



IMINT / VISINT

Görsel İstihbarat ve Açık Kaynak Doğrulama

Sade Türkçe başlangıç kitapçığı

EĞİTİM - DOĞRULAMA - GÜVENLİK FARKINDALIĞI

IMINT / VISINT nedir?

IMINT, görüntülerden anlam çıkarmaya odaklanan istihbarat türüdür. VISINT ise fotoğraf, video, kamera kaydı, ekran görüntüsü ve benzeri görsel kaynakların dikkatli incelenmesidir.

Açık kaynak dünyasında bu işin amacı bir kişiyi hedef almak değil, görünen bir iddiayı doğrulamaktır. Görselin nerede, ne zaman ve hangi bağlamda ortaya çıktığı araştırılır.

Yeni başlayan biri için en sağlam kural şudur: Görsel tek başına kanıt değildir. Görsel, kaynak ve bağlamla birlikte değerlendirilince anlam kazanır.

Günlük örnek

Bir haber fotoğrafı aynı gün çok paylaşılmış olabilir. Fakat tersine arama, fotoğrafın yıllar önce başka bir ülkede çekildiğini gösterebilir. Bu durumda görsel gerçek olsa bile iddia yanlış bağlama oturtulmuştur.



Görsel istihbaratı neden önemlidir?

İnternette dolaşan iddiaların büyük bölümü bir görselle güçlendirilir. İnsanlar fotoğrafı görünce olaya daha hızlı inanır. Bu yüzden görsel doğrulama, yanlış bilginin yayılmasını yavaşlatan temel becerilerden biridir.

Görsel inceleme sadece kriz ve haber takibinde kullanılmaz. Güvenlik farkındalığı, eğitim, kurumsal risk analizi ve araştırmacı gazetecilikte de aynı mantık geçerlidir.

İyi bir görsel analizci, gördüğü ilk detaya değil, detayların birbirini destekleyip desteklemediğine bakar.

Günlük örnek

Bir okul yangınına ait olduğu söylenen görüntü paylaşılır. Görseldeki itfaiye aracı, tabela dili ve hava durumu iddia edilen şehirle uyuşmuyorsa şüphe oluşur. Sonuç için tek işaret değil, bütün işaretler birlikte incelenir.



OSINT ile ilişkisi

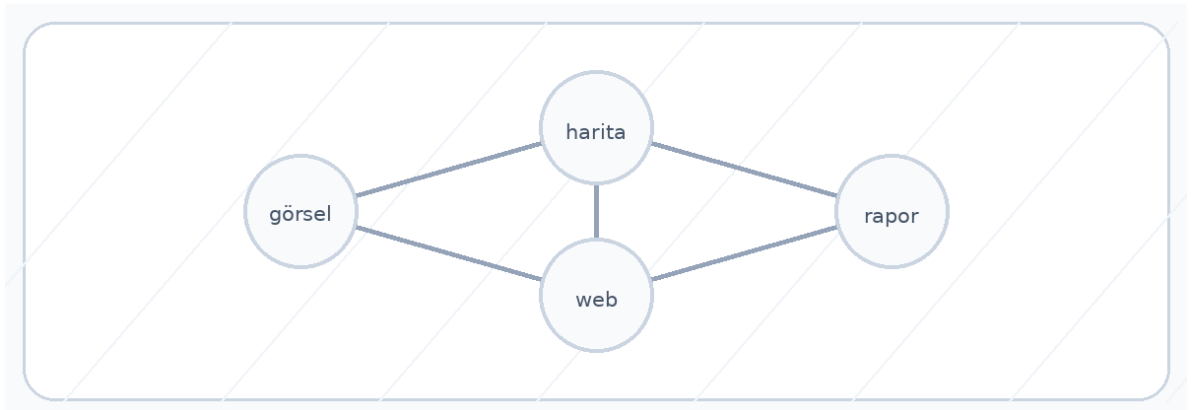
OSINT, açık kaynaklardan bilgi toplama ve doğrulama yaklaşımıdır. IMINT / VISINT bu yaklaşımın görsel tarafıdır. Fotoğraf, video, harita, uydu görüntüsü ve kamera kayıtları bu alanın ana malzemesidir.

