**1-** **GİRİŞ**

Autopsy yazılımı 2000li yıllarda Basis Technology tarafından piyasaya sürülmüştür. Birçok açık kaynaklı program ve eklentinin dağıtımını kolaylaştırmıştır. Grafiksel ve kullanıcılar tarafından kolayca öğrenilebilen ve kullanıcı dostu bir yazılımdır. Adli bilişim yazılımı olarak sıkça kullanılan Ücretsiz ve açık kaynak kodlu bir yazılımdır. Açık kaynak kodlu ve ücretsiz olması en büyük avantajlarındandır.

Basis Technology ayrıca ürüne yani bu yazılıma özel eğitimler de vermektedir. Uygulamayı yazarken en büyük 4 ilkeyi dikkate almışlardır.

· *Genişletilebilir* — kullanıcı, temel alınan veri kaynağının tamamını veya bir kısmını analiz edebilen eklentiler oluşturarak yeni işlevler ekleyebilmelidir.

· *Merkezileştirilmiş* — araç, tüm özelliklere ve modüllere erişmek için standart ve tutarlı bir mekanizma sunmalıdır.

· *Kullanım Kolaylığı* — Otopsi Tarayıcısı, kullanıcıların aşırı yeniden yapılandırma olmadan adımlarını tekrar etmelerini kolaylaştırmak için sihirbazlar ve tarihsel araçlar sunmalıdır.

· *Birden Fazla Kullanıcı* — araç, tek bir araştırmacı tarafından kullanılabilir olmalı veya bir ekibin çalışmasını koordine etmelidir.

2- KURULUM

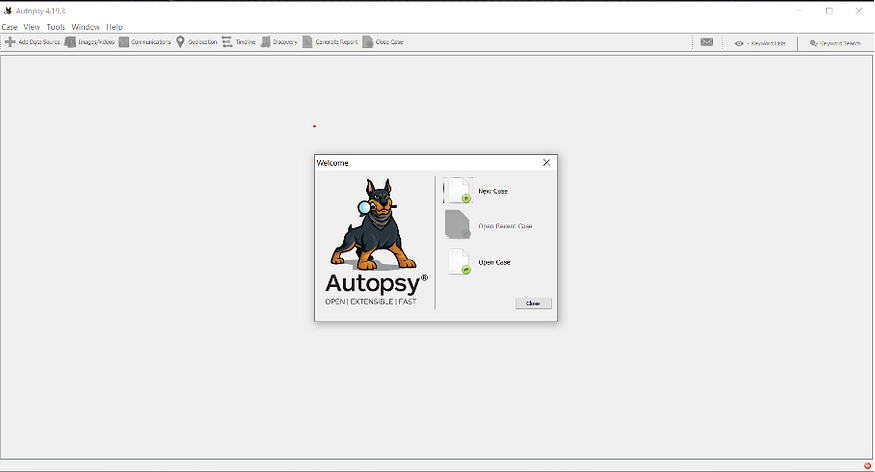
Autopsy programının kullanılması için öncelikle internet üzerinden indirmek gerekmektedir. Lakin internet üzerinde bin bir çeşit zararlı yazılımlar bulunduğu için kendi websitesinden indirmeyi şiddetle tavsiye ederim yoksa kişisel bilgisayarınıza yanlışlıkla yani bilmeyerek zararlı yazılım yükleyebilirsiniz. sözü çok uzatmadan kurulum için gerekli linki buraya bırakıyorum : <https://www.autopsy.com/download/>

Yukarıdaki linkten Autopsy uygulamasını güvenle indirebilirsiniz. Linke tıkladıktan sonra karşınıza gelen websitesinde kendi işletim sisteminize uygun olan kısıma tıklayarak indirme işlemini başlatabilirsiniz. Benim bilgisayarımda Windows kullanıyorum şu anda o yüzden Windows 64 bit seçeneğine tıklıyorum.

İndirme işlemi tamamlandıktan sonra indirdiğimiz setup dosyasını yönetici olarak çalıştıralım.

