ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

2 Aylık Siber Güvenlik Dergisi • 14 TL • 7. SAYI - 2019

"Adaletsizliğe şahit olduğumuz ve tepki göstermediğimiz her an, kişiliğimizi pasif kalması için eğitmiş; sonunda da hem kendimizi hem de sevdiklerimizi haksızlık karşısında savunma yeteneğimizi yitirmiş oluyoruz."

Julian Assange

ISSN 2618-6373 07

9 772618 637008

KÜNYE

YIL: 2 Sayı: 7 - ISSN: 2618-6373 - www.arkakapidergi.com

2 ayda bir yayımlanır.

Abaküs Kitap Yayın Dağıtım Hizmetleri adına sahibi:

Selda Ustabaş Demiryakan

Merkez: Hobyar Mah. Cemal Nadir Sok. No:24/178 Cağaloğlu - İST. Tel: 0212 514 68 61

Genel Yayın Yönetmeni: Cevahir Demiryakan - cevahir@cirakdergi.com

Sorumlu Yazı İşleri Müdürü: Ziyahan Albeniz - ziyahan@arkakapidergi.com

Grafik Tasarım: Cem Demirezen - grafik@abakuskitap.com

Düzelti: Huriye Özdemir

Dış Haber: Oğuz Aydınyılmaz

Yayın Koordinatörü: Şahin Solmaz

İletişim Sorumlusu ve Reklam: Seba Bingöl - muhasebe@abakuskitap.com

Hukuk Müşaviri: Avukat Mehmet Pehlivan - Pehlivan İlkakın Hukuk Bürosu

Sosyal Medya: Oğuz Aydınyılmaz - Recep Kızılarslan

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

Baskı: Ezgi Matbaacılık San. Tic. Ltd. Şti. Sanayi Cad. Altay Sok. No:14
Çobançeşme-Yenibosna/İSTANBUL
Tel: 0212 452 23 02 / Matbaa Sertifika No: 12142

EDİTÖRDEN

Yeni bir sayıdan merhaba!

Yazacak ne çok şey birikmiş.

Bu yazıyı yazdığımız tarih 1 Mayıs. Uluslarası emek ve dayanışma günü. Tüm işçi ve emekçilere, emek dostlarına kutlu olsun. Ülkemize barış, demokrasi ve adalet getirsin.

Yaşamın içerisinde öyle harikuladelikler var ki, çoğumuz için vaka-ı adiyeden olmuşlar. Ya içlerine doğmuşuz ya akli baliğ olduğumuzda önümüzde hazır bulmuşuz.

Uluslararası bir çalışma standardı olan 8 saatlik iş günü de bunlardan biri.

Oysa 1 Mayıs'ı 1 Mayıs yapan; 19. yüzyıl sonlarında işçilerin burjuva sınıfı ile insanca yaşam koşulları için giriştiği kıran kırana mücadele idi.

8 saatlik iş günü talebi için Chicago'da yükselen işçi eylemlerinde pek çok işçi hayatını kaybetti. Bu işçi hareketine önderlik eden dört işçi idam edildi: Albert PERSONS, Adolph FISCHER, George ENGEL ve August SPIES...

Bugün alelade bir realite sayılan 8 saatlik iş günü hakkı için işte böylesi bedeller ödenmişti. Dünyanın bambaşka yerlerinde düşünce ve ifade özgürlüğü, hak talepleri için mücadeleler devam ediyor, bedeller ödeniyor.

Bedel ödeyen kahramanlardan biri de Julian Assange. Dünyadaki zorba düzeni, bu düzenin iki yüzlülüklerini ifşa ederek yeneceğini düşünen, bu amaç için Wikipedia'yı kuran hacker, gazeteci ve aktivist Assange!

Assange, 2012 yılından bu yana politik sığınmacı statüsünde kaldığı Londra'daki Ekvador Büyükelçiliği'nden, uluslararası hukuk çiğnenerek yaka paça çıkartıldı. Her ne kadar ölüm cezasının olmadığı bir ülkeye iade edileceği "taahhüt" edilse de ABD başta olmak üzere dünya devletlerinin pek çoğunun, bu gözü pek gazetecinin kanına susadığını; imkân olsa bir bardak suda boğacaklarını biliyoruz. Assange'ın Ekvador Büyükelçiliği'ni insansız hava uçakları ile vurmayı konuşacak kadar gözünü karartmış zorbaların elinde olması kendilerini Assange'ın dava arkadaşları olarak gören bizler için büyük bir üzüntü kaynağı.

Assange için hazırlanan iddianame gazetecilik faaliyetini; gazetecinin kaynaklarını korumak ve kaynağı ile kendi arasında güvenli bir iletişim tesis etme gayretini suç addediyor. Ne ülkemizde, ne de dünyada gazetecilik suç değildir. Assange dahil mesleklerini icra ettikleri için kovuşturulan, tutuklanan tüm gazetecilerin serbest bırakılmasını talep ediyoruz.

Cemil Meriç'in sözleri ile ifade edecek olursak dergiler hür fikrin kalesidir. Bu kalenin muhafızlığı konusunda bendeniz 1 yıldır emre amade olarak, çoğu zaman eksiklerle de olsa bu görevi ifa etmeye çalışıyor idim. Arka Kapı Dergi kadrosunun oybirliği ile bu görevi sevgili kardeşim, yoldaşım Şahin Solmaz'a devrediyorum. 8. sayımızdan itibaren Şahin Solmaz kardeşimizin yönetiminde dergimiz çok daha iyi işler başaracak, umarım bu yeni dönemde hak ettiği gerçek teveccühe mazhar olacaktır. Kendilerine başarılar dilerim.

Bendeniz elbette ki bir onur payesi addettiğim Arka Kapı Dergi yazarlığına sürdürecek, karınca kararınca bu güzide çalışmanın mütevazi bir emektarı olmaya devam edeceğim.

Bilgi güçtür. Güç, adalete ve özgürlüğe inananlarla olsun!

Ziyahan Albeniz - editor@arkakapidergi.com

İÇİNDEKİLER

Mayıs-Haziran '19 Siber Güvenlik & Bilişim Etkinlikleri

İstanbul Bilgi Güvenliği Konferansı #İstSec'19

02 Mayıs 2019 | İstanbul

İstanbul Medeniyet Üniversitesi'nde gerçekleştirilecek olan etkinlikte, birçok saldırı yöntemlerine ve güvenlik konularına değinilecektir.

Bilgi: https://bit.ly/2VZPV7G

CISA Hazırlık Eğitimi

6-10 Mayıs 2019 Şişli, İstanbul

ISACA İstanbul Chapter tarafından organize edilen CISA hazırlık eğitimi sonucunda kursiyerlerin Bilgi Teknolojileri ve İş Sistemlerine yönelik denetim, kontrol, izleme ve değerlendirme alanında kendilerini geliştirmelerini amaçlamaktadır. Eğitim ücretlidir.

Bilgi: http://isaca-istanbul.org/egitim/cisa

Cloud Security Day

11 Mayıs 2019, Microsoft Türkiye İstanbul Ofisi

Etkinlikte bulut sistemlerinin yaygınlaşması ile beraberinde gelen güvenlik sorunları anlatılacak olup güvenlik çözümleri uygulamalı olarak gösterilecektir.

Bilgi: https://cozumpark.com

Özgür Yazılım ve Linux Günleri '19

11-12 Mayıs 2019 | İstanbul Bilgi Üni., Santral Kampüsü E3 Binası

Linux Kullanıcıları Derneği tarafından yılda bir kez düzenlenen, Türkiye'de özgür yazılımın yaygınlaştırılmasını amaçlayan konferansa katılım ücretsizdir.

Bilgi: ozguryazilimgunleri.org.tr/2019/

ICCI 2019

28-30 Mayıs 2019 | İstanbul Fuar Merkezi

Bu yıl fuarda yalnızca enerji ve çevre konuları değil, yapay zeka, siber güvenlik, gerçek zamanlı veri teknolojisi gibi konuları da yer almaktadır.

Bilgi: http://www.icci.com.tr/tr/konferanslar/konferanslar/odak-konular

Siber Güvenlik Uzmanı Eğitim Programı

01 Haziran 2019, 10:00 | Beylerbeyi Mahallesi Mehmet Akif Ersoy Caddesi Türk Telekom Binası Üsküdar 34676 İstanbul - Türkiye

USGF tarafından düzenlenecek olan bu etkinliğe katılan katılımcılar, eğitim sonunda sınava tabi tutulacaklar ve eğer başarılı olurlarsa sertifika alacaklardır.

Bilgi: https://www.usgf.org.tr/konferans/siber-guvenlik-uzmani-egitim-programi/

Temel Network Eğitimi Programı

01 Haziran 2019, 15:04 | Beylerbeyi Mahallesi Mehmet Akif Ersoy Caddesi Türk Telekom Binası Üsküdar 34676 İstanbul - Türkiye

Linux ve bilgisayar ağları yapısı ile beraber VPN kurulumu, Firewall güvenliği gibi konuların yer aldığı eğitimin sonunda başarılı olan katılımcılara sertifika verilecektir.

Bilgi: https://www.usgf.org.tr/konferans/siber-guvenlik-uzmani-egitim-programi/

BTvizyon Kayseri 2019

13 Haziran 2019, 09:00 | Wyndham Grand Hotel Kayseri

Etkinlikte teknoloji sunuları yapılacak, çözüm gösterileri alanlarında ürünler ve çözümleri tanıtılacaktır.

Bilgi: https://bilisimzirvesi.com.tr/tr/etkinlikler/etkinlik/btvizyon-kayseri-2019

Kripto Para Haberleri

20 Mart 2019 Bitcoin'den sonra:

Türkiye'de Ethereum ile futbolcu transferi

Çanakkale'de bir futbol kulübü, 32 yaşındaki bir futbolcuyu 1 ton buğday ve 1 ton ay çekirdeğinin yanı sıra 4 bin 500 TL'lik Ethereum karşılığında kadrosuna kattı. Geçtiğimiz yılın ocak ayında dünyanın ilk Bitcoin ile futbolcu transferi de Türkiye'de gerçekleştirilmişti.

21 Mart 2019

Son 3 haftada Bitcoin ve altında güçlü ilişki:

Son haftalarda bir numaralı kripto para Bitcoin ile altın arasındaki güçlü korelasyon dikkat çekiyor. Her iki varlık da son birkaç haftayı birbirlerini izler şekilde yükseliş eğiliminde geçirdi.

22 Mart 2019

Ödeme devi Western Union'dan Stellar ortağı ile iş birliği:

Dünyanın en büyük para transferi şirketlerinden biri olan Western Union, Stellar ortağı Thunes ile iş birliği yaptığını açıkladı. Western Union, geçtiğimiz yıl Ripple'ı test etmiş fakat sonuçlardan memnun olmamıştı.

23 Mart 2019

MIT: Binance büyük kumar oynuyor ve kaybedecek:

Massachusetts Teknoloji Enstitüsü'nün (MIT) bir yayını olan Technology Review'in haberine göre, boğa piyasasındaymışız gibi faaliyetlerine devam eden Binance, düzenleyicilerle kumar oynuyor ve nihayetinde bu oyunu kaybedecek.

23 Mart 2019

Buterin'den 'Ethereum liderliğini yitiriyor' itirafı:

Ethereum'un kurucusu Vitalik Buterin, verdiği bir röportajda Ethereum'un eski hakimiyetini bir dereceye kadar kaybettiğini açıkladı. Buterin, bunu büyük ölçüde Ethereum'un bu alandaki ilk proje olmasına ve ondan sonra çıkan projelerin Ethereum'dan öğrendiklerinin üzerine katarak ortaya çıkmalarına bağladı.

24 Mart 2019

Twitch, Bitcoin kabulünü sessiz sedasız durdurdu:

2018'in ortalarında kripto paralarla ödeme almaya başlayan canlı yayın platformu Twitch, bu seçeneği yakın bir zamanda ortadan kaldırdı. Bu kararın nedeni belirsizliğini korusa da, çoğu kullanıcının bu seçeneğin varlığından bile haberdar olmaması, bu işin arkasında düşük işlem hacimlerinin olabileceğini gösteriyor.

24 Mart 2019

Bitcoin'in piyasa payı hatalı mı? Bu araştırma öyle diyor:

Likiditenin hesaba katıldığı yeni bir araştırmaya göre, CoinMarketCap'in verileri hatalı ve Bitcoin'in piyasa hakimiyeti %80 gibi bir oranla oldukça yüksek. Likiditenin hesaba katılmadığı CoinMarketCap verilerinde ise, bu oran %50'nin biraz üzerinde seyrediyor.

25 Mart 2019

Binance'te satılan token, listelenmeyi takiben %400 yaptı:

Geçtiğimiz hafta Binance Launchpad üzerinde ön satışı gerçekleştirilen Celer Network'ün token'ı CELR, borsada listelenmesinin ardından yüzde 400 değer kazandı. İlk olarak Launchpad'de 0.0067 dolardan satışa sunulan CELR, 6 gün sonra Binance'te listelendi ve fiyatı 0.025$'ın üstüne çıktı.

25 Mart 2019

EVX'te neler oluyor? Saatler içinde %250 arttı:

Sınır ötesi para transferleri, doğrudan ödemeler, kripto paradan itibari paralara takaslar ve blockchain üzerinde kredi vermeye odaklanan bir blockchain şirketi olan Everex'in token'ı EVX, ABD'nin New Jersey eyaletinden faaliyetleri için yasal onay aldığını duyurmasının ardından saatler içinde %250 yükseldi.

25 Mart 2019

Facebook'un gizli Blockchain bölümü büyüyor:

Gizli kapaklı bir şekilde kendi kripto parasını ve Blockchain uygulamalarını geliştirdiği bilinen Facebook, Blockchain alanında harıl harıl yeni eleman arıyor. Facebook'un LinkedIn sayfasında şu anda Blockchain ile ilgili 22 açık pozisyon olduğu görülüyor.

26 Mart 2019

1 ayda %750 arttı: MXM'yi kim alıyor?

Maximine Coin, Mart ayının başından bu yana %750 oranında değer kazandı. MXM yükselişin etkisi ile en büyük 40 kripto para arasına girdi. Böyle bir yükseliş için ortada çok fazla neden olmaması, yükselişin yapay bir yükseliş olabileceği izlenimini yaratıyor.

26 Mart 2019

Büyük Singapurlu Bitcoin borsasını hack'lediler:

Yaygın olarak Çinlilere hizmet veren Singapur merkezlli büyük kripto para borsası DragonEx, saldırıya uğradığını ve kullanıcılarının kripto paralarını çaldırdığını duyurdu. Borsa tarafından yapılan açıklamada, kullanıcıların kaybı için sorumluluğun üstlenileceği belirtildi.

27 Mart 2019

Binance'ten önce davrandılar: OKEx'ten Türkiye hamlesi:

Binance'in Türk Lirası ile kripto para alıp satmaya olanak tanıyacağı konuşulurken, rakip OKEx erken davrandı. Dün İstanbul'da düzenlediği etkinlikte Türkiye piyasasına resmen girdiğini duyuran OKEx, Türk Lirası işlemlerine çok yakın bir zamanda başlayacağını açıkladı.

27 Mart 2019

Binance'te sahte haberle %250 artan kripto para, saatler içinde çakıldı:

Dün Binance üzerinde 0.14 dolardan işlem gören OAX, bir gün içinde %250 arttı. Fakat saatler içinde yüzde 50'ye yakın değer kaybetti. Bu durum, artışın bir pompala-boşalt operasyonu olabileceği şüphesi yarattı çünkü yükselişi destekleyen herhangi bir yeni gelişme yoktu.

28 Mart 2019

İstanbul'da operasyon: 50 milyon TL'yi Bitcoin'le kaçırmışlar:

Milliyet'ten Ferit Zengin'in haberine göre geçtiğimiz hafta İstanbul, Batman ve İzmir'de gerçekleştirilen operasyonlarla çökertilen bahis çetesinin faaliyetlerinin ayrıntılarına ulaşıldı. Yasa dışı bahis oynatan bu çetenin elde ettiği kazancı Bitcoin ile yurt dışına gönderdiği tespit edildi. Çetenin bu yolla 50 milyon TL aktardığı anlaşıldı.

28 Mart 2019

Borsalarda token satış furyası sürüyor: Yaklaşan önemli IEO'lar

2017 ve 2018'deki ICO furyasına benzer şekilde son dönemde kripto para borsalarında da bir IEO furyası var. Binance ve Huobi gibi borsaların liderlik ettiği sürece başka borsalar da dahil oldu. Bu borsalarda Nisan ayı içerisinde dört IEO gerçekleştirilecek.

28 Mart 2019

Bitcoin'de işlemler zirveye yaklaştı, SegWit rekor kırdı:

Bitcoin ağında gerçekleştirilen günlük işlem sayısı 383,186'ya ulaştı. Bu seviye Bitcoin'in 17,000$ olduğu 4 Ocak 2018'den bu yana görülen en yüksek seviye. Öte yandan, işlem hızını artıran ve daha ucuz transfere olanak tanıyan bir Bitcoin teknolojisi olan SegWit'in kullanım oranı da rekor düzeye çıktı.

29 Mart 2019

Bitcoin son 1 ayın zirvesinde ve Binance'in CEO'sundan büyük tahmin:

Bitcoin, Bitstamp üzerinde 4070 doları görerek son bir ayın zirvesine ulaştı. Alternatif kripto paralarda da çift haneli artışlar sürerken Binance'in CEO'su CZ'den de bir tahmin geldi. CZ, kripto paraların itibari paralara karşı 1000 kattan daha fazla artacağını söyledi.

29 Mart 2019

Kripto para devlerinden %8 faizli sabit kripto para:

Bittrex'in de aralarında olduğu bir grup kripto para şirketi, önümüzdeki ay yıllık %8 faizli ve Avro ile desteklenen bir sabit kripto para çıkarmaya hazırlanıyor. Grup yaptığı açıklamada, evrensel euro (UPEUR) adlı token'ın düşük volatiliteli kripto para arayan kullanıcıları hedeflediğini belirtti.

30 Mart 2019

Bithumb'da milyonlarca dolarlık hırsızlık: Hırsız içeriden çıktı!

Güney Kore ve dünyanın önde gelen Bitcoin borsalarından biri olan Bithumb, saldırıya uğradı. Milyonlarca dolar değerinde kripto paranın çalındığı bildirilen saldırının Bithumb çalışanı ya da çalışanları tarafından yapıldığı açıklandı.

31 Mart 2019

Litecoin'in fiyatı 6 ayın zirvesine, hash oranı tarihi zirveye dayandı:

Önde gelen kripto paralardan biri olan Litecoin'de hash oranı tarihi zirvesine yaklaşırken fiyat da son 6 ayın en yüksek seviyesine çıktı. Aralık ayının ortasında 20 dolara geriledikten sonra istikrarlı bir yükselişe geçen Litecoin, %215'lik bir artışla dün 63 dolara ulaştı. Fiyat en son bu seviyede bulunduğunda tarih 28 Eylül 2018'di.

31 Mart 2019

Bitcoin'in geleceğine yeni teori, büyük servet transferi:

Araştırma şirketi Messari'nin CEO'su Ryan Selkis, önümüzdeki 20 yıl içinde ebeveynlerinden milenyumlulara geçecek 30 trilyon dolarlık bir servetin olduğuna dikkat çekti ve bu paranın büyük bir kısmının dijital varlıklara gidebileceğini söyledi. Ona göre, bu durumda BTC ihtiyatlı bir tahminle 50 bin dolar olabilir.

2 Nisan 2019

Bitcoin 5000 doları aştı: Ayı piyasası resmen bitti mi?

Bitcoin, bu sabah % 23 artarak 5078 dolara kadar tırmandı. Bir numaralı kripto para, 2018 yılının Kasım ayından bu yana en yüksek seviyesini gördü. Peki, ayı piyasası resmen bitti diyebilir miyiz? Analist Alex Krüger, bu haftanın başlarında Bitcoin'in 4200$'ın üstüne çıkması durumunda teknik olarak 16 aydır devam eden ayı piyasasının son bulacağını söylemişti.

2 Nisan 2019

Reuters: Bitcoin'in fiyatını tek bir 'gizemli' alıcı yükseltti

Bugün Reuters'ta yayınlanan bir haberde 4150 dolardan 5070 dolara tırmanan Bitcoin'in fiyatını tek bir kişinin yükselttiği yazıldı. Bu kişinin algoritmalar aracılığıyla farklı borsalarda eş zamanlı olarak 20 bin BTC'lik emir verdiği söyleniyor.

3 Nisan 2019

Ekonomist: Rus oligarklar, 8.6 milyar dolarlık Bitcoin aldı

Daha önce Rusya'nın rezervlerinin bir bölümünü Bitcoin'e ayırmaya başlayacağını öne süren Rus ekonomist Vladislav Ginko, şimdi de Rus şirketler ve varlıklı bireylerin 8.6 milyar dolarlık Bitcoin satın aldığını iddia etti.

3 Nisan 2019

40'tan fazla merkez bankası Blockchain'i deniyor:

Dünya Ekonomik Forumu'nun raporuna göre, en az 44 merkez bankası Blockchain teknolojisini deniyor ve bazıları bu işle 2016'dan beri uğraşıyor. Raporda, Fransa ve Kamboçya Merkez Bankaları'nın yanı sıra daha pek çok merkez bankasının bu alandaki çalışmalarından söz ediliyor.

4 Nisan 2019

SEC, 6 aydır üzerinde çalıştığı kripto para kılavuzunu yayınladı:

ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), token çıkarmak isteyenler için yaklaşık 6 aydır üzerinde çalıştığı düzenleyici kılavuzunu yayınladı. Kılavuzda kripto paraların hangi şartlar altında menkul kıymet sınıfına dahil olacağı özetleniyor.

4 Nisan 2019 Beklenen Binance DEX için kritik zaman verildi

Kripto para borsası Binance'in merkezsiz borsası Binance DEX'in ne zaman test sürümünden tam olarak faaliyete geçeceği bir süredir merak ediliyordu. Konuyu netliğe kavuşturan Binance CEO'su Changpeng Zhao, merkezsiz borsanın açılışı için bu ayı işaret etti.

4 Nisan 2019

Türkiye merkezli Blockchain girişimine ConsenSys desteği

Kendisini "Yeni nesil aracısız enerji ticareti" olarak tanımlayan Türkiye merkezli Blockchain girişimi Blok-Z, Ethereum'un kurucu ortağı Joseph Lubin'in başında bulunduğu ConsenSys'ten 100 bin dolarlık para desteğinin yanı sıra mentorluk desteği de alacak.

5 Nisan 2019

Wall Street analisti: Bitcoin'in gerçek değeri 14.000 dolar

Fundstrat Global Advisors'ın araştırma şefi ve yönetici ortağı Tom Lee, Bitcoin'in gerçek değerinin 14,000 dolar olduğunu ileri sürdü. Lee ayrıca eski balina cüzdanlarının kitlesel Bitcoin alımlarına başladığını iddia etti.

5 Nisan 2019

İspanya'da binlerce kripto para kullanıcısına vergi bildirimi:

İspanya Hazine Bakanlığı, binlerce vatandaşına kripto para işlemleriyle ilgili olarak vergi ödemek zorunda kalabilecekleri konusunda bir uyarı metni gönderdi. Metinde, kripto paralardan elde edilen gelirlerin tabii gelir teşkil ettiği belirtildi.

6 Nisan 2019

Rus Facebook'u, kendi kripto parasını resmen piyasaya sürdü:

Rusya'nın en büyük sosyal medya platformu olan Vkontakte, VK Coin adını verdiği madenciliği yapılabilen kripto parasını piyasaya sürdü. Bu paranın Blockchain tabanlı bir kripto para mı yoksa sadece platformda kullanılan bir dijital para mı olduğu, şu anda belirsizliğini koruyor.

7 Nisan 2019

Binance Coin'e Samsung Galaxy S10 desteği:

Kripto para borsası Binance'in kripto parası Binance Coin, Samsung'un amiral gemisi telefonu Galaxy S10 tarafından varsayılan olarak destekleyeceği sayılı kripto paralar arasına alındı.

9 Nisan 2019

Çin'den Bitcoin madenciliğine darbe hazırlığı:

Reuters, Çin'in makroekonomik politikaları hazırlamaktan sorumlu devlet kurumunun kripto para birimi sektöründe artan bir hükümet baskısının işareti olarak Bitcoin madenciliğini yasaklamak istediğini bildirdi.

11 Nisan 2019

Coinbase ve Visa arasında kripto para iş birliği:

ABD merkezli büyük kripto para borsası Coinbase, İngiltere'de yaşayan müşterilerinin kripto para ile çevrimiçi ya da fiziksel mağazalarda ödeme yapmalarına imkan tanıyan bir Coinbase Card çıkardı.

11 Nisan 2019

Assange'ın tutuklanması sonrası WikiLeaks'in Bitcoin bağışları sıçradı:

ABD'li diplomatların gizli yazışmalarını yayınlayan WikiLeaks'in kurucusu Julian Assange, 11 Nisan 2019 sabah saatlerinde yedi yıldır sığınmacı olarak kaldığı Londra'daki Ekvador Büyükelçiliği'nde İngiliz polisi tarafından yaka paça gözaltına alındı. Assange'in tutuklanması sonrası Wikileaks'te Bitcoin ve diğer kripto para bağışlarında önemli bir artış görüldü.

11 Nisan 2019

WikiLeaks'in binlerce Bitcoin'i tehlikede olabilir:

Kurucusu Julian Assange'ın tutuklanmasının ardından WikiLeaks'e ait binlerce Bitcoin, dava konusu olabilir. Gizli Servis'in karanlık ağ pazaryeri Silk Road'ın dijital cüzdanlarına el koyması gibi WikiLeaks'in Bitcoin'lerinin başına da benzer bir şeyin gelebileceğinden endişe ediliyor.

12 Nisan 2019

Telegram'ın kripto parası sessiz ve derinden geliyor!

Telegram'ın Blockchain platformu ve kripto parası piyasaya sürülmeye bir adım daha yaklaştı. Telegram Open Network (TON) özel beta sürümü tamamlandı ve birçok kripto programcısı ve beta test mühendisi çok konuşulan bu platforma giriş izni aldı.

13 Nisan 2019

IMF ve Dünya Bankası'ndan ortak kripto para:

Uluslararası Para Fonu (IMF) ile Dünya Bankası, gelişen teknolojiyi daha iyi anlamak için Learning Coin adı verilen özel bir Blockchain ve kripto para geliştirecek. Bu para, iki kurum dışında erişilmez olacak ve hiçbir parasal değer taşımayacak. Ayrıca, bu paranın Bitcoin gibi bir kripto para özelliği de olmayacak.

15 Nisan 2019

Litecoin ağında meteorik yükseliş:

Litecoin'de 6 Ağustos 2019'da gerçekleşmesi beklenen blok ödülü yarılanması her geçen gün yaklaşırken Litecoin ağında hash oranı, kripto paranın piyasaya çıktığı 2011'den bu yana en yüksek seviyeye ulaştı. Litecoin ağında görülen bu durum, gelecek olan blok ödülü yarılanması ile fiyatın artacağı beklentisinin madencileri harekete geçirdiğini gösteriyor.

15 Nisan 2019

Bitcoin SV, Binance sonrası iki platformdan daha çıkarılıyor:

Kripto para topluluğunda tartışmalı bir proje olan Bitcoin SV, Binance'in ardından iki platformda daha liste dışı edilme yolunda. Kraken bu konuda kullanıcılarına bir anket yöneltirken, diğer platform ShapeShift'in CEO'su da, 48 saat içinde Bitcoin SV'yi platformlarından kaldıracaklarını açıkladı.

16 Nisan 2019

Binance 15.6 milyon dolarlık BNB'yi yok etti:

Kripto para borsası Binance, bugün yaptığı açıklama ile 7. BNB yakımını tamamladığını bildirdi. Buna göre borsa, toplam değeri 15.6 milyon dolar olan yaklaşık 830 bin BNB'yi dolaşımdan tamamen çıkardı.

16 Nisan 2019

Herkes BSV'yi liste dışı ederken bu borsa Bitcoin Cash'i çıkarıyor:

Herkes, art arda Bitcoin SV'yi liste dışı ederken Japon finansal hizmetler devi SBI Holdings'in geçtiğimiz yıl faaliyete geçen kripto para borsası SBI Virtual Currencies ise Bitcoin Cash'i kaldırıyor. Borsa tarafından bugün yapılan açıklamada BCH'nin Haziran ayında platformdan çıkarılacağı bildirildi.

16 Nisan 2019

Bitcoin borsası Binance'ten ilk çeyrekte parmak ısırtan kâr

Önde gelen kripto para borsası Binance, 2019 yılının ilk çeyreğinde bir önceki çeyreğe göre yüzde 66 artışla 78 milyon dolar kâr etti.

17 Nisan 2019

Binance'te şaşkınlık yaratan olay: Fiyat aniden %99 düştü

Kripto para borsası Binance'de Waves'in fiyatı 2.7 dolardan işlem görürken aniden % 99.9 düştü ve 0.00052 dolara indi. Sonrasında fiyat hızla toparlanıp aynı seviyeye geri dönse de bu sert çöküş akıllarda soru işaretleri yarattı. Yaşanan bu duruma 506,000 Waves satmak isteyen bir kripto para balinasının limitsiz bir satış emri vermesinin neden olduğu düşünülüyor.

18 Nisan 2019

McAfee: Bitcoin'in yaratıcısı hâlâ hayatta

Ünlü siber güvenlik uzmanı John McAfee, Satoshi Nakamoto'nun gerçek kimliğini bildiğini ve kendisini açığa çıkarmazsa açıklamak niyetinde olduğunu söyledi. McAfee isim vermese de, Bitcoin'i yaratanın bir grup insan olduğunu,

teknik belgenin ise şu anda ABD'de yaşayan tek bir adam tarafından yazıldığını söyledi.

19 Nisan 2019

ABD'nin konuştuğu Müller Raporu'nda çarpıcı Bitcoin gerçeği:

ABD'nin konuştuğu Müller Raporu'na göre Rus istihbarat birimleri, ABD başkanlık seçimlerini manipüle etmek için giriştiği operasyonları Bitcoin'le finanse etti. Dahası, bu Bitcoin'lerin önde gelen borsalardan CEX.io'da saklandığı belirtiliyor.

19 Nisan 2019

Bitcoin'i risk-kazanç oranına göre masaya yatırdılar, işte sonuç:

Adamant Capital'in yakın tarihli bir raporuna göre, piyasa değeri ile en büyük kripto para Bitcoin, risk-kazanç oranı bakımından şu an dünyadaki en iyi yatırım.

20 Nisan 2019

Dur duraksız ilerleyen BNB'den tarihi rekor:

Bir süredir kripto para piyasasını kasıp kavuran Binance'in kripto parası Binance Coin (BNB), sabah saatlerinde 25.49$'ı görerek ABD doları bazında tüm zamanların en yüksek seviyesine ulaştı. Bir önceki zirve 25.18$'dı.

20 Nisan 2019

Ethereum'un kurucusu Vitalik Buterin, Ripple'ın kapısından dönmüş:

Ethereum'un kurucusu Vitalik Buterin, Ethereum henüz ortada yokken 2013 yılının ortalarında Ripple'da staj yapmayı denediğini fakat ABD vizesi alamadığı için yapamadığını itiraf etti.

Tayfur Özkara - tayfurozkaras@gmail.com

SİBER SAHA

CyberEventDays

Sivas Cumhuriyet Üniversitesi Siber Güvenlik Topluluğu tarafından 9-10 Mart 2019 tarihleri arasında organize edilen "**CyberEventDays**" etkinliği üniversite bünyesinde bulunan İktisadi ve İdari Bilimler Fakültesi laboratuvarlarında gerçekleşti.

Topluluk, siber güvenlik ve bilgi güvenliği alanlarında farkındalık oluşturmayı ve yetenekli gençleri eğitimler ve konferanslar sayesinde sektördeki oyuncularla bir araya getirerek İç Anadolu Bölgesi'nde bir ekosistem oluşturmayı amaçlıyor.

İki gün süren CyberEventDays etkinliğinin ilk gün sabah saatlerinde konferans düzenlenirken, öğleden sonra ise eğitimlere başlandı. Etkinlikte bir dizi başlıkta konferanslar ve eğitimler yer aldı.

Konferanslar, büyük veri ve siber güvenlik, Scada ve Exploit geliştirme, siber istihbaratın ülkeler için önemi gibi başlıklarda iken; eğitimler zararlı yazılım analizi, Exploit geliştirme ve network saldırı yöntemleri konularında gerçekleştirildi.

Eğitmenlerin TÜBİTAK çalışanı olması ise siber güvenliğe devlet tarafından atfedilen önemin bir nevi kanıtı oldu.

Etkinliğe katılan 15 yaşındaki Diyarbakırlı lise öğrencisi Ali'nin öğrenme azmi ve merakı ise diğer katılımcıların gözlerinden kaçmadı. Onun bu azminin Türkiye'deki diğer lise öğrencilerine örnek olması dileğiyle.

Organizasyonun ikinci günü uygulama kısımları ağırlıklı olmak üzere eğitimler devam etti. Hem teorik hem de uygulamalı eğitim alan katılımcılara ise eğitim sonunda katılım belgeleri verildi.

Etkinlik süresince topluluk üyelerinin; etkinlik katılımcılarının hiçbir sorun yaşamaması adına sarf ettiği yoğun gayret etkinlik bileşenlerinin takdirlerini topladı

Etkinlik katılımcılar arasında yapılan hediye çekilişi ile son buldu.

HACKİNG SETİ
(YAZILIM GÜVENLİĞİ VE SİBER GÜVENLİĞE GİRİŞ)

%40 indirim
248,15 TL
148,89 TL

Linux Komut Satırı

Ağ Yöneticiliğinin Temelleri

Kablosuz Ağ Güvenliği

Siber Güvenlik ve Hacking

Uygulamalı Sızma Testleri Pentest Lab

Java Diliyle Kriptoloji Uygulamaları

Kali ile Ofansif Güvenlik

Ethical Hacking Offensive&Defensive

HEDİYE: Oracle Veritabanı Güvenliği

abaküs

Cansu Topukçu - topukcucansu@gmail.com

JULIAN ASSANGE

"Adaletsizliğe her şahit olup eyleme geçmeyişimizde, karakterlerimizi kendi varlığı içinde pasif olmaya eğitiriz ve dolayısıyla zamanla kendimizi ve sevdiklerimizi koruma yetimizi kaybederiz. Modern ekonomide, insanın kendisini adaletsizlikten uzaklaştırması mümkün değildir."

Hepimiz onu kendini ateşe atışıyla, Wikileaks'i kurup yönetmesi ile ve son olarak Ekvador Büyükelçiliği'ndeki sığınma hakkının iptal edilmesiyle birlikte gözaltına alınışıyla biliyoruz. Gazeteci, hacker, cypherpunk, aktivist ve bir baba olan Julian Assange - doğum adı ile Julian Paul Hawkins- 3 Temmuz 1971'de Townsville, Queensland, Avustralya'da, bir görsel sanatçı anne (Christine Ann Hawkins) ile savaş karşıtı bir inşaatçı babanın (John Shipton) çocuğu olarak doğmuştur.

Ebeveynleri o doğmadan önce boşanan Assange, çocukluğunda annesi ve üvey babası Richard Brett Assange ile birlikte gezgin bir hayata sahip olduğu için biraz zor bir çocukluk geçirmiştir. Bu yüzden eğitim hayatı boyunca - 20'li yaşlarının ortalarına gelene kadar 30'un üstünde şehirde yaşayıp 37 farklı okula gitmiştir ve hatta sıkça evde eğitim gördüğü olmuştur (buna üniversite dahil değildir). Assange, üvey babası Richard Brett Assange'ı babası olarak gördüğü için onun soyadını almayı tercih etmiştir. Brett Assange'ın aktardığına göre Julian Assange, çocukluğunda her daim *mazlumların yanında duran o sivri çocuk* olmuştur.

1979'da annesi ile üvey babası boşanır ve annesi bir süre sonra Avustralyalı bir tarikat olan The Family ile bağlantısı olan bir adamla evlenir ve bu adamdan da bir oğlu olur. 30'u aşkın şehirde yaşadıktan sonra Assange 20'li yaşlarının ortasındayken kardeşi ve annesi ile birlikte Melbourne'e yerleşmiştir.

Assange 1987 yılında Latince yalancı anlamına gelen Mendax takma adı ile hacking aktivitelerine, yani hacktivism'e başlamıştır. İki tane daha arkadaşı ile International Subversives adında bir hacking grubu kurmuşlardır. 1991 yılında Kanada tabanlı çok-uluslu bir telekomünikasyon ekipmanları üreten

şirket olan Nortel'i hacklemiş ve Avustralya Federal Polis'inin telefonunu dinlemeye alıp bunu keşfetmesiyle ekim sonunda evine baskın yapılmıştır. 1993 yılında Victoria Polisi Çocuk İstismarı Birimi'ne danışmanlık yapıp kovuşturmalara yardım etmiş ve aynı yıl Avustralya'daki ilk ISP'lerden olan Suburbia Public Access Network'ün kuruluşunda yer almıştır.

Daha sonra, 1994'te Nortel dahil olmak üzere 31 tane hacking ve bağlantılı suçları gerçekleştirmekle suçlanmış ve 1996'da bunların 6'sı düşerek 25 tanesi hakkında suçlu görülerek 2100$ tazminat ödemesine ve iyi davranış yemini etmesi kararı ile serbest bırakılmıştır.

Assange 1994 yılında, programlamaya başlamıştır (örneğin, 1996'da PostgreSQL, NNTPCache ve deniable encryption sistemi Rubberhose için patch yazması). Aynı zamanda Best of Security adından bilgisayar güvenliği hakkında önerilerde bulunan ve 1996'da 5000 abonesi bulunan bir siteyi yönetti. 1998 yılında Earthmen Technology'i kurdu ve bir yıl sonra 1999'da leaks.org alan adını satın aldı fakat o zamanlar henüz bu konuda bir şeyler yapmamıştı. Central Queensland University'de (1994) ve University of Melbourne'de (2003-2006) programlama, matematik ve fizik eğitimleri almış fakat herhangi birinden mezun olmamıştır.

University of Melbourne'de kısa bir sürelik çalışma süresinin ardından, Assange ve birkaç arkadaşı 2006 yılında WikiLeaks'i kurdu. Assange burada danışma kurulu üyeliği yapmaktadır ama kendi deyimiyle sadece bir editördür. Wikileaks'te yayımlanacak her belge en son Assange'ın onayından geçer ve ancak o zaman yayınlanabilir. WikiLeaks, gizli bilgileri, sızıntı haberleri ve anonim kaynaklardan alınmış gizli medyaları içerir. Assange, WikiLeaks ile ilgili olarak 2007 yılından 2010'a kadar Afrika, Asya, Avrupa ve Kuzey Amerika'ya sık sık seyahatleri olmuştur. 2015 yılında WikiLeaks'de 10 milyonun üzerinde belge ve ilişkili analizler yayınlanmıştır.

Assange hakkında farklı görüşler mevcuttu - hâlâ bu ayrım devam etmektedir. Örneğin, Avustralya Başbakanı, Assange'ın eylemlerini yasadışı olarak tanımlasa da Avustralya polisi yasalara aykırı hiçbir şey yapmadığını söylemişti. ABD Başkan Yardımcısı Joe Biden ise terörist olarak nitelendirmeyi seçmişti. Bu dönemde Assange'a destek çıkan insanlara örnek olarak Brezilya Cumhurbaşkanı Luiz Inacio Lula da Silva, Ekvador Cumhurbaşkanı Rafael Correa, Rus Başbakan Dmitry Medvedev, Jeremy Corbyn, Pablo Iglesias… gibi isimleri sayabiliriz.

2010 yılında Assange hakkında suçlamalar başladıktan ve bu suçlamalar haksız çıktıktan sonra İsveç'i terketti. 20 Kasım'da ise Interpol tarafından kırmızı bülten ile aranmaya başladı ve kendisi teslim oldu ama destekçilerinin verdiği 240.000 dolarlık kefalet ücreti ile beraat etti. Birleşik Krallık'ta Assange'ın kendilerine iadesi için 2012 yılına mücadele kadar devam etti (Assange'ın avukatları İsveç'e döndüğü takdirde ABD'ye geri iade edilebileceği hususunda kendisini uyardılar). Kendisini Avustralya hükûmeti tarafından terk edilmiş hisseden Assange sığınma için Ekvador Büyükelçiliği'ne başvurur (19 Haziran 2012'de Ekvador Dışişleri Bakanı Ricardo Patino Julian Assange'ın sığınma hakkı için elçiliğe başvurduğunu söylemiştir). 2012 yılının Temmuz ayında ise Knightsbridge'deki Ekvador Büyükelçiliği Assange'ın Birleşik Krallık tarafından tutuklanmasını engellemek için Assange'a politik sığınma hakkı vermiştir. Fransa, Assange'ın bu talebini reddetmiştir. Bir cypherpunk olan Assange, aynı yıl Cypherpunks: Freedom and the Future of the Internet adında bir kitap yayınladı. Kısaca bahsetmek gerekirse bu kitapta toplumun bilgi güvenliği ile ilişkisi irdelenmektedir. Assange'ın kitabın giriş kısmında da dediği gibi, bu kitap bir manifesto değil, bir uyarıdır.

Assange 2 Temmuz 2013'te Avustralya Senatosuna adaylığını koyup kaybettikten sonra buna bir tepki olarak WikiLeaks Party adında mikro-politik bir parti kurulmuştur. Partinin konseyi Assange, Matt Watt, Gail Malone, John Shipton, Omar Todd ve Gerry Georgatos'tan oluşmaktaydı. Parti daha sonra 23 Temmuz 2015'te dağılmıştır.

Eylül 2016'da, dönemin başkanı Barack Obama'ya çok ses getiren belgelerin yayınlanmasında rol oynayan ve Amerikan ordusundan bilgi sızdırdığı suçlamasıyla tutuklu bulunan Chelsea Manning'e merhamet gösterilmesi durumunda ABD'de hapse girmeye razı olacağını belirtmiştir. Büyükelçilikte zaman zaman balkona çıkıp toplanan insanlara ve basına açıklamalarda bulunmuştur, hatta bu konuşmalarından birinde polisle dinlemeye gelen - aktivistler arasında çıkan olaylardan ötürü tutuklananlar bile olmuştur. 3 Nisan 2019 tarihinde WikiLeaks Ekvador Büyükelçiliği'nin Assange'ı birkaç saat veya gün içerisinde bünyesinden çıkaracağını iddia etmiştir. Her ne kadar Ekvador'un Dışişleri Bakanı Jose Valencia bu bilgiyi yalanlamış olsa da Assange 11 Nisan 2019 tarihinde Ekvador Hükûmeti tarafından büyükelçiliğe davet edilen Britanyalı yetkililerce elçilikten çıkarılmış, fahri vatandaşlığı ve sığınma hakkı iptal edilip tutuklanmıştır.

