EKRAN GÖRÜNTÜSÜ ADLİ DELIL OLARAK NE KADAR GÜVENİLİR?

Metadata Yokluğu, Manipülasyon Riski ve Doğrulama Standartları

Söyleşi / Interview

Dr. Burak Olgun
burakolgun@soluitonhome.net
Solution Home Bilişim Tekn.ve Dan.Hizm., İstanbul.

Anahtar Kelimeler: *Ekran Görüntüsü • Dijital Delil • Metadata • Manipülasyon • Doğrulama*

ÖZET

Ekran görüntüsü (screenshot), günümüzün en yaygın dijital delil türlerinden biri haline gelmiştir. Mesajlaşma uygulamaları, sosyal medya paylaşımları ve e-posta yazışmaları; çoğunlukla ekran görüntüsü biçiminde mahkeme süreçlerine taşınmaktadır. Ancak standart bir ekran görüntüsü, içeriğin orijinal kaynağından bağımsız olarak yakalanan bir piksel kümesidir ve kriptografik bütünlük, özgün metadata ya da doğrulanabilir zaman damgası barındırmaz. Bu yapısal eksiklik, ekran görüntüsünü manipülasyona son derece açık kılar. Bu söyleşide, ekran görüntüsünün teknik yapısı, sahtecilik yöntemleri, mevcut doğrulama teknikleri ve uluslararası hukuki kabul standartları incelenmektedir.

Anahtar Kelimeler: *ekran görüntüsü, dijital delil, metadata, kriptografik hash, manipülasyon, adli bilişim, doğrulama, zaman damgası*

EDİTÖR NOTU: Bu söyleşi, ekran görüntüsünün adli delil olarak sunulmasında karşılaşılan teknik sorunları bağımsız bir adli bilişim uzmanının perspektifinden ele almaktadır. Herhangi bir davaya ya da kişiye doğrudan atıf yapılmamış; amaç teknik farkındalık oluşturmaktır.

I. Ekran Görüntüsünün Teknik Yapısı

SORU: Standart bir ekran görüntüsü teknik açıdan ne içerir, ne içermez?

Bu soruyu yanıtlamak, pek çok yanlış anlamanın önüne geçer. Bir ekran görüntüsü, işletim sisteminin belirli bir anda ekranda görünen pikselleri bir görüntü dosyasına (PNG, JPEG vb.) dönüştürmesiyle oluşur. Bu dosya yalnızca **görünen piksel bilgisini** içerir.

Ne içermez? Orijinal mesajın sunucu tarafı zaman damgasını içermez. Gönderenin kimliğini kriptografik olarak doğrulayan hiçbir veri içermez. Mesajın gerçekten o hesaptan o kişi tarafından gönderildiğini kanıtlayan meta bilgi içermez. İçeriğin hiç değiştirilmemiş olduğuna dair doğrulanabilir bütünlük kanıtı içermez. Burgess Forensics (2025) bu durumu açıkça ifade etmektedir: 'Ekran görüntüleri zayıf delildir; ancak adli yöntemlerle elde edilen veriler çok daha ikna edici ve kabul edilebilir olurdu.'

Metadata Perspective (2025) de bu ayrımı netleştiriyor: Kamera ile çekilen bir fotoğraf, cihaz bilgisini, GPS koordinatını ve kesin çekim zamanını içeren EXIF metadata barındırır. Bunlar doğrulanabilir izler bırakır. Ekran görüntüsü ise yeni bir dosyadır; orijinal içeriğin metadata'sı bu yeni dosyaya taşınmaz.

TEMEL SORUN: *Bir ekran görüntüsü, içeriğin orijinal kaynağından kopuk bir kopyasıdır. Kaynakla bağlantısı doğrulanamaz; bu yapısal bir sınırlılıktır, kullanıcı hatası değil.*

SORU: Ekran görüntüsü ne kadar kolaylıkla manipüle edilebilir?

Son derece kolaylıkla. Ve bu çarpıcı bir gerçek çünkü görsel inceleme bu manipülasyonu çoğunlukla tespit edemez. Birkaç somut yöntem: Metin düzenleyicilerle metin baloncukları değiştirilebilir, tarih-saat bilgileri silinebilir ya da değiştirilebilir. Fotoğraf düzenleme yazılımlarıyla görüntü içeriği piksel düzeyinde değiştirilebilir. Geliştiricinin araçlarıyla (tarayıcı inspect element) bir web sayfasının görüntüsü değiştirilerek ekran görüntüsü alınabilir. Yeniden sıkıştırma yoluyla değiştirilen alanlar gizlenebilir.

TrueScreen (2026) bu konuyu mahkeme perspektifinden ele alarak Sedona Conference'a atıfla şunu vurguluyor: Ekran görüntüleri 'eksik ve hatalı veri yakalamaları' oluşturur ve bunlar yalnızca bir tanığın kişisel bilgisine dayalı olarak doğrulanabilir. Bu, adli bir doğrulama yöntemi değildir.

Hata Düzeyi Analizi (Error Level Analysis — ELA) ve klon tespit algoritmaları gibi adli teknikler bazı manipülasyonları ortaya çıkarabilir; ancak bu tekniklerin etkinliği sınırlıdır. Özellikle bütünsel düzenlemeler ya da yeniden sıkıştırma uygulandığında tespit güçleşir.

II. Doğrulama Yöntemleri ve Standartlar

SORU: Bir ekran görüntüsünü mahkeme açısından güvenilir hale getirmek teknik olarak mümkün müdür?