Kurarken dikkat etmeniz gereken en önemli hususlardan birisi de uygulamayı nereye kuracağınızdır varsayılan olarak C:// dizini altına kuruyor bunu istediğiniz şekilde yeniden yapılandırabilirsiniz.

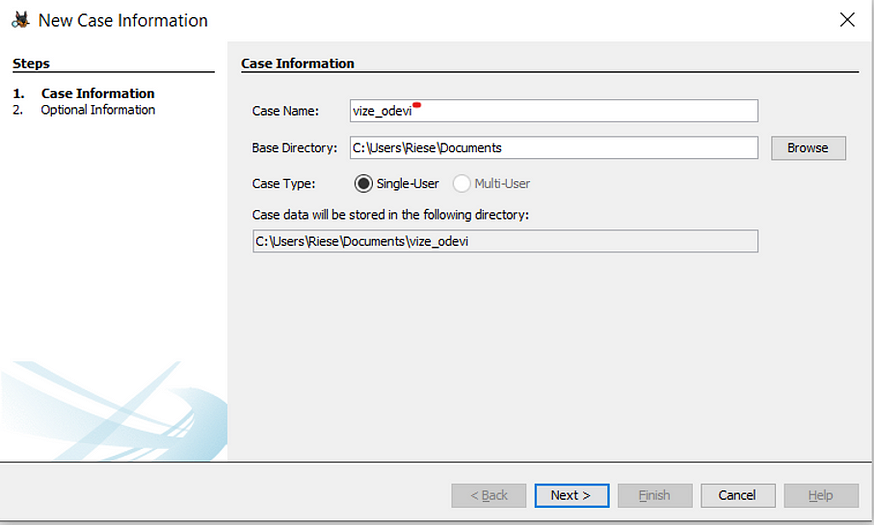
Kurulumu tamamladıktan sonra uygulamamızı çalıştırabileceğimiz bir masaüstü simgesi otomatik olarak oluşturulmaktadır. Onu yönetici olarak çalıştıralım. Karşımıza ilk gelen kısım şekil-1 de görünmektedir.



şekil-1

Bu kısımdan new caseye tıklayarak yeni bir vaka oluşturuyoruz. Ya da önceden oluşturmuş olduğumuz bir vaka varsa open case kısmına tıklayarak önceden oluşturmuş olduğumuz vakayı açabiliyoruz. DD, Encase ve AFF uzantılı adli kopyalar üzerinde inceleme yapabiliyoruz.

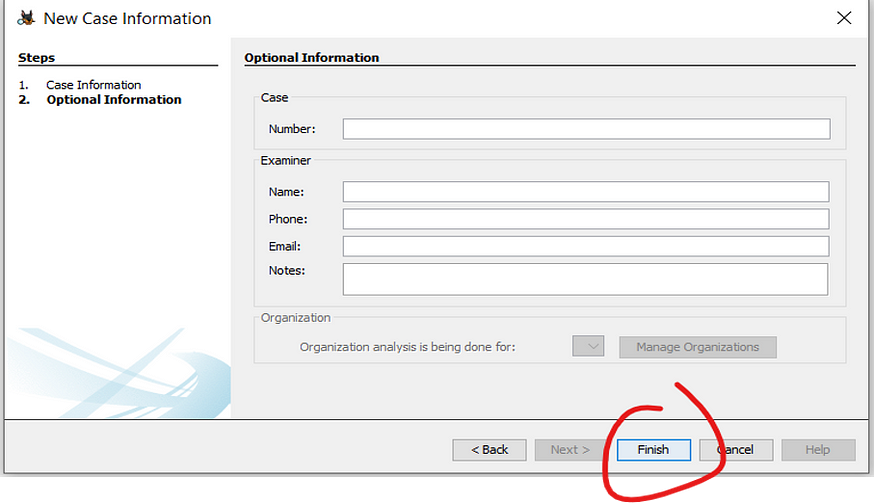
Ben yeni bir vaka oluşturacağım için new case seçeneğine tıkladım şekil-2de görüldüğü gibi