Bir görseli incelerken çoğu zaman tek araç yetmez. Harita, hava durumu, haber arşivi, sosyal medya paylaşımı ve resmi açıklamalar birlikte kontrol edilir.

Bu nedenle IMINT, tek başına sihirli bir yöntem değil; açık kaynak araştırmasının parçası olan dikkatli bir doğrulama disiplindir.

Günlük örnek

Bir protesto videosunun yeri araştırılırken önce belirgin binalar bulunur. Sonra OpenStreetMap veya uydu görüntüsüyle sokak yapısı karşılaştırılır. En son aynı gün oradan gelen başka güvenilir paylaşımlar aranır.



Bir görsel nasıl analiz edilir?

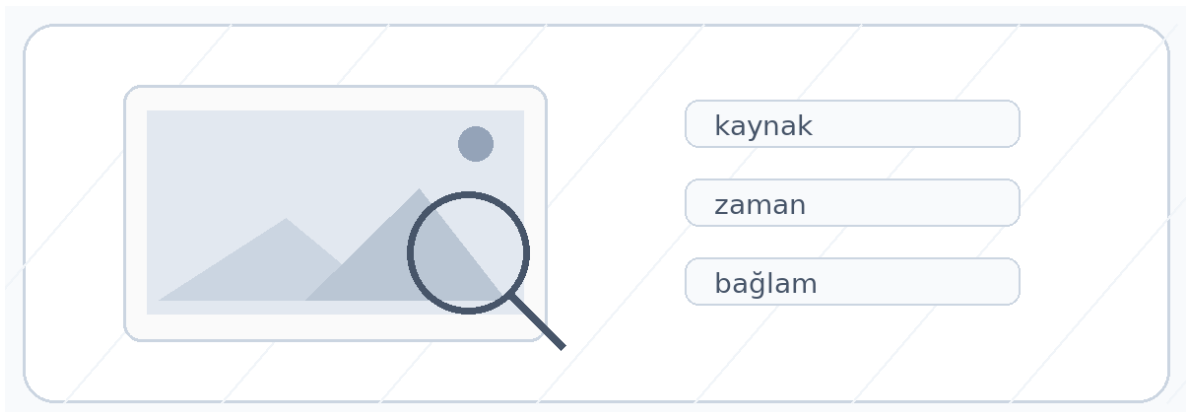
İlk bakışta görselin “ne söylediğine” değil, “ne gösterdiğine” odaklanmak gerekir. Kadraj, ışık, yazılar, yollar, bina çizgileri, gölgeler, araçlar ve arka plandaki küçük detaylar not edilir.

Sonra görselin kaynağına bakılır. İlk kim paylaşmış, daha eski kopya var mı, açıklama metni sonradan mı eklenmiş, aynı görsel başka olaylarda kullanılmış mı?

Analizin sonunda kesinlik derecesi açık yazılır. “Doğrulandı”, “uyumlu görünüyor”, “bağımsız doğrulanamadı” gibi ifadeler araştırmayı daha dürüst yapar.

Günlük örnek

Bir fotoğrafta mağaza tabelası, yol çizgisi ve yağmurlu hava görülüyor. Bu üç detay aynı şehir, aynı cadde ve aynı tarih ile uyuyorsa iddia güçlenir. Yine de tek başına yeterli sayılmaz.



Reverse image search mantığı

Tersine görsel arama, bir görselin internetteki benzerlerini veya eski kopyalarını bulmaya çalışır. Amaç, görselin ilk bağlamına yaklaşımdır.

Arama motorları bazen aynı görseli bulur, bazen sadece benzer sahneleri getirir. Bu yüzden sonuçlar doğrudan kanıt gibi değil, araştırma ipucu gibi okunmalıdır.