Parola Yöneticilerinin Karşılaştırmalı Bir İncelemesi

Hem bireysel olarak günlük hayatımızda hem de iş dünyasında önemli bir ihtiyaç haline gelen parola yönetim uygulamaları, gittikçe bir yığın haline gelen ve insan hafızasını zorlayan parolaların saklanması ve yönetilmesi için oldukça önemli bir kolaylık sağlıyor. Tabii güvenliğe önem veren biri iseniz ve bir parolayı birden çok platformda kullanmıyorsanız hayat sizin için daha zor ve bu söyleyeceğim uygulamalar tam da sizler için geçerli. Çünkü biliyoruz ki kullandığımız herhangi bir parola ele geçirildiğinde aynı parolayı kullandığımız diğer platformlardaki hesaplarımızın da ele geçirilmesi kaçınılmaz. Parola yöneticileri söz konusu olduğunda hem açık kaynak hem de ücretli birçok yazılım bulunuyor. Kullanıcılar olarak yüksek gizlilik seviyesine sahip oturum verilerimizi bu yazılımlardan birine emanet etmeden önce iyi bir karşılaştırma yapmalı ve bizlere en uygun olanını özellik ve imkanlarına göre değerlendirmeliyiz.

Açık kaynaklı uygulamalardan biri olan KeePassXC uygulamasının kullanımını ilk sayımızda *"Parolalarınızı Tek Bir Yerden Yönetin: KeeePassXC"* başlıklı yazı ile Arka Kapı Dergi ekibi olarak sizlerle paylaşmıştık. Daha fazla entegre edilmiş özellik ve alternatif seçeneklerin sunulması açısından bu yazıda ise karşılaştırmalı olarak inceleyeceğimiz bazı uygulamalar olacak. Bu uygulamalar sırası ile *Lastpass, Dashlane, Keeper, 1Password ve Bitwarden*.

Öncelikle bu beş uygulamada da ortak bulunan ve güvenlik ya da kullanım kolaylığı açısından olmazsa olmaz diyebileceğimiz bazı özelliklerden bahsedip daha sonra bu uygulamaları birbirlerinden ayıran farklılıkları yansıtan bir tablo ile son karşılaştırmaları yapmanızı sağlayacağım.

Ortak Özellikler

İki Faktörlü Kimlik Doğrulama

İki farklı aşamada (2FA- Two Factor Authentication) kullanıcının kimlik doğrulamasının yapıldığı bu güvenlik önlemi neyse ki belirtmiş olduğum 5 uygulamada da bulunuyor. Son zamanlarda yaşanan SMS tabanlı iki faktörlü kimlik doğrulamasının da saldırganlar tarafından atlatılabiliyor olduğunu gördükten sonra, sorulması gereken asıl soru bu özelliğin uygulamada olup olmadığı değil, hangi şekilde uygulandığı oluyor.

Yubikey Uyumluluğu

Yubikey cihazı iki aşamalı doğrulamada kullanılan ve USB portundan bilgisayara bağlanan anahtar görünümünde hafif ve ince bir cihazdır. Donanımı bilgisayarınıza bağladıktan sonra herhangi bir hesaba giriş yaparken ikinci adımda Yubikey üzerindeki parola soruluyor ve cihaz üzerindeki tuşa bastığınızda giriş işleminiz gerçekleşiyor. Parolanız çalınmış olsa bile ikinci doğrulama için ana parolaya bağlı kalarak her seferinde tek kullanımlık bir parola üretildiği için saldırganlar tarafından tekrar kullanılamıyor. Bu 5 uygulama da Yubikey bağlantısını destekliyor.

Otomatik Form Doldurma

Parolalarınızın güvenli bir şekilde saklandığından emin olduktan sonra da kullanım kolaylığı açısından kullanıcının beklediği en önemli özellik otomatik form doldurma özelliği oluyor. Android ve iOS'da desteklenen bu özellik ile herhangi bir hesaba giriş yaparken bilgileriniz otomatik olarak dolduruluyor.

Paylaşılan Klasör Oluşturma

Bir grupla, örneğin ailenizle ya da takım arkadaşlarınızla paylaşmak istediğiniz ortak verileriniz varsa bu verileri e-mail ya da başka bir yoldan açık metin şeklinde paylaşmak güvenlik risklerini de beraber getireceğinden, bu uygulamalar üzerinden şifreli, paylaşılan bir klasör oluşturup istediğiniz kişiyi istediğiniz şekilde yetkilendirebiliyorsunuz.

Güvenli Notlar

Bu uygulamalar hesap form giriş bilgileri tutmanın yanı sıra, gizlilik derecesi sizler için önemli olan notlarınızı da (örneğin WiFi parolanızı) güvenli bir şekilde saklıyor. Bu notları kategorilendirebiliyor, parolanız ile kilitleyebiliyor ve e-mail adresleri vasıtası ile başkaları ile de paylaşmanızı sağlıyorlar.

Güçlü Parola Oluşturucu

Sürekli farklı platformlar için karmaşık parolalar üretmek zorunda kalmadan bu uygulamaların üretmiş olduğu tahmin edilemez özellikteki güçlü parolalardan kolayca faydalanabiliyoruz. Parolada olmasını istediğiniz karakter özelliklerini kendiniz belirleyip uzunluğunu da dilediğiniz şekilde ayarlayabilirsiniz.

Farklı Platformlar ile Senkronizasyon

Parolalarımızı kullandığımız telefon, tablet, bilgisayar gibi birçok farklı cihaz için senkronize edebilmek oldukça önemli ve vazgeçilmez bir özellik. Uygulamaya giriş yapıldığında belli periyotlarla senkronizasyon işlemi gerçekleştiriliyor. Senkronizasyon devre dışı bırakıldığında ise uygulamanın sunucusundan verileriniz siliniyor ve sadece sizin cihazınızda depolanıyor.

Karşılaştırmalı Tablo

Yukarıda sıralamış olduğum 5 uygulama içinde bulunan ortak özelliklerin yanı sıra bu uygulamaların kendilerine has bazı farklı özellikleri de bulunuyor. Hangi uygulamanın sizi memnun edeceği konusu ise hangi özelliğe öncelik verip tercih ettiğinize bağlı olarak değişiyor. Bu özellikleri karşılaştırıp değerlendirebilmeniz için aşağıdaki tabloyu inceleyebilirsiniz. Uygulamada bulunan özellik + işareti ile gösterilmiştir. Boş olan kutular, ilgili satırdaki özelliğin, ilgili kolondaki uygulama tarafından desteklenmediğini belirtmektedir.

Özellikler	Lastpass	Dashlane	Keeper	1Password	Bitwarden
Merkezi bir panelden kullanıcı kontrolü	+	+	+	+	
Yöneticinin diğer kullanıcıların parolalarını sıfırlayabilme yetkisi	+	+		+	
Aktif dizin bağlantısı	+				+
Kullanıcıyı yöneticinin seçtiği güvenlik politikalarına zorlama	+	+	+	+	
Tek oturum açma (single sign on)	+	+			
Kişisel veriler için dark web izleme ve uyarı mesajı gönderme özelliği		+			
WiFi koruması için VPN bağlantısı		+			
Kullanıcı aktivitesi raporlama	+		+	+	
Güvenlik denetim testleri	+		+		+
Offline çalışma özelliği				+	
Slack entegrasyonu				+	
Her kullanıcı için oluşturulmuş şifreli cüzdan	+		+		+
Komut satırı arayüzü			+		+
Linux desteği	+	+	+		+
Linux üzerine veri çıkarabilme			+	+	+
Tarayıcı entegrasyonu	Chrome Firefox Safari Opera Edge IE	Chrome Firefox Safari Opera IE Edge	Chrome Firefox Safari Edge Opera IE	Chrome Firefox Safari Edge	Chrome Firefox Safari Opera Brave Edge Tor Browser

Kaynakça:

https://medium.com/@QuantopianCyber/head-to-head-evaluation-of-five-password-managers-8faa4851c767

https://www.codeinwp.com/blog/best-password-manager/

https://www.lastpass.com/

https://www.dashlane.com/

https://1password.com/

https://bitwarden.com/

https://keepersecurity.com/


Privia
CYBER SECURITY CONSULTING
Privacy For You!
Teknoloji Çağının Savunma Sanatı
/Priviasec
info@priviasecurity.com
www.priviasecurity.com

AVCI

Redefine Your Security

Advanced Vulnerability Centralized Interface

Güvenlik Araçlarınızı Tek Merkezden Yönetin!

/avcilabs

www.avcilabs.com

Powered by KODiA

Şahin Solmaz - sahin@arkadergi.com

Görünmeyen Köy Kılavuz İstiyor

"Haydi bir fotoğraf çekinelim", "Aa! Ne güzel manzara!", "Radyoda çalan ah şu şarkı, hemen arkadaşıma göndereyim.", "Şu konuda bir şeyler yazayım."

Çektiğimiz fotoğrafta, izlediğimiz videoda, dinlediğimiz şarkıda, okuduğumuz makalede gördüklerimizden - duyduklarımızdan çok daha fazlası, metadata'lar var.

Örneğin: çektiğiniz bir fotoğrafın dijital arka planında, fotoğrafın çekilme tarihi ve saati, çözünürlüğü, türü, boyutu, çekimi yapan cihazın markası, modeli, kameranın lens türü, flash kullanılıp kullanılmadığı, lokasyon bilgisi, fotoğrafı çeken kişinin- cihazın adı (author) yer alıyor olabilir. Ya da oluşturduğunuz bir dokümanın arka planında, o dokümanın adı, türü, boyutu, açıklaması, oluşturulma - değiştirme - son erişim tarih ve saat bilgileri, ilgili cihaz (örn: Lenovo-PC) gibi bilgiler varsayılan olarak tutulmaktadır.

Şöyle bir özetlemek gerekirse:

- Başlık ve tanım,
- Etiketler ve kategoriler,
- Kim, ne zaman oluşturdu,
- Kim, ne zaman düzenledi,
- Kim, ne zaman erişti, gibi bilgiler yer almaktadır.

Fotoğraflar için tutulan metadata, EXIF (Exchangeable Image File Format) olarak adlandırılır.

Bu beş madde genel anlamda metadata'nın başlıca unsurlarıdır. Tabii bu unsurların arasında konum bilgisinin olmadığı dikkatinizi çekmiş olmalı. Genel unsurlar arasında yer almasa da bu bilgiler arasında lokasyon bilgisi de yer alabilir. İşte tüm bu bilgilere, metadata (üst-veri) diyoruz. Teknik bir tanım yapmak gerekirse; *metadata, veri hakkında tutulan veridir*, diyebiliriz. Bu verilerin ve içeriklerinin hakkında tutulan özet bilgidir.

Daha somut bir iki örnekle aktaralım. Elinizdeki bu dergiyi düşünün, derginin içerisindeki makaleler veri iken, derginin kapakları, sayfa sayısı, editör yazısı, künye bilgisi ve içindekiler de metadata'sı oluyor. Hatta bu makalenin üst kısmında yer alan makale adı, yazar adı, yazarın e-posta adresi gibi bilgiler bu makalenin metadata'sı oluyor.

Peki **metadata'lar neden tutuluyor**? Aslında çok basit, dosyaların kullanım ve anlaşılma kolaylığını sağlamak için tutuluyor. Yani bu sayede cihazlar, dosyaların ne olduklarını daha kolay anlayabiliyor, bu dosyaları daha kolay arayıp - bulabiliyor, kolayca sıralama yapabiliyor.

Metadata'lar nerede, hangi tür dosyalar için tutulur? Aslında normal şartlarda metadata'sız dijital bir dosyanın varlığının mümkün olmadığını söyleyebiliriz. Yani, fotoğraflardan müziklere, web sitesi dosyalarından hatta isteklerinden, filmlere kadar, dijital ortamda karşılaştığımız her dosyanın bir metadata'sı vardır. Üst-veri isminden de anlaşılacağı üzere, dosyaların header - başlık kısmında yer alır, genellikle bir dosyanın arka planındaki ilk satırlarındadır (byte'lardır). Buraya kadar neredeyse hep dosyalar üzerinden konuştuk.

Tabii **sadece bu kadar değil**! Mesela en son kiminle, ne zaman, ne kadar süreliğine görüştüğünüzün bilgisi de bir metadata'dır. Yukardaki tanımımıza da uyuyor. Bu bilgiler birçok devlet, hükümet ya da ilgili kurumlar tarafından resmi/gayri-resmi olarak kayıtlara alınır. Ama gizlilik? Bu durumda,

örneğin NSA, verinin kendisini değil; metadata'sını tuttuğunu söyler. Bu kısım bugünkü asıl konumuz değil ama genel bir bilgi vermek icap ederse Kurt Opsahl'dan bir alıntıya müracaat edebiliriz:

"Onlar sizin HIV testi yapan bir şirketle, ardından doktorunuzla ve ardından hayat sigortanızın şirketi ile aynı saatlerde konuştuğunuzu bilirler ama ne konuştuğunuzu bilmezler." (1)

Bu örnekte ne konuştuğumuz verinin kendisi; hangi saatlerde, kimlerle ve ne kadar süre görüştüğümüz ise bu verilerin metadata'sıdır. İlgilileri için anahtar kelime: HTS'dir.

Metadata türleri:

İç metadata; standart dosya içinde tutulan metadata'lardır. Dış metadata; iç metadata kaydının mümkün olmadığı ya da güvenli olmadığı durumlarda farklı bir kaynakta saklanan metadata'lardır. Üçüncüsü ise, güvenliğin had safhada olduğu durumlarda tercih edilir. Tutulan metadata kaydının farklı ve genellikle uzak bir veritabanı sisteminde saklandığı metadata'lardır. (2)

Metadata'nın önemi:

Metadata deyip geçmeyin! Zira, her şeyin başı olmasa da birçok şeyin başı olabilir. Nasıl yani? Metadata, "olumlu" ve "olumsuz" olmak üzere birçok şeyi ifade edebilir. Mesela, gizliliğinize halel getirebilir ya da bazen ayak iziniz, bazen parmak iziniz dahi olabilir! Hatta bazen mumla aranan bir ispat da olabilir.

Örneğin, adli davaların aydınlatılmasında, kumpasların ortaya çıkmasında ve hatta ülkelerin savaşa dahil olmasında bile önemli bir payı vardır. Grafiği yeterince yükseltip, önemini arz edebildiğimizi düşünüyorum. Şimdi ise daha gündelik yaşamdan bir örnek paylaşalım.

Iphone telefonunu çaldıran Bahar Anahmias, dedektifleri aratmayacak yöntemlerle çalınan telefonunu nasıl bulduğunu, Arka Kapı Dergi'nin ilk sayısında kaleme almıştı. İpucu tabii ki metadata! :)

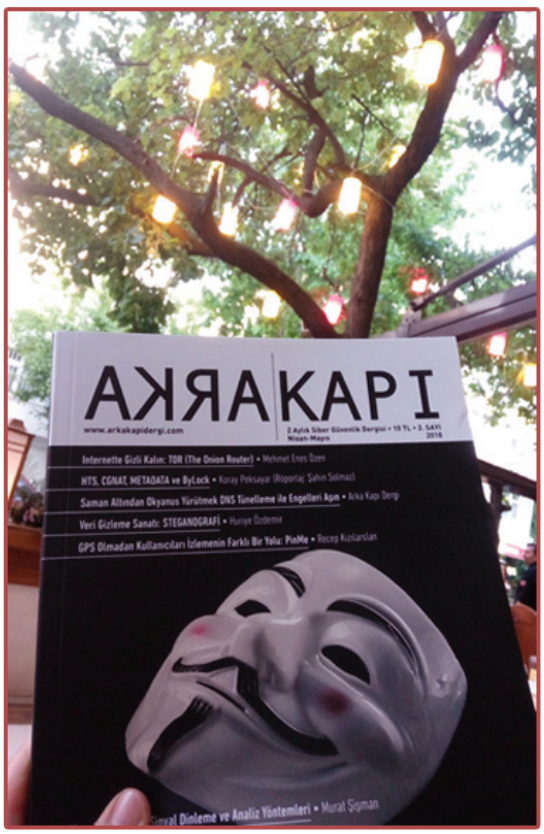
Metadata nasıl okunur, yazılır, düzenlenir, kaldırılır?

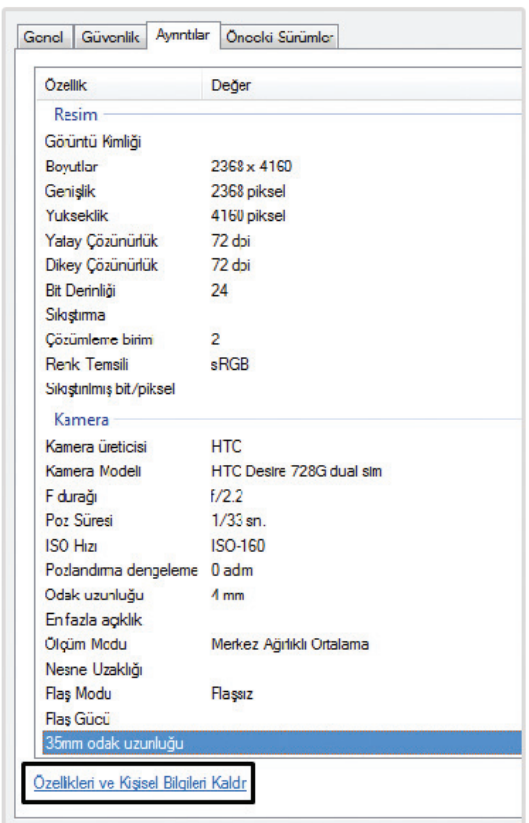
Bu düzenlemeleri yapabileceğimiz açık kaynak birkaç tane araç var. Bunlar:

- EXIF Tool: ExifTool, platformdan bağımsız ve belki de güncel, en eski metadata aracıdır. (okuma, yazma, silme işlemlerini gerçekleştirebilirsiniz.) https://sno.phy.queensu.ca/~phil/exiftool/
- MAT: Metadata Anonymisation Toolkit (https://mat.boum.org/ web sitesi sizi yeni kaynağa yönlendirecek, endişelenmeyiniz: https://0xacab.org/jvoisin/mat2).
- Android için Scrambled Exif var, Google Play'de de mevcut: https://f-droid.org/packages/com.jarsilio.android.scrambledeggsif/
- PDF-redact-tools ve https://github.com/firstlookmedia/pdf-redact-tools
- PDF paranoia aracına da ayrıca bakabilirsiniz. https://github.com/kanzure/pdfparanoia

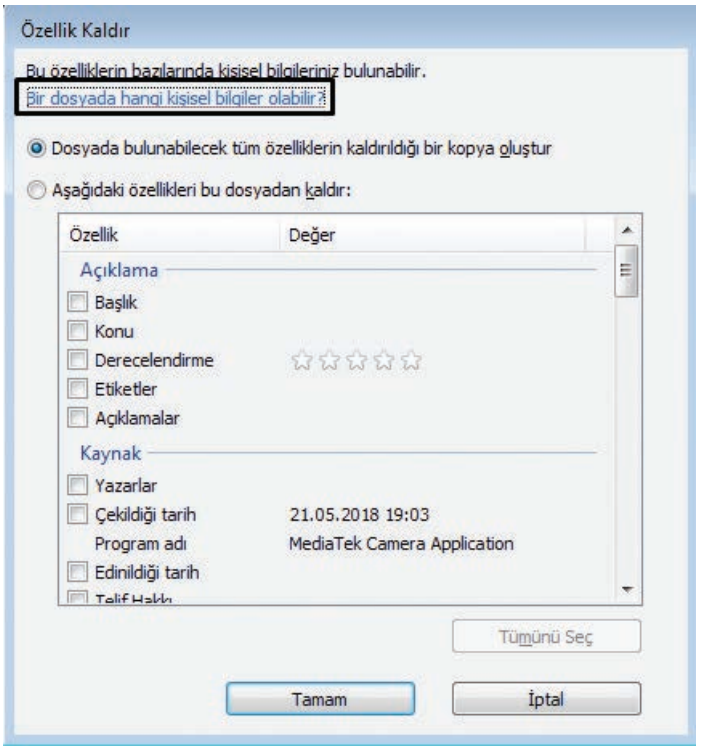
Bilmeyenler için küçük bir sürpriz! Bu özellik aslında Windows'ta da var, haydi bir bakalım. Örnek fotoğrafımıza sağ tık -> **Özellikler** -> **Ayrıntılar** diyerek bu fotoğrafa ait metadata'ları inceleyebiliriz.

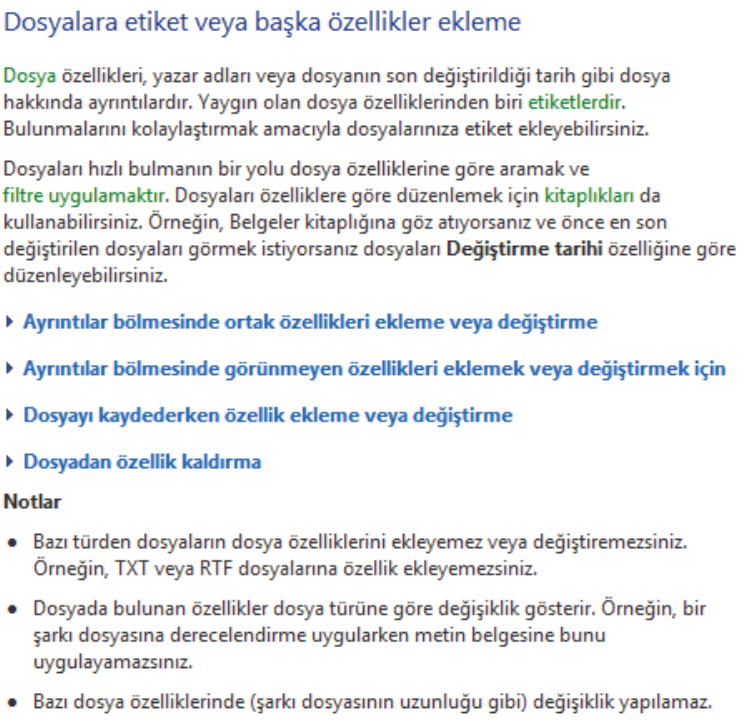
Sağ taraftaki tüm bilgiler, metadata oluyor.





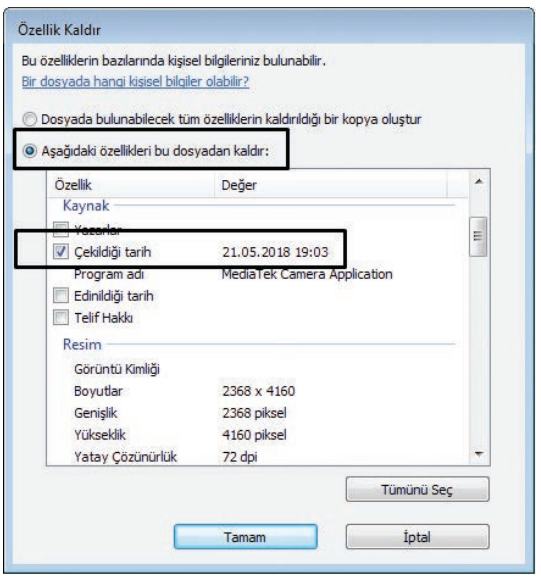
"Özellikleri ve Kişisel Bilgileri Kaldır" butonuna tıklayalım ve bakalım burada neler varmış:





İlgili seçenekler üzerinden genel bir bilgi aldıktan sonra, ilgili fotoğrafımızı seçelim ve ilgili klasörü tam ekran yapalım. Böylece klasör görüntüleyicinin alt kısmında metadata özet bilgilerini göreceğiz. Hatta buradan bazı verileri değiştirebiliyoruz. Örneğin, başlığa "Arka Kapı II. Sayı - Gizlilik" yazalım ve "**Kaydet**" diyelim.

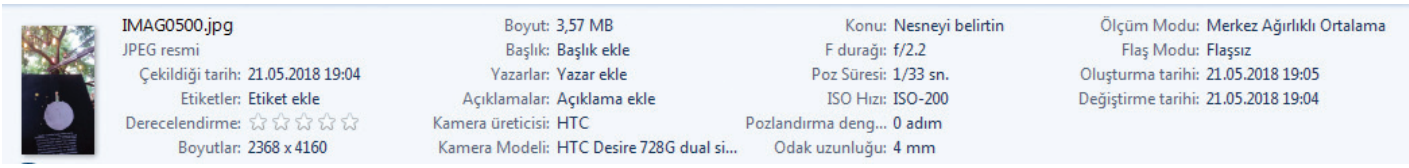
Böylece fotoğrafımıza bir başlık eklemiş olduk, şimdi de çekildiği tarihi ve kamera bilgilerini kaldıralım:



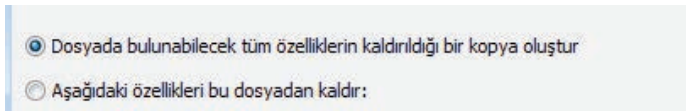
Tekrar bakalım: evet, başlık gelmiş ve çekilme tarihi ve kamera bilgileri de silinmiş.

Şimdi de farklı bir fotoğraf üzerinden, *"Dosyada bulunabilecek tüm özelliklerin kaldırıldığı bir kopya oluştur."* seçeneğini deneyelim:

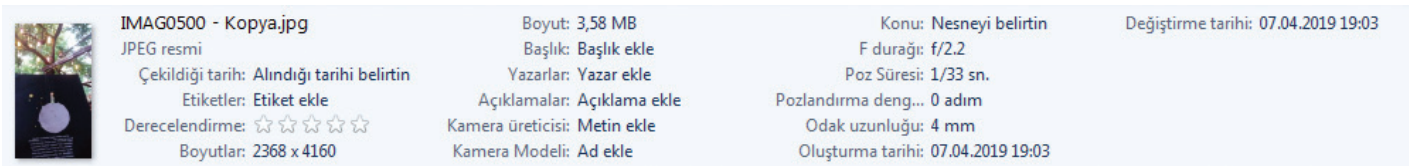
Orjinal hali:



Aynı kısımdan (Araçlar -> Özellikler -> Özellikleri ve Kişisel Bilgileri Kaldır) ilgili seçeneğimizi seçtik.



Ve sonuç: Aynı dizinde bir kopya oluşturdu ve birçok metadata bilgisini silmiş oldu:



Bu görselde küçük bir ayrıntı dikkatinizi çekmiş olmalı: boyut. Orjinal görselimiz, 3.58 MB (disk boyutu: 3.760.128 bayt) iken, üst-verileri kaldırdığımız yeni görselin boyutu: 3,57 MB (diskteki boyutu: 3.747.840 bayt) oldu. *(Söylemeden geçemeyeceğim: aklıma gündemdeki malum konu geldi... :)*

Yukarıda da bahsettiğimiz üzere, dosya iç metatadata'ları dosyanın içerisinde tutulduğu için, biz de bu verilerden bazılarını silince, boyut bir miktar düşmüş oldu.

Bittabi, kuşkulu akıllara hemen şu soru geliyor: Acaba gerçekten her şey göründüğü gibi mi ilerledi, yani bu veriler gerçekten silindi mi? Hızlıca bir bakalım. En pratik yoldan ilerliyoruz, EXIF datalarını inceleyebileceğimiz birçok online ve ücretsiz web sitesi var, bir tanesinden hemen bakıyoruz.

http://exif.regex.info/

Bir de gördük ki!

EXIF

Exif Image Size	2,368 × 4,160
Image Description	
Software	MediaTek Camera Application
Modify Date	**2018:05:21** 19:04:04 10 months, 16 days, 14 hours, 17 minutes, 21 seconds ago

Aynı sorgu ekranından farklı bir tablo, uyarı ile birlikte bize gerçeği tekrar göstermiş oldu.

Composite
This block of data is computed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized.

Aperture	2.20
Megapixels	9.9
Shutter Speed	1/33
Modify Date	**2018:05:21** 19:04:04.79 10 months, 16 days, 14 hours, 17 minutes, 21 seconds ago
Focal Length	3.5 mm

Yani, Windows'un metadata remover özelliği bizi yanıltmış oldu. Orjinal görselin adı: IMAG0500.jpg idi, sonuçlar gördüğünüz üzere orjinal görseldeki verilerle uyuşuyor. Yani, sildiğimizi düşündüğümüz 2018 verisinin hâlâ duruyor olduğunu gördük. O halde hemen ExifTool'a geçiş yapalım.

ExifTool

ExifTool, Phil Harvey tarafından geliştirilen, 2003'ten bu yana varlığını sürdüren efsane bir araçtır. Platform bağımsız (Win. - Mac - Unix) bir Perl kütüphanesinin yanı sıra birçok dosya türündeki metadata bilgisini okumak, yazmak ve düzenlemek için kullanılan bir komut satırı uygulamasıdır.

Mümkün olan en hızlı ve basit yolu tercih ederek kuruluma başlıyoruz. *Bu örnekte Linux tabanlı bir işletim sistemi kullanılmıştır. Farklı platformlar için endişelenmeyiniz, yazının sonunda işinizi ciddi anlamda kolaylaştıracak bir web sitesi paylaşacağız.*

Aşağıdaki adresten aracımızı indirelim.

- http://owl.phy.queensu.ca/~phil/exiftool/

İlgili klasöre geçiş yapalım,

- # cd ~ /Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35

```
root@kali:/#
root@kali:/# cd ~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35
root@kali:~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35#
```

- Kurulum için aynı klasör içerisinde iken, sırasıyla aşağıdaki komutları çalıştıralım:
  - `# perl Makefile.PL`
  - `# make`
  - `# make install`
- Kurulum tamamlandı:

```
Installing /usr/local/bin/exiftool
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/perllocal.pod
root@kali:~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35#
```

Hemen örnek bir görsel üzerinden bir metadata okuması yapalım:

- # exiftool t/images/ExifTool.jpg

İşte örnek görselin çıktısı *(yaklaşık 4 sayfa civarında bir çıktı verdi):*

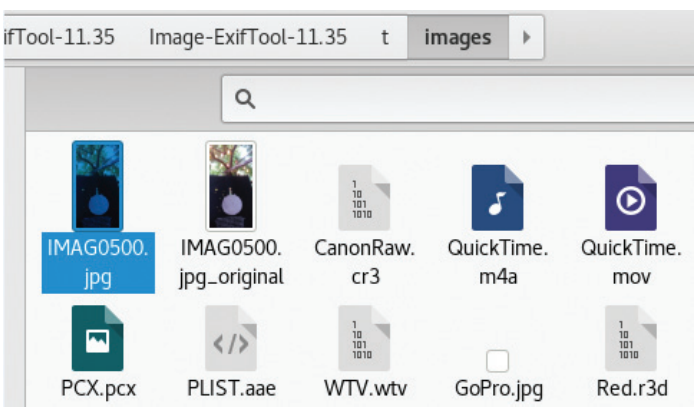
```
ExifTool Version Number         : 11.35
File Name                       : ExifTool.jpg
Directory                       : t/images
File Size                       : 25 kB
File Modification Date/Time     : 2014:09:23 16:15:01+03:00
File Access Date/Time           : 2019:04:09 22:11:35+03:00
File Inode Change Date/Time     : 2019:04:09 22:11:35+03:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Image Description               : A witty caption
Orientation                     : Horizontal (normal)
Software                        : Adobe Photoshop 7.0
Modify Date                     : 2004:02:26 09:36:46
Artist                          : Phil Harvey
Y Cb Cr Positioning             : Co-sited
F Number                        : 3.5
Exposure Program                : Program AE
ISO                             : 100
Exif Version                    : 0210
Create Date                     : 2001:05:19 18:36:41
Components Configuration        : Y, Cb, Cr, -
Compressed Bits Per Pixel       : 1.6
Brightness Value                : 2
Max Aperture Value              : 3.5
Metering Mode                   : Multi-segment
Flash                           : Fired
Focal Length                    : 6.0 mm
Flashpix Version                : 0100
Exif Image Width                : 100
Exif Image Height               : 80
Focal Plane X Resolution        : 3053
Focal Plane Y Resolution        : 3053
Focal Plane Resolution Unit     : cm
```

- Şimdi de yukarıda bahsi geçen IMAG0500.jpg'e ait tüm metadata'ları silelim,

```
# exiftool -all = t/images/IMAG0500.jpg
```

```
root@kali:~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35# exiftool -all= t/images/IMAG0500.jpg
    1 image files updated
root@kali:~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35#
```

dedik ve fotoğrafın orjinalini koruyarak, metadata'ların silinmiş olduğu bir kopyasını oluşturduk:



- Hızlıca farklı bir (online) tool (http://exif.regex.info/) üzerinden test ediyoruz, ve işte sonuç:

File — basic information derived from the file.

File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
File Size	3.4 MB
Image Size	2,368 × 4,160
Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)

Composite
This block of data is computed based upon other items. Some of it may l
resized.

Megapixels	9.9

Harika! Her şey silinmiş. Şimdi bir de bir üst-veri yazalım,

```
# exiftool -artist=”Thank you Phil” -copyright=”Arka Kapi” t/images/IMAG0500.jpg
```

```
rka Kapi" t/images/IMAG0500.jpg
    1 image files updated
root@kali:~/Downloads/Image-ExifTool-11.35/Image-ExifTool-11.35#
```

```
# exiftool t/images/IMAG0500.jpg
```

komutu ile sonuca bir bakalım,

```
Artist                          : Thank you Phil
Y Cb Cr Positioning             : Centered
Copyright                       : Arka Kapi
```

Evet, böylece ExifTool ile metadata'lar nasıl okunur, nasıl silinir ve nasıl yazılır sorularını birer örnek ile cevaplamış olduk. Tabii ki birden fazla dosya için hatta x klasöründeki tüm dosyalar ya da uzantısı sadece y olan dosyalar için benzer işlemleri yapabilirsiniz. İlgili bağlantılar bu konuda faydalı olacaktır.

“Keşke bir arayüzü olsaydı!” diyenler, aşağıdaki site sizin için. Evet, bir arayüzü yok ama Windows, Mac ve *Nix sistemler için ihtiyacınız olan tüm komutların birer örnekleri burada mevcut.

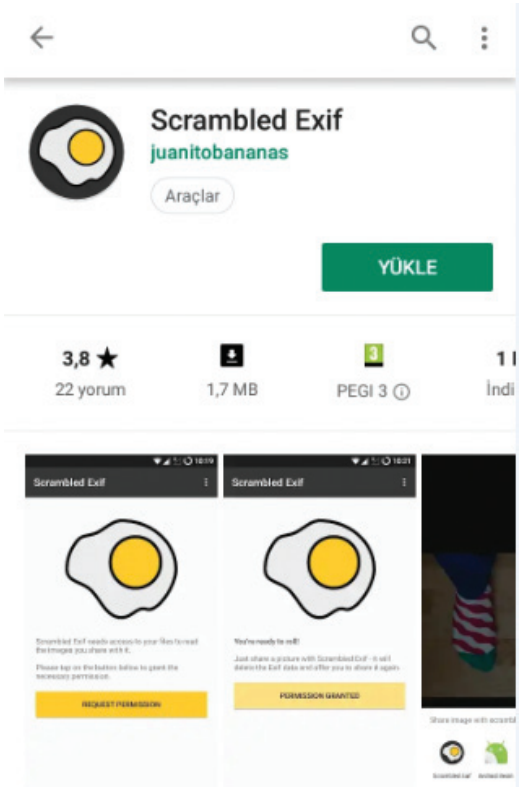
http://owl.phy.queensu.ca/~phil/exiftool/examples.html

Sırada Android kullanıcıları için geliştirilen Scrambled Exif isimli uygulama var.

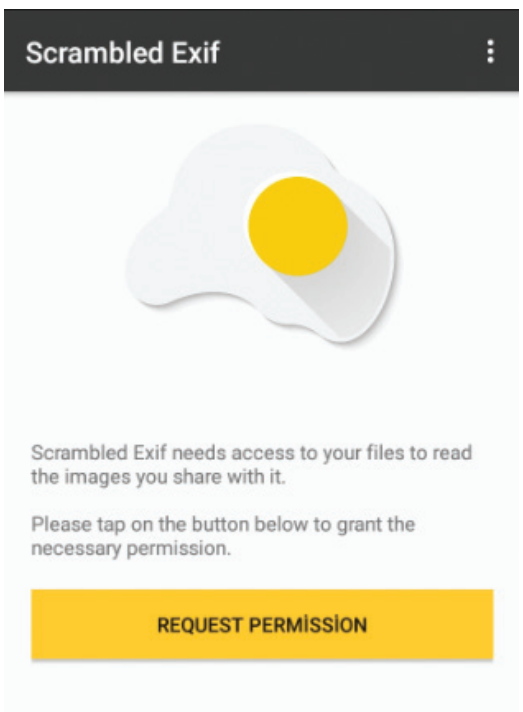
Scrambled Exif

Android kullananlar için ücretsiz bir uygulama olan Scrambled Exif'e hızlıca bir bir göz atalım.

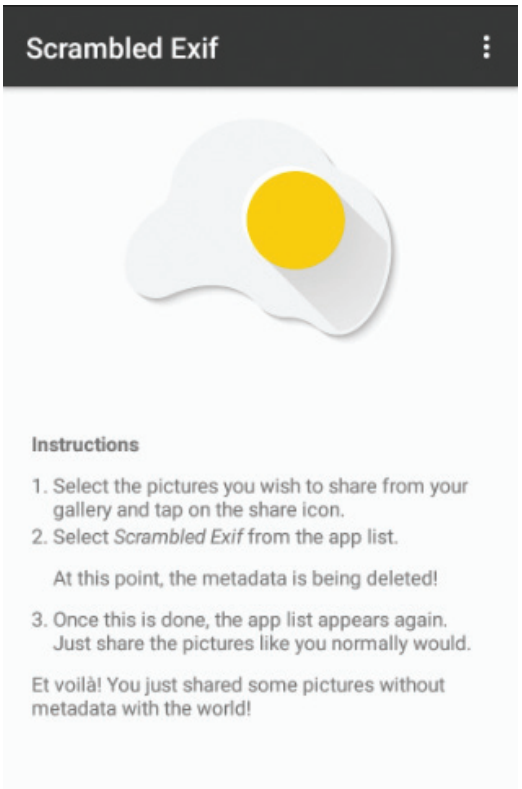
- Yükleyeceğimiz uygulama: Scrambled Exif



- Yükledikten sonra uygulamamıza izin veriyoruz.



Görselde de belirtildiği üzere, galeriye gidiyoruz. Herhangi bir görseli açıyoruz. Paylaş, seçeneği üzerinden Scrambled ikonuna tıklıyoruz. İşte o anda uygulamamız ilgili görsele ait tüm metadata'ları silmiş oluyor. Daha sonra ise, göndermek istediğiniz yere göre ilgili uygulamamızı (örn: Gmail) seçip, gönderiyoruz.



Evet, hepsi bu kadar!

Not: Lütfen bu makalede bahsi geçen uygulama ve yöntemleri bizzat denemeden kesin bir sonuca vardığınızı düşünmeyiniz. En az ikinci bir araçla (mümkünse farklı bir platformda) işleminizi doğrulayınız.

İlgili bağlantılar:

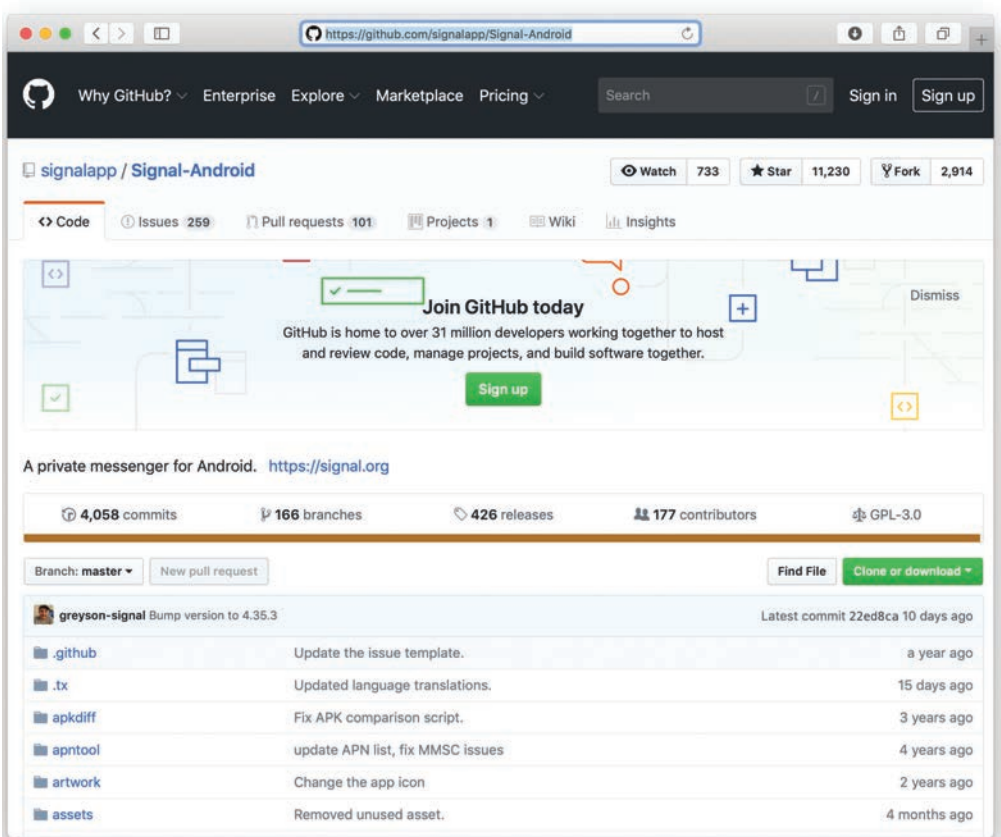
1. https://www.eff.org/deeplinks/2013/06/why-metadata-matters
2. Arka Kapı Dergi II. Sayı - Koray Peksayar - Şahin Solmaz (Söyleşi - Sf. 37)
3. https://github.com/exiftool/exiftool
4. http://owl.phy.queensu.ca/~phil/exiftool/
5. http://owl.phy.queensu.ca/~phil/exiftool/examples.html
6. https://play.google.com/store/apps/details?id=com.jarsilio.android.scrambledeggsif&hl=en_US

Murat Şişman - info@muratsisman.com

Signal ile Kendi Mesajlaşma Uygulamamızı Yapalım

Son günlerde mesajlaşma uygulamalarındaki güvenlik soruları sıkça gündemde yer buluyor. Arka Kapı Dergisinin önceki sayılarında hangi mesajlaşma uygulamasının hangi güvenlik yöntemlerini kullandığını detaylı şekilde anlatan yazılar yayınlanmıştı fakat bu sefer kendi güvenli mesajlaşma uygulamamızı kendimiz yapıyoruz.