şekil-2

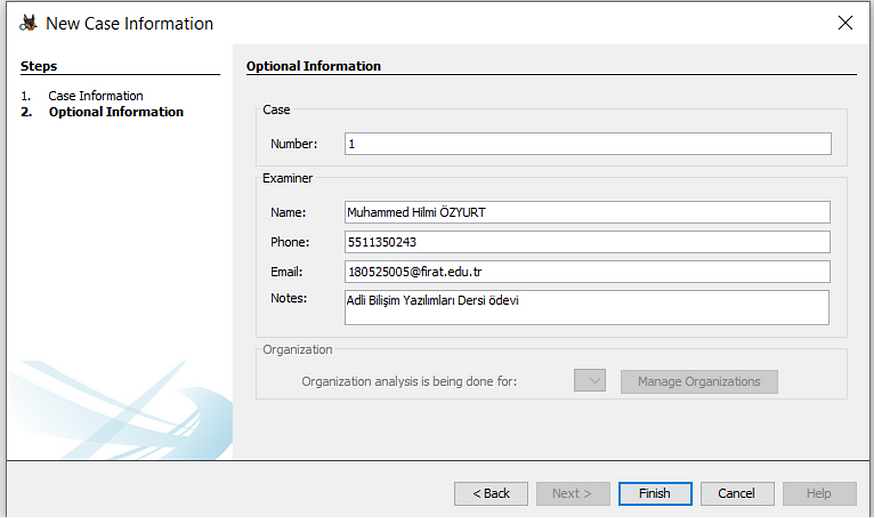
Case name kısmına vaka adını yazıyoruz ben vize ödevi yazdım next diyoruz.

Daha sonra bize vaka numarası ve inceleyen hakkında sorular soruyor şekil-3te görüldüğü üzere



şekil-3

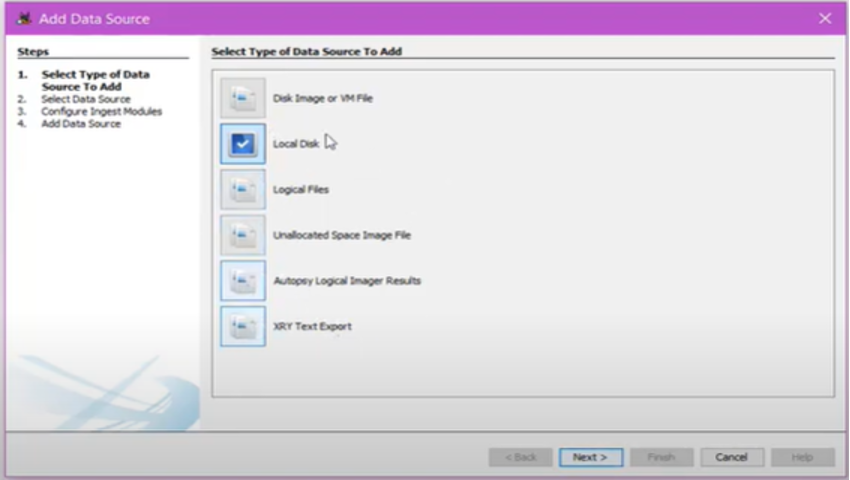
Examiner kısmına vakayı inceleyen kişi hakkındaki bilgileri girmemiz gerekmektedir. Case kısımındaki number kısmına ise vaka numarasını yazıyoruz.



şekil-4

Ben bu şekilde doldurup finish kısmına bastım.

Vakayı oluşturduktan sonra ilk yapmamız gereken şey kaynak eklemek.

