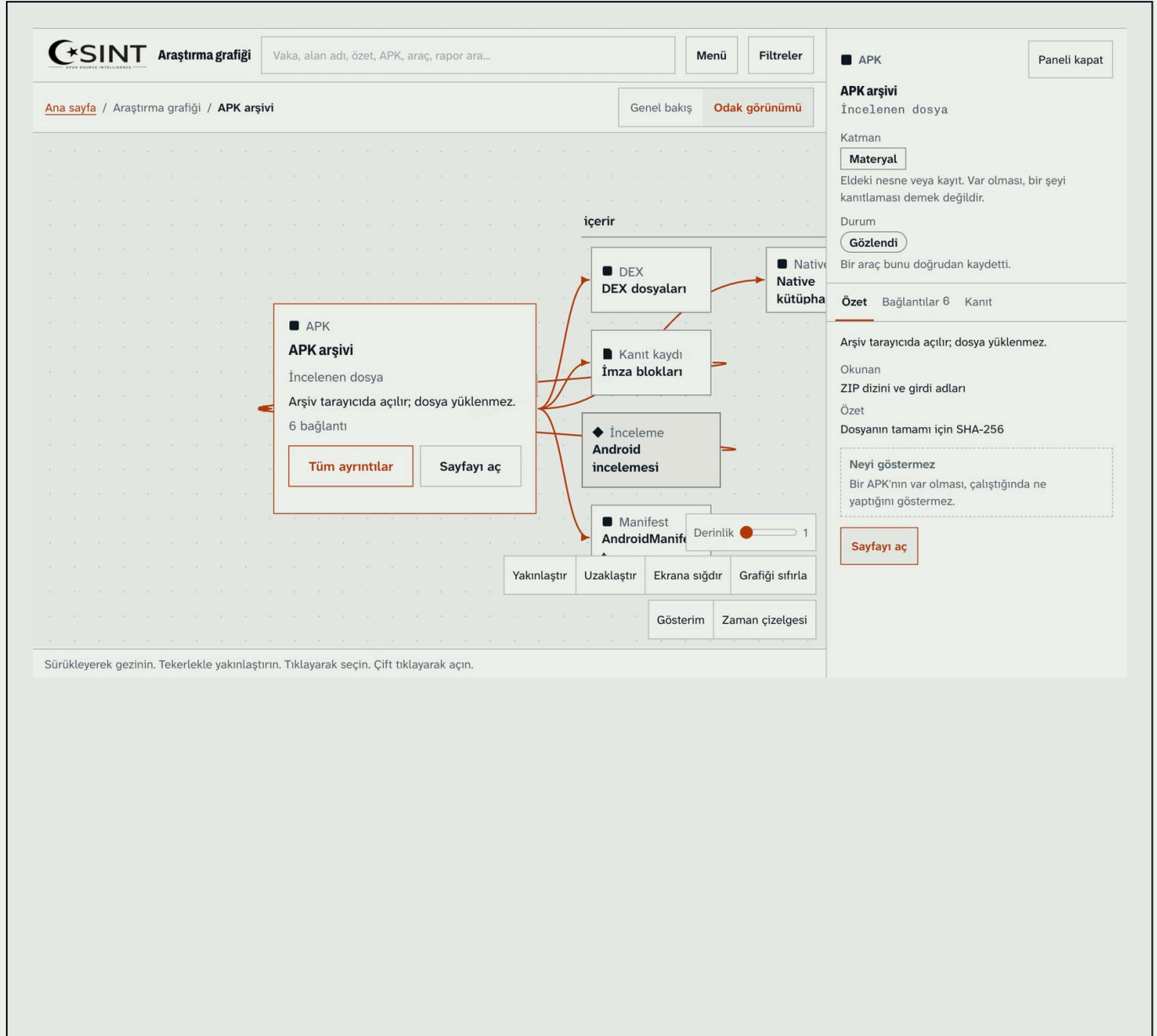




Araştırma grafiği nasıl kuruldu

Araştırma grafiği, sitede yayımladığım incelemeleri, materyalleri, gözlemleri, kanıtları ve yorumları tek bir bağlı haritada gösteriyor. Bu kılavuzda verinin nereden geldiğini, grafiğin nerede kurulduğunu ve katmanları neden ayrı tuttuğumu anlatıyorum.

1 Grafik ne için var

Sitede vaka dosyaları, araçlar, yöntem sayfaları ve inceleme zincirleri ayrı sayfalarda duruyor. Bir APK incelemesinin hangi araçla yapıldığını ya da bir vakanın hangi kaynağa dayandığını görmek için birkaç sayfa gezmek gerekiyordu. Grafik bu bağlantıları tek yerde gösteriyor.