Signal; açık kaynak olarak ve ücretsiz dağıtılan bir sistem olup kullanıcılarına uçtan uca şifreleme ile güvenli bir mesajlaşma ortamı sunuyor. Android ve iOS gibi cihazlar için önceden hazırlanmış çalışır haldeki uygulama kodları Github üzerinde de yayınlanmakta olup dileyen herkes bu kodları bilgisayarlarına indirip gerekli düzeltmeleri gerçekleştirerek başka isimler altında diledikleri gibi yayınlayabilirler. Tıpkı PTT Messenger gibi.



(Signal iOS ve Android uygulaması kaynak kodlarına https://github.com/signalapp adresinden erişilebilir)

Bilindiği üzere geçtiğimiz yıllarda tüm haber kanalları ve gazetelerde kamu ve kolluk kuvvetlerimizin kullanımı için Türk mühendislerinin %100 yerli ve milli olarak geliştirdiği mesajlaşma sistemi olan *PTT Messenger'ın* kullanılacağı haberleri gündeme oturmuştu. Dönemin Başbakanı ve Genel Kurmay Başkanı dahi bu uygulamayı kullanırken görüntüleri medyaya yansımıştı. Oysa %100 Türk mühendislerinin geliştirdiği söylenen uygulama, Signal'in Github hesabından indirilen kaynak kodlarının yalnızca Logo değiştirilerek yeniden derlenmesinden başka bir şey değildi. Kim bu projeyi gerçekleştirdi bilinmez ama ülkemizin başbakanının dahi uygulamayı %100 yerli-milli, Türk mühendisler tarafından geliştirildi şeklinde duyurması o günlerde oldukça tepki almıştı. Birçok kişinin, konuyla ilgili yetkililere bu uygulamanın devletimize ne kadar ücrete mal olduğunu sormasına rağmen bir cevap alınamaması da ayrıca üzücü bir durum oluşturmuştu.

Tarafınıza Gönderilen Cevaplar

Cevap Gönderilme Zamanı: 26.04.2019 14:25:49
Cevap Seri No: 20190426142549
Cevap Metni:

Sayın Şahin Solmaz,
İlgi : 2019-816796 Numaralı Info Başvurunuz,

PTT Messenger Uygulaması PTT A.Ş. ye bağlı PTT Bilgi Teknolojileri A.Ş. tarafından üretilmiştir. Ürünün maliyeti hakkında bilgi verilmemektedir.
Saygılarımla,

ELEKTRONİK POSTA D. BŞK.-ELEKTRONİK HİZMETLER ŞUBE MÜDÜRLÜĞÜ

Tarafınıza Gönderilen Cevaplar

Cevap Gönderilme Zamanı: 02.05.2019 15:30:54
Cevap Seri No: 20190502153054
Cevap Metni:

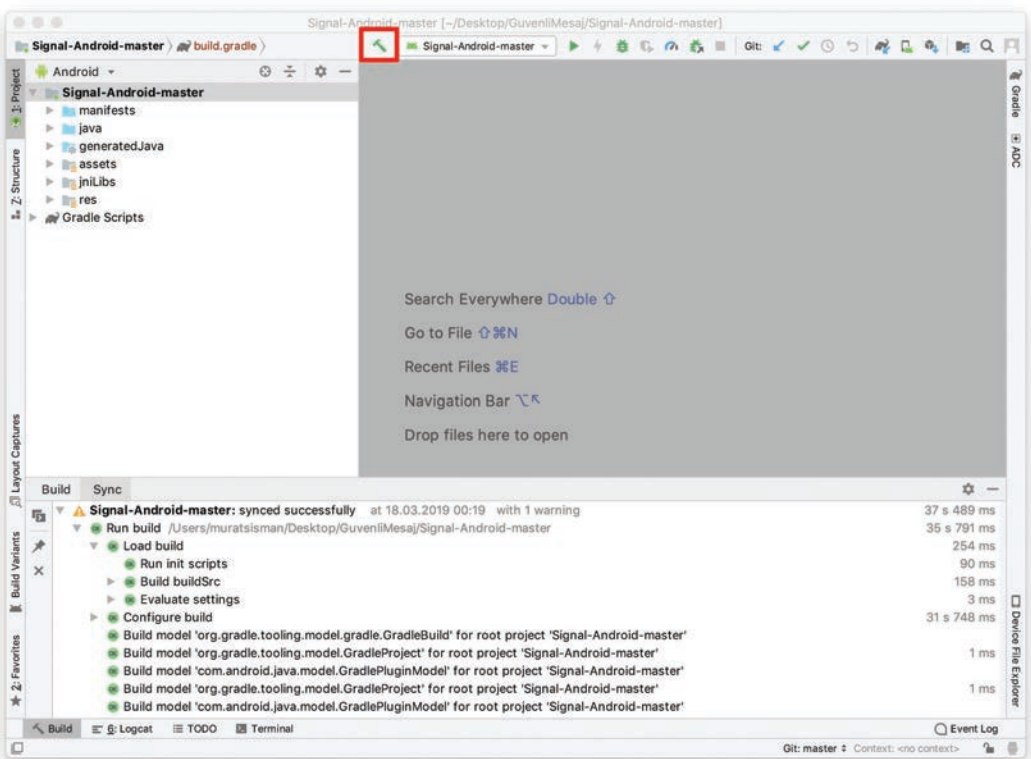
Sayın Şahin Solmaz,
İlgi : 2019-818904 Numaralı Info Başvurunuz,
PTT Messenger ürününün kullanıcısı kamu kurumları olmasından dolayı tarafınızla herhangi bir ilgisi tespit edilememiştir. Anılan ürüne ilişkin olarak Şirketimizin Gizlilik Prensipleri göz önüne alındığında ticari sır teşkil edeceğinden söz konusu ürünle ilgili olarak tarafınıza bilgi verebilmemiz mümkün değildir.
Saygılarımla,

ELEKTRONİK POSTA D. BŞK.-ELEKTRONİK HİZMETLER ŞUBE MÜDÜRLÜĞÜ

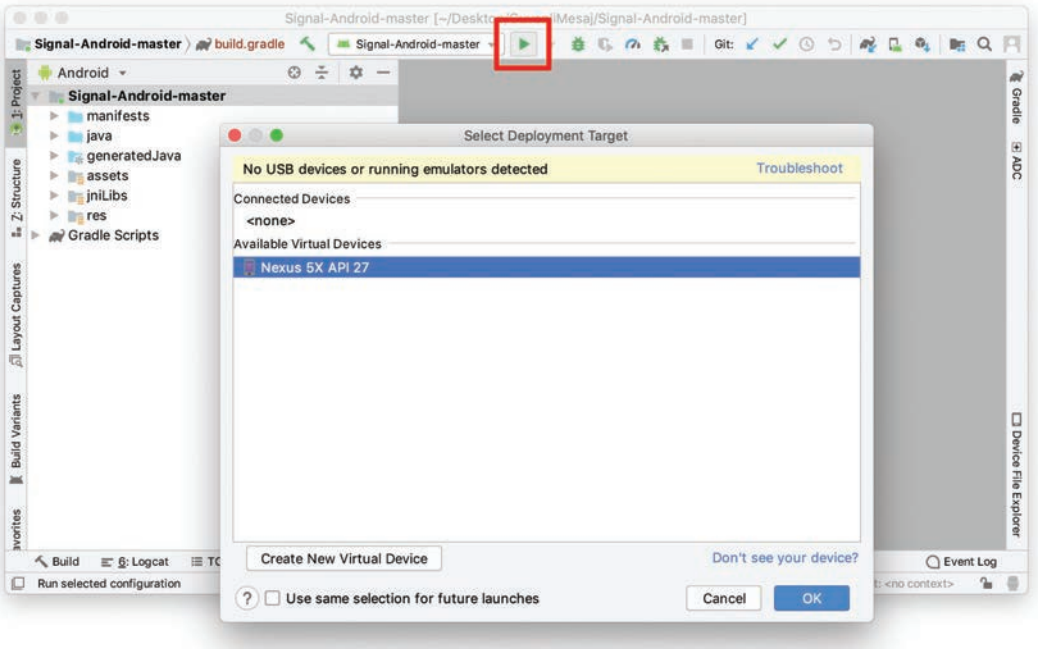
Yazımızda hazırlayacağımız mesajlaşma uygulamasının Android sürümünü oluşturacağız, dileyen okuyucularımız iOS sürümünü de aynı Github hesabından indirebilirler.

Güvenli Mesaj V1.0

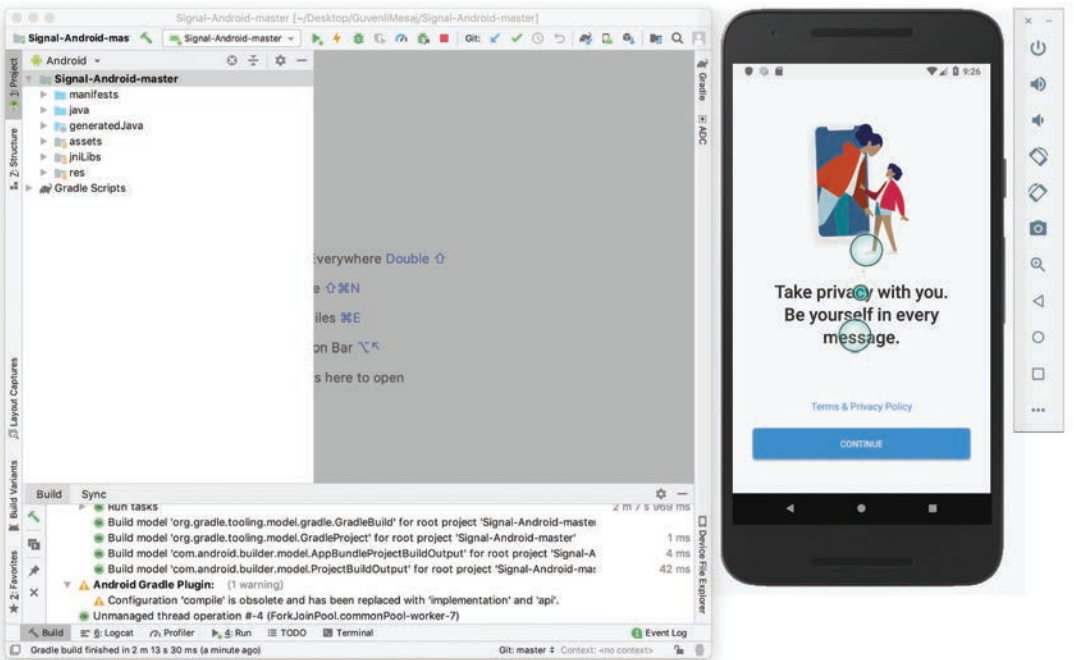
Github hesabından indirdiğimiz Android uygulamasına ait kodları *Android Studio* yazılımı ile açtıktan sonra çekiç simgesine tıklayıp *Gradle Build* işlemini gerçekleştirerek hazır hale getirmeliyiz. İşlem başarıyla tamamlandıktan sonra Signal-android-master modülü görünür olacaktır ve çalıştır butonuna tıkladığımızda Virtual Device (simülatör) veya cihazdan test edebilir hale gelecektir.

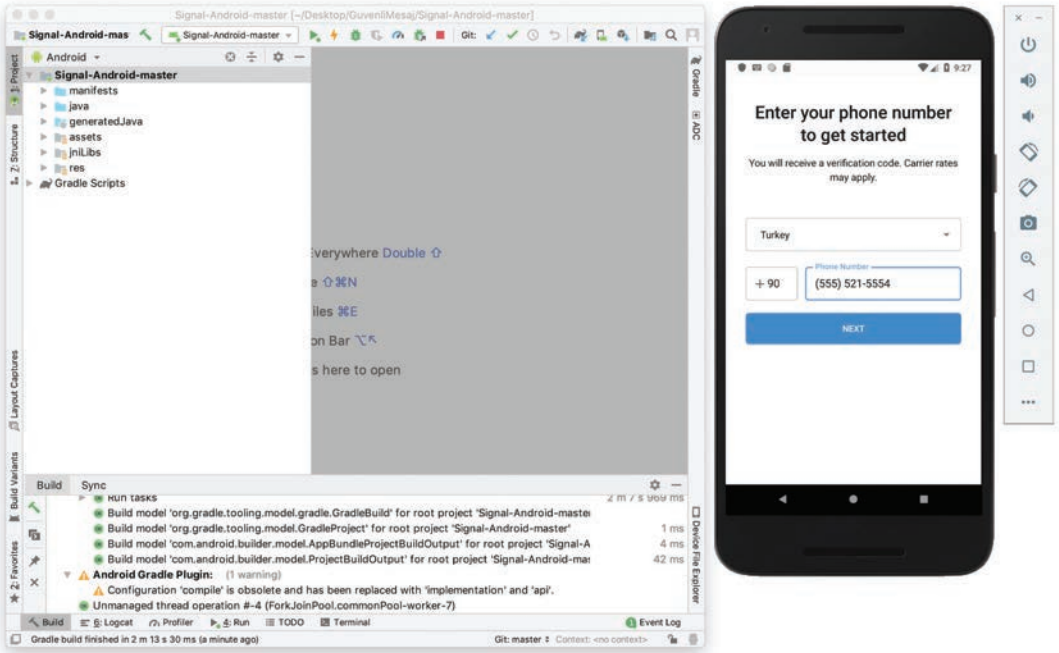


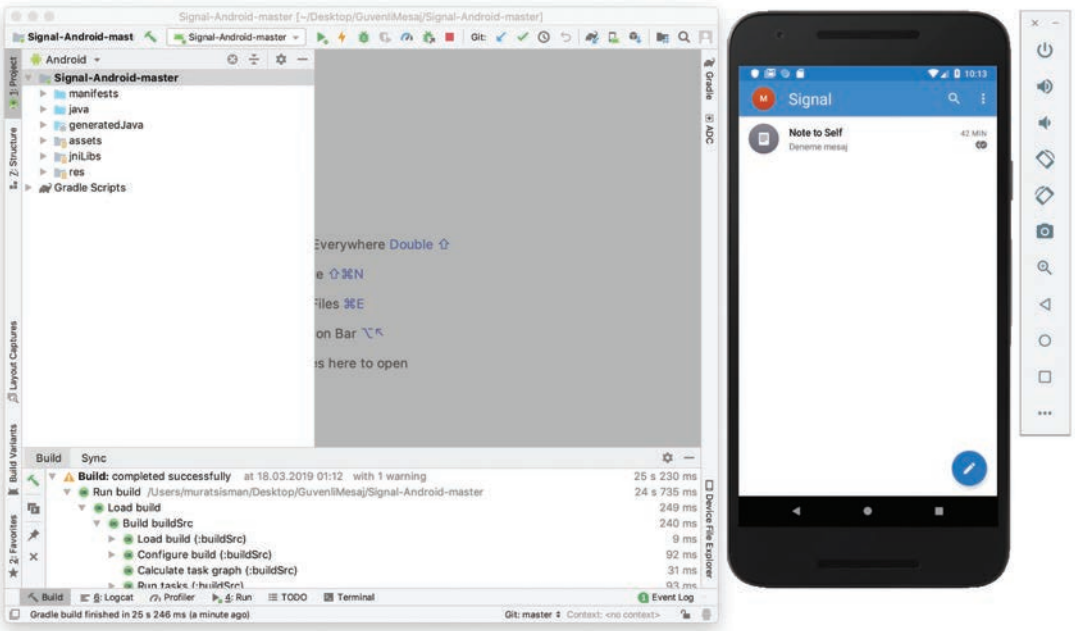
Android Studio içerisinde Run butonuna bastığımızda uygulamanın çalışacağı cihazın seçilmesi için bir ekran ortaya çıkmaktadır. Eğer USB kablo ile cihazınız bilgisayar bağlı ise bu listede görünecektir ya da yeni bir Virtual Device (simülatör) oluşturarak burada çalışmasını sağlayabilirsiniz.



İşte karşımızda Signal uygulaması!



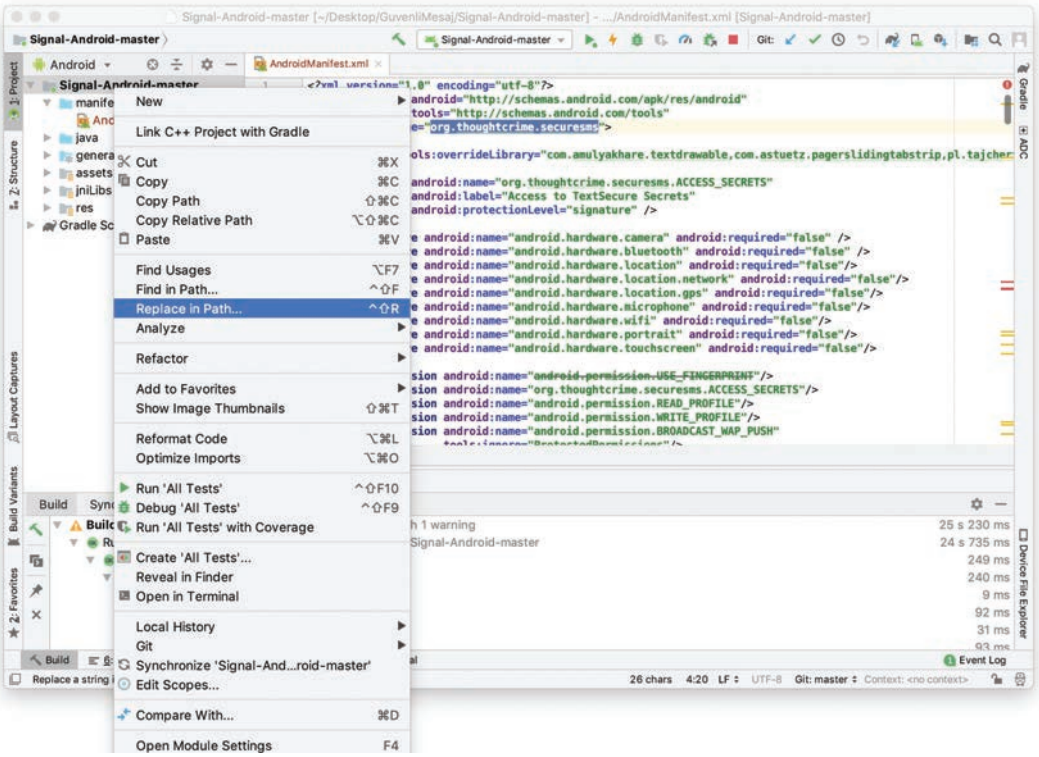




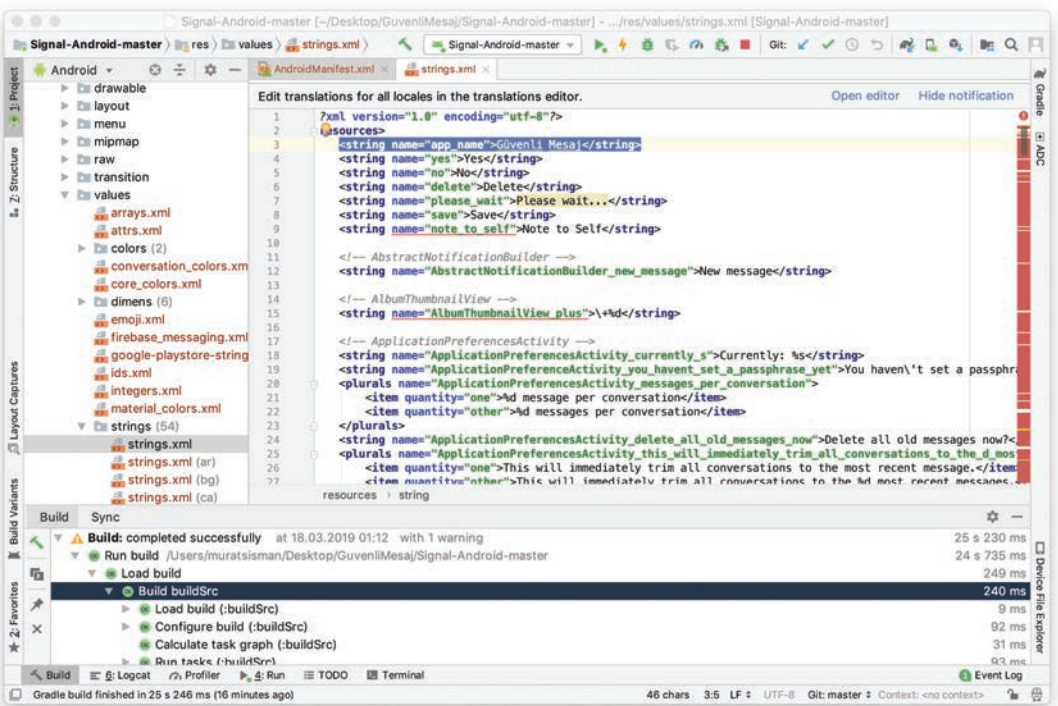
Signal Android uygulaması birçok yabancı dil desteğine sahip olduğu için ayrıca Türkçeleştirmek için vakit harcamamıza gerek yoktur. Görsellerde simülatör dili İngilizce olduğu için varsayılan olarak İngilizce görünmektedir.

Dikkat etmemiz gereken en önemli nokta şudur; şu ana kadar Signal uygulamasının orijinal sürümünü derleyip simülatörde çalıştırdık yani orijinal Signal uygulamasını yeniden derlemiş olduk. Şimdi bu kodları kendimize ait yeni bir uygulamaya çevirmemiz gerekiyor.

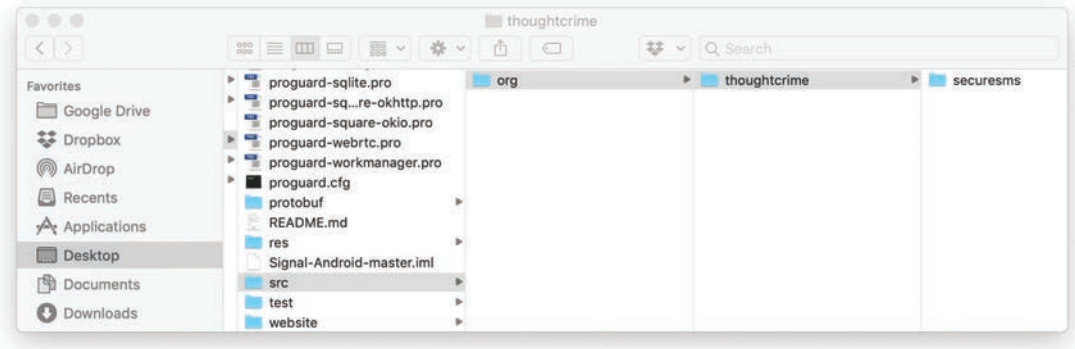
AndroidManifest.xml dosyasının ilk satırlarında yer alan *package* bölümünde yazan *org.thoughtcrime.securesms* Signal'in orijinal ismi olup bunu kendimize ait bir isimle değiştirmeliyiz. Örneğimizde uygulama paket adını *com.muratsisman.guvenlimesaj* olarak belirleyeceğimiz için tüm *org.thoughtcrime.securesms* içeriğini *com.muratsisman.guvenlimesaj* olarak değiştirmemiz gerekmektedir. En kısa yoldan tüm dosyaların içeriğinde bu değişikliği yapmak için projeyi sağ tıklayıp, açılan context menü'den *Replace in Path* özelliğini kullanabiliriz.



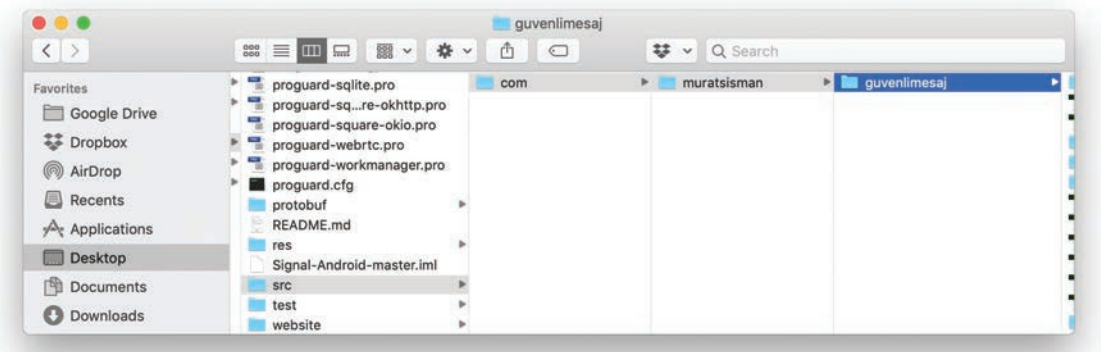
Son adım olarak uygulamamızın cihaz ekranında görünen ismini Güvenli Mesaj olarak değiştirmek için *strings.xml* dosyasındaki *app_name* alanını ve ardından kaynak kodların bulunduğu klasördeki isimleri *com.muratsisman.guvenlimesaj* olarak düzenliyoruz.



(strings.xml içerisinde app_name alanı)

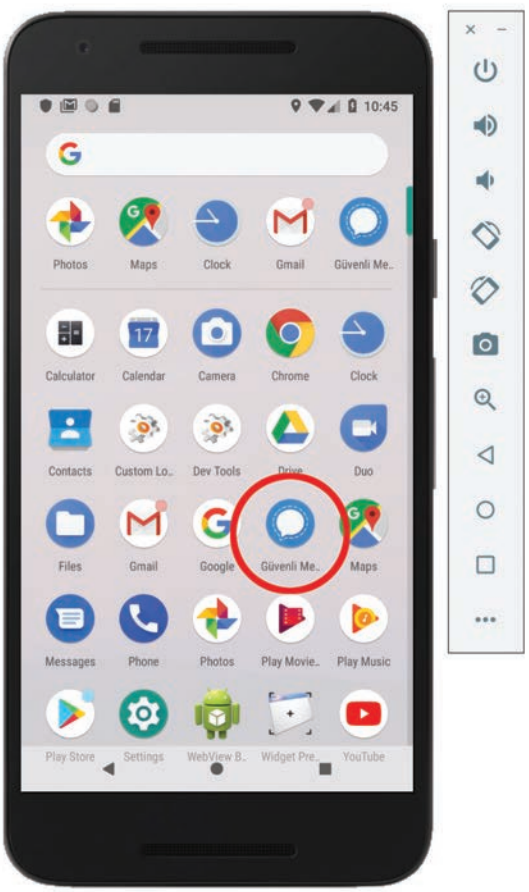


(src -> org -> thoughtcrime -> securesms)



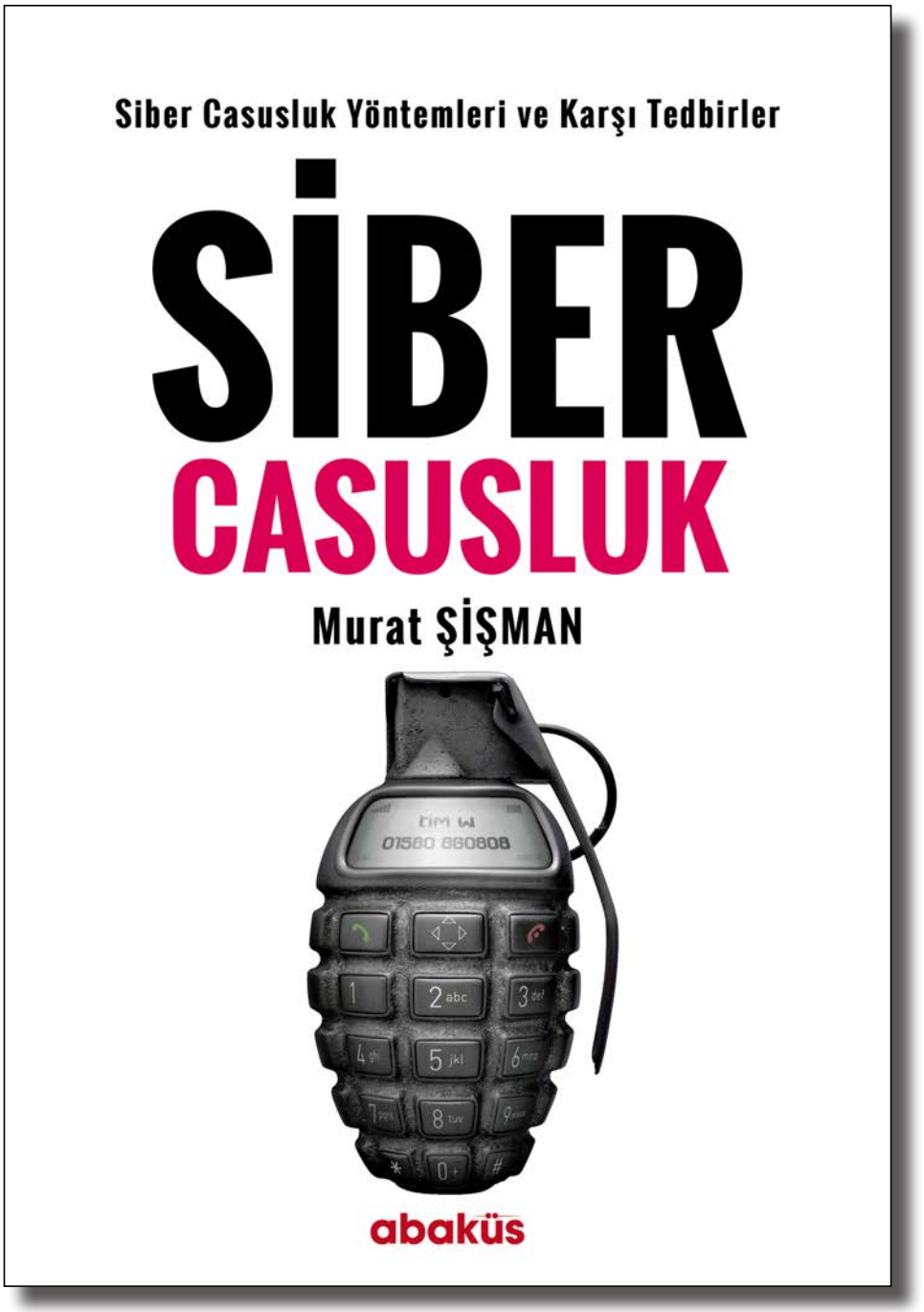
(src -> com -> muratsisman -> guvenlimesaj)

Uygulamamız Güvenli Mesaj adı altında orijinal Signal'den tamamen farklı olarak hazırlanmış oldu. Logo ve içeriğinde görsel öğeleri de değiştirerek kendinize ait güvenli mesajlaşma uygulamanızı GooglePlay mağazasında yayınlayabilirsiniz.



SİBER CASUSLUK

MURAT ŞİŞMAN



abaküs

Besim Altınok - besimaltnok@gmail.com

Eduroam Akademi Ağlarında Büyük Tehlike!

Bu yazıda sizlere kablosuz ağ üzerinden gelebilecek korkunç bir saldırı ve bunun muhtemel risklerinden bahsedeceğim. Çoğumuzun yolu üniversite sıralarından geçmiştir. Hepimiz öğrencilik hayatımızda **Eduroam** ağlarına bağlanmışızdır. Öğrenci ve akademisyenler için vazgeçilmez durumlardan bir tanesidir. Ancak faydası olduğu kadar kişisel gizliliği bozabilecek ve yetkisiz erişimlere kapı açacak bir yapıya da sahiptir! Herhangi birisinin sizin öğrenci bilgi sistemine erişiminde kullandığınız parola bilgisini elde edebildiğini bir düşünün. Belki de ileride, bu haberden sonra, daha çok **"Notunu değiştirerek mezun oldu"** haberlerini duyacağız.

Konuya girmeden önce sizlerle bazı temel bilgileri paylaşmak istiyorum. Konuyu ve tehdidi daha iyi anlayabilmeniz açısından oldukça faydalı olacaktır.

Eduroam nedir?

Eduroam, Education Roaming (Eğitim Gezintisi) kelimelerinin kısaltmasıdır. RADIUS tabanlı altyapı üzerinden 802.1x güvenlik standartlarını kullanarak, Eduroam üyesi kurumların kullanıcılarının diğer eğitim kurumlarında da sorunsuzca ağ kullanımını amaçlamaktadır.

Eduroam üyesi kurumların kullanıcıları, kendi kurumlarında (Ev Kurum) ağa bağlanmak için kullandıkları kullanıcı adı ve parola çifti ile Eduroam üyesi olan başka bir kurumda (Misafir Kurum) da ağa bağlanabilirler.

Kullanıcı misafir kurumda iken Eduroam yayınına bağlantı talebi gönderdiğinde, misafir kurumun yetkilendirme sunucusu, o kullanıcıyı kendi ev kurumunun yetkilendirme sunucusuna yönlendirerek, yetkili olup olmadığını belirler. Tüm bu sorgulamaların, sunucular arasında oluşturulan şifreli bir tünel içinden yapılması, kullanıcı adı ve parola çiftinin kullanıcının kendi ev sunucusu haricinde görülmesini engeller. Bu durumda kullanıcıların yapması gereken tek şey, misafir olduğu kurumda yer alan Eduroam kablosuz ağını, kendi kurumunun ağına bağlanır gibi tanımlamasıdır. (**Kaynak**: http://www.eduroam.org.tr/whatis.php)

Eduroam federasyon hiyerarşisine sahiptir. Halen dünyada iki konfederasyon bulunmaktadır: Avrupa Eduroam Konfederasyonu ve Asya-Pasifik (APAN) Eduroam Konfederasyonu. Eduroam üyesi kurumlar kendi ülkelerinde yer alan Eduroam federasyonlarına, ülkelerin federasyonları da bağlı bulundukları konfederasyonlara sorgu göndermektedir. Türkiye'nin bağlı bulunduğu Avrupa Eduroam Konfederasyonu'na ve APAN Konfederasyonu'na katılan her yeni federasyon ve onlara katılan her yeni kurum, bu hiyerarşi sayesinde dahil olan herkesçe tanınabilmektedir. (**Kaynak**: http://www.eduroam.org.tr/whatis.php)

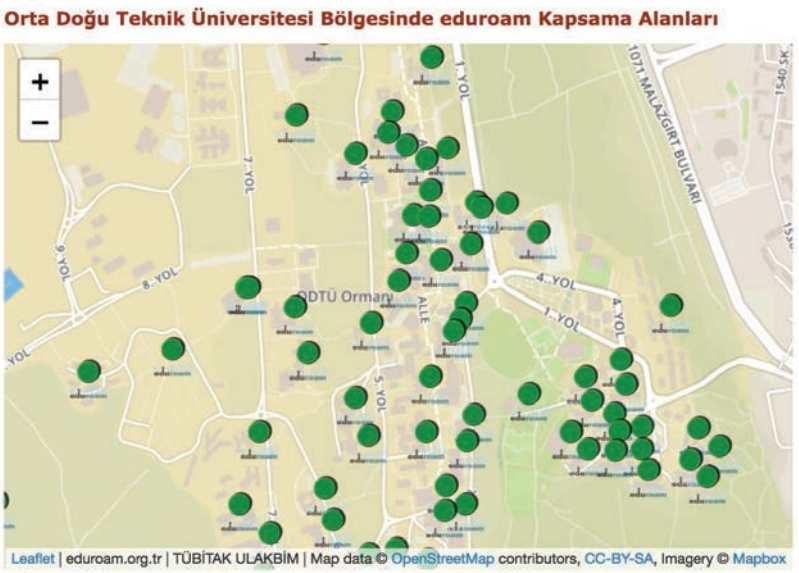
Eduroam Türkiye Katılımcıları

Türkiye'de yaklaşık 125 kurum Eduroam sistemini kullanmaktadır. Türkiye'nin en büyük ve prestijli üniversiteleri de bu altyapıya dahildir. Yandaki haritada Türkiye'deki dağılımı görebilmeniz mümkündür.

Dilerseniz daha detaylı erişim noktası dağılımları için http://eduroam.org.tr/participants.php adresini ziyaret edebilirsiniz.

Bir lokasyona ait Eduroam erişim noktaları

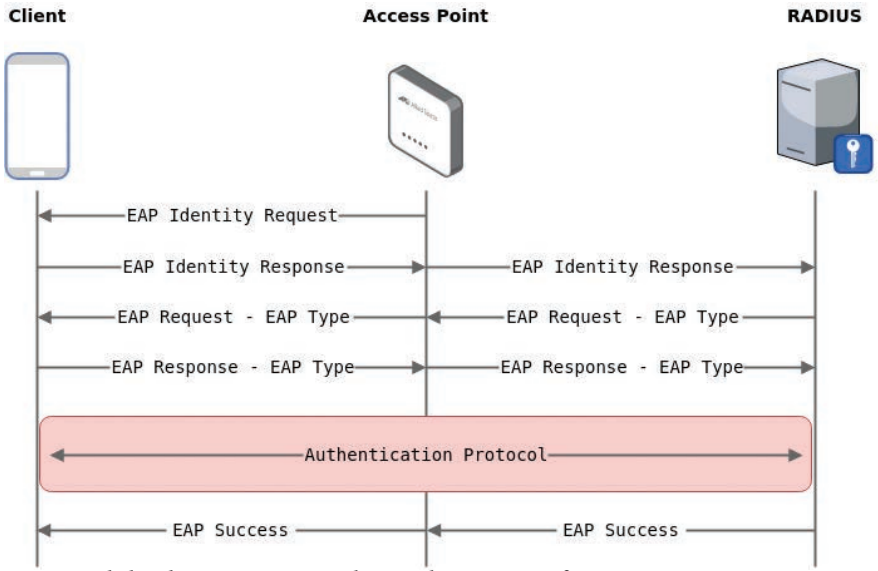
Yandaki görselde görüleceği üzere Eduroam ağlarına ait detay ve lokasyon bilgilerini elde edebilirsiniz.



Yetkilendirme Türleri

Üye üniversiteler üzerinde yaptığımız genel analiz neticesinde yetkilendirme tipi olarak **EAP-TTLS** ve **Inner Authentication** olarak da **PAP** kullanıldığını gözlemledik. Bu noktada protokollerin genel özellikleri için detaylı bir anlatım yapmayacağız. Sadece genel yapıyı anlaşılması açısından özet açıklamalar ile yetinilecektir.

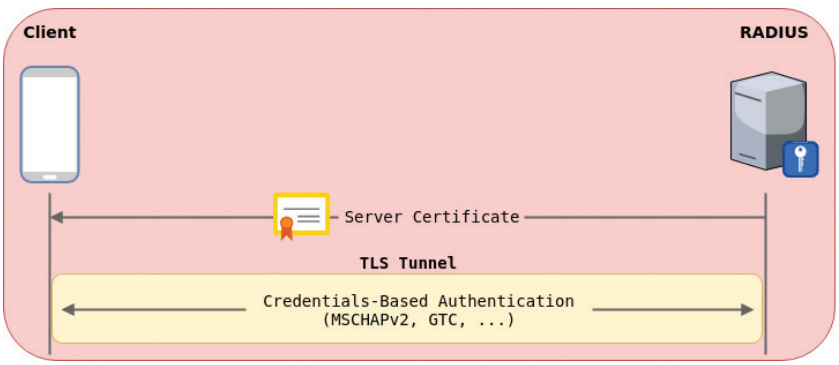
- **EAP-TLS:** Yalnızca sertifika tabanlı kimlik doğrulamasına izin veren bir yetkilendirme metodudur. Güvenlik kimlik denetimi için TLS protokolünü kullanmaktadır.
- **PEAP:** EAP yetkilendirme tipini bir TLS tünel içerisinde işletmeyi sağlayan metot. Aslında bir yöntemden çok bir kapsülleme olarak adlandırabiliriz.
- **EAP-TTLS:** TLS tüneli üzerinde bir EAP sağlamak amacı ile kullanılmaktadır.



Şekil 1: https://pwn.no0.be/exploitation/wifi/wpa_enterprise/

Inner Authenticaion Yöntemleri

Bu yöntemler **Tunneled Authentication** olarak da adlandırılabilir. Yani ilk olarak sertifika tabanlı bir doğrulama sağlanır ve daha sonra kullanıcı adı parola göndermek için bu yöntemler kullanılır.

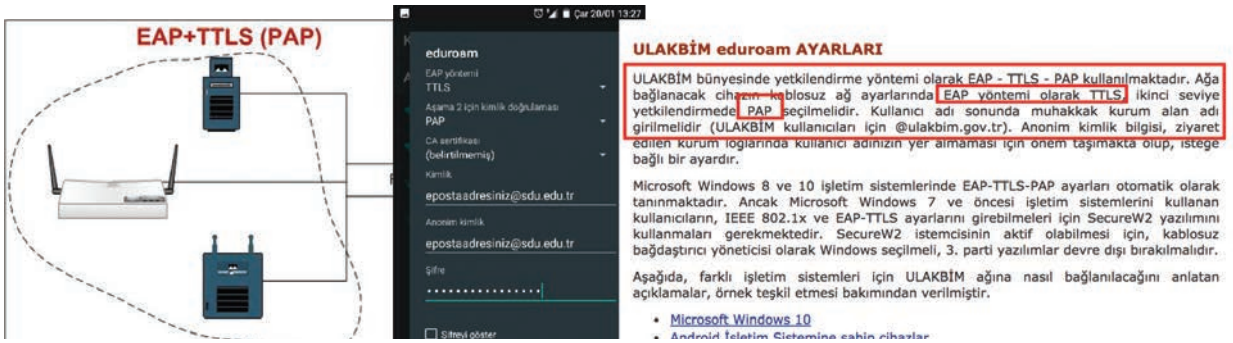


Şekil 2: https://pwn.no0.be/exploitation/wifi/wpa_enterprise/

- *Password Authentication Protocol (**PAP**)*
- *Challenge Handshake Authentication Protocol (**CHAP**)*
- *Microsoft CHAP (**MS-CHAP**)*
- *Microsoft CHAP version 2 (**MS-CHAP-V2**)*
- *EAP-MD5 Challenge (**EAP-MD5**)*
- *EAP-Generic Token Card (**EAP-GTC**)*

Problem?

Bu kadar yapı içerisinde Eduroam kullanan kişileri en çok zora sokan nokta EAP-TTLS ve Inner Authentication olarak PAP kullanmalarıdır. İşin daha korkunç yanı ULAKBİM sayfasında da böyle bir yönergenin olması… Aşağıda, üniversitelerin web sayfalarından alınan yönergelerin ekran görüntülerini paylaşıyorum.



