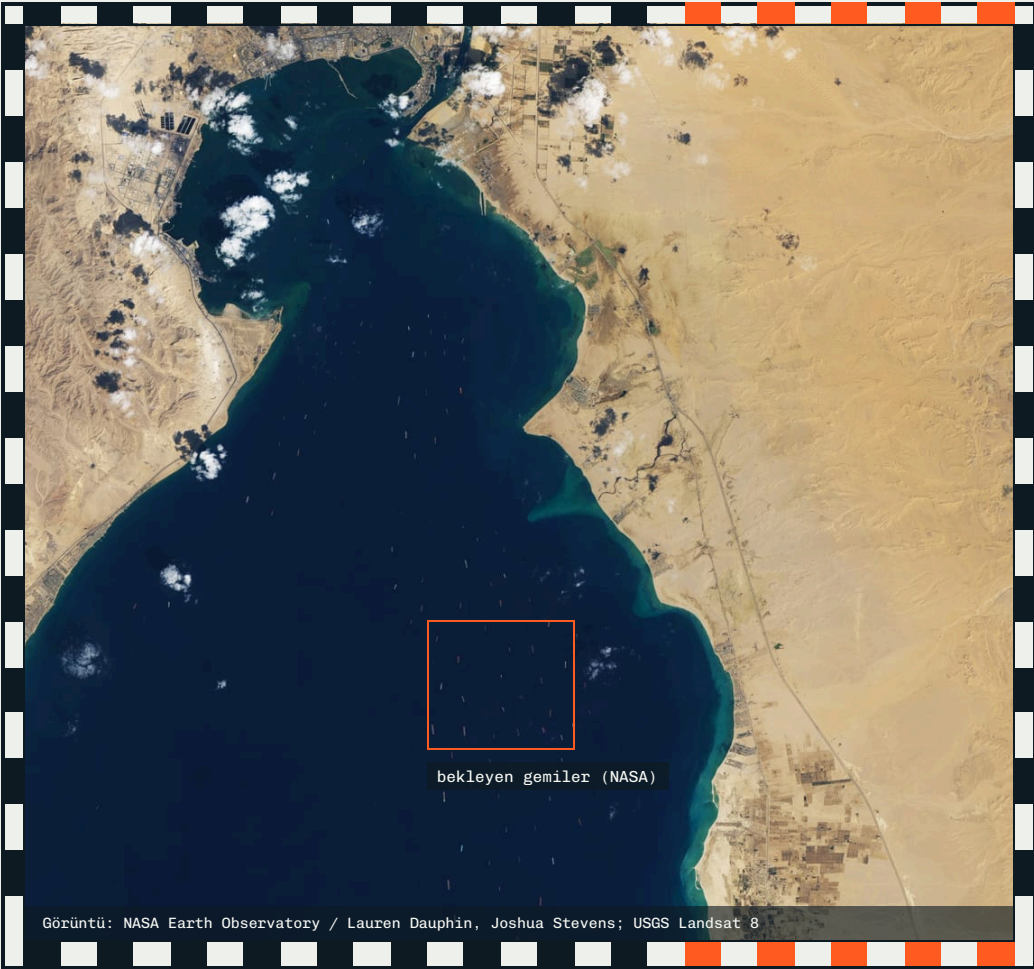




Görüntü: NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; USGS Landsat 8

CSINT - BOOK - 2026 - 001

KİTAP

OSINT, adım adım

Gerçek vakalarla açık kaynak araştırması

Ücretsiz bölümler: 1, 2, 3 ve 19

Ahmet Göker

Birinci baskı, 2026 / CSINT Research

OSINT, adım adım

Gerçek vakalarla açık kaynak araştırması

Yazar	Ahmet Göker
Baskı	Birinci baskı, 2026
Yayıncı	CSINT Research
Paftalar	18 yöntem bölümü, 9 gerçek vaka
Bu dosya	Ücretsiz bölümler: 1, 2, 3 ve 19

OSINT, adım adım

Gerçek vakalarla açık kaynak araştırması

Ahmet Göker

Birinci baskı, 2026

CSINT Research, csintresearch.org

CSINT-BOOK-2026-001

Bu bağımsız bir kitaptır. GIAC veya SANS yayını değildir, bu kurumların onayını da taşımaz. Okurun kamuya açık GOSI sınav alanlarına hazırlanmasına yardımcı olur. Sınav sorusu içermez ve başarıyı garanti etmez.

Gerçek vakalarda kamuya açık kayıtlar kullanıldı. Her kayıt kullanıldığı yerde tarihi ve sınırıyla birlikte gösterilir. Görsellerin kaynağı altlarında yazılıdır ve kitabın sonunda listelenir. Bu kitaptaki hiçbir görsel yapay zeka ile üretilmedi.

Kapak: Süveyş Körfezi, 27 Mart 2021, Landsat 8. NASA, denizdeki küçük izleri bekleyen gemiler olarak açıklıyor. Görüntü, 19. bölümde incelenen kayıtlardan biridir. NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; USGS Landsat 8.

Kapaktaki konum, NASA Earth Observatory sayfasının bu görüntüler için verdiği harita noktasıdır: 29.8256 N, 32.5661 E. Kaynak görüntünün köşe koordinatlarını vermiyor, bu yüzden kapakta köşe koordinatı yok.

© 2026 Ahmet Göker, CSINT Research. Tüm hakları saklıdır. Kanunun izin verdiği durumlar dışında, yazılı izin alınmadan kitabın hiçbir bölümü kopyalanamaz, paylaşılamaz veya yeniden yayımlanamaz. Bu ücretsiz dosya, kitabın ücretsiz okunabilen bölümlerini içerir ve kişisel okuma içindir.

İçindekiler

Bu dosyada kitabın ücretsiz okunabilen bölümleri var: 1, 2, 3 ve 19. Diğer bölümler kitabın tam sürümünde. Tam sürümün içeriği bu dosyanın sonunda.

Yazardan	5
Bu kitap nasıl okunur?	7
Başlamadan önce	8
GOSI çalışma haritası	9

Kısım 1: Önce nasıl düşünürüz?

01	Önce soruyu yaz	12
02	Kaynak ile iddiayı ayır	24
03	Aramadan önce ortamı hazırla	36

Kısım 6: Gerçek vakalar

19	Süveyş 2021’de kanal açılınca kuyruk da bitti mi?	47
	Cevap anahtarı	60
	Görseller ve haklar	63
	Kitabın tam sürümü	64
	Yazar hakkında	66

Yazardan

Bulmacaları severim. Bir yapbozun parçalarını önüme dizip resmin hangi köşesinin eksik kaldığını bulmak bana hep iyi gelmiştir. Boş akşamlarımda da çoğu zaman gerçek suç belgeselleri izlerim. Seri katil dosyaları da bunların arasında. Bir insanın neden öyle davrandığını anlamaya çalışıyorum, yıllarca kapalı kalan bir dosyanın küçük bir ayrıntıyla nasıl açıldığını görmek istiyorum. BTK soruşturmasında bir disketin dosya bilgilerindeki bir ad ile bir kilise adı, birlikte arandığında soruşturmacıları bir kişiye götürdü. Gilgo Beach dosyasında ise bir tanığın hatırladığı kamyonetin kaydı, yıllar sonra bir isim verdi.

OSINT'e bu merakla geldim. Bir dosyanın nasıl açıldığını yalnızca izlemek yerine aynı kayıtlara kendim bakmak istedim. GOSI'ye hazırlanırken sekiz hafta boyunca kendi notlarımı ve sınavda bakmak için hazırladığım konu dizinimi tuttum. Bu kitap o çalışmadan doğdu. Teknik terimleri İngilizce halleriyle koruyup her konuyu küçük adımlarla anlatmak istedim. Her bölüme gerçek bir kayıt, bir şema ve kısa bir alıştırma koydum. Son kısımda da gerçek vakaları baştan sona anlattım.

Bazı görüntüler beni öfkeliyor, bazıları korkutuyor. Bazı iddialar da zaten inandığım şeye benziyor. Böyle anlarda duygum ya da siyasi görüşüm öne geçerse kaynağı yeterince sorgulamadan sonuca atlarım. Bunu çalışırken yakalamaya uğraşıyorum.

Notlarımda gördüğüm ayrıntıyı, yorumumu ve eksik bilgiyi ayrı satırlara yazıyorum. Fotoğrafta gördüğümü başka bir yazıdan okuduğumdan ayrı tutuyorum. Görüşüme uyan bir iddiayı da ötekiler kadar sıkı sınıyorum.

Elimdeki kayıt bazen soruyu cevaplamaya yetmiyor. O zaman eksik kalanı yazıyorum. Okuyan kişi, vardığım sonucun hangi kaynağa dayandığını görebilmeli.

Bu kitapta kurbanların fotoğrafı yok. Şiddeti ayrıntısıyla anlatmadım, olayla ilgisi olmayan akrabaların adını da yazmadım. Gerçek suç dosyalarında soruşturmacıların attığı adımları ve bu adımların dayandığı

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

kayıtları izliyorum.

Ahmet Göker

Bu kitap nasıl okunur?

Kitap altı kısımdan oluşuyor. İlk beş kısım her bölümde bir yöntem öğretiyor: soruyu nasıl kuracağını, kaydı nasıl saklayacağını, bir web ya da e-posta kaydını nasıl okuyacağını ve bildiğini nasıl yazacağını. Altıncı kısım bu yöntemleri gerçek olaylara baştan sona uyguluyor.

Her yöntem bölümü kısa bir özet sayfasıyla açılıyor. Ardından konu, adım adım bir örnek, akılda tutulacak bir nokta ve küçük bir alıştırmaya geliyor. Cevaba bakmadan önce alıştırmayı kendin dene. Cevaplar kitabın sonunda, her alıştırmayın yanında cevabın sayfası yazıyor.

Teknik terimler İngilizce kalıyor, çünkü araçlarda, kayıtlarda ve sınavlarda onları böyle göreceksin. Her bölüm kendi terimlerini “Bu bölümün terimleri” başlığında açıklıyor, hepsi sondaki dizinde de var.

Şekillerde renkler her bölümde aynı. Mavi kutu kaydın gösterdiği şey, kesikli hardal kutu gerekçe isteyen yorumun. Mor baklava bir soru, yeşil çizgi evet, kırmızı çizgi hayır. Kalın turuncu kutu yazabileceğin sonuç.



Bazı bölümlerin sonundaki yatay sayfalar çalışma ekranlarım. Onları YouTube videolarımdaki OSINT VM (sanal makine) görünümüyle yeniden çizdim. İçlerindeki belgeler, işaretler, notlar ve Python çıktıları gerçek. Python kodunu kaydettiğim dosyalarda yeniden çalıştırdım, sayıları aynı dosyalarla sen de tekrarlayabilirsin.

Gerçek vakalarda her kayıt tarihiyle, kaynağıyla ve sınırıyla birlikte gösteriliyor. Bir kayıt soruyu cevaplamaya yetmiyorsa bunu açıkça yazıyor ve orada duruyorum.

Her yöntem bölümü “Sahada: kendin dene” ile bitiyor. Bunlar gerçek kamu kayıtlarında kendin tekrarlayabileceğin görevler. Her görevin altında o gün açtığım sayfanın ekran görüntüsü ya da komutun gerçek çıktısı var, bulduğum değer işaretli.

Başlamadan önce

“Sahada” görevlerinin çoğu için tarayıcı yeter. “Aç” yazıyorsa adresi orada aç, “Ara” yazıyorsa sorguyu arama motorunda ara. “Çalıştır” yazıyorsa komutu terminale yazıp Enter’a bas. “Aç + çalıştır” ikisini de ister. Sonucu görevin altındaki görüntüyle karşılaştır. Sayfada arama için Ctrl+F, Mac’te Command+F kullan.

macOS’ta Terminal’i Uygulamalar klasörünün içindeki İzlenmeler klasöründe bulursun. curl, dig, whois, grep ve shasum hazır gelir.

Windows 11 ya da desteklenen Windows 10’da learn.microsoft.com/windows/wsl/install sayfasını izle. PowerShell’i yönetici olarak aç, wsl --install yaz, yeniden başlat ve Ubuntu’yu aç. Ubuntu ya da Debian’da sudo apt update ve sudo apt install curl dnsutils whois jq gnupg çalıştır. Linux’ta shasum -a 256 yerine aynı SHA-256 değeri için sha256sum kullan.

15. bölüm için GnuPG (gpg), 17. bölüm için jq gerekir. macOS’ta gnupg.org/download ve jqlang.org/download adreslerine bak ya da Homebrew ile brew install gnupg jq çalıştır.

Tarayıcı görevinin altındaki “Aynı kayıt komut satırında” görüntüsü ek bir kontroldür, komutu yazman gerekmez. Komutları okumayı 17. bölüm anlatıyor.

Kayıtlar 27 Eylül 2026’dan sonra değişebilir. Kendi tarihini sonucun yanına yaz.

Görevlerin çoğu herkese açık kayıtları kullanır. 3. bölümde kendi tarayıcını test eder, istersen gelen kutundaki bir bağlantının adresine bakarsın. O bağlantıyı açma ya da paylaşma. Görevler senden bir sistemi taramanı ya da başka birinin özel bilgisini aramanı istemez.

GOSİ çalışma haritası

Bu kitabı GOSİ sınavına hazırlananlar ve günlük araştırma yapanlar için yazdım. Bağımsız bir çalışma. GIAC ya da SANS'ın resmi ders kitabı değil. Kamuya açık altı sınav alanının hangi bölümlere denk geldiğini çalışma haritasında bulursun. Alıştırmaları bu kitap için ben yazdım. Sınavda hangi soruların çıkacağını bilemem, geçeceğine de söz veremem.

Sınav alanı	Bölümler	Ne çalışmalı
Yöntem ve raporlama	1. Önce soruyu yaz 2. Kaynak ile iddiayı ayır 18. Bildiğini kısa yaz	Soruyu, kapsamı, kaynakları ve sonucu yaz. Başka bir olası açıklamayı da sına.
Gizlilik ve OPSEC	3. Aramadan önce ortamı hazırla 5. Bulduğun şeyi kaybetme 15. Gizlilik ve anahtarlar	Bir işlemin kimi haberdar ettiğini ve hangi veriyi açığa çıkardığını açıkla.
Arama ve veri işleme	4. Aramayı daralt 5. Bulduğun şeyi kaybetme 6. Fotoğrafa üç açıdan bak 7. Nerede? Ne zaman? 8. Satırları düzenle 16. Aracı yaptığı işle öğren 17. Küçük bir dosyayla çalış	Sorgu kur. Kayıt sakla. Dosyayı işle. Sonucu küçük bir örnekte kontrol et.
Kişi araştırması	9. Hesap ile kişiyi ayır 6. Fotoğrafa üç açıdan bak 7. Nerede? Ne zaman? 13. E-postada hangi ad kontrol edilir?	Hesapları zaman ve kaynak bilgisine göre karşılaştır. Olası bir yanlış eşleşmenin nedenini açıkla.