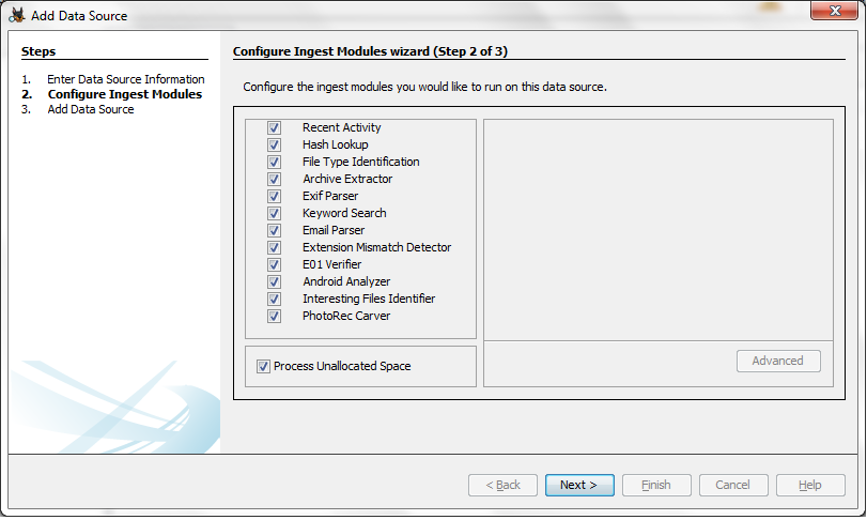


şekil-5

Şekil-5 te görüldüğü gibi kaynak ekleme kısmını göreceğiz.

Bu kısımdan istediğiniz kaynak türünü seçebilirsiniz isterseniz disk imajı seçebilirsiniz ya da daha önceden imajı alınmış bir cihazı da bu kısımdan seçip ekleyebilirsiniz.

Veri kaynağı dahil edildikten sonra, alım modülleri bilgileri parçalamak için gözden kaybolur. Sonuçlar sürekli olarak arayüzde sunulur ve önemli olan uyarıları verir. Model alma modülleri, karma sayım ve sorgu, parola arama ve web kalıntısı çıkarma işlemlerini içerir. Üçüncü taraf modüller oluşturulabilir ve boru hatlarına eklenebilir.



şekil-6

Verilerin manuel olarak analiz edilmesinin gözden geçirilmesi

Kullanıcı, “kanıtları belirlemek için arayüzde, dosya içeriklerinde ve giriş modülü sonuçlarında” gezinir.

**Adım 5:** Sonuçları Etiketleyin

İlginç öğeler daha sonra raporlama ve analiz için etiketlenebilir.

**6. Adım:** Rapor Oluşturma

Kullanıcı, seçilen etiketlere veya sonuçlara dayalı olarak bir nihai rapor başlatır.

· **Dağıtım Türleri**

İki tür dağıtım vardır. (a) Masaüstü/Tek Kullanıcı (b) Küme/Çok Kullanıcılı.

* **Masaüstü/Tek Kullanıcı:**

**İşlevsellik:** Bu tipte kasalar aynı anda sadece bir kişi tarafından açılabilir.

**Teknik:** Her şey tek bir bilgisayarda çalışır. Tek bir yükleyici ile kutudan çıkar çıkmaz çalışır. Otopsiyi başlatmak tüm gömülü hizmetleri (yani Veri tabanları, Metin indeksleme vb…) başlatacaktır.

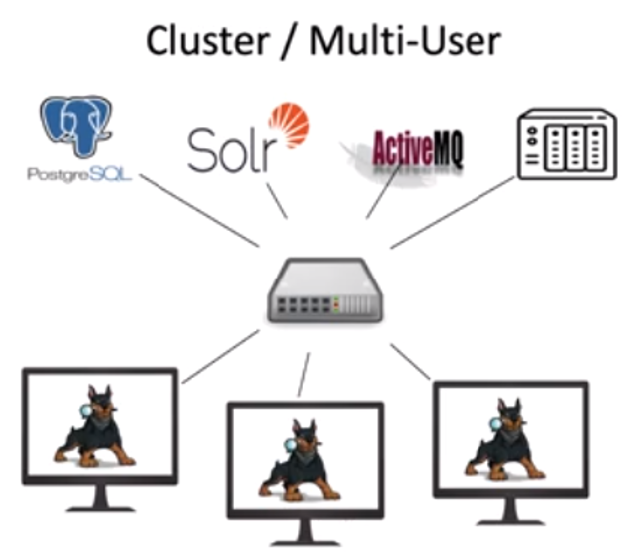


şekil-7

* **Küme/Çok kullanıcılı**

**İşlevsellik:** Kutular aynı anda birden fazla kullanıcı tarafından açılabilir. Yeni medyanın birden fazla mod tarafından 7 gün 24 saat otomatik olarak analiz edildiği “Otomatik Alım” moduna izin verir. Veri tabanı genellikle daha hızlı olduğu için daha hızlı analiz sağlar.