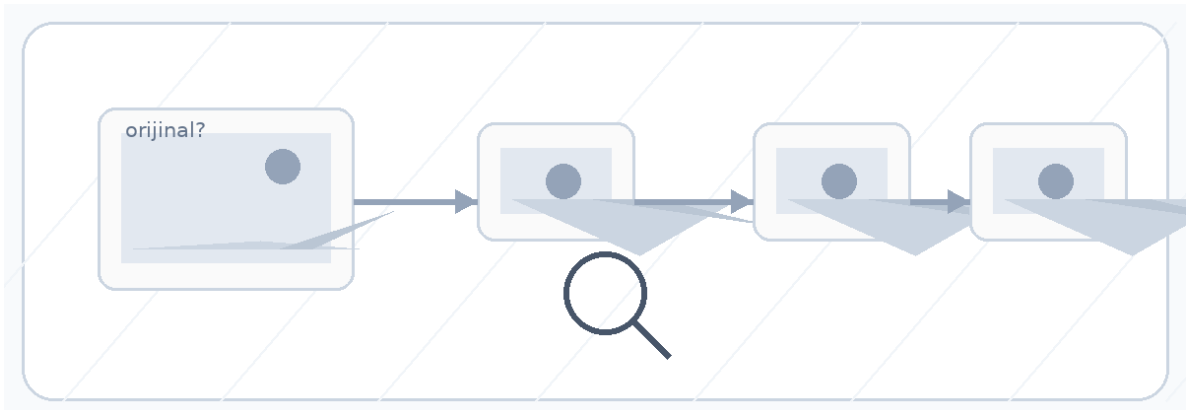
En iyi sonuç için görselin tamamı yanında belirgin kareler de denir. Videolarda birkaç net frame çıkarıp ayrı ayrı aramak daha sağlıklı olabilir.

Günlük örnek

Bir patlama görüntüsü yeniymiş gibi paylaşılır. Tersine arama, aynı karenin iki yıl önce başka bir olayda kullanıldığını gösterirse iddia zayıflar. Görsel gerçek olsa bile zaman bilgisi yanlış olabilir.

Küçük yöntem notu

Görseli indir, net bir kare seç, birkaç arama motorunda dene ve en eski güvenilir kaynağı ara. Sonuçları tarih ve bağlamla karşılaştı.



Google Lens, Yandex ve Bing kullanımı

Google Lens, Yandex Images ve Bing Visual Search benzer amaçla kullanılır ama aynı sonuçları vermez. Bir araç sonuç bulamadığında diğerinin bulması normaldir.

Google Lens nesne, ürün ve yer tanımda güçlü olabilir. Yandex bazı görsel benzerliklerde iyi sonuç verebilir. Bing ise özellikle web üzerindeki benzer görselleri hızlıca gösterebilir.

Araçların sonucu kesin hüküm değildir. Arama sonucu yalnızca yeni bir kapı açar; güvenilirlik kontrolü yine araştırmacıya kalır.

Günlük örnek

Bir fotoğraftaki heykel veya bina, Lens ile benzer görseller üzerinden bulunabilir. Sonra aynı yapının haritadaki konumu kontrol edilir. Bulunan yer ile iddia edilen yer farklıysa bu açıkça rapora yazılır.



Metadata (EXIF) nedir?

Metadata, dosyanın içinde veya yanında duran teknik bilgidir. Fotoğrafın çekim tarihi, cihaz modeli, çözünürlük, yazılım bilgisi ve bazı durumlarda konum bilgisi buna örnektir.

EXIF, fotoğraflarda sık görülen metadata türlerinden biridir. Ancak sosyal medya platformları yüklenen görsellerin metadata bilgisini çoğu zaman temizler veya değiştirir.

Bu yüzden metadata faydalıdır ama her zaman bulunmaz. Bulduğunda bile tek başına kesin kanıt sayılmamalıdır; görsel içerikle ve kaynak bilgisiyle birlikte okunmalıdır.

Günlük örnek

Bir fotoğraf dosyasında cihaz modeli ve çekim saati görünebilir. Fakat dosya mesajlaşma uygulamasından geçtiyse bu bilgi silinmiş olabilir. Silinmiş metadata, görselin sahte olduğu anlamına gelmez.

Araç kutusu

ExifTool gibi araçlar dosyadaki teknik bilgileri okumaya yarar. Kullanımda en önemli nokta, dosyanın orijinal kopyasıyla çalışmak ve sonucu bağlamdan koparmamaktır.



Metadata'dan hangi bilgiler çıkabilir?

Metadata bazen çekim zamanı, kamera ayarı, yazılım izi, dosya oluşturma tarihi veya GPS koordinatı gösterebilir. Bu bilgiler araştırmayı hızlandırabilir.