Sınav alanı	Bölümler	Ne çalışmalı
Kurum araştırması	10. Markanın arkasındaki kaydı bul 14. Sunucu kimin? Kanıt ne? 15. Gizlilik ve anahtarlar 18. Bildiğini kısa yaz	Doğru kurumu bul. İhlal iddiasını, kablosuz ağ kaydını ve iş etkisini ayrı ayrı değerlendir.
Ağ ve altyapı	11. Ad, adres ve DNS 12. Sertifikadaki adı oku 13. E-postada hangi ad kontrol edilir? 14. Sunucu kimin? Kanıt ne?	DNS, IP, kayıt ve sertifika verisini oku. Sağlayıcıyı ve müşteriyi birbirinden ayır.

Herkese açık güncel GOSI sayfasına göre sınavda 75 soru var, süre 2 saat ve geçme puanı yüzde 69. Kendi sınav sürümünü GIAC hesabında kontrol et. Sınavda internet ve elektronik not kullanılamaz. GIAC, soru-cevap biçimindeki basılı materyali de yasaklıyor. Bu kitabın alıştırma PDF'sini sınava götürebileceğini varsayma.

16 Eylül 2026'da GIAC hedeflerini, kamuya açık SEC497 konu listesini ve 28 sayfalık kaynak PDF'i yan yana koydum. Bu eşleştirme yalnızca herkese açık alanları bölümlere bağlıyor. GIAC'ın soru bankasını görmedim. Sınava hazırlanırken bu kitabın sana yeteceğini de söyleyemem.

Önce nasıl düşünürüz?

Aramaya başlamadan önce ne öğrenmek istediğini yaz,
kaynağı iddiadan ayır ve çalışma ortamını hazırla.

- 01 Önce soruyu yaz
- 02 Kaynak ile iddiayı ayır
- 03 Aramadan önce ortamı hazırla

Önce soruyu yaz

Aramaya başlamadan önce neyi öğrenmek istediğini bir cümleyle yaz.

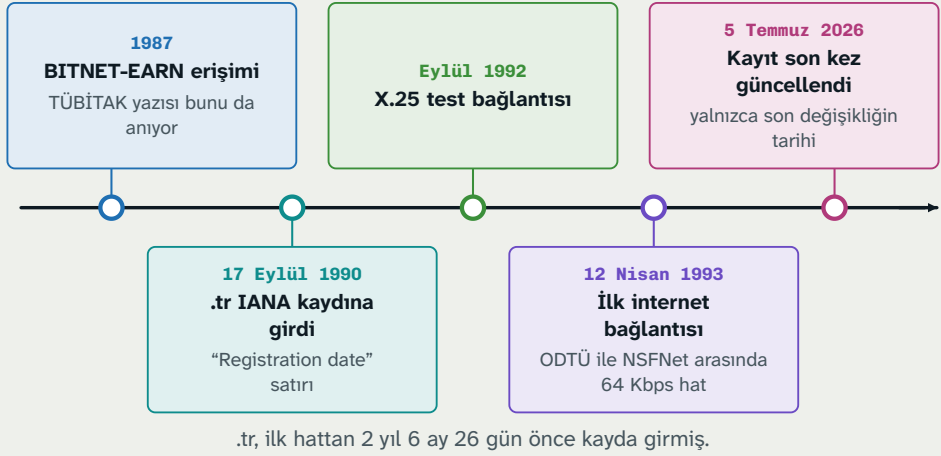
Bu bölümde

- 1.1** Küçük bir soru seç
- 1.2** Cevaba nasıl gideriz?
- 1.3** Veriden karara
- 1.4** Sahada: kendin dene

1.1 Küçük bir soru seç

Mart 2021’de Ever Given adlı konteyner gemisi Süveyş Kanalı’nda karaya oturdu. Bu olay üzerinde çalışmaya “Süveyş’te ne oldu?” diye başlasaydım nerede duracağımı bilemezdim: gemi, kanal, ticaret, sigorta, hepsi bu sorunun içine girer. Ben soruyu ikiye böldüm ve ilkini şöyle yazdım: “Kanal 29 Mart 2021’de yeniden açıldı mı?”

Bu soruyu bir kayıtlı cevaplayabilirim. Tarihi de sorunun içine koydum. “Dün açıldı” gibi bir ifade, haberi hangi gün okuduğuna göre başka bir güne denk gelir.



Şekil 1.1 Soruyu ikiye bölünce iki ayrı tarih çıkıyor. Kayıt tarihiyle bağlantı tarihini karıştırmamak için her olayın kaynağını yanına yaz.

1.2 Cevaba nasıl gideriz?

Süveyş’te kuyruğun 29 Mart’ta dağılmadığını görünce kuyruğun hangi gün dağıldığını sormaya başladım. Sorudan cevaba, cevaptan yeni bir soruya dönen bu akışın adı Intelligence cycle (istihbarat döngüsü). Aşamaların kısa tanımlarını aşağıdaki şekle koydum. Tabloda ise her aşamanın Süveyş çalışmamda gerçekte neye karşılık geldiğini yazdım:

Direction	İki soruyu ayrı yazdım: Kanal 29 Mart 2021’de yeniden açıldı mı? Bekleyen gemiler o gün dağıldı mı?
------------------	---

01

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17

18

19

20

21

22

23

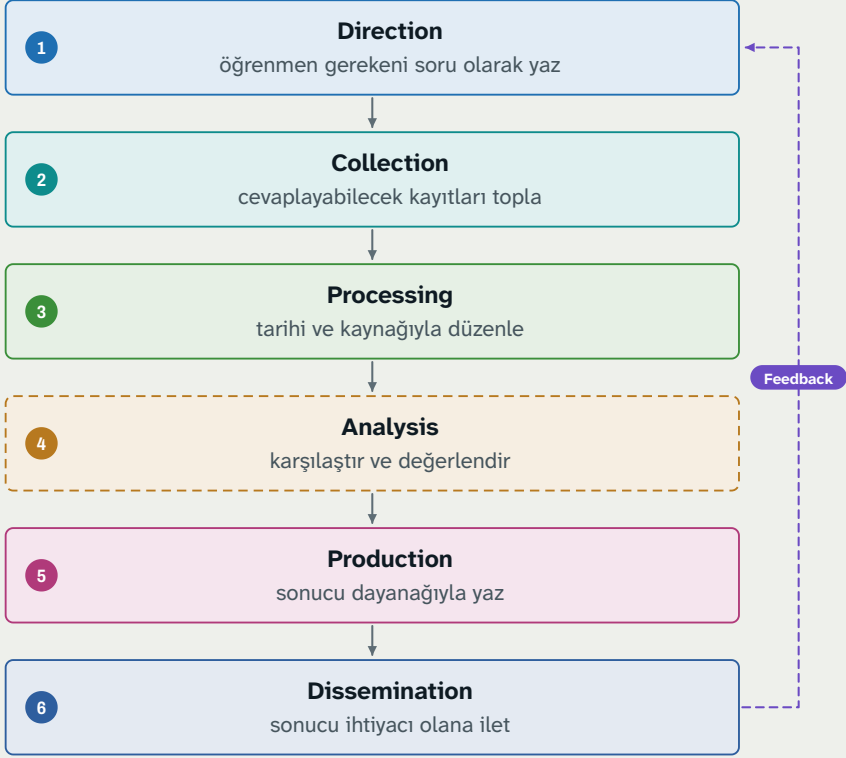
24

25

26

27

Collection	NASA'nın gündüz ve gece uydu görüntülerini, Süveyş Kanal İdaresinin 29 Mart duyurusunu ve ESA'nın radar karşılaştırmasını topladım.
Processing	Her kaydı yayın tarihi ve çekim tarihiyle birlikte bir tabloya yazdım.
Analysis	Kayıtları karşılaştırdım. NASA'nın yazısına göre kanal 29 Mart'ta açıldı. Kanal idaresinin duyurusu ise geminin yüzdürüldüğünü ve geçişin gemi tamamen hizalanınca başlayacağını bildiriyor. Kanalin açıldığını yazmıyor. NASA'nın Leth Agencies'ten aktardığı sayıya göre 30 Mart'ta hala 184 gemi bekliyordu. Kuyruk 29 Mart'ta dağılmamıştı.
Production	Sonucu kaynaklarıyla birlikte kısa bir nota yazdım ve neyi bilmediğimi de ekledim.
Dissemination	Notu bir araştırma dosyası olarak yayımladım.
Feedback	Bir okur "Kuyruk hangi gün dağıldı?" diye sorarsa iş bu yeni soruyla başa döner.



Şekil 1.2 Raporu okuyan kişi bir yorum ya da yeni bir soruyla dönerse iş yeniden Direction adımıyla başlar.

1.3

Veriden karara

Bir kayda bakınca önce ne işe yarayacağını sor: aynı kayıt, farklı sorularda farklı bir şey söyleyebilir. Aşağıdaki satırlar, Süveyş Körfezi'nin uydu görüntülerinden adım adım bir değerlendirmeye nasıl varıldığını gösteriyor.

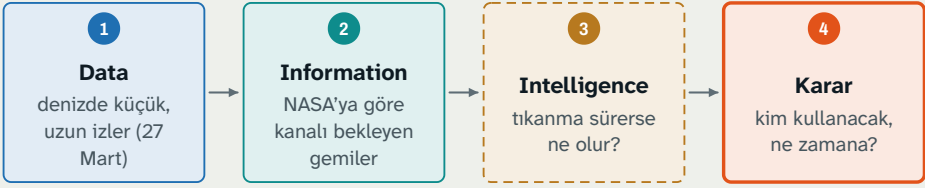
Data	27 Mart 2021 tarihli uydu görüntüsünde denizde küçük, uzun izler var. Henüz yorum eklenmedi.
Information	Kayıtlar karşılaştırılınca anlam kazanıyor: 11 Mart görüntüsünde bu izler çok daha az ve NASA onları kanala girmeyi bekleyen gemiler olarak açıklıyor.

Intelligence

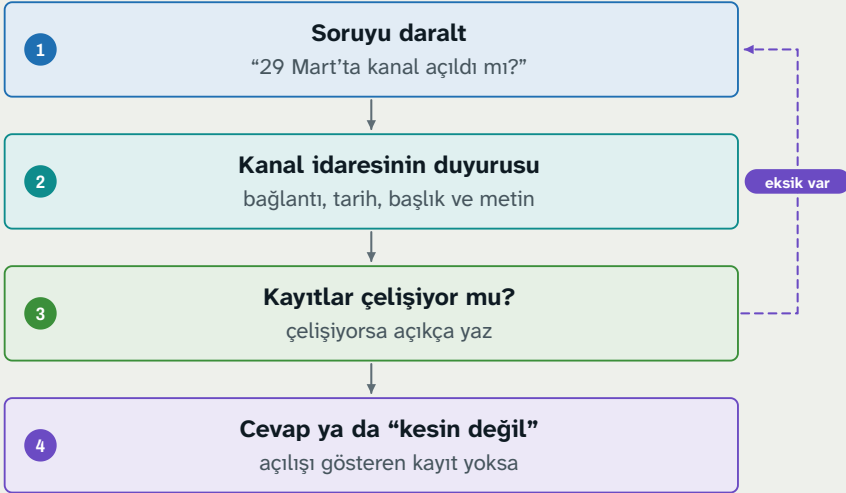
Tıkanma sürdükçe bekleyen gemilerin artacağı ve kanaldan geçecek yüklerin gecikeceği sonucuna varabilirsin. Bu bir değerlendirmedir. Dayanağını ve eksiklerini birlikte yaz.

Decision

Cevabı kimin, ne zamana kadar kullanacağını ve senin hangi işlemleri yapmaya yetkili olduğunu kaydet. Scope (kapsam) bu işin sınırlarını belirler.



Şekil 1.3 27 Mart görüntüsündeki izler, NASA'nın açıklamasıyla kanalı bekleyen gemilere dönüşüyor. Kesikli çerçevedeki soru kayıta yok, onu sen soruyorsun.



Şekil 1.4 Soru dar ve tarihliyse hangi kaydı arayacağını bilirsin.

Adım adım örnek

Birlikte yapalım

Görevin, Süveyş Kanalı'nın 29 Mart 2021'de yeniden açılıp açılmadığını bulmak. Bunun için mürettebatın ya da kanal çalışanlarının kişisel hesaplarına bakman gerekmez. Kanalı işleten kurumun kendi duyurusundan başla.

- 01 Soruyu tarihiyle birlikte yaz: "Kanal 29 Mart 2021'de yeniden açıldı mı?"
- 02 Süveyş Kanal İdaresinin 29 Mart duyurusunu bul. Bağlantısını, yayın tarihini, başlığını ve metnini ayrı ayrı not et.
- 03 Başlık ile metin ya da iki kaynak farklı şeyler yazıyorsa bunu açıkça not et. Kanalın açıldığını gösteren bir kayıt bulamazsan kesin bir cevap verme.

Bu örneğin alındığı vaka: Bölüm 19, Süveyş 2021'de kanal açılınca kuyruk da bitti mi? (sayfa 47).



Şekil 1.5 Dört parçayı ayrı satırlara yaz. Başlık ile metin farklı şeyler söylüyorsa bunu notuna açıkça geçir.

1.4

Sahada

Kendin dene

1

Soruyu ikiye böl

Aç <https://www.iana.org/domains/root/db/tr.html>

Yap “Türkiye internete ne zaman bağlandı?” sorusunu ikiye böl: “tr IANA kaydına ne zaman girdi?” ve “İlk internet hattı hangi gün açıldı?” IANA, .com ve .tr gibi alan adı uzantılarının ana listesini tutan kurumdur. IANA’nın bu sayfasında en alta in. “Registration date” ile “Record last updated” satırlarını not et. Sonra TÜBİTAK’ın bilimgenc.tubitak.gov.tr/makale/turkiyede-internet-25-yasinda yazısında ilk internet bağlantısının kurulduğu günü bul ve “Registration date” ile karşılaştır.



1990-09-17 kayıt tarihi, IANA’nın .tr sayfasının en altında kırmızı çerçevede. IANA, ekran görüntüsü 27.09.2026

Benim bulduğum Sayfanın en altında “Registration date 1990-09-17” ve “Record last updated 2026-07-05” yazıyordu. TÜBİTAK’ın 12 Nisan 2018 tarihli yazısı ilk bağlantıyı 12 Nisan 1993 olarak veriyor. ODTÜ ile ABD’deki NSFNet arasında 64 Kbps’lik kiralık bir hat kurulmuş. Aynı yazı 1987’deki BITNET-EARN erişimini ve Eylül 1992’deki X.25 test bağlantısını da anıyor. Buna göre .tr, ilk hattan 2 yıl 6 ay 26 gün önce kayda girmiş.