Bir düğüm seçince ona bağlı düğümler açılıyor. Her düğüm hangi katmanda durduğunu ve ne kadar emin olunduğunu yazıyor. Grafik yeni bilgi üretmiyor. Yalnız sitede zaten yayımlanmış olanı birbirine bağlıyor.

Birkaç kelime

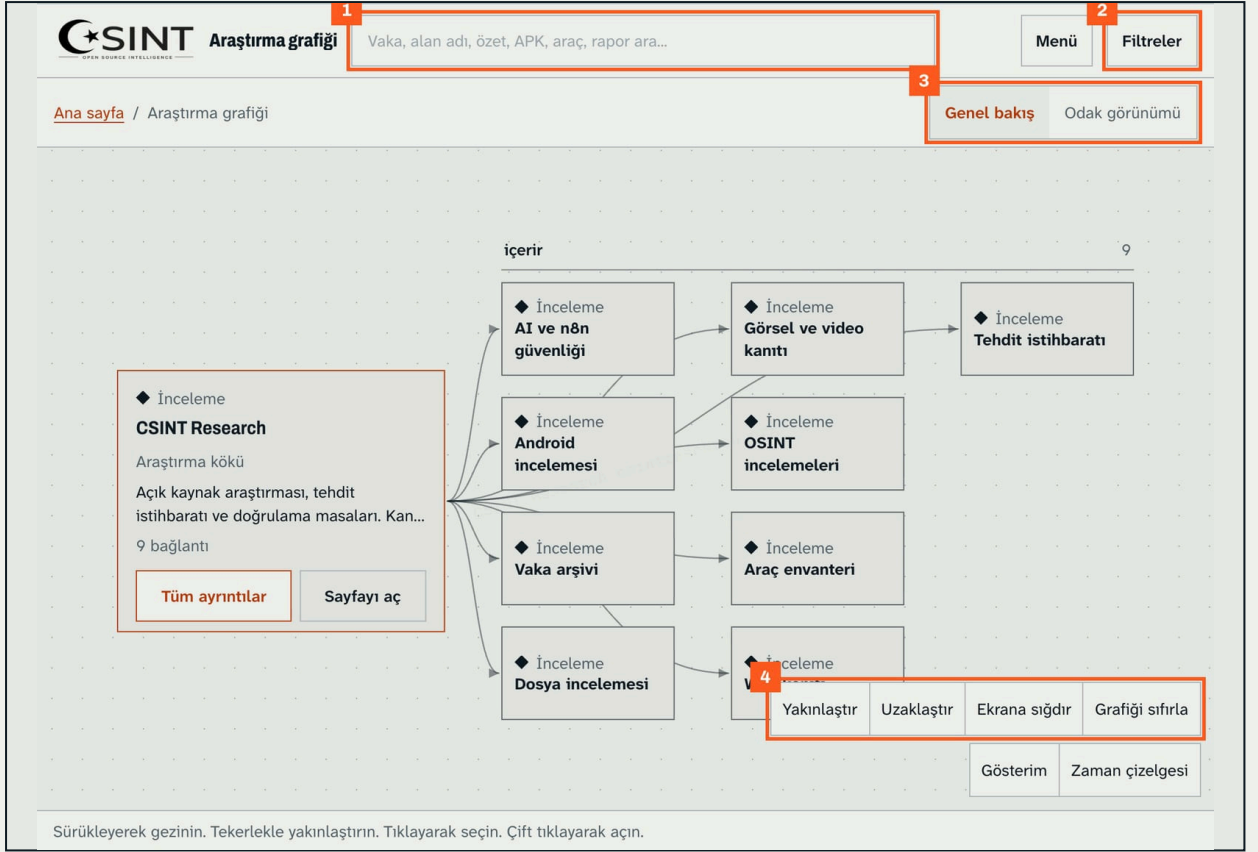
Düğüm	Grafikteki bir kutu. Bir vaka, bir dosya, bir araç, bir kaynak ya da bir bulgu olabilir.
Kenar	İki düğüm arasındaki çizgi. Üzerinde içerir, kullanır, dayanır gibi bir ilişki adı taşır.
Katman	Düğümün zincirdeki yeri. İnceleme, materyal, gözlem, kanıt ya da yorum olabilir.
Kayıt durumu	Bilginin nasıl elde edildiği. Değeri gözlemlendi, çıkarım, kaydedilmedi ya da bilinmiyor olur.

2 Ne nerede çalışır

Grafik tamamen tarayıcıda kurulur. Sayfa açılırken hiçbir sunucuya istek gitmez, tarayıcıya bir şey kaydedilmez ve bir hesap gerekmez.