Fakat metadata kolayca silinebilir, değişebilir veya kopyalama sırasında bozulabilir. Bu nedenle metadata "kesin gerçek" değil, doğrulanması gereken teknik işarettir.

Gizlilik açısından da dikkat gerekir. Başkasına ait dosyalarda kişisel verileri yaymak doğru değildir. Eğitim ve raporlama sırasında gereksiz kişisel bilgi maskelenmelidir.

Günlük örnek

Bir görselin EXIF alanında GPS bilgisi varsa haritada kontrol edilir. Ama aynı görselin başka kaynaklarda daha eski kopyaları da aranır. Konum bilgisi tek başına araştırmayı bitirmez.



Görsellerde konum analizi

Konum analizi, görseldeki sabit unsurları harita ve açık kaynaklarla karşılaştırma işidir. Bina cephesi, yol şekli, tabela, dağ çizgisi, kıyı hattı ve elektrik direği gibi detaylar işe yarar.

En güvenli yaklaşım, değişmesi zor işaretlere ağırlık vermektir. Reklam afişleri veya geçici panolar hızla değişebilir; bina, kavşak ve doğal şekiller daha dayanıklı ipuçlarıdır.

Konum doğrulaması yapılırken özel kişilerin adresini ifşa etmekten kaçınılmalıdır. Kamu yararı yoksa hassas yer bilgisi paylaşılmaz.

Günlük örnek

Bir videoda dar bir sokak, sarı bir bina ve karşıda minare görünüyor. Haritada benzer sokak yapısı bulunur, sonra bina rengi ve görüş açısı kontrol edilir. Uyum varsa “konumla uyumlu” denir; kesinlik abartılmaz.



Gölge, hava ve zaman analizi

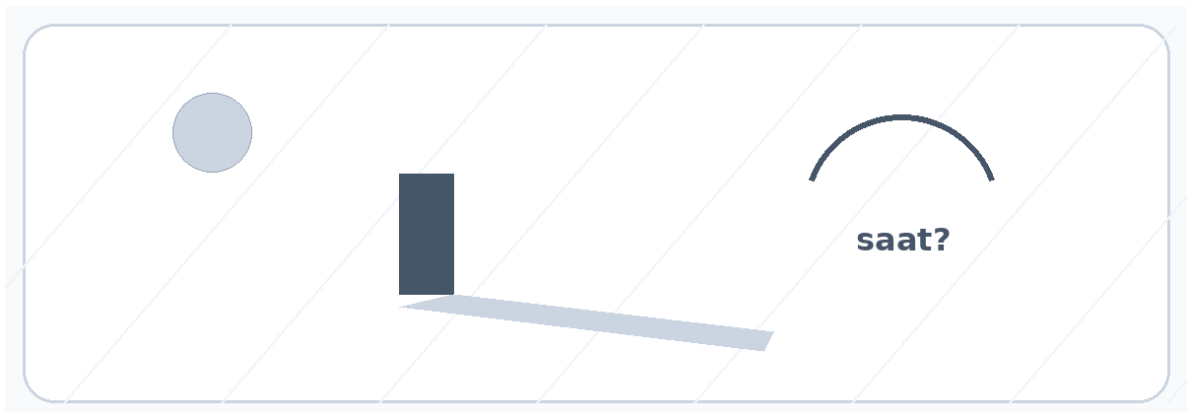
Gölge yönü, güneşin konumu hakkında fikir verebilir. Bu da görselin yaklaşık saatini veya iddia edilen zamanla uyumunu kontrol etmeye yardımcı olur.

Hava durumu da önemli bir ipucudur. Yağmur, kar, sis, bulut yoğunluğu ve zemin ıslaklığı olayın anlatılan tarihle uyuşup uyuşmadığını gösterebilir.

Bu analizler hassastır ve hata payı taşır. Gölge tek başına karar verdirmez; harita, hava raporu, kaynak tarihi ve diğer görsellerle birlikte değerlendirilir.

Günlük örnek

Bir fotoğraf öğle saatinde çekildi deniyor ama gölgeler çok uzun görünüyor. Bu, iddiayı otomatik çürütmez; mevsim, konum ve güneş açısı kontrol edilmeden kesin sonuç yazılmaz.