Dikkat “Registration date” uzantının kayda girdiği gün. O gün Türkiye’de bir bağlantının olması gerekmiyor. “Record last updated” da son değişikliğin tarihi.

2

Sayının tarihini ve sınırını yaz

Aç <https://veriportali.tuik.gov.tr/tr/press/53899>

Yap “Türkiye’nin nüfusu kaç?” yerine “31 Aralık 2025’tе Türkiye’de ikamet eden kaç kişi vardı?” diye yaz. Bültenin başındaki “Yayım Tarihi” satırını ve ilk paragrafta sayının ait olduğu tarihi ayrı ayrı not et. Sayfanın altındaki (1) numaralı açıklamayı oku.



Telefonda açılan TÜİK bülteni. Kırmızı çerçevedeki satır yayım tarihi, 09 Şubat 2026 10:00. Türkiye İstatistik Kurumu (TÜİK), ekran görüntüsü 27.09.2026

Benim bulduğum Bültenin başında “Yayım Tarihi: 09 Şubat 2026 10:00” yazıyordu. İlk paragrafta göre 31 Aralık 2025 itibarıyla Türkiye’de ikamet eden nüfus 86 milyon 92 bin 168 kişi. (1) numaralı açıklamaya göre geçici koruma statüsündeki Suriyeliler ve turizm gibi nedenlerle 90 günden kısa vize ya da ikamet izniyle bulunan yabancılar bu sayıya dahil değil.

Dikkat Bu sayı “Türkiye’de bugün kaç kişi var?” sorusunu cevaplamaz. Bir yıl sonu kayıdır ve bazı grupları dışarıda bırakır.

3

Arşivde ülke adının değiştiği haftayı bul

Aç <https://web.archive.org/web/20220531130855/https://www.un.org/en/about-us/member-states>

Yap Soruyu tarihiyle yaz: “BM'nin üye ülkeler sayfası 31 Mayıs 2022'de Türkiye'nin adını nasıl yazıyordu?” Sayfada (Ctrl+F) Tunisia'yı ara ve hemen altındaki satırı oku. Sonra adresteki 20220531130855'i (arşivin bu kopyayı aldığı an, 31 Mayıs 2022 13.08.55) 20220607132805 yap ve aynı satıra bak.

```
Terminal: Wayback Machine (CDX) 27.09.2026

$ curl -s 'https://web.archive.org/cdx/search/cdx?url=www.un.org/en/about-us/member-states&from=20220531&to=20220607&fl=timestamp,statuscode'
20220531055112 200
20220531055631 200
20220531104115 200
20220531130855 200
20220607132805 200

$ for t in 20220531130855 20220607132805; do echo $t; curl -s https://web.archive.org/web/${t}/https://www.un.org/en/about-us/member-states | grep -A 2 -E '>(Turkey|Türkiye)<' | sed -e 's/<[^>]*>/g' -e 's/^[[[:space:]]*///' | grep .; done
20220531130855
Turkey
Date of Admission: 24-10-1945
20220607132805
Türkiye
Date of Admission: 24-10-1945
```

Aynı kayıt komut satırında

27 Eylül 2026'daki CDX sorgusu ve iki arşiv kaydı. Turkey ve Türkiye satırlarını, iki zaman damgasıyla birlikte sarıyla işaretledim.

Benim bulduğum 31 Mayıs 2022 13.08 UTC (evrensel saat, Türkiye saatinin 3 saat gerisi) kaydında “Turkey Date of Admission: 24-10-1945” yazıyor. 7 Haziran 2022 13.28 UTC kaydında ise “Türkiye Date of Admission: 24-10-1945” var. Arşivde bu ikisinin arasında başka kayıt yok. BM Türkiye sitesindeki 3 Haziran 2022 tarihli yazıya göre ad değişikliği mektubu 1 Haziran'da alınmış ve değişiklik o andan itibaren geçerli olmuş.

01

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

Dikkat

Arşivden sayfanın değiştiği anı öğrenemezsin. Elinde arşivin aldığı iki kayıt arasındaki aralık var, burada 7 gün.

Aklında kalsın

Arama sırasında başta yazdığın soruya dön ve bulduğun şeyin o soruyu cevaplayıp cevaplamadığına bak.

**Şimdi sen**

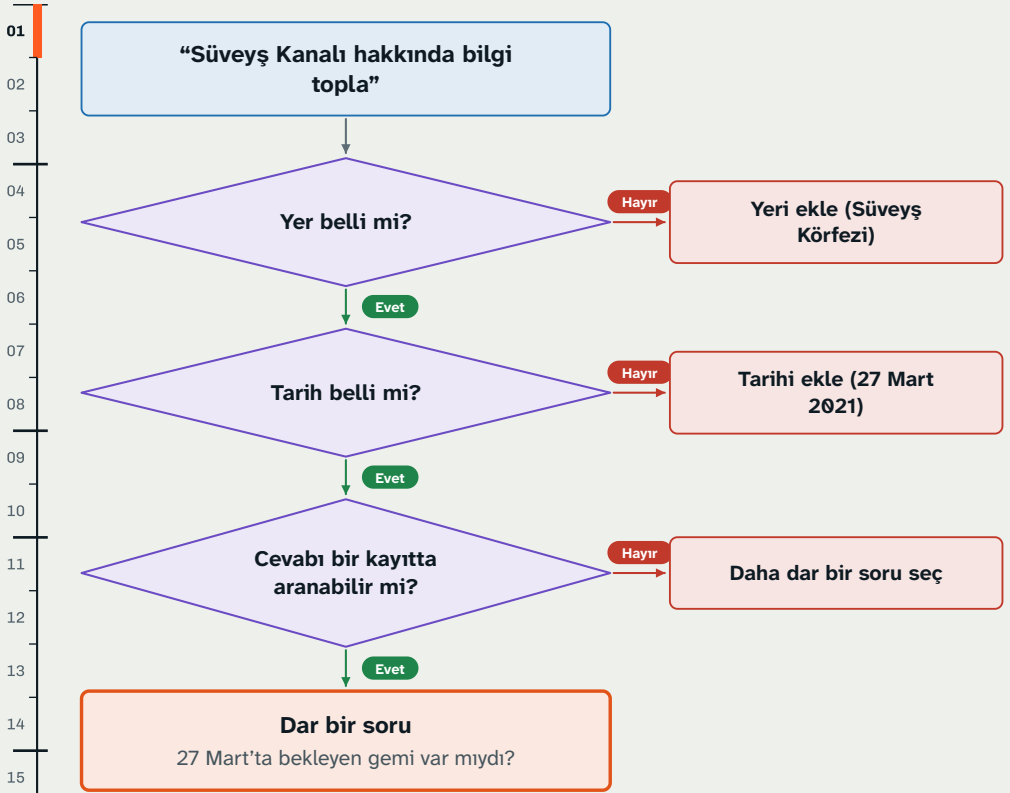
“Süveyş Kanalı hakkında bilgi topla” görevini nasıl daraltırsın?

Cevabı: sayfa 60

**Bulmaca**

İlk kaydedilen .com alan adı olarak bilinen symbolics.com’un RDAP kaydında (alan adının kayıt bilgisi, rdap.verisign.com/com/v1/domain/symbolics.com) kayıt zamanı 1985-03-15T05:00:00Z, bitiş zamanı 2027-03-16T04:00:00Z. Tarihle saati aradaki T ayırır, sondaki Z ise saatin UTC olduğunu gösterir. Aynı kayıta saat neden bir yerde 05.00, öbür yerde 04.00? İpucu: yaz saatini düşün.

Cevabı: sayfa 60



Şekil 1.6 Her basamakta soruya bir parça ekle. Sonunda soru, NASA'nın o güne ait uydu görüntüsü gibi tek bir kayıtta aranabilir hale gelir.



Öğrendiğini kontrol et

Görev, bir hizmet kesintisinin kurumu etkileyip etkilemediğini bulmak. İlk listende 500 çalışan adı var. Ne yaparsın?

Cevabı: sayfa 60

Bu bölümün terimleri

OSINT

Açık kaynak istihbaratı: herkese açık kaynakları inceleyerek bir soruya dayanağı gösterilmiş bir cevap verme işi.

Intelligence requirement

Araştırmanın cevaplaması gereken soru.

Scope

İşin sınırı: konu, tarih ve izinli işlemler.

Seed / Pivot

Başladığın ilk ipucu / o ipucunu kullanarak yeni bir



kayda geçmek.

Stop condition

Aramayı ne zaman bitireceğini baştan belirleyen koşul.

Data / Information / Intelligence

Ham kayıt / bağlamı eklenip anlam kazanmış kayıt / karar vermeye yardım eden değerlendirme.

Kaynaklar

1. GIAC, GOSI objectives

<https://www.giac.org/certifications/open-source-intelligence-gosi>

2. NASA Earth Observatory, Traffic Jam on the Suez Canal (31 March 2021)

<https://science.nasa.gov/earth/earth-observatory/traffic-jam-on-the-suez-canal-148114/>

3. Suez Canal Authority, Successful Refloating of EVER GIVEN (29 March 2021)

https://www.suezcanal.gov.eg/English/MediaCenter/News/Pages/nav_29-03-2021.aspx

Kaynak ile iddiayı ayır

Güvendiğin bir kaynak da yanılabilir. NASA'nın 31 Mart yazısı kanalın yeniden açıldığını yazıyor, ama bunu NASA kendisi gözlemedi. Yazının kaynakçasında kanal idaresinin duyurusu ve Reuters var. Her cümlenin hangi kayda dayandığını bul.

Bu bölümde

- 2.1 Üç ayrı satır tut
- 2.2 Kopyaların ilk kaynağını bul
- 2.3 Kaynağı ve iddiayı ayrı ayrı değerlendir
- 2.4 İlk fikrini sına
- 2.5 Sahada: kendin dene

2.1 Üç ayrı satır tut

Bir kütüphanenin duyurusunda “Pazar kapalı” yazıyor. Not alırken gördüğünü, ondan çıkardığını ve doğru saydığını ayrı satırlara yaz:

Fact	Kaydettiğim duyuruda “Pazar kapalı” yazıyor.
Inference	Kütüphane bu pazar da kapalı olabilir.
Assumption	Duyurunun hala geçerli olduğunu kabul ediyorum.

Yalnızca ilk satır bir kayda dayanıyor. Diğer ikisi bu pazarın saatlerini henüz doğrulamıyor. Önce duyurunun tarihine bak.

2.2 Kopyaların ilk kaynağını bul

Beş hesap aynı duyurunun fotoğrafını paylaşabilir. Hepsi aynı duyuruyu kopyalıyorsa elindeki kaynak sayısı bir. Kopyaların izini sür ve duyurunun ilk yayımlandığı yeri bul. Bu sırada kendi fikrine uymayan kayıtlar da çıkabilir. Onları da not et. Yalnızca beklediğin cevabı destekleyen bilgiyi aramaya Confirmation bias (doğrulama yanlılığı) denir.



Şekil 2.1 Kopyaların izini sürüp ilk kaynağa git. Yolda fikrine uymayan bir kayıt çıkarsa onu da not et.

2.3 Kaynağı ve iddiayı ayrı ayrı değerlendirir

Burada iki ayrı soru sorarsın. Source reliability (kaynak güvenilirliği), kaynağın geçmişine ve bu bilgiye nasıl ulaştığına bakar. Information credibility (bilginin inandırıcılığı) ise tek bir iddianın neye dayandığını sorar. İkisini ayrı tutmak gerekir, çünkü güvenilir bir kaynak da yanlış bilgi verebilir.

Admiralty / NATO-style grading

Kaynak A'dan E'ye kadar harflerle, bilgi 1'den 5'e kadar rakamlarla derecelendirilir. F ve 6, o değerlendirmenin yapılamadığını gösterir. Kurumlar ölçeği farklı tanımlayabilir. Çalıştığın kurumun tanımlarına bak.

F6

Kaynağı da iddiayı da değerlendirmeye yetecek bilgi yok. İddia yine de doğru olabilir.

Confidence

Kanıtın sonucu ne kadar güçlü desteklediğini anlatan derece. Low, moderate ya da high (düşük, orta, yüksek) yazdığında nedenini de ekle.

Impact

İddia doğruysa ne kadar zarar ya da değişiklik doğar? Etkinin büyüklüğünü kanıta duyduğun güvenden ayrı yaz. Büyük bir etki, iddiayı daha olası kılmaz.



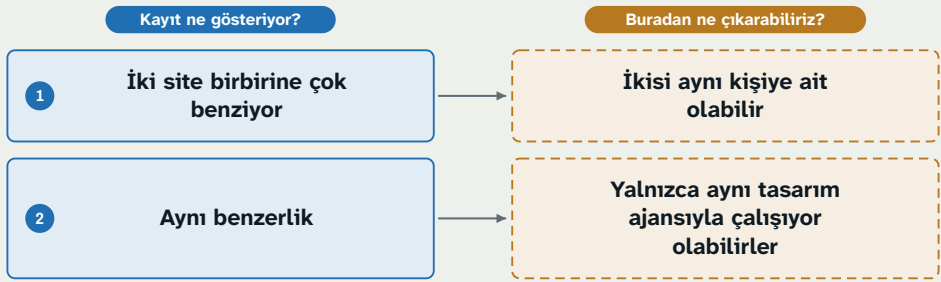
Şekil 2.2 Kaynağı ve iddiaya ayrı not ver. Ölçeğin tanımı kurumdan kuruma değişebilir, çalıştığın yerin tanımlarına bak.

2.4

İlk fikrini sına

Bir açıklama yazdıktan sonra onu zayıflatabilecek bir kayıt ara. Örneğin birbirine çok benzeyen iki site aynı kişiye ait olabilir, ama yalnızca aynı tasarım ajansı ile çalışıyor da olabilirler. Hangi bulgunun bu iki açıklamayı birbirinden ayıracağını sor. Aşağıdaki yanlışlıklar bu sınamayı atlama yol açabilir.

Confirmation bias	Sadece ilk fikrini destekleyen bilgiyi seçmek.
Anchoring / Premature closure	İlk ipucuna fazla ağırlık vermek / erken karar verip aramayı bitirmek.
Availability / Authority bias	Yeni veya akılda kalan olayları fazla önemsemek / ünlü kaynağa sorgulamadan güvenmek.
Mirror imaging	Karşıdaki kişinin senin gibi düşüneceğini varsaymak.
Correlation / Causation	İki olayın birlikte görülmesi / birinin diğerine yol açması. İkisini birlikte görünce nedeni bulmuş olmazsın. Nedeni ayrı bir kayıta ararsın.



Bu iki açıklamayı birbirinden ayıracak bulguyu ara.

Şekil 2.3 İki satırdaki benzerlik aynı. Ona ne kadar uzun bakarsan bak, iki açıklamadan birini seçemezsin.



Şekil 2.4 İddiadan başla ve dallara tek tek bak. Her kutudaki soruyu cevapla. Güvenini yalnızca bulduğun kayıtlara dayandır.