Şekil 3: Üniversite ve ULAKBİM web sayfalarından örnek bağlantı yönergeleri

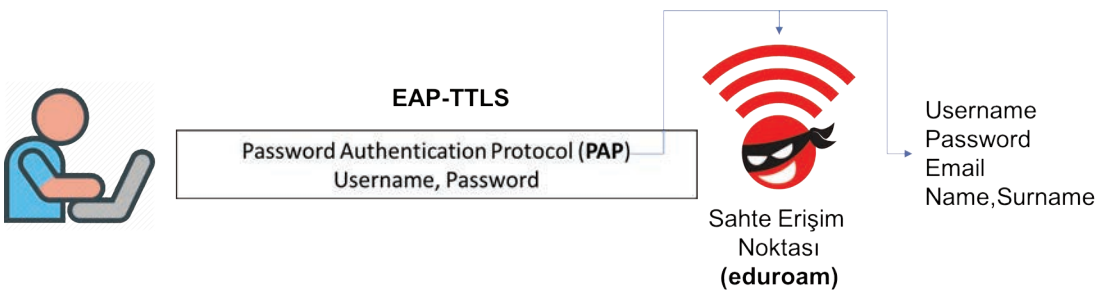
```
<false/>
<key>EncryptionType</key>
<string>WPA</string>
▼<dict>
  <key>TLSAllowTrustExceptions</key>
  <true/>
  <key>TTLSInnerAuthentication</key>
  <string>PAP</string>
  <key>EAPFASTUsePAC</key>
  <false/>
  <key>EAPFASTProvisionPAC</key>
  <false/>
  <key>EAPFASTProvisionPACAnonymously</key>
  <false/>
  <key>AcceptEAPTypes</key>
▼<array>
    <integer>21</integer>
  </array>
```

Şekil 4: Apple cihazlarına ait yapılandırma dosyaları

PAP (Password Authentication Protocol) incelendiğinde bilgileri açık bir şekilde ilettiğini RFC1334 standartlarından görebiliriz.

Ancak bu verileri doğrudan yakalamak mümkün değildir. Daha önce bahsettiğimiz üzere TLS tünelleme yöntemi ile bu veriler için güvenli bir kanal oluşturulmaktadır. Aslında **PAP (Password Authentication Protocol)** tarafındaki bu zafiyet bir nevi bu yöntemle giderilmiştir. Siz bir ağ kartını monitor mode durumuna alarak etrafı dinlemeye çalışırsanız, **clear-text** (açık metin) olarak bir veri göremeyeceksiniz.

Ancak bu verileri açık bir şekilde görmenin bir yolu var. Bu yöntem iletişimin bir ucunda olmaktır. **Point** to **Point**. İletişimin bir ucunda olmayı başaran bir saldırgan Eduroam ağına daha önce bağlanmış neredeyse herkesin kullanıcı adı, e-posta ve parola bilgisini açık bir şekilde elde edebilmektedir.



Üniversite öğrencilerinin yoğunlukta olduğu bir kafeye oturun ve **Eduroam** adında **Enterprise** bir sahte kablosuz ağ açın, sonuçlar **korkutucu!** Çünkü **e-posta, öğrenci numarası, kullanıcı adı ve parola gibi bilgileri** rahatlıkla görebileceksiniz.

İşte size korkunç bir parça örnek:

```
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: STA [redacted] IEEE 802.1X: Identity received from STA: '[redacted]@[redacted]tepe.edu.tr'
wlan0: STA d0:25:98:9b:7d:dd IEEE 802.11: disassociated
```

Kullanıcı adı, e-posta, üniversite ve parola bilgisinin elde edilmesi!

```
eap-ttls/pap: [redacted]
        username:       [redacted]8@metu.edu.tr
        password:       [redacted]
wlan0: CTRL-EVENT-EAP-FAILURE 10:7b:44:70:2e:e1
```

Oluşabilecek Tehlikeler

Oluşabilecek tehditleri sıralarken aslında sınırsız bir saldırı haritası çıkarmak mümkün. Ancak en ön planda olan birkaçını sıralamak istiyoruz:

1. Mahremiyet ortadan kalkıyor ve bu işi yapan biri başkalarının hesaplarına erişim sağlayabiliyor.
2. Başkalarının hesaplarına erişim sağlayan kişiler notlarını değiştirebilme şansına sahip olabilir.
3. Bir öğretim görevlisinin veya rektörün parola bilgisi elde edilirse, okuldaki herkese zararlı yazılım bulaştırılma ihtimali olabilir.
4. Öğretim görevlileri arasında bir kaos yaratabilir.
5. Eğer ele geçirilen parola başka alanlarda da kullanılıyorsa, kişinin diğer iletişim hesapları etkilenebilir.

Çözüm önerisi olarak bu konuda esas sorun teşkil eden noktayı PAP oluşturduğu için Inner Authentication yönteminde PAP kullanımından vazgeçilmelidir.

Eşref Erol - esreferol_aal@hotmail.com

O Gemi Bir Gün Hacklenecek

Deniz yolları, dünya ticaret taşımacılığının neredeyse yüzde 80-90 kadarını sırtında taşımaktadır. Tabii ki bu yolların en büyük unsurları gemiler. Peki bu gemiler bir şekilde hacklenebilir mi, hacklenirse ne olur? Ticari gemiler ve yolcu gemilerinde hacklenme olayı ciddi can kaybına ve maddi hasara yol açabilir mi? Bu soruların cevabını bu yazımızda mümkün olduğunca bulmaya çalışacağız.

Gemilerin hacklenmesi konusu son yıllarda dünyada gittikçe popülerleşen bir konu. Bu konuda dünya çapında konferanslar, seminerler düzenleniyor ve araştırmalar yayınlanıyor. Peki Türkiye'de durum nasıl? Türkiye'de maalesef yine dünyanın gündeminde olan fakat bizde sonradan hatırlanan çoğu konu gibi kuytu bir köşede araştırılmayı bekliyor. Güvenlik önlemleri konusunda da diğer ülkelerden ne kadar ileride ya da gerideyiz orasını maalesef tahmin edemiyorum.

Gerek ticaret yollarında kapladığı hacim gerekse son yıllarda artan kazalar, son olarak da Samsun açıklarında meydana gelen kazada yaşanan hadiseler bu konuda merakımın uyanmasına sebep oldu ve "*Acaba bir hacklenme olayının doğurduğu manipülasyon sonucu böyle olaylar olabilir mi?*" diye düşünmeye başladım. Sonrasında yaptığım araştırmalarda ise bir geminin ya da gemi ile ilgili çevre sistemlerin hacklenmesi ile patlama, çarpışma, yük dengesinden dolayı batma, hırsızlık ve güzergâh sapması gibi olayların olabileceğini öğrendim. Yani "*O gemi bir gün gelecek*." diye bekleyen bir arkadaşımızın hiç beklemediği bir anda karşısına normalde güzergahı farklı olan bir gemi çıkabilir.

Peki gemilerdeki ya da çevredeki hangi unsurlar bu hacklenme olayına sebebiyet verebilir gelin onları sıralayıp sonrasında incelememize başlayalım.

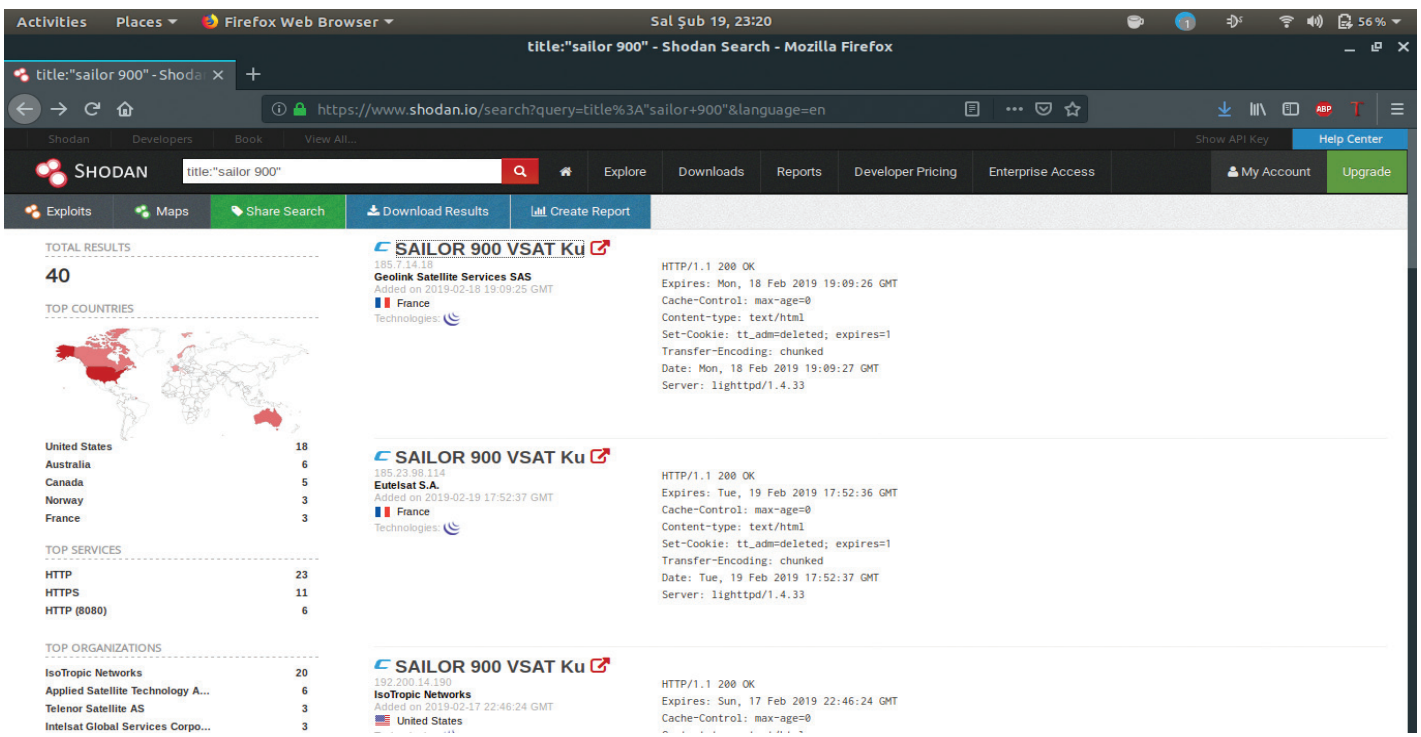
- İnsan Faktörü
- AIS Transponder
- ECDIS
- GPS
- Seri Ağlar
- EDIFACT Mesajları
- Deniz Uyduları
- VoIP Telsizler
- Otopilot
- BNWAS

Elimizden geldiğince, beraber bu unsurları ve oluşturdukları risk faktörlerini incelemeye çalışacağız. Teknik araç ve konulara geçmeden, öncelikle her sistemde olduğu gibi gemilerde de insan faktörünün ne gibi bir manipülasyona maruz kalabileceğinden bahsetmek istiyorum.

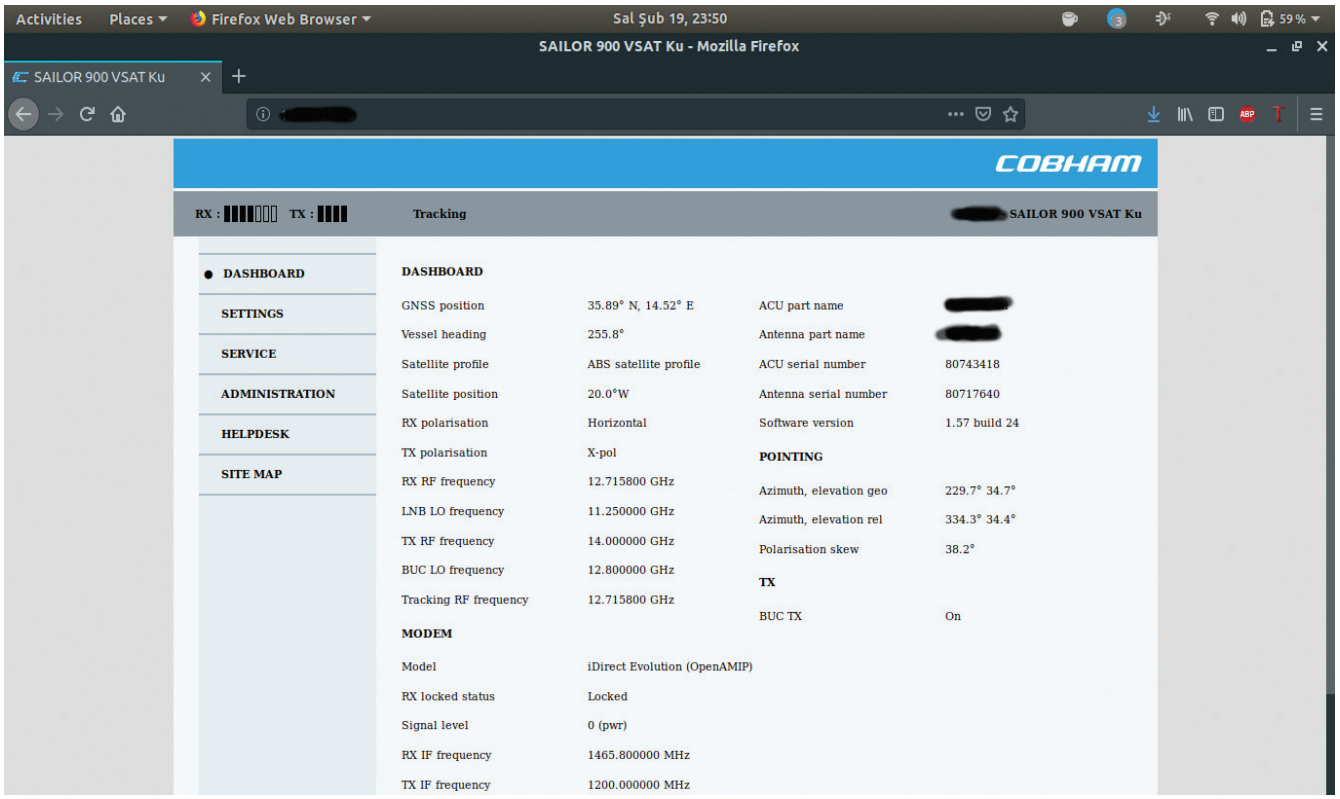
İnsan Faktörü ve Deniz Uyduları

İnsanlara dair bilgi toplama konusunda gerek kendi bloğumda gerekse internette bulabileceğiniz birçok kaynak bulunmakta. Fakat biz burada genel bilgi toplama unsurlarının dışında gemi ile alakalı aldığımız bilgileri nasıl kullanabiliriz buna değineceğiz. Bunun için de deniz uydularından faydalanacağız. Deniz için uydu alıcıları birçok şirket ve kuruluş tarafından üretilmektedir. Bunlardan en çok bilinen ve tercih edilenlere örnek olarak Cobham, KVH, Inmarsat Solutions, Telenor Satellite'i verebiliriz. Gelin kadim dostumuz olan Shodan'da biraz arama yapalım.

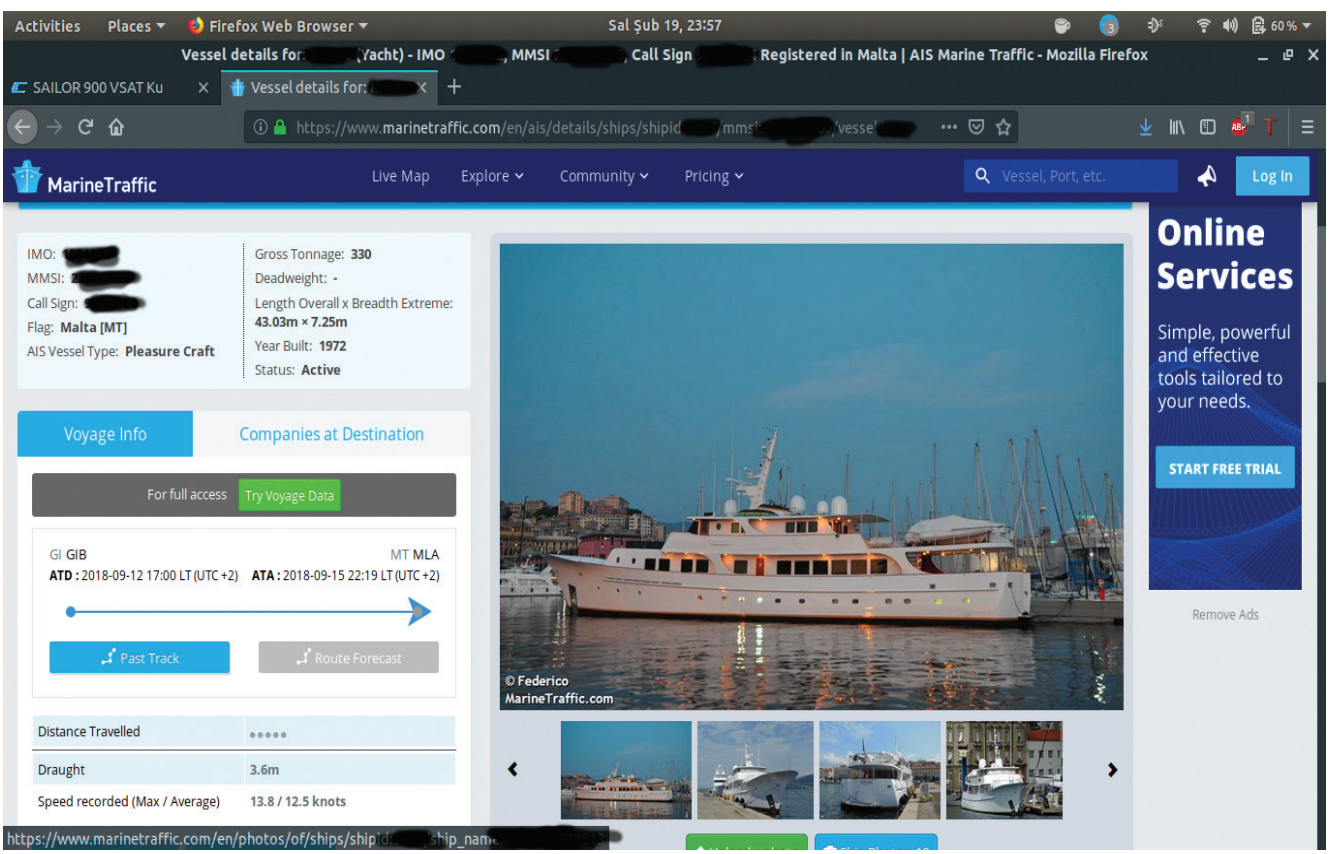
Shodan arama çubuğuna yukarıda belirttiğim şirketlerden birisi olan Cobham'ın Sailor 900 adlı uydu alıcısı için bir araştırma yaptığımızda karşımıza şöyle bir sonuç çıkıyor.



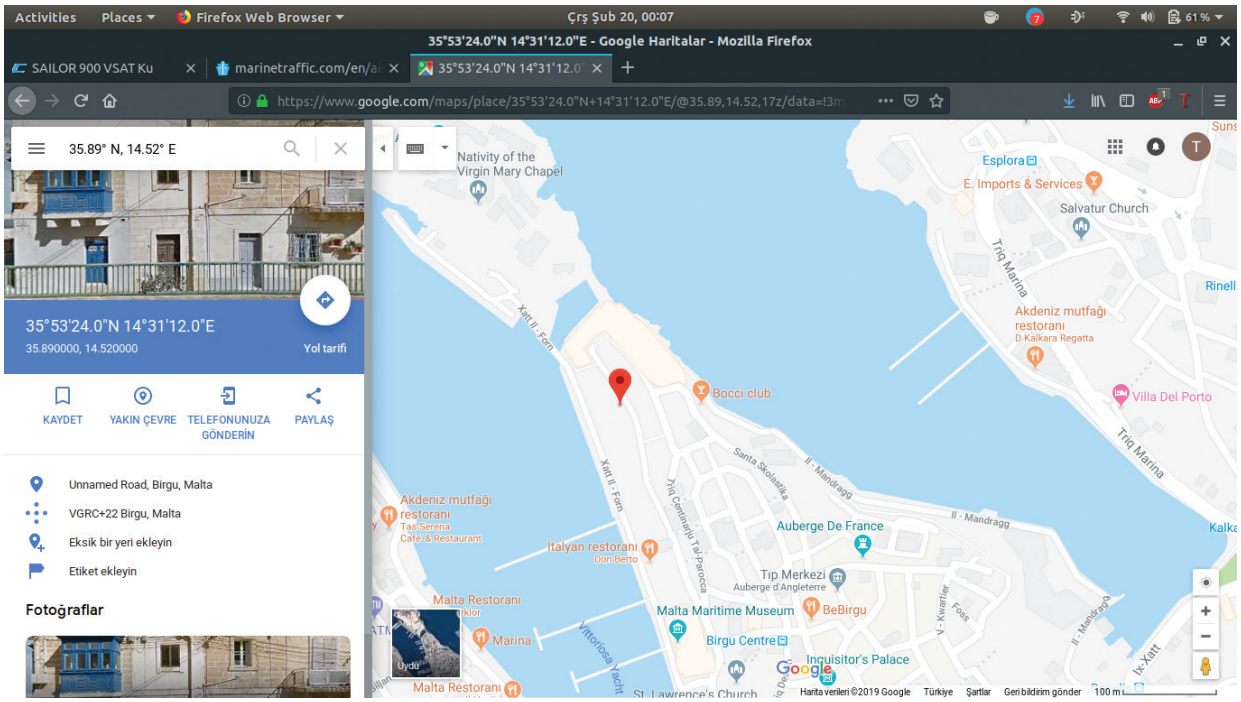
Karşımıza ilk çıkan sunucuya girelim bakalım bizi ne karşılayacak.



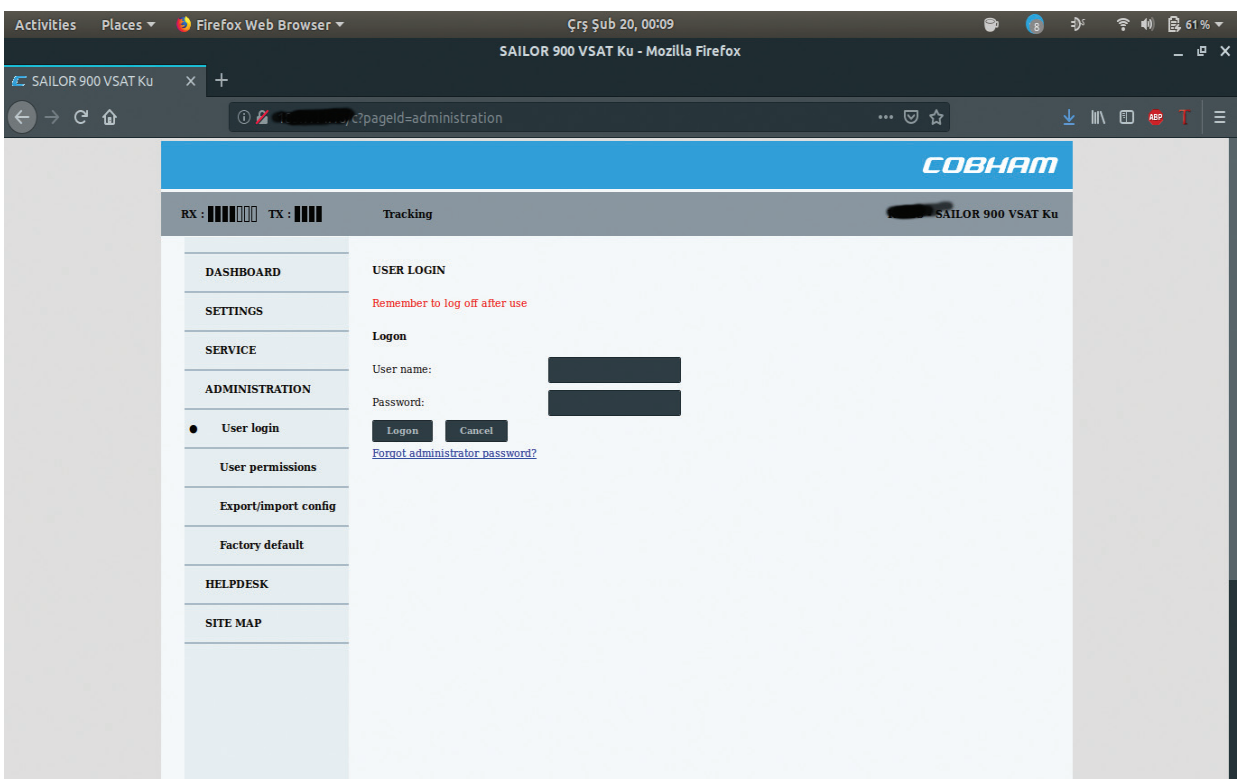
Karşımıza geminin ismi, konumu ve seyir hali gibi bilgiler çıktı. Gelin bu gemimizi bir de MarineTraffic'te arayalım.



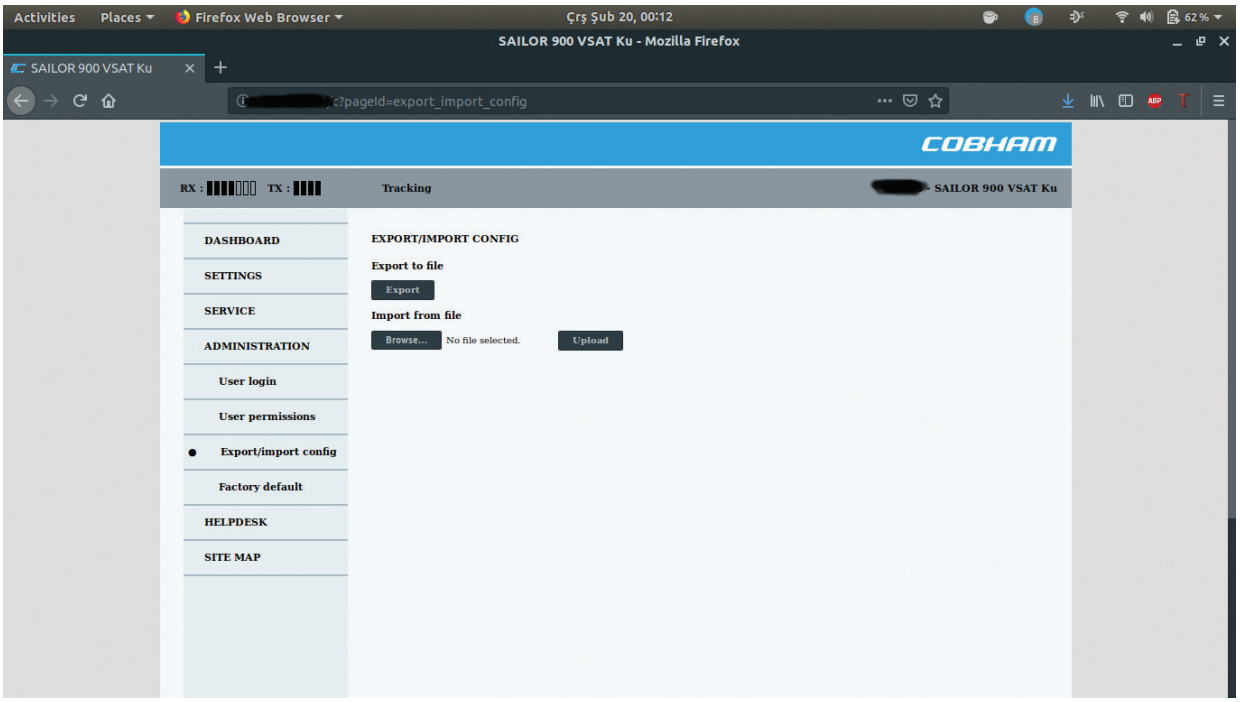
Karşımıza gayet güzel bir yat çıktı. Görsellere ek olarak yatın güzergahı, boyutu, çağrı numarası, konumu gibi birçok bilgi de bize sunuldu. Tüm bu bilgilere ek olarak bizim için daha kullanışlı olabilecek bilgilerden birisi olan yatın isminin tarihsel değişim süreci ve iletişim bilgileri de MarineTraffic'te mevcut. Dilerseniz konum bilgisi bizim kullandığımız uydu arayüzü ile eşleşiyor mu diye kontrol edebilirsiniz.



Şimdi gelin uydu arayüzümüze geri dönelim. Bakalım Administration kısmında neler yapabileceğiz.



Karşımıza çıkan panele kullanıcı adı ve parola olarak ilk iki denememde admin/admin ve admin/pass'ı denedim fakat sonuç başarılı olmadı. Sonrasında admin/1234 kombinasyonunu denedim ve başarılı bir şekilde panele giriş yaptım.

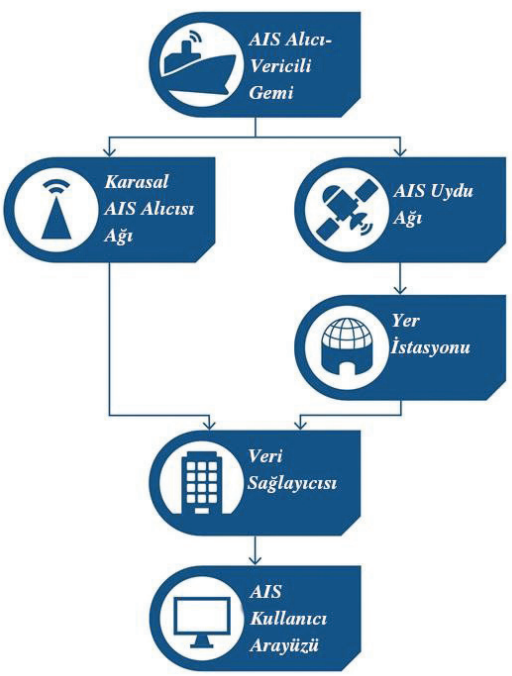


Ben şöyle bir ekran görüntüsü bırakayım gerisi hayal gücümüze kalsın. Burada dikkat çekmek istediğimiz nokta bu uyduların bir web arayüzüne sahip oldukları ve arayüzlerdeki yetkilendirme işleminde kullanılacak değerlerin varsayılan değerde bırakıldığıdır. Bilgi toplama kısmında biraz Shodan'ı kurcalar ve biraz da Instagram'ın konum tabanlı aramasından faydalanırsanız ilginç şeylere erişebileceksiniz. Hatta yazımızın ilerleyen kısımlarında değineceğimiz cihazların modellerine kadar içeren selfieler de bulunmakta fakat ben bunları burada paylaşmayıp sizin araştırma gücünüze bırakıyorum. Şimdi bu kısmı fazla uzatmadan diğer unsurlarımızı inceleyelim.

AIS Transponder

AIS (Automatic Identification System - Otomatik Tanımlama Sistemi) Nedir?

AIS deniz taşıtlarının izlenmesini sağlayan bir sistemdir. Sistem sayesinde çevredeki gemilerin rotası, hızı, konumu, ismi gibi bilgiler edinilebilir. AIS yayın yaparken VHF Deniz telsizi frekanslarını kullanır. Yayınının izlenebilmesi ve çözülmesi için AIS Receiver (Alıcı) ve AIS Transponder (Alıcı-Verici) gerekmektedir. AIS transponderlarda Tip A ve Tip B olmak üzere iki çeşit bulunmaktadır. A tipi transponderlar uluslararası ticaret gemilerinde kullanılırken B Tipi transponderlar daha küçük çaplı yük ve yolcu gemilerinde kullanılmaktadır. A tipindeki transponderların menzilleri B tipi transponderlara göre daha fazladır. A tipi transponderlarda menzil 15-20 deniz mili iken B tipi transponderlarda 5-10 deniz mili gibi bir mesafedir. Elbette ki menzil kullanılan antenlerin çok yönlü ya da tek yönlü olmasına bağlı olarak da değişebilmektedir.



AIS Manipülasyonu

Önemli şirketlerden birisi olan Trend Micro 2014 yılında "*A Security Evaluation of AIS*" adlı, AIS güvenliğine dair bir rapor yayımladı. Bu raporda AIS manipülasyonuna sebep olabilecek etkenler ve bunun nasıl gerçekleşeceği detaylı bir şekilde gözler önüne serildi. Buna ek olarak da örnek bir manipülasyon işlemi gerçekleştirildi. Bu rapora göre AIS manipülasyonunu doğurabilecek iki adet unsur bulunmakta. Bunlardan birincisi RF yani radyo frekansları, diğer unsur ise AIS yazılımı. Oluşabilecek tehditler ise üç ana kategoride sınıflandırılmış ve alt kategorilere bölünmüştür.

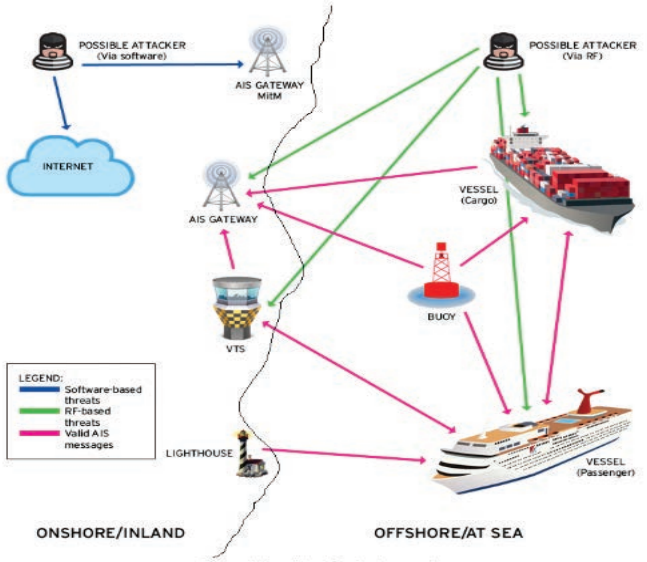
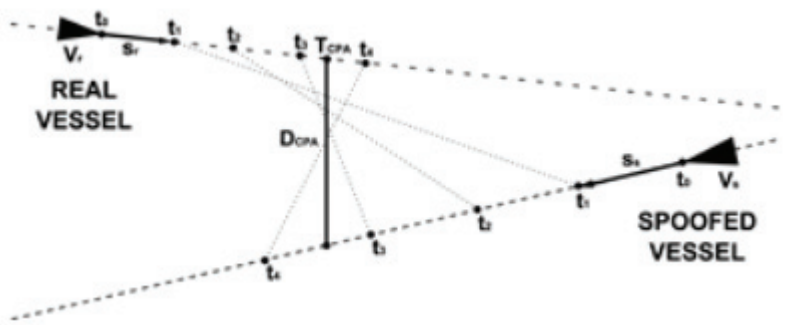


Figure 1: Possible AIS attack scenarios

Gelin bunları inceleyelim.

A) RF Tabanlı Tehditler:

1-CPA Spoofing:



Çarpışmadan kaçınmak AIS'de hedeflenen temel şeylerden birisidir ve AIS bir çarpışma tespit edildiğinde veya beklendiğinde otomatik olarak yanıt verir. CPA ise en az biri hareket halinde olan iki gemi arasındaki minimum mesafeyi hesaplayarak çalışır ve herhangi bir çarpışma tehdidinin olduğu durumlarda kaptana görsel ya da sesli olarak uyarı verecek bir şekilde yapılandırılabilir.

Yukarıda görmüş olduğunuz şema CPA'nın çalışma algoritmasını göstermekte. Şemada bulunan TCPA, CPA noktasına ulaşmadan önce kalan zamanı; DCPA, ise CPA noktasına ulaşmadan önce gemiler arasındaki mesafeyi gösterir. W(ti) ise herhangi bir t zamanında gemiler arasında kalan mesafeyi göstermektedir. Sr ve Ss ise gemilerin vektörleridir. Burada bahsi geçen D ve T parametrelerinden ikisinden birisinin CPA yapılandırılmasında baz alınan seviyelerinin altına inmesiyle CPA alarm verir. CPA spoofing ise bir gemiyle olası bir çarpışmayı varmış gibi göstermeyi içerir. Bu durum CPA alarmını tetikler bu durumda sığ sularda bir kayaya çarpmaya ya da karaya oturmaya neden olabilir.

2)AIS-SART Spoofing

SART'ın Türkçe karşılığı "*Arama ve Kurtarma Alıcı-Vericisi*"dir. Acil durumda bulunan bir geminin çevresindeki gemilerin radarlarına sinyal gönderilerek kendi yerinin tespitinin sağlanmasını amaçlayan bir aktif radar reflektörüdür. Cihaz acil durum botlarında ya da kişilerde bulunabilir.

SART spoofing ise saldırganlar tarafından belirlenmiş koordinatlarda sahte tehlike işaretleri oluşturma mantığı ile çalışır. Amaç, hedef gemiyi kendi istedikleri koordinata getirmektir ve gemilerin yasaya göre, bir SAR mesajı aldıklarında kurtarma operasyonuna katılmaları zorunludur.

2) Sahte Hava Tahminleri

AIS konum bilgileri gibi verilere ek olarak akımlar ve hava durumu gibi çevre koşulları hakkında da bilgi verir. Sahte hava durumu bilgisi sunmanın amacı fırtınalı bir günü güneşli bir günmüş gibi göstermek olabilir.

3) Slot Starvation

Bu saldırıyı örnek verecek olursak DHCP Starvation saldırısı gibi düşünebilirsiniz. Saldırıdaki amaç kapsama alanı dahilindeki istasyonların birbirleriyle iletişim kurmalarını engellemektir. Bu istasyonlar, trafik izlemede kullanılan gemileri, AtoN'ları (Aids to Navigation) yani deniz feneri gibi yön bulma yardımcılarının AIS'de belirtilmesini sağlayan cihazları ve AIS ağ geçitlerini içerir. Sonuç olarak saldırganlar AIS'i büyük ölçüde devre dışı bırakabilirler.

4) Frekans Atlaması (Frequency Hopping)

Saldırganlar denizcilik makamlarını taklit ederek, bir veya daha fazla AIS transponder'ına üzerinde çalıştıkları frekansları değiştirme talimatını verir ve böylece farklı frekans yayınıyla AIS'in devre dışı kalmasını sağlarlar. Alıcı istasyonların denizcilik makamlarının verdiği talimatları uygulaması zorunlu olduğundan da bu tür saldırılar hâlâ devam etmektedir. Sistemin yeniden başlatılması ise bu sorunu çözmemektedir çünkü frekanslar sadece yetkili denizcilik makamından bir talimat geldiğinde değiştirilmektedir.

5) Zamanlama Saldırıları

Saldırganlar komutları yenileyerek, transponder'lara iletim sürelerini geciktirmelerini söyleyebilir ve böylece gemilerin konumlarıyla ilgili bilginin aktarımını engelleyebilirler. Bu durum da gemilerin AIS radarlarından kaybolmasına sebep olur. Ayrıca saldırganlar iletim süresinin geciktirilmesinin tam tersi bir şekilde, sürekli konum bilgisi gönderimini ve çok sık durum bilgisi güncellemesinin yapılmasını sağlayarak deniz trafiğinin aşırı yüklenmesine sebep olabilirler.

B) Yazılım ve RF Tabanlı Saldırılar:

1) Ship Spoofing

Bu durum gerçekte olmayan bir geminin varmış gibi gösterilmesini ifade eder. Gemi ismi, hızı, varış yeri, rotası, bayrağı gibi bilgiler sahte bir gemi için oluşturulur.

2) AtoN Spoofing

AtoN'lar kanallar veya limanlar boyunca gemi trafiği yönetimine yardımcı olmak amacıyla kullanılırlar ya da açık denizdeki tehlikeler, sığ sular, kayalık çıkıntılar hakkında kaptanı uyarırlar. AtoN sahtekarlığı gemilere manevra yaptırmak için sahte veriler üretme sürecine dayanır. Sahte şamandıralar vb. uyarıcılar kullanılarak, ayrıca senaryoya Ship Spoofing de eklenerek değişik senaryolar oluşturulabilir.

3) AIS Hijacking

AIS Hijacking, mevcut AIS istasyonları hakkında herhangi bir bilgiyi değiştirmeyi içerir. Saldırganlar AtoN'lar hakkındaki verileri değiştirebilir. Hijacking'in yazılım kısmında ise saldırganlar devam eden haberleşme sürecini dinleyebilir (MITM saldırıları) ve AIS bilgisini değiştirebilirler. RF kısmında ise daha yüksek frekanslı mesajlar yollayarak AIS mesajlarını geçersiz kılabilirler.

C) **Yazılım Tabanlı Saldırılar**

Saldırılara geçmeden önce AIVDM hakkında biraz bilgi verelim. AIS'in uygulama katmanında kullandığı protokol AIVDM olarak geçer. AIVDM her biri kendisine özgü amaçlar barındıran 27 tip mesaj türüne sahiptir.

Category	Message	Description
Standard	1	Scheduled position report (class A)
	2	Assigned position report (class A)
	3	Special position report (class A)
	5	Static report (class A)
	9	SAR aircraft position report
	18	Position report (class B)
	19	Extended position report (class B)
	24	Static report (classB)
	27	Long range position report
AToN	21	AToN report
Timing	4	Base station report
	10	UTC inquiry
	11	UTC response
Safety	12	Addressed text message
	13	Acknowledgment
	14	Broadcast text message
Binary	6	Addressed binary
	7	Binary acknowledgment
	8	Broadcast binary
	17	GNSS update
	25	Short binary (no acknowledgement)
	26	Binary with communications state
Other	15	Interrogation for specific messages
	16	Assignment mode command
	20	Data link management
	22	Channel management
	23	Group assignment command

AIVDM iki katmanlı bir protokoldür. Dış katman, navigasyon sistemleri arasındaki veri alışverişini için eski bir standart olan NMEA 0183'ün bir varyantıdır.

Yazılım tabanlı saldırılar için incelemelerde bulunan Trend Micro, raporunda 3 adet büyük AIS sağlayıcısı olan MarineTraffic.com, AIS Hub ve Vessel Finder'ı hedef almış. Yaptıkları analizlerde öncelikle sağlayıcıların kaynaklarını kontrol etmedikleri, gelen mesajların gerçekten gönderen gemilerden gelip gelmediğini incelemedikleri sonucuna varmışlar. Ayrıca AIVDM'de gönderen kimliğini doğrulamak için bir yol olmadığı ve bunun da *spoofing* ve MiTM gibi saldırılara sebep verdiğini belirten araştırmacılar bunun için de kendileri örnek bir senaryo gerçekleştirmişler.