**Teknik:** Kullanıcı deneyimi tamamen aynıdır. Veritabanı, metin indeksi vb. için merkezi düzeyde sunucular kullanır. Ayrıca merkezi düzeyde yüksek hızlı depolama kullanır.



şekil-8

* **Merkez depo**

Bu durumda, geçmiş vakalardan veri depolayan Veritabanı. MD5 karma değerleri, yorumları ve wifi SSID’lerini içerir.

Otopsi tipik olarak vakaya özel veri tabanlarına sahiptir. Veritabanlarını daha küçük ve yönetimi daha kolay tutar. Arşivleme vb. işlemlere izin verir.

**Merkezi Depo dağıtım türleri:**

İki tür desteklenir:

* (i) SQLite — Başka kurulum gerektirmez. Aynı anda sadece bir kullanıcı tarafından kullanılabilir.
* (ii) PostgreSQL — Veritabanı bir sunucuda saklanır. Aynı anda birden fazla kullanıcı tarafından kullanılabilir. Çok kullanıcılı durumlar için aynı sunucuyu kullanabilir.

**VAKALAR VE VERİ KAYNAKLARI**

1. **VAKALAR**

Bir vaka, en azından bilgi kaynakları (disk görüntüsü, disk aygıtları ve mantıksal dosyalar) içerebilir. Veri kaynakları, tek bir PC’deki çeşitli sürücülerden veya çok sayıda PC’den olabilir.

Bir vaka, analiz edeceğiniz araştırma verilerini gruplandırır. Kaç vaka oluşturacağınız size bağlıdır: ya araştırma yoluyla ya da bir araştırma içinde barındırıcı tarafından olabilir.

Her vakanın, vaka adına bağlı olarak adlandırılan kendi indeksi (dizini) vardır. Dizin, yapılandırma dosyalarını, bir veritabanını, raporları ve modüllerin oluşturduğu farklı kayıtları içerecektir.

Temel Otopsi vaka yapılandırma dosyası bir “.aut” büyütmesine sahiptir.

**Faktörler:**

* Bir seferde yalnızca bir dava açılabilir.
* Raporlama vaka düzeyinde yapılır.
* Vakalar otomatik olarak kaydedilir.

4. **Vaka Oluşturma**



şekil-9

Yeni bir vaka oluşturmanın birkaç yolu vardır:

* Açılış ekranının yeni bir vaka oluşturmak için bir düğmesi vardır.
* “Dosya”, “Yeni Vaka Oluştur” menü öğesi

5. **Vaka dizini**

Her Otopsi vakasının (Çoklu ve Tekli kullanıcı) bir dizini vardır. Ya bir ‘temel’ dizin kavramına sahiptir ya da temel dizinde vaka adıyla bir klasör oluşturur.

Not: Çok kullanıcılı bir kümede, tüm denetçilerin aynı yoldan vaka dizinine erişimi olması gerekir.

**Vaka dizini içeriği:**

* **Autopsy.db**— SQLite veritabanı, temel vaka bilgilerini ve veri kaynağı bilgilerini depolayacaktır.
* **Dışa aktarma klasörü**— Dışa aktarılan dosyaları depolamak için varsayılan konum.
* **Raporlar klasörü — Raporları** depolamak için varsayılan konum.
* **Modül çıktı klasörü — Modüllerin çıktı** yazacağı varsayılan konum.