Adım adım örnek

Birlikte yapalım

Süveyş için elimde aynı olayı anlatan üç kayıt vardı. Biri Süveyş Kanal İdaresinin 29 Mart 2021 duyurusuydu. İkincisi Avrupa Uzay Ajansının (ESA) 26 Mart'ta yayımladığı Sentinel-1 radar karşılaştırmasıydı. Üçüncüsü NASA'nın 31 Mart yazısıydı. Üçü aynı şeyi göstermiyor. Duyuru kanal idaresinin kendi açıklaması. ESA ile NASA ise farklı uydularla yapılmış iki ayrı gözlem. Bir haber sitesi NASA'nın görüntüsünü yeniden yayımlarsa elime yalnızca aynı kaydın bir kopyası geçer.

- 01** Her kaydın kimden geldiğini yaz: duyuru kanal idaresinin kendi açıklaması, radar karşılaştırması ESA'nın, gündüz ve gece görüntüleri NASA Earth Observatory'nin (USGS Landsat 8 ve Suomi NPP VIIRS verisiyle).
- 02** Yayın tarihini, kaydın dayandığı gözlemin tarihinden ayır: ESA 26 Mart'ta yayımladı ama 21 ve 25 Mart kayıtlarını karşılaştırıyor. NASA 31 Mart'ta yayımladı, görüntüleri 1 Şubat ile 29 Mart arasında çekildi.

- 03 Bağımsız gözlemleri kopyalardan ayır. NASA ile ESA farklı uydularla baktığı için görüntüleri birbirini destekliyor. NASA'nın yazısındaki açılış cümlesi ise kendi gözlemine dayanmıyor. Yazısının kaynakçasında kanal idaresinin duyurusu ve Reuters var.



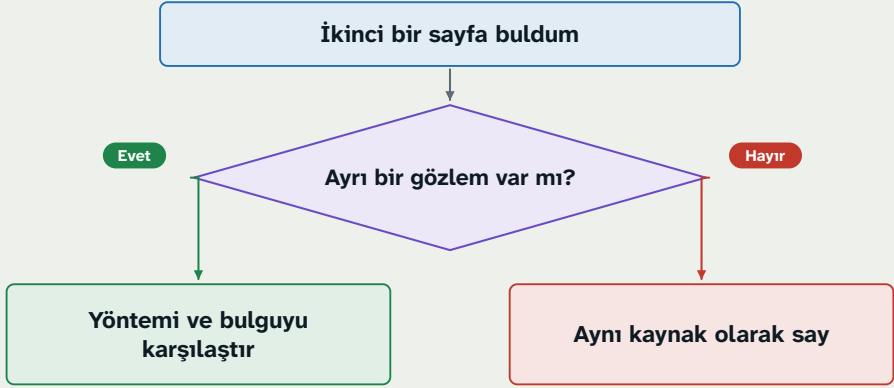
Şekil 2.5 Her kaydın iki tarihi var. Önce gözlemin tarihini bul, sonra yayın tarihini ayrı bir satıra yaz.

Gerçek kayıttan

İki sayfa, aynı harita

Beyrut çalışmasında NASA ve NASA Earth Observatory sayfalarını karşılaştırdım ve her birinin hangi ölçümlere dayandığına baktım.

- Harita ARIA ve Earth Observatory of Singapore ekibinin analizine dayanıyor.
- Aynı analiz başka bir arka plan üzerinde de gösteriliyor. İki sayfa da aynı çalışmaya dayanıyor.



Şekil 2.6 Soruyu oku ve cevaba uyan dalı izle.

Yazabileceğim sonuç

Notuma iki bağlantı yazıyorum.
Bağımsız kanıt sayısını ikiye
çıkarmıyorum.

Bu vakanın tamamı: Bölüm 21, tam sürümde.

Burada duruyorum

İkinci sayfa bana yeni bir gözlem
getirmedi.

2.5

Sahada

Kendin dene

1

Sözün ilk kaydını bul

Aç <https://quoteinvestigator.com/2017/03/23/same/>

Yap Einstein'a mal edilen "Delilik, aynı şeyi tekrar tekrar yapıp farklı sonuç beklemektir" sözünün sayfasını aç. Sözün bilinen en eski kaydını (sayfada "earliest strong match") ve sayfaya göre Einstein'a bağlandığı ilk yılı yaz. Sayfanın sonundaki "Update History" notunu da oku.

```

Terminal: curl + grep 27.09.2026

$ curl -sL --compressed https://quoteinvestigator.com/2017/03/23/same/
| sed -e 's/<[>]*>/g' | grep -oE "There is no substantive evidence
[^.]*\.|The (second)?earliest strong match known to QI appeared in
[^.]*|By 1990 the saying was being attributed to Einstein\.|Update Hi
story: On July 31, 2019 [^.]*\."
There is no substantive evidence that Einstein wrote or spoke the stat
ement above.
The earliest strong match known to QI appeared in October 1981 within
a Knoxville, Tennessee newspaper article describing a meeting of AL-An
on, an organization designed to help the families of alcoholics
The second earliest strong match known to QI appeared in a pamphlet pr
inted by the Narcotics Anonymous organization in November 1981
By 1990 the saying was being attributed to Einstein.
Update History: On July 31, 2019 the October 11, 1981 citation was add
ed to the article.
$ curl -sL https://www.nobelprize.org/prizes/physics/1921/einstein/bio
graphical/ | grep -oE "He died on [^.]*\."
He died on April 18, 1955 at Princeton, New Jersey.

```

Aynı kayıt komut satırında

Sarı satırlarda en eski kayıt, sözü 1990'da Einstein'a bağlayan cümle ve güncelleme notu var. Satırları 27 Eylül 2026'da curl ile çektim.

Benim bulduğum Sayfaya göre sözü Einstein'ın yazdığına ya da söylediğine dair "substantive evidence" (sağlam kanıt) yok. Bilinen en eski güçlü eşleşme, Knoxville News-Sentinel gazetesinin 11 Ekim 1981 tarihli bir AL-Anon toplantısı haberi. Sözü adı verilmeyen bir katılımcı söylüyor. Söz 1990'da Austin American-Statesman gazetesinde Einstein'a bağlanmış. Nobel sitesine göre Einstein 18 Nisan 1955'te ölmüştü.

Dikkat

"Bilinen en eski" kayıt, sözün ilk söylendiği yer olmayabilir. Sayfanın notuna göre 11 Ekim 1981 kaydı yazıya 31 Temmuz 2019'da eklenmiş. O güne kadar en eski güçlü eşleşme, Kasım 1981 tarihli bir Narcotics Anonymous broşürüydü.

2

Kopyaların dayandığı düzenlemeyi bul

Aç https://en.wikipedia.org/w/index.php?title=Maurice_Jarre&action=history&offset=20090401000000&limit=60

Yap Besteci Maurice Jarre'ın Wikipedia sayfasının bu değişiklik geçmişinde "02:29, 30 March 2009" yazan satırı bul ve satırın başındaki "prev" (önceki sürümle karşılaştı) bağlantısını aç. Açılan karşılaştırmada eklenen "Quotes" bölümünü oku. Sonra Guardian'ın 31 Mart 2009 tarihli ölüm yazısının en altındaki düzeltme notunu oku:
theguardian.com/film/2009/mar/31/maurice-jarre-obituary

```
Terminal: Wikipedia API (compare) 27.09.2026

$ curl -s 'https://en.wikipedia.org/w/api.php?action=compare&fromrev=280558491&torelative=prev&prop=ids|timestamp|size&format=json&formatversion=2' | jq -c '.compare | {torevid, totimestamp, fromsize, tosize}'
{"torevid":280558491,"totimestamp":"2009-03-30T02:29:43Z","fromsize":11583,"tosize":12318}

$ curl -s 'https://en.wikipedia.org/w/api.php?action=compare&fromrev=280558491&torelative=prev&prop=diff&format=json&formatversion=2' | jq -r '.compare.body' | grep 'diff-addedline' | grep -v '<br />' | sed -e 's/<[^>]*>/' -e 's/^ */'
==Quotes==
[...]
One could say my life itself has been one long soundtrack. Music was my life, music brought me to life, and music is how I will be remembered long after I leave this life. When I die there will be a final waltz playing in my head and that only I can hear.
[...]
```

Aynı kayıt komut satırında

30 Mart 2009 02.29 UTC düzenlemesi ve eklediği "Quotes" bölümü, Wikipedia API'sinden 27 Eylül 2026'da aldığım karşılaştırmada sarı zeminde.

Benim bulduğum Geçmişte 30 Mart 2009 02.29 UTC tarihli bir düzenleme sayfaya "Quotes" bölümünü ekliyor. İçinde "my life itself has been one long soundtrack" diye süren bir söz var. Guardian'ın ölüm yazısı 31 Mart 2009 tarihli. Altındaki 3 Nisan 2009 notunda yazının bu uydurma sözle açılıp kapandığı belirtiliyor. Nota göre söz Jarre'ın Wikipedia sayfasına bilerek eklenmiş görünüyor ve oradan çeşitli sitelere kopyalanmış.

Dikkat

Bir söz birçok gazetede çıktı diye doğrulanmış olmaz. Hepsi aynı kaynaklı düzenlemeye dayanıyorsa elinde tek bir kaynak vardır.

3**Gözlem tarihini yayın tarihinden ayır**

Aç <https://science.nasa.gov/photojournal/pale-blue-dot-revisited/>

Yap Sayfadaki “Image Addition Date” satırını ve görüntülerin çekildiği anı veren cümleyi (“They were taken at” diye başlıyor) ayrı ayrı not et. Sonra metindeki PIA00452 bağlantısını (özgün 1990 sürümünün sayfası) açıp aynı satıra bak.

```
Terminal: curl + grep 27.09.2026

$ curl -sL https://science.nasa.gov/photojournal/pale-blue-dot-revisited/ | grep -oE 'Image Addition Date:</span><time[^>]*>[^<]*|They were taken at [^<]*'
Image Addition Date:</span><time class="" datetime="2020-02-12">02/12/2020
They were taken at 4:48 GMT on Feb. 14, 1990, just 34 minutes before Voyager 1 powered off its cameras forever.

$ curl -sL https://photojournal.jpl.nasa.gov/catalog/PIA00452 | grep -oE 'Image Addition Date:</span><time[^>]*>[^<]*'
Image Addition Date:</span><time class="" datetime="1996-09-12">09/12/1996
```

Aynı kayıt komut satırında

İki NASA sayfasından 27 Eylül 2026'da curl ile çektiğim satırlar. 2020 ekleme tarihini ve karelerin 14 Şubat 1990'da çekildiğini yazan cümleyi sarıya boyadım.

Benim bulduğum 2020 sürümünün sayfasında “Image Addition Date: 02/12/2020” yazıyor. Metne göre kareler 14 Şubat 1990'da 04.48 GMT'de, Voyager 1 kameralarını kalıcı olarak kapatmadan 34 dakika önce çekilmiş. Özgün PIA00452 sayfasında ise “Image Addition Date: 09/12/1996” var. 2020 sürümü yeni bir gözlem değil. Aynı 1990 verisi modern yazılımla yeniden işlenmiş ve renk kanallarının parlaklığı yeniden dengelenmiş.

Dikkat

“Image Addition Date” görüntünün kataloğa eklendiği gün. Çekim günü bu satırda yok. Sayfa tarihi ay/gün/yıl sırasıyla yazıyor, bu yüzden 02/12/2020, 12 Şubat 2020 demek.

Aklında kalsın**Her kopyanın hangi kayda dayandığını kontrol et.****Şimdi sen**

Admiralty sisteminde F6 “yanlış” anlamına mı gelir?

Cevabı: sayfa 60

**Bulmaca**

Guardian’ın okur temsilcisi 4 Mayıs 2009 tarihli yazısında, uydurma sözün Wikipedia’ya ikinci eklenişinde sayfada yalnızca altı dakika, üçüncüsünde yaklaşık 25 saat kaldığını yazdı. Maurice Jarre sayfasının 30 ve 31 Mart 2009 geçmişine göre altı dakika kalan ekleme hangisi? İpucu: 2. görevdeki geçmiş sayfasında her satırın artı ya da eksi bayt sayısına bak. Sözü ekleyen ve silen satırları “prev” ile doğrula.

Cevabı: sayfa 60

**Öğrendiğini kontrol et**

Üç haber aynı isimsiz paylaşımına dayanıyor. Kaynak sayısını nasıl yazarsın?

Cevabı: sayfa 60

Bu bölümün terimleri

Fact Elindeki bir kaydın doğrudan desteklediği bilgi.

Inference Kanıttan çıkardığın sonuç.

Assumption Şimdilik doğru kabul ettiğin şey.

Confidence Kanıtın sonucu ne kadar güçlü desteklediği.

Circular reporting Birçok yazının aynı kaynağı tekrar etmesi. Kopyalar bağımsız doğrulama gibi görünür.

Source reliability / Information credibility Kaynağın ne kadar güvenilir olduğu / tek bir iddianın ne kadar iyi desteklendiği.



Admiralty / F6

Kaynağı harfle, bilgiyi rakamla derecelendiren sistem. F6, iki değerlendirmeyi de yapmaya yetecek bilgi olmadığını gösterir.

Bias / Competing hypotheses

Düşünceni bir yöne çeken eğilim / aynı bulguyu açıklayabilecek, birbiriyle karşılaştırılan farklı açıklamalar.

Kaynaklar

1. NASA Earth Observatory, Traffic Jam on the Suez Canal (31 March 2021)
<https://science.nasa.gov/earth/earth-observatory/traffic-jam-on-the-suez-canal-148114/>
2. Suez Canal Authority, Successful Refloating of EVER GIVEN (29 March 2021)
https://www.suezcanal.gov.eg/English/MediaCenter/News/Pages/nav_29-03-2021.aspx
3. ESA, Suez Canal traffic jam seen from space (26 March 2021)
https://www.esa.int/ESA_Multimedia/Images/2021/03/Suez_Canal_traffic_jam_seen_from_space

Aramadan önce ortamı hazırla

Bir sayfayı açtığın anda o site ziyaretini kaydedebilir.