Öncelikle bir AIVDM encoder kullanarak sahte AIVDM mesajları oluşturulmuş ve bu mesajlar AtoN raporları için olan 21 ve şamandıralar için olan 13 tipindeki mesajlarmış. Sonrasında ise demir atmış bir gemi için sahte bir rapor oluşturup bunu mail yolu ile AIS sağlayıcısına göndermişler.

```
To: report@marinetraffic.com

MMSI=247320161
LAT=44.3522
LON=8.5665
SPEED=0
COURSE=243
TIMESTAMP=2013-11-11 13:11
```

Son olarak da Akdeniz'de PWNED kelimesinden oluşan güzergahta giden bir geminin varlığını gösteren bir veri akışı oluşturacak şekilde AIS istasyonuna sahte veriler yollayacak bir betik hazırlamışlar ve bu üç deney de başarılı olmuş.

AIS ile ilgili incelememizi yaptığımıza göre gelin bir de AIS'in entegre kullanıldığı ECDIS'e bir göz atalım.

ECDIS

ECDIS (Electronic Chart Display and Information System - Elektronik Harita Gösterim ve Bilgi Sistemi) Nedir?

ECDIS, kâğıt üzerindeki haritalara alternatif olarak kullanılabilen bir deniz haritası sistemidir. Tek başına harita görüntülemesi işlevi için kullanılabildiği gibi GPS, AIS, radar benzeri ek seyir sistemlerinin sensörleri ile de entegre bir şekilde kullanılabilmektedir ki çoğunlukta kullanımı bu şekildedir. ECDIS bu işlemi gerçekleştirirken iki tip veri kullanmaktadır. Bunlar ENC (ESH) ve RNC (RSH)'dir. Bizim yazımızda daha çok üzerinde duracağımız kısım bu veri tipleri hakkında olacak. Gelin ENC ve RNC neymiş bir inceleyelim.

RNC: RNC'ler kâğıt üzerinde bulunan haritaların taranarak

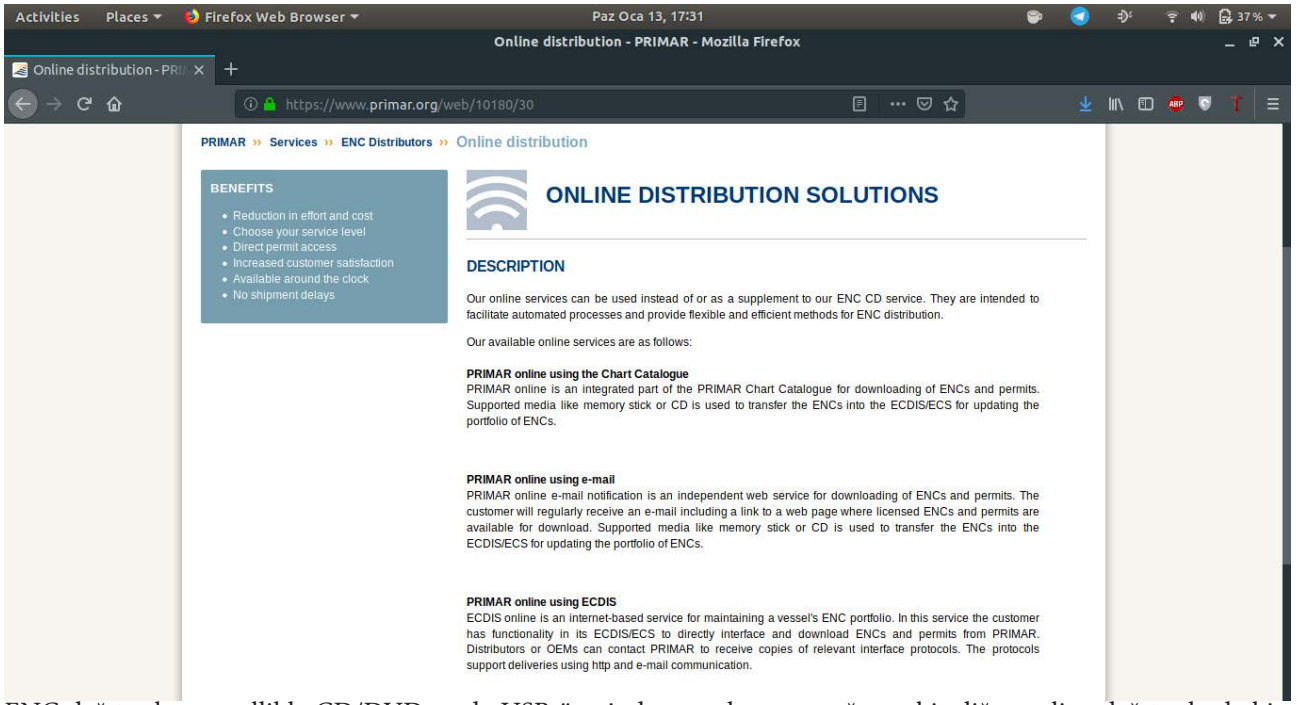
dijitale aktarılmış halleridir. ENC'lerin tahsis edilemediği durumlarda ECDIS tarafından kullanılabilmektedirler.

ENC: ENC'ler ise dijital ortamda hazırlanmış vektörel çizimlerdir ve ECDIS'lerin asıl veri kaynağını oluştururlar. ENC'ler Uluslararası Hidrografi Örgütü'nün (IHO) belirlemiş olduğu standartlara göre hazırlanır ve kullanıma sunulur. ENC'lerin dağıtımı konusunda ise RENC'ler devreye girmektedir. Günümüzde iki adet RENC bulunmaktadır ve bu kurumlar birbirleri ile entegre şekilde çalışmaktadır. Bunlardan bir tanesi İngiltere'de bulunan IC-ENC bir diğeri ise Norveç'te bulunan Primar-Stavanger'dir. Bu kurumlar kendilerine bağlı olan ENC üreticilerinden aldıkları ENC'leri kendisine bağlı olan dağıtıcılara göndermektedirler. Burada üreticilerden kastımız ise aslında ülkelerdir. Örneğin IC-ENC'de şu an üretici olarak aralarında Türkiye'nin de bulunduğu 43 adet ülke bulunmaktadır. Dağıtıcıları incelediğimiz zaman ise aşağıda ki görselde bulunan 7 adet kuruluşu görmekteyiz.

AVCS ADMIRALTY Vector Chart Service · ChartCo · ChartWorld Navigation Experts · C-MAP · DATEMA NAUTICAL SAFETY · NAVTOR · PRIMAR®

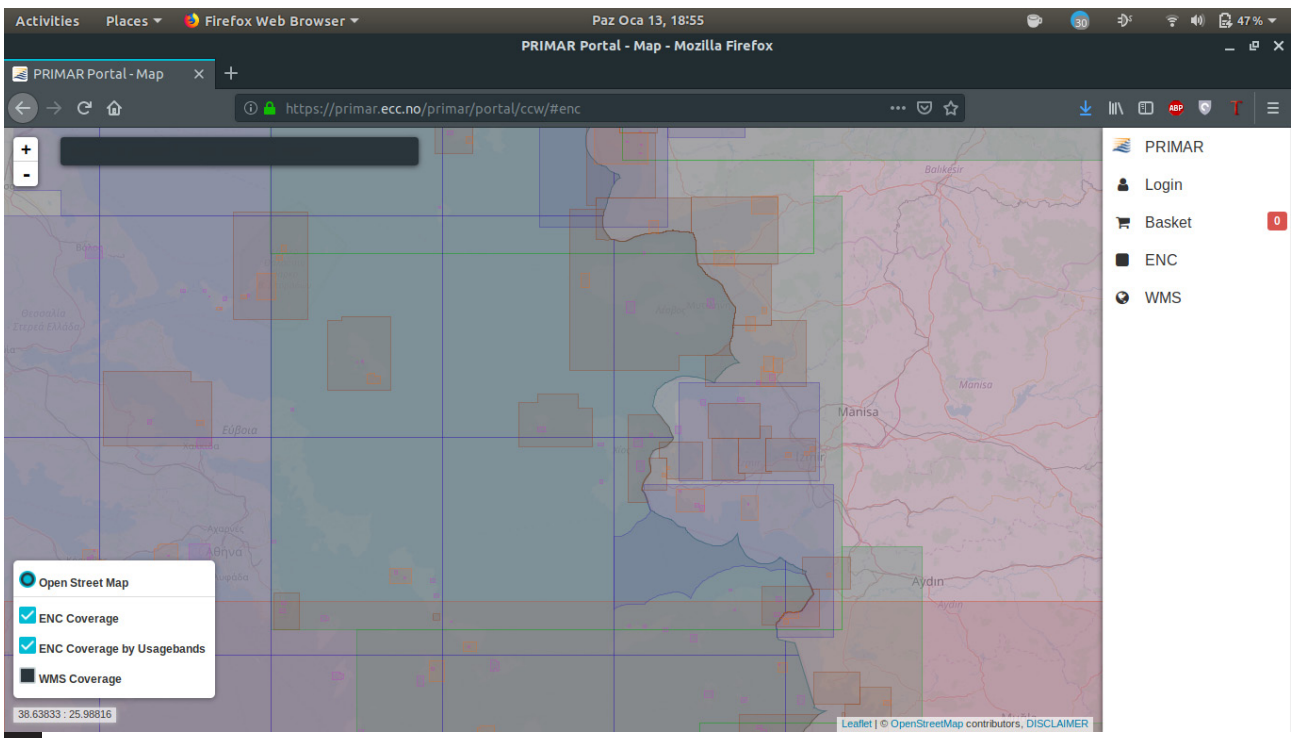
ENC'lerin Dağıtımı

Bu sistemde başlı başına bir risk faktörü oluşturan unsur ise ENC'lerin dağıtımı. Günümüzde internet bağlantısı üzerinden ENC dağıtımı alan gemiler bulunmakta. Örneğin dağıtıcılardan birisi olan Primar'ı incelediğimiz zaman online olarak ECDIS'e ENC sağlama imkânı sağladığını görebiliriz. Peki bu online dağıtım güvenlik açısından ne gibi bir problem doğurabilir?



ENC dağıtımları genellikle CD/DVD ya da USB üzerinden yapılmasına rağmen bir diğer online dağıtımlarda bir web uygulaması kullanılmakta ve örneğin Primar'ın kendi sitesinde belirttiğine göre veri aktarımı yapılırken HTTP ve e-mail'den faydalanılmakta. Cümleyi okurken HTTP'yi gören okuyucularımızın gözlerinin parladığını görür gibiyim. Eğer geminin ağına dahil olunulursa yapılacak bir "Ortadaki Adam" (MiTM) saldırısında ENC sağlanması ya da güncelleme gelmesi durumunda sağlayıcı olarak Primar'ın servisinin değil de saldırganlar tarafından oluşturulmuş bir servisten sağlanan yine saldırganlar tarafından derlenmiş bir ENC'nin ECDIS sistemine dahil edilmesi güvenlik açısından büyük bir sorun yaratacaktır. Bunun tam tersi yönde bir aktivite olarak ECDIS üzerinden internete çıkılıp yanlış yapılandırılmış bir ENC'nin ya da başka bir yazılım güncelleştirmesinin yüklenmesi de aynı şekilde büyük bir risk faktörü olacaktır. Web arayüzüne bir örnek olarak Primar'ın aşağıdaki bağlantısını inceleyebilirsiniz.

https://primar.ecc.no/primar/portal/ccw



Bu konuda ENC'lerde güvenliği sağlamak açısından ENC'ler kopyalanmasın ve yasadışı olarak dağıtılmasın diye IHO'nun belirlediği S-63 standartına göre şifreleniyor. Standarta göre veri transferinde kullanılan veritabanı Blowfish algoritmasına göre şifreleniyor ve verilerin SHA1 ile özeti (hash) alınıyor, buna ek olarak CRC32 kontrol sistemi olaya dahil ediliyor. Yine aynı standart baz alınarak kullanıcıların şifreli veriyi çözmesi ve kullanabilmesi için DSA formatında imzalar tanımlanıyor ancak standart maalesef ECDIS üreticileri tarafından çok zayıf bir şekilde uygulanıyor.

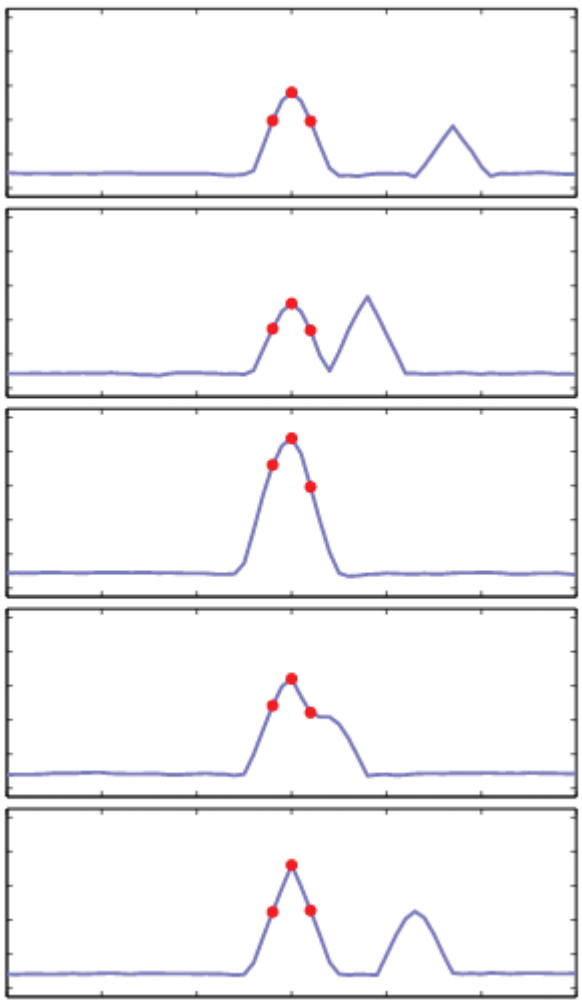
ECDIS İçin Risk Faktörleri

- ENC dağıtımı için kullanılan CD/DVD ya da USB bellek gibi araçlarda zararlı yazılım barındırılabilmesi ki burada insan faktörü ciddi anlamda ön plana çıkıyor. Bu yolla direkt olarak zararlı yazılım yüklenmese bile aracı olarak ağa bağlanılıp oradan bir indirme ve çalıştırma işlemi ya da hatalı bir yazılım güncelleştirmesi yükleme işlemi gerçekleşebilir.
- Online olarak gerçekleştirilen ENC dağıtımlarında ENC'nin çalınma ya da değiştirilmesi.
- Sensörlerden gelen verilerin alınması ve ECDIS'e yanlış tanıtılması.
- ECDIS üzerinden internete çıkılarak LAN'da bulunan diğer cihazlara, Wi-Fi erişim noktalarına, diğer bilgisayarlara ya da ağlara erişim sağlanabilmesi.

Şimdi sırada ECDIS'e de entegre olarak kullanılabilen bir diğer unsur olan GPS var gelin biraz da onun hakkında konuşalım.

GPS Spoofing

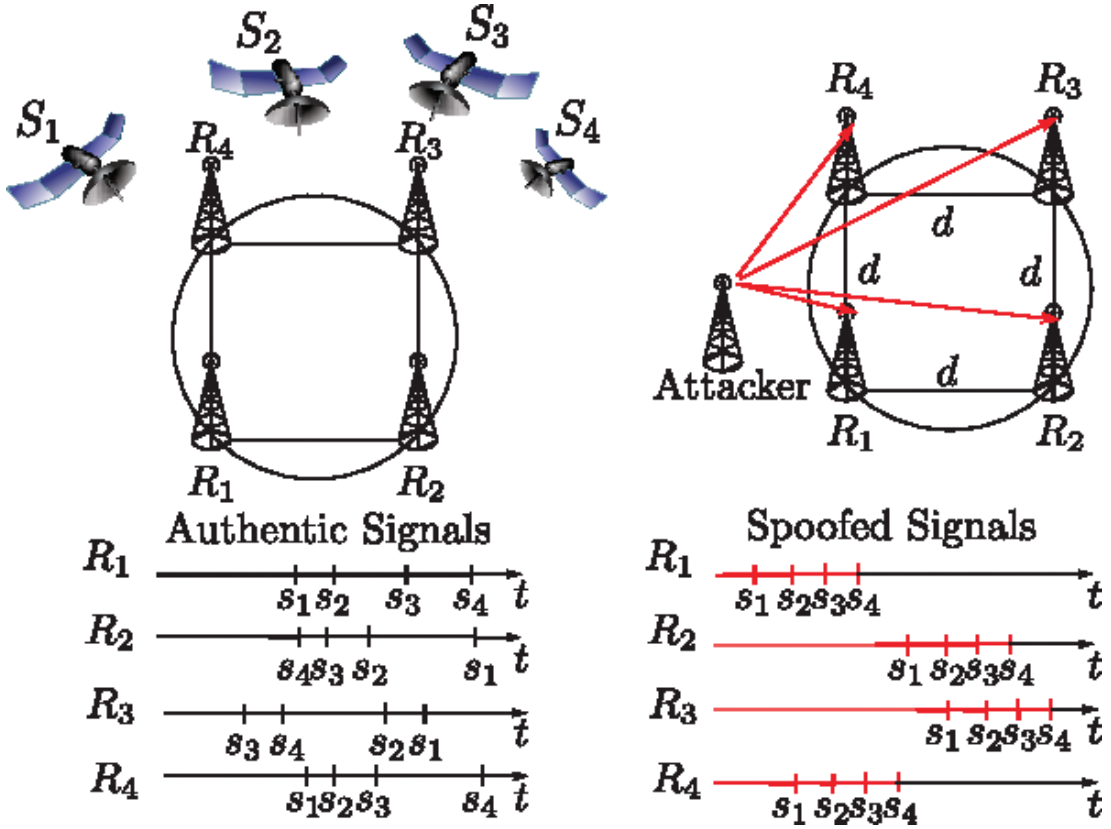
GPS spoofing son yıllarda oldukça popüler konulardan birisi oldu. Amerikan ordusuna ait olan iki adet devriye botunun İran karasularına girmesi ve 2017 yılında Karadeniz'de yirmiye yakın geminin güzergahlarından sapması vb. birçok vaka GPS spoofing'i dünya çapında gündem haline getirmişti.



Tek kanala yapılan başarılı bir GPS Spoofing Saldırısı

GPS spoofing saldırılarının temelinde hedef sisteme gerçek birer GPS sinyaliymiş gibi sahte GPS sinyalleri göndermek ya da önceden kaydedilmiş gerçek GPS sinyallerini sonrasında göndermek yatmaktadır. Genelde saldırıda başlangıç olarak hedefin normalde aldığı sinyallerden çok fazla farklı olmayan sinyaller kullanılır ve sonrasında git gide sahte sinyallerin gücü arttırılır ve cihaz bu sinyallere bağlı kalır.

Önceden var olan bir sinyalin kaydıyla gerçekleşen saldırılarda USRP B210 gibi donanımlar sinyal kaydında kullanılırken sinyalin tekrar yayınlanması için de bladeRF gibi donanımlar kullanılmaktadır.



Eğer sinyalinizi önceden kaydetmek yerine kendiniz oluşturmak istiyorsanız da öncelikle simülasyon için kullanacağınız parametreleri ve yörüngeyi belirlemeniz gerekiyor. Sonrasında ise GNSS Signal Architect gibi bir yazılımla IQ veri dosyasını oluşturuyorsunuz. Ardından oluşturduğunuz IQ veri dosyasını USRP N210 gibi bir cihaza radyo frekansı şeklinde yayınlamak için gönderiyorsunuz. Tabii anlattığım bu konu bu kadar kolay değil. Teknik birçok ayrıntısı bulunmakta. Fakat kaydedilen gerçek bir sinyalin sonrasında kullanımı bir tık daha basit ve daha yaygındır.

GPS spoofing dedik fakat bu GPS verilerinin GPS anteninden bilgisayar ekranına aktarımını da konuşmazsak olmaz.

Seri Ağlar

Gemiler tipik olarak 2 çeşit ağa sahiptir. Bunlardan birincisi IP/Ethernet ağıdır ve sektörel sistemler, mürettebatın mailleri, web servisleri için kullanılır. İkincisi ise "Seri Ağlar"dır ve dümen, motor itme gücü, denge ve navigasyonu içeren operasyonel teknolojiler (OT) için kullanılır.

Seri Ağ Nedir?

Seri ağ, verinin seri bir şekilde yani bir veri içerisindeki bitlerin aynı hat üzerinden art arda yollandığı iletişim şekli olan seri iletişimin kullanıldığı ağdır. Bu iletişim tipinde sık kullanılan iki adet standart bulunmaktadır. Bunlardan birincisi RS-232 diğeri RS-485'dir.

Seri Ağları Nasıl Hacklenir?

Peki biz gemideki bir seri ağa nasıl bağlanabiliriz? IP ağı ile seri ağlar arasında geçiş için köprü noktaları bulunmaktadır. Seri ağa bağlanabilmek ağdaki hangi cihazın seri ağ ve IP ağı arasında bir köprüye sahip olduğunu bulmanız gerekmektedir. Bunun için de birçok örnek cihaz gemilerde bulunmaktadır. Bunlara ECDIS, AIS Transponder, seri-IP dönüştürücülerini örnek olarak verebiliriz.

Dönüştürücüleri Sömürmek

Moxa, Perle ve bunlar gibi diğer dönüştürücüler IP/Ethernet ağı kabloları ile seri veri göndermek için kullanılırlar. Bu dönüştürücüleri sömürmek için üç adet yol gösterebiliriz.

1) Varsayılan Dönüştürücü Parolaları

Dönüştürücüler genelde yapılandırma yapabilmek için birer web arayüzüne sahiptirler. Bu arayüzleri için gerekli olan bilgiler de genelde dönüştürücü üreticilerinin kendi web sitelerinde yayınladıkları varsayılan kullanıcı adı ve parolalardır.

2) Sömürülebilir Dönüştürücüler

Bazı Moxa dönüştürücüler için exploitler geliştirilmiştir. Buna örnek olarak CVE-2016-9361 açığına geliştirilen metasploit modüllerini verebiliriz. Bu modüller sayesinde saldırganlar admin parolasını kurtarma işlemi yaparak kendileri belirleyebilir ya da öğrenebilirler.

3) Ortadaki Adam Saldırıları

Örneğin GPS'den gelen veri akışına bu saldırı yapılabilir. Ağ üzerine yapılacak bir ARP Poisoning saldırısı ile seri ağın saldırganın bilgisayarı üzerinden yönlendirilmesinin yapılması sağlanabilir.

İletişime değinmişken gelin bir de limanla gemi arasındaki iletişime değinelim.

EDIFACT Mesajları

EDI Nedir?

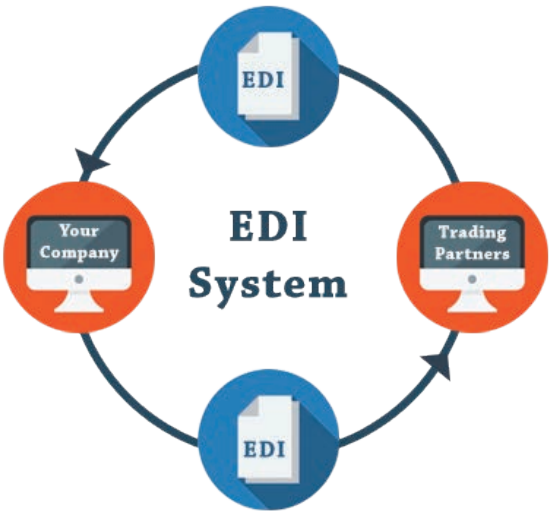
EDI (Electronic Data Interchange) Türkçe karşılık olarak "Elektronik Veri Değişimi" anlamını taşımaktadır fakat bizim ilgilendiğimiz kısmı elbette çevirisi değil. EDI, işletmeler arasında iletilecek olan ticari belgelerin elektronik ortamda iletimini sağlayan, bu belgelerin ve verilerin iletimindeki hız, güvenlik ve kontrolün sağlanması için oluşturulan standartlar bütünüdür. Bu sistem, ticaretin olduğu neredeyse her sektörde ve hatta ticaret dışı veri uygulamalarında da kullanılmaktadır. Şimdiye kadar standartlar dedik fakat bu standartlar neler?

EDI kavramı ortaya çıktıktan sonra bu konuda ileri sürülen birçok standart ortaya çıktı. Bunlardan en çok bilinenleri Kuzey Amerika'ya ait olan ANSI X12 ve BM'ye ait olan UN/EDIFACT standartları. Bu standartlar veri iletiminin kapsamı ve yöntemini içinde barındırmakta.

EDI Nasıl Çalışır?

EDI'nin çalışmasında dört adet ana unsur bulunmakta, bunlar: Standart, veri dönüşümü, haritalama, iletişim.

Gelin bu unsurları inceleyelim.



1) Standart

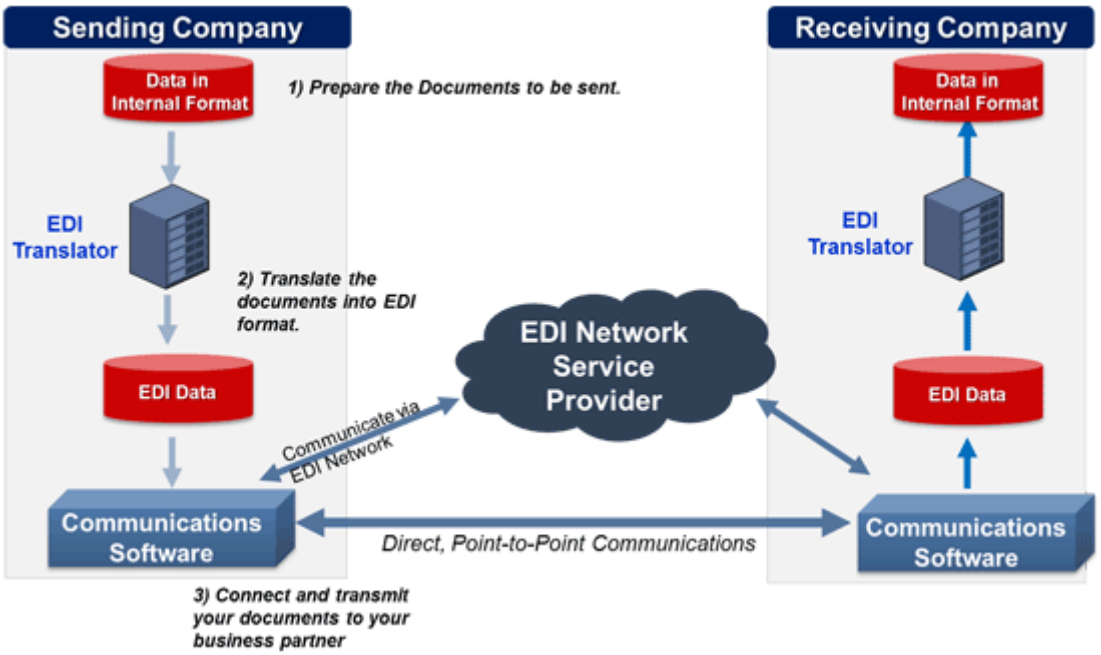
EDIFACT, X12, AIAG gibi oluşturulmuş olan kural setleri bütünüdür. EDI'nin hangi standarda uygun olarak kullanılacağı bu aşamada belirlenir.

2) Veri Dönüşümü

Herhangi bir işleme tabi tutulmamış dökümanın EDI formatına ya da EDI formatındaki bir dökümanın okunabilir hale dönüştürülmesi işlemidir. Dönüştürme işlemi EDI dönüştürücüsü ile EDI standartlarına göre yapılır.

3) Haritalama

EDI formatına dönüştürülen verinin .TXT, .XML gibi ortamlarda kullanımı daha kolay olan veri tipine dönüştürülmesidir.



4) İletişim

Bu aşama hedefe iletim tipinin belirlendiği aşamadır. Bunun için iki seçenek mevcuttur bunlardan birisi VAN (Katma Değerli Ağ) diğeri ise doğrudan iletişimdir. Bu iletişim seçeneklerinden VAN için özelleştirilmiş ağ iletişim havuzu diyebiliriz. Bu havuzlar işletmelerin iletişim için kurdukları ağlardır. Doğrudan iletişimde FTP(S), HTTP(S), SMTP, AS2 gibi iletişim protokolleri kullanılmaktadır.

EDIFACT Mesajları Nasıl Bir Risk Oluşturur?

Burada EDIFACT mesajlarının gemilerin hacklenmesi ve risk durumu teşkil etmesiyle ilgili kafanızda soru işaretleri oluşmuş olabilir. Şimdi o soru işaretlerini gidermeye çalışalım. EDI birçok sektörde kullanıldığı gibi limanlarda da yaygın bir şekilde kullanılmaktadır. Gemilere yüklenecek yüklerin cinsinden konumuna, yüklerin faturalarına ve diğer özel bilgilere, geminin yük dengesine kadar birçok veri bu mesajların içerisinde barınmaktadır. Bu bilgiler de BAPLIE olarak nitelendirilen mesaj grubuna dairdir. Manipülasyonlar bu gruba yapılmaktadır.

```
UNB+UNOB:1+PARTNER_ID:ZZ+0038977332:01:MFGB+020331:1230+00000000000001++INVOIC++++1'
UNH+0001+INVOIC:S:93A:UN'
BGM+380+INVOICE-NBR+9'
DTM+137:20000101:102'
RFF+ON:CUST_ORDER_NO'
NAD+RE+  ::92++MANUFACTURER NAME'
RFF+VA:DE12931720 6'
CTA+AR+:JANE DOE'
COM+00 49 89 9933-2543:TE'
NAD+ST+  ::92++COMPAQ COMPUTER CORP.'
NAD+BY+  ::92++COMPAQ COMPUTER CORP.'
CUX+2:USD:4'
ALC+C++6++ABG'
PCD+1:2.5'
MOA+204:200.00'
LIN+1+10+240152:AB'
QTY+47:3.00:EA'
PRI+AAA:1310.00:CT'
UNS+S'
MOA+77:4378.28:USD'
TAX+7+VAT+++:::15+S'
MOA+176:248.28:USD'
UNT+22+0001'
UNZ+1+00000000000001'
```

Yani bu mesajların manipülasyonu ile bir gemi batırılabilir, patlatılabilir veya gemiden yüklenen yükler çalınabilir. Burada gemilerde olası bir patlamaya, yangına sebep olabilecek bir manipülasyonu örnek olarak göstermeye çalışacağım. Bunun için SMDG'nin kendisinin yayınladığı kod tablosundaki örneklerden faydalanacağız.

Tablonun tamamına kaynakçadan ulaşabilirsiniz.

SMDG

v201501 (January 2015)

SMDG code lists for ATT segment in DGS group
(this sheet contains the definition of 4 code lists)

ATTRIBUTE TYPE (composite C955)
codes to be used in C955.9021

SMDG DG Attribute Types List
DE 1131 = DGATT
Example: ATT+26+UNX:DGATT:306+0403:CVL:399'

Code	Name	Description	last change	valid from	valid before
AGR	Aggregate State	Aggregate state of a hazardous substance		2013-09-30	
BNR	DG booking reference number	DG item's booking reference		2013-09-30	
PSN	Proper Shipping Name	Proper shipping name as defined by IMDG Code		2013-09-30	
HAZ	Special Hazard	Identification of a special hazard		2013-09-30	
QTY	Special Quantity	being applied		2013-09-30	
SEG	Segregation Group	Segregation group as defined by IMDG Code		2013-09-30	
TNM	Technical Name	Technical name, if different from propper shipping name		2013-09-30	
UNX	UN-number extended information	Code as generated by Exis Ltd.		2013-09-30	

ATTRIBUTE DETAIL (composite C956)
codes to be used in C956.9019

Şimdi örnek bir mesajı inceleyelim.

ATT+26+AGR:DGATT:306+G:DGAGR:306'

Nitelik Tipi
Mesaj Başlığı

Nitelik Durumu

Madde Tipi(Gaz)

Burada görmüş olduğumuz mesaj gemiye yüklenecek yükün gaz halinde olan bir yük olduğunu belirtiyor.

ATT+26+AGR:DGATT:306+XS:DGAGR:306'

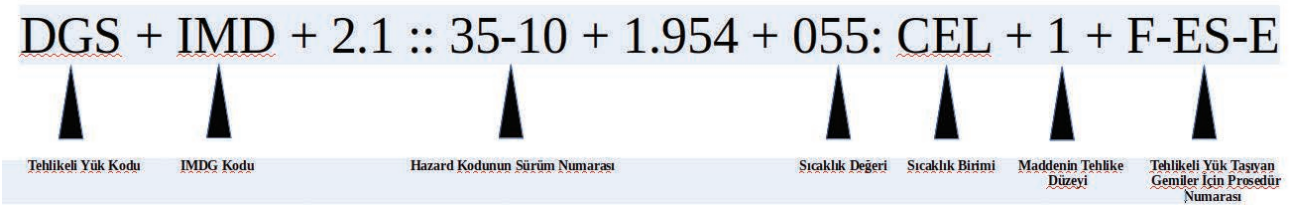
Burada ise maddenin halini değiştirerek maddenin patlayıcı bir madde olduğunu belirtmiş olduk. Eğer bir gemiye yüklenecek madde patlayıcı bir nitelik taşıyorsa burada geçen "XS" kodu mesajda bulunmak zorunda fakat biz bu kodu değiştirip patlayıcı maddeyi güvenli sıvı bir madde olarak betimleyebiliriz ve bu sebeple patlayıcı maddenin taşınmasına dair alınacak güvenlik önlemleri alınmadan gemi seyre çıkmış olacak. Bunu da aşağıdaki gibi yapabiliriz.

ATT+26+AGR:DGATT:306+L:DGAGR:306'

Yük tipini değiştirmek gibi nitelik ayrıntısını da değiştirebiliriz. Bunun için de "HAZ" kodu ile oynama yapacağız. O da şu şekilde:

ATT+26+HAZ:DGATT:306+FLVAP:DGHAZ:306'

Burada da "FLVAP" kodu değişikliği yaparak yakıtın yanıcı bir buhar olduğunu belirtmiş olduk. Tüm bunları yapabildiğimiz gibi taşınacak yük eğer yanıcı bir madde ise bunun için tepkimeye gireceği sıcaklığın bildirildiği mesajı değiştirerek de seyri tehlikeli bir duruma sokabiliriz.



Mesajımızda gördüğümüz sıcaklık değerinin değiştirilmesi ya da birimin Celcius'u temsil eden "CEL" kodu yerine Fahrenheit için kullanılan "FAH" kodunun gelmesi bile geminin seyrini ciddi anlamda tehlikeye sokacaktır.

Patlama ve yangın olayları dışında yük dengesinin bozulmasına ilişkili olarak da mesaj manipülasyonları yapılabilmektedir. Ayrıntılı bilgiler için BAPLIE mesajlarını inceleyebilirsiniz.

Benim değineceğim unsurların sonuna gelmiş bulunmaktayız. Yazının başlangıcında listeleyip burada bahsedemediğim unsurların yanı sıra elbette bunlardan daha fazlası da olacaktır. Bu yazıyı yazmamdaki amaç en azından bu konuda az da olsa farkındalık yaratabilmek ve detaylıca araştırılmasına ışık tutabilmekti. Umarım atladığımız şeyler bu konuda meraklı olan diğer arkadaşlarımız tarafından incelenip bizimle paylaşılır.

Kaynakça:

http://iho.int/iho_pubs/standard/S-63/S-63_e1.1.1_EN_Apr12.pdf

http://smdg.org/assets/assets/BAPLIE3.0.1e-MIG.pdf

http://smdg.org/assets/assets/BAPLIE3-MIG12-Master-Document.pdf

http://www.gemitrafik.com/vhf-deniz-telsizi/epirb-ve-sart-nedir/

http://www.shodb.gov.tr/shodb_esas/index.php/tr/urunler/haritalar/elektronik-seyir-haritalari

http://www.smdg.org/assets/assets/SMDG-CODES-FOR-DGS-ATT-v201501.xlsx

https://en.calameo.com/read/004474480397d2632c1e3

https://tools.ietf.org/html/rfc4130

https://www.boatus.org/study-guide/navigation/aids/

https://www.edibasics.com/what-is-edi/

https://www.pentestpartners.com/security-blog/hacking-serial-networks-on-ships/

https://www.pentestpartners.com/security-blog/making-prawn-espressos-or-hacking-ships-by-deciphering-baplie-edifact-messaging/

https://www.primar.org/distributors

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

Mithat Göğebakan - mithatgogebakan@gmail.com

Web Uygulamalarında Client-Side Statik Analiz Nasıl Yapılır?

Başlıkta geçen client-side ifadesi ile açıklamak istediğimiz kısım, tarayıcı ortamında görüntülediğimiz bir web uygulamasının, yine tarayıcı ortamından erişilebilen kaynaklarının analiz edilmesi.

Analiz edilmesi derken şüphesiz Javascript dosyalarından bahsediyorum.

Front-end Javascript kütüphaneleri hem geliştiricilerin hem de son kullanıcıların günlük hayatını fazlasıyla kolaylaştıran teknolojiler. Hâl böyle olunca da kısa sürede yaygınlaşarak, neredeyse her yerde karşılaştığımız teknolojilere dönüştüler.

AngularJS, ReactJS, Vue.js gibi front-end Javascript kütüphanelerini duymamış olmak neredeyse imkânsız…

Yazının ilerleyen kısımlarında cevap aramaya çalıştığımız soruların ne olduğunu özetleyecek olursak:

- Bu teknolojilerinin yaygınlaşması güvenlik açısından bize ne ifade ediyor?
- Zafiyet ararken işimiz kolaylaşıyor mu?
- Kullanan sitelerde hangi zafiyetleri, nasıl aramalıyız?

Statik analiz nedir sorusuna da en özet haliyle cevap vermek gerekirse, hedef yazılım çalıştırılmadan yapılan analizlerdir, yani şimdilik bizi ilgilendiren kısmı sadece burası.

Web uygulamasını tarayıcıda görüntülerken yapılan isteklerden farklı bir istek yapmadan, tarayıcımızın üzerinde bulunan geliştirme araçlarını kullanarak ya da benzer şekilde kullanımı basit araçlardan yardım alarak uygulamada zafiyet arayacağız.

Statik analiz yaparken ne arıyor olacağız?

Bu yazıda Recon yöntemlerine değinmeyeceğiz ama evet URL ve subdomainleri arıyor olacağız. Şirket içi amaçlarla kullanılan diğer ortamlar, private keyler, API endpointleri, ve dosya/dizinler yine aradığımız önemli bilgilerden olacak.

Kullanıldığı yerlerde potansiyel tehlikeleri işaret eden kodlar (eval vs) ve out-of-date kütüphaneler -özellikle de zafiyet içerdiği bilinen versiyonlar- aradığımız diğer detaylar olacak.

Uygulamanın kaynak dosyalarının toplanması

Tarayıcı ortamında uygulamayı gezinerek bir kısım kaynağa ulaşsak da bu her zaman yeterli olmuyor. Mesela görüntüleme yetkimizin olmadığı sayfalara ulaşamayacağız ya da uygulama arayüzünde gözle görmediğimiz bazı sayfalar olacak. Peki alternatiflerimiz nelerdir?

Web uygulamasının geçmişinden yararlanmak (Wayback Machine.)

archive.org bildiğiniz üzere web uygulamalarının arşivlerini tutuyor.

Görüntülediğiniz web uygulaması zaman içerisinde değişmiş olsa da, eskiden kalan bazı sayfalar hâlâ orada duruyor olabilir. Buradan elde edeceğimiz bilgiler bazen işinizi tahmin edemeyeceğiniz kadar kolaylaştırabilir.

Github'da buradaki arşivlerin içinde daha rahat arama yapmanızı sağlayacak bazı araçları bulmak mümkün.

Javascript dosyalarından full URL ve relative path bilgilerinin elde edilmesi

Analiz ettiğimiz web sitesi/sunucusu üzerinde ne kadar çok içerik tespit edebilirsek, zafiyet bulma ihtimalini aynı oranda arttırmış olacağız.

Hatalı yapılandırılmış bir servise, dışarıdan erişime açık unutulmuş ve default parolalar ile girmenin mümkün olduğu yönetici paneline ya da debug servisine ulaşma ihtimalimiz de olabilir.

Bu alanlarda dosya yükleme ya da komut çalıştırma gibi fonksiyonlar çoğunlukla tasarım gereği bulunduğundan, başka bir zafiyet aramaya gerek kalmayabilir.

relative-url-extractor hem local hem de remote Javascript dosyalarında doğrudan kullanabileceğimiz bir araç. (1)

ruby extract.rb https://www2.assets.

```
mg@Netsparker-VirtualBox:~/relative-url-extractor$ ruby extract.rb https://www2.assets.
/
/a
//
/events/
/log
/contact-sales
/html/continuous-delivery/ci-animation.html
/html/continuous-delivery/ci-flow-animation.html
/html/dynos/dyno-build.html
/event_tags.json
/html/kafka/kafka.html
/html/opex/opex-diagram.html
/html/platform-scale/platform-scale.html
/html/spaces/spaces.html
//cdn.jsdelivr.net/algoliasearch/2/
/1/indexes/
/1/logs?
/1/indexes
/1/keys
/1/keys/
/1/places/query
```

LinkFinder: **https://github.com/GerbenJavado/LinkFinder** (2)

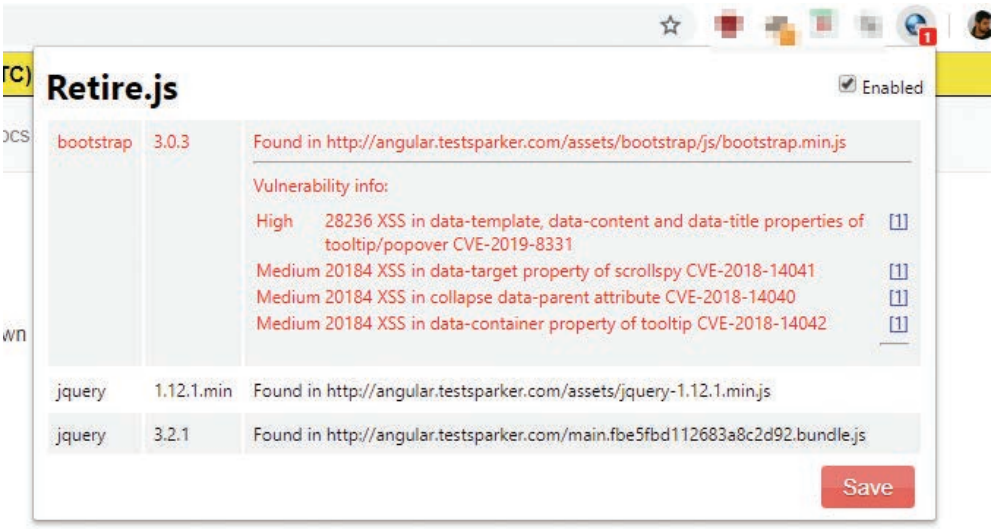
python linkfinder.py -i http://angular.testsparker.com -d -o cli

```
mg@Netsparker-VirtualBox:~/relative-url-extractor/LinkFinder$ python linkfinder.py -i http://angular.testsparker.com -d -o cli
https://fonts.googleapis.com/icon?family=Material+Icons
https://fonts.googleapis.com/css?family=Roboto:300,400,500,700,400italic
```

Vulnerable JavaScript kütüphanelerinin tespit edilmesi

Test ettiğiniz uygulama, daha önce zafiyet tespit edilmiş bir kütüphaneyi kullanıyor olabilir. Eğer böyle bir durum varsa, daha önce tespit edilmiş olan zafiyeti test ettiğimiz uygulama üzerinde aynı şekilde exploit etmek de mümkün olabilir. Peki bunu nasıl kontrol edeceğiz?