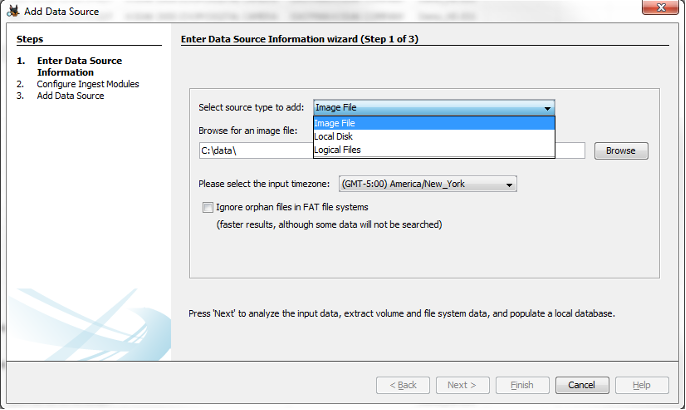
2. **Veri kaynakları**

İncelemeniz gereken bir veri kaynağı. Bir plaka resmi, bazı yasal kayıtlar, bir mahalle gezintisi ve benzeri olma eğilimindedir. Otopsiye bir veri kaynağı eklemeden önce bir vaka açmalısınız.

**Veri Kaynağı Ekleme**

Bir veri kaynağını birkaç farklı yolla dahil edebilirsiniz:

* Bir servis talebi oluşturduktan sonra, doğal olarak sizden bir veri kaynağı eklemenizi ister.
* Bir servis talebi açıkken bir Veri Kaynağını dahil etmek için bir araç çubuğu şeyi vardır.
* Bir vaka açıkken “Dosya”, “Veri Kaynağı Ekle” menüsü şeyi.



şekil-10

Otopsi, üç tür veri kaynağını destekler:

* Disk Görüntüsü: Bir sabit sürücünün veya ortam kartının bayt bayt kopyası olan bir dosya (veya dosya grubu).
* Disk Görüntüsü Ekleme

Otopsi, aşağıdaki formatlardaki disk görüntülerini destekler:

* Raw Single (Örneğin: \*.img, \*.dd, \*.raw, vb.)
* Ham Bölme (Örneğin: \*.001, \*.002, \*.aa, \*.ab, vb.)
* EnCase (Örneğin: \*.e01, \*e02, vb.)

Disk görüntüsü eklemek için:

* Çekme işleminden başlayarak “Görüntü Dosyası”nı seçin.
* Disk görüntüsündeki ilk dosyaya göz atın. Sadece ilk dosyayı belirlemelisiniz ve Otopsi gerisini keşfedecektir.
* Disk görüntüsünün kaynaklandığı saat dilimini seçin. Bu, zaman dilimi verilerini saklamadığından ve Otopsi, UTC’ye nasıl standartlaştırılacağını anlamadığından, FAT kayıt çerçevelerini dahil ederken genellikle önemlidir.
* FAT dosya sistemlerinde yetim dosya bulmayı seçin. Otopsi’nin gadget’taki her alana bir göz atmasını gerektireceğinden, bu zaman yoğun bir prosedür olabilir.

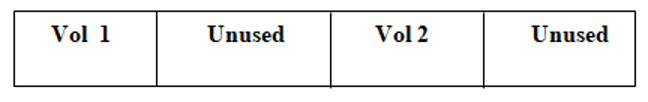
**Disk Görüntü Analizi**

Görüntünün içeriğini analiz etmek için The Sleuth Kit’i (TSK) kullanır. Ve diski bölümlere ayıran birim sistemlerini algılar. Ayrıca, dosyaların saklanabilmesi için bir bölüm düzenleyen dosya sistemlerini de algılar.

**Hacim Sistemi Analizi**

Birim sistemleri, disk görüntüsünü bir veya daha fazla birim (veya bölüm) halinde düzenler. Disk görüntüsünün başlangıcına yakın bir yerde bulunur. Autopsy/TSK şunları destekler: disk işletim sistemi (DOS), GUID Partition Table (GPT), Macintosh (Mac), Berkeley Software Distribution (BSD) ve Solaris.

Otopsi, bir birimde olmayan disk alanlarını gösterecektir.



şekil-11

Her birim, bir dosya sistemi aramak için analiz edilir. Birim bulunamazsa, tüm görüntü bir dosya sistemi için analiz edilir.

**Dosya Sistemi Analizi**

Dosyaların saklanmasını sağlar. Tipik olarak disk görüntüsünün başında veya birimin içinde bulunur.

