (RAW) veya E01 formatında tam bir kopyası alındı mı?
- [ ] **Hash Hesaplama:** Orijinal diskin Hash değeri (MD5/SHA-256) not edildi mi?
- [ ] **Doğrulama:** İmajın Hash değeri ile orijinal diskin Hash değeri eşleşiyor mu?
- [ ] **Yedekleme:** İmajın bir kopyası güvenli bir depolama alanına (vault) kaldırıldı mı?

3. Autopsy Analiz Süreci

- [ ] **Case Oluşturma:** Vaka numarası ve analist bilgileri doğru girildi mi?
- [ ] **Zaman Dilimi:** Sistem saati ve "Time Zone" ayarları (UTC offset) doğru yapılandırıldı mı?
- [ ] **Ingest Modülleri:** Vaka türüne uygun modüller (Keyword, Email, Registry vb.) seçildi mi?
- [ ] **NSRL Filtresi:** Bilinen sistem dosyalarını elemek için Hash Set yüklendi mi?

4. Derinlemesine İnceleme

- [ ] **Keyword Search:** Vaka ile ilgili özel terimler ve Regex kalıpları aratıldı mı?
- [ ] **Timeline Analizi:** Olayın gerçekleştiği tarih aralığındaki aktiviteler incelendi mi?
- [ ] **Artifact Kontrolü:** Web geçmişi, USB geçmişi ve kullanıcı hesapları analiz edildi mi?
- [ ] **Unallocated Space:** Silinmiş dosyalar için "Carving" işlemi yapıldı mı?

5. Raporlama ve Kapanış

- [ ] **Etiketleme:** Önemli bulgular "Tag" sistemi ile işaretlendi mi?
- [ ] **Ekran Görüntüleri:** Kritik bulguların ekran görüntüleri (metadataları ile birlikte) alındı mı?
- [ ] **Tarafsız Dil:** Rapor subjektif yorumlardan arındırılıp teknik verilere dayandırıldı mı?
- [ ] **Hash Final:** Raporun sonuna imajın değişmediğini gösteren hash doğrulaması eklendi mi?

Profesyonel Tavsiye: Eğer bu listedeki tek bir maddeyi bile atladıysanız, analizinizi mahkemede savunmanız oldukça güçleşecektir. Her zaman "önce belgele, sonra işle" prensibiyle hareket edin.

Bölüm 28 — Autopsy İngilizce–Türkçe Terimler Sözlüğü

28.1 Temel Arayüz Terimleri

İngilizce Terim	Türkçe Karşılık	Kısa Açıklama
Case	Vaka / İnceleme Dosyası	İnceleme çalışma alanı
Data Source	Veri Kaynağı	Analiz edilen imaj / klasör
Ingest	Otomatik Analiz	İlk tarama / parse süreci
Module	Modül	Belirli analiz bileşeni
Results	Sonuçlar	Ingest çıktıları
Views	Görünümler	Kategorik veri görünümü
Timeline	Zaman Çizelgesi	Olay sıralaması
Report	Rapor	Dışa aktarılan çıktı
Tag	Etiket	Önemli bulgu işareti
Bookmark	Yer İşareti	Kritik nokta kaydı

28.2 Dosya Sistemi ve Artefakt Terimleri

İngilizce	Türkçe	Açıklama
Deleted Files	Silinmiş Dosyalar	Silinmiş veri kalıntıları
Recycle Bin	Geri Dönüşüm Kutusu	Silinen dosya alanı
File Carving	İmza Tabanlı Kurtarma	Header / footer ile kurtarma
Metadata	Üst Veri	Dosya teknik bilgisi
File Signature	Dosya İmzası	Dosya tipi izi
Header	Başlık Verisi	Dosya başlangıç yapısı
Footer	Sonlandırıcı Veri	Dosya sonu yapısı
Slack Space	Boşluk Alanı	Diskte artakalan veri
Unallocated Space	Ayrılmamış Alan	Dosya sistemi dışı boş alan
Cluster	Küme	Disk veri birimi

28.3 Web ve Kullanıcı Aktivite Terimleri

İngilizce	Türkçe	Açıklama
Browser History	Tarayıcı Geçmişi	Ziyaret edilen siteler
Cache	Önbellek	Geçici web verisi
Cookies	Çerezler	Oturum / tercih verisi
Downloads	İndirilenler	İndirilen dosya kayıtları
Upload	Yükleme	Dış ortama veri gönderimi

İngilizce	Türkçe	Açıklama
Session	Oturum	Kullanıcı web etkileşimi
Recent Activity	Son Aktiviteler	Son kullanıcı hareketleri
Search Query	Arama Sorgusu	Kullanıcı araması

28.4 Zaman ve Olay Korelasyon Terimleri

İngilizce	Türkçe	Açıklama
Timestamp	Zaman Damgası	Tarih / saat bilgisi
Created Time	Oluşturma Zamanı	Dosya ilk oluşum
Modified Time	Değiştirme Zamanı	Son içerik değişimi
Accessed Time	Erişim Zamanı	Son erişim
Changed Time	Metadata Değişimi	NTFS değişiklik izi
Timezone	Saat Dilimi	Bölgesel saat farkı
Correlation	Korelasyon	Olay ilişkilendirme
Event Sequence	Olay Sırası	Zaman akışı
Timestomping	Zaman Manipülasyonu	Tarih değiştirme

28.5 Delil ve Raporlama Terimleri

İngilizce	Türkçe	Açıklama
Evidence	Delil	İncelenen veri
Chain of Custody	Delil Zinciri	Delil teslim süreci
Acquisition	İmaj Alma / Toplama	Delil toplama işlemi
Hash	Özet Değer	Bütünlük doğrulama
SHA-256	SHA-256	Güçlü hash algoritması
Verification	Doğrulama	Bütünlük kontrolü
Export	Dışa Aktarma	Çıktı alma
Findings	Bulgular	Tespit edilen teknik veriler
Conclusion	Sonuç	Teknik değerlendirme

28.6 Analist İçin Sık Kullanılan Teknik Kavramlar

İngilizce	Türkçe	Açıklama
False Positive	Yanlış Pozitif	Hatalı alarm / bulgu
Noise	Gürültü	Gereksiz veri yükü
Triage	Hızlı Ön İnceleme	İlk risk taraması
Deep Analysis	Derin Analiz	Ayrıntılı inceleme
Artifact	Dijital İz / Artefakt	Sistem kalıntısı

İngilizce	Türkçe	Açıklama
Parse	Ayrıştırma	Veriyi çözümleme
Indexing	İndeksleme	Hızlı arama hazırlığı
Log	Kayıt	Sistem kayıt verisi
Volatile Data	Uçucu Veri	Anlık silinebilen veri

Kitap Kapanışı: Profesyonel Etik ve Gelecek

Kankam, bu rehberle birlikte **Autopsy 4.22.1** dünyasına tam donanımlı bir giriş yapmış olduk. Unutma, dijital adli bilişim sadece teknik bir iş değil, aynı zamanda yüksek bir etik sorumluluktur. Bulduğun her kanıt bir insanın hayatını veya bir kurumun geleceğini değiştirebilir.

Autopsy 4.22.1 Arayüz Hiyerarşisi (Ağaç Yapısı)

- **[Case Name] (Vaka Adı)**
  - 📂 **Data Sources (Veri Kaynakları)**
    - 📁 *[Image/Disk Name]* (Disk İmajı Adı)
      - 📄 *Volume System* (Birim Sistemi / Partitionlar)
        - 📂 *File System* (Dosya Sistemi - NTFS, FAT, Ext4 vb.)
          - 📁 $OrphanFiles (Sahipsiz/Yetim Dosyalar)
          - 📁 [Root] (Kök Dizin)

🔍 **Views (Görünümler)**

- 🖼️ **File Types (Dosya Türleri)**
  - 📝 *By Extension* (Uzantıya Göre - Documents, Images, Videos)
  - ⚙️ *By MIME Type* (İçerik Türüne Göre - Gerçek dosya türleri)
- 🗑️ **Deleted Files (Silinmiş Dosyalar)**
  - 📄 *FileSystem* (Dosya sisteminden silinenler)
  - ⛏️ *All* (Tüm silinmiş izleri)
- 📦 **File Size (Dosya Boyutu)**
  - 📊 *50MB - 200MB* (Büyük veri bloklarını bulmak için)

🎯 **Results (Analiz Sonuçları)**

- 🧩 **Extracted Content (Ayıklanan İçerik)**
  - 🌐 *Web History* (Tarayıcı Geçmişi)

    - 📧 *E-mail Messages* (E-posta Mesajları)
    - 📱 *Call Logs / SMS* (Arama Kayıtları ve Mesajlar)
    - 💻 *Installed Programs* (Yüklü Programlar)
    - 🔑 *Operating System User Accounts* (Kullanıcı Hesapları)
- 🚩 **Keyword Hits (Anahtar Kelime Eşleşmeleri)**
    - 🔎 *Exact Match* (Tam Eşleşen Kelimeler)
    - 🧬 *Regex Match* (Kalıp/Desen Eşleşmeleri)
- ⚠️ **Hashset Hits (Hash Seti Eşleşmeleri)**
    - 🚫 *Notable Files* (Dikkat Çekici / Yasaklı Dosyalar)
- 📍 **Geolocation (Coğrafi Konum)**
    - 🗺️ *GPS Trackpoints* (Konum Bilgileri)

🏷️ **Tags (Etiketler)**

- 📌 *Follow Up* (Takip Edilecekler)
- 🏅 *Evidence* (Kesin Kanıtlar)

📊 **Reports (Raporlar)**

- 📄 *HTML / Excel / PDF Reports*

Hiyerarşi Rehberi (Kısa Notlar)

- **Data Sources:** Verinin **fiziksel** konumuna bakmak için kullanılır. "Bu dosya hangi klasörün içindeydi?" sorusuna yanıt verir.
- **Views:** Verinin **mantıksal** yapısına odaklanır. "Dosya nerede olursa olsun bana tüm videoları göster" diyen analist burayı kullanır.
- **Results:** Autopsy modüllerinin (Ingest Modules) **akıllı** analizlerinin sonucudur. Ham veriden anlamlı bilgiye (Artifact) dönüşmüş kısımdır.
- **Tags:** Analistin **subjektif** kararlarıdır. Binlerce dosya içinden rapora gidecek olanları burası ayıklar.

Autopsy Veri Hiyerarşisi (Tree Structure)

Autopsy'de veriler, bir ağacın kökünden uç dallarına doğru şu mantıkla ilerler:

- **Root (Kök): Case Name**
    - **Data Sources (Ana Gövde):** İmaj dosyalarınız (E01, RAW, VMDK).
        - *Partition (Bölüm):* Disk bölümleri (C:, D: vb.).
            - *File System:* Dosyalar ve klasörler.
    - **Views (Görünüm Dalları):** Dosyaların "ne" olduğuna göre filtrelenmiş hali.
        - *File Types:* Resimler, Videolar, Dökümanlar, Executable'lar.
        - *Deleted Files:* Sadece silinmiş dosyaların toplandığı dal.
        - *File Size:* Boyutlarına göre ayrılmış dosyalar.
    - **Results (Analiz Meyveleri):** Ingest modüllerinin ürettiği kanıtlar.
        - *Extracted Content:* Web geçmişi, e-postalar, yüklü programlar.
        - *Keyword Hits:* Bulunan anahtar kelimeler.
        - *Hashset Hits:* Kara listedeki dosyalar.
    - **Tags (İşaretli Yapraklar):** Sizin "Kanıt" olarak mühürlediğiniz her şey.

Bu Yapının Mantığı Nedir?

1. **Gövde (Data Sources):** Verinin fiziksel yerini söyler. ("Bu dosya diskin neresinde?")
2. **Dallar (Views & Results):** Verinin fonksiyonunu söyler. ("Bu dosya bir suç aleti mi yoksa sistem dosyası mı?")
3. **Yapraklar (Tags):** Sizin kararınızı söyler. ("Bu dosya rapora girecek mi?")

Autopsy Kullanıcı Dokümantasyonu 4.22.1

Vakalar ve Veri Kaynakları

Autopsy, verileri vaka bazında düzenler. Her vakanın bir veya daha fazla veri kaynağı olabilir ; bunlar disk görüntüsü, mantıksal dosya kümesi, USB bağlantılı cihaz vb. olabilir.

Vakalar tek kullanıcılı veya çok kullanıcılı olabilir. Çok kullanıcılı vakalar, birden fazla uzmanın verileri aynı anda incelemesine ve işbirliği yapmasına olanak tanır, ancak bazı ek açık kaynak sunucularının yapılandırılmasını gerektirir.

Birden fazla veri kaynağınız varsa ve bir vaka oluşturmaya karar verirken şunları göz önünde bulundurun:

Aynı anda yalnızca bir dosya açık olabilir.

Raporlar vaka bazında oluşturulmaktadır.

Aynı dosyada çok sayıda büyük veri kaynağı olduğunda uygulama yavaşlayabilir.

Dava Oluşturma

Bir vaka oluşturmak için, Karşılama ekranındaki "Yeni Vaka Oluştur" seçeneğini veya "Vaka" menüsünü kullanın. Bu, Yeni Vaka Sihirbazını başlatacaktır . Vakanın adını ve vaka sonuçlarının saklanacağı bir dizini belirtmeniz gerekecektir. İsteğe bağlı olarak vaka numaraları ve inceleyici adları da sağlayabilirsiniz.

Veri Kaynağı Ekleme

Sonraki adım, vakaya bir giriş veri kaynağı eklemektir. Veri Kaynağı Ekleme Sihirbazı, vaka oluşturulduktan sonra otomatik olarak başlayacaktır veya "Vaka" menüsünden veya araç çubuğundan manuel olarak başlatabilirsiniz. Eklenecek giriş veri kaynağının türünü (resim, yerel disk veya mantıksal dosyalar ve klasörler) seçmeniz gerekecektir. Ardından, eklenecek kaynağın konumunu belirtin.

Disk imajı için, dosya setindeki ilk dosyaya göz atın (Autopsy geri kalan dosyaları bulacaktır). Autopsy şu anda E01 ve ham (dd) dosyalarını desteklemektedir.

Yerel disk için, algılanan disklerden birini seçin. Autopsy, diskin mevcut görünümünü vakaya ekleyecektir (yani meta verilerin anlık görüntüsü). Ancak, tek tek dosya içerikleri (meta veriler değil) diskte yapılan değişikliklerle güncellenir. İsteğe bağlı olarak, yerel diskten okunan tüm verilerin bir kopyasını bir VHD dosyasına oluşturabilirsiniz; bu, önceliklendirme durumları için yararlı olabilir.

Tüm diskleri algılamak için Autopsy'yi Yönetici olarak çalıştırmanız gerekebileceğini unutmayın.

Mantıksal dosyalar (tek bir dosya veya dosya klasörü) için, sisteminizdeki bir veya daha fazla dosyayı veya klasörü vakaya eklemek üzere "Ekle" düğmesini kullanın. Klasörler özyinelemeli olarak vakaya eklenecektir.

Ardından, Veri Alma Modüllerini yapılandırmanız istenecektir.

Veri Alma Modülleri

Veri alma modülleri, veri kaynağının içeriğini analiz etmekten sorumludur ve arka planda çalışır. Veri alma modülleri, dosyaları öncelik sırasına göre analiz eder; böylece bir kullanıcının dizinindeki dosyalar, diğer klasörlerdeki dosyalardan önce analiz edilir. Veri alma modülleri üçüncü taraflarca geliştirilebilir.

Autopsy ile birlikte gelen standart veri alma modülleri şunlardır:

Son Etkinlik Modülü, web tarayıcıları ve işletim sistemi tarafından kaydedilen kullanıcı etkinliğini çıkarır. Ayrıca kayıt defteri kovanında Regripper'ı çalıştırır.

Hash Arama Modülü, NIST NSRL'den bilinen dosyaları yok saymak ve bilinen hatalı dosyaları işaretlemek için hash kümeleri kullanır. Bu işlem sırasında kullanılacak hash kümelerini eklemek ve yapılandırmak için "Gelişmiş" düğmesini kullanın. Veri alımı gerçekleşirken bilinen hatalı dosya eşleşmeleri hakkında güncellemeler alacaksınız. Daha sonra ana arayüzdeki Araçlar -> Seçenekler menüsünden hash kümeleri ekleyebilirsiniz. NIST NSRL dizinini http://sourceforge.net/projects/autopsy/files/NSRL/ adresinden indirebilirsiniz.

Dosya Türü Tanımlama Modülü, dosya türlerini imzalara göre belirler ve MIME türüne göre raporlar. Sonuçları Blackboard'a kaydeder ve birçok modül buna bağlıdır. Tika açık kaynak kütüphanesini kullanır. Araçlar, Seçenekler, Dosya Türleri bölümünden kendi özel dosya türlerinizi tanımlayabilirsiniz.

Dosya Uzantısı Uyumsuzluğu Algılama Modülü, Dosya Türü Tanımlama sonuçlarını kullanır ve dosyanın algılanan türüyle geleneksel olarak ilişkilendirilmemiş bir uzantıya sahip dosyaları işaretler. 'Bilinen' (NSRL) dosyaları yok sayar. MIME türlerini ve MIME türüne göre dosya uzantılarını Araçlar, Seçenekler, Dosya Uzantısı Uyumsuzluğu bölümünde özelleştirebilirsiniz.

Gömülü Dosya Çıkarma Modülü, ZIP, RAR, diğer arşiv formatları, Doc, Docx, PPT, PPTX, XLS ve XLSX dosyalarını açar ve bu dosyalardan elde edilen dosyaları analiz için veri alım hattına geri gönderir.

Resim Analiz Modülü, JPEG dosyalarından EXIF bilgilerini çıkarır ve sonuçları ana kullanıcı arayüzündeki ağaç yapısına yerleştirir. Ayrıca HEIC/HEIF dosyalarını JPEG formatına dönüştürür ve bu JPEG'lerden EXIF verilerini çıkarır.

Anahtar Kelime Arama Modülü, belirli kelimeleri içeren dosyaları tanımlamak için anahtar kelime listeleri kullanır. Otomatik olarak aranacak anahtar kelime listelerini seçebilir ve "Gelişmiş" düğmesini kullanarak yeni listeler oluşturabilirsiniz. Anahtar kelime aramasıyla, veri alımı tamamlandıktan sonra da arama yapabileceğinizi unutmayın. Veri alımı sırasında seçtiğiniz anahtar kelime listeleri belirli aralıklarla aranacak ve sonuçları gerçek zamanlı olarak alacaksınız. Anahtar kelime araması yapmadan önce tüm dosyaların indekslenmesini beklemenize gerek yoktur; ancak arama yaptığınızda yalnızca indekslenmiş dosyalardan sonuç alacaksınız.

E-posta Ayrıştırma Modülü, dosya imzalarına göre Thunderbird MBOX dosyalarını ve PST formatındaki dosyaları tanımlar, bunlardan e-postaları çıkarır ve sonuçları Blackboard'a ekler.

Şifreleme Algılama Modülü, şifrelenmiş dosyaları arar.

İlginç Dosyalar Tanımlayıcı Modülü, Araçlar, Seçenekler, İlginç Dosyalar bölümünde kullanıcı tarafından belirtilen kurallara göre dosya ve dizinleri arar. "Dosya Uyarı Modülü" gibi çalışır. Belirtilen dosyalar bulunduğunda gelen kutusuna mesaj gönderir.

Merkezi Depo Modülü, ilerideki ilişkilendirmeler için dosya özetlerini ve diğer çıkarılan özellikleri merkezi bir depoya ekler ve daha önce dikkat çekici olan dosyaları işaretler.

PhotoRec Carver Modülü, ayrılmamış alandan dosyaları çıkarır ve dosya işleme zincirinden geçirir.

Sanal Makine Veri Çıkarma Modülü, sanal makine dosyalarından veri çıkarır.

Veri Kaynağı Bütünlüğü Modülü, E01 dosyaları üzerinde bir sağlama toplamı hesaplar ve eşleştiğinden emin olmak için E01 dosyasının dahili sağlama toplamıyla karşılaştırır.

DJI Drone Analyzer, drone dosyalarından veri çıkarır.

Plaso, zaman çizelgesi etkinliklerioluşturmak için Plaso'yu kullanır

Android Analiz Modülü, Android cihazlardan sık karşılaşılan öğeleri ayrıştırmanıza olanak tanır. Oluşturulan verileri BlackBoard'a yerleştirir.

GPX Analyzer, .gpx dosyalarından coğrafi konum verilerini çıkarır.

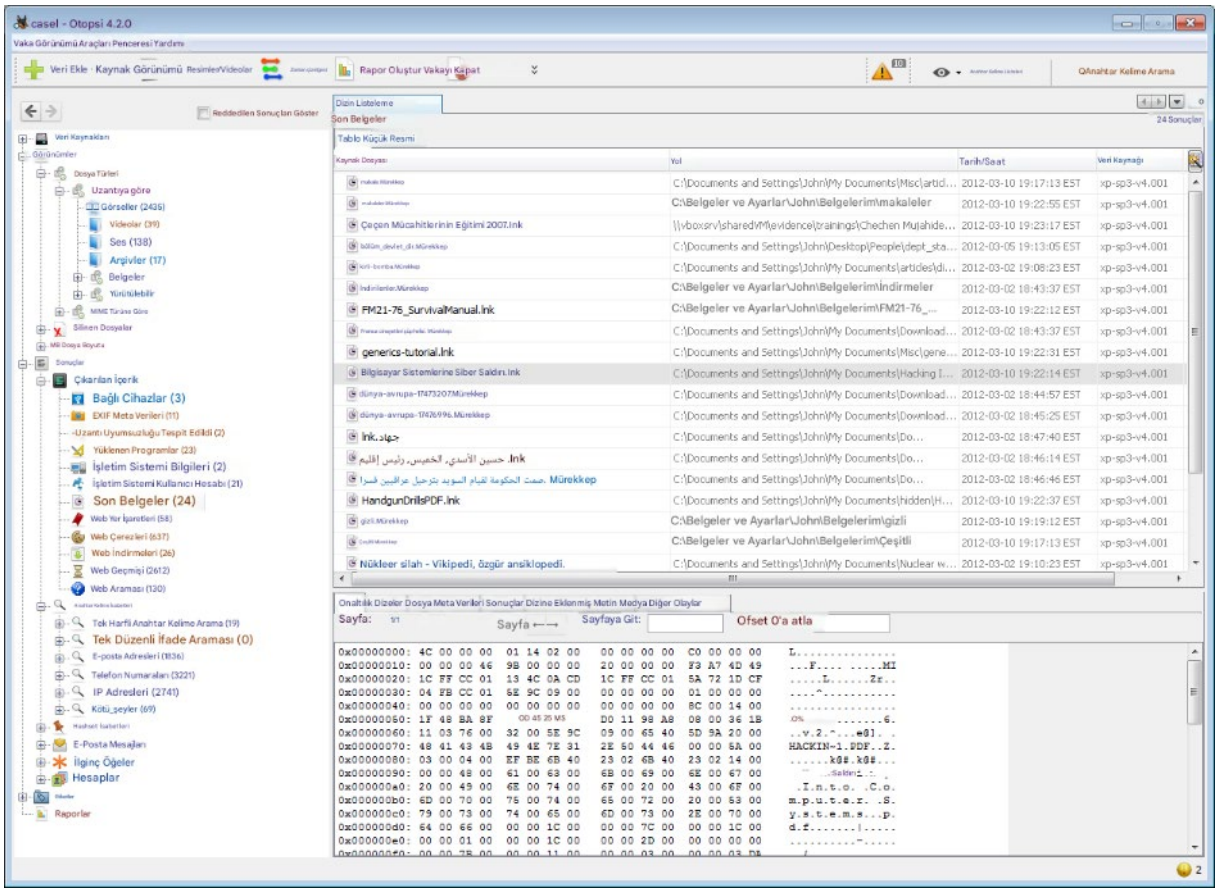
iOS Analyzer (iLEAPP), iOS veri kaynaklarından veri çıkarır.