Retire.js (3) buradaki tüm ihtiyaçlarımızı karşılıyor olacak. Tarayıcı eklentisi olarak Chrome ve Firefox'a kurabilirsiniz. Kurulduğu siteleri ziyaret ederken bizi aşağıdaki gibi bir ekran karşılıyor olacak.



Doğrudan tarayıcı üzerinden kullanmak, sayfaları gezmeyi gerektirdiğinden genellikle pratik olmuyor. Böylesi durumlarda komut satırından kullanmak çoğu zaman etkili ve kolay oluyor.

```
mg@Netsparker-VirtualBox:~$ retire -h

  Usage: retire [options]

  Options:

    -h, --help               output usage information
    -V, --version            output the version number

    -p, --package            limit node scan to packages where parent is mentioned in package.json (ignore node_modules)
    -n, --node               Run node dependency scan only
    -j, --js                 Run scan of JavaScript files only
    -v, --verbose            Show identified files (by default only vulnerable files are shown)
    -x, --dropexternal       Don't include project provided vulnerability repository
    -c, --nocache            Don't use local cache

    --jspath <path>          Folder to scan for javascript files
    --nodepath <path>        Folder to scan for node files
    --path <path>            Folder to scan for both
    --jsrepo <path|url>      Local or internal version of repo
    --noderepo <path|url>    Local or internal version of repo
    --cachedir <path>        Path to use for local cache instead of /tmp/.retire-cache
    --proxy <url>            Proxy url (http://some.sever:8080)
    --outputformat <format>  Valid formats: text, json, jsonsimple, depcheck (experimental) and cyclonedx
    --outputpath <path>      File to which output should be written
    --ignore <paths>         Comma delimited list of paths to ignore
    --ignorefile <path>      Custom ignore file, defaults to .retireignore / .retireignore.json
    --severity <level>       Specify the bug severity level from which the process fails. Allowed levels none, low, medium, h
    --exitwith <code>        Custom exit code (default: 13) when vulnerabilities are found
    --colors                 Enable color output (console output only)
```

https://retirejs.github.io/retire.js/ adresinde hangi kütüphanelerin tespit edilebildiğinin kapsamlı listesi var, detaylı kontrol edilebilir.

Synk (4) benzer amaçlarla kullanabileceğimiz başka bir araç.

Bu araçları kullanırken sıklıkla göreceğiniz false positive bulgular olacaktır,

API keyleri, kullanıcı parolaları gibi kritik bilgilerin çıkarılması

Javascript dosyalarında bulabileceğimiz diğer kritik bilgiler ise, unutulmuş API keyleri, kullanıcı parolaları gibi doğrudan sistemde kullanacabileceğimiz bilgilerdir.

Bu noktada bize yardımcı olabilecek araçların izlediği temel birkaç yaklaşım var. Bunlardan biri Regex tabanlı arama ve eşleştirme yapan araçlar. Bu araçlar bildiğimiz regex mantığı ile arama yapıyor. Hedef olarak girilen depoda/dizinde/sayfada daha önceden girilmiş kurallarla ulaşılmak istenen verileri tespit edebiliyorlar. Bu araçlar genellikle kullanıcı adı ve parolaları tespit etmekte başarılı oluyor.

Diğer yöntem ise Entropy tabanlı aramalar yapan araçlar. Bu araçlar ise API key ve token gibi bilgileri bulmada başarılı genellikle.

Hem regex hem de entropy tabanlı araçlar sıklıkla FP verebiliyor.

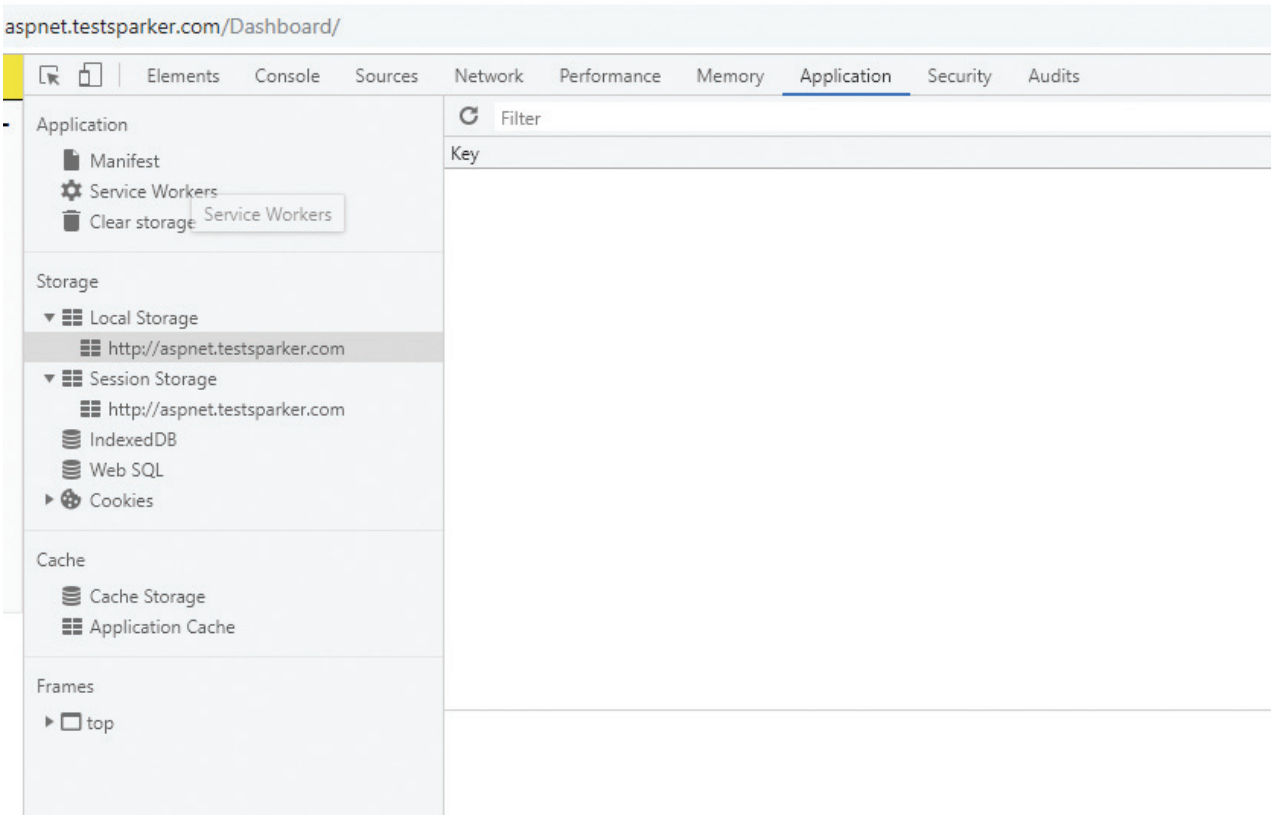
truffleHog: https://github.com/dxa4481/truffleHog

trufflehog --regex --entropy=False https://github.com/dxa4481/truffleHog.git

```
mg@Netsparker-VirtualBox:~$ trufflehog --regex --entropy=False https://github.com/dxa4481/truffleHog.git
~~~~~~~~~~~~~~~~~~~~~~
Reason: Generic Secret
Date: 2018-08-25 06:32:36
Hash: 2e064ae3275a44f9b382c3d0cb5fedff72105942
Filepath: test_all.py
Branch: origin/dev
Commit: Merge branch 'dev' into bugfix/wrong-commit-hash
secret = '9ed54617547cfca783e0f81f8dc5c927e3d1e345'
~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~
Reason: Generic Secret
Date: 2018-08-13 10:32:04
Hash: d98e54c5185afefac7c1fceb5d002e687f8ddce1
Filepath: test_all.py
Branch: origin/dev
Commit: Fix bug with commit hash error.
secret = '9ed54617547cfca783e0f81f8dc5c927e3d1e345'
~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~
```

Cookie'ler ve tarayıcıda bulunan diğer datalar

Browser Storage bizim için anlamlı olabilecek bilgilere ulaşabileceğimiz başka bir yer. DevTools'da Application sekmesinde bu datalara kolaylıkla ulaşabiliriz.



Buradan iki farklı yerde bilgi saklamak mümkün, bunlar Local Storage ve Session Storage. Bunların arasındaki en temel fark Session Storage'de bulunan verinin uygulama ile iletişim kesildiğinde-tarayıcı kapatıldığında ya da ilgili tarayıcı sekmesi kapatıldığında- silinmesi. Local Storage'da bulunan veriler için özel bir koşul tanımlanmamışsa, silinene kadar ulaşılabilir.

İlgili bağlantılar ve referanslar:

(1) https://github.com/jobertabma/relative-url-extractor

(2) https://github.com/GerbenJavado/LinkFinder

(3) https://github.com/RetireJS/retire.js

(4) https://snyk.io/

Performing JavaScript Static Analysis by Lewis Ardern [Video]

https://medium.com/@_bl4de/how-to-perform-the-static-analysis-of-website-source-code-with-the-browser-the-beginners-bug-d674828c8d9a

Siber Yıldız 2019 Çözümleri

Siber Yıldız, Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet gösteren Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından 2017 yılından itibaren organize edilen, hem genç yeteneklerin keşfine hem de istihdamına imkân veren bir yarışma.

2017 yılında yarışmaya dair BTK tarafından yapılan ilk duyuruda mezuniyet şartı aranmaksızın, tüm yeteneklerin değerlendirileceği ve başarı nispetinde istihdam edilecekleri belirtildiğinde büyük bir heyecana neden olan yarışma 2019 yılında da gençlerin ilgilerinin odağındaydı.

Arka Kapı Dergi, 7. Sayısında Esra Nur Soylu tarafından kaleme alınan write-up'ı yayınlayarak yarışma heyecanını ve tecrübesini tüm okurları ile paylaşmayı hedeflemektedir. Katkılarından ötürü Esra Nur Soylu'ya teşekkürlerimizi sunar, katkılarının devamını dilediğimizi siz okurların huzurunda bir kez daha belirtiriz. (e.n.)

Hazırlık Sorusu 1:

Bilişim şirketimizde çalışmak ister misin?

Sayfa kaynağını incelediğimde:

```
<p class="copyright">
    &copy; Maxim Theme. All rights reserved.
    <div class="credits">
        <!--       !!!  Yonetici Panelini tespit edebilecek misin?                    -->
        <a href="https://bootstrapmade.com/">Free Bootstrap Themes</a> by BootstrapMade.com
    </div>
</p>
```

Yönetici panelini bulmamızı istiyordu. Ben de **dirb** çalıştırmaya karar verdim ve admin panelinin adresini bulup, bu sayfa üzerinden bayrağı elde etmiş oldum:

Hazırlık Sorusu 2:

Dikkatle incelersen cevabı bulabilirsin.

```
<html lang="tr">
<head>
<meta charset="utf-8">

<title>Beni bul</title>
</head>
<body>
Bakalım beni bulabilecek misin ?
<!-- Buraya baktığın iyi oldu : 87habythi15ng151.php dosyasını bir incele. -->
</body>
</html>
```

Sayfa kaynağına baktığımızda ilgili yönerge, başka URL'e bakmamız gerektiğini söylüyordu.

URL'e gittiğimizde çözmemiz gereken bir algoritma yapısı görüyoruz. Anahtarı bulmak için URL'in path ayracı olarak kullanılan "/" (forward slash) ile bölümlenmesi gerektiğini belirtiyor. Bayrağın ise bu bölümlenmeden sonra elde edilen dizinin dördüncü elemanında. Tabii dizinin dördüncü eleman değerini md5 hash algortimasından geçirmemiz gerekiyor. Sonuç, bayrak elinizde!

Ekran görüntüsü sizi yanıltmış olabilir. Aslında sayfanın URL'i adres çubuğunda gözükmeyen şemayı da içeriyor, yani

http://85.111.95.17/……../87habythi15ng151.php

URL'i incelediğimizde algoritmanın anlattığına göre 4. anahtardan sonraki kısım bize bayrağı verecektir.

"87habythi15ng151.php" ifadesini md5 encoder ile oluşturduğumuzda bayrağı elde ediyoruz.

YARIŞMA SORULARI

Soru: Bu gerçekten kolay

Bu adımda CTF *dikkatli.bak.dms* adında bir dosya indirilmesini sağlıyordu. Bu dosyayı herhangi bir text editör ile açtığımızda aşağıdaki ifadeyi görüyorduk.

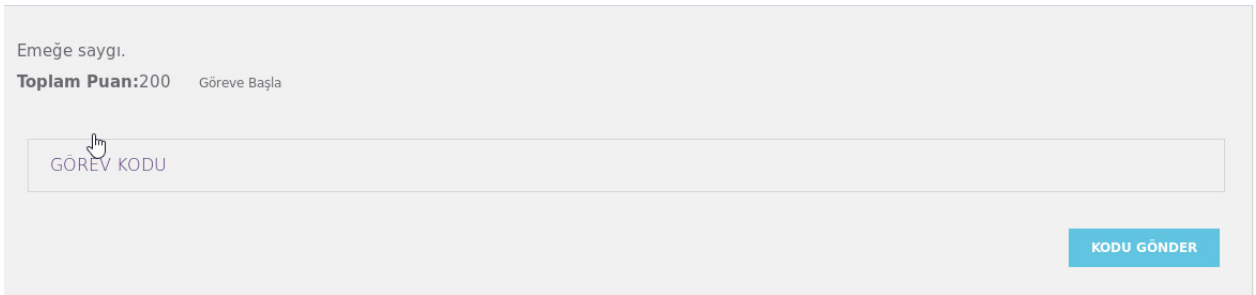
```
flag: RDcxVWV3SUFLM29RazBGV1Rnb0dsbURpWDJnckg1MUgvZ09WWFZmbkFBWmhjczk3S291TGprSnZEMENtYmxnd2R6d0tOc2pKeHZKVW8zVHczSUtIRUE9PQ==N
```

Soru: Hala ısınmalardasın

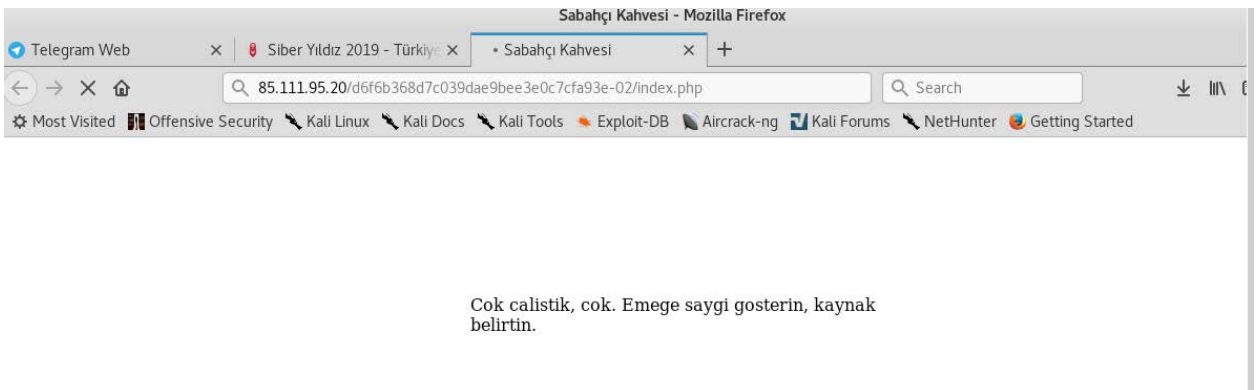
```
    <script src="js/creative.min.js"></script>

    <!-- Şu script şurda dursun da sonra sileriz-->
    <script language=javascript>
        var _0xdbf2=["\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65"];eval(String[ _0xdbf2[0]](70,108,97,103,58,32,78,106,74,74,100,84,74,90,82,122,90,107,83,50,70,84,97,49,
    </script>

</body>
```

Sorunun kaynak kodunu incelediğimizde Javascript dilinde hazırlanmış bir içerik olduğunu görüyoruz. Rakamları char code decoder ile çözdüğümüzde flag'i elde etmiş oluyoruz:

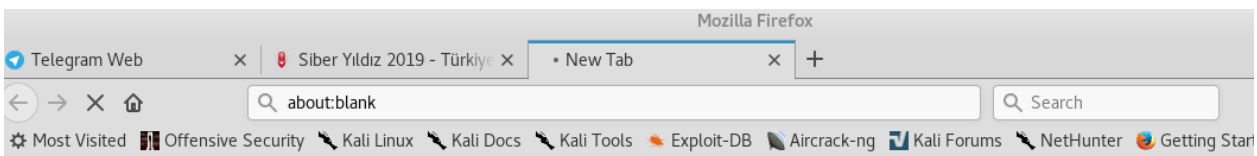
Soru: Emeğe Saygı

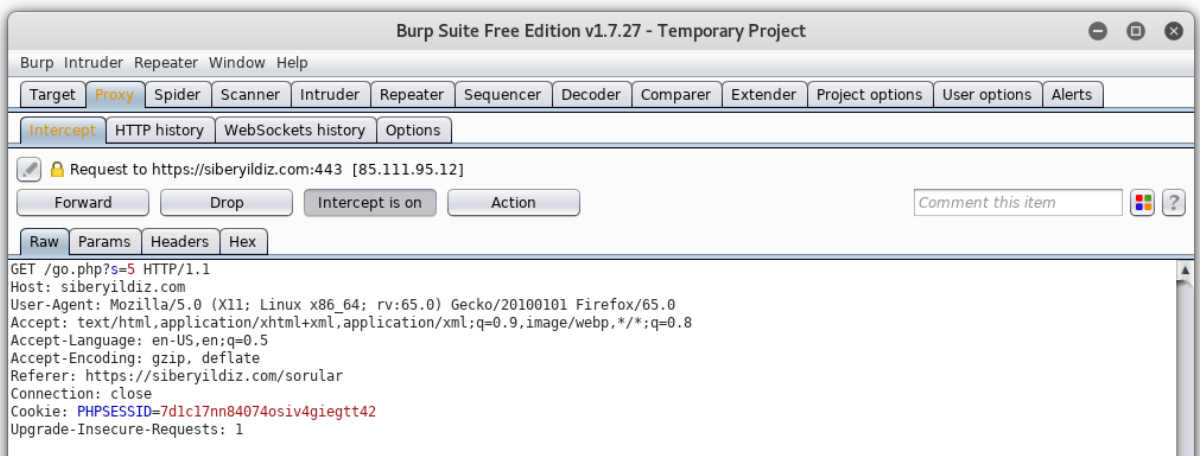


Cevap:



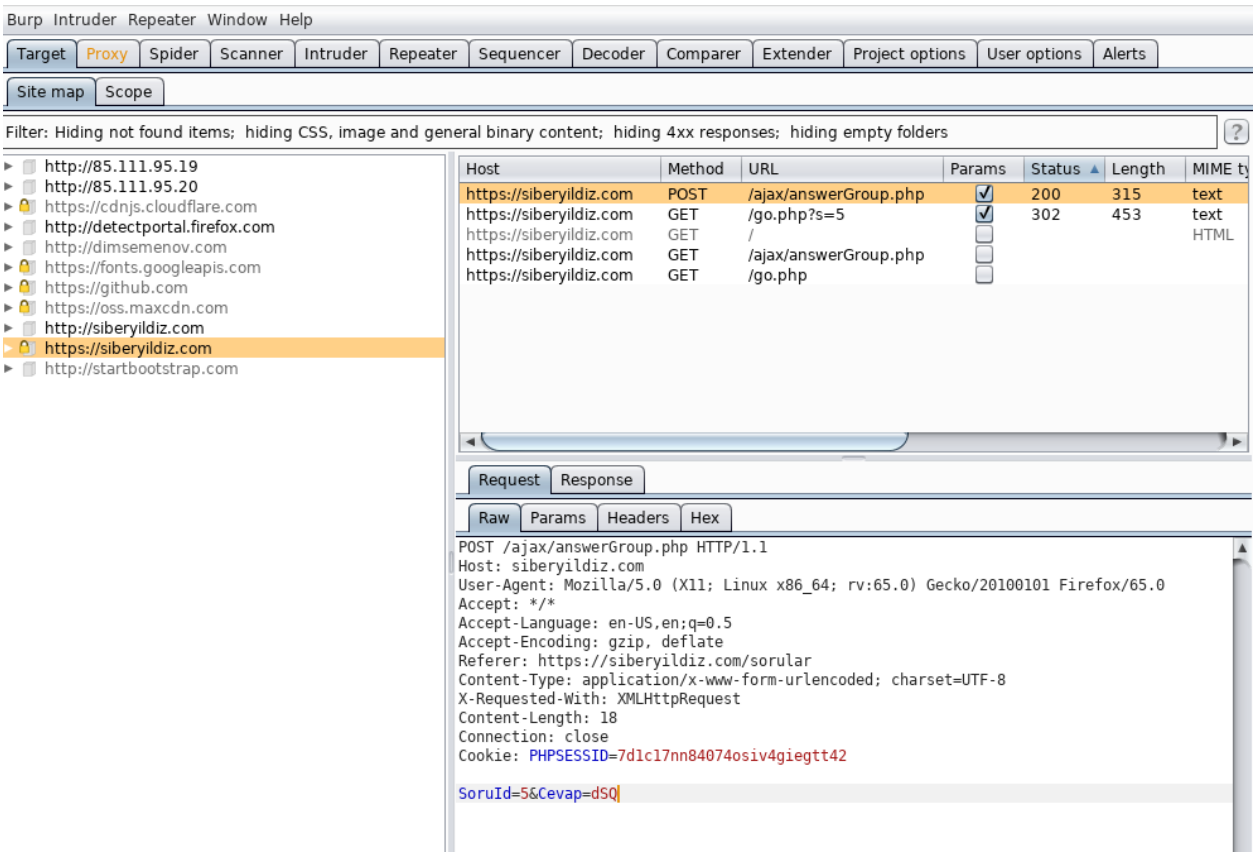
Sayfayı açtığımızda *"Cok calistik ,cok. Emege saygi gosterin, kaynak belirtin."* şeklinde bir yazı karşılıyordu.





Burp ile inceleme karar verdik. HTTP isteğinde Cookie ve "Referer" header'ları vardı. Referer'da rastgele oynamalar yapıp request'i yolladığımızda gelen response kısmında *"Kaynak belirtenlere hediyelerimizi gönderdik. Sağ olun, var olun."* şeklinde yazı görüyorduk. Bu yazıyı gördüğümüze göre doğru kısımdayız ancak "Referer" kısmını değiştirmemiz gerekiyor, diye düşündük. Referer kısmına denemeler yapmaya başladık.

Web sayfasının title kısmındaki "Sabah Kahvecisi" bize bir ipucu vermesi gerekir diyerek Google'da araştırdığımızda Ferdi Tayfur'un Sabahçı Kahvesi şarkısını gördük. Bu Youtube linkini Referer kısmına verdik ancak başarısız olduk.



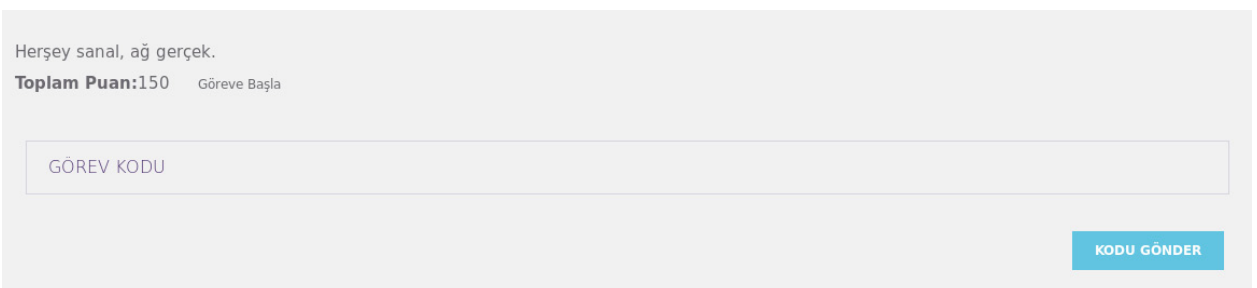
Burp üstünden sitemap kısmına baktığımda SoruId yanında Cevap diye bir kısım gördüm. Ancak gereksiz heyecan oldu bu sadece. :)

Yapılması gereken Referer'e istek attığını düşünerek sniffer ile gelen istekleri kaydeden dosya hazırlamaktı. Dosyaya baktığımızda bayrak geliyordu:

[HTTP_REFERER] => iste ödülün :

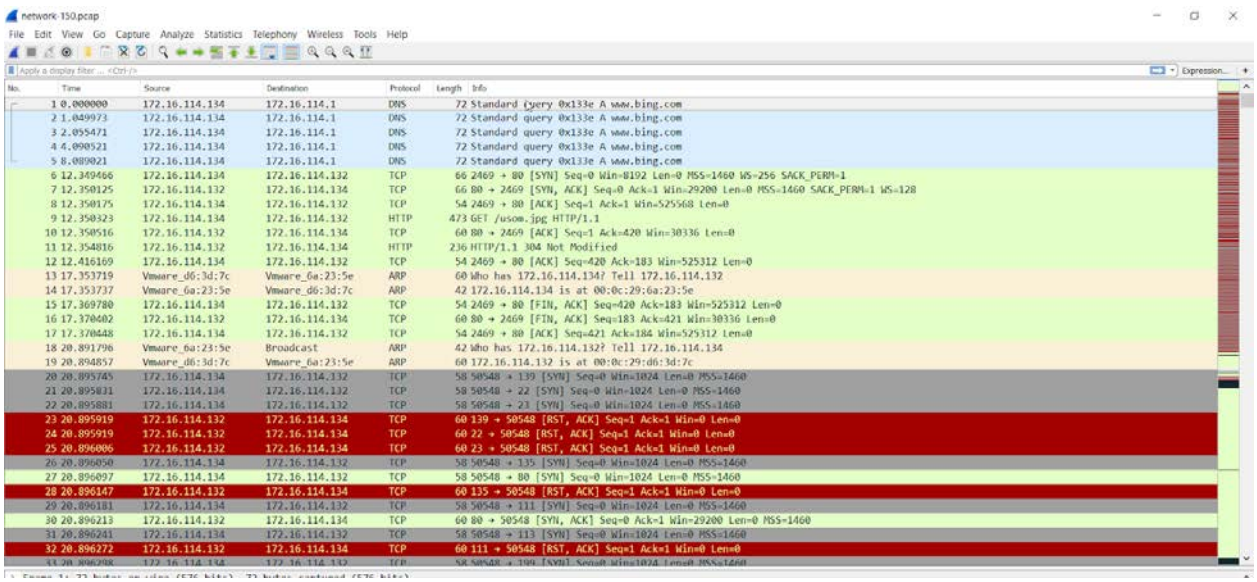
aFZPL0hkSjhvaThneGdIdkFMcUd1UFZLOGNhMGxGSG1lak1VbXlROFVGO

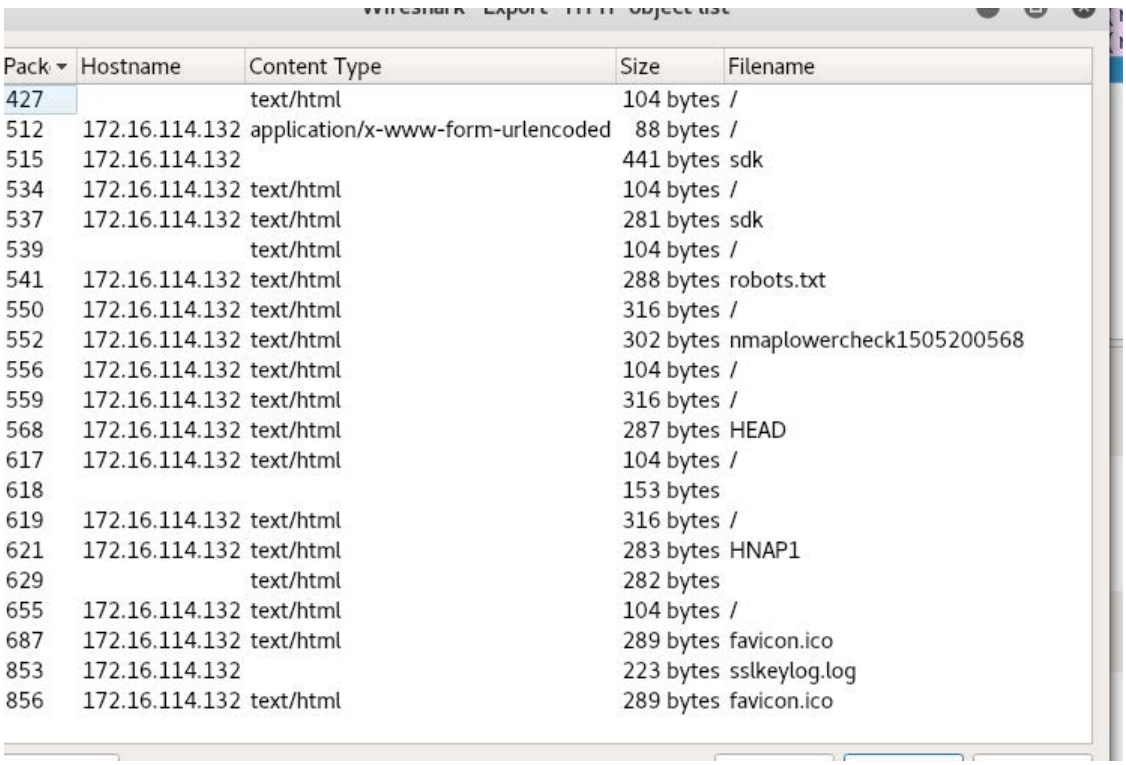
FdxVWI3bjFYTW10bVVFMk5ZdTVQV3daRSsxWFZsbmZWZ3dLOFMveHZxQnc9PQ==



Soru: Her şey sanal, ağ gerçek.

Göreve başladığımızda sıkıştırılmış bir biçimde (ZIP) Wireshark dosyası indirdik.

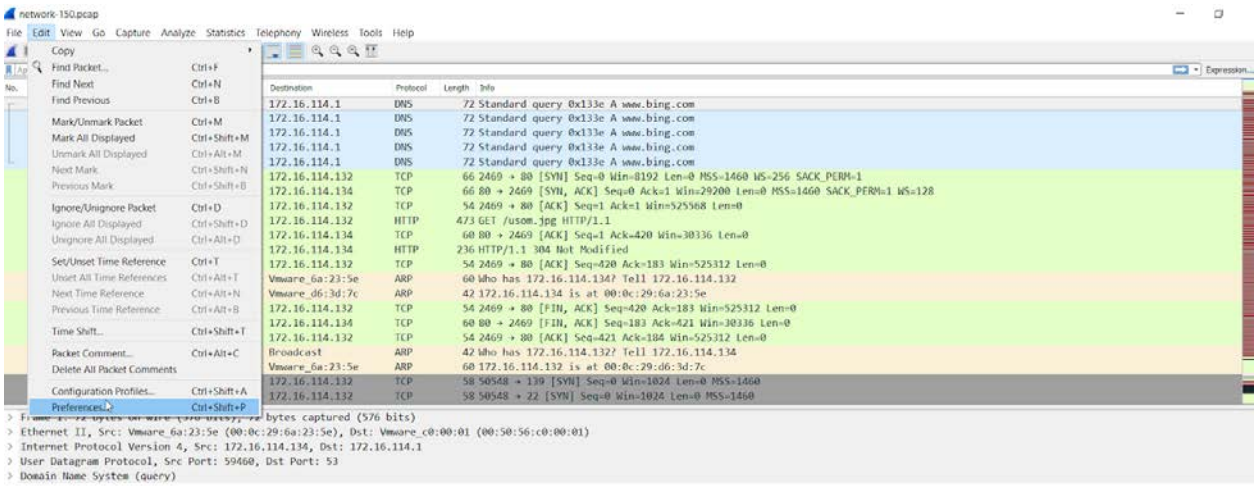


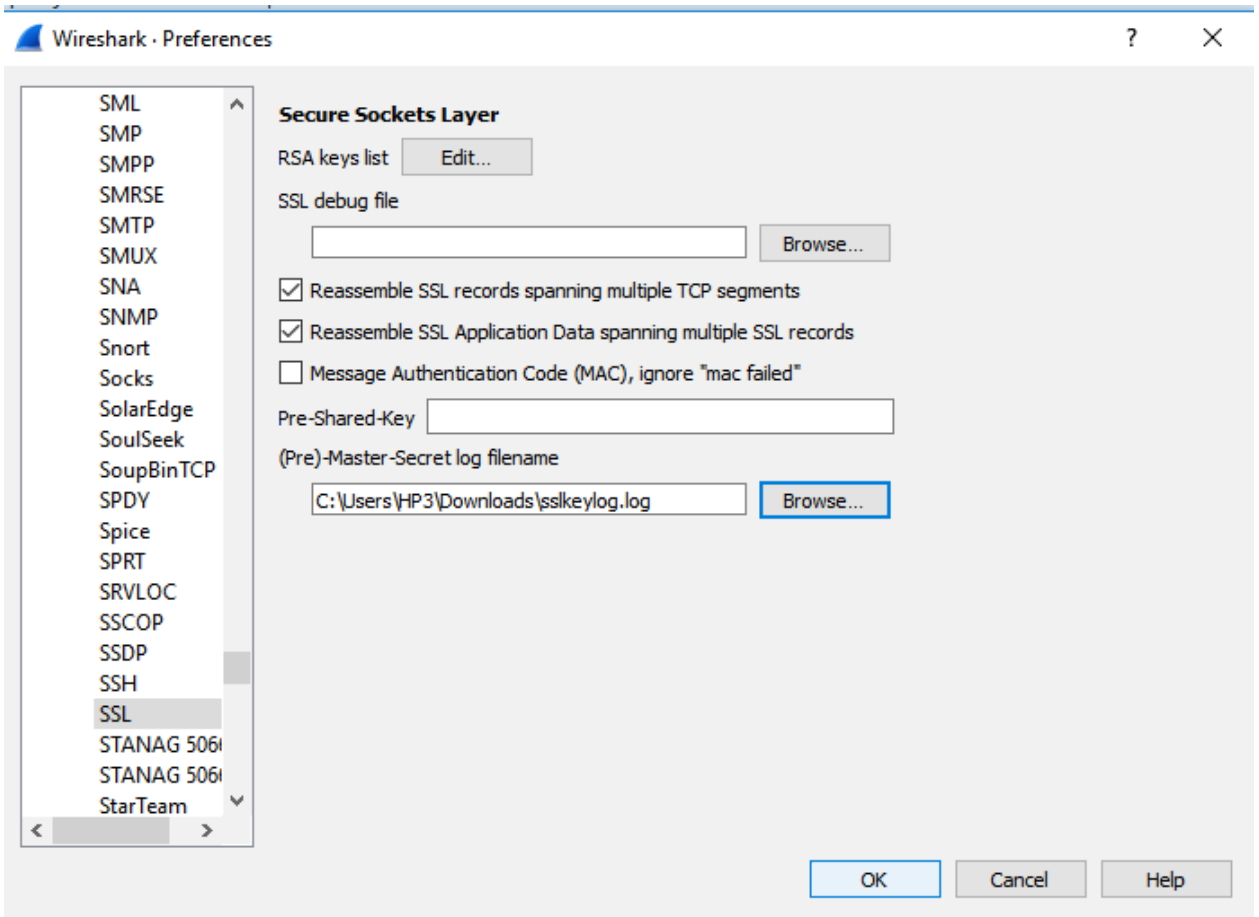


Pack	Hostname	Content Type	Size	Filename
427		text/html	104 bytes	/
512	172.16.114.132	application/x-www-form-urlencoded	88 bytes	/
515	172.16.114.132		441 bytes	sdk
534	172.16.114.132	text/html	104 bytes	/
537	172.16.114.132	text/html	281 bytes	sdk
539		text/html	104 bytes	/
541	172.16.114.132	text/html	288 bytes	robots.txt
550	172.16.114.132	text/html	316 bytes	/
552	172.16.114.132	text/html	302 bytes	nmaplowercheck1505200568
556	172.16.114.132	text/html	104 bytes	/
559	172.16.114.132	text/html	316 bytes	/
568	172.16.114.132	text/html	287 bytes	HEAD
617	172.16.114.132	text/html	104 bytes	/
618			153 bytes	
619	172.16.114.132	text/html	316 bytes	/
621	172.16.114.132	text/html	283 bytes	HNAP1
629		text/html	282 bytes	
655	172.16.114.132	text/html	104 bytes	/
687	172.16.114.132	text/html	289 bytes	favicon.ico
853	172.16.114.132		223 bytes	sslkeylog.log
856	172.16.114.132	text/html	289 bytes	favicon.ico

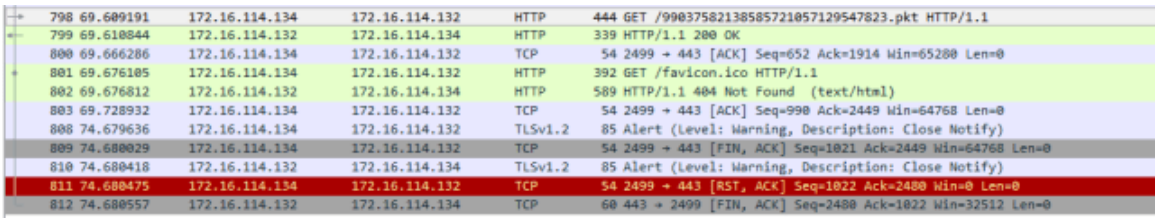
Paketi incelediğimizde bir birkaç URL gezinmeleri olmuştu ve anlamsız paketler, Nmap logları görüyorduk.

İçerisindeki dosyaları export ettiğimizde anlamsız dosyalar buldum, ancak içerisinde işimize yarayabilecek *sslkeylog.log* isimli bir dosya vardı. Bu sayede sunucu anahtarına sahip değilsek bile SSL/TLS ile decrypt edilmiş trafiği çözebilirdik. (*sslkeylog.log* isimli dosya, Firefox and Chrome tarayıcılarının trafiğin şifrelenmesinde kullanılan simetrik oturum anahtarını logladıkları bir dosyadır. Bu dosyayı Wireshark'a göstererek elde ettiği şifrelenmiş trafiği okumasını sağlayabiliriz. en.)

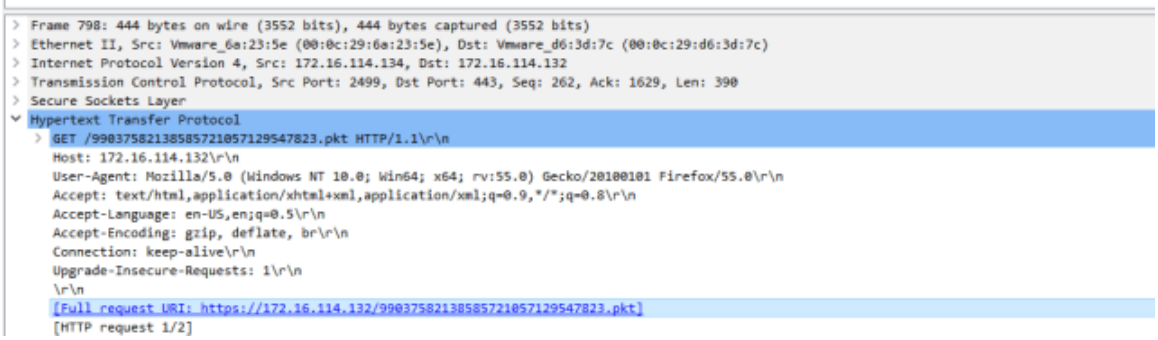




Wireshark ayarlarında "prokotoller" kısmının "SSL" bölümüne *sslkeylog.log*'u gömdüğümüzde Pcap içinde decrypted loglar göründü, bunları incelediğimde bazı yerlere giriş yapıldığı görülüyordu.



798	69.609191	172.16.114.134	172.16.114.132	HTTP	444 GET /990375821385857210571295478 23.pkt HTTP/1.1
799	69.610844	172.16.114.132	172.16.114.134	HTTP	339 HTTP/1.1 200 OK
800	69.666286	172.16.114.134	172.16.114.132	TCP	54 2499 → 443 [ACK] Seq=652 Ack=1914 Win=65280 Len=0
801	69.676105	172.16.114.134	172.16.114.132	HTTP	392 GET /favicon.ico HTTP/1.1
802	69.676812	172.16.114.132	172.16.114.134	HTTP	589 HTTP/1.1 404 Not Found (text/html)
803	69.728932	172.16.114.134	172.16.114.132	TCP	54 2499 → 443 [ACK] Seq=990 Ack=2449 Win=64768 Len=0
808	74.679636	172.16.114.134	172.16.114.132	TLSv1.2	85 Alert (Level: Warning, Description: Close Notify)
809	74.680029	172.16.114.134	172.16.114.132	TCP	54 2499 → 443 [FIN, ACK] Seq=1021 Ack=2449 Win=64768 Len=0
810	74.680418	172.16.114.132	172.16.114.134	TLSv1.2	85 Alert (Level: Warning, Description: Close Notify)
811	74.680475	172.16.114.134	172.16.114.132	TCP	54 2499 → 443 [RST, ACK] Seq=1022 Ack=2480 Win=0 Len=0
812	74.680557	172.16.114.132	172.16.114.134	TCP	60 443 → 2499 [FIN, ACK] Seq=2480 Ack=1022 Win=32512 Len=0

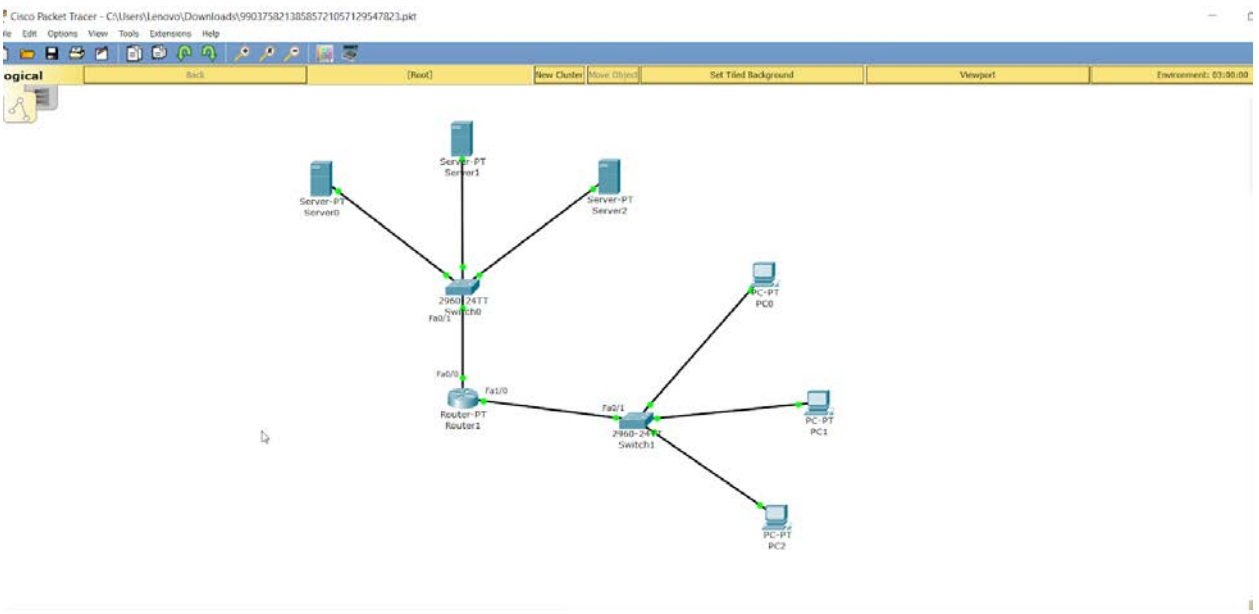