1. Sitenin kendi verisi Vaka arşivi, araç kataloğu, yöntem grafiği ve elle yazılmış inceleme zincirleri. Hepsi sitenin kaynak kodunda.	2. Derleme Bu veriler statik sitenin içine paketlenir. Ayrı bir veri dosyası indirilmez.	3. Tarayıcı Sayfa açılınca grafik bir kez hesaplanır, düğümler yerleştirilir ve çizilir.	4. Sen Arar, süzer, bir düğüm seçer, ayrıntısını okur ya da bağlı sayfayı açarsın.
Veri kaynağı	Sitede yayımlanmış içerik. Canlı bir akış ya da dış bir servis okunmaz.		
Çizim	Açık kaynaklı React Flow kütüphanesi. Yerleşim sitenin kendi yerleşim kodunda hesaplanır.		
Saklanan	Hiçbir şey. Seçtiğin düğüm ya da süzgeç sayfa yenilenince sıfırlanır.		
Güncelleme	Yeni bir vaka ya da araç yayımlandığında site yeniden derlenir ve grafik kendiliğinden genişler.		

3 Genel bakış



arastirma-grafigi sayfası, genel bakış. Solda araştırma kökü, sağda ana koleksiyonlar.

1 Arama

Vaka, alan adı, özet, APK, araç ya da rapor adıyla arar. Sonuçlar genel bakışta açılır.

2 Süzgeçler

Tür ve katmana göre süzme panelini açar.

3 Görünüm

Genel bakış kökü ve ana koleksiyonları gösterir. Odak görünümü yalnız seçili konuyu ve ona bağlı olanları gösterir.

4 Tuval düğmeleri

Yakınlaştır, uzaklaştır, ekrana sığdır ve sıfırla. Altında gösterim anahtarı ve zaman çizelgesi düğmesi var.

4 Tür ve katman



Süzgeç paneli açık.

1 Türle göre

Yedi grup var. Bunlar inceleme, kişi ve gruplar, teknik materyal, araçlar, altyapı, bulgu ve rapor, kaynak ve kanıt.

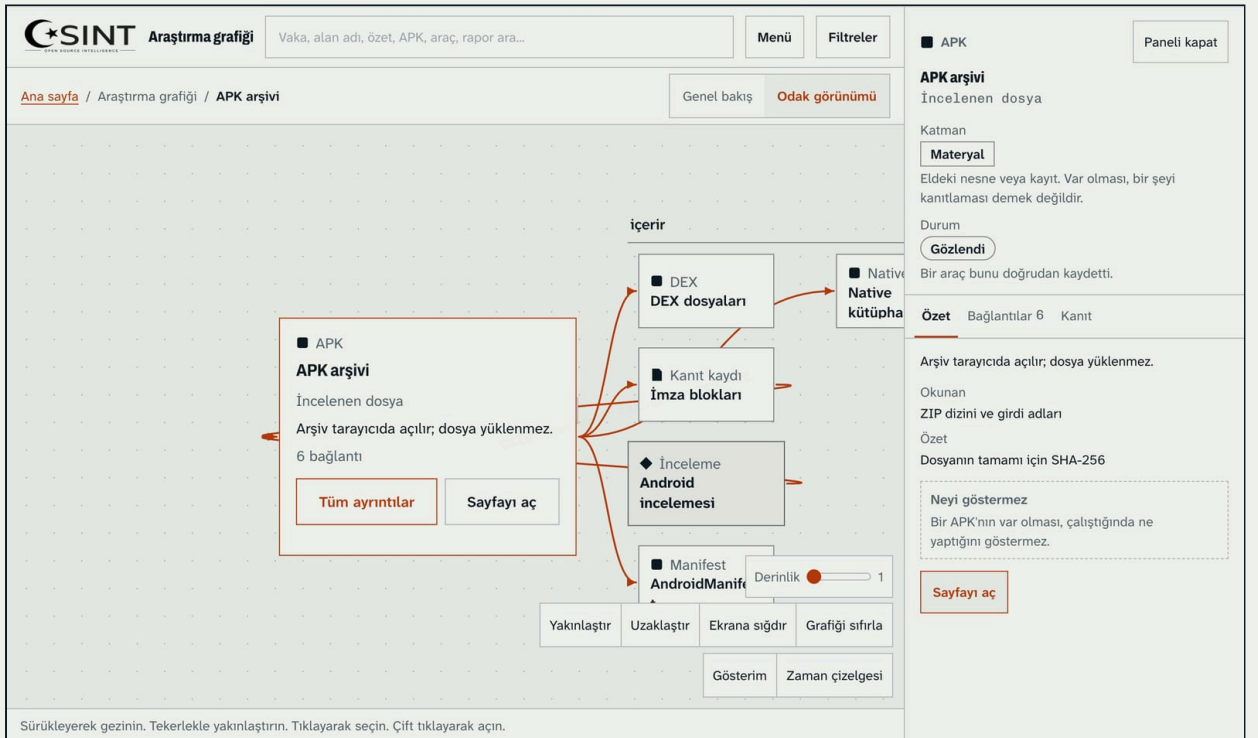
2 Katmana göre

Beş katman var. Okuma sırasıyla inceleme, materyal, gözlem, kanıt ve yorum.