Bir modül seçtiğinizde, ayarlarını değiştirme seçeneğiniz olacaktır. Örneğin, veri alımı sırasında hangi anahtar kelime arama listelerinin kullanılacağını ve hangi karma kümelerinin kullanılacağını yapılandırabilirsiniz. Her modülün yapılandırılmasıyla ilgili ayrıntılar için ilgili modülün yardımına bakın.

Veri alım modülleri arka planda çalışırken, sağ alt köşede bir ilerleme çubuğu göreceksiniz. Gelen sonuçları incelemek ve aynı anda veri alımı devam ederken diğer görevleri gerçekleştirmek için grafik kullanıcı arayüzünü (GUI) kullanabilirsiniz.

Analiz Temelleri

Veri alım modülleri veri kaynağını analiz etmeye başladıktan sonra, ana analiz arayüzünü göreceksiniz. Belirli öğeleri arayabilir, belirli klasörlere göz atabilir veya veri alım modülü sonuçlarını inceleyebilirsiniz.



Analiz tekniklerinizin tamamına soldaki ağaçtan başlayacaksınız.

Veri Kaynakları kök düğümü, dosyadaki tüm verileri gösterir.

Görüntüdeki tek tek düğümler, disk görüntülerinin veya yerel disklerin dosya sistemi yapısını gösterir.

LogicalFileSet düğümleri, vakadaki mantıksal dosyaları gösterir.

Görünüm düğmesi, aynı verileri dosya türüne göre düzenlenmiş gibi farklı bir bakış açısından gösterir.

Sonuçlar düğmesi, veri alma modüllerinden gelen çıktıyı gösterir.

Soldaki ağaçtan bir düğüm seçtiğinizde, sağ üstte dosya listesi gösterilecektir. Resimleri görüntülemek için sağ üstteki Küçük Resim görünümünü kullanabilirsiniz. Sağ üstten bir dosya seçtiğinizde, içeriği sağ altta gösterilecektir. Dosyanın metnini, resmini veya onaltılık verilerini görüntülemek için sağ alttaki sekmeleri kullanabilirsiniz.

Görünümler ve Sonuçlar düğümlerinden dosya görüntülüyorsanız, dosyanın dosya sistemi konumuna gitmek için dosyaya sağ tıklayabilirsiniz. Bu özellik, kullanıcının şu anda görüntülediğiniz dosya ile aynı klasörde başka neleri sakladığını görmek için kullanışlıdır. Ayrıca, dosyayı yerel sisteme çıkarmak için de dosyaya sağ tıklayabilirsiniz.

Tekil anahtar kelimelerle arama yapmak istiyorsanız, programın sağ üst köşesindeki arama kutusunu kullanabilirsiniz. Sonuçlar sağ üst köşedeki bir tabloda gösterilecektir.

Soldaki ağaç yapısında ve sağdaki tabloda, görünür bir düğümü hızlıca bulmak için kullanılabilecek bir Kullanıcı Arayüzü Hızlı Arama özelliği bulunmaktadır.

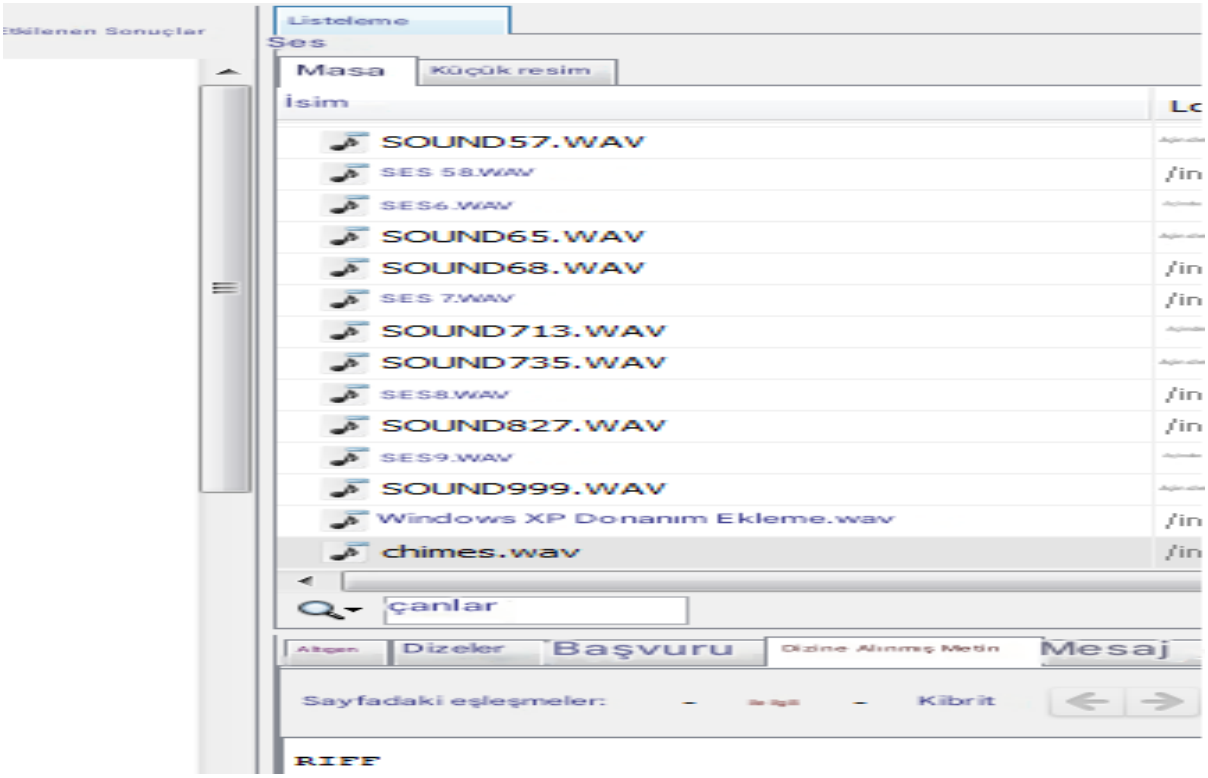
İstediğiniz dosyaları etiketleyerek (yer imi ekleyerek) daha sonra daha hızlı bulabilir veya bir rapora özellikle dahil edebilirsiniz.

Kullanıcı Arayüzü Hızlı Arama

Kullanıcı arayüzündeki hızlı arama özelliği, bir paneldeki veriler içinde belirli bir metin dizesini aramanıza olanak tanır; gizli sütunlardaki veya daraltılmış düğümlerdeki verileri aramaz.

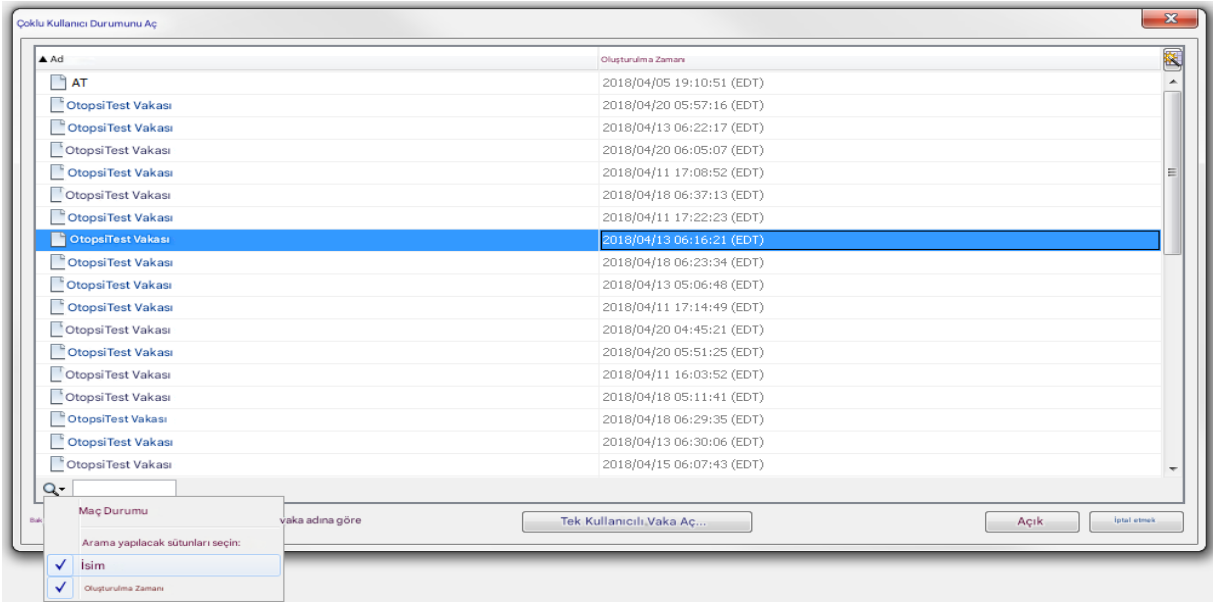
Nasıl kullanılır?

Arama özelliğini kullanmak için, arama yapmak istediğiniz alandaki herhangi bir öğeyi seçmeniz ve yazmaya başlamanız gerekir. Seçtiğiniz alanda kullanıcı arayüzü hızlı arama özelliği mevcutsa, alanın sol alt köşesinde bir arama alanı görünecektir. Aradığınız dizeyi yazdıkça, dizeyle eşleşen sonuçlardan birini seçmek için otomatik olarak güncellenecektir. Yazdığınız dizeyle eşleşen sonuçlar arasında yukarı ve aşağı ok tuşlarıyla geçiş yapabilirsiniz. Arama, normal ifadelerin kullanımını desteklemez, ancak arama yaptığı alanlardaki herhangi bir alt dizeyle eşleşir, yalnızca alanın başındaki dizeyle değil.



Yapılandırma

Varsayılan olarak, arama, şu anda seçili alanda bulunan tüm alanlardaki verilerle eşleşir. Arama ayrıca varsayılan olarak büyük/küçük harf duyarlılığını yok sayar. Bu varsayılan davranışlardan herhangi birini değiştirmek isterseniz, aşağı ok simgeli büyüteç simgesine tıklayarak hangi sütunların aranacağını ve aramanın büyük/küçük harf duyarlılığını yok sayıp saymayacağını yapılandırabilirsiniz.



Kullanılabileceği yerler

Ağaç gözlemcisi

Tablo görünümü

Açık çok kullanıcılı kasa paneli

Zaman Çizelgesi aracının tablo görünümü

İletişim Görselleştirme Aracı'nın göz atma paneli

İletişim Görselleştirme Aracı'nın mesaj paneli

Ana pencerenin sol tarafındaki ağaç yapısı, dosyadaki veri kaynaklarındaki dosyaları inceleyebileceğiniz ve otomatik analizden (veri alımı) kaydedilmiş sonuçları bulabileceğiniz yerdir. Ağaç yapısının yedi ana alanı vardır:

Kişiler / Sunucular / Veri Kaynakları: Bu, veri kaynaklarının dizin ağacı hiyerarşisini gösterir. Burada belirli bir dosyaya veya dizine gidebilirsiniz. Vakaya eklenen her veri kaynağı ayrı bir alt ağaç olarak temsil edilir. Bir veri kaynağını birden fazla kez eklerseniz, birden fazla kez görünür.

Dosya Görünümleri: Burada, veri kaynaklarından gelen belirli dosya türleri, türe veya diğer özelliklere göre gruplandırılarak gösterilir. Buradaki dosyalar birden fazla veri kaynağından gelebilir.

Veri Yapıtları: Bu, Veri Alma Modüllerinin çalıştırılmasından elde edilen sonuçların göründüğü ana yerlerden biridir .

Analiz Sonuçları: Bu, Veri Alma Modüllerinin çalıştırılmasından elde edilen sonuçların göründüğü diğer ana yerdir .

İşletim Sistemi Hesapları: Burada hem arka planda çalışan otomatik analiz (veri alımı) sonuçlarını hem de arama sonuçlarınızı görebilirsiniz.

Etiketler: Burada etiketlenmiş dosyalar ve sonuçlar gösterilir .

Raporlar: Burada sizin oluşturduğunuz veya veri alım modüllerinin oluşturduğu raporlar görünür.

Görünüm Seçenekleri aracılığıyla erişilebilen "Kişi/Ana Bilgisayara Göre Gruplandır" seçeneğini kullanarak Görünümler, Sonuçlar ve Etiketler ağaç düğümlerini ilgili kişi ve ana bilgisayarın altına taşıyabilirsiniz. Bu, çok büyük durumlarda her alt ağacın boyutunu küçültmek için faydalı olabilir.

Kişiler / Sunucular / Veri Kaynakları

Varsayılan olarak, ağaç görüntüleyicisinin en üst düğümü, dosyadaki tüm veri kaynaklarını içerecektir. Veri Kaynakları düğümü, önce sunucuya, ardından veri kaynağının kendisine göre düzenlenmiştir. Ağacın Veri Kaynakları alanındaki çeşitli düğümlere sağ tıklamak, her veri kaynağı ve içeriği için daha fazla seçenek elde etmenizi sağlayacaktır.

Veri Alma Modülleri

Veri alma modülleri, bir veri kaynağındaki verileri analiz eder. Dosyaların tüm analizini gerçekleştirir ve içeriklerini ayrıştırır. Örnekler arasında karma hesaplama ve arama , anahtar kelime araması ve web yapıtı çıkarma yer alır .

Bir vakaya veri kaynağı ekledikten hemen sonra (bkz. Veri Kaynakları), üzerinde çalışacak veri alım modüllerini yapılandırmak için bir iletişim kutusuyla karşılaşacaksınız. Yapılandırıldıktan sonra, bu modüller arka planda çalışacak ve ilgili bilgileri bulduklarında size gerçek zamanlı sonuçlar sağlayacaktır.

Bu sayfa, veri alma modüllerinin kullanımını kapsamaktadır. Belirli modüllerin yapılandırması, ilgili sayfalarda ele alınacaktır. Üçüncü taraf veri alma modüllerinin kurulumu hakkında ayrıntılı bilgi için Üçüncü Taraf Modüllerin Kurulumu sayfasına bakın.

Çoklu iş parçacıklı ve Öncelikli

Veri alma modülleri, kullanıcı içeriğini hızlı bir şekilde bulacak şekilde yapılandırılmıştır. Veri alma modülleri işlem hatları halinde gruplandırılır ve her dosya işlem hattından modül modül geçer. Bir işlem hattında modüller şu sırayla bulunabilir:

Birden fazla işlem hattı aynı anda çalışabilir. Varsayılan olarak iki işlem hattı çalışır, ancak sisteminizdeki çekirdek sayısına bağlı olarak daha fazlasını ekleyebilirsiniz. Çalıştırılacak işlem hattı sayısını "Araçlar", "Seçenekler", "Genel" alanında yapılandırabilirsiniz.

Autopsy, diğer dosya türlerine kıyasla kullanıcı içeriğine öncelik verir ve "Belgeler ve Ayarlar" veya "Kullanıcılar" klasöründeki verileri "Windows" klasöründen önce işlem hatlarına gönderir. Kullanıcı içeriğinin diğer içeriklerden önce analiz edilmesini sağlamak için sistemdeki her klasöre öncelik verir.

Veri Alma Modüllerini Çalıştırma

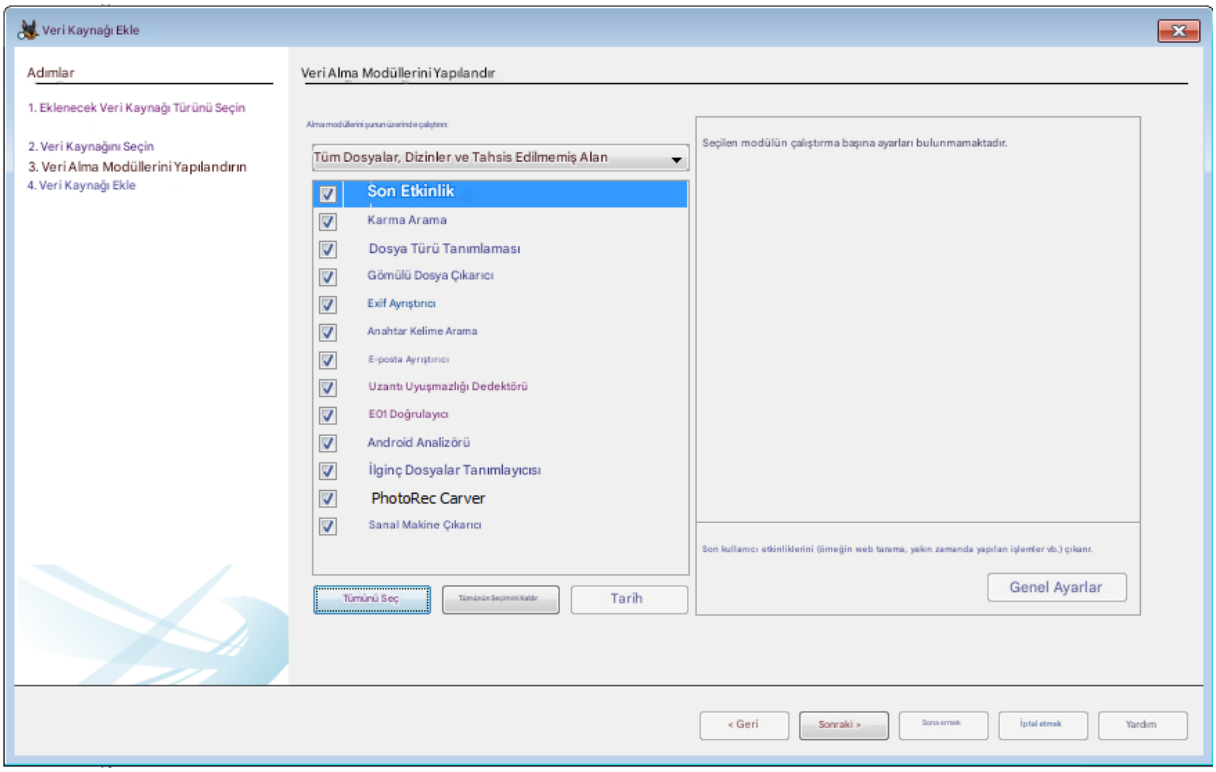
Veri alma modüllerini başlatmanın iki yolu vardır: Veri kaynağı ekledikten hemen sonra Ana arayüzdeki ağaç yapısından bir veri kaynağına sağ tıklayıp "Veri Alma Modüllerini Çalıştır" seçeneğini seçerek bunu yapabilirsiniz.

Veri alımı başlatıldıktan sonra, ana pencerenin sağ alt köşesindeki görev çubuğunda şu anda çalışan veri alım görevlerini inceleyebilirsiniz. Kullanıcı dilerse veri alım görevlerini iptal edebilir.

Not: İptal işlemi, veri alma modülünün o anda ne yaptığına bağlı olarak, bazen birkaç saniye veya daha uzun sürebilir.

Veri Alma Modüllerinin Yapılandırılması

Karşınıza veri alım modüllerini yapılandırmak için bir arayüz çıkacaktır. Buradan, analiz edilecek dosya türlerini seçebilir ve her modülü etkinleştirebilir veya devre dışı bırakabilirsiniz. Bazı modüllerin daha fazla yapılandırma ayarı olacaktır.



Üstteki seçim kutusu, veri alma modüllerinin hangi dosyalarda çalışacağını kontrol eder. İki yerleşik seçenek "Tüm dosyalar, dizinler ve ayrılmamış alan" ve "Tüm Dosyalar ve Dizinler"dir. Özel Dosya Filtreleri bölümü, özel dosya filtrelerinin nasıl oluşturulacağını açıklar. Seçilen filtre, tüm veri alma modüllerine uygulanır.

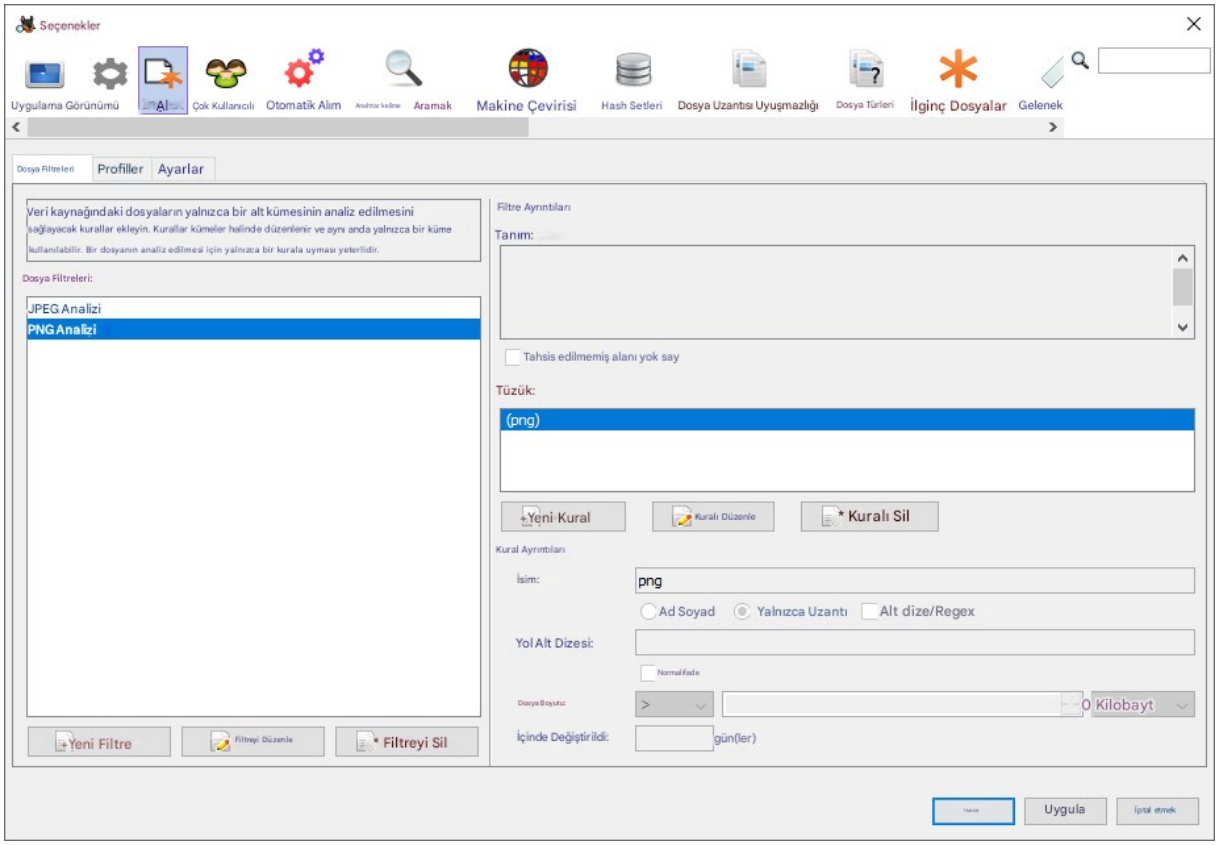
Veri alma modüllerini yapılandırmak için iki yer bulunmaktadır. Modül adını seçtiğinizde, sağdaki panelde yapılandırabileceğiniz bazı "çalışma zamanı" seçenekleri olabilir. Bunlar genellikle imajdan imaja değiştirmek isteyebileceğiniz ayarlardır.