```
> Frame 798: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits)
> Ethernet II, Src: Vmware_6a:23:5e (00:0c:29:6a:23:5e), Dst: Vmware_d6:3d:7c (00:0c:29:d6:3d:7c)
> Internet Protocol Version 4, Src: 172.16.114.134, Dst: 172.16.114.132
> Transmission Control Protocol, Src Port: 2499, Dst Port: 443, Seq: 262, Ack: 1629, Len: 390
> Secure Sockets Layer
v Hypertext Transfer Protocol
  > GET /990375821385857210571295478 23.pkt HTTP/1.1\r\n
    Host: 172.16.114.132\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate, br\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: https://172.16.114.132/990375821385857210571295478 23.pkt]
    [HTTP request 1/2]
```

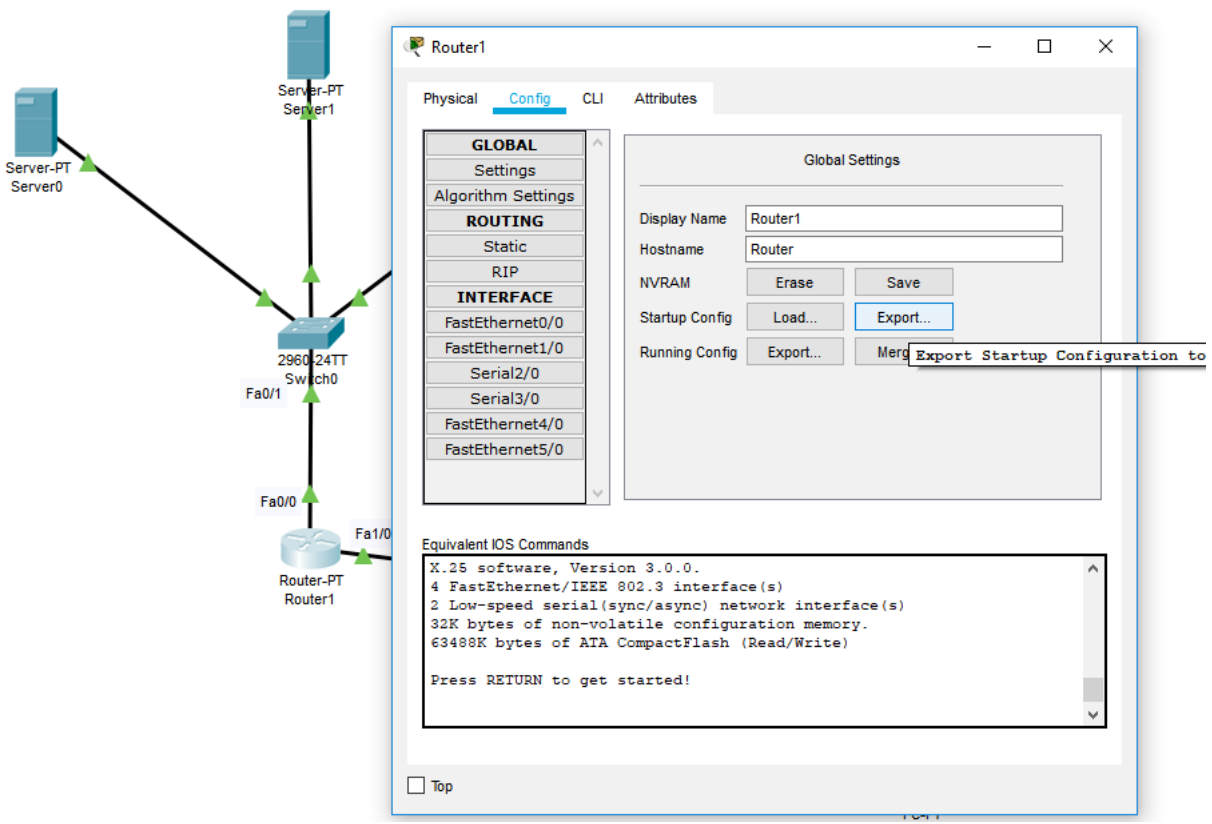
```
GET /990375821385857210571295478 23.pkt HTTP/1.1
Host: 172.16.114.132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 12 Sep 2017 03:32:08 GMT
Server: Apache/2.4.27 (Debian)
Last-Modified: Tue, 12 Sep 2017 03:30:18 GMT
ETag: "0-558f5a993e8bf"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

GET /favicon.ico HTTP/1.1
Host: 172.16.114.132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

HTTP/1.1 404 Not Found
Date: Tue, 12 Sep 2017 03:32:08 GMT
Server: Apache/2.4.27 (Debian)
Content-Length: 290
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /favicon.ico was not found on this server.</p>
<hr>
<address>Apache/2.4.27 (Debian) Server at 172.16.114.132 Port 443</address>
</body></html>
```

HTTP Stream Görüntüsü

Pcap'de yer alan bir dosya("990375821385857210571295478 23.pkt") gözümüze çarptı. Sunucudan o dosyayı indirdik.

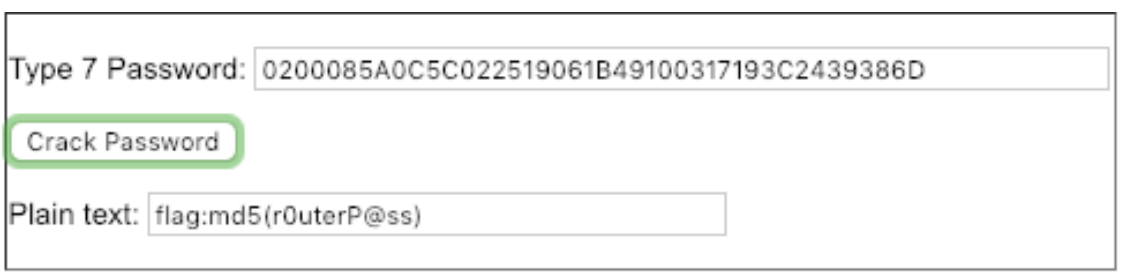


Dyalog diye bi programlama dili dosyası olduğunu gördük. Biraz daha araştırma yaptığımızda packet tracer dosyası olduğunu bulduk ve programı indirip elimizdeki "990375821385857210571295478 23.pkt" dosyasını açtık.



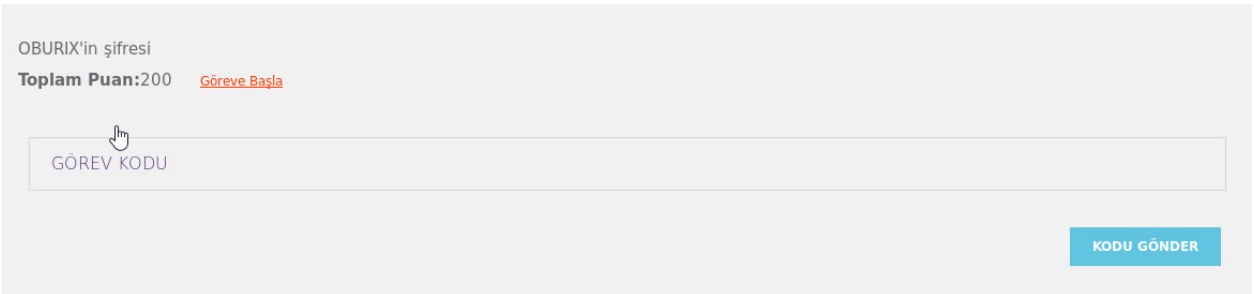
Router'ı incelediğinizde Config kısmından "Startup config" dosyasını dışarı aktardık.

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no logging console
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username usom password 7 0200085A0C5C022519061B49100317193C2439386D
!
!
!
```

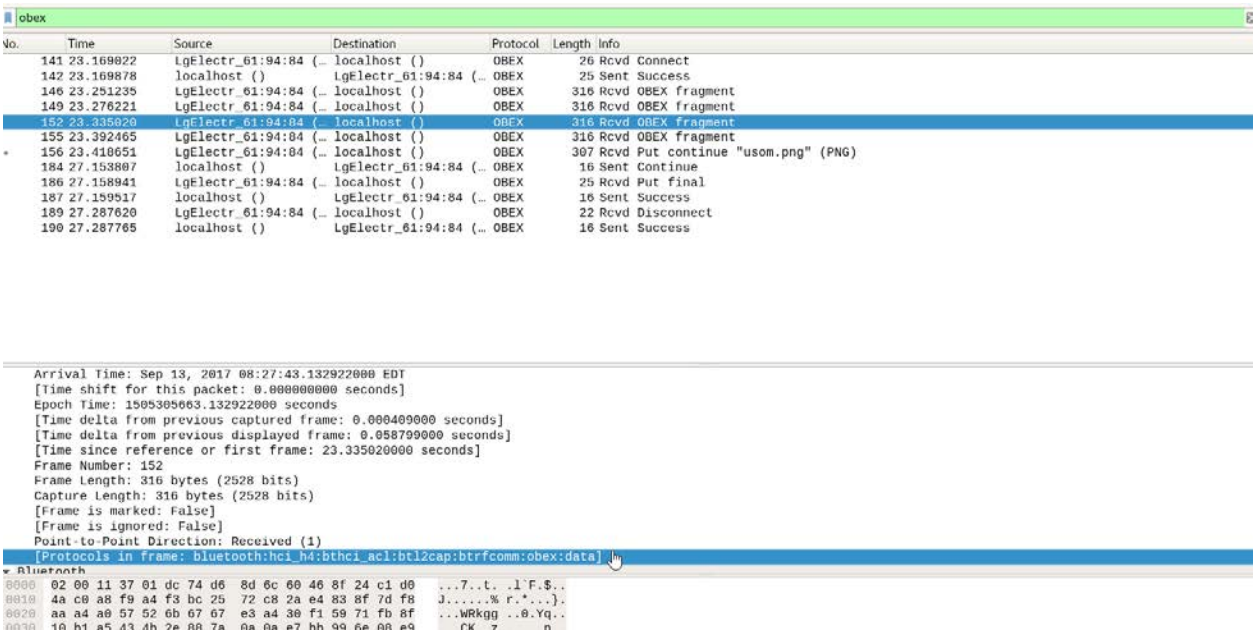


Cisco Password Cracker ile baktığımızda içerisinde "r0uterP@ss" gördük.

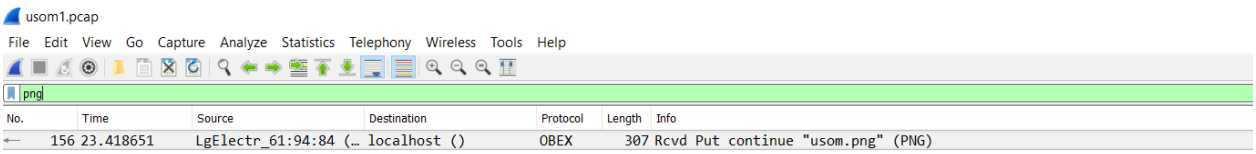
Soru: OBURIX'in şifresi

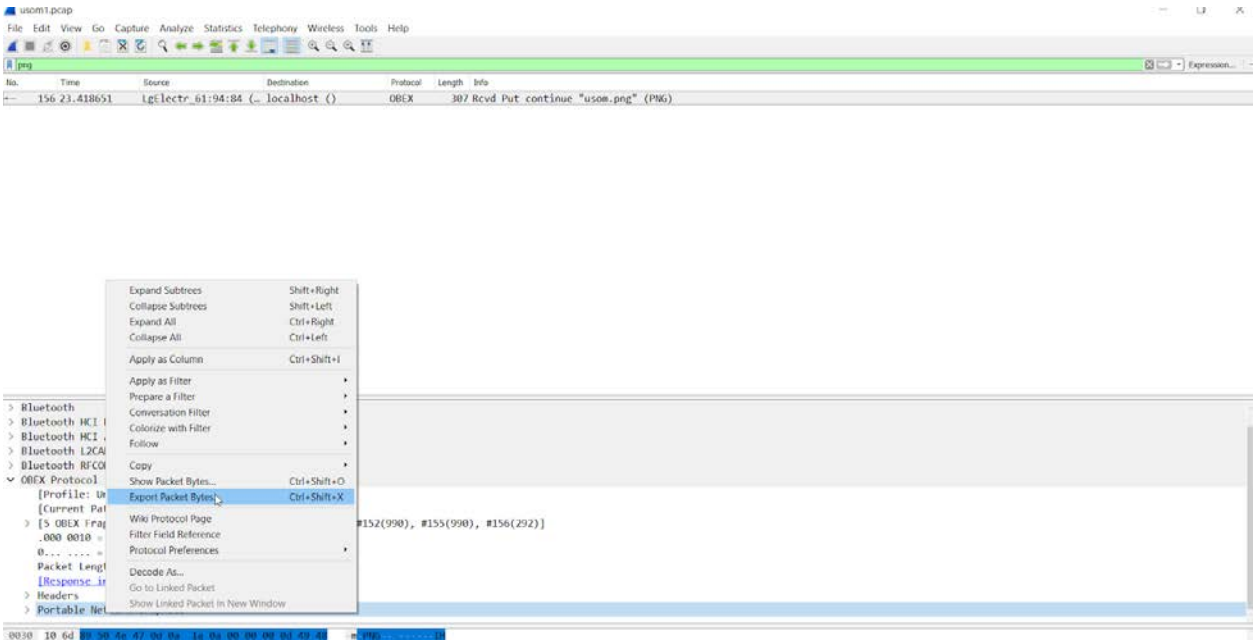


Bu adım için de yine bir pcap dosyası indiriyoruz.



PCAP dosyasını incelediğimde soru ismi ile benzerliğinden dolayı obex kelimesi gözüme çarpıyor. Sorunun ismi OBURIX olunca filtreleme kısmına direk "obex" yazarak başladım.





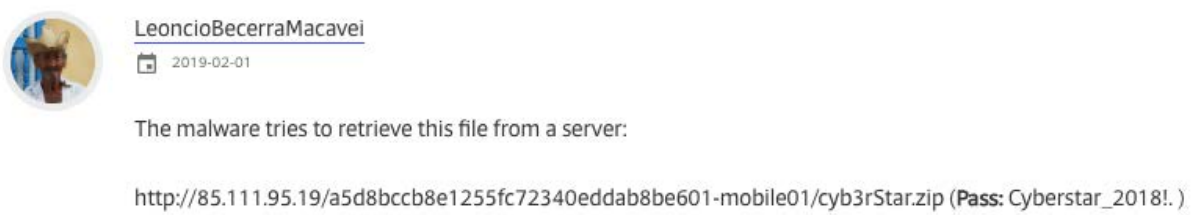
PCAP dosyasını incelediğimiz bu sefer Bluetooth trafiği olduğunu görüyorduk. Biraz daha incelediğimizde usom.png kısmı gözümüze çarpttı. Bu dosyayı Binwalk ile indirmeye çalıştık. Ancak dosya bozuk olarak indi. Biz de başka indirme alternatifleri ararken filtre kısmına png yazarak direk pcap dosyasından indirmeyi denedik.

Farede sağa tıklayarak Export Packet Bytes seçeneğinden indirdiğimizde resim bize direk flagi söylüyordu.

K0JwaTdxRUoydk9Ea3VpTW8rRVM1UT09

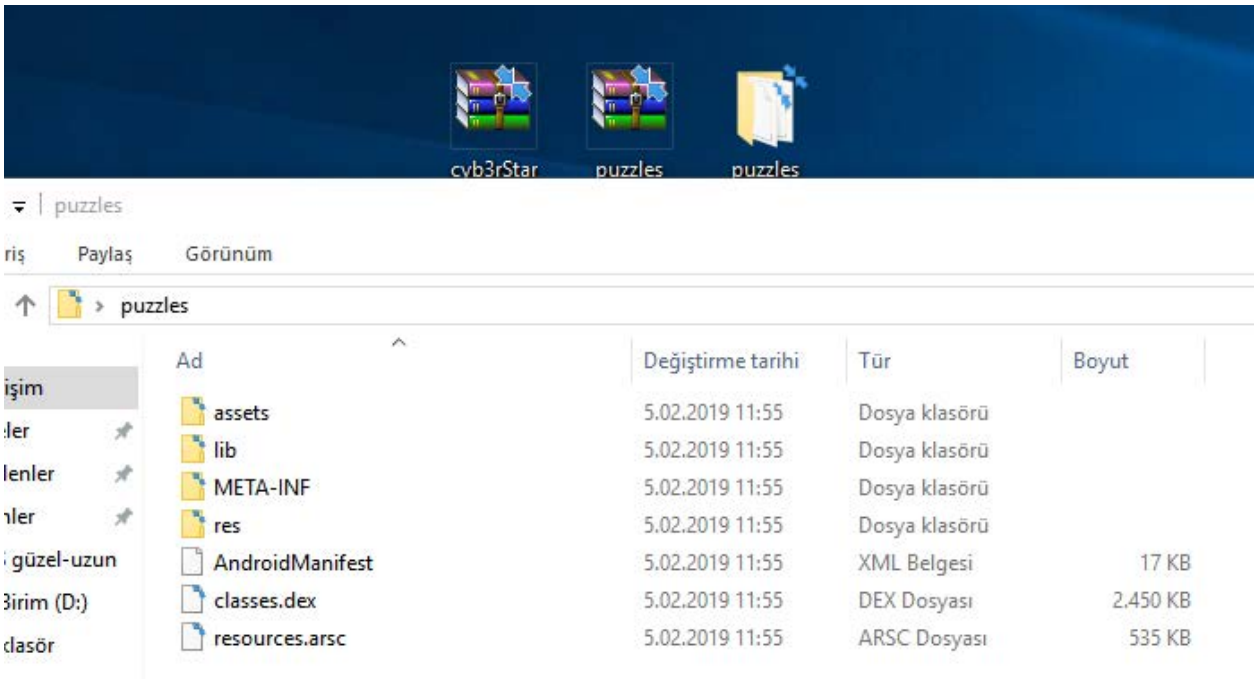
Soru: Bir bakan var, bir de aranan.

Göreve başladığımızda "0827206450376af3dce61d788ddeba21f58dba35257fdb43c1872c096a36287f" şeklinde bir hash değeri ile karşılaşıyorduk.



Bu hash değerini VirusTotal ile arattığımızda ise bir yorum görüyorduk.

ZIP'lenmiş dosyayı indirip açtığımızda karşımıza puzzles.apk adlı bir dosya çıkıyordu.



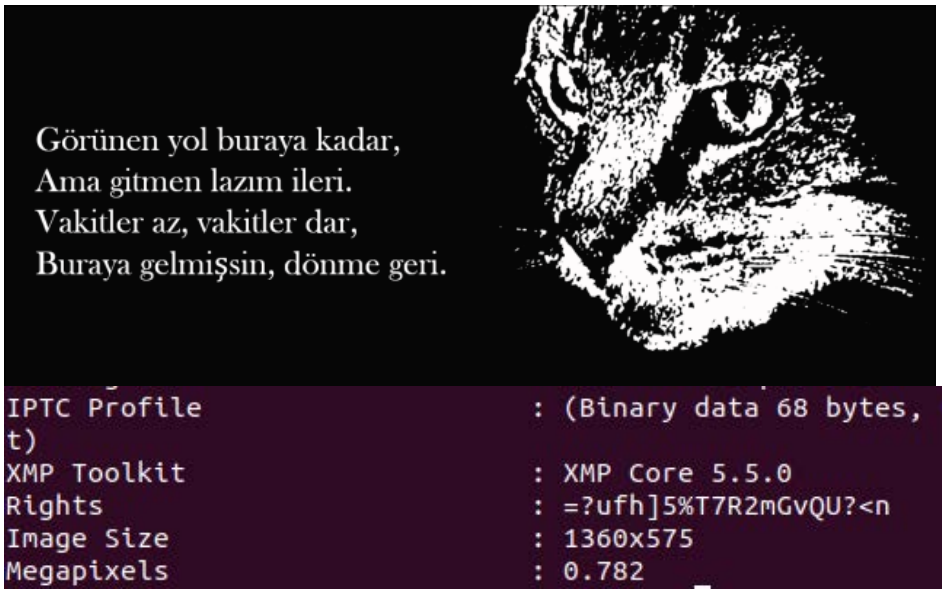
Dosyayı ZIP uzantısı ile değiştirip baktığımızda içerisinde dosyalar gördük. /res/drawable içerisine girdiğimizde resim dosyaları gördük.

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
115805        0x1C45D         Zip archive data, at least v2.0 to extract, name:
gizlidosya/
115878        0x1C4A6         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar.gif
123023        0x1E08F         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_1.gif
130170        0x1FC7A         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_2.gif
137317        0x21865         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_3.gif
144464        0x23450         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_4.gif
151611        0x2503B         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_5.gif
158758        0x26C26         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 7620, name: gizlidosya/thankyoucyberstar_6.gif
```

Binwalk ile incelediğimizde çoğu resimde gördüğümüz "thankyoucyberstar.gif" içeriği vardı.

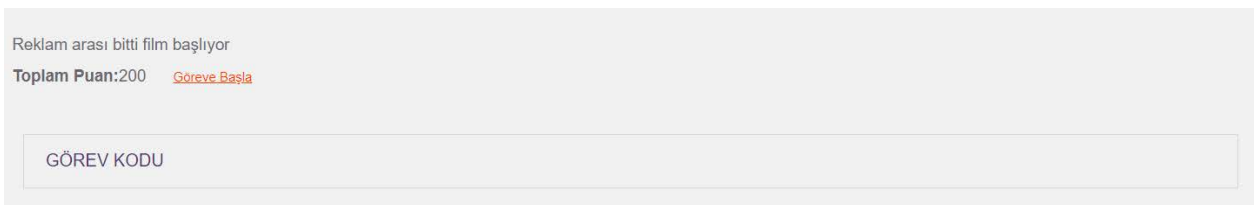
```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
145579        0x238AB         Zip archive data, at least v1.0 to extract, name:
gizlidosya/
145648        0x238F0         Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 1342466, uncompressed size: 2100998, name: gizlidosya/hadib
ul.b64
1488383       0x16B5FF        End of Zip archive, footer length: 22
```

Ancak ortakoy.jpg içerisinde ZIP'li bir dosya gördük. Extract etmeye çalıştığımızda parola korumalı olduğunu gördük.

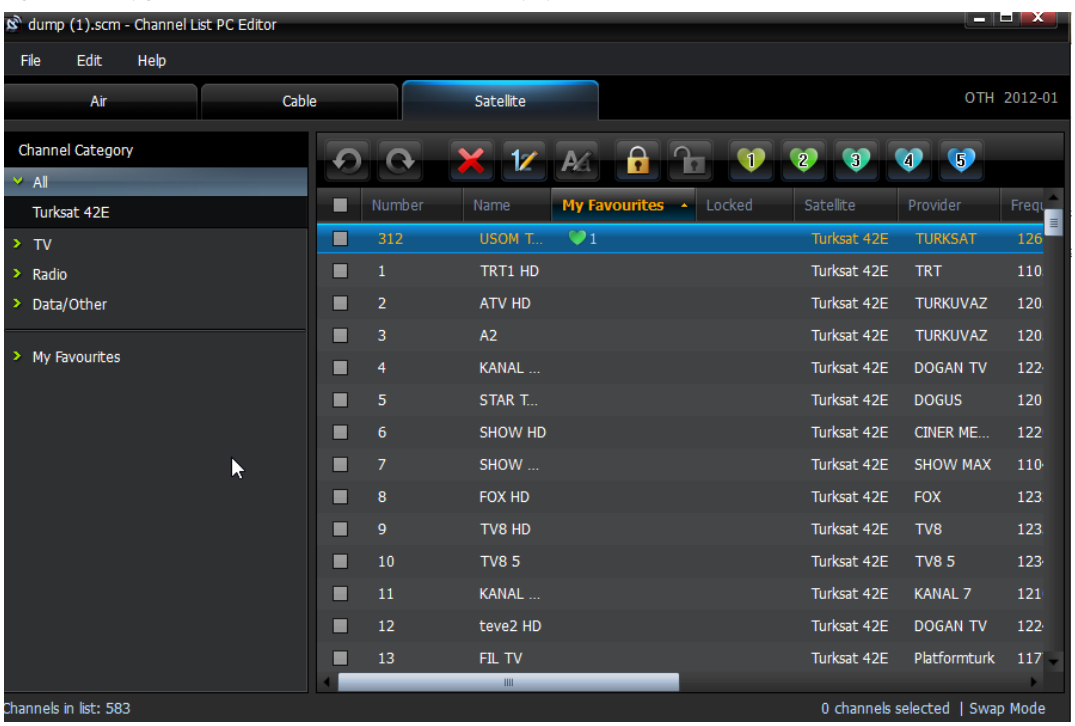


sairnedemis.png içerisine EXIFTool ile baktığımızda ZIP parolasını bulmuş oluyorduk. Dosyayı açtığımızda "hadibul.b64" dosyasını buluyorduk ve bu APK dosyasını çalıştırdığımızda karşımıza flag çıkıyordu.

Soru: Reklam arası bitti film başlıyor.



Göreve başladığımızda bize "dump.scm" adlı dosyayı veriyordu. .scm uzantılı dosyayı açmak için Google'da bir araştırma yaptığımızda uygun editörü bulup indirdik ve dosyayı açtık.

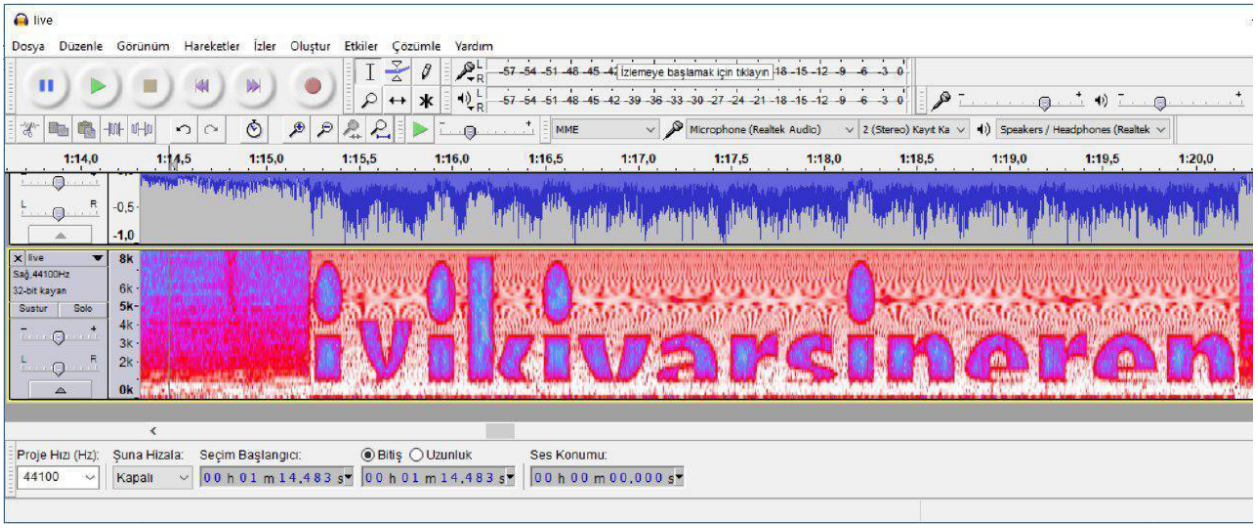


Karşımıza USOM TV çıkıyordu. Editörde bunu açtığınızda Yıldızlararası - Interstellar filminden bir sahne veriyordu. Bu kadar yorgunluğun üstüne oturup çok sevdiğim bu filmde o sahneyi izlemek şifa gibi geldi diyebilirim :) (Katıldığımız takımla söz verdik filmi tekrar CTF bitiminde izleyeceğiz diye).

Filmin bir yerinde MORS kodları vardı bu olabilir diye kağıt kalemi kaparak notlarımızı almaya başladık ama boşa çabalamıştık.

Videonun ilerleyen kısımlarında cızırtılı bir bozukluk vardı. Biz de voice dosyasını ayrıştırıp incelemeye karar verdik. Voice için forensic toollarından Audacity kullanarak incelemeye başladık.

Audacity açıldığında solda kısımda bulunan live'e tıklayıp split diyoruz ve bozuk kısmı incelemeye başlıyoruz. Ve bayrak "iyikivarsineren" diye çıkıyor. Bunu md5 encode olarak yazdığımızda ise bayrağı bulmuş olduk.



Soru: Karekod Okuyucu

Sayfada bir giriş ekranı ve kullanıcıları listeleyen bir kısım vardı. Kullanıcılara bakmak isteyince "sadece yöneticinin QR kodu kabul edilir" diyordu. Ben de hemen bir karekod oluşturdum ve içine metin olarak SQL Injection gömdüm ve PNG olarak kaydettim. Bu resmi siteye yüklediğimde işe yaramıştı.

Karşımıza şu şekilde bir metin çıkıyordu:

"1 admin 6b71dfdc4c5603272482f5b80db96a0a 5e14ce1f1fa3524ba07cb109549c594e"

MD5 decode edince parolanın "admin1234567890" olduğunu görüyorduk. Tekrar admin olarak giriş yaptığımızda ise bayrağı elde etmiş oluyorduk.

Soru: Kahramanmaraş dondurması sever misin?

Bu soruda yarışmacıyı bir oyun karşılıyordu. Bu oyun bitince

yenibasliyor.php?r=6FAD329DF3870D30696C93460EBB7C29_498D3C6BFA033F6DC1BE4FCC3C370AA7_

348DF46154717306D71E71C277E71082_

URL'ine gidiyordu. Dikkatimizi çeken oyun oynarken kontrol her zaman bizde değildi. Bilerek yanmaya çalışırsak kontrol elimizden gidip bizim kaybetmemize mani olmaya çalışıyordu. Bu sayfada bir şey var diyerek URL kısmına ve kaynak kodlarına baktık.

```
<!DOCTYPE html>
<html>

<head>
    <meta charset="utf-8" />
    <title>Oyun Zamanı</title>
    <style>* { padding: 0; margin: 0; } canvas { background: #eee; display: block; margin: 0 auto; }</style>