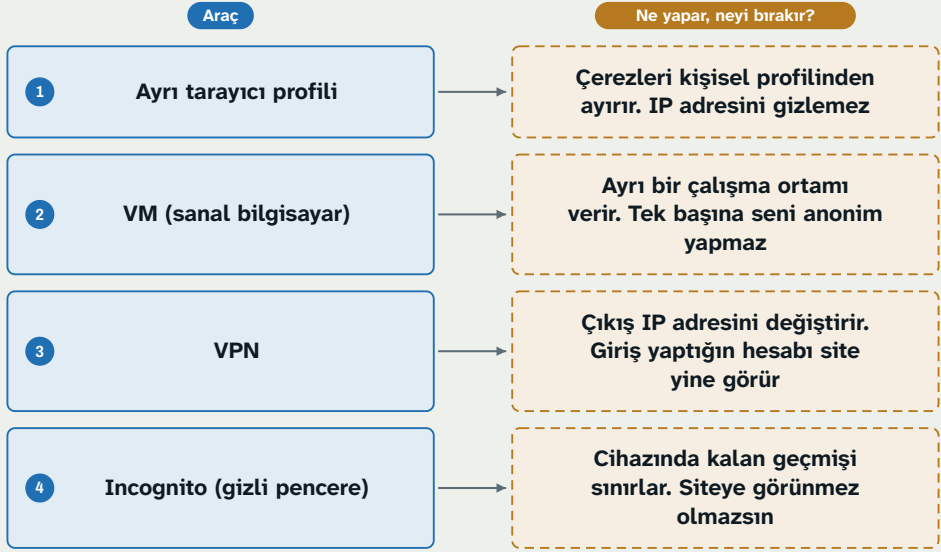
Aramaya başlamadan önce çalışma ortamını hazırla.

Bu bölümde

- 3.1** Aracın sınırını bil
- 3.2** İşlem hedefe gider mi?
- 3.3** Araştırmadan önce neleri ele verdiğini kontrol et
- 3.4** Dosyayı açmadan önce
- 3.5** Sahada: kendin dene

3.1 Aracın sınırını bil

Ayrı bir browser profile (tarayıcı profili) çerezleri kişisel profilinden ayırır. IP adresini ise gizlemez. VM (kendi bilgisayarının içinde çalışan sanal bir bilgisayar) sana ayrı bir çalışma ortamı verir, ama seni anonim yapmaz. VPN, sitelerin gördüğü çıkış IP adresini değiştirir. Kişisel hesabına giriş yaparsan site o hesabı yine görür. Incognito (gizli pencere) yalnız cihazında kalan geçmiş sınırlar. Site seni yine görür.



Başlamadan önce hangi hesapla giriş yaptığını ve hangi bağlantıyı kullandığını kontrol et.

Şekil 3.1 Her satırda bir aracın değiştirdiği şeyi ve açıkta bıraktığı şeyi oku. Birkaçını birlikte kullansan da hesabını ve bağlantını ayrıca kontrol et.

3.2 İşlem hedefe gider mi?

Bir veri sağlayıcının önceden kaydettiği arama sonucunu okursan isteğin o sağlayıcıya gider. Canlı siteyi açarsan hedefin sunucusuna gider. Ama aradaki ayrım her zaman net değil. Ekran görüntüsü alan bir araç, görüntüyü almak için siteyi ziyaret eder. Bir arşiv sayfası canlı siteden

resim yükleyebilir. Üçüncü taraflar da ziyaretini kaydedebilir. Bu yüzden bir araca pasif demeden önce, adı ne olursa olsun, gerçekte hangi isteği nereye gönderdiğine bak.

3.3 Araştırmadan önce neleri ele verdiğini kontrol et

Ayrı bir araştırma hesabı açtıktan sonra da iz bırakırsın. IP adresin, açık oturumların, tarayıcının özellikleri ve dosyaların içindeki bilgiler araştırmayı sana ya da kurumuna bağlayabilir. Başlamadan önce hangi verinin kime gideceğini yaz.

Browser fingerprint / Cookies	Dil, ekran boyutu gibi tarayıcı özellikleri bir araya gelince seni ayırt eden bir iz oluşturabilir. Cookies (çerezler) yeni ziyaretini önceki oturumlarına bağlayabilir.
Sock puppet	Yalnızca araştırma için kullanılan ayrı hesap. Gerçek bir kişiyi taklit etmemeli. Kişisel oturumlarını, fotoğraflarını ve hesap kurtarma bilgilerini (yedek e-posta, telefon) bu hesaba karıştırma.
VM / VPN / Incognito	Her biri tek bir şeyi değiştirir: VM çalışma ortamını ayırır, VPN çıkış IP adresini değiştirir, Incognito ise cihazında kalan geçmişi sınırlar. Hiçbiri tüm kimlik izlerini silmez.
Pre-flight check	Başlamadan önceki kısa kontrol: izin, IP adresi, DNS (alan adlarını IP adresine çeviren sistem), açık oturumlar, tarayıcı uzantıları, otomatik doldurma ve kanıtların kaydedileceği klasör.

3.4 Dosyayı açmadan önce

Beklenmedik bir dosyanın uzantısına güvenme: adı “.pdf” ile biten bir dosya başka türden olabilir. Orijinali olduğu gibi sakla, hash’ini al (dosyanın içeriğinden hesaplanan kısa değer, dosya değişirse o da değişir) ve bir kopya üzerinde çalış. Önce kopyayı, kodunu çalıştırmadan incele. Buna statik inceleme denir. Dosyayı izole bir ortamda açacaksan o ortamın ağ bağlantısını, kendi bilgisayarınla paylaşılan klasörlerini ve panosunu ayrıca kontrol et.

**Tracking pixel /
Canary token**

Uzak bir sunucudan yüklenen resim ya da işaretlenmiş bir dosya, açıldığı anda bir istek gönderebilir. Bu istek, dosyanın ne zaman ve hangi IP adresinden açıldığını ele verebilir.

Public upload

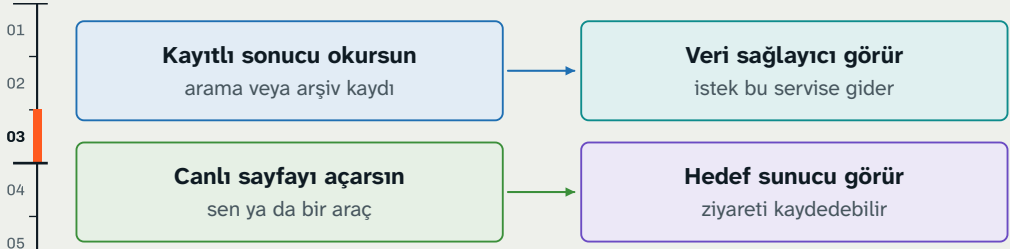
Herkese açık bir tarama servisine yüklediğin dosya başkalarıyla paylaşılabilir. Bu yüzden hassas bir kanıtı onay almadan yükleme.

**Retention / Need
to know**

Veriyi ne kadar süre saklayacağını ve kimin görmesi gerektiğini işin başında belirle. Yalnızca bilmesi gerekenler erişsin.



Şekil 3.2 Böylece dosyanın hiçbir kodu çalışmadan önce aslını korumuş ve ortamı sınırlamış olursun. Açıldığı anda istek gönderebilen dosyalar olduğu için ağ bağlantısını ayrıca kontrol et.



Şekil 3.3 Her satırda solda yaptığın işi, sağda isteği kimin gördüğünü oku. Ayrım her zaman net değil. Arşiv sayfası canlı siteden resim yükleyebilir, ekran görüntüsü aracı da siteyi ziyaret eder. Hedefle temas gerekiyorsa önce izni ve kapsamı kontrol et.

Adım adım örnek

Birlikte yapalım

22. bölümde WannaCry'nin kontrol ettiği alan adını inceliyorum. Bu alan adına gönderdiğim her istek, karşıdaki sunucuya IP adresimi ve isteğin saatini gösterir. Kötü amaçlı yazılımla bağlantılı bir adrese bakmadan önce neyi ele vereceğimi ve her isteğin nereye gideceğini planlıyorum.

- 01** İznini ve işin sınırını kontrol et. Kişisel hesaplarını ve tarayıcı oturumlarını bu işin dışında tut.
- 02** Önce hedefe hiç gitmeyen kayıtlarla başla: RDAP kaydını kayıt sunucusundan, sertifikaları CT günlüklerinden okursun. Bu istekler alan adının sunucusuna gitmez.
- 03** Canlı sunucuya bir istek gerekiyorsa yalnız başlıkları iste (HTTP HEAD), sayfanın içeriğini indirme. İsteği ayrı bir çalışma ortamından gönder ve saatini UTC olarak not et.



Şekil 3.4 Hedefe hiç gitmeyen kayıtlardan başla. Canlı sunucuya giden tek istek en sona kalır ve IP adresinle saati karşı tarafa gösterir.

3.5

Sahada

Kendin dene

1

Tarayıcının parmak izine bak

Aç <https://coveryourtracks.eff.org/>

Yap Sayfayı araştırmada kullandığın tarayıcıda aç. “Test Your Browser” tarayıcının özelliklerini EFF’ye gönderir, bu yüzden istemiyorsan testi atlayıp aşağıdaki örnek sonucu oku. Çalıştırsan gerçek takip şirketi seçeneğini kapatabilirsin. Sonuçta “unique” ifadesini, bit değerini (sayı büyüdükçe tarayıcın daha kolay ayırt edilir), Time Zone ve Language satırlarını not et.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

https://coveryourtracks.eff.org/results?&aat=1&a=1111&t=1111&dnt=1111&fpi_whorls=... 27.09.2026

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	No
Blocking invisible trackers?	No
Protecting you from <u>fingerprinting</u> ?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique among the 348,199 tested in the past 45 days.**

Currently, we estimate that your browser has a fingerprint that conveys **at least 18.41 bits of identifying information.**

“unique” ifadesi, 348.199 tarayıcı ve 18,41 bit, Cover Your Tracks sonucunda kırmızı çerçevede. EFF Cover Your Tracks (CC BY), ekran görüntüsü 27.09.2026

Benim bulduğum Testin sonucu “Your browser has a unique fingerprint” idi. Kullandığım tarayıcı, son 45 günde test edilen 348.199 tarayıcı arasında tekti ve en az 18,41 bit ayırt edici bilgi taşıyordu. Ayrıntılarda saat dilimi “Europe/Istanbul”, dil “tr-TR” görünüyordu. Sayfaya göre her 221,36 tarayıcıdan yalnızca birinin dil değeri “tr-TR”.

Dikkat Sonuçta adın yok. Ama VPN açıkken de saat dilimi ve dil aynı kalır. Bu iki değeri tarayıcı gönderir ve VPN onlara dokunmaz.

2

PDF'in içindeki adları oku

Aç https://commons.wikimedia.org/wiki/File:JFKennedy_on_Ataturk_1963.pdf

Yap Sayfanın en altındaki “Metadata” (üst veri, dosyanın görünen metninden ayrı saklanan bilgiler) tablosuna in. “Short title”, “Author”, “Software used” ve “Conversion program” satırlarını yaz. Sonra “File history” bölümündeki yükleme tarihine bak.

```

Terminal: Wikimedia Commons API 27.09.2026

$ curl -s 'https://commons.wikimedia.org/w/api.php?action=query&titles=File:JFKennedy_on_Ataturk_1963.pdf&prop=imageinfo&iiprop=timestamp|metadata&format=json&formatversion=2' | jq -r '.query.pages[0].imageinfo[0] | "timestamp: \(.timestamp)", (.metadata[] | select(.name | IN("Title", "Author", "Creator", "Producer", "Page size")) | "\(.name): \(.value)")"'
timestamp: 2007-10-23T10:24:36Z
Title: JFKennedy1963_text.PDF
Author: mum
Creator: JFKennedy1963_text - Microsoft Word
Producer: Acrobat PDFWriter 4.05 for Windows NT
Page size: 596 x 842 pts (A4)

```

Aynı kayıt komut satırında

Author ve Creator satırları sarıda. Sayfadaki tabloda Creator, Software used adıyla geçiyor. Üst veriyi Commons API'sinden 27 Eylül 2026'da aldım.

Benim bulduğum Tabloda Short title “JFKennedy1963_text.PDF”, Author “mum” ve Software used “JFKennedy1963_text - Microsoft Word” yazıyordu. Conversion program satırında “Acrobat PDFWriter 4.05 for Windows NT”, Page size satırında “596 x 842 pts (A4)” vardı. Dosya Commons’a 23 Ekim 2007’de yüklenmiş. Kennedy’nin 1963 mesajının metni bir Word belgesinden Acrobat PDFWriter ile PDF’e çevrilmiş. Dosyanın içinde hala dosya adı ve bir kullanıcı adı duruyor.

Dikkat “Author” alanına dosyayı üreten program kendi kayıtlı kullanıcı adını yazar. Buradaki “mum” bu yüzden Kennedy değil.

3

Bülten bağlantısındaki kimliği tanı

Aç <https://mailchimp.com/developer/marketing/docs/e-commerce/>

Yap Sayfada (Ctrl+F, Mac’te Command+F) mc_eid’i ara ve geçtiği paragrafı oku. Gelen kutunda bir bülten varsa bağlantıyı açmadan sağ tıkla ya da telefonda basılı tut, adresini kopyala ve “?” işaretinden sonraki parametreleri (sunucuya gönderilen ek bilgiler, aralarında & işareti olur) yaz. Bülten yoksa sayfadaki mc_eid örneğini incele. Kendi bağlantı adresini kimseyle paylaşma.

```

Terminal: curl + grep 27.09.2026

$ curl -sL https://mailchimp.com/developer/marketing/docs/e-commerce/
| sed -e 's/<[^>]*>/g' | grep -oE 'The mc_eid parameter is [^.]*\\.|To
find a contact[^.]*\\.|For example, if your subscriber[?]*\\?unique_ema
il_id=[0-9a-f]*|The mc_cid parameter is [^.]*\\. '

The mc_eid parameter is a unique Mailchimp ID that identifies the reci
pient's email address, which you can use to associate orders with a co
ntact.

To find a contact's email address, make an API call to the Members end
point with the mc_eid as the value for the unique_email_id parameter.

For example, if your subscriber's link contains the tracking parameter
mc_eid=18d3c1adfe, you can find that customer's email address by makin
g a GET request to /lists/{list_id}/members?unique_email_id=18d3c1adfe
The mc_cid parameter is the Mailchimp ID for the campaign that generat
ed the link.

```

Aynı kayıt komut satırında

Mailchimp'e göre mc_eid e-posta adresine geri çevrilebiliyor. Bunu yazan iki satırı, 27 Eylül 2026'da geliştirici sayfasından curl ile çektiğim cümlelerde işaretledim.

Benim bulduğum Mailchimp'in geliştirici sayfasında mc_eid, alıcının e-posta adresini tanımlayan benzersiz bir Mailchimp kimliği olarak geçiyor. Sayfaya göre gönderen, bu değeri Members uç noktasına (Mailchimp'te abone bilgisini veren sorgu adresi) sorarak kişinin e-posta adresini bulabiliyor. Örnek değer mc_eid=18d3c1adfe. mc_cid ise bağlantıyı üreten kampanyanın kimliği.

Dikkat mc_eid'de e-posta adresin açıkça yazmaz. Gönderen onu yine de adrese çevirebilir. Böyle bir bağlantıyı açmak ya da başkasına iletmek, tıklayanın sen olduğunu gösterebilir.