Alt köşede etkinleştirilmiş bir "Gelişmiş" düğmesi de bulunabilir. Bu düğmeye basmak, tek bir görüntüye özgü olmayan genel ayarları değiştirmenize olanak tanır. Bu gelişmiş yapılandırma paneli genellikle "Araçlar", "Seçenekler" menüsünde de bulunur.

Örnek olarak, karma arama modülü, "çalışma zamanı" seçenekleri panelinde karma kümelerini etkinleştirmenize veya devre dışı bırakmanıza olanak tanır, ancak Autopsy yapılandırmasına karma kümeleri eklemek veya kaldırmak için "Gelişmiş" iletişim kutusuna gitmeniz gerekir.

Özel Dosya Filtreleri

Dosya filtreleri paneli, veri alma modülü seçim panelinden veya ana seçenekler panelindeki Veri Alma sekmesinden açılabilir. Dosya filtreleri, veri alma modüllerinin yalnızca dosyaların bir alt kümesi üzerinde çalıştırılmasına olanak tanır. Aşağıdaki örnekte, yalnızca "png" uzantılı dosyalar üzerinde çalışacak bir filtre ayarlanmıştır.



Her filtre, dosya adı, yolu, dosya boyutu ve dosyanın ne kadar yakın zamanda değiştirildiği gibi faktörlerin bir kombinasyonuna dayalı olarak dosya seçmek için bir veya daha fazla kural içerir. Bir dosya, bu kurallara göre belirlenen bir kural kümesiyle eşleşecektir:

Bir kural kümesinde hiç kural yoksa, hiçbir dosya bu kümeyle eşleşmez.

Eğer yalnızca dosyaları hariç tutan kurallar varsa, dosya bu hariç tutma kurallarından birine uymadığı sürece kümeye dahil edilir.

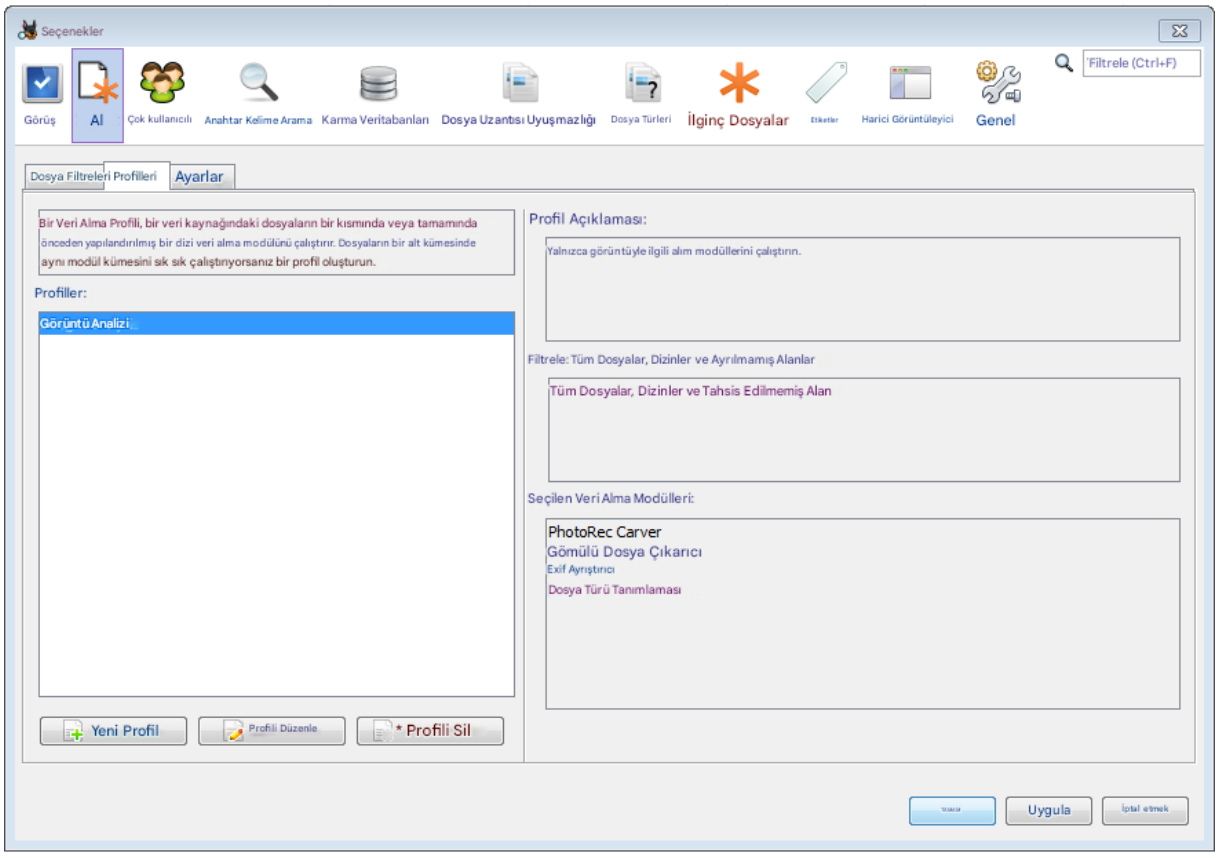
Hem kapsayıcı kurallar hem de dışlayıcı kurallar mevcutsa, bir dosyanın kümeye dahil edilebilmesi için kapsayıcı kurallardan birine uyması ve dışlayıcı kurallardan hiçbirine uymaması gerekir.

Yalnızca kapsayıcı kurallar varsa, bir dosyanın kümeye dahil edilebilmesi için kurallardan birine uyması gerekir.

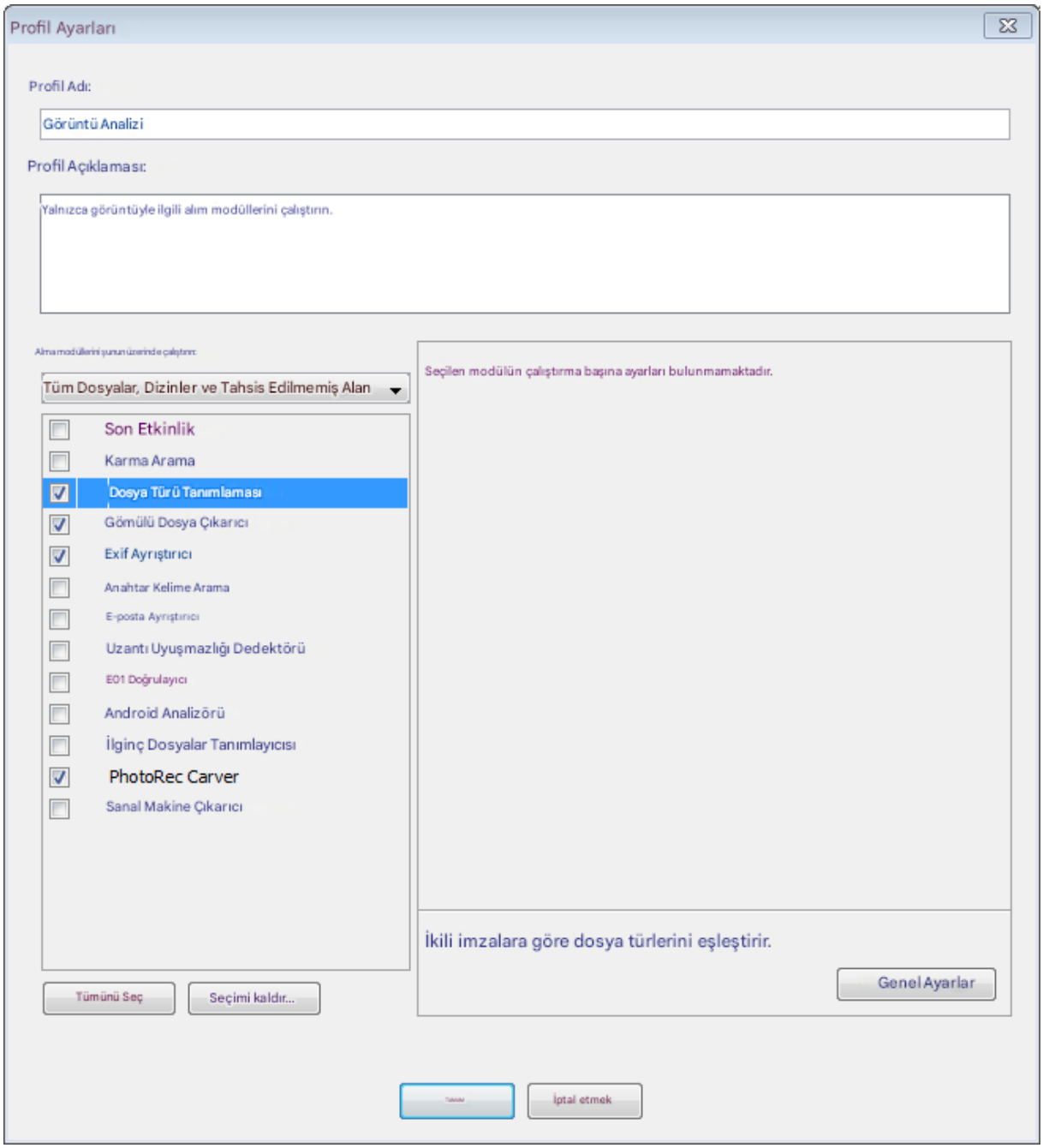
Ek olarak, virgülle ayrılmış birden fazla dosya uzantısı girebilirsiniz. Tüm dosyalar ağaç görünümünde yine de görüntülenecektir, ancak veri alma modülleri yalnızca bir alt küme üzerinde çalışacaktır. Önceki örneği kullanarak karma modülünü çalıştırırsak, yalnızca .png ile biten dosyaların karma değeri hesaplanacaktır.

Veri Alma Profillerini Kullanma

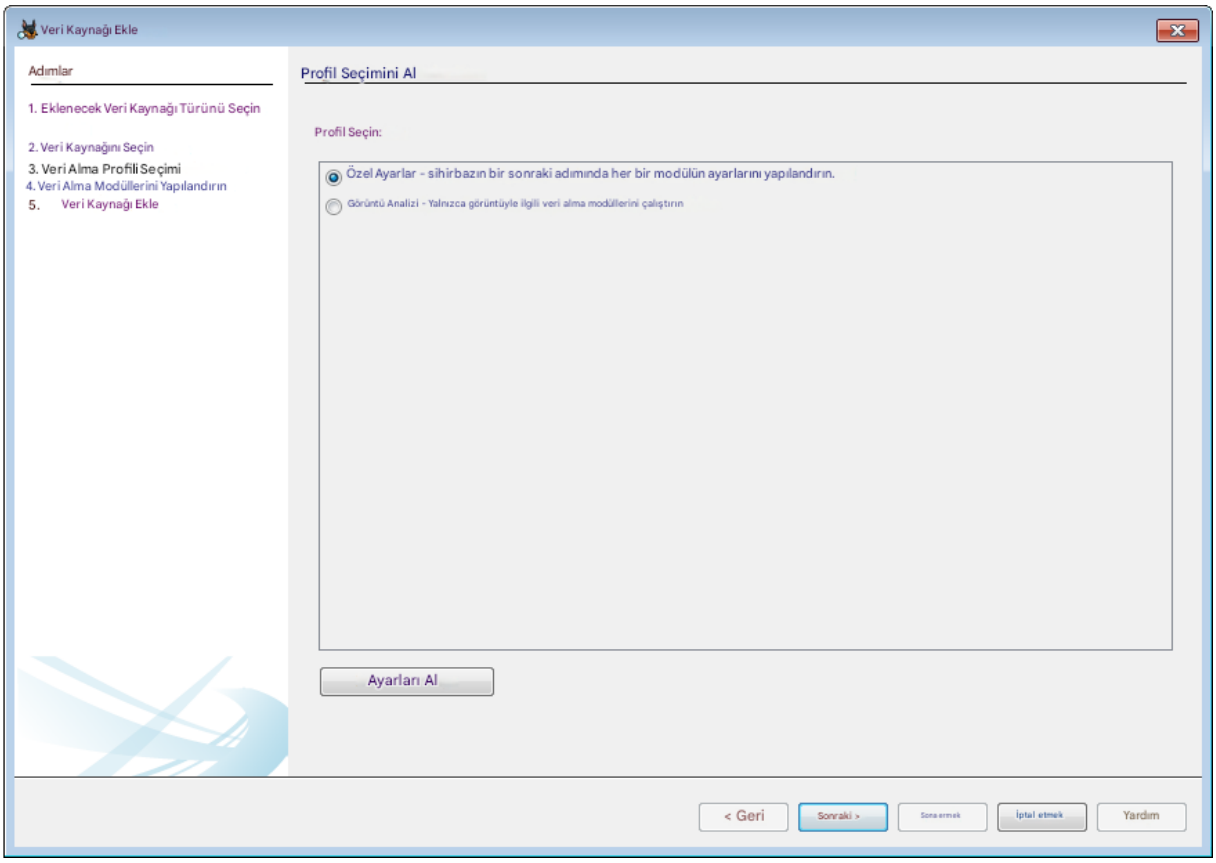
Veri alım profilleri, çalıştırılacak tanımlı bir veri alım modülü kümesini hızlıca seçmenize olanak tanır. Bu, farklı veri türlerinde farklı veri alım modülü kümeleri (veya bu veri alım modüllerinin farklı yapılandırmaları) çalıştırıyorsanız faydalı olabilir. Veri alım profilleri, seçenekler panelindeki Veri Alım sekmesi aracılığıyla yapılandırılabilir.



Her profil, her bir veri alma modülü için farklı çalıştırma ayarları belirtebilir ve önceden tanımlanmış veya özel bir dosya filtresi kullanmayı seçebilirsiniz (bkz. Özel Dosya Filtreleri).



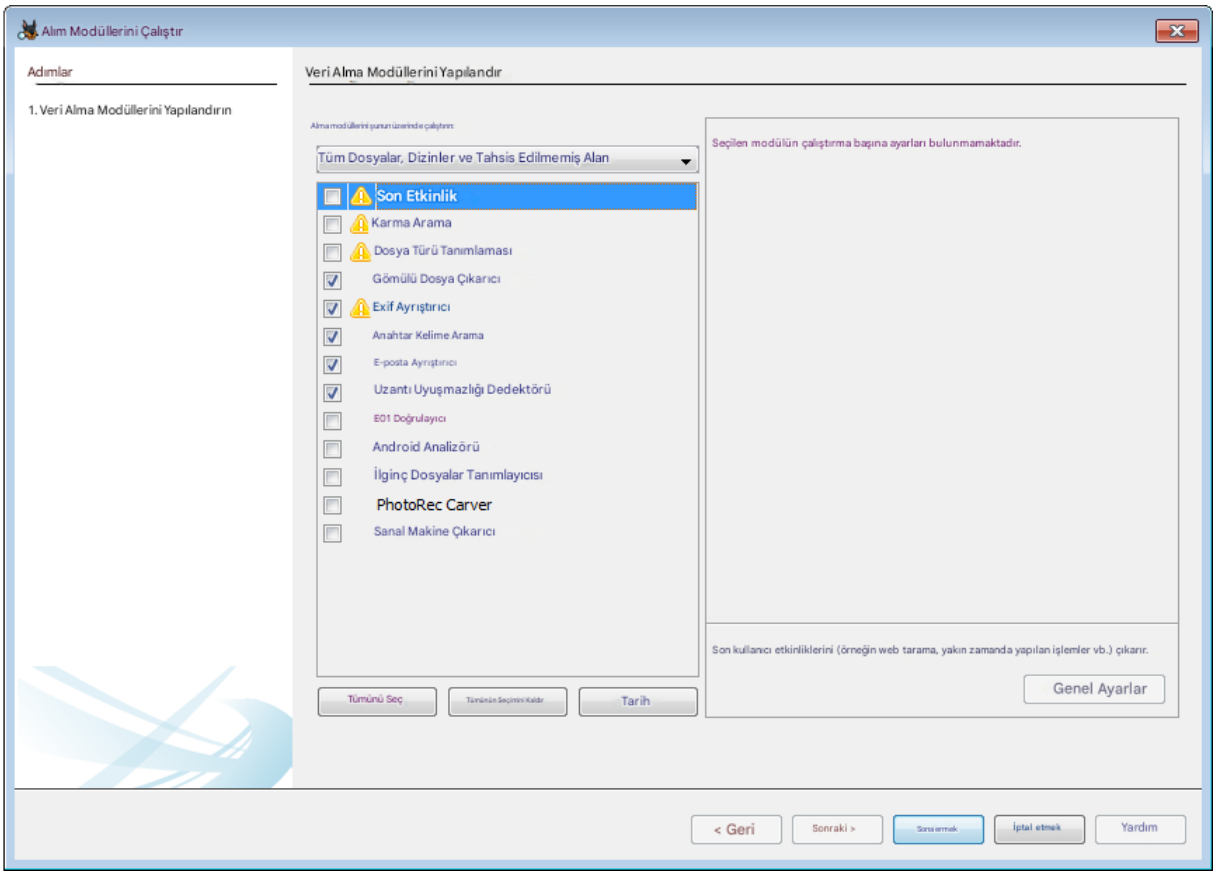
Eğer özel profiller mevcutsa, veri kaynağı ekleme sihirbazında yeni bir ekran açılacaktır.



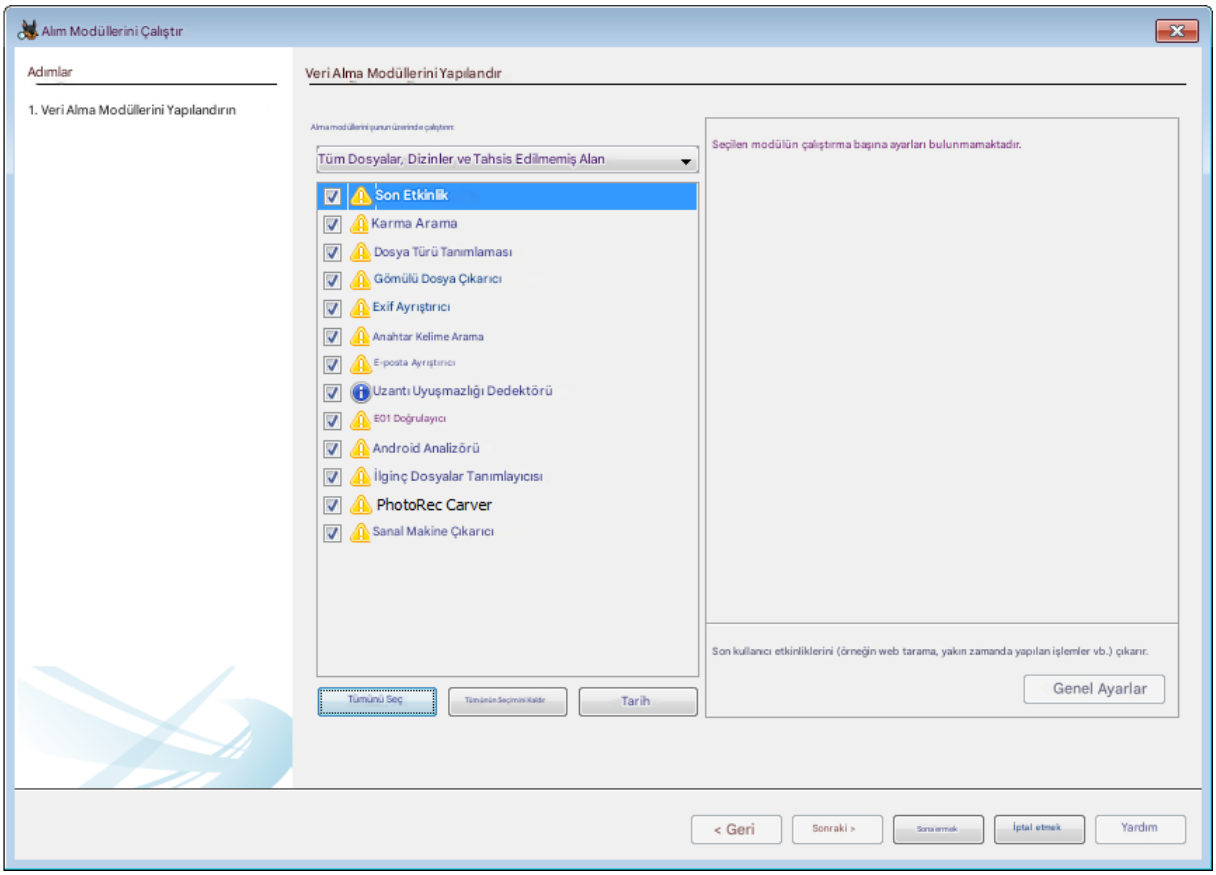
Özel ayarları seçerseniz, normal veri alma modülü seçim paneli açılacaktır. Kullanıcı tanımlı bir profil seçerseniz, veri alma modülü ekranı tamamen atlanacak ve o profildeki veri alma modülleri veri kaynağında çalıştırılacaktır. Profil seçim paneli, ağaçtan bir veri kaynağına sağ tıklayarak veri alma işlemi çalıştırıldığında da görünecektir.

Veri alımının zaten tamamlandığı bildirimi

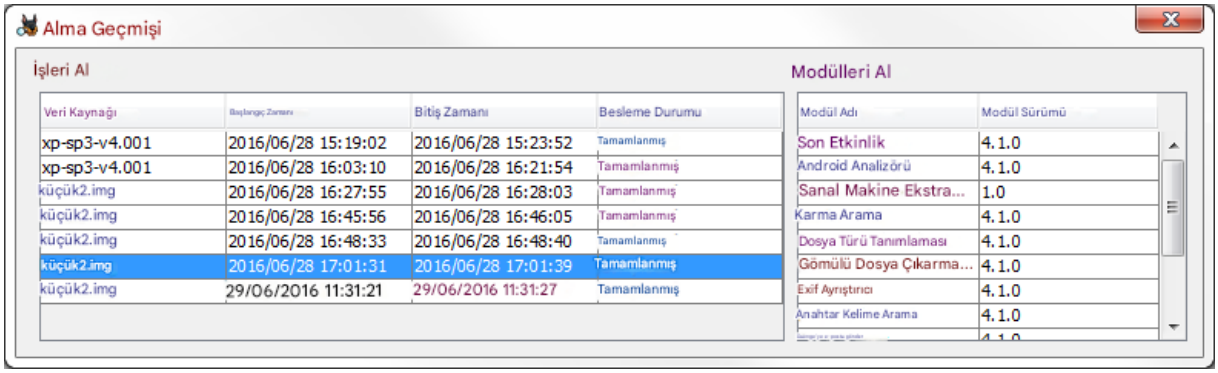
Belirli bir veri kaynağı için bir veri alma modülü daha önce çalıştırılmışsa, aşağıdaki ekran görüntüsünde gösterildiği gibi, "Veri Alma Modüllerini Çalıştır" iletişim kutusunda modülün yanında ünlem işareti bulunan üçgen şeklinde sarı bir simge göreceksiniz.



Belirli bir veri kaynağı için daha eski bir sürümde veri alma modülü çalıştırılmışsa, aşağıdaki ekran görüntüsünde gösterildiği gibi, "Veri Alma Modüllerini Çalıştır" iletişim kutusunda modülün yanında "i" harfi bulunan yuvarlak mavi bir simge göreceksiniz.



"Veri Alım Geçmişini Görüntüle" seçeneğine tıkladığınızda, veri alım geçmişi tablo şeklinde görüntülenecek ve aşağıdaki ekran görüntüsünde gösterildiği gibi hangi modüllerin hangi veri kaynaklarında ne zaman çalıştırıldığını görebileceksiniz.