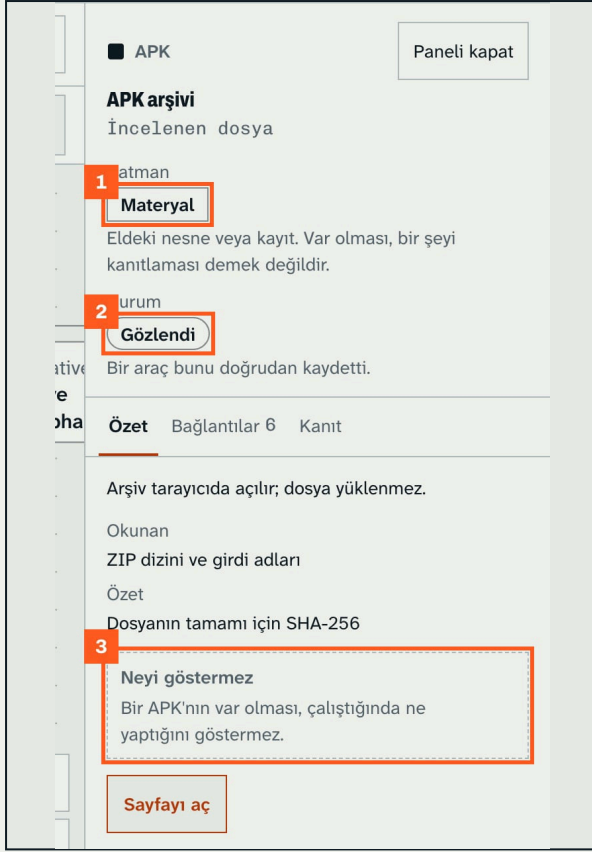
Katmanları bilerek ayrı tuttum. Arayüzdeki hiçbir şey bir düğümü kendiliğinden bir üst katmana taşımaz. Bir aracın kaydettiği şeyin bulguya dönüşmesi analistin kararıdır, çizimin değil.

5 Bir düğümün ayrıntısı

Aşağıdaki örnekte Android incelemesi zincirinde APK arşivi düğümünü seçtim ve tüm ayrıntılarını açtım. Ekran geniş olduğunda panel sağda durur. Dar ekranda alttan açılan bir pencereye dönüşür.



APK arşivi düğümü, odak görünümü ve ayrıntı paneli.



Ayrıntı paneli yakından.

Panelde her zaman özet ve bağlantılar sekmesi var. Düğümün kanıt kaydı varsa kanıt sekmesi, tarihi varsa zaman sekmesi de açılır. Sayfayı aç bağlantısı düğümün geldiği sayfaya gider, burada dosya inceleme aracına.

1

Katman

Bu düğüm materyal katmanında. Yanındaki not, bir nesnenin elde olmasının bir şeyi kanıtladığı anlamına gelmediğini hatırlatıyor.

2

Kayıt durumu

Gözlendi, yani bir araç bunu doğrudan kaydetti. Kaydedilmedi durumu ise yokluk demek değildir, yalnız kaydın olmadığını söyler.

3

Neyi göstermez

Bu alan birçok düğümde var. Burada bir APK'nın var olmasının, çalıştığında ne yaptığını göstermediği yazıyor.

6 Neyi yapmaz

- × Tam bir vaka kaydı değildir. Yalnız sitede yayımlanmış olanı bağlar.
- × Canlı takip yapmaz. Bir kişiyi, alan adını ya da sistemi izlemez, dışarıya sorgu atmaz.
- × Doğruluk garantisi vermez. İki düğüm arasındaki çizgi, ilişkinin kaynağında yazılanı gösterir. İlişkinin doğru olduğunu ayrıca kanıtlamaz.
- × Anahtar kelimedenden bağlantı tahmin etmez. Her kenar verideki yazılı bir ilişkiden gelir.

Grafiği bir içindekiler sayfası gibi kullan. Bir konuyu bul, bağlantılarına bak, sonra asıl sayfasını açıp orada oku.