Aklında kalsın

Ayrı bir çalışma ortamı kurmuş olsan bile hangi hesapla giriş yaptığını ve hangi bağlantıyı kullandığını kontrol et.



Şimdi sen

VPN açık. Kişisel hesabına da giriş yaptın. Kimliğin gizli mi?

Cevabı: sayfa 61

**Bulmaca**

Cover Your Tracks testini bitirdiğimde adres çubuğundaki sonuç bağlantısında fpi_whorls adlı, çözüldüğünde (adres için kodlanmış hali düz metne çevrildiğinde) 1.022 karakter tutan bir parametre vardı. Bu bağlantıyı bir forumda paylaştıyordum, adresle birlikte neyi paylaşmış olurdum? İpucu: testi kendin çalıştır ve adres çubuğunda fpi_whorls'tan sonra gelen kelimeleri oku.

Cevabı: sayfa 61

**Öğrendiğini kontrol et**

Hedef sitenin arşivlenmiş bir kopyasını açıyorsun. Hedefin bu ziyareti hiç görmeyeceğini varsayabilir misin?

Cevabı: sayfa 61

Bu bölümün terimleri**OPSEC**

Operasyon güvenliği: araştırma sırasında kimliğini, yaptığın işi ve topladığın veriyi koruma.

Threat model

Kimin neyi görebileceğini ve bunun nasıl zarara yol açabileceğini baştan düşünme.

Passive collection

Burada: başka bir yerde zaten kayıtlı veriyi okuma.

Active collection

Burada: hedefe yeni istek gönderme.

Data minimization

Yalnızca iş için gereken veriyi tutma.

Sock puppet / Browser fingerprint

Yalnızca araştırma için açılmış ayrı hesap / dil, ekran boyutu gibi tarayıcı özelliklerinden oluşan ve seni ayırt edebilen iz.

Canary token / Tracking pixel

Açıldığında veya kullanıldığında bir sunucuya istek gönderebilen gizli işaret. Örneğin uzak bir resim ya da işaretli bir dosya.

Kaynaklar

1. CSINT Research, WannaCry kill-switch domain records, captured 8 September 2026
<https://csintresearch.org/haber/wannacry-kill-switch>
2. Google, Incognito limits
<https://support.google.com/chrome/answer/9845881?hl=en>
3. Thinkst, Canarytokens
<https://docs.canarytokens.org/guide/>

Gerçek vakalar

Bu kısımda her bölüm tek bir gerçek olayı ele alıyor. Soruyu yazıyorum, kamuya açık kayıtları tarihleriyle diziyorum, her kaydın neyi gösterip neyi göstermediğini ayırıyorum. Kitabın ilk beş kısmındaki yöntemleri burada gerçek belgeler üzerinde görüyorsun.

- 19 Süveyş 2021'de kanal açılınca kuyruk da bitti mi?
- 20 Kilauea'nın zirvesi 2018'de ne kadar sürede çöktü?(tam sürümde)
- 21 2020 Beyrut hasar haritasındaki kırmızı hücreler(tam sürümde)
- 22 WannaCry alan adındaki üç tarih(tam sürümde)
- 23 Vice'ın McAfee yazısındaki iki fotoğraf dosyası(tam sürümde)
- 24 BTK disketindeki ad ve onu sınavan kayıtlar(tam sürümde)
- 25 Gilgo Beach kefalet belgesinde sınavabildiklerim(tam sürümde)
- 26 2026 ortalama zincirinde hangi bulgu kimin?(tam sürümde)
- 27 Bamako'daki 2025 kitleyi yoldaki saldırılara ne bağlıyor?(tam sürümde)

Süveyş 2021'de kanal açılınca kuyruk da bitti mi?

Kanal 29 Mart 2021'de yeniden açıldı. NASA'nın Leth Agencies'ten aktardığı sayıya göre ertesi gün 184 gemi hala bekliyordu. Bu bölümde açılışı ve kuyruğu iki ayrı soru olarak sınıyorum.

Olay Süveyş Körfezi, Mısır, 23-29 Mart 2021

Soru 29 Mart 2021'de kanal yeniden açıldığında, girişte bekleyen gemi kuyruğu da dağılmış mıydı?

Bu bölümde

19.1 Ne olmuştu?

19.2 Elimdeki kayıtlar

19.3 Gündüz görüntüsündeki küçük izler

19.4 Aynı körfeze gece bakınca

19.5 29 Mart duyurusunda ne yazıyor?

19.1 Ne olmuştu?

Ever Given adlı konteyner gemisi 23 Mart 2021'de Süveyş Kanalı'nda karaya oturdu. Akdeniz ile Kızıldeniz arasındaki geçiş kesildi ve kanala girmek isteyen gemiler iki uçta beklemeye başladı. Avrupa Uzay Ajansı'nın (ESA) 26 Mart'ta yayımladığı Sentinel-1 radar karşılaştırmasında 21 Mart'taki olağan trafik ile 25 Mart'taki tıkanma yan yana görülüyor.

29 Mart'ta Ever Given yüzdürüldü ve gemiler kanaldan yeniden geçmeye başladı. Ben ise girişte biriken gemilerin de o gün dağılıp dağılmadığını merak ediyordum. İki soru aynı olaya ait, ama cevapları farklı kayıtlarda duruyor. Bu yüzden onları baştan ayrı yazdım.



Şekil 19.1 Kanal 29 Mart'ta açıldı, ertesi gün 184 gemi hala sıradaydı. Bu iki günü birbirine karıştırma.

19.2 Elimdeki kayıtlar

Her kayıt için iki tarihi ayrı yazdım. Biri kaydın yayımlandığı gün, öteki görüntünün çekildiği gün. NASA'nın yazısı 31 Mart'ta yayımlandı, ama içindeki görüntüler 1 Şubat ile 29 Mart arasında çekildi.

NASA'nın dosya adları da bir tarih taşıyor. suezcanaL_oli_202186_lrg.jpg adındaki 202186, 2021 yılının 86. günü demek. Bu da 27 Mart. Beş dosya adındaki gün numaralarını tarihe çevirdim. Beşi de NASA'nın yazdığı çekim tarihleriyle aynı çıktı.

Kayıtlar, yayın ve çekim tarihleriyle

Kayıt	Yayın	Çekim veya olay
NASA Earth Observatory, gündüz görüntüleri (Landsat 8)	31 Mart 2021	11 ve 27 Mart 2021
NASA Earth Observatory, gece görüntüleri (VIIRS)	31 Mart 2021	1 Şubat, 27 ve 29 Mart 2021
Süveyş Kanal İdaresi duyurusu	29 Mart 2021	Geminin yüzdürülmesi
ESA, Sentinel-1 radar karşılaştırması	26 Mart 2021	21 ve 25 Mart 2021

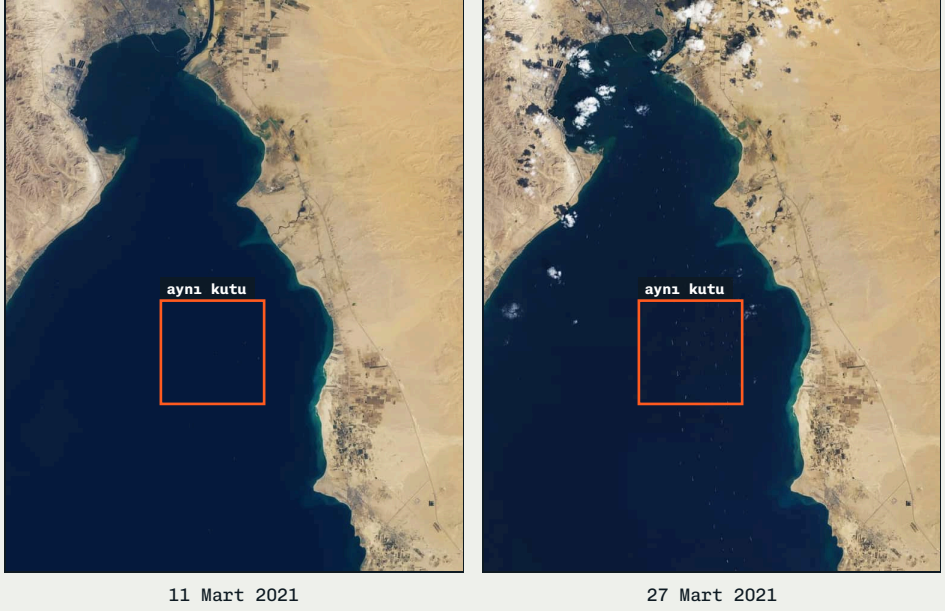


Şekil 19.2 Aynı adımları NASA'nın beş dosya adına uyguladım. Sen de bir dosya adındaki gün numarasını takvimde bul ve yazılan çekim tarihiyle karşılaştırdım.

19.3 Gündüz görüntüsündeki küçük izler

İki gündüz görüntüsü 11 ve 27 Mart'ta çekilmiş. Önce aynı yere baktığımdan emin olmak istedim. Kıyı çizgisi ve körfezin daralan kuzey ucu iki görüntüde de aynı. Bu yüzden ikisine aynı kırpmayı uyguladım.

27 Mart'ta deniz üzerinde çok daha fazla küçük, uzun iz seçiliyor. NASA bu izleri bekleyen gemiler olarak açıklıyor. Ben izleri saymadım. Bulutlar bazı bölgeleri örtüyor ve yan yana duran küçük izler her zaman birbirinden ayrılmıyor. Bu görüntüden bir gemi sayısı çıkarsaydım, göremediğim şeyi sayıyormuş gibi yapmış olurum.

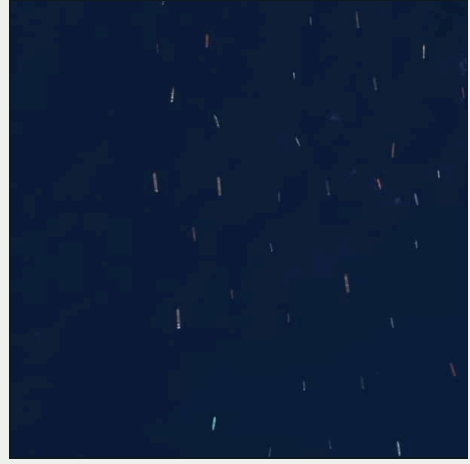


Şekil 19.3 Kıyı çizgisi ve körfezin kuzey ucu iki karede aynı, bu yüzden kutuyu iki görüntüde aynı piksellere koydum. 27 Mart karesinde kutunun içinde çok daha fazla küçük, uzun iz var.

Görsel: NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; USGS Landsat 8. NASA görsel kullanım yönergeleri: kaynak gösterilerek kullanılabilir. NASA'nın bu kitabı onayladığı anlamına gelmez.



11 Mart, kutunun içi



27 Mart, kutunun içi

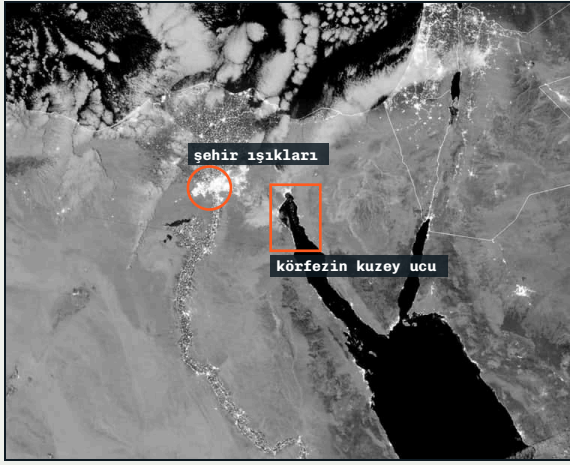
Şekil 19.4 Kutunun içini NASA'nın tam çözünürlüklü dosyasından kestim. NASA bu çizgileri bekleyen gemiler olarak açıklıyor. Bulutlu yerler ve yan yana duran izler yüzünden onları saymadım.

Görsel: NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; USGS Landsat 8. NASA görsel kullanım yönergeleri: kaynak gösterilerek kullanılabilir. NASA'nın bu kitabı onayladığı anlamına gelmez.

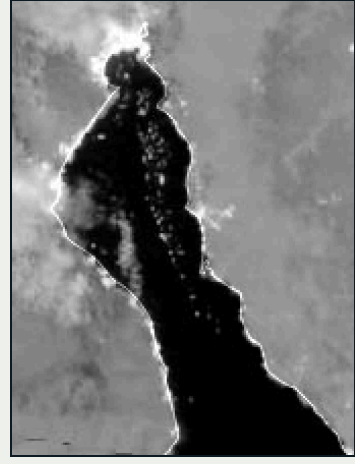
19.4 Aynı körfeze gece bakınca

Gece görüntüleri, Suomi NPP uydusundaki VIIRS aygıtından geliyor. Bu aygıt geceleri ışığı kaydediyor. Görüntüye bakarken önce karadaki şehir ışıklarını buldum, sonra körfezin içindeki noktalara geçtim. Böyle bakınca deniz üzerindeki ışıkların birikmesi daha kolay fark ediliyor.

Gündüz ve gece görüntülerinin çözünürlüğü farklı. Bu yüzden onları üst üste koyup piksel piksel eşleştirmedim. Bir ışık noktasından geminin adını ya da yükünü de çıkaramadım. Gece görüntüsünden öğrendiğim tek şey, o gece körfezin içinde ışık olduğu.



27 Mart 2021 gecesi



Kutunun içi, 4 kat

Şekil 19.5 Önce karadaki şehir ışıklarını buldum, sonra körfezin içine baktım. Sağdaki büyütmede pikselleri yumuşatmadım, her kare görüntünün kendi pikseli. Işık noktalarından gemi adı ya da sayısı çıkmıyor.

Görsel: NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; Suomi NPP VIIRS. NASA görsel kullanım yönergeleri: kaynak gösterilerek kullanılabilir. NASA'nın bu kitabı onayladığı anlamına gelmez.

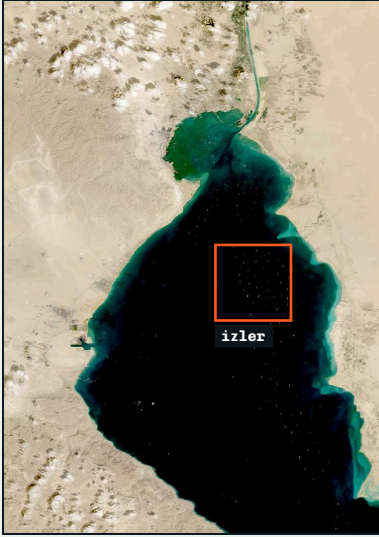


Şekil 19.6 Gece görüntüsünden çıkan tek şey körfezde ışık olduğu. Gemi sayısı ya da gemi adı için başka bir kayıt lazım.

19.5 29 Mart duyurusunda ne yazıyor?