Veri Alma Modülü Sonuçlarını Görüntüleme

Veri alma modülleri arka planda çalışır. Bir veri alma modülü size çeşitli şekillerde sonuç sağlayabilir, ancak biz belirli yöntemleri öneriyoruz:

Sonuçları Blackboard'a yüklerlerse, bunları ana arayüzdeki ağaç yapısının "Sonuçlar" alanında bulabilirsiniz.

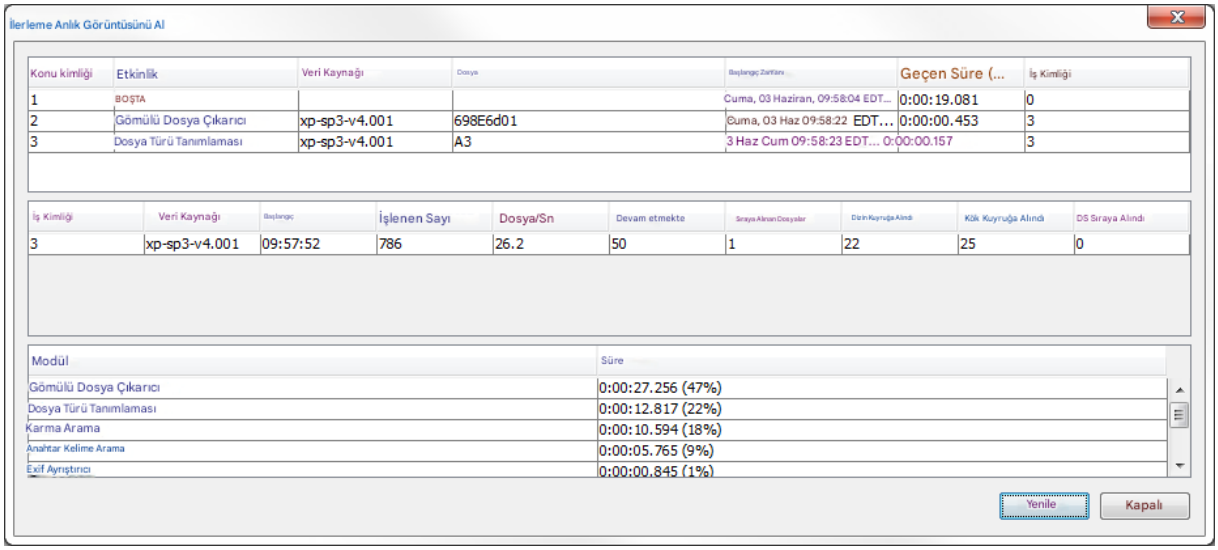
Önemli bir şey bulunduğunda size her seferinde bir mesaj gönderebilmeleri için, gelen kutusuna bir mesaj gönderebilirler.

Eğer modül başka bir adli bilişim aracının etrafını saran bir sarmalayıcı ise, o aracın çıktısına bir bağlantı sağlayabilirler; bu durumda ağacın "Raporlar" alanında yeni bir giriş göreceksiniz.

Autopsy'nin tüm resmi modülleri sonuçları kara tahtaya gönderir, ancak üçüncü taraf uygulamalar yüklerseniz, bunlar herhangi bir yaklaşımı seçebilirler; buna, bir şey bulduklarında her seferinde bir açılır pencere göstermek de dahildir.

Devam Eden Veri Alma Etkinliğini Görüntüleme

Veri alımı çalışırken, o anki etkinlikleri görmek için "Veri Alımı İlerleme Anlık Görüntüsü" aracını kullanabilirsiniz. Aşağıdaki ekran görüntüsünde gösterilen iletişim kutusunu görüntülemek için "Yardım", "Veri Alımı İlerleme Anlık Görüntüsü Al" seçeneklerine tıklayın.



Görünümü yenilemek için "Yenile" düğmesini kullanın.

Etiketleme ve Yorum Yapma

Etiketleme (veya Yer İşareti Ekleme), bir dosyaya veya nesneye referans oluşturmanıza ve daha sonra kolayca bulmanıza veya bir rapora dahil etmenize olanak tanır. Etiketleme ayrıca merkezi depoda öğeleri önemli olarak işaretlemek için de kullanılır . Etiketleri kullanarak veya merkezi depo aracılığıyla dosyalara ve sonuçlara yorum ekleyebilirsiniz.

Etiketleme öğeleri

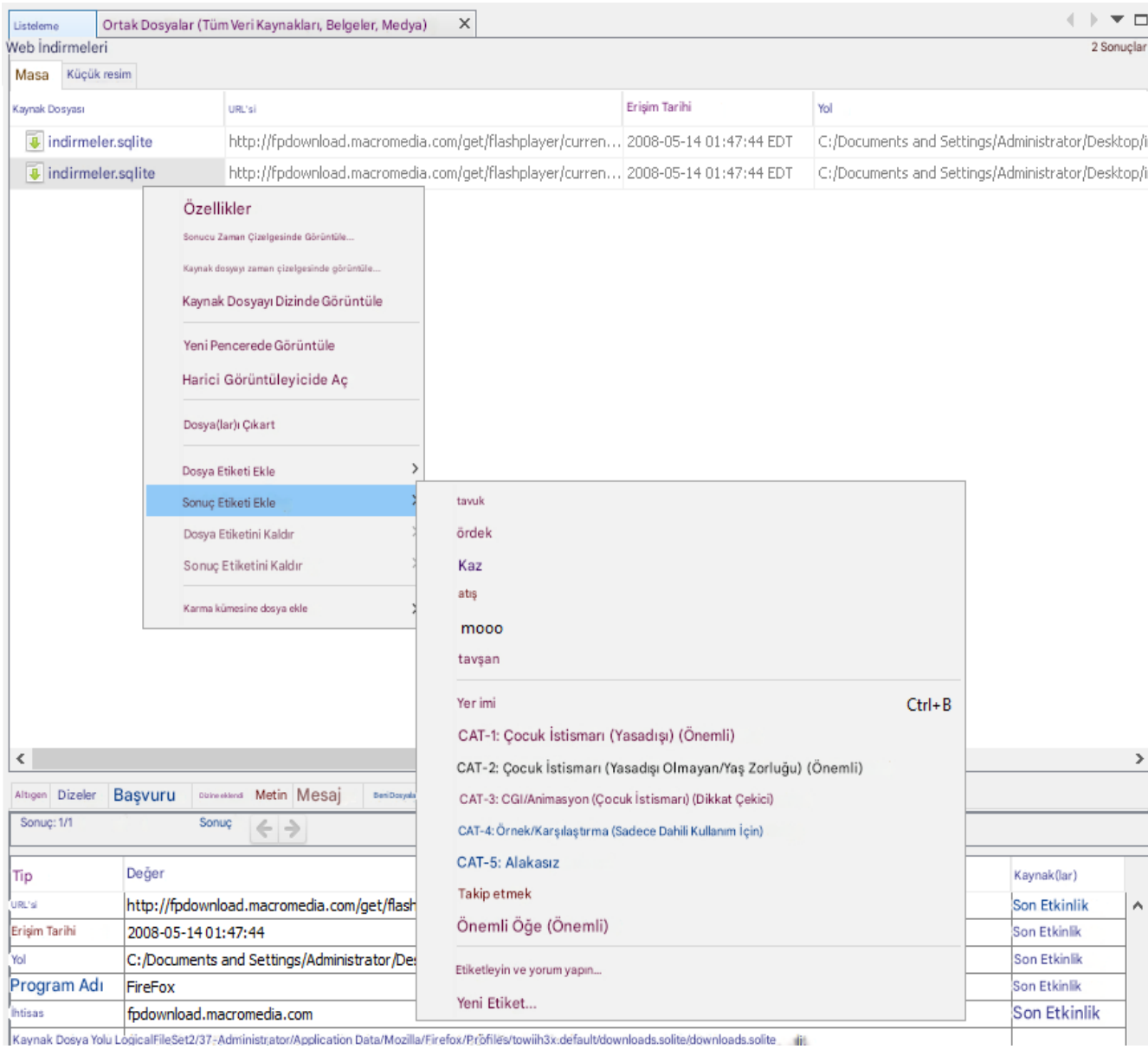
İlginç bir öğe keşfedildiğinde, kullanıcı öğeye sağ tıklayıp etiket seçeneklerinden birini seçerek onu etiketleyebilir.

Blackboard çıktısına etiket eklerken şu seçeneklerden birini tercih edebilirsiniz:

Etiket Dosyası – dosyanın kendisi ilgi çekici olduğunda bunu kullanın.

Etiket Sonucu – sonuç ilginizi çektiğinde bunu kullanın.

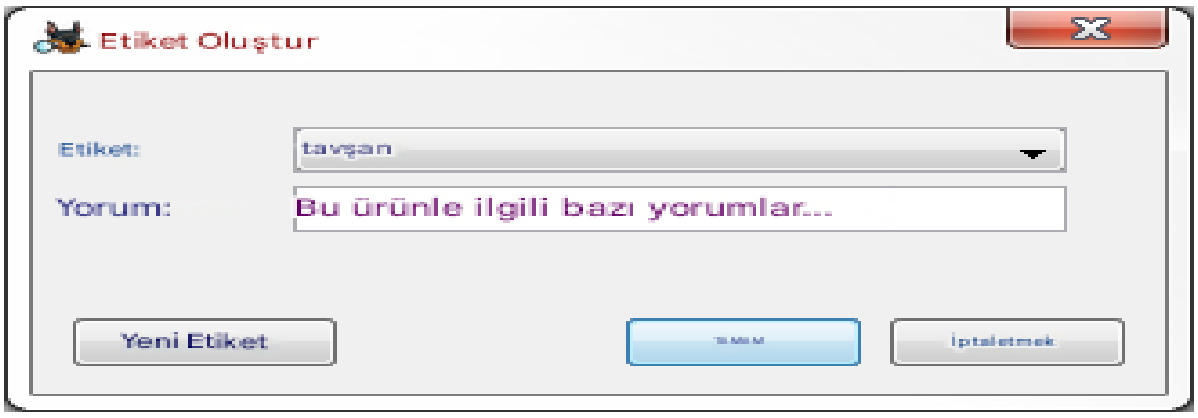
Hangi yöntemi seçeceğiniz, bağlama ve nihai raporda ne istediğinize bağlıdır.



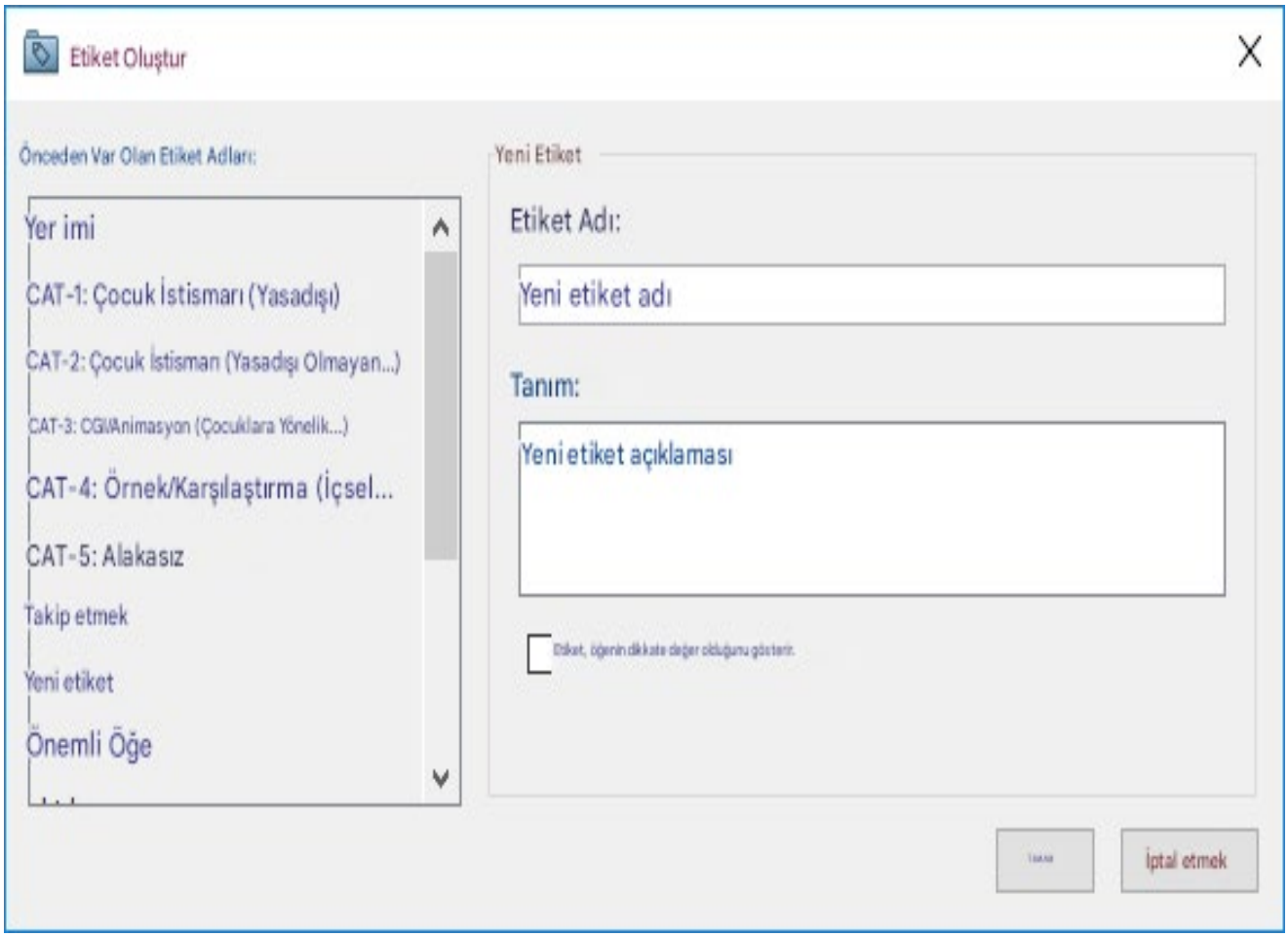
Bu noktada üç seçenek mevcut:

Mevcut etiketlerden birini kullanarak, yorum eklemeden dosyaya/sonuca ekleyin.

Etiket ve Yorum – bu etiketle ilgili bir yorum eklemeniz gerekiyorsa bunu kullanın.



Yeni etiket – Yeni bir etiket oluşturun ve dosyaya/sonuca ekleyin.



Birkaç varsayılan etiket adı vardır:

Yer imi - İlgi çekici dosyaları işaretlemek için varsayılan etiket

CAT-1'den CAT-5'e kadar - Kolluk kuvvetleri kullanımı için

Takip Et - Takip edilecek dosyaları işaretlemek için kullanılan varsayılan etiket.

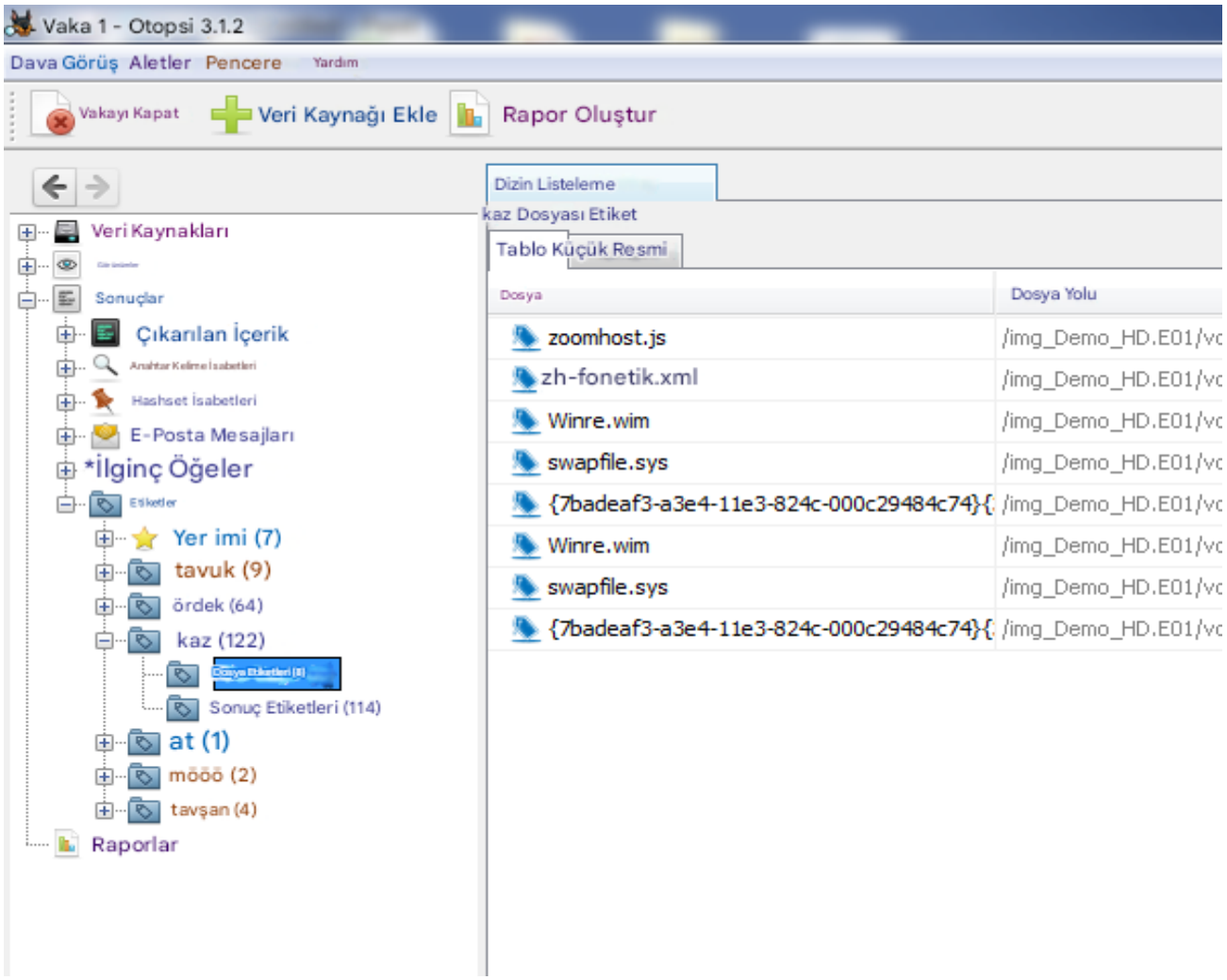
Önemli öğe - Merkezi depoda bir öğenin önemli olarak işaretlenmesi gerektiğini belirtmek için kullanılan varsayılan etiket.

Ayrıca özel etiket adları da oluşturabilirsiniz. Bu etiket adları otomatik olarak kaydedilecek ve ileride kullanılmak üzere varsayılan etiket adlarının üstünde görüntülenecektir.

Öğeyi varsayılan "Yer İşareti" etiketiyle etiketlemek istiyorsanız, menülerden geçmek yerine Ctrl+B klavye kısayolunu da kullanabilirsiniz.

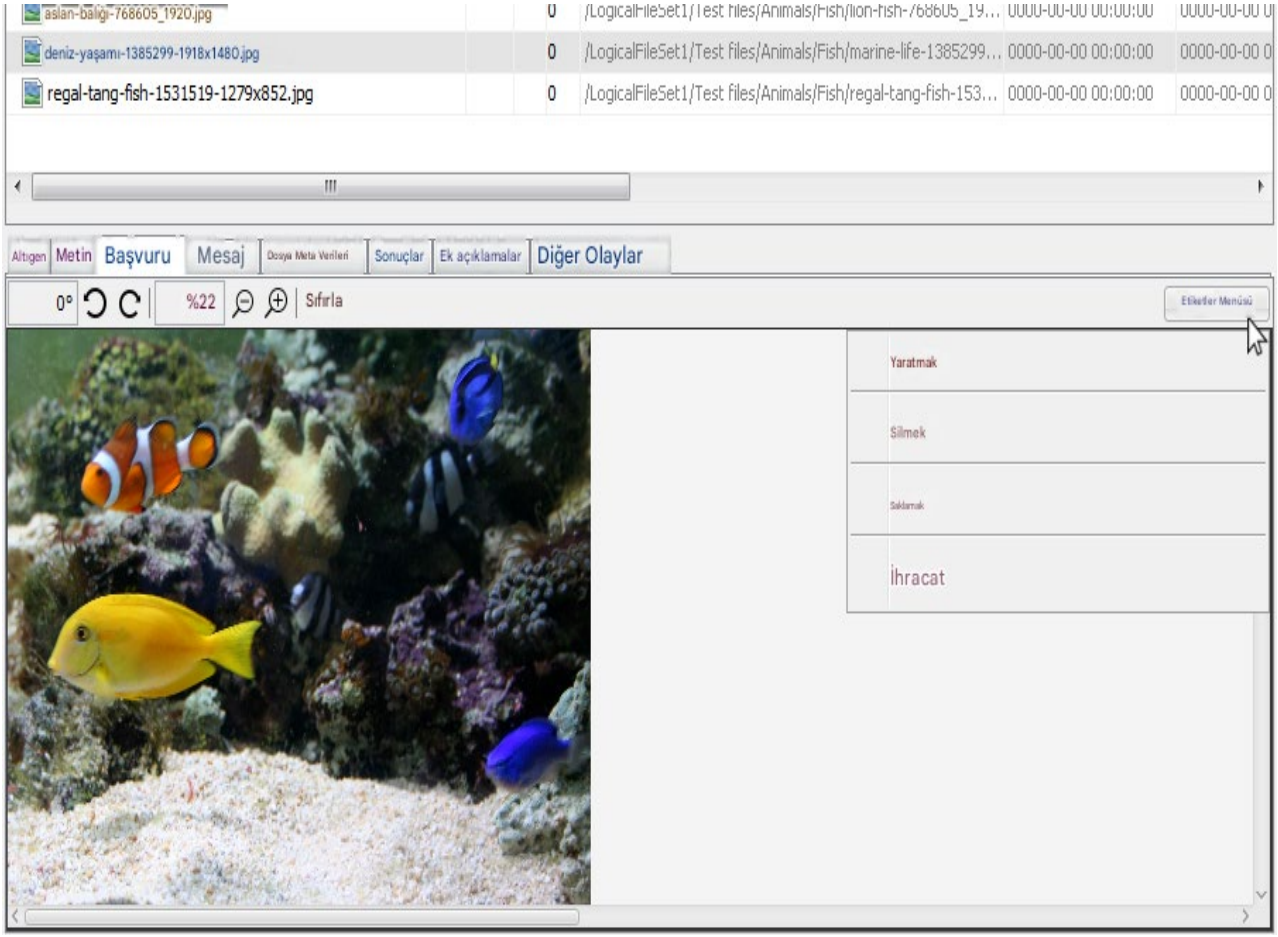
Ayrıca, öğe gruplarına aynı anda etiket uygulayabilirsiniz. Blackboard'ta birden fazla öğe seçin, sağ tıklayın ve uygun etiketi ekleyin. Öğeler birden fazla etikete sahip olabilir.

Etiketlenmiş sonuçlar, ağacın "Sonuçlar" bölümünde "Etiketler" altında gösterilir. Etiketlenmiş öğeler ayrıca Sonuç Görüntüleyici'de de vurgulanır.