Kıyafet ve obje analizi

Kıyafet, çanta, tabela, cihaz, arma, yol levhası ve küçük nesnelere görselin bağlamı hakkında ipucu verebilir. Ama bu tür detaylar kolayca yanlış yorumlanabilir.

Marka veya model benzerliği, kişiyi veya yeri kesin olarak belirlemez. Aynı ürün birçok ülkede satılabilir, benzer kıyafet çok sayıda kişide bulunabilir.

Bu bölümde amaç kişiyi hedef göstermek değil, olayın bağlamını doğrulamaktır. Özel hayatı ilgilendiren ayrıntılar gereksizse rapora alınmamalıdır.

Günlük örnek

Bir fotoğraftaki okul arması veya yerel otobüs kartı, şehir hakkında ipucu verebilir. Ancak bu bilgi bir kişinin kimliğini açığa çıkarmak için kullanılmamalıdır. İpucu sadece iddiayı doğrulama amacıyla değerlendirilir.



Araç modeli ve plaka inceleme mantığı

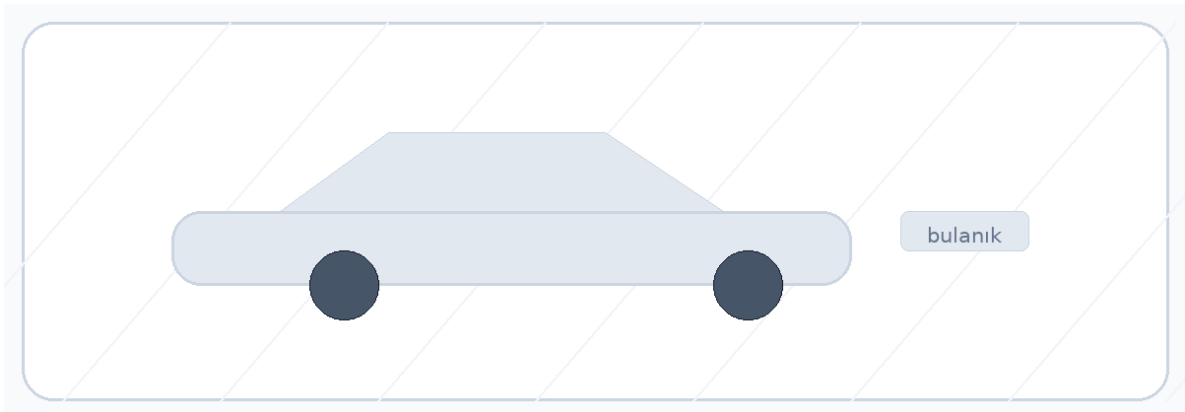
Araçlar görsel doğrulamada sık görülür. Far yapısı, gövde çizgisi, renk, taksit işareti, yol kullanımı veya resmi araç işareti yer ve zaman hakkında ipucu verebilir.

Plaka gibi kişisel veya hassas bilgiler özel dikkat ister. Eğitim ve raporlama sırasında tam plaka paylaşmak yerine maskeleye tercih edilir.

Araç analizi, güvenli kullanımda olay bağlamını anlamaya yarar. Bir kişiyi takip etmek, hedef göstermek veya özel hayatına ulaşmak için kullanılmamalıdır.

Günlük örnek

Bir olay fotoğrafında aracın direksiyon tarafı, yol çizgileri ve taksit rengi ülke hakkında fikir verebilir. Tam plaka okunuyorsa raporda maskelenir; gerekli değilse hiç yazılmaz.



Sosyal medya görselleri nasıl incelenir?