Desteklenen biçimler şunlardır: NT Dosya Sistemi (NTFS), Dosya Ayırma Tablosu (FAT), Genişletilebilir Dosya Ayırma Tablosu (EXFAT), Hiyerarşik dosya sistemi (HFS+), ISO9660, Ext 2/3/4, Android Dosyasının Tersine Mühendislik Sistem (YAFFS2), Evrensel Flash Depolama (UFS).

**Yetim Dosyalar**

Yetim dosyalar, silinen ve artık bir üst klasörü olmayan dosyalardır. Bunlara “$OrphanFiles” klasöründen erişilebilir. Ve FAT dosya sisteminde yetim dosyaları bulmak zaman alıcıdır. Her küme okunmalı ve analiz edilmelidir ve resim eklendiğinde devre dışı bırakılabilir.

**Yerel Sürücü: Yerel depolama aygıtı (yerel sürücü, USB’ye bağlı sürücü vb.)**

***Yerel Sürücü Ekleme***

Otopsi, yerel bir sürücüyü, başlangıçta bunun bir kopyasını oluşturmayı beklemeden bozabilir. Bu, bir oluşturma engelleyici aracılığıyla USB’ye eklenmiş bir aygıtı bozarken çok değerlidir.

Not: Yenilenmekte olan bir mahalle sürüşünü bozuyorsanız, o noktada Otopsi, bilgi kaynağı olarak ekledikten sonra eklenen belgeleri görmez.

Tüm gadget’ları görmek için Otopsiyi Yönetici olarak çalıştırıyor olmalısınız.

Bir mahalle sürüşü eklemek için:

* Çekme işleminden başlayarak “Yerel Sürücü” seçeneğini seçin.
* Çekme listesinden başlayarak gadget’ı seçin.
* Yetim dosya bulma işlemini gerçekleştirmeyi seçin.

**Mantıksal Dosyalar: Yerel dosyalar veya klasörler.**

***Mantıksal Dosya Ekleme***

Yerel bilgisayarınızda (veya paylaşılan bir sürücüde) bulunan dosya veya klasörleri disk görüntüsüne yerleştirmeden ekleyebilirsiniz. Bu, yalnızca analiz etmek istediğiniz bir dosya koleksiyonunuz varsa kullanışlıdır.

Bunu yaparken dikkat edilmesi gereken bazı noktalar:

* Otopsi, bu şekilde eklediği dosyalardaki zaman damgalarını yok sayar çünkü bunlar, inceleme cihazınıza kopyalandıklarında zaman damgaları olabilirler.
* Analiz etmekte olduğunuz USB’ye bağlı bir cihazınız varsa ve bu yöntemi kullanarak cihazın içeriğini eklemeyi seçerseniz, cihazın ayrılmamış alana veya silinmiş dosyalara bakmayacağını unutmayın. Otopsi sadece tahsis edilen dosyaları görebilecek. Ayrılmamış alanı analiz etmek için cihazı “Mantıksal Sürücü” olarak eklemelisiniz.

Mantıksal dosyalar eklemek için:

* Açılır menüden “Mantıksal Dosyalar”ı seçin.
* “Ekle” düğmesine basın ve eklenecek bir klasöre veya dosyaya gidin. Bir klasör seçmek, tüm içeriğinin (alt klasörler dahil) eklenmesine neden olur.
* Tüm dosya ve klasörler seçilene kadar “Ekle”ye basmaya devam edin.

Panele eklediğiniz tüm dosyalar, ana kullanıcı arayüzünde “LogicalFileSet” adı verilen tek bir veri kaynağında gruplandırılacaktır.

**SONUÇ**

Otopsi Adli Tarayıcısı, gelişmiş bir kriminolojik incelemeye liderlik etmenizi sağlar. The Sleuth Kit ve farklı cihazlar için grafiksel bir arayüzdür. Otopsi, bir sabit sürücüye veya cep telefonuna bakmanıza ve ondan kanıt almanıza izin verir. Bu teknik inceleme, Otopsi’yi kullanmanıza yardımcı olacaktır. Autopsy’nin şu anki sürümü, iyi bir sistem konfigürasyonu ile daha iyi çalışır.