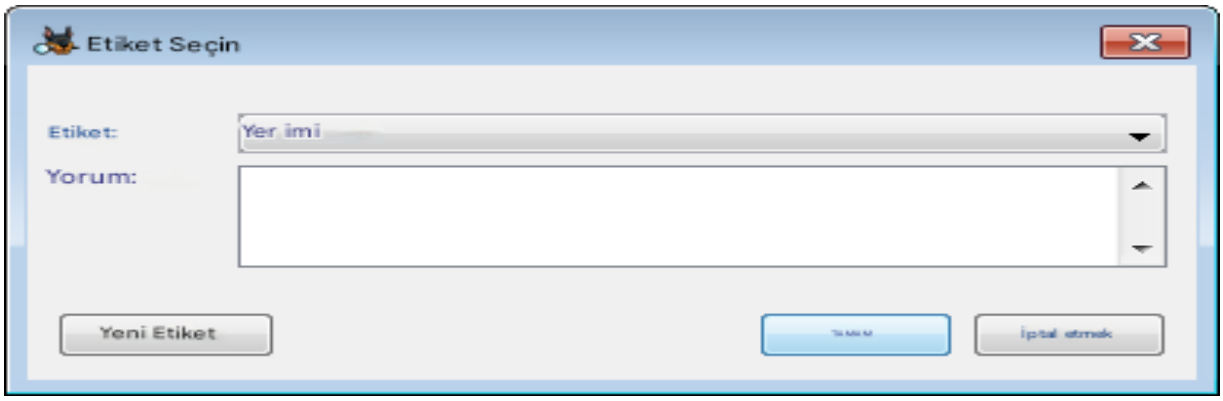
Görüntü etiketleme

Sonuç Görüntüleyici'de bir resim seçtiğinizde , "Uygulama" İçerik Görüntüleyici'nin sağ üst köşesinde "Etiketler Menüsü" seçeneğini göreceksiniz . Bu, resmin yalnızca seçili bir alanını etiketlemenizi sağlar. Resim etiketleme şu anda yalnızca Windows'ta etkinleştirilmiştir.

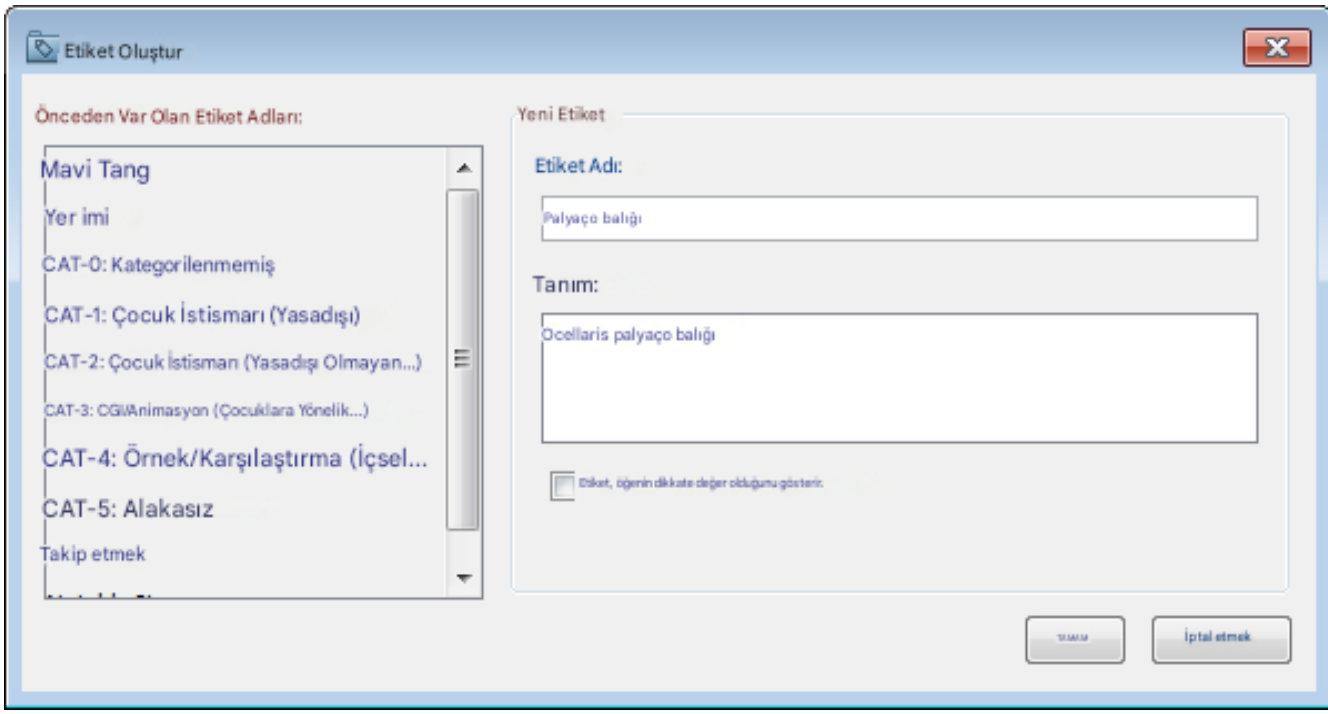


Resim etiketi oluşturma

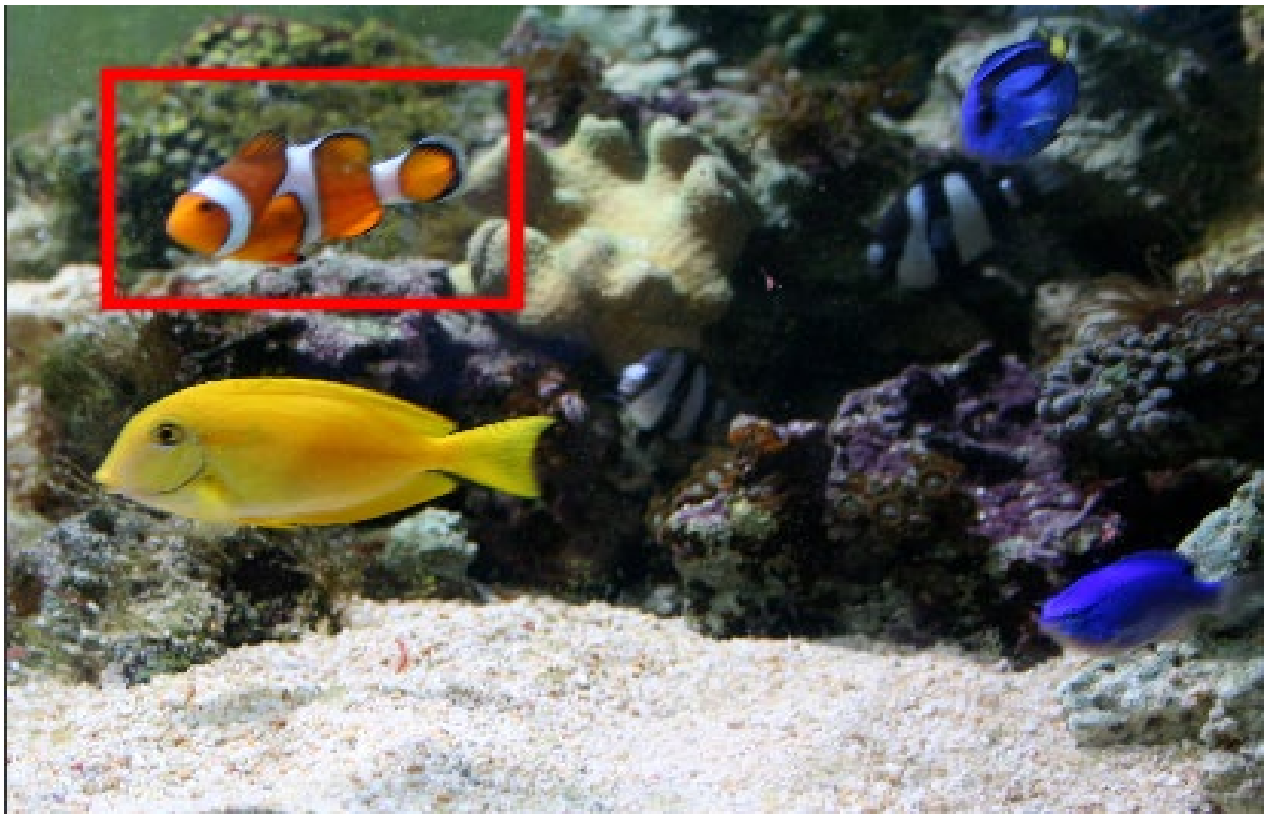
Başlamak için, etiketler menüsünden "Oluştur" seçeneğini seçin. Ardından, bir dikdörtgen oluşturmak için (bu sizin 'etiketiniz' olacaktır) resme sol tıklayıp sürükleyebilirsiniz. Fareyi bıraktığınızda, resim etiketinize bir etiket adı (ve isteğe bağlı olarak bir yorum) uygulayabileceksiniz.



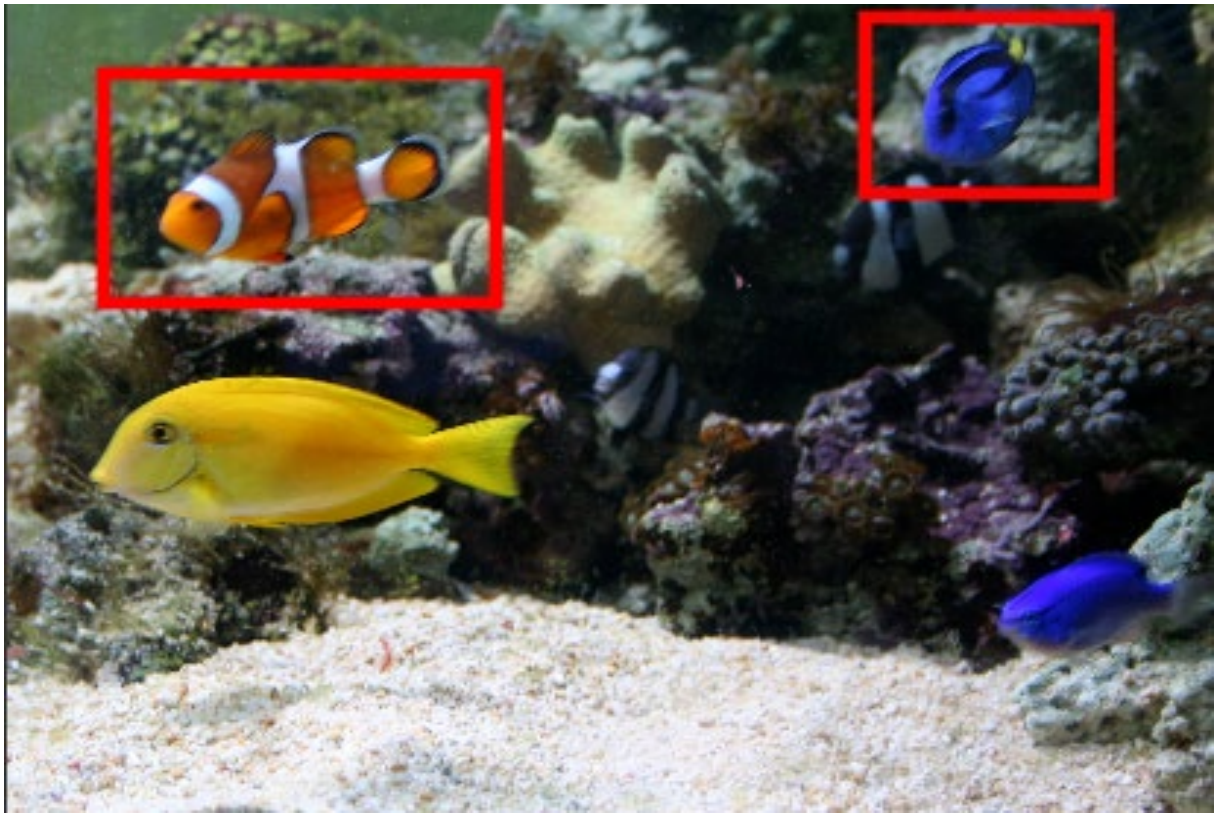
"Yeni Etiket" düğmesini kullanarak yeni bir etiket adı ekleyebilirsiniz.



Etiket adını seçtikten sonra, seçtiğiniz bölümün etrafında resimde kırmızı bir çerçeve göreceksiniz.



Aynı görselde birden fazla etiket oluşturabilirsiniz.

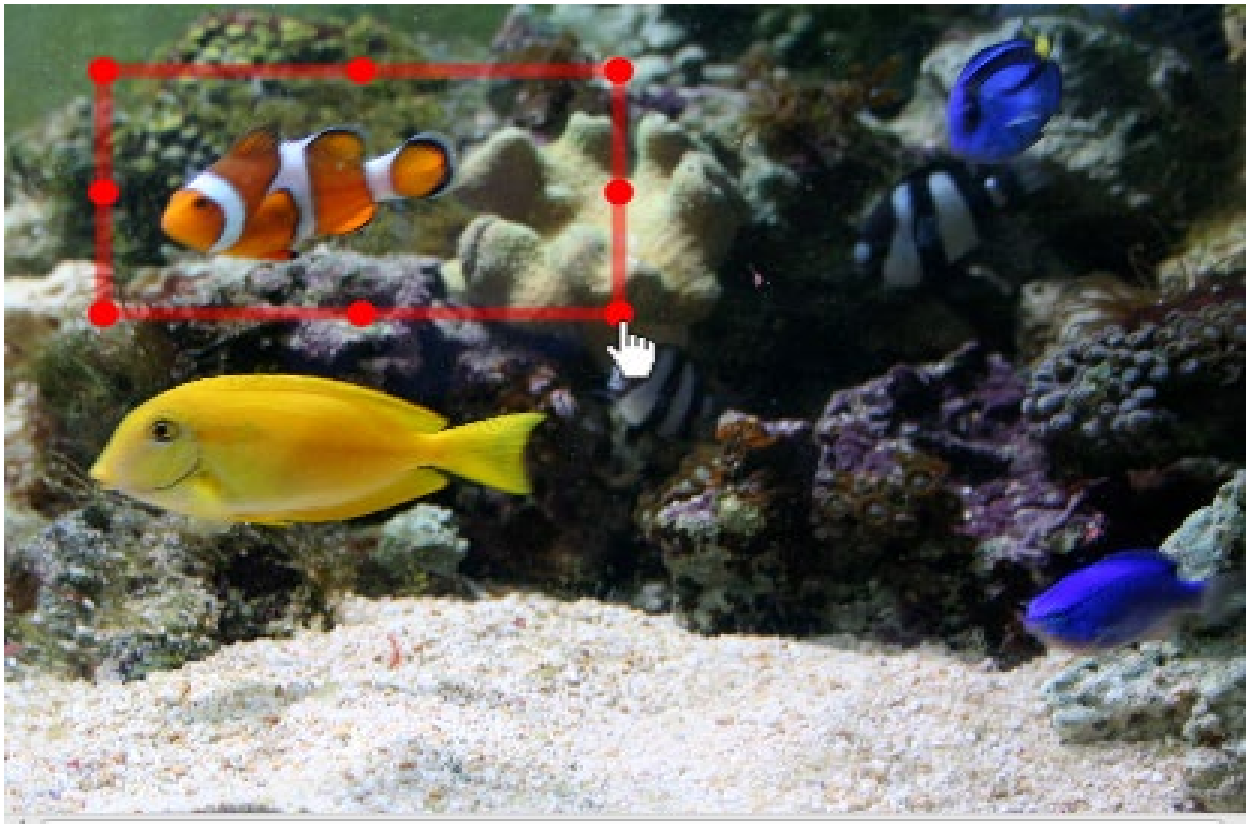


Etiket çerçevelerini geçici olarak gizlemek istiyorsanız, etiketler menüsünden "Gizle"yi seçin. Ardından tekrar görmek için "Göster"i seçebilirsiniz. Sonuç

Görüntüleyici'de farklı bir öğeye geçip geri döndüğünüzde de çerçeveler yeniden görünecektir.

Görüntü etiketini seçme, yeniden boyutlandırma ve silme

Bir resim etiketini yeniden boyutlandırmak veya silmek için öncelikle onu seçmeniz gerekir. Bunu, resim etiketinin içinde (veya üzerinde) herhangi bir yere sol tıklayarak yapabilirsiniz. Seçili etiketler, görünen 8 tutamaçtan herhangi birini sürükleyerek yeniden boyutlandırılabilir. Fare bırakıldığında yeniden boyutlandırılmış boyutlar otomatik olarak kaydedilir.

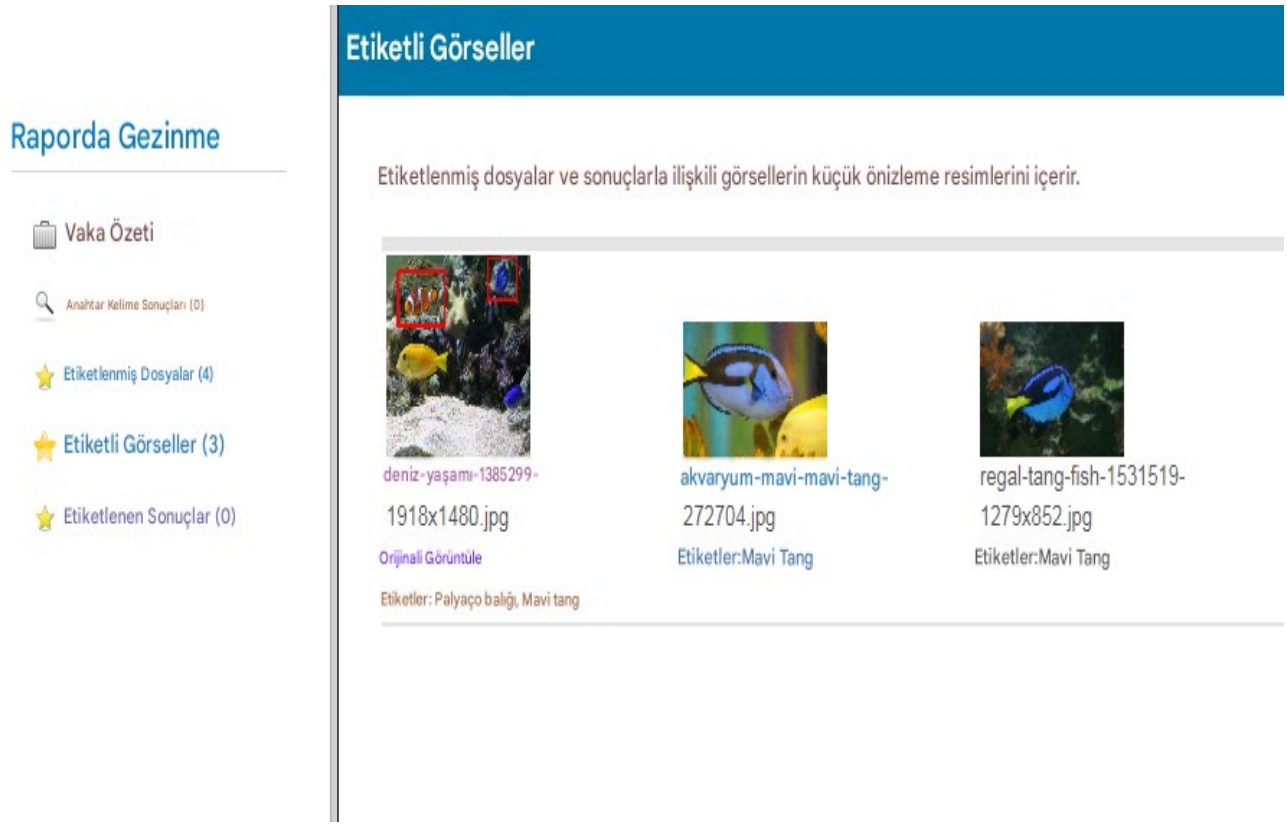


Bir etiketi seçmek, etiketler menüsünde "Sil" seçeneğini de etkinleştirecektir. Etiket silme işlemi geri alınamaz bir işlemdir, bu nedenle lütfen dikkatli olun.

Görüntü etiketlerinin dışa aktarılması ve raporlanması

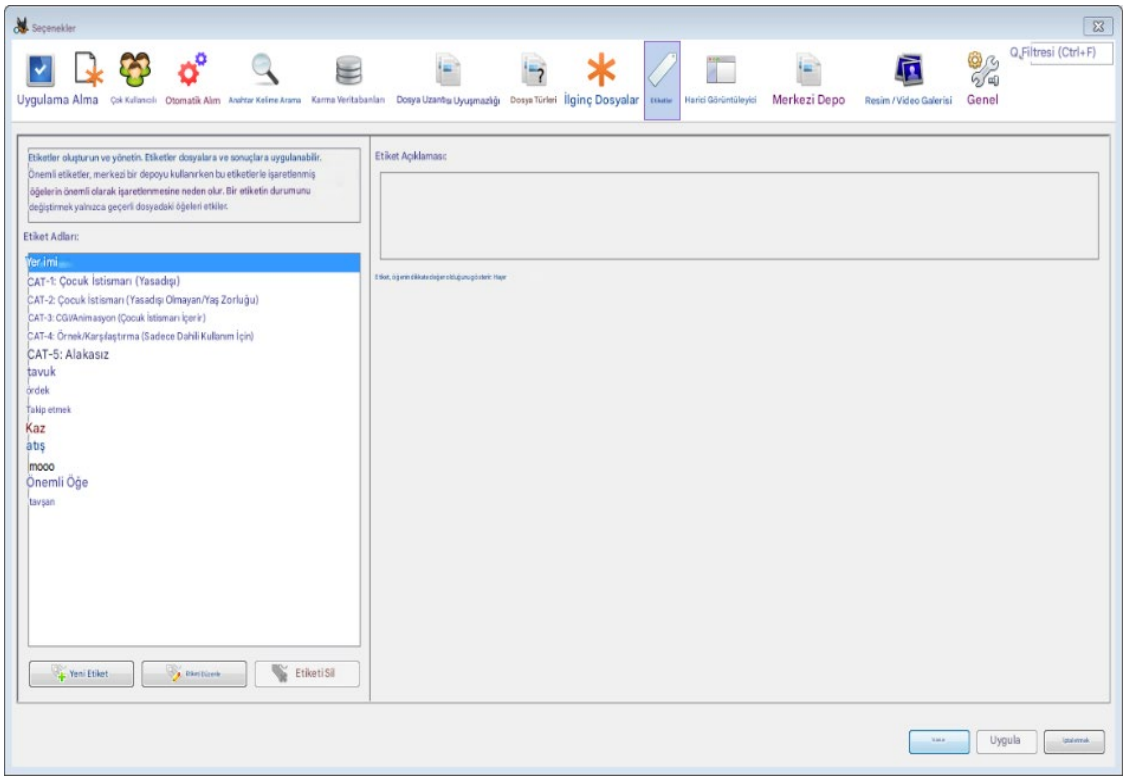
Etiket ana hatlarıyla birlikte görüntüyü kaydetmek istiyorsanız, etiketler menüsünden "Dışa Aktar"ı seçin. Sonuç her zaman bir PNG dosyası olacaktır. Sonuç Görüntüleyici'de sağ tıklama menüsünden "Dosyaları Çıkar" seçeneğini kullanmanın orijinal görüntüyü dışa aktaracağını unutmayın.

Ayrıca HTML raporunda resim etiketlerini de görebileceksiniz .