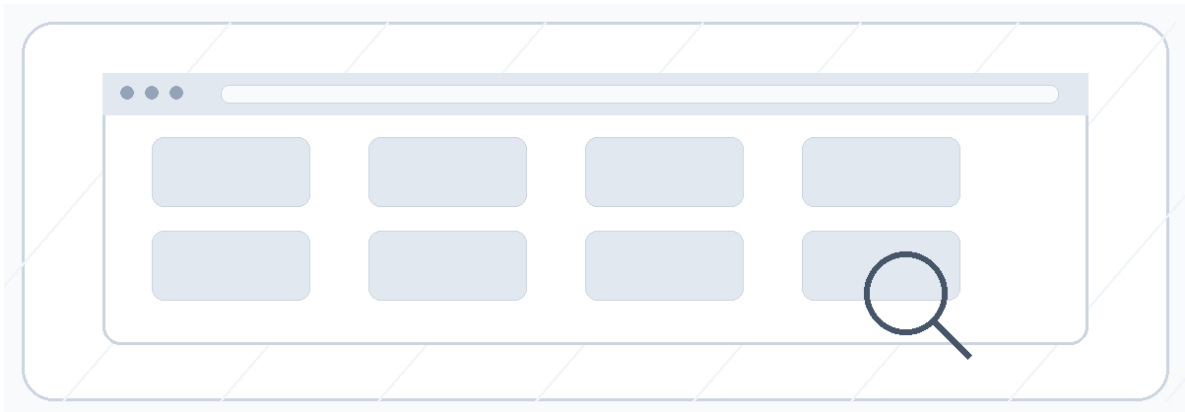
Sosyal medyadaki görseller çoğu zaman bağlamından kopar. Açıklama metni, paylaşım zamanı, yorumlar, eski gönderiler ve aynı görselin başka platformlardaki kopyaları birlikte kontrol edilmelidir.

Platformlar görselleri sıkıştırabilir ve metadata bilgisini silebilir. Bu nedenle sosyal medya ekran görüntüsü yerine mümkünse orijinal paylaşım bağlantısı ve arşiv kaydı saklanır.

Kişisel hesaplar incelenirken sınır net olmalıdır. Herkese açık bilgi bile sınırsız kullanım hakkı vermez; gereksiz kişisel ayrıntılar rapora taşınmaz.

Günlük örnek

Bir kullanıcı aynı fotoğrafı “bugün” diye paylaşır. Başka bir platformdaki eski paylaşım, fotoğrafın daha önce çekildiğini gösterebilir. Bu durumda fotoğraf değil, fotoğrafın yeniymiş gibi sunulması sorunludur.



Uydu görüntüsü ve harita analizi

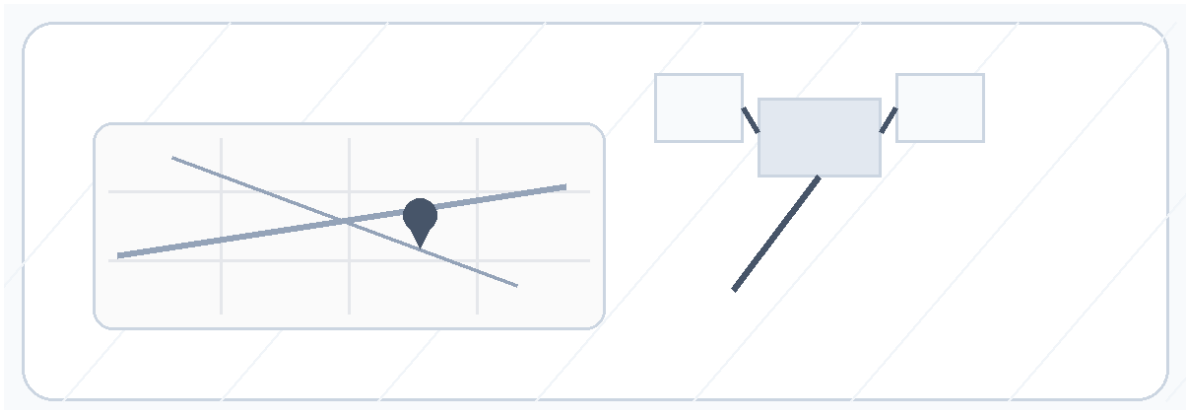
Uydu görüntüleri geniş alanları karşılaştırmak için kullanılır. Yol ağları, tarla sınırları, bina dizilimi, kıyı çizgisi ve arazi yapısı görsel konumlandırmada yardımcı olur.

NASA Earthdata, Sentinel Hub, Copernicus kaynakları ve OpenStreetMap gibi servisler farklı amaçlara hizmet eder. Bazıları güncel görüntü sunar, bazıları tarihsel karşılaştırma için daha uygundur.

Uydu görüntüsünde çözünürlük, tarih ve bulutluluk mutlaka kontrol edilir. Yanlış tarihli görüntüyle yapılan karşılaştırma hatalı sonuca götürebilir.