</head>

<body>

    <canvas id="myCanvas" width="480" height="320"></canvas>
    <script type="text/javascript" src="game/04.js"></script>
    <script>
        var _0x4082 = ['keydown', 'keyup',
            'mousemove', 'debugger',
            'constructor', 'apply',
            'return (function() ',
            '{}.constructor("return this")( )',
            'console', 'warn',
            'debug', 'info',
            'error', 'exception',
            'trace', 'log',
            'getElementById',
            'myCanvas', 'width',
            'keyCode', 'clientX',
            'offsetLeft', 'status',
            'location',
            'yenibasliyor.php?r=6FAD329DF3870D30696C93460EBB7C29_498D3C6BFA033F6DC1BE4FCC3C370AA7_348DF46154717306D71E71C277E71082_',
            'beginPath', 'arc',
            'fillStyle', '#0095DD',
            'fill', 'closePath',
            'rect', 'height',
            'font', '16px Arial',
            'fillText', 'Score: ',
            'clearRect', 'GAME OVER',
            'reload',
            'addEventListener'
        ];
        (function (_0x5729bc, _0x27cd87) {
            var _0x2b9b8d = function (_0x3548f7) {
                while (--_0x3548f7) {
                    _0x5729bc['push'](_0x5729bc['shift']());
```

Kaynak kodlarında ise HEX şeklinde olan çok fazla ifade vardı ancak bir script içine yazılmıştı. Hex to ASCII text yaptığımızda base64 encoded text görüyorduk bunu da decode ettiğimizde text halini alıyorduk. Tek tek elle bunları çevirmek çok zor olacağından bunun için script yazmakla uğraştık. Kaynak kodu elde etmiş olduk.

Found : **baglanti**
(hash = 6fad329df3870d30696c93460ebb7c29)

Found : **son**
(hash = 498d3c6bfa033f6dc1be4fcc3c370aa7)

Found : **1ekle**
(hash = 348df46154717306d71e71c277e71082)

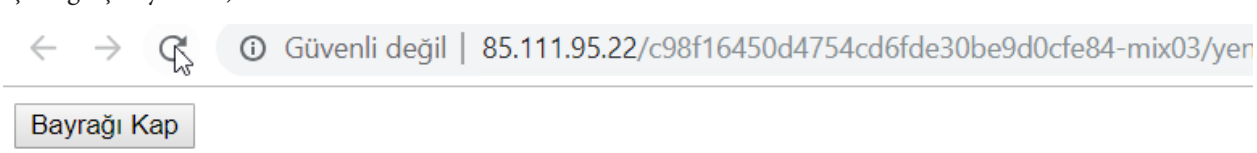
URL kısmında 3 tane MD5 ile encode edilmiş texti gördük ve decode ettik.

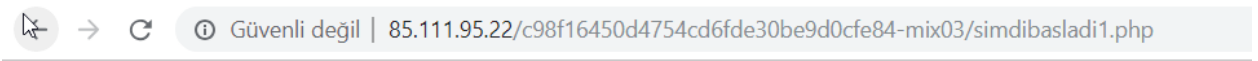
Daha sonra "1" in MD5 encode halini (C4CA4238A0B923820DCC509A6F75849B) alarak URL sonuna eklediğimizde:

yenibasliyor.php?r=6FAD329DF3870D30696C93460EBB7C29_

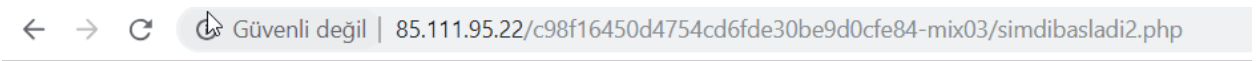
498D3C6BFA033F6DC1BE4FCC3C370AA7_348DF46154717306D71E71C277E71082_C4CA4238A0B923820D-CC509A6F75849B

URL'ini elde ettik. Bu URL'e gittiğimizde bizle biraz dalga geçerek ve sorunun isminin hakkını vererek dondurmayı almamız için uğraştırıyordu :)

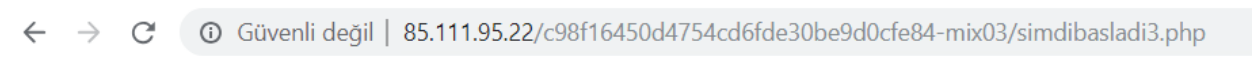




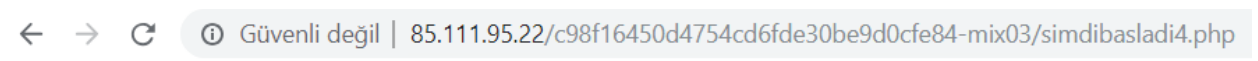
Hadi bakalım.



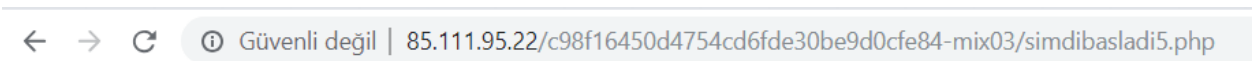
sonu yok bu gidisin



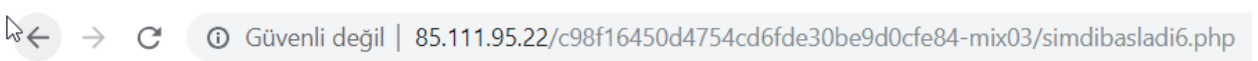
bence vazgec



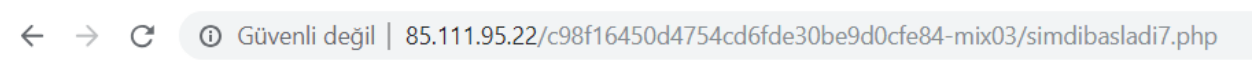
sonuna kadar ilerleyebilirim ?



vakit varken bırak bu işleri

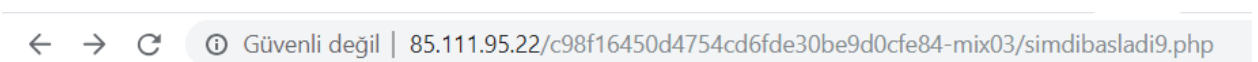


benim limitim max url karakter sayısı kadar !

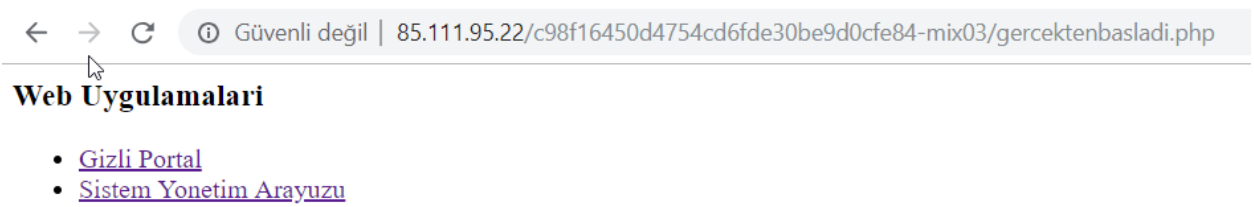


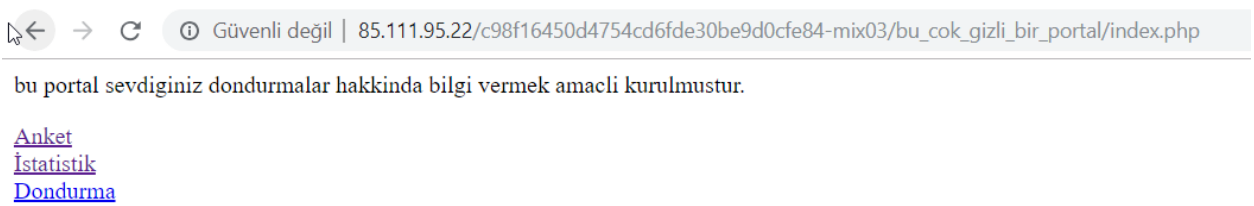
pof, senle ugrasmak zaman kaybi.

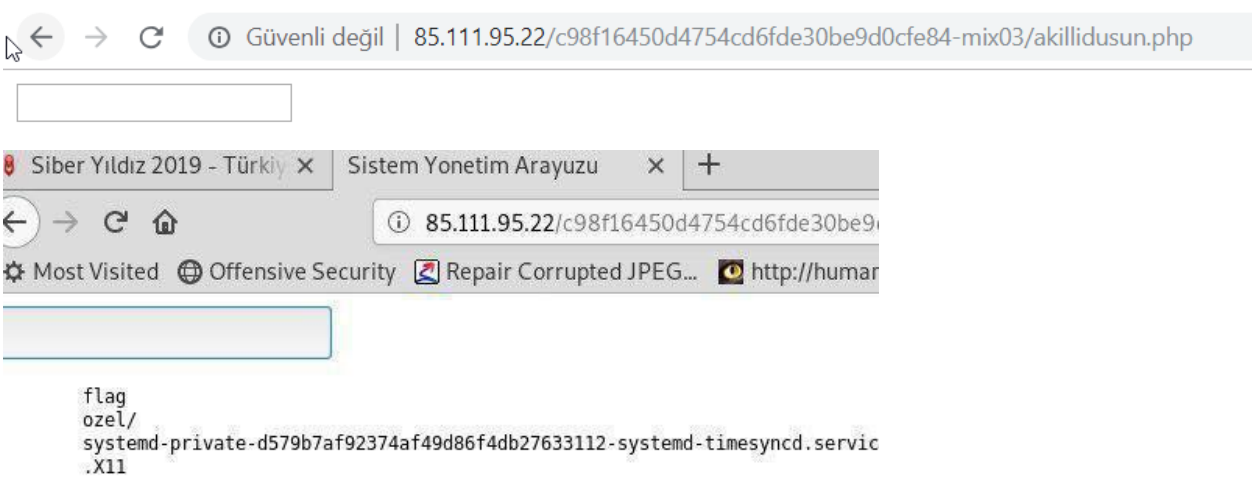
404 Not Found



Buradan devam et.







Sayfalarda gezindikten sonra komut çalıştırabileceğimiz bir yer bulduk. Burada bir textbox vardı, ve "ls" komutu çalıştırabiliyorduk. "ls /tmp" diyince flag ve ozel/ dosyalarının listelendiğini gördük. Evet çok yaklaştık diye heyecanlanmışken cat komutu ile "cat /tmp/flag" dosyasını okuyamadığımızı farkettik. Sadece bir dosya okunur cevabı alıyorduk. "ls /tmp" yapmamıza dahi izin yoktu. Maalesef bu soruyu çözemeden süremiz doldu.

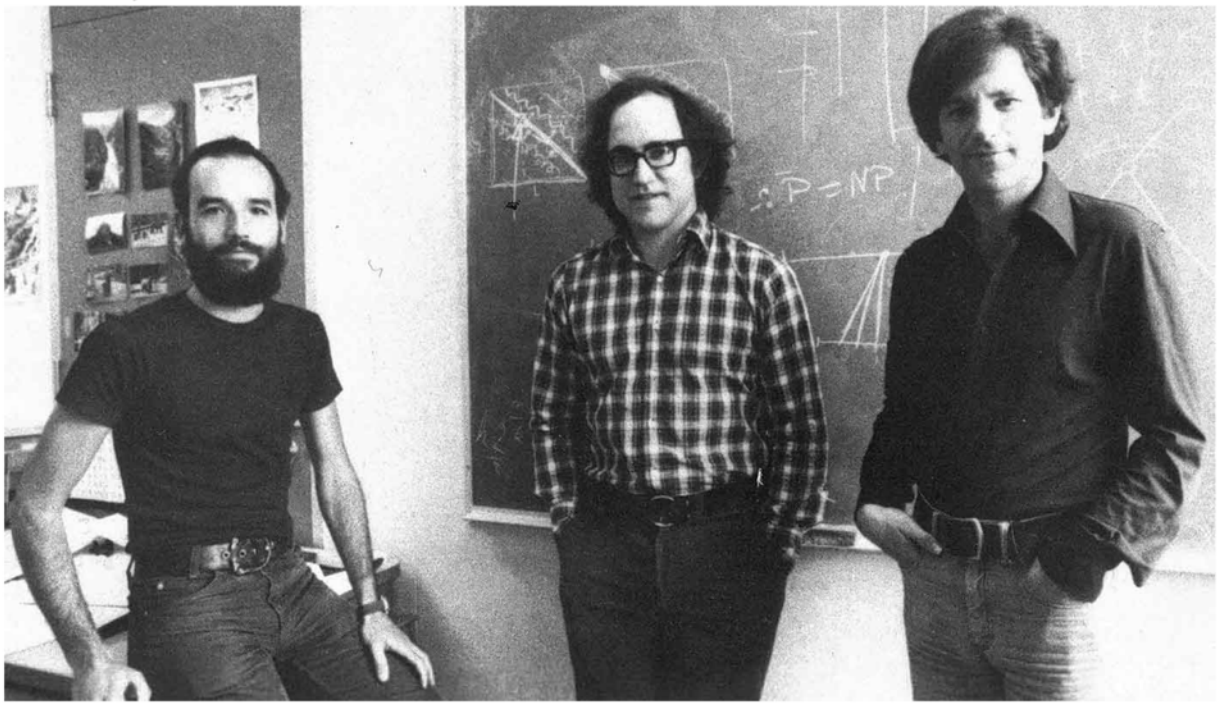
Bayram Gök – bayram@arkakapidergi.com

Sayısal Sırdaşımız RSA

"The enemy knows the system"
Claude Shannon

RSA nedir ne değildir? Baştan peşinen söyleyelim bir yazılım diline ait kod parçası değildir. RSA matematiğin dili ile ifade edilmiş Leonhard [1] Euler'in teoremine dayanan eşitliklerdir. Bizler, yazılımcılar matematik diliyle yazılmış eşitlikleri bilgisayar diline tercüme eden aracılarız. RSA algoritmasını kırmak, saldırıda bulunmak, açığını aramak ile uğraşırken de bunu matematik dili ile ifade etmeliyiz. Bilgisayar diline yapılan tercüme esnasında yazılımcıdan, yazılımdan, donanımdan kaynaklanan zafiyetler RSA'nın haklı ününe zarar getirmez. RSA algoritmasını Qbasic, C#,Java, Python gibi herhangi bir yazılım dili ile uygulayabilirsiniz. Algoritmanın güvenilirliği yazılım kodundan tamamen bağımsızdır.

Bu yazımız RSA tarihçesi ile ilgili değil. Bu konuda yeterince kaynak bulunabiliyor. Teorisi, matematiği ve uygulaması konusunda derli toplu Türkçe bir doküman oluşturmayı amaçladım. RSA Kriptoloji bilimi tarafından Asimetrik şifreleme sınıfında tanımlanır. Arka kapı dergi 6. Sayısında konuyla ilgili bilgiler bulabilirsiniz. 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir. Algoritma geliştiricilerinin isimlerin ilk harflerinden oluşan kısaltma ile adlandırılmıştır.



Görsel 1 soldan sağa efsanenin üçlüsü Adi Shamir , Ron Rivest , Leonard Adleman

RSA Algoritmasının Euler Teoremine göre ispatı

RSA algoritmasının matematik dili ne söyler, ispatı nasıl yapılır? Bu sorularımızı Arka Kapı Dergi yazarlarımızdan *Halit İnce* hocamız bizim için cevapladı. Algoritmanın Matematik dili şu an benim için gerekli değil diyorsanız bu ispatı okumadan da devam edebilirsiniz.

Euler Teoremi: a herhangi bir tamsayı ve n, a ile aralarında asal bir tamsayı ise $a^{\varphi(n)} = 1(mod\ n)$ eşitliği sağlanır.(yazının ilerleyen bölümlerinde c şifreli metni, m açık metni, n anahtarı $\varphi(n)$ phi sayısını e ve d sayıları üs değerlerini göstermek üzere)

c^d m 'ye neden eşit çıkıyor?

$c^d = (m^e)^d = m^{ed} = m^{1+k\varphi(n)} = m.(m^{\varphi(n)})^k = m.1^k = m\ (mod\ n)$ ile m elde edilir.

6 tane eşitlik var. Her birini açıklayalım.

1. Eşitlik: Burada sadece c yerine m^e yazılmıştır. $c = m^e\ (mod\ n)$ olduğunu hatırlayalım.

2. Eşitlik: Açıktır.

3. Eşitlik: $ed = 1\ mod\ \varphi(n)$ olduğu için ed 'nin $\varphi(n)$ ye bölümünden kalan 1 ve bölüm k gibi herhangi bir tamsayıdır. Yani $ed = k\varphi(n) + 1$ olur. Bu eşitlikte bunu kullandık. Zaten ilk d'nin seçimi yapılırken de bu eşitlik böyle gelsin diye seçilmişti.

4. Eşitlik: Üslü sayı yeniden yazılmıştır.

5. Eşitlik: İki durum var:

Durum 1: m ile n aralarında asal ise; $m^{\varphi(n)} = 1\ (mod\ n)$ olduğu Euler teoreminden elde edilir ve 4. eşitlikte $m^{\varphi(n)}$ yerine 1 yazılır. m ile n nin aralarında asal olduğu için bu teoremi kullanabiliyoruz.

Durum 2: m ile n aralarında asal değil ise: O halde

$m.(m^{\varphi(n)})^k = m.(m^{(p-1)(q-1)})^k = m.(m^{(p-1)})^{(q-1)k} = m.(1)^{(q-1)k}\ mod\ p$

Son eşitlikte $m^{(p-1)} = 1\ mod\ p$ (Euler Teoremi) kullanıldı. $\varphi(p) = p - 1$ ve m ile p aralarında asal olduğunu gözlemleyin.

$m.(m^{\varphi(n)})^k = m.(m^{(p-1)(q-1)})^k = m.(m^{(q-1)})^{(p-1)k} = m.(1)^{(p-1)k}\ mod\ q$

Son eşitlikte $m^{(q-1)} = 1\ mod\ q$ (Euler Teoremi) kullanıldı. $\varphi(q) = q - 1$ ve m ile q aralarında asal olduğunu gözlemleyin.

Bu durumda $m.(m^{\varphi(n)})^k$ ifadesi hem $mod\ p$ ye göre 1, hem $mod\ q$ ya göre 1 çıktığı için,

$m.(m^{\varphi(n)})^k = 1\ mod(pq) = 1\ mod\ n$ olur.

Böylece 5. Eşitlikte her iki durumda da $m^{\varphi(n)}\ mod\ n$ yerine 1 yazabiliriz.

6. eşitlik: Açıktır.

O halde $c^d\ (mod\ n)$ işleminin sonucu her zaman m açık metnini verir.

İspatı Halit İnce hocamızın kaleminden verdikten sonra yazımıza kendi mecrasında devam edebiliriz. RSA algoritmasını uygulamada iki aşamada inceleyebiliriz. İlk aşama sistemde sürekli kullanılacak anahtarların oluşturulması, kurulum işlemidir. Bu işlemler bir defa yapılır ve oluşturulan anahtarlar kullanıldığı sürece tekrarlanmaz. İkinci aşama ise anahtarların şifreleme ve çözme işlemlerinde kullanıldığı rutin tekrarlayan işlemlerdir.

A- SİSTEMİN KURULMASI

Titizlikle uygulanması gereken 5 adımdan oluşur.

1- RSA algoritmasında Gizli (*private*) ve Açık (*public*) anahtar oluşturmanın ilk adımı iki tane rastgele sayı üretmektir. Bu sayıları seçerken uyulması gereken katı kurallar vardır. Çünkü bütün haberleşme ve veri gizliliğinizi sağlayan RSA algoritmasını bu katı kurallar güvenilir kılıyor.

Üreteceğimiz sayılar p ve q olsun

- p ve q rastgele seçilmelidir! Rastgele seçeceğiniz bu sayıları en küçük bir düzenle ilişkilendirirseniz saldırganlar bu fırsatı değerlendireceklerdir. Arka Kapı dergisi 6. sayısında yayınlanan "*Rastgele Sayılar Rastgele Olmayınca*" başlıklı yazısında Chris Stephenson hocamız rastgele sayı üretimi ve elde edilen sayı arasındaki ilgi bağının ne kadar tehlikeli olabileceğini gösterdi. Detayları yazısından okuyabilirsiniz.
- p ve q sayıları **kesinlikle** asal olmalıdır. RSA algoritmasında kullanılan matematik asal sayıların özellikleri üzerine oturtulmuştur. Olmazsa olmazdır. Ürettiğimiz her p ve q sayılarının asal sayı olduğunu mutlaka doğrulamamız gerekiyor. Asal olmayan p ve q sayıları kullanan sözde RSA ile gizlilik sağlayan uygulamalardan uzak durulmalıdır. Uygulamalar da bu hassasiyetin her zaman gösterilmediği hakkında araştırmalar var. Çünkü 1024, 2048, 4096 bit gibi büyük basamaklı sayılara asallık testi uygulamak ciddi bir donanım ve zaman maliyeti getiriyor. Asal sayıların tespitinde bilinen en eski yöntemlerden birisi Eratostenes Kalburu'dur [2]. Küçük sayılar için işe yarayabilecek bu yöntem devasa basamaklı sayılarda pek performanslı olmaz. Hantal kalır. Sayılar büyüdükçe asallık testlerinde karşılaşılan ciddi performans sorunlarına çözüm üretmek gerekir. Ticari odaklı hiçbir uygulama kullanıcıya fare imlecini birkaç saniyeden uzun süre kum saati simgesi halinde göstermek istemez. Bu yüzden büyük sayılarda asallık testlerine daha çok performans odaklı yaklaşılır. Basamak sayısı arttıkça bir sayının asal olmadığını kesinlikle söyleyebilen ama asal olduğunu kesinlikle ifade edemeyen yöntemler kullanılmaya başlanır. Uygulamamızda nispeten küçük sayılarla işlem yaptığımız için kesin sonuç üreten güvenilir Eratostenes Kalburu algoritmasını kullanacağız. Detayları da uygulama içerisinde bulabilirsiniz.

> **Asal Sayılar** [3]
> Okul günlerimizden kalan, zihnimizin bir köşesinde hemen hatırlanacak kadar taze duran "sadece kendisine ve 1'e kalansız bölünebilen pozitif tamsayılara asal sayı denir" tanımlamasını biliriz. Asal sayılara sayıların atomu da denir. Asal sayılar sonsuz sayılar kümesinin etliye sütlüye karışmayan, asosyal üyeleridir. Komşuluk ilişkileri yoktur. Sanki halk arasına karışmadan malikânesinde yaşayan gizemli oldukları düşünülen insanlara benzerler. Haklarında türlü türlü teoriler üretilir. {2,3,5,7,11,13,17,19...} gibi sonsuz sayıda asal sayı vardır.
>
> Arka Kapı Dergisi 3. Sayısında yayınlanan Halit İnce hocamızın "Asal Sayılar Üzerine" başlıklı yazısında asal sayılar üzerine detaylı bilgiler bulabilirsiniz.

- p ve q sayıları yakın uzunlukta (basamak sayısı) olmalıdır. RSA algoritmasını çözebilmenin tek yolu üretilen anahtarı çarpanlarına ayırmaktır. Şimdilik bildiğimiz tek yol budur. Şifreleme yöntemimizin güvenliği ve sağlamlığını arttırmak için kırıntı kadar da olsa her imkânı değerlendirmeliyiz.

> **Asal Çarpanlarına Ayırma**
> İki asal sayının çarpımı şeklinde yazılabilen sayılara **yarı asal** sayılar denir. Asal sayılar dışında kalan bütün pozitif sayılara da **bileşik sayı** denir. Bileşik sayılar ise kendilerinden daha küçük tamsayıların çarpımı şeklinde ifade edilebilirler. Asal çarpanlarına ayırma bir bileşik sayının, çarpıldıklarında yine aynı sayıyı verecek şekilde, bir ve kendisi dışındaki bölenlerine ayrılması işlemdir. Sayılar büyüdükçe çarpanlara ayırma işlemi de gittikçe zorlaşır. Her sayının çarpanlarına ayrılma zorluğu da aynı değildir. Yakın uzunlukta olan sayıları asal çarpanlarına ayırmak daha zordur. Rastgele ve yakın uzunlukta seçilmiş, oldukça büyük (ör: 1024 bit) asal çarpanları olan yarı asal sayıları çarpanlarına ayırmak şu anki teknolojik imkânlarla pek mümkün değil. En azından pratik değil. Halen çarpanları ayırma işlemini hızlandıracak bir algoritma da bulunamamıştır. Bir grup araştırmacı 2009 yılında 768 bitlik RSA anahtarını yüzlerce bilgisayarı kullanarak ancak 2 yılda çarpanlarına ayırabildiler [4].

- p ve q sayıları birbirlerine çok yakın da **olmamalıdır**. İleride göreceğimiz gibi anahtar, buna n sayısı diyelim, basit ve sade $n = p \times q$ ifadesi ile elde edilir. Emin olun saldırganın ilk deneyeceği yöntem $\sqrt{n}$ değerini bulup, yani anahtarın karekökünü alarak p ve q sayılarını bu değere yakın yerlerde aramak olacaktır. Bu sebeple p ve q sayıları asla bir birbirlerine çok yakın değerlerde üretilmemelidir. Günün teknolojik imkânları da dikkate alınarak deneme-yanılma saldırılarını boşa çıkaracak kadar iki sayı arasında yeterince büyük aralık bırakılmalıdır.
- p ve q sayıları arasında belirli bir ilişki, düzen **olmamalıdır**. Örneğin { 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377…} şöyle bir sayı kümesi verilse hemen "Bunlar Fibonacci sayıları. Çünkü Fibonacci sayı dizisinde her sayının değeri kendisinden önceki ardışık 2 sayının toplamına eşittir" diyeceğinizden eminim. Fibonacci sayıları belirli bir kurala göre hesaplanabilen sayılardır. Asal sayılar için Fibonacci sayılarına benzer ispatlanmış bir kural henüz bulunamamıştır. Bu kuralı siz bulursanız yaşınıza bakmadan önümüzdeki bir kaç dönemin Field Madalyalarını [5] size verirler. RSA da o zaman sizin yüzünüzden çöpe atılır, bu yazı da değerini yitirmiş olur. Ancak asal sayıların arasındaki ilişkiler üzerinde Riemann hipotezi [6]gibi ciddiye alınan ancak daha ispatı yapılamamış çalışmalar da vardır.
- p ve q sayıları gizli (*private*) sayılardır. Asla paylaşılmaz!

2- Tüm katı kuralları yerine getirerek ürettiğimiz p ve q sayılarını kullanarak şifreleme anahtarının oluşturulmasına geçebiliriz. n sayısı hem açık (*public*) hem de gizli (*private*) anahtarın bir parçası olmak üzere ; $n = p \times q$ 'dur. Hepimizin ilkokul yıllarından öğrendiği basit bir çarpma işlemi ile RSA anahtarımızın önemli bir parçasını hesaplamış olduk. Sadece sayılar çok büyük! n sayısının bit uzunluğu RSA algoritmasının anahtar basamak (ikili sistemde bit) uzunluğu olarak verilir. n sayısı gizli (*private*) anahtar ve açık (*public*) anahtar için modüler taban olarak kullanılır. Dikkatli bir okurumuzun aklına "p, q sayılarını üretmek için niye bu kadar uğraştık? Doğrudan çok büyük bir n sayısı üretebilirdik" sorusu geleceğinden eminim. Bu uğraşın birkaç sebebi var. Açıklayalım

Aritmetiğin Temel Teoremi [7]

Aritmetiğin Temel Teoremi şunu söyler: 1'den büyük her doğal sayı ***sonlu*** *sayıda asal sayının çarpımı şeklinde yazılabilir. Sayıların yer değiştirmesi dikkate alınmazsa bu çarpım* ***tektir****. Basitçe ifade etmeye çalışalım. .* a *ve* b *sayıları asal olsun.* $c = a \times b$ veya $c = b \times a$ *dizilişi dışında çarpımları* c *sayısını verecek başka asal sayılar grubu yoktur*[8].

p, q asal sayılarını kendimiz belirlediğimiz için n sayısının asal çarpanlarını da biz belirlemiş oluyoruz. Saldırganı katı kurallar ile belirlediğimiz iki adet asal sayı bulmaya zorluyoruz. İşini zorlaştırıyoruz. Atalar sözümüz ile tanımlarsak saldırgana " Samanlıkta iğne" aratıyoruz. **Çünkü n sayısı herkese açık (*public*) bir sayıdır.** RSA algoritmasının can damarıdır. Düşman sistemi biliyorsa anahtarı iyi korumalısınız. Kanımca Kriptoloji de paranoyak olmak sağlık belirtisidir, işinizi titizlikle yaptığınızı gösterir.

p, q asal sayılarını kendimizin üretmesinin bir diğer faydası ise sonraki adımda *Totient*, kısaca $\varphi(n)$ yada *phi* sayısını hesaplarken kolaylık sağlıyor olmasıdır. n sayısını doğrudan üretseydik $\varphi(n)$ sayısını üretmekte çok zorlanırdık. Şöyle ki : $\varphi(n)$ sayısını bulabilmek için 1'den n sayısına kadar her sayıyı n ile aralarında asal mı diye kontrol etmemiz gerekecekti. Bu işlem 300 basamaklı bir sayıyı asal çarpanlarına ayırmak gibi zorlu bir yazılım süreci olacaktı.

3- n sayısını hesapladıktan işlem sırası $\varphi(n)$ değerini bulmaya geldi. $\varphi(n)$ sayısı gizli (*private*) bir sayıdır. Asla paylaşılmaz.

Totient[9] , kısaca φ, sayılar teorisinde, bir tam sayının o sayıdan daha küçük ve o sayı ile aralarında asal olan sayma sayıları sayısını (adedini) bulan fonksiyondur. İsviçreli matematikçi *Leonhard Euler* tarafından geliştirilmiştir.

Örneğin $\varphi(20) = 8$ 'dir. 20 sayısı ile aralarında asal bu sayıların listesi { 1,3,7,9,11,13,17,19}'dur ve 8 adettir.

- Örneğin $\varphi(23) = 22$ 'dir.Çünkü 23 bir asal sayıdır. Dolayısıyla 23 sayısı ile aralarında asal kendinden küçük 22 adet sayma sayısı vardır. O halde x bir asal sayı olmak üzere $\varphi(x) = x - 1$eşitliği de doğrudur.
- Eğer x ve y aralarında asal sayılar ise Totient fonksiyonunun çarpım özelliği de vardır : $\varphi(xy) = \varphi(x) \times \varphi(y)$ifadesi doğrudur.

Kendi ürettiğimiz p ve q sayıları birer asal sayı oldukları için kendi aralarında da asaldırlar. Verdiğimiz iki örnekten faydalanarak:

$\varphi(p) = p - 1$ ve $\varphi(q) = q - 1$ $yazabiliriz.$

$n = p \times q$ olduğundan Totient fonksiyonunun çarpım özelliği gereği $\varphi(n) = \varphi(p) \times \varphi(q)$ olur.

Buradan $\varphi(n) = (p - 1) \times (q - 1)$

4- Sıradaki işlem $1 < e < \varphi(n)$ ve obeb$(e, \varphi(n)) = 1$ koşullarını sağlayan e sayısının rastgele hesaplanması veya belirlenmesini gerektiriyor. e sayısı açık (*public*) anahtarın üs değeri olarak kullanıldığı için herkese açık bir veridir.

$1 < e < \varphi(n)$ aralığında rastgele bir sayı üretip e sayısı olarak kullanılabilir. Üretilen e ayısı $\varphi(n)$ sayısı ile aralarında asal olmak zorundadır. İki sayının aralarında asal olabilmesi için en büyük ortak bölenlerinin 1 olması gerekir. ebob$(e, \varphi(n)) = 1$ olmalıdır.

En Büyük Ortak Bölen - ebob(Greatest Common Divisor-gcd) [10] [11] [12]

Bu algoritma bulan matematikçi Öklid'in adıyla bilinir. Muhtemelen bir inşaat sorununa çözüm bulmak amacıyla geliştirmiş. Şöyle ki: Mutfağınıza güzel seramikler döşetmek istiyorsunuz diyelim. Bu yöntemle mutfağınızın enine ve boyuna tam adette sığacak karoların bir kenarının uzunluğunu hesaplayabilirsiniz. Böylece yarım karolar göz zevkinizi bozmaz. Wikipedia sayfasında güzel bir animasyon var, izleyiniz.

$1 < b < a$ *iki pozitif tamsayı olsun. Hem* a *hem* b *sayılarını bölen en büyük sayıyı hesaplayabiliriz.* a *bölünen,* b *bölen,* q *bölüm,* r *kalan olmak üzere* $\frac{a}{b}$ $bölme\ işlemini\ a = bq + r$ *şeklinde yazabiliriz.* b*'yi eşitlikten çekersek*

$a = bq_1 + r_1$
$b = r_1q_2 + r_2$
$r_1 = r_2q_3 + r_3$

ve işlemi tekrarlayarak kalan 0 (sıfır) oluncaya kadar devam ederiz. $ebob(a, b)$*sıfırdan farklı son kalandır. Basitçe* a*'yı* b*' ye bölerek ve tekrar tekrar her kalanı, sıfır kalan elde edene kadar bölünene bölerek işlemi yineleriz. Kısaca* $ebob(a, b)$ *- ing* $gcd(a, b)$*- şeklinde gösterilir.*

Ör: $ebob(8,23) = ?$
$23 = 8(2) + 7$
$8 = 7(1) + 1$
$7 = 1(7) + 0$
$ebob(8,23) = 1$

not: Parantez içindeki rakamlar çarpandır.

Eğer rastgele sayı üretmek istemiyorsanız obeb$(e, \varphi(n)) = 1$ koşulunu sağlayan yani $\varphi(n)$ ile aralarında asal olan sayıları e sayısı olarak seçebilirsiniz. Hamming ağırlığı düşük (Hamming ağırlığı bir dizi içerisinde geçen sıfırdan farklı sembollerin sayısını gösterir. Ör: 1101101110100 için Hamming ağırlığı=8'dir) ve küçük değerli (ör: 65537 = 0001000000000000001, Hamming ağırlığı=2) sayıları seçmek verimlidir. Ancak çok küçük (Ör:3) sayıların seçilmesinin güvenlik sorunları oluşturduğu gözlenmiştir.

5- $d \times e \equiv 1\ mod\ \varphi(n)$ denkliği ile d sayısı hesaplanır.

d sayısını kendimiz **belirleyemeyiz**. Verilen denkliği sağlamak zorunda olduğundan hesaplanarak bulunması gerekiyor. Yapmamız gereken e sayısının $mod\ \varphi(n)$ 'e göre tersini hesaplamaktır. Bu ifadeyi " $(d \times e)$ işlemi sonucunun $\varphi(n)$tabanına göre mod değeri 1 olmalıdır" şeklinde okuyabiliriz. Benim gibi matematiğe ihtiyaç duydukça başvuranlar için bu daha kolay idrak edilebilen bir yaklaşım. Basit yol gayet açıktır. e ve $\varphi(n)$ sayılarının değerlerini bildiğimize göre 1'den başlayarak d

sayısına sırayla 1 artan değer verir ve sonucu hesaplarız. Denediğimiz d sayısı denkliği sağlayıncaya kadar bu döngüye devam ederiz. e sayısı ne kadar küçük olursa ve $\varphi(n)$ sayısı ne kadar büyük olursa – zaten koskocaman – çok sabırlı olmalıyız. Çünkü bu döngü sonsuza kadar sürebilir. Üstelik e ve $\varphi(n)$ aralarında asal oldukları için maalesef ortak bölenleri de yoktur. Neyse ki büyük sayılarda Öklid algoritmasının değiştirilmiş bir hali d sayısını makul bir sürede hesaplamamıza olanak veriyor. e ve $\varphi(n)$ aralarında asalsa modüler ters vardır ve hesaplanabilir.

Genişletilmiş Öklid Algoritması [13]

Aralarında asal olan sayıların modüler aritmetikte çarpımsal ters alma işlemini yapmak için Öklid Algoritmasından yararlanabiliyoruz. Öklid algoritması tersten işletildiğinde modüler aritmetikte çarpımsal ters alma işlemini gerçekleştirebiliyor. Biraz karışık, otomobili geri viteste kullanmaya benziyor. Ama zor değil!

$0 < b < a$ iki pozitif tamsayı olsun. a bölünen, b bölen, q bölüm, r kalan olmak üzere standart Öklid algoritmasında $a = bq + r$ şeklinde yazmıştık. Bu sefer eşitlikten kalanı yani r'yi çekersek

$a = bq_1 + r_1 \quad \rightarrow \quad r_1 = a - bq_1$

$b = r_1q_2 + r_2 \quad \rightarrow \quad r_2 = b - r_1q_2$

$r_1 = r_2q_3 + r_3 \quad \rightarrow \quad r_3 = r_1 - r_2q_3$

sağ taraftaki eşitlikleri elde ederiz. Bu işleme kalan 0 oluncaya kadar devam edilir.

Varsayalım ki obeb - obeb değeri kalanın 0 olduğu işlemden önceki eşitlikteki kalandır. Algoritma bu eşitlikten geriye doğru işletilmelidir - değerini elde ettiğimiz adım $r_3 = r_1 - r_2q_3$ olsun. Eşitlikteki r_2 değeri yerine bir önceki $r_2 = b - r_1q_2$ eşitliği koyarsak $r_3 = r_1 - (b - r_1q_2)q_3$ elde ederiz. Böylece en sondan en başa doğru kalan ifadelerini yerine koymaya devam eder, sadeleştirme işlemleri yaparsak $r_n = ax + by$ eşitliğine ulaşırız.

Özel olarak ebob$(a, b) = 1$, a ve b sayısı aralarında asal olduğu koşulda $1 \equiv by \bmod a$ denkliğini sağlar. y' ye $mod\ a$ 'nın çarpımsal tersi denir.

Ör: $1 = 8x + 23y$
1. adım ebob(8,23) değerini hesaplıyoruz.
$23 = 8(2) + 7 \rightarrow 7 = 23 - 8(2)$
$8 = 7(1) + 1 \rightarrow 1 = 8 - 7(1)$
$7 = 1(7) + 0 \rightarrow 0 = 7 - 1(7)$

2. adımda obeb değerini bulduğumuz adımdan geriye doğru algoritmayı uyguluyoruz. Çarpanları parantez içinde yazıp, çarpım işlemlerini yapmayarak, çarpanları toplayıp 8 ve 23 sayılarını elde etmeyi amaçlamalıyız.

$1 = 8(1) - 7(1)$
$1 = 8(1) - (23 - 8(2))(1)$
$1 = 8(1) - 23 + 8(2)$
$1 = 8(3) - 23(1)$
$\Rightarrow x = 3, y = -1$

Hangi sayının modüler tersi aranıyorsa o sayının yanındaki çarpan kendisinin tersi olur. Örneğimizdeki sayılar $e = 8$ ve $\varphi(n) = 23$ olsaydı. e sayısının tersini aradığımız için 8 sayısının yanındaki çarpanı alıp $d = 3$ diyecektik. d sayısını negatif bulduğumuz durumlarda $d = \varphi(n) + (-d)$ işlemini yaparız.
Ör çarpan -1olsaydı $d = 23 + (-1), d = 3$ bulunurdu.

Kolayladık, derin bir nefes alabiliriz.

B- MESAJ ŞİFRELEME ve ÇÖZME İŞLEMLERİ

1- Mesaj Şifreleme

Şifreleme işlemi yapmadan önce mesajı ulaştırmak istediğimiz kişi veya kurumun açık (*public*) anahtarı olan (e, n) çiftini bilmeliyiz. Sonraki işlem ise göndereceğimiz mesaja ait verilerin tam sayıya çevrilmesi gerekiyor. Göndereceğimiz mesaj bir metin içeriyorsa, metnin her harfi ASCII veya UTF (Unicode Transformation Format) gibi bir standarda ait tam sayı karşılığının değerine çevrilmelidir. Örneğin büyük A harfinin ASCII tablosundaki karşılığı 65'dir.Mesaj verileri zaten tamsayılardan oluşuyorsa doğrudan şifreleyebilirsiniz. Şifreleme işlemi yapılmadan önce dolgu şemalarından faydalanarak düz metin ataklarına karşı ek önlemler alınır. Örneğimizde dolgu işlemini uygulamayacağız.

c şifrelenmiş sayı, $0 \leq m < n$ olmak üzere mesajın şifrelemesi basit $c = m^e \ (mod\ n)$ işlemi ile yapılır. Bu işlemde karşılaşılacak teknik zorluk yine büyük sayılar ve büyük sayılarla üs alma işlemidir. m sayısı küçük olsa bile e sayısı onlarca basamaklı bir sayı olabilir. Küçük de olsa bir sayıyı milyonlarca, milyarlarca kez kendisiyle çarpmak maliyetli bir iştir. Üstelik üs alma işlemi sonucunda elde edilen sayıda binlerce basamaklı olabiliyor. Pahalı donanımlara ihtiyaç vardır. Üstelik bu işlemi mesaja ait her birim tamsayı için yapacaksanız daha çok pahalı donanımlara ihtiyaç vardır. Üs alma işlemini hızlandıran klasik çarpma işleminden farklı yöntemler uygulanır.

Modüler üs alma - ikili üs alma metodu

Kendimize şunu soralım : $A^x \ mod\ C$'yi x'in değeri 2'nin kuvveti { 1,2,4,8,16,32..} olmak koşulu ile nasıl hesaplarız? Hızlıda olsun!

Modüler Aritmetikte çarpma işleminin
$(A \times B)\ mod\ C = (A\ mod\ C \times B\ mod\ C)\ mod\ C$ özelliğinden faydalanarak $A^2\ mod\ C$ 'yi $A^2\ mod\ C = (A\ mod\ C \times A\ mod\ C)\ mod\ C$ halinde yazabiliriz. A Sayısının üs değeri 2'nin kuvvetidir.

Ör : 5^4 mod 11 değerini hesaplayalım.
1-) $5^1 \bmod 11 = 5$
2-) $5^2 \bmod 11 = (5^1 \bmod 11 \times 5^1 \bmod 11) \bmod 11$
3-) Önceki bulduğumuz $5^1 \bmod 11 = 5$ değerini kullanarak
$5^2 \bmod 11 = (5 \times 5) \bmod 11 = 3$
4-) $5^4 \bmod 11 = (5^2 \bmod 11 \times 5^2 \bmod 11) \bmod 11$
5-) Önceki bulduğumuz $5^2 \bmod 11$ değerini kullanarak
$5^4 \bmod 11 = (3 \times 3) \bmod 11 = 9$
6-) Sağlamasını yapalım $5^4 = 625 \Rightarrow 625\ mod\ 11 = 9$'dur

Bu metot gayet basit ve hızlı görünüyor. Peki, A^x mod C'yi x'in değeri 2'nin kuvveti olmadığı zaman nasıl hesaplayacağız? İşimiz biraz uzuyor ama çaresiz değiliz. Üs değeri x'i ikilik (binary) sayı tabanında yazacağız

Ör : 5^{23} mod 11 değerini hesaplayalım.

Üs değerini ikilik sayı tabanında yazalım $23 = 00010111 = (2^0 + 2^1 + 2^2 + 2^4)$
$5^{23} \bmod 11 = 5^{(1+2+4+16)} \bmod 11 = (5^0 \times 5^1 \times 5^2 \times 5^4) \bmod 11$
Önceki örneğimizde $5^1, 5^2, 5^4$ değerlerini hesaplamıştık. Kaldığımız yerden devam edelim
1-) $5^8 \bmod 11 = (5^4 \bmod 11 \times 5^4 \bmod 11) \bmod 11$
2-) Önceki örneğimizde bulduğumuz5^4 mod 11 değerini kullanalım
$5^8\ mod\ 11 = (9 \times 9)\ mod\ 11 = 4$
3-)$5^{16}\ mod\ 11 = (5^8\ mod\ 11 \times 5^8\ mod\ 11)\ mod\ 11$
4-) Önceki örneğimizde bulduğumuz$5^8\ mod\ 11$ değerini kullanalım
$5^{16}\ mod\ 11 = (4 \times 4)\ mod\ 11 = 5$
5-) Hesaplanan değerleri yerine koyalım
$5^{23}\ mod\ 11 = 5^{(1+2+4+16)}\ mod\ 11 = (5 \times 3 \times 9 \times 5)\ mod\ 11$
$5^{23}\ mod\ 11 = 4$

2- Mesaj Çözme

Şifrelenmiş mesajı çözme işlemi aynı şifreleme işlemine benziyor. Tek farkı şifreli mesajı çözmek için anahtarın gizli (*private*) (d,n) çiftini kullanmamız gerekiyor. m çözülmüş sayı, c şifreli sayı $0 \leq c < n$ olmak üzere mesajın çözülmesi $m = c^d \ (mod\ n)$ işlemi ile yapılır. Bu işlem şifreli mesaja ait tüm tamsayı sayılar için gerçekleştirilir. Sonraki işlem ise gelen mesaja ait veriler bir metin içeriyorsa, çözülen her sayı ASCII veya UTF (Unicode Transformation Format) gibi bir standarda ait tablodan harf karşılığına çevrilmelidir. Veya alınan veri bir dosyaya kaydedilip dosya formatını tanıyan program aracılığı işlenebilir.

Örnek şifreleme ve çözme işlemi

Örneğimizi basit ve anlaşılır kılmak için küçük sayılar ile çalışacağız. Daha büyük sayılarla denemeler yapmak için için uygulamayı indirebilirsiniz.

1. $p = 47$, $q = 83$ asal sayıları olsun.
2. $n = p \times q$ eşitliğiniz kullanarak $n = 47 \times 83 = 3901$ sayısını hesaplarız
3. $\varphi(n) = (p-1) \times (q-1)$ eşitliğini kullanarak $\varphi(n) = (47-1) \times (83-1) = 3772$
4. $\varphi(n)$ ve e sayıları aralarında asal olmalıdır. O yüzden $e = 5$ asal sayısı olsun. obeb testi yapmamıza gerek kalmaz.
5. $d \times e \equiv 1\ mod\ \varphi(n)$ denkliği ile d sayısı hesaplanır. $d \times 5 \equiv 1\ mod\ 3772$ d =?
   Önce Öklid algoritması ile obeb bulalım
   $1 = 5x + 3772y$
   $3772 = 5(754) + 2 \rightarrow 2 = 3772 - 5(754)$
   $5 = 2(2) + 1 \rightarrow 1 = 5 - 2(2)$
   $2 = 1(2) + 0 \rightarrow 0 = 2 - 1(2)$

   $1 = 5 - 2(2)$
   $1 = 5 - \big(3772 - 5(754)\big)(2)$
   $1 = 5 - \big(3772 - 5(1508)\big)$
   $1 = 5(1509) - 3772(1)$
   e yani 5 sayısının yanındaki çarpan ile ilgileniyoruz. Pozitif olduğu için doğrudan kullanıyoruz $d = 1509$

Hesaplamalar sonucunda açık (*public*) anahtarımız $(e,n) = (5,3901)$ ve gizli (private) anahtarımız $(d,n)(1509,3901)$ ortaya çıkar. Hemen deneyelim. Yazının yazıldığı güne atıfta bulunalım. Şifreleyeceğimiz metnimiz "**ÇANAKKALE GEÇİLMEZ**" olsun.

1- RSA algoritması ile şifreleyebilmek için metni ASCII tablosunu kullanarak sayı dizisine çeviriyoruz.

Tablodan "Ç" harfi yerine 195 yazıyoruz. Metnin her harfini bu işlemden geçirip, hazırlığımızı bitiriyoruz. "ÇANAKKALE GEÇİLMEZ" ASCII karşılığı 195, 135, 065, 078, 065, 075, 075, 065, 076, 069, 032, 071, 069, 195, 135, 196, 176, 076, 077, 069, 090 sayılar dizisidir

2- Açık anahtarı $(e,n) = (5,3901)$ kullanarak her sayıya $c = m^e \ (mod\ N)$ işlemini uyguluyoruz. İlk sayımız "Ç" harfi karşılığı olan 195

$c = 195^5 \ (mod\ 3901) = 281950621875 \ (mod\ 3901) = 3177, c = 3177$

Açık anahtarımızla şifrelenmiş "Ç" harfinin karşılığı 3177 sayısıdır. İşlemi dizideki diğer sayılara uyguluyoruz

Tüm işlemlerimizi bitirdiğimizde {3177, 1201, 0491, 1357, 0591, 2258, 2258, 0591, 0208, 3419, 1931, 1247, 3419, 3177, 1201, 2829, 1396, 0208, 1188, 3419, 3112} sayı dizisi oluşur. Bu dizi metnimizin şifrelenmiş halidir.

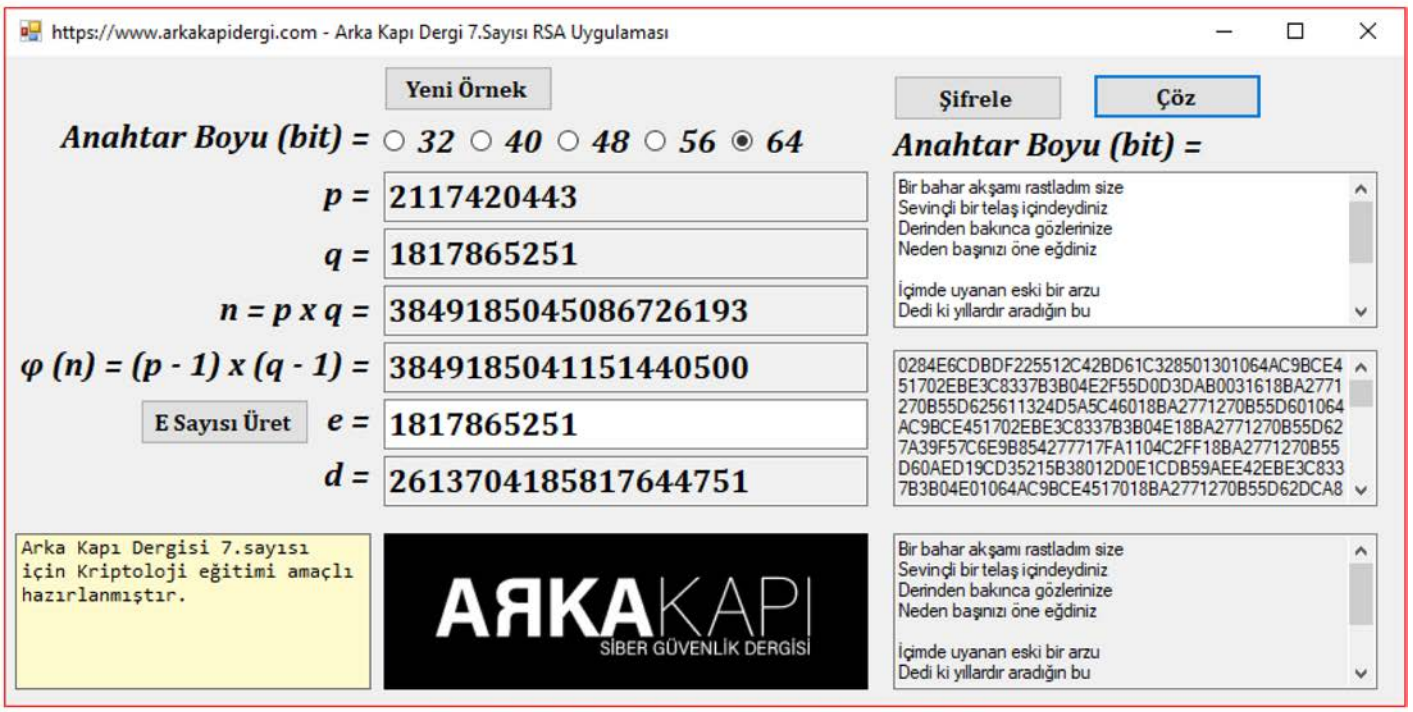
3- Gizli anahtarı $(d, n) = (1509,3901)$ kullanarak her sayıya $m = c^d \ (mod\ N)$ işlemini uyguluyoruz. İlk çözeceğimiz sayı 3177 'dir

$m = 3177^{1509}\ (mod\ 3901) = 34 \ldots . (mod\ 3901) = 195$

3177^{1509} İşleminin sonucu tam 5285 basamaklı bir sayıdır. Derginin yaklaşık tam bir sayfasını dolduracağı için yazamadım. Bu sayıyı görmek isteyen okurlarımız çok büyük sayılarla işlem yapabileceğiniz https://defuse.ca/big-number-calculator.htm [14] çevrimiçi hesap makinesini kullanabilirler. İfade (expression) kısmına **3177^1509%3901** formülünü girip sonucu inceleyiniz. Elde ettiğimiz 195 sayısının ASCII tablosundaki karşılığı "Ç" harfidir. Kendinizi sınamak için {3177, 1201, 0491, 1357, 0591, 2258, 2258, 0591, 0208, 3419, 1931, 1247, 3419, 3177, 1201, 2829, 1396, 0208, 1188, 3419, 3112} şifreli sayı dizisinin diğer elemanlarını kendiniz çözünüz.

Son Söz

Aklınıza şu soru gelebilir, gelmelidir de " *Büyük sayıları asal çarpanlarına ayırmanın zorluğu nasıl oluyor da RSA algoritmasını koruyor? RSA'nın zayıf yönü aynı zamanda neden çarpanlarına ayırma işlemidir* ?" Artık RSA nedir diye öğrendiğinize göre ürettiğimiz p, q asal sayılarından $n = p \