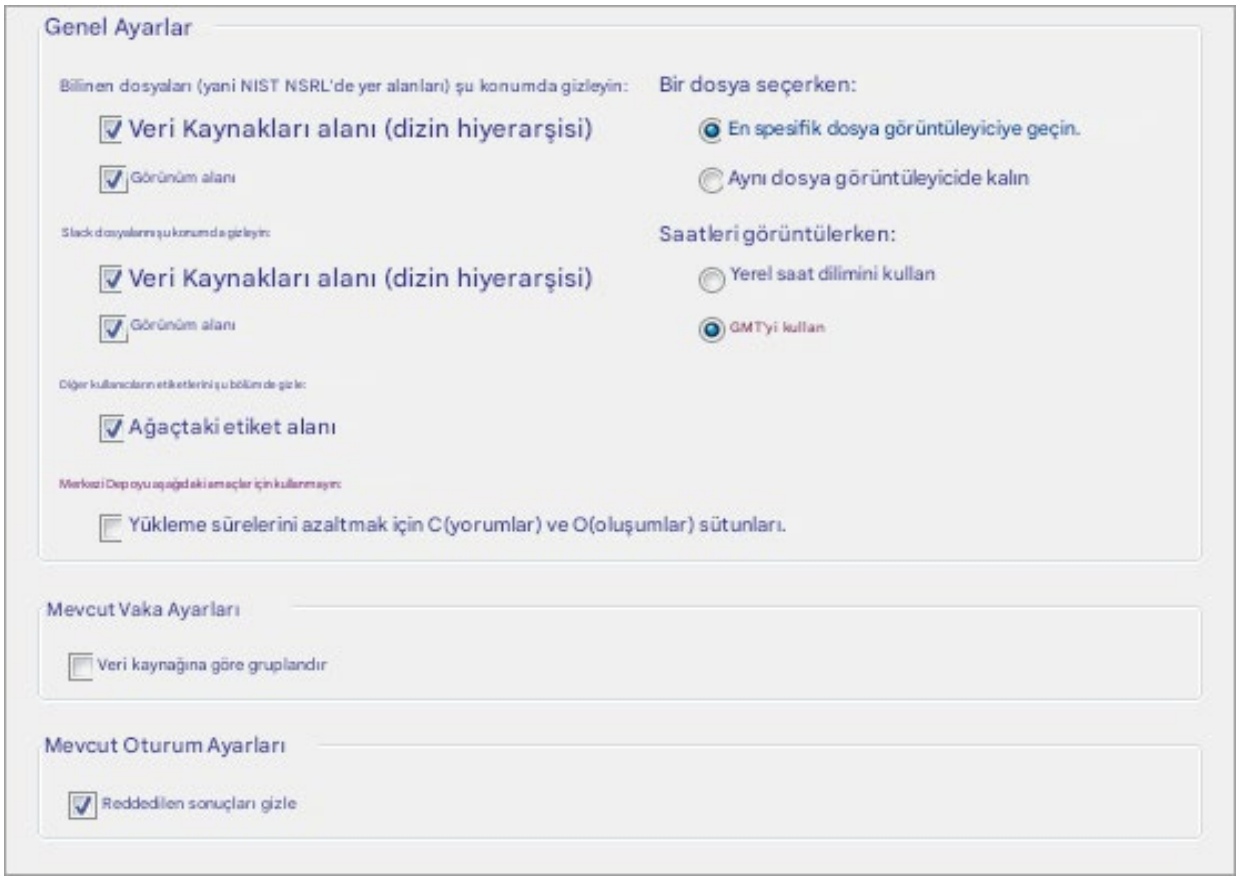


Etiketleri yönetmek

Etiket listesi, Seçenekler menüsündeki Etiketler sekmesi aracılığıyla düzenlenebilir.

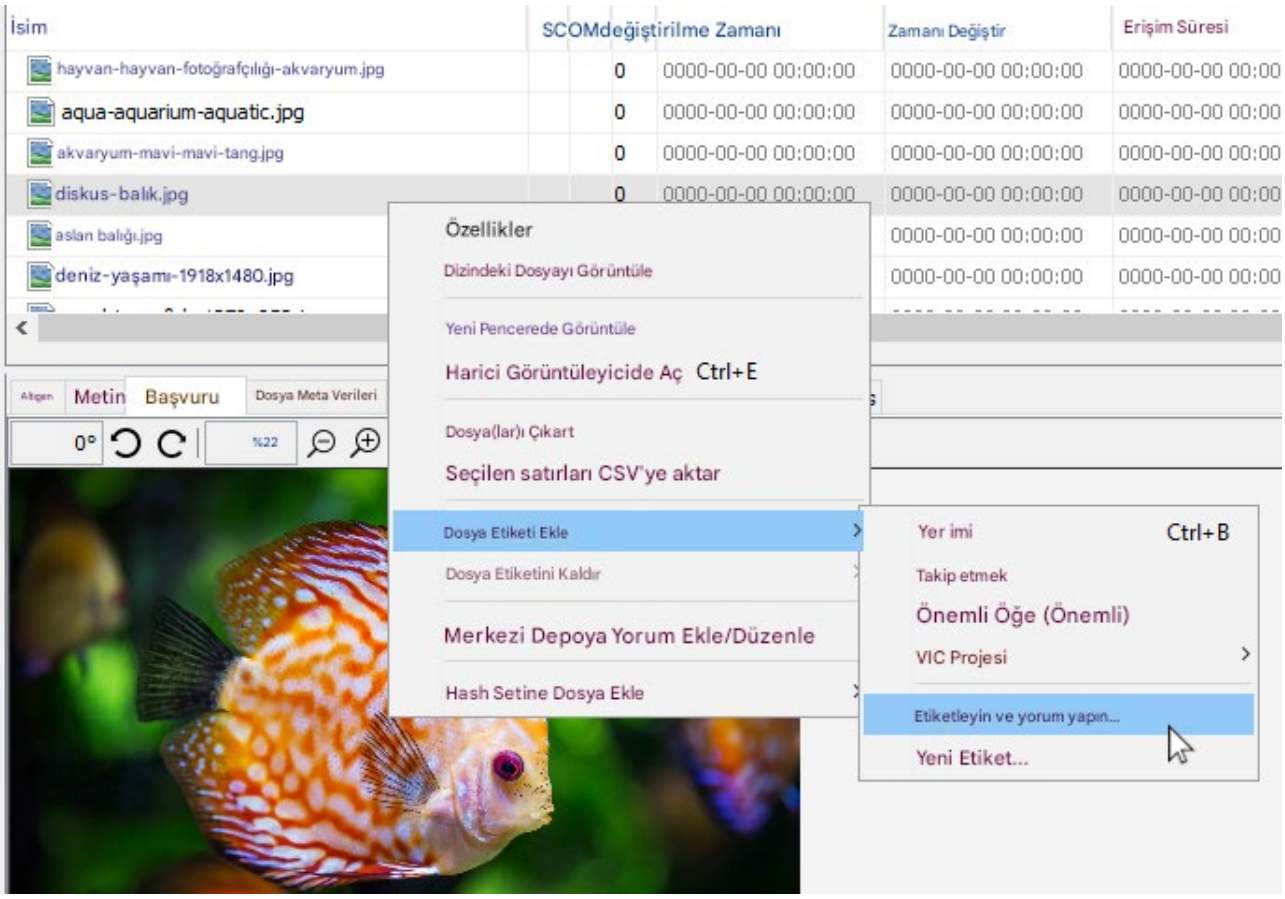


Diğer kullanıcılar tarafından etiketlenmiş tüm etiketli dosyaları ve sonuçları, dizin ağacının "Etiketler" alanında gizlemek mümkündür. Bunun için, dizin ağacının üzerindeki dişli simgesinden veya Araçlar->Seçenekler menüsünden Görünüm Seçenekleri menüsünü açın ve ardından diğer kullanıcıların etiketlerini ağacın etiketler alanında gizlemek için onay kutusunu işaretleyin.



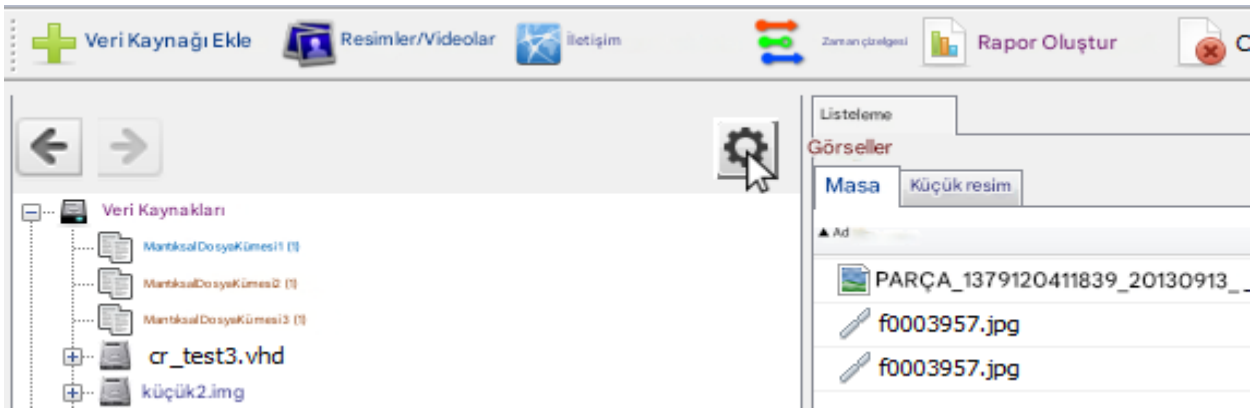
Yorum yapma

Dosyalara ve sonuçlara yorum eklemenin iki yöntemi vardır. İlk yöntem, " Öğeleri Etiketleme " bölümünde ele alınmıştır. İlgilendiğiniz dosyaya veya sonuca sağ tıklayın, "Dosya Etiketi Ekle" veya "Sonuç Etiketi Ekle" ve ardından "Etiketle ve Yorumla" seçeneklerini seçin. Bu, öğe hakkında bir yorum eklemenizi sağlar. Aynı dosyaya veya sonuca birden fazla etiket ve yorum ekleyebilirsiniz.

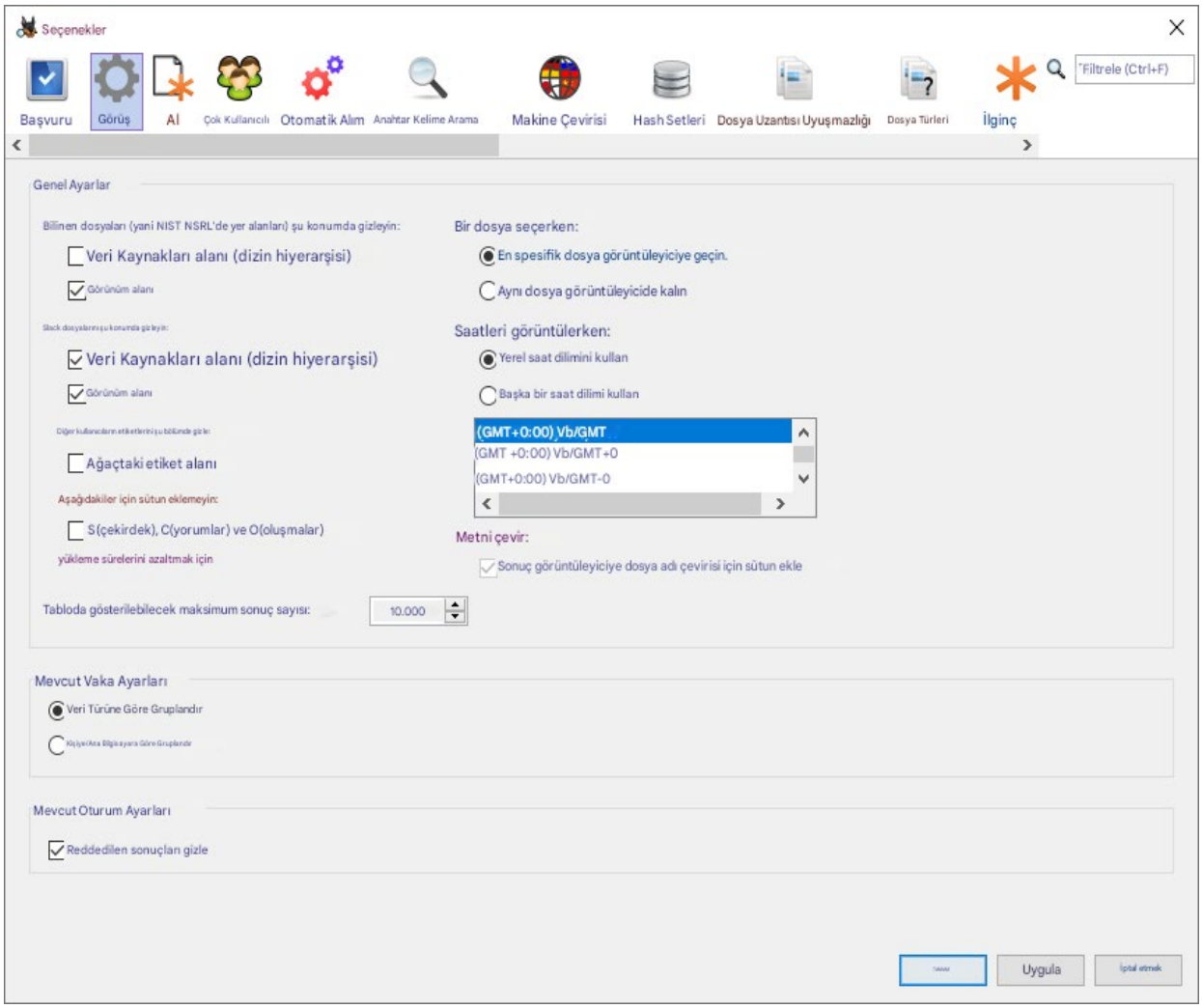


İçerik görüntüleyicisindeki "Ek Açıklamalar" sekmesi aracılığıyla bir öğeye ait tüm yorumları görüntüleyebilirsiniz.

Görünüm seçenekleri, Autopsy kullanıcı arayüzünde verilerin nasıl görüntüleneceğini yapılandırmanıza olanak tanır.Seçeneklere erişmenin iki yolu vardır. Birincisi, dizin ağacının üzerindeki dişli çark simgesini kullanmaktır:



İkinci yöntem ise Araçlar->Seçenekler'e gidip ardından "Görünüm" sekmesini seçmektir:



Küresel Ayarlar

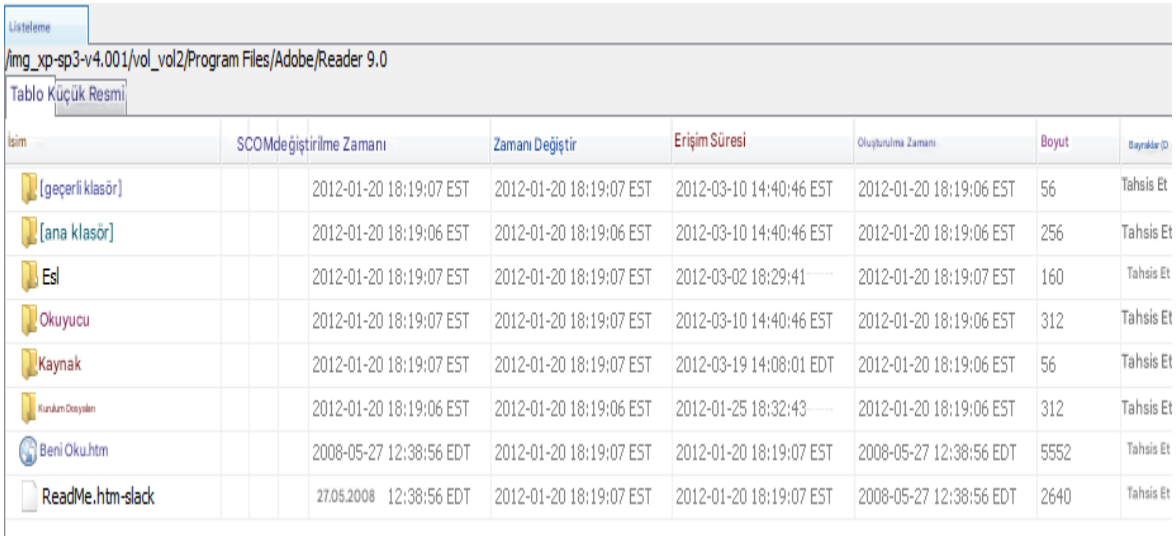
Bu bölümdeki ayarlar, uygulama kapatıldıktan sonra da geçerliliğini korur.

Bilinen dosyaları gizle

Bu seçenek, hash_db_page tarafından "bilinen" olarak işaretlenmiş dosyaları gizlemenizi sağlar. Veri kaynakları alanında bilinen dosyaları gizleme seçeneği, bu dosyaların sonuç görünümünde görüntülenmesini engelleyecektir. Benzer şekilde, görünümler alanında slack dosyalarını gizleme seçeneği, slack dosyalarının ağacın Görünümler bölümünde görünmesini engelleyecektir.

Slack dosyalarını gizle

Autopsy, bir dosyanın sonundaki fazladan boşluklardan ("-slack" uzantılı) slack dosyaları oluşturur. Bu dosyalar, veri kaynakları alanında ve/veya görünümler alanında görüntülenebilir veya gizlenebilir. Aşağıda, sonuç görünümünde bir slack dosyası gösterilmektedir:



Veri Kaynağı Gruplandırması

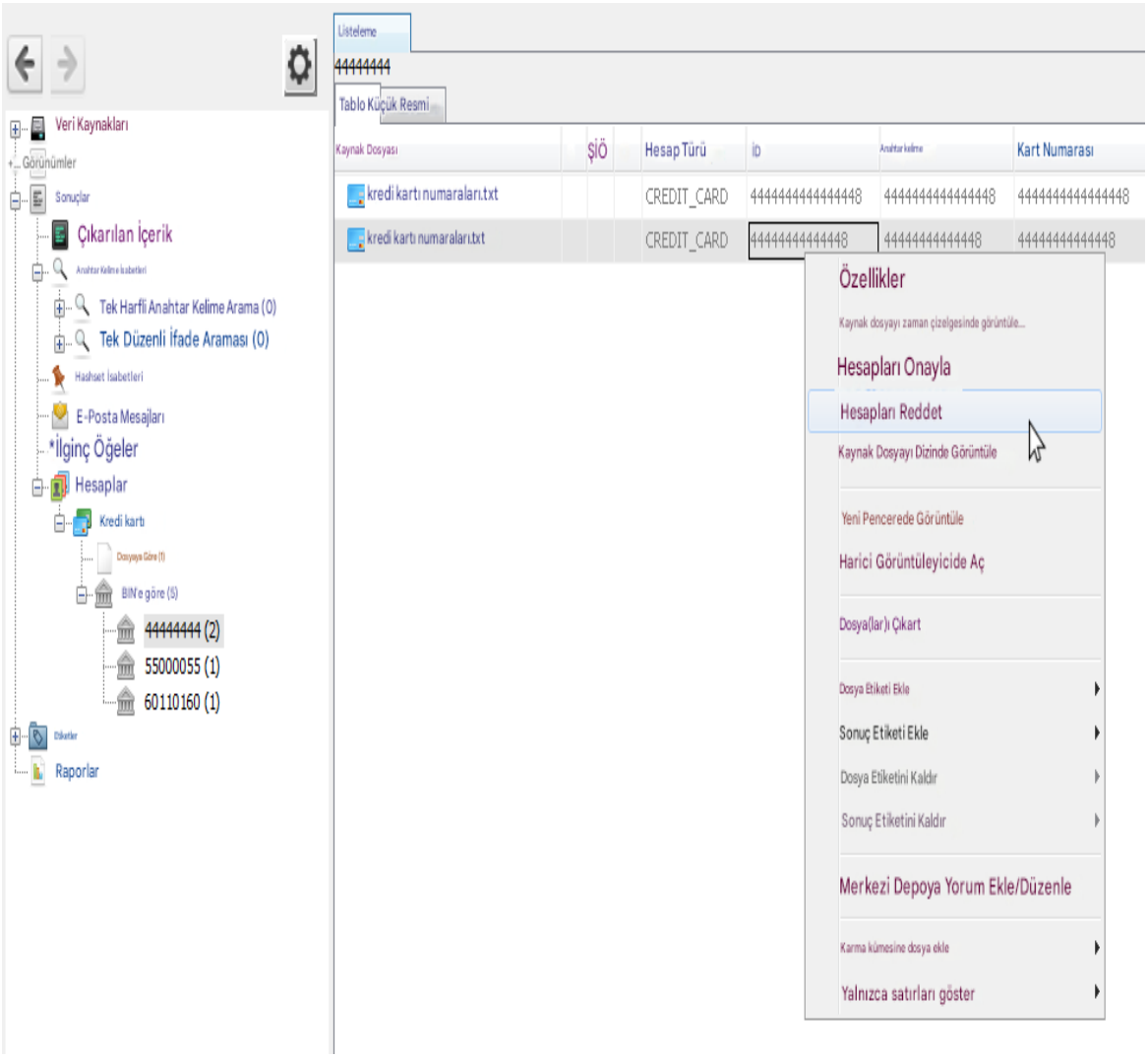
Buradaki seçenekler, Ağaç Görüntüleyici'de verilerin nasıl görüntüleneceğini seçmenize olanak tanır . En üstteki seçenek ("Veri Türüne Göre Gruplandır"), tüm veri kaynakları için birleştirilmiş sonuçları görüntüler. Ağaçtaki tüm düğümler, söz konusu durumda tüm veri kaynakları için birleştirilmiş sonuçları içerecektir.

Geçerli Oturum Ayarları

Geçerli oturumun ayarları, uygulamayı kapatana kadar geçerli kalacaktır.

Reddedilen sonuçları gizle

Aşağıdaki ekran görüntüsünde gösterildiği gibi, hesaplar kullanıcı tarafından onaylanabilir veya reddedilebilir.



Reddedilen hesaplar rapora dahil edilmeyecek ve varsayılan olarak kullanıcı arayüzünde gizlenecektir. Yanlışlıkla bir hesabı reddettiyseniz ve durumunu değiştirmeniz gerekiyorsa veya sadece reddedilen hesapları görüntülemek istiyorsanız, "reddedilen sonuçları gizle" seçeneğinin işaretini kaldırabilirsiniz.

Veri Kaynakları

Sunucuların altında, her veri kaynağı için düğümler bulunur.

Tahsis edilmemiş alan, dosya sisteminin şu anda hiçbir şey için kullanılmayan bölümleridir. Tahsis edilmemiş alan, silinmiş dosyaları ve diğer ilginç kalıntıları içerebilir. Bir görüntü veri kaynağında, tahsis edilmemiş alan, dosya sisteminde farklı konumlara sahip bloklar halinde saklanır. Ancak, veri işleme araçlarının çalışma şekli nedeniyle, bu araçlara tek, büyük bir tahsis edilmemiş alan dosyası beslemek daha iyidir. Autopsy, tahsis edilmemiş alana bakmanın her iki yöntemine de erişim sağlar.

Birimdeki ayrı bloklar Her birim için "$Unalloc" adlı bir "sanal" klasör bulunur. Bu klasör, imajın depoladığı şekilde, ardışık sıralardaki tüm ayrı tahsis edilmemiş

blokları (tahsis edilmemiş alan dosyaları) içerir. Veri Kaynakları alanında diğer dosya türlerini çıkarabildiğiniz gibi, herhangi bir tahsis edilmemiş alan dosyasını sağ tıklayarak çıkarabilirsiniz.

Tek Dosyalar: Birime sağ tıklayın ve "Tahsis Edilmemiş Alanı Tek Dosya Olarak Çıkar" seçeneğini seçerek birimdeki tüm tahsis edilmemiş alan dosyalarını tek, sürekli bir dosyada birleştirin. (İstenirse, bir imaja sağ tıklayıp "Tahsis Edilmemiş Alanı Tek Dosyalara Çıkar" seçeneğini seçerek de aynı işlemi yapabilirsiniz, ancak bu işlem imajdaki her birim için bir kez gerçekleştirilir.)