Günlük örnek

Bir köprü hasarı iddiası incelenirken önce haritadaki köprü yapısı bulunur. Sonra olay tarihine yakın uydu görüntüsü aranır. Görüntünün tarihi eskiyse sonuç “bu görüntü olay gününü göstermiyor” diye not edilir.



Deepfake ve yapay görselleri anlama

Yapay görseller ve deepfake içerikler giderek daha inandırıcı hale geliyor. Bu nedenle sadece “göze garip geldi” demek yeterli değildir.

Tutarsız ışık, anormal yansıma, bozuk yazı, şekil devamlılığında hata ve kaynak geçmişinin zayıf olması şüphe işaretidir. Fakat bu işaretler tek başına kesin kanıt değildir.

En sağlıklı yaklaşım, içeriğin ilk kaynağını, paylaşım zincirini ve bağımsız doğrulamasını aramaktır. Görselin yapay olup olmadığı kadar hangi iddiayı desteklemek için kullanıldığı da önemlidir.

Günlük örnek

Bir liderin konuşma yaptığı kısa video paylaşılır. Dudak hareketi garip görünüyorsa bu sadece şüphedir. Aynı konuşmanın resmi kaydı, haber ajansları ve orijinal yükleme zamanı kontrol edilmeden kesin hüküm verilmez.



Manipüle edilmiş görseller nasıl fark edilir?

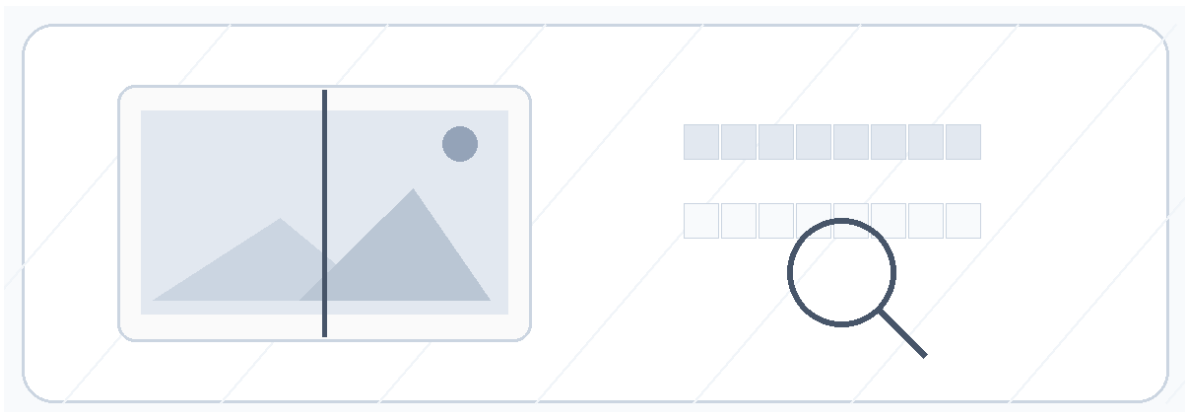
Manipülasyon bazen çok basittir: kırpma, renk değişimi, eski görseli yeni gibi sunma veya açıklama metnini değiştirme. Her manipülasyon gelişmiş montaj olmak zorunda değildir.

Daha teknik işaretler arasında keskinlik farkı, ışık yönü uyumsuzluğu, tekrar eden desenler, bozuk kenarlar ve doğal olmayan gölgeler sayılabilir.

Yine de görsel hata analizi tek başına yeterli değildir. Aynı sahnenin başka açılardan görüntüleri, kaynak geçmişi ve güvenilir haber kayıtlarıyla karşılaştırma yapılmalıdır.

Günlük örnek

Bir kalabalık fotoğrafı daha büyük görünmesi için dar açıyla kırılmış olabilir. Geniş açıdaki başka bir görüntü, kalabalığın aslında sınırlı bir alanda olduğunu gösterebilir. Bu da görselin bağlamını değiştirir.



Kanıt toplama ve arşivleme

İyi araştırma, sadece bulmak değil, bulguyu sonradan anlaşılır şekilde saklamaktır. Bağlantı, ekran görüntüsü, arşiv kaydı, tarih, saat ve kısa açıklama birlikte tutulmalıdır.