Evet, mümkündür; ancak bu doğrulanmış bir ekran görüntüsü, sıradan bir ekran görüntüsünden teknik olarak *tamamen farklı* bir süreçle elde edilir. TrueScreen (2026) ve adli bilişim standartları üç temel gereksinimi ortaya koymaktadır:

1. Kriptografik hash (SHA-256): Görüntünün yakalandığı anda SHA-256 gibi güçlü bir kriptografik özet değeri hesaplanır ve bağımsız olarak kaydedilir. Bu değer daha sonra değişmezlik kontrolü için kullanılabilir.

2. Nitelikli zaman damgası: Tanınmış bir sertifikasyon otoritesi tarafından sağlanan zaman damgası, görüntünün yakalandığı anı kriptografik olarak belgeler. AB'deki eIDAS yönetmeliği (EU 910/2014) ve güncellenmiş eIDAS 2.0 (Mayıs 2024) bu konuda standart çerçeve sunar.

3. Adli araçla doğrudan kaynak extraksiyon: Cihazdan ya da bulut hesabından Cellebrite, Magnet AXIOM veya Oxygen Forensics gibi adli araçlarla doğrudan veri çekimi yapıldığında, tam metadata ve bütünlük kaydı korunur. Bu yöntemle elde edilen veri, ekran görüntüsünden çok daha güçlü bir delil oluşturur.

ALTIN KURAL: *Bir ekran görüntüsü delil olarak sunulacaksa, kriptografik hash + nitelikli zaman damgası + adli zincir muhafazası üçlüsü aranmalıdır. Bunlardan yoksun ekran görüntüsü güçlü itirazla karşılaşabilir.*

SORU: WhatsApp, Telegram gibi mesajlaşma uygulamalarındaki konuşmaların ekran görüntüsü delil olarak nasıl değerlendirilmeli?

Bu tür platformlar uçtan uca şifreleme kullandığından, mesaj içeriğine sunucu tarafından erişim çoğu durumda mümkün değildir. Bu gerçek, ekran görüntüsünü bazen tek pratik kayıt yöntemi haline getirir; ancak bu zorunluluk, ekran görüntüsünün teknik sınırlılıklarını ortadan kaldırmaz.

Doğrulanmamış bir WhatsApp ekran görüntüsü, savunma tarafından şu sorularla kolayca itirazla karşılaşabilir: Görüntünün alındığı cihaz incelendi mi? Görüntü dosyasının hash değeri mevcut mu? Zaman damgası doğrulandı mı? Uygulamanın sunucusundan ya da cihazından adli çekimle elde edilen verilerle karşılaştırma yapıldı mı? Bu soruların yanıtsız kalması, delil gücünü önemli ölçüde zayıflatır.

III. Uluslararası Hukuki Çerçeve

SORU: Farklı yargı çevrelerinde ekran görüntüsünün delil olarak kabul edilmesi için hangi koşullar aranıyor?

ABD Federal Delil Kuralları'nın 901(a) maddesi, sunulan her delilin *ne olduğunun* kanıtlanmasını zorunlu kılar; ekran görüntüleri için bu, içeriğin doğruluğunun tanık beyanı veya teknik kanıtla desteklenmesi anlamına gelir. 702. madde ise uzman tanıklığının güvenilir metodolojiye dayanmasını şart koşar.

AB'de eIDAS 2.0 çerçevesinde elektronik belgeler; nitelikli elektronik imza, nitelikli zaman damgası ya da elektronik mühür taşıdıklarında yasal geçerlilik kazanır. Standart bir ekran görüntüsü bu özellikleri doğası gereği barındırmaz.

Türk hukukunda CMK 217. maddesi delillerin hukuka uygun elde edilmesini şart koşar; dijital delillerin doğruluğuna yönelik itiraz hakkı ise sanığın temel güvencesidir. Ekran görüntüsünün herhangi bir doğrulama mekanizması olmaksızın delil olarak sunulması, bu güvenceyi fiilen işlevsiz kılabilir.

SORU: Son olarak: Ekran görüntüsü hiç güvenilir bir delil olamaz mı?

'Hiç' kelimesini kullanmak doğru olmaz. Doğru bağlamda, destekleyici delillerle birlikte ve sınırlılıkları açıkça beyan edilerek kullanılan bir ekran görüntüsü, delil havuzuna katkı sunabilir.

Ancak tek başına, doğrulama mekanizması olmaksızın, özellikle ağır suçlamalarda birincil delil olarak sunulan bir ekran görüntüsü, ciddi metodolojik sorunlar barındırır. Mahkemenin ve bilirkişinin bu sınırlılıkları değerlendirmesi; hem doğru kararlar alınması hem de olası yargısal hatalardan kaçınılması açısından kritik öneme sahiptir.

— Söyleşi Sonu —

Kaynakça

Burgess, S. (2025). Screenshots are barely evidence: How to authenticate digital data in court. Burgess Forensics. https://burgessforensics.com/screenshots-are-barely-evidence-how-to-authenticate-digital-data-in-court/

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

European Union. (2014). Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union.

Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLOS ONE, 20(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

Metadata Perspective. (2025). Metadata matters: Camera original photos vs. screenshots in court. https://metadataperspective.com/2025/11/04/metadata-matters-camera-original-photos-vs-screenshots-in-court/

Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to computer forensics and investigations (5th ed.). Cengage Learning.

Sedona Conference. (2023). Commentary on proportionality in electronic discovery (3rd ed.). The Sedona Conference.

TrueScreen. (2026). Screenshot evidence in court: Admissibility guide [2026]. https://truescreen.io/articles/screenshot-evidence-court-admissibility/

Vacca, J. R. (2017). Computer forensics: Computer crime scene investigation (2nd ed.). Charles River Media.