Tek dosya çıkarma seçeneğine bir örnek aşağıda gösterilmiştir.

Dosya Görüntülemeleri

Görünümler, dosyanın belirli bir özelliğine göre kasadaki tüm dosyaları filtreler.

Dosya Türleri, dosyaları dosya uzantısına veya MIME türüne göre sıralar ve uygun gruba yerleştirir. Örneğin, .mp3 ve .wav uzantılı dosyalar "Ses" grubuna yerleştirilir.

Silinen Dosyalar: Silinmiş ancak adları kurtarılmış dosyaları görüntüler.

Dosya Boyutu Dosyaları boyutlarına göre sıralar.

Veri Yapıtları

Bu bölümde, veri alım işlemi çalıştırılarak oluşturulan veri öğeleri gösterilmektedir. Genel olarak, veri öğeleri veri kaynağından çıkarılan somut bilgiler içerir. Örneğin, iletişim kayıtlarından alınan çağrı kayıtları ve mesajlar veya tarayıcı veritabanından çıkarılan web yer işaretleri.

Analiz Sonuçları

Bu bölümde, veri alımı çalıştırılarak oluşturulan analiz sonuçları gösterilmektedir. Genel olarak, analiz sonuçları kullanıcının ilgilendiğini belirttiği bilgileri içerir.

Örneğin, kullanıcı önemli hash'lerden oluşan bir liste oluşturursa , hash kümesi eşleşmeleri burada görünecektir.

İşletim Sistemi Hesapları

Bu bölümde, dosyada bulunan işletim sistemi hesapları gösterilmektedir. Örnek için İşletim Sistemi Hesapları bölümüne bakın.

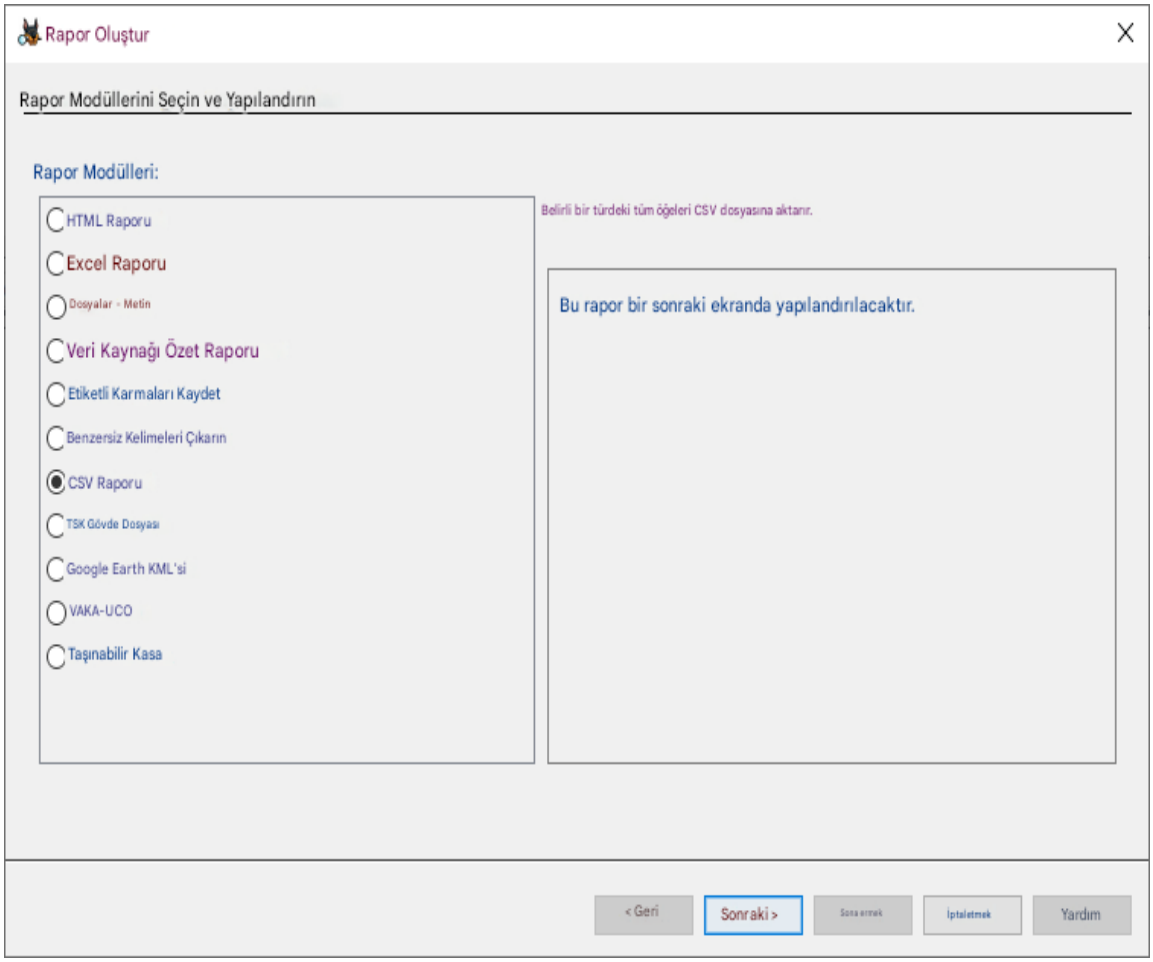
Etiketler

Etiketlediğiniz her öğe burada görünür, böylece onu kolayca tekrar bulabilirsiniz. Daha fazla bilgi için Etiketleme ve Yorum Yapma bölümüne bakın.

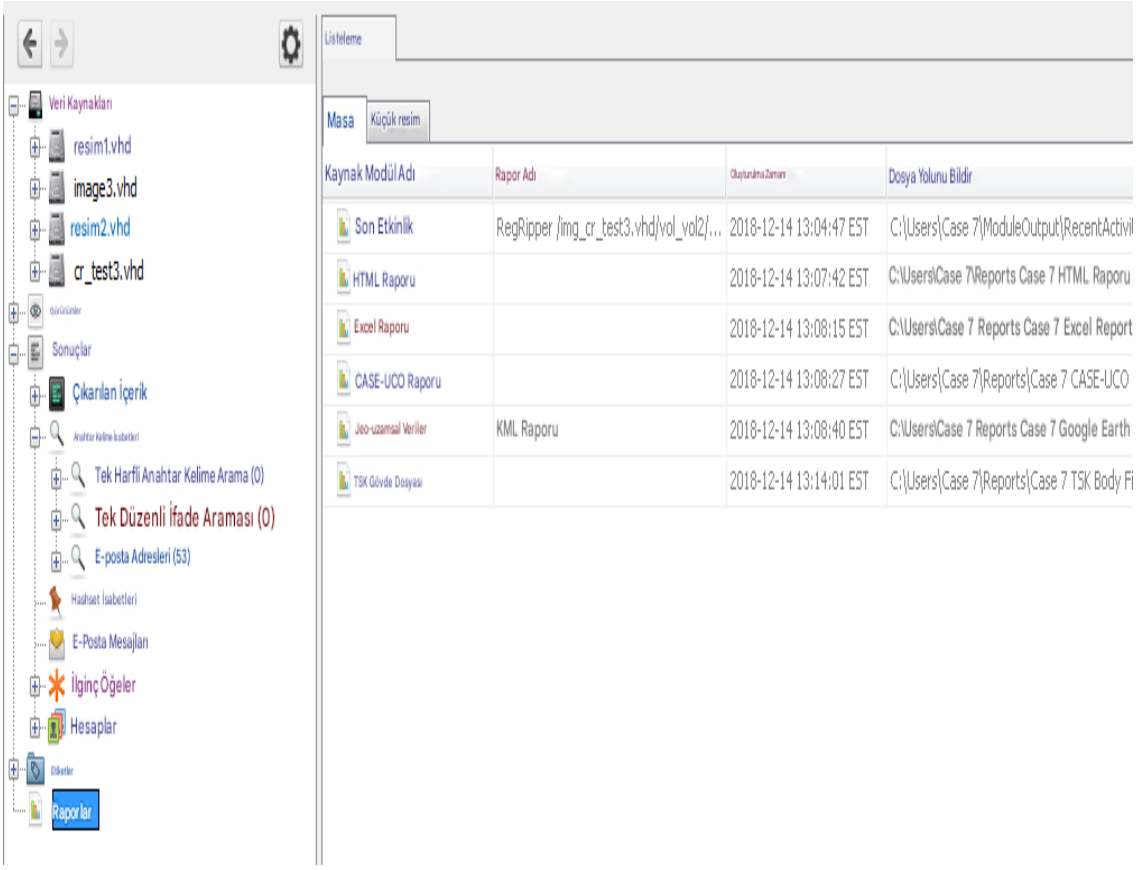
Raporlar

Raporlar, Veri Alma Modülleri aracılığıyla eklenebilir veya Raporlama aracı kullanılarak oluşturulabilir .

Rapor modülleri, kullanıcının bir vakadan önemli bilgileri çeşitli formatlarda çıkarmasına olanak tanır. Bu, bir vakadan çıkarılan tüm içeriği, anahtar kelime eşleşmelerini vb. içeren bir HTML veya Excel raporu oluşturmayı veya Google Earth gibi yazılımlara yüklemek üzere bulunan koordinatlardan bir KML dosyası oluşturmayı içerir.



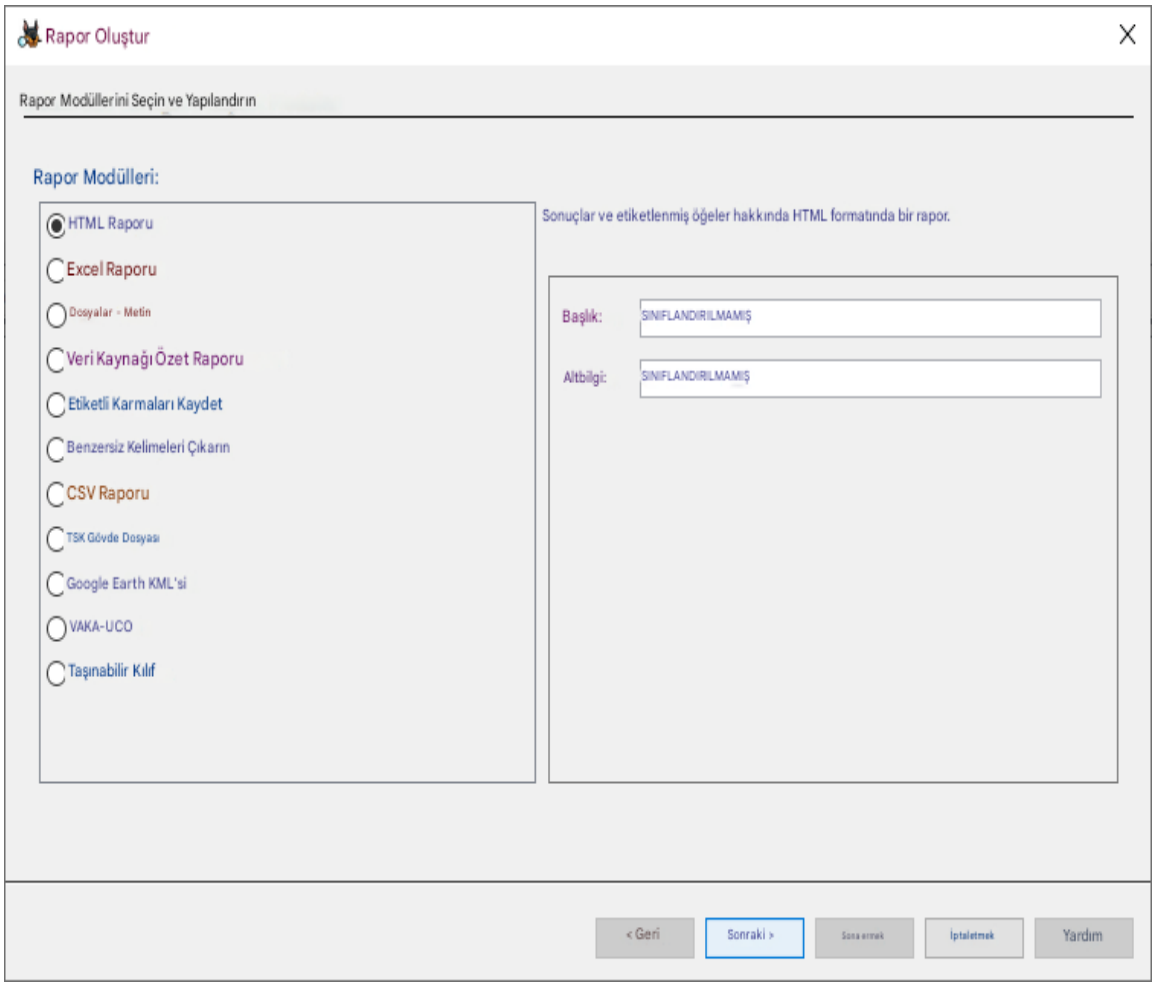
Aşağıda farklı rapor türleri açıklanacaktır. Rapor modüllerinin çoğu, Ağaç Görüntüleyici'nin "Raporlar" düğümü altında görüntülenecek bir rapor dosyası oluşturacaktır.



Rapor Türleri

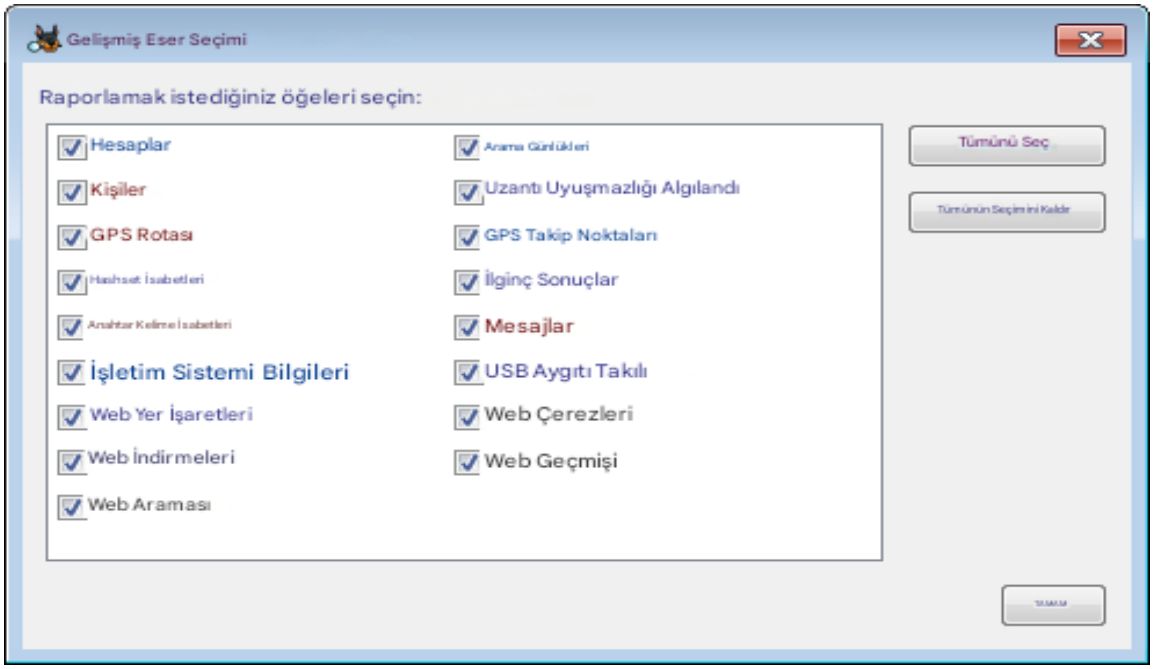
HTML Raporu

HTML raporları için öncelikle sonuçlarınızda görüntülenecek bir başlık ve altbilgi girmeyi seçebilirsiniz. Örneğin, bir sınıflandırma başlığı eklemek isteyebilirsiniz.

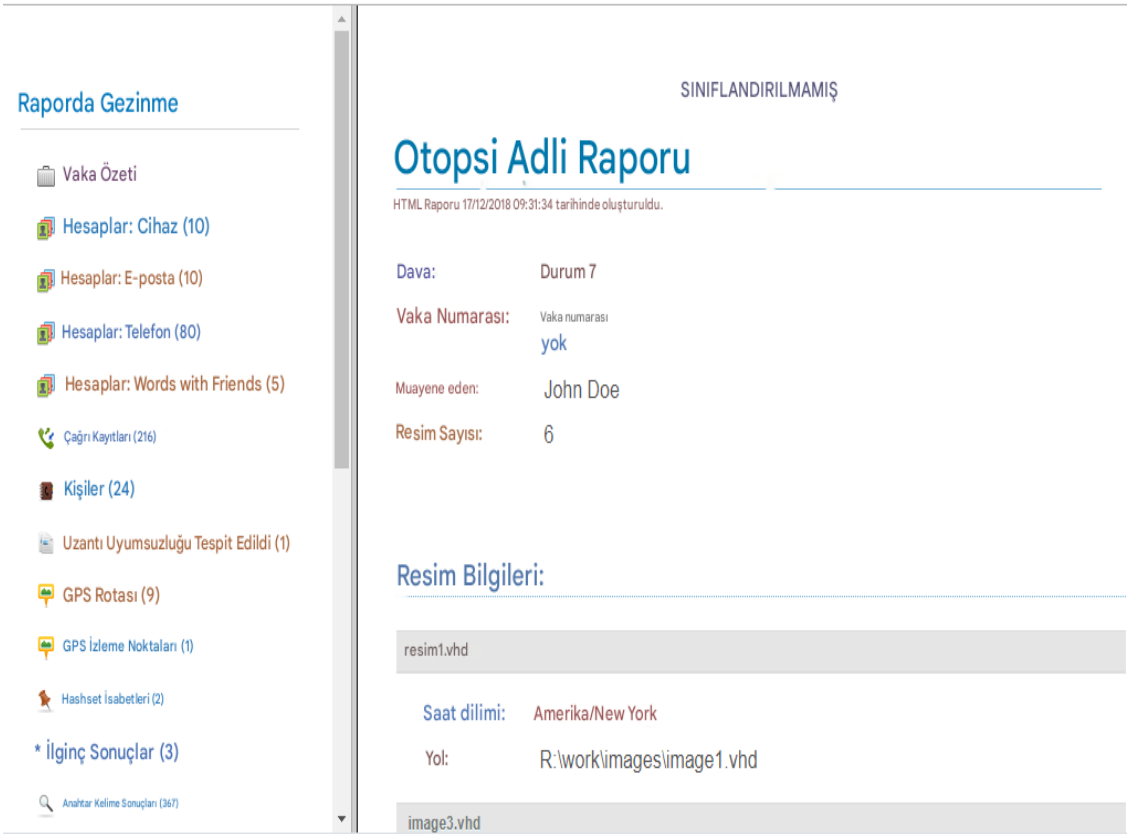


Rapor oluştururken iki seçenek vardır: tüm sonuçları dahil et veya yalnızca etiketlenmiş sonuçları dahil et.

"Tüm Sonuçlar"ı seçerseniz, isteğe bağlı olarak "Veri Türleri" düğmesini kullanarak rapora hangi veri türlerinin dahil edileceğini seçebilirsiniz.

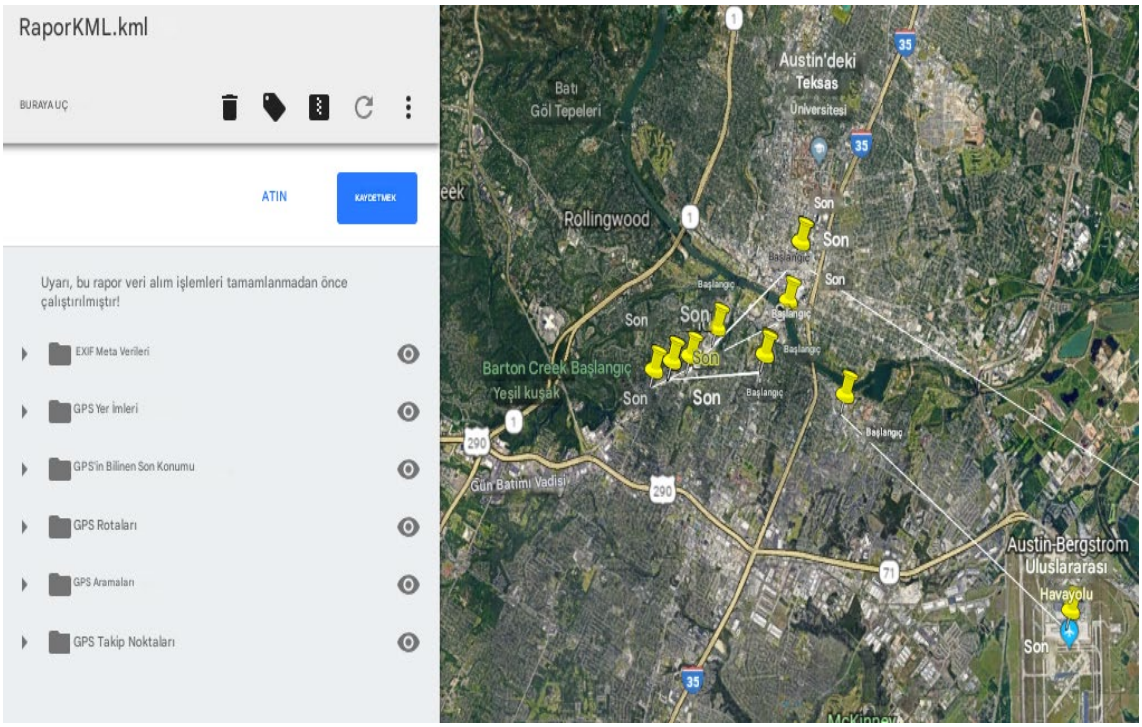


Tamamlanmış rapor aşağıdaki gibi görünecektir:



Google Earth KML

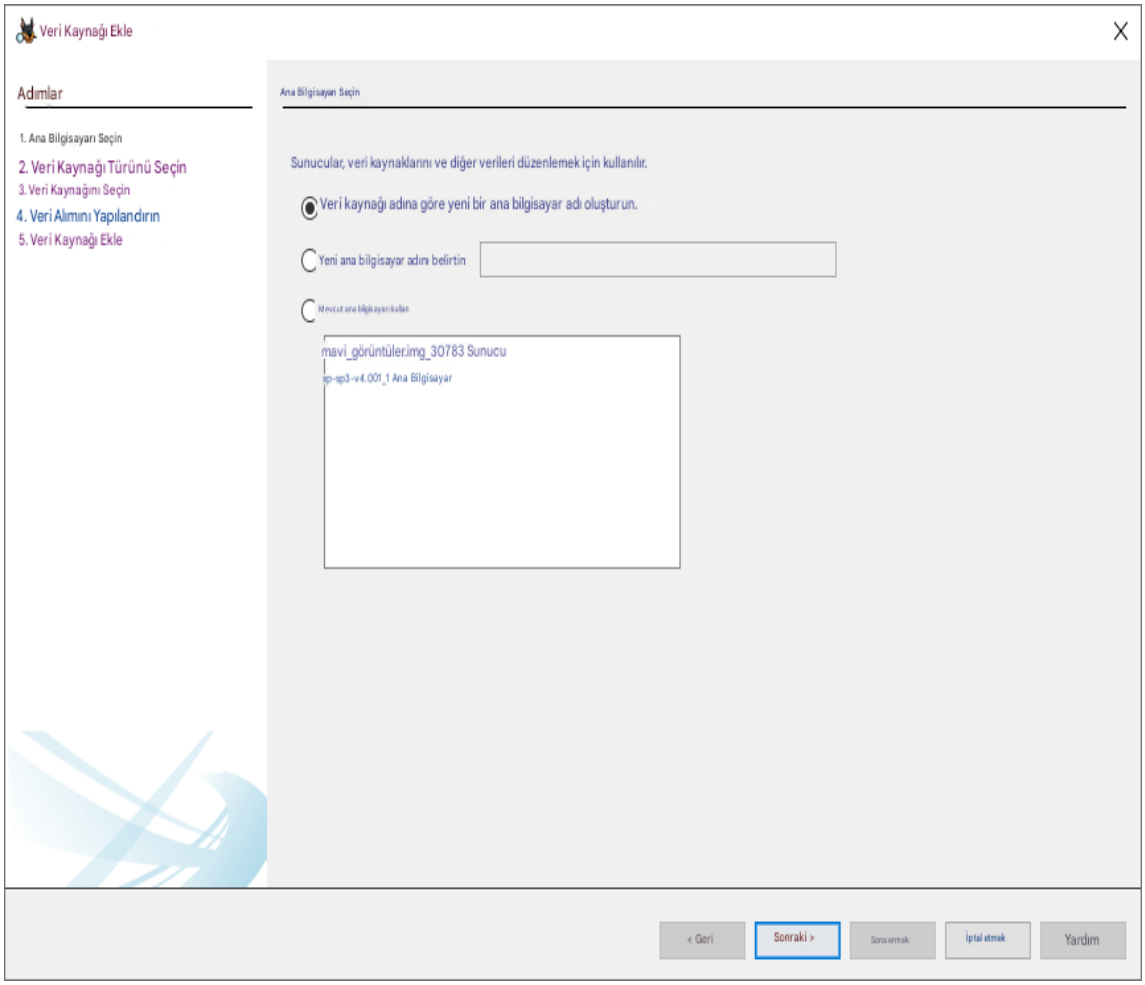
Bu rapor modülü, vakadaki tüm GPS verilerinden bir KML dosyası oluşturur. Bu dosya daha sonra Google Earth ile kullanılabilir.