Süveyş Kanal İdaresinin 29 Mart duyurusunun başlığında Ever Given'ın başarıyla yüzdürüldüğü yazıyor. Yalnızca başlığı okusaydım işin bittiğini düşünebilirdim. Metinde ise geminin yönünün yüzde 80 düzeltildiği, manevraların süreceği ve geçişin gemi tamamen hizalandıktan sonra başlayacağı yazıyor.

NASA 31 Mart'taki yazısında gemilerin 29 Mart'ta kanaldan yeniden geçmeye başladığını, bekleyen gemilerin dağılmasının ise zaman alacağını yazıyor. Aynı yazı, kanal hizmet şirketi Leth Agencies'e dayanarak 30 Mart'ta hala 184 geminin beklediğini aktarıyor. Duyuru ile bu yazı birbiriyle çelişmiyor. Aynı günün farklı anlarını anlatıyorlar. Leth Agencies'in verdiği sayıya göre kuyruk 29 Mart'ta dağılmamıştı. Bu sayıyı NASA'dan okudum, kendim doğrulamadım.



29 Mart 2021, Sentinel-2



Kutunun içi, 3 kat

Şekil 19.8 Duyurunun yayımlandığı gün körfezde hala çok sayıda iz var. Worldview bu görüntü için yalnız günü veriyor, saati vermiyor. Bu yüzden görüntünün gemi yüzdürülmeden önce mi sonra mı çekildiğini bilmiyorum.

Görsel: NASA Worldview (ESDIS); HLS S30, NASA LP DAAC; contains modified Copernicus Sentinel data 2021. NASA verisi, kullanım kısıtı yok. Worldview kaynak olarak anılıyor.

Duyurudan, özetle (29 Mart 2021)

Başlık: Successful Refloating of EVER GIVEN

Yön düzeltmesi: %80

Durum: manevralar sürüyor

Geçiş: gemi tamamen hizalanınca

Duyurunun tam metni için kaynak listesine bak.

Kayıt ne gösteriyor?**Buradan ne çıkarabiliriz?**

1

27 Mart gündüz
görüntüsünde denizde daha
çok küçük iz

NASA bunları bekleyen gemiler
diye açıklıyor. Sayılmadı

2

29 Mart gece kaydında
körfez içinde ışıklar

Gemiler hala bekliyor
olabilir. Açılışa göre saati
belli değil

3

29 Mart duyurusuna göre
yön yüzde 80 düzeltildi

Geçiş, gemi tamamen
hizalanınca başlayacak.
Kuyruğun dağıldığı yazmıyor

Şekil 19.7 Sol sütun her kaydın gösterdiğini, kesikli sağ sütun bundan ne okunabileceğini verir. AIS verisi kullanılmadığı için gemi kimliği veya kesin kuyruk uzunluğu çıkarılamaz.

Kayıtlarla söyleyebileceğim

- Kanal 29 Mart 2021'de yeniden açıldı. Bu tarih NASA'nın yazısında var. Kanal idaresinin duyurusu da geçişin gemi tamamen hizalandıktan sonra başlayacağını bildiriyor.
- 27 Mart'ta körfezde 11 Mart'a göre çok daha fazla iz var. NASA bunları bekleyen gemiler olarak açıklıyor.
- 29 Mart duyurusu işin sürdüğünü anlatıyor. NASA'nın Leth Agencies'ten aktardığı sayıya göre 30 Mart'ta hala 184 gemi bekliyordu.

Söyleyemeyeceğim

- Görüntülerden kaç gemi beklediğini. İzleri saymadım. Yukarıdaki 184 sayısını NASA, Leth Agencies'ten aktarıyor.
- Görüntülerdeki herhangi bir geminin adını ya da yükünü.
- Kuyruğun tam olarak hangi gün ya da saatte dağıldığını.
- Tıkanmanın ekonomik zararını ya da kimin sorumlu olduğunu.

Bu vakada kullandığım yöntemler

- Bölüm 1, Önce soruyu yaz (sayfa 12)
- Bölüm 2, Kaynak ile iddiayı ayır (sayfa 24)
- Bölüm 6, Fotoğrafa üç açıdan bak (tam sürümde)
- Bölüm 7, Nerede? Ne zaman? (tam sürümde)

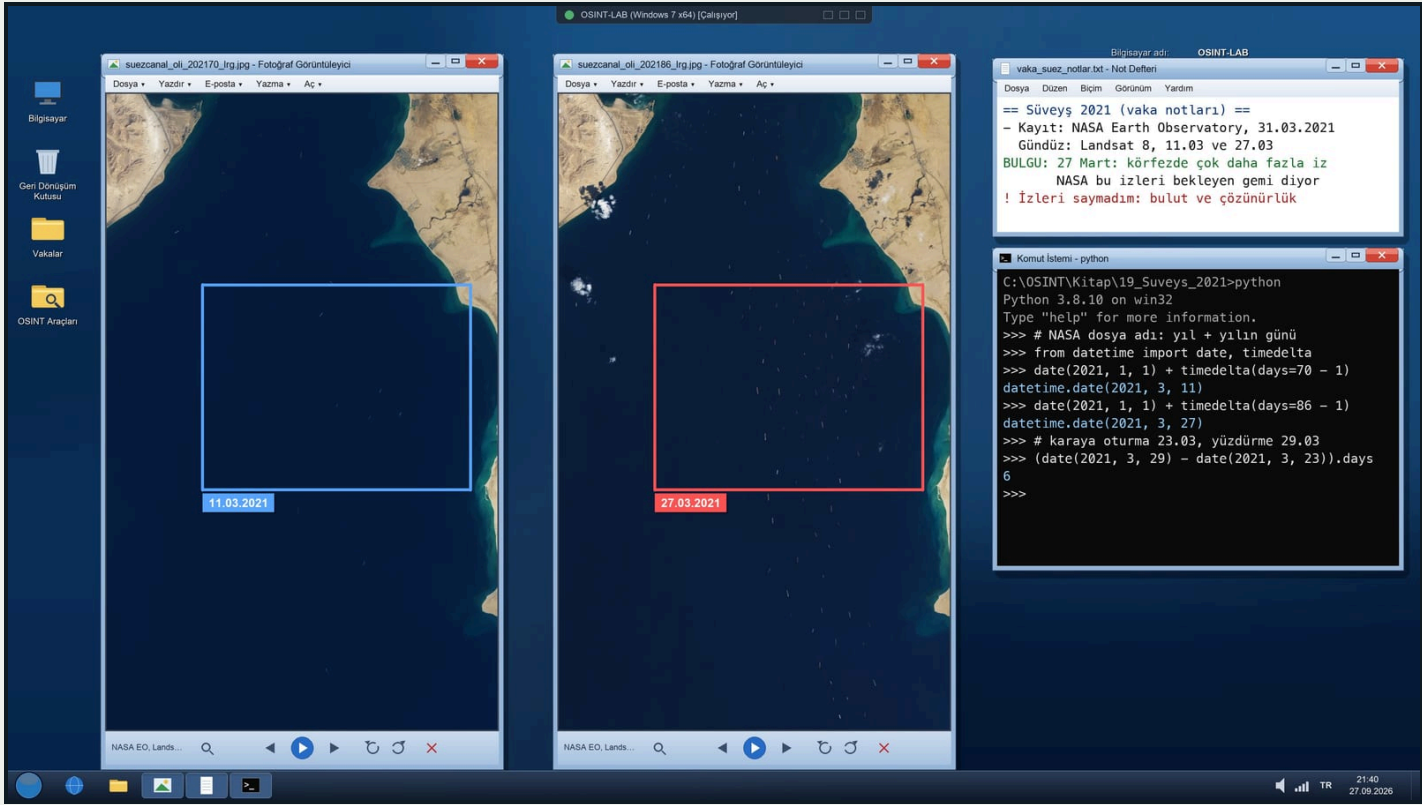
Şimdi sen

Bir haber sitesi 29 Mart akşamı “Süveyş'te trafik normale döndü” diye yazsaydı, bu cümleyi hangi kayıtlarla sınırdın? Bu bölümdeki kayıtlardan hangisi bu sınamada eksik kalırdı?

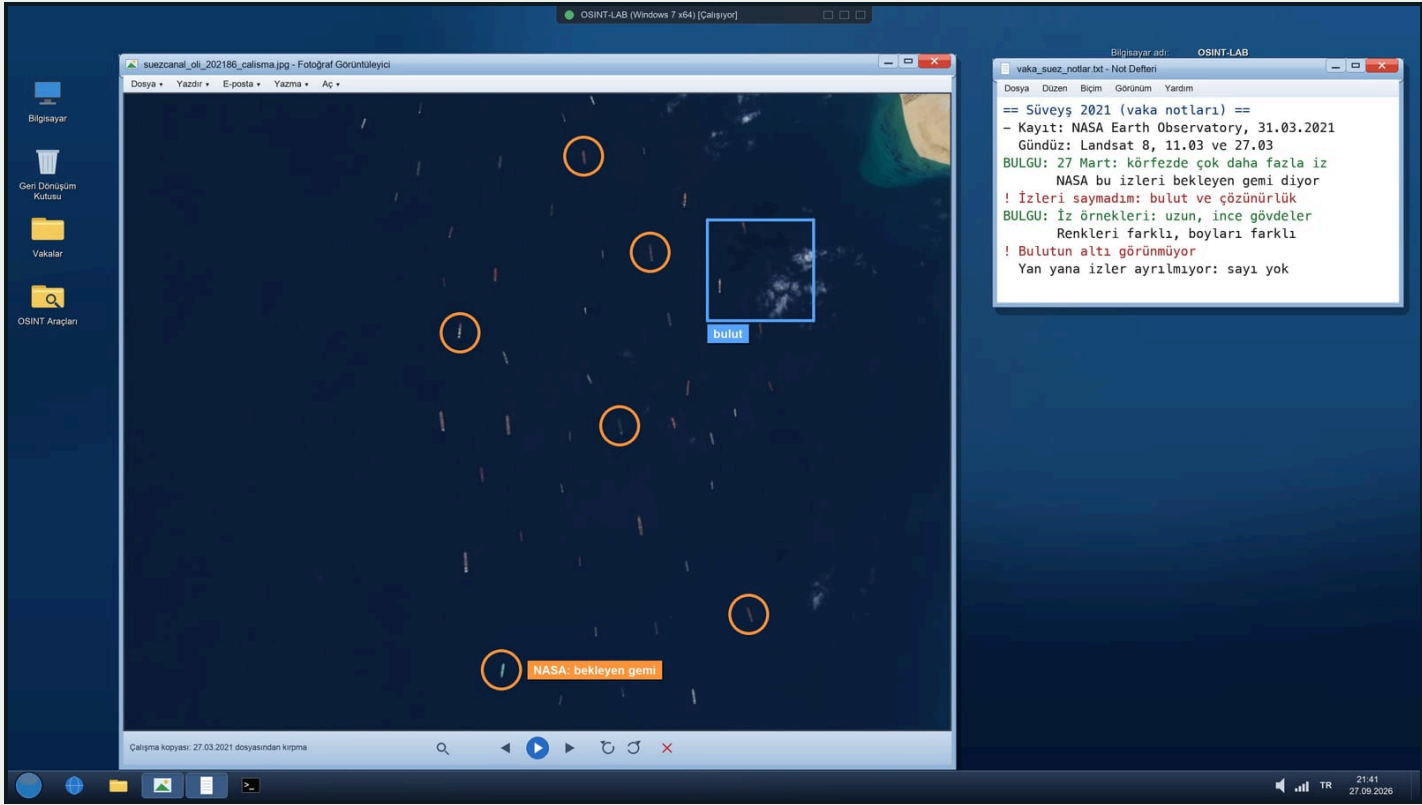
Cevabı: sayfa 62

Kaynaklar

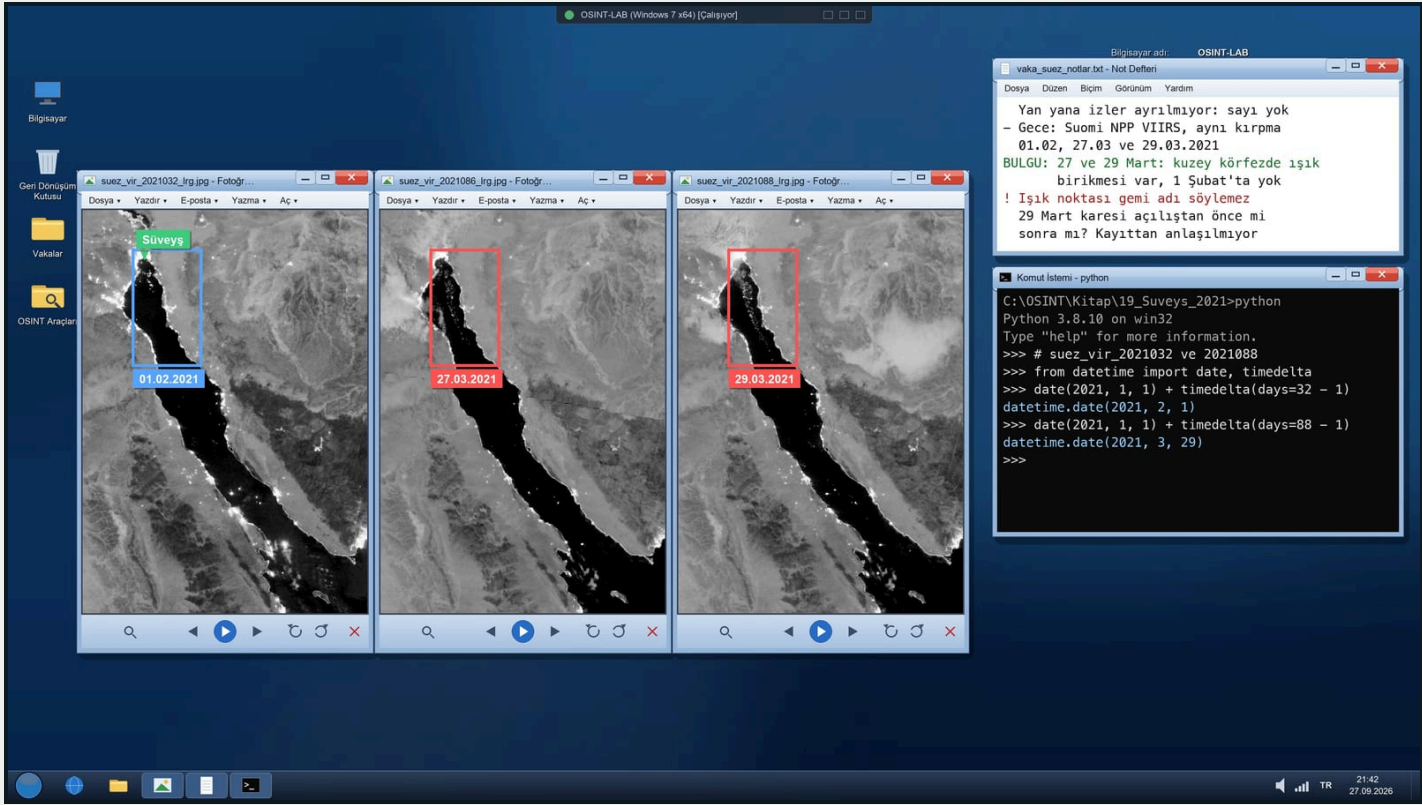
1. NASA Earth Observatory, Traffic Jam on the Suez Canal (31 March 2021). Gündüz ve gece görüntüleri, çekim tarihleri ve NASA'nın yorumu.
<https://science.nasa.gov/earth/earth-observatory/traffic-jam-on-the-suez-canal-148114/>
2. Suez Canal Authority, Successful Refloating of EVER GIVEN (29 March 2021). Başlık ile metin birlikte okundu.
https://www.suezcanal.gov.eg/English/MediaCenter/News/Pages/nav_29-03-2021.aspx
3. ESA, Suez Canal traffic jam seen from space (26 March 2021). Aynı bir radar gözlemi. Görselleri bu kitapta kullanılmadı.
https://www.esa.int/ESA_Multimedia/Images/2021/03/Suez_Canal_traffic_jam_seen_from_space
4. NASA, Images and Media Usage Guidelines. NASA görsellerinin kullanım koşulları.
<https://www.nasa.gov/nasa-brand-center/images-and-media/>



Şekil 19.9 Gündüz görüntüsündeki küçük izler. Aynı kırpmayı, iki tarih: solda 11 Mart, sağda 27 Mart 2021. Kutu iki karede aynı yeri gösteriyor. Python oturumu, NASA'nın dosya adlarındaki gün numarasını tarihe çeviriyor. Görüntüler: NASA Earth Observatory, USGS Landsat 8.