Ekran görüntüsü tek başına zayıf kalabilir; çünkü kolayca düzenlenebilir. Bu yüzden mümkünse orijinal bağlantı, arşiv bağlantısı ve dosyanın hash değeri de not edilir.

Delil toplarken kişisel veri minimizasyonu önemlidir. Gerekli olmayan isim, plaka, yüz, telefon ve adres bilgileri maskelenir.

Günlük örnek

Bir paylaşım yanlış bilgi içeriyor gibi görünüyorsa bağlantı kaydedilir, tarih ve saat not edilir, arşivlenir ve iddiayı gösteren ekran görüntüsü alınır. Rapor gereksiz kullanıcı bilgileri kapatılır.

Basit kayıt düzeni

Kaynak bağlantısı, erişim zamanı, arşiv bağlantısı, kısa açıklama ve doğrulama durumu aynı satırda tutulursa rapor sonradan çok daha kolay kontrol edilir.



Etik ve hukuki sınırlar

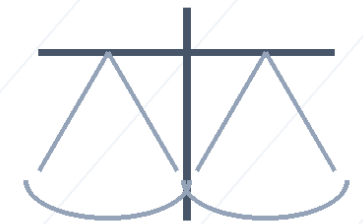
IMINT / VISINT çalışması, başkalarının mahremiyetini ihlal etme hakkı vermez. Açık kaynak bilgi, sınırsız kullanım izni anlamına gelmez.

Kişisel veriler, yüzler, adresler, plakalar ve çocuklara ait görüntüler daha dikkatli ele alınmalıdır. Kamu yararı yoksa hassas bilgi toplanmaz, paylaşılmaz ve rapora eklenmez.

Hukuki sınırlar ülkeye göre değişebilir. Türkiye için KVKK, Avrupa Birliği için GDPR gibi kişisel veri kuralları dikkate alınmalıdır. Şüpheli durumda hukuki danışmanlık alınmalıdır.

Günlük örnek

Bir olayın yerini doğrulamak için bina cephesi yeterliyse apartman sakininin adı, kapı numarası veya araç plakası rapora konmaz. Doğrulama için gerekmeyen ayrıntı, risk üretir.



mahremiyet + doğrulama

Sonuç ve kaynakça

IMINT / VISINT, iyi soru sorma ve sabırlı doğrulama işidir. Bir fotoğrafın etkileyici olması, doğru bağlamda kullanıldığı anlamına gelmez.

Sağlam çalışma; kaynağı bulur, zamanı kontrol eder, konumu sınır, metadata varsa dikkatle okur ve sonucu abartmadan raporlar. En önemlisi, araştırma yapılırken insanların güvenliği ve mahremiyeti korunur.

Kapanış notu

Bu kitapçık başlangıç rehberidir. Gerçek vakalarda tek araçla karar vermek yerine, bağımsız kaynaklarla çapraz kontrol yapmak ve emin olunmayan noktaları açıkça belirtmek gerekir.

Başlangıç için güvenilir kaynaklar

Bellingcat Guides

<https://www.bellingcat.com/category/resources/how-tos/>

Bellingcat video verification

<https://www.bellingcat.com/resources/how-tos/2017/06/30/advanced-guide-verifying-video-content/>

Google Fact Check Tools

<https://toolbox.google.com/factcheck>

Google Lens

<https://lens.google/>

Yandex Images

<https://yandex.com/images/>

Bing Visual Search

<https://www.microsoft.com/en-us/bing/visual-search>

ExifTool

<https://exiftool.org/>

InVID Verification Plugin

<https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

Amnesty / Citizen Evidence YouTube DataViewer

<https://citizenevidence.org/2014/07/01/youtube-dataviewer/>

NASA Earthdata

<https://www.earthdata.nasa.gov/>

NASA Worldview

<https://worldview.earthdata.nasa.gov/>

Sentinel Hub

<https://www.sentinel-hub.com/>

OpenStreetMap

<https://www.openstreetmap.org/>

Verification Handbook

<https://verificationhandbook.com/>

Verification Handbook 3

<https://datajournalism.com/read/handbook/verification-3>

EU Data Protection / GDPR

https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

KVKK

<https://www.kvkk.gov.tr/>