Hosts Kullanımı

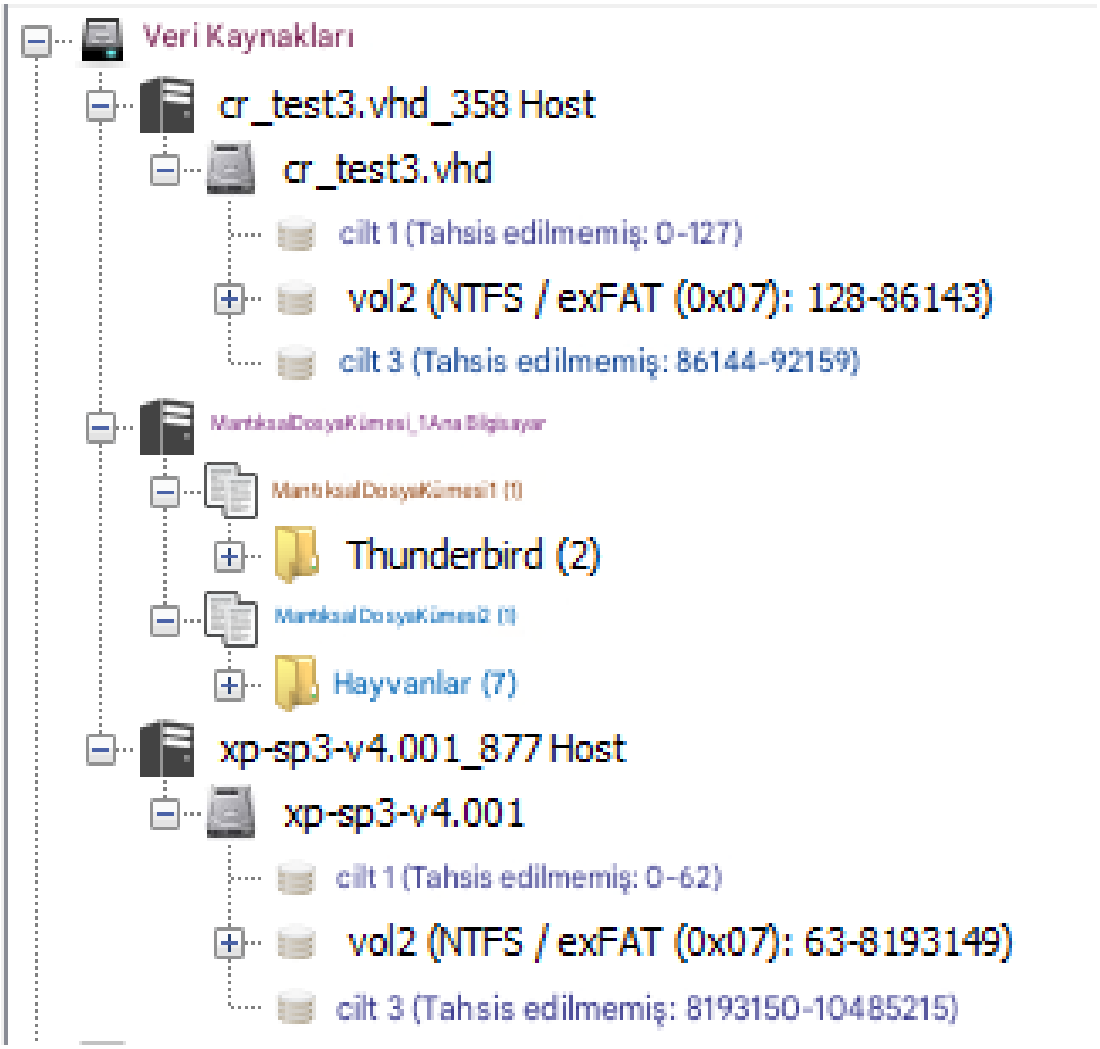
Bir Veri Kaynağını Bir Sunucuyla İlişkilendirme

Her veri kaynağı bir sunucuyla ilişkilendirilmelidir. Veri kaynağı ekleme işleminin ilk adımı , vakaya eklemek üzere olduğunuz veri kaynağı için bir sunucu seçmektir. Bu sunucu otomatik olarak oluşturulabilir, kullanıcı tarafından girilebilir veya vakada zaten mevcut olan sunucular listesinden seçilebilir.



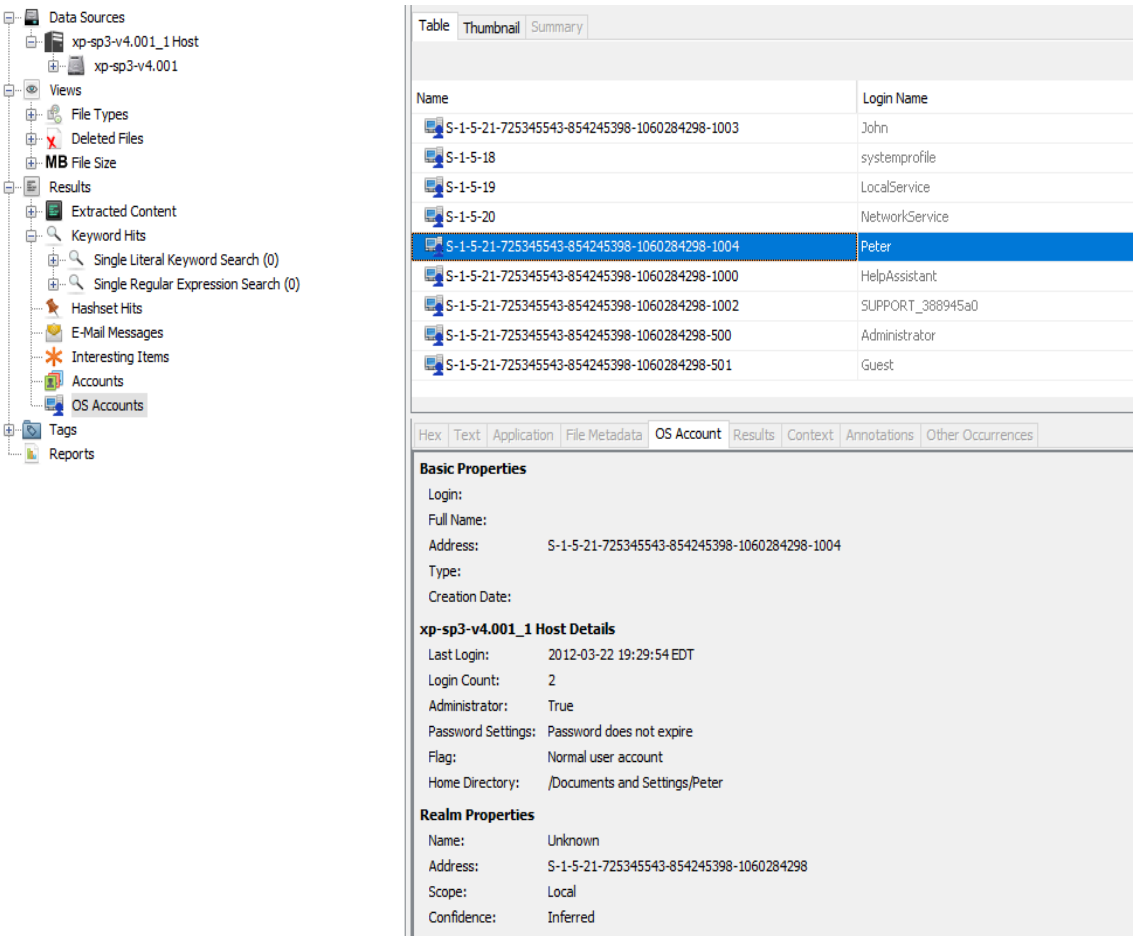
Ev Sahiplerini Görüntüleme

Ev sahipleri Ağaç Görüntüleyici'de görüntülenir . Seçilen Görüntüleme Seçeneklerine bağlı olarak , ev sahipleri kişiler altında gruplandırılabilir.



İşletim Sistemi Hesapları

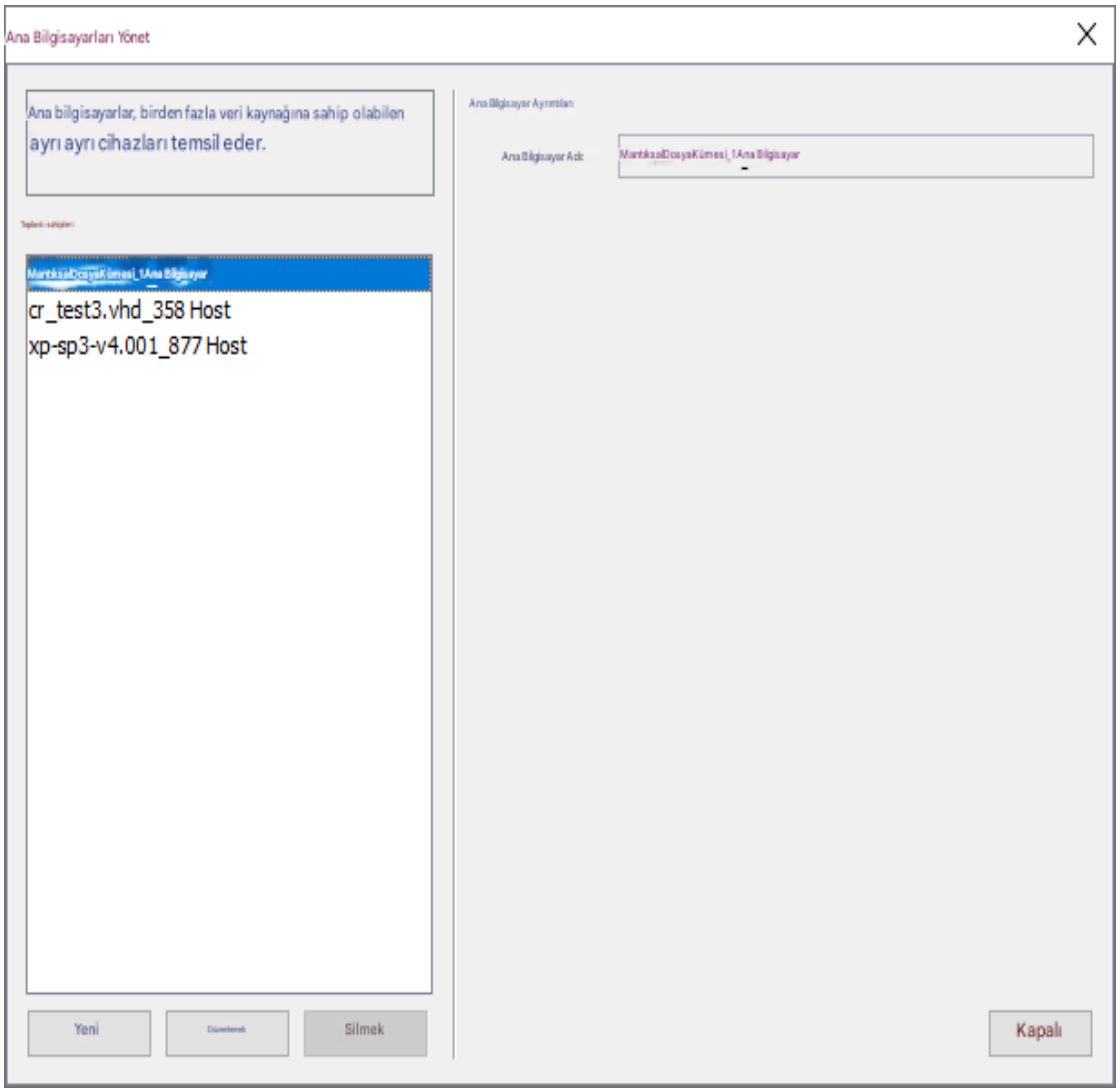
İşletim sistemi hesapları, ağaç görüntüleyicisinin İşletim Sistemi Hesapları düğümünde görüntülenebilir. Her işletim sistemi hesabı bir ana bilgisayarla ilişkilidir ve ana bilgisayar bilgileri içerik görüntüleyicisinin İşletim Sistemi Hesabı sekmesinde görüntülenir.



Sunucuları Yönetme

Sunucuları Yönet Menüsü

Sunucu yönetim paneline erişmek için Vaka -> Sunucuları Yönet seçeneğine gidin.

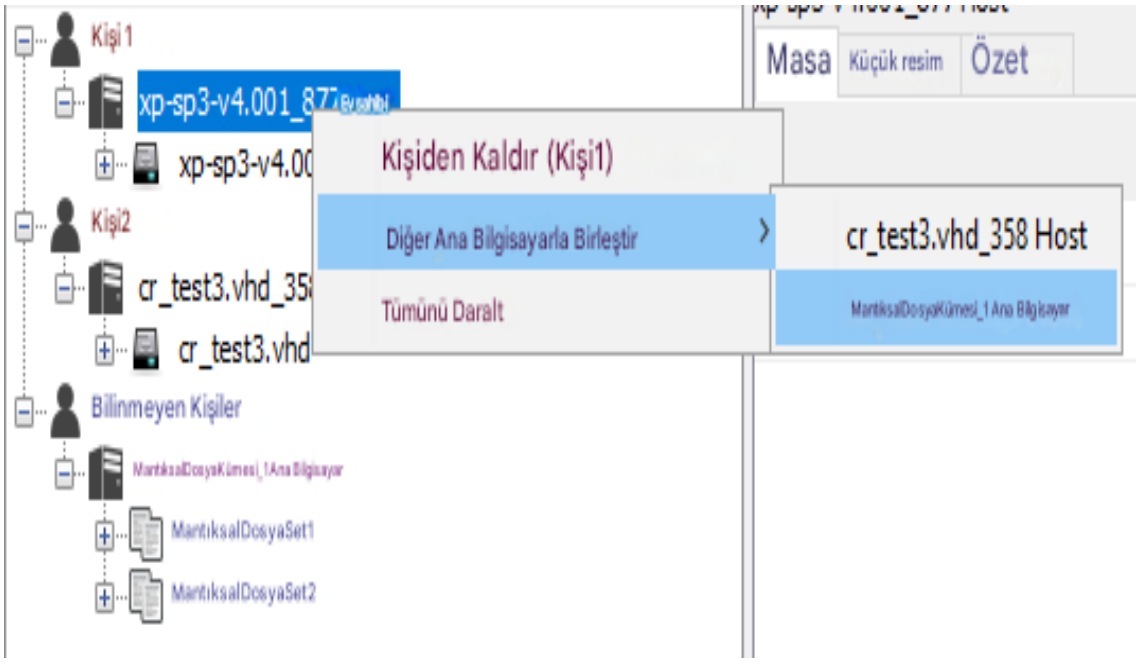


Burada, ilgili tüm sunucuları görebilir, yeni sunucular ekleyebilir, mevcut bir sunucunun adını değiştirebilir ve kullanılmayan sunucuları silebilirsiniz.

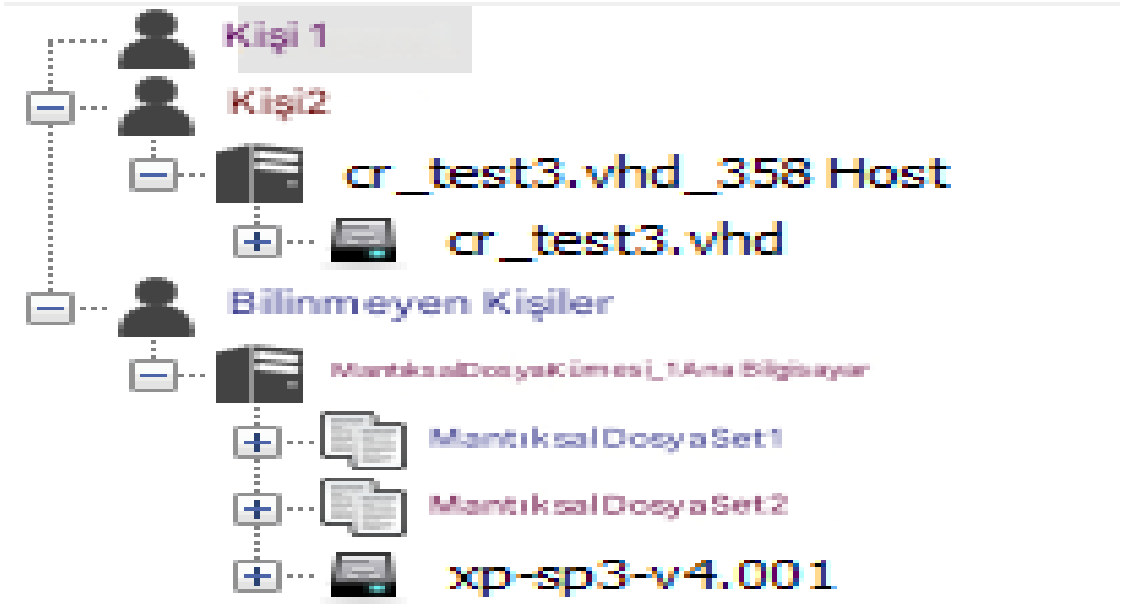
Sunucuları Birleştirme

Bir vakayı işleme sürecinde, iki (veya daha fazla) sunucunun birleştirilmesi gerektiği ortaya çıkabilir. Bir sunucuyu diğerine birleştirmek, kaynak sunucudaki tüm veri kaynaklarını hedef sunucuya taşıyacak ve bulunan tüm işletim sistemi hesaplarını taşıyacak veya birleştirecektir.

Sunucuları birleştirmek için, birleştirmek istediğiniz sunucuya sağ tıklayın.



Bu işlemin geri alınamayacağını belirten bir onay iletişim kutusu görüntülenecektir. Devam ettikten sonra, sunucular birleştirilecek ve ağaç görüntüleyici düğümü birleştirilmiş verileri gösterecek şekilde güncellenecektir.



Kaynakça (References)

Bu rehberin hazırlanmasında kullanılan temel kaynaklar, yazılımlar ve akademik referanslar aşağıda listelenmiştir:

1. Resmi Yazılım Dökümantasyonları

- **Autopsy User Documentation.** (2026). *Autopsy 4.22.1 Official Guide.* Sleuth Kit Official.
- **The Sleuth Kit (TSK) Library.** *File System Analysis Framework.* Sleuth Kit Hub.
- **Apache Solr Reference Guide.** *Indexing and Search Engine Optimization.* Apache Software Foundation.

2. Akademik ve Teknik Kitaplar

- **Carrier, B.** (2005). *File System Forensic Analysis.* Addison-Wesley Professional. (Dosya sistemi analizi ve TSK'nın temelleri için başucu eseri).
- **Casey, E.** (2011). *Digital Evidence and Computer Crime.* Academic Press. (Hukuki süreçler ve kanıt zinciri standartları).
- **Luttgens, J. T., Pepe, M., & Mandia, K.** (2014). *Incident Response & Computer Forensics.* McGraw-Hill Education.

3. Standartlar ve Protokoller

- **NIST (National Institute of Standards and Technology).** *Computer Forensic Tool Testing (CFTT) Project.* nist.gov.
- **SWGDE (Scientific Working Group on Digital Evidence).** *Best Practices for Computer Forensics.*
- **ISO/IEC 27037:2012.** *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.*

4. Geliştirici ve Topluluk Kaynakları

- **Autopsy Python Plugin Module Development.** *Jython Scripting for Autopsy API.* Sleuth Kit Github.
- **ALEAPP & iLEAPP Projects.** *Android/iOS Logs Events And Protobuf Parser.* Alexis Brignoni Repository.
- **Volatility Foundation.** *Memory Forensics Analysis Framework.* volatilityfoundation.org.

Yazar Hakkında

Recep Şenel, bilişim, sistem yönetimi ve dijital adli bilişim alanlarında 30 yılı aşkın saha tecrübesine sahip bağımsız bir analisttir.

Kamu kurumlarında başlayan mesleki yolculuğu boyunca:

- sistem altyapıları,
- olay inceleme,
- bilgi güvenliği,
- teknik analiz,
- kullanıcı davranışı ve dijital iz takibi
  alanlarında aktif görev almıştır.

Özellikle son yıllarda çalışmalarını:

- dijital adli bilişim (DFIR),
- Windows artefakt analizi,
- olay korelasyonu,
- delil bütünlüğü,
- teknik metodoloji
  üzerine yoğunlaştırmıştır.

Yazarın temel yaklaşımı; bir aracı kullanmaktan çok,veriyi doğru okumaya, izleri doğru yorumlamaya ve olayın teknik gerçeğini tarafsız biçimde ortaya koymaya dayanır.

Bu anlayışla;

- açık kaynak projeler,
- teknik rehberler,
- Türkçe kaynak üretimi,
- saha odaklı eğitim içerikleri
  üzerinde çalışmalar yürütmektedir.

Recep Şenel'e göre dijital adli bilişim: "Yalnızca log okumak değil; verinin sessiz bıraktığı boşlukları da anlamaktır." Bu kitap da,yıllar içinde edinilen saha disiplini, teknik deneyim ve öğretici bir yaklaşımın sonucu olarak hazırlanmıştır. Amaç; Türkçe kaynak eksikliğini azaltmak, mesleğe ilgi duyanlara güvenilir bir başlangıç sunmak
ve analitik düşünmeyi teşvik etmektir.

Dijital dünyada her işlem bir iz bırakır.
Silinen bir dosya, açılan bir web sayfası, takılan bir USB bellek ya da değiştirilen bir zaman damgası… Hepsi, doğru yöntemle okunduğunda bir olayın teknik hikâyesini anlatır.