Şekil 19.10 Gündüz görüntüsündeki küçük izler. 27 Mart görüntüsünün çalışma kopyası. Halkalar, NASA'nın bekleyen gemi olarak açıkladığı izlerden birkaçını işaretliyor. Mavi kutudaki bulutun altı görünmüyor. İzleri saymadım. Görüntü: NASA Earth Observatory, USGS Landsat 8.



Şekil 19.11 Aynı körfeze gece bakınca. Üç gece, aynı kırpma: 1 Şubat, 27 Mart ve 29 Mart 2021. Kutular körfezin kuzey ucunu gösteriyor. 27 ve 29 Mart'ta orada ışık birikiyor. Görüntüler: NASA Earth Observatory, Suomi NPP VIIRS.

Cevap anahtarı

1. Önce soruyu yaz

“Süveyş Kanalı hakkında bilgi topla” görevini nasıl daraltırsın?

Örneğin “27 Mart 2021’de Süveyş Körfezi’nde kanala girmeyi bekleyen gemiler var mıydı?” diye sorabilirsin. Bu soruda hem yer hem tarih belli. Cevabını NASA’nın o güne ait uydu görüntüsü gibi bir kayıttan arayabilirsin. Aynı ölçüde dar başka bir soru da seçebilirsin.

İlk kaydedilen .com alan adı olarak bilinen symbolics.com’un RDAP kaydında (alan adının kayıt bilgisi, rdap.verisign.com/com/v1/domain/symbolics.com) kayıt zamanı 1985-03-15T05:00:00Z, bitiş zamanı 2027-03-16T04:00:00Z. Tarihle saati aradaki T ayırır, sondaki Z ise saatin UTC olduğunu gösterir. Aynı kayıttan saat neden bir yerde 05.00, öbür yerde 04.00? İpucu: yaz saatini düşün.

İkisi de New York saatiyle gece yarısı. IANA saat dilimi veritabanına göre ABD’de 1976 ile 1986 arasında yaz saati nisanın son pazarı başlıyordu. 15 Mart 1985’te yaz saati henüz başlamamıştı, New York UTC-5’teydi ve gece yarısı 05.00 UTC ediyordu. 2007’den beri yaz saati martın ikinci pazarı başlıyor.

Bu yüzden 16 Mart 2027’de New York yaz saatinde (UTC-4) olacak ve gece yarısı 04.00 UTC edecek. Eylülde kaydedilen google.com’un kayıt zamanı da 04.00 UTC, çünkü o gün de yaz saati geçerliydi.

Görev, bir hizmet kesintisinin kurumu etkileyip etkilemediğini bulmak. İlk listede 500 çalışan adı var. Ne yaparsın?

Önce kurumun hangi hizmeti kullandığını kontrol ederim. 500 kişilik çalışan listesi bu soruyu cevaplamaz. Sorunun gerektirmediği kişisel veriyi de saklamam.

2. Kaynak ile iddiayı ayır

Admiralty sisteminde F6 “yanlış” anlamına mı gelir?

Hayır. F6 yazan kişi, ne kaynağın güvenilirliğini ne de bilginin inandırıcılığını ölçebildiğini kaydeder. Bilmediğin bir şeyi yanlış ilan edemezsin.

Guardian'ın okur temsilcisi 4 Mayıs 2009 tarihli yazısında, uydurma sözün Wikipedia'ya ikinci eklenişinde sayfada yalnızca altı dakika, üçüncüsünde yaklaşık 25 saat kaldığını yazdı. Maurice Jarre sayfasının 30 ve 31 Mart 2009 geçmişine göre altı dakika kalan ekleme hangisi? İpucu: 2. görevdeki geçmiş sayfasında her satırın artı ya da eksi bayt sayısına bak. Sözü ekleyen ve silen satırları "prev" ile doğrula.

Üçüncüsü. Geçmişte söz üç kez ekleniyor. Birincisi 30 Mart 02.29'da eklenip 11.51'de silinmiş. İkincisi 30 Mart 14.13'te eklenmiş ve 31 Mart 15.07'de "no unsourced quotes" notuyla silinene kadar yaklaşık 25 saat kalmış. Üçüncüsü 31 Mart 17.03'te eklenmiş, 17.09'da geri alınmış. Sayfada 6 dakika kalan bu. Yazıdaki sıra sayfa geçmişleriyle uyuşmuyor. Yazıya göre söz 30 Mart'ta iki kez silinmiş, ama geçmişte o gün tek silme var.

Üç haber aynı isimsiz paylaşımı dayanıyor. Kaynak sayısını nasıl yazarsın?

Üç yayın var ama bilginin tek bir kaynağı var. Aynı bilginin tekrarını yeni kanıt saymam. Bağımsız bir doğrulama ararım.

3. Aramadan önce ortamı hazırla

VPN açık. Kişisel hesabına da giriş yaptın. Kimliğin gizli mi?

Hayır. VPN çıkış IP adresini değiştirir ama giriş yaptığın hesabı gizlemez. Site o hesabı görür.

Cover Your Tracks testini bitirdiğimde adres çubuğundaki sonuç bağlantısında fpi_whorls adlı, çözüldüğünde (adres için kodlanmış hali düz metne çevrildiğinde) 1.022 karakter tutan bir parametre vardı. Bu bağlantıyı bir forumda paylaştıyım, adresle birlikte neyi paylaşmış olurdum? İpucu: testi kendin çalıştır ve adres çubuğunda fpi_whorls'tan sonra gelen kelimeleri oku.

Tarayıcımın parmak izinin bir parçasını. Parametre, adrese gömülü bir JSON (verileri ad ve değer çiftleri halinde yazan bir metin biçimi). İçinde plugins (eklenti listesi), hardware_concurrency (işlemci çekirdeği sayısı), audio (ses parmak izi), canvas_hash_v2 ve webgl_hash_v2 (çizim

testlerinin hash değerleri) alanları var. Adım ya da IP adresim yok, ama sayfa, canvas sonucunun aynı makinede genelde kullanıcıyı ayırt edecek kadar sabit kaldığını yazıyor.

Hedef sitenin arşivlenmiş bir kopyasını açıyorsun. Hedefin bu ziyareti hiç görmeyeceğini varsayabilir misin?

Hayır. Arşiv sayfası bazı resimleri canlı siteden yükleyebilir. Hangi isteğin nereye gittiğini kontrol etmeden hedefle temas olmadığını varsaymam.

19. Süveyş 2021’de kanal açılınca kuyruk da bitti mi?

Bir haber sitesi 29 Mart akşamı “Süveyş’te trafik normale döndü” diye yazsaydı, bu cümleyi hangi kayıtla sınardın? Bu bölümdeki kayıtlardan hangisi bu sınamada eksik kalırdı?

Cümle kanaldaki trafikle ilgili. Onu sınamak için 29 Mart’tan sonraki günlerde kanaldan geçen gemileri tarihleriyle sayan bir kayıt gerekir. Kanal idaresinin sonraki duyuruları ya da tarihli gemi izleme (AIS) verisi bu işi görür. NASA’nın Leth Agencies’ten aktardığı sayı (30 Mart’ta 184 bekleyen gemi) cümleyle zaten çelişiyor.

Ama bu ikinci el bir sayı ve onu birinci elden bir kayıtla doğrulamak gerekir. 29 Mart duyurusu işe yaramaz, çünkü orada manevraların sürdüğü yazıyor. 29 Mart gece görüntüsü de işe yaramaz. Görüntüde çekim saati yok ve ışıkların hangi gemilere ait olduğu belli değil.

Görseller ve haklar

Şekiller ve tablolar, açıkladıkları metne dayanarak bu kitap için çizildi. Fotoğraflar ve uydu görüntüleri kamuya açık kayıtlardır, sahiplerinin istediği atıfla kullanıldı. Sahada görevlerindeki ekran görüntüleri, kamuya açık sayfalardan inceleme amacıyla kaynağı ve tarihiyle alıntılanmış kesitlerdir. Terminal görüntüleri çalıştırdığım komutları ve gerçek çıktılarını gösteriyor. Görsellerin hiçbirini yapay zeka ile üretilmedi.

1. Kapak: Süveyş Körfezi, 27 Mart 2021, Landsat 8. NASA, denizdeki küçük izleri bekleyen gemiler olarak açıklıyor. Görüntü, 19. bölümde incelenen kayıtlardan biridir. NASA Earth Observatory / Lauren Dauphin, Joshua Stevens; USGS Landsat 8.
2. Bölüm 19, çalışma ekranı: Aynı kırpma, iki tarih: solda 11 Mart, sağda 27 Mart 2021. Kutu iki karede aynı yeri gösteriyor. Python oturumu, NASA'nın dosya adlarındaki gün numarasını tarihe çeviriyor. Görüntüler: NASA Earth Observatory, USGS Landsat 8.
3. Bölüm 19, çalışma ekranı: 27 Mart görüntüsünün çalışma kopyası. Halkalar, NASA'nın bekleyen gemi olarak açıkladığı izlerden birkaçını işaretliyor. Mavi kutudaki bulutun altı görünmüyor. İzleri saymadım. Görüntü: NASA Earth Observatory, USGS Landsat 8.
4. Bölüm 19, çalışma ekranı: Üç gece, aynı kırpma: 1 Şubat, 27 Mart ve 29 Mart 2021. Kutular körfezin kuzey ucunu gösteriyor. 27 ve 29 Mart'ta orada ışık birikiyor. Görüntüler: NASA Earth Observatory, Suomi NPP VIIRS.
5. Bölüm 1, sahada: 1990-09-17 kayıt tarihi, IANA'nın .tr sayfasının en altında kırmızı çerçevede. IANA, ekran görüntüsü 27.09.2026.
6. Bölüm 1, sahada: Telefonda açılan TÜİK bülteni. Kırmızı çerçevedeki satır yayım tarihi, 09 Şubat 2026 10:00. Türkiye İstatistik Kurumu (TÜİK), ekran görüntüsü 27.09.2026.
7. Bölüm 3, sahada: "unique" ifadesi, 348.199 tarayıcı ve 18,41 bit, Cover Your Tracks sonucunda kırmızı çerçevede. EFF Cover Your Tracks (CC BY), ekran görüntüsü 27.09.2026.

Kitabın tam sürümü

Bu dosyada kitabın 27 bölümünden 1, 2, 3 ve 19. bölümler var. Tam sürümde 18 yöntem bölümü ve kamuya açık kayıtlardan adım adım izlenen 9 gerçek vaka bulunuyor. Kitabın sonunda “Türkiye’de kamuya açık kayıtlar ve hukuki çerçeve” başlıklı bir ek, bütün alıştırma cevapları, terim dizini ve kaynakçanın tamamı yer alıyor. Kitap PDF biçiminde.

Kısım 1: Önce nasıl düşünürüz?

- 01 Önce soruyu yaz *(bu dosyada)*
- 02 Kaynak ile iddiayı ayır *(bu dosyada)*
- 03 Aramadan önce ortamı hazırla *(bu dosyada)*

Kısım 2: Bul, sakla, kontrol et

- 04 Aramayı daralt
- 05 Bulduğun şeyi kaybetme
- 06 Fotoğrafa üç açıdan bak
- 07 Nerede? Ne zaman?
- 08 Satırları düzenle

Kısım 3: İnsanlar ve kurumlar

- 09 Hesap ile kişiyi ayır
- 10 Markanın arkasındaki kaydı bul

Kısım 4: İnternetin kayıtları

- 11 Ad, adres ve DNS
- 12 Sertifikadaki adı oku
- 13 E-postada hangi ad kontrol edilir?
- 14 Sunucu kimin? Kanıt ne?

Kısım 5: Çalışmayı bitir

- 15 Gizlilik ve anahtarlar
- 16 Aracı yaptığı işle öğren
- 17 Küçük bir dosyayla çalış
- 18 Bildiğini kısa yaz

Kısım 6: Gerçek vakalar

19 Süveyş 2021’de kanal açılınca kuyruk da bitti mi? (bu dosyada)

20 Kilauea’nın zirvesi 2018’de ne kadar sürede çöktü?

21 2020 Beyrut hasar haritasındaki kırmızı hücreler

22 WannaCry alan adındaki üç tarih

23 Vice’ın McAfee yazısındaki iki fotoğraf dosyası

24 BTK disketindeki ad ve onu sınavan kayıtlar

25 Gilgo Beach kefalet belgesinde sınavabildiklerim

26 2026 ortalama zincirinde hangi bulgu kimin?

27 Bamako’daki 2025 kitleyi yoldaki saldırılara ne bağlıyor?

Tam sürüm için: csintresearch.org/gosi-kitap

Yazar hakkında

Ahmet Göker açık kaynak araştırmacısı ve tehdit analisti. CSINT Research'te araştırma dosyalarını, geliştirdiği araçları ve çalışma notlarını yayımlıyor. Gerçek vakaları adım adım anlattığı videolar YouTube'da @shadowintel_ kanalında. Bulmacaları ve gerçek suç belgesellerini seviyor. En çok ilgisini çeken şey, yıllarca kapalı kalan bir dosyanın küçük bir ayrıntıyla nasıl açıldığı.

csintresearch.org

youtube.com/@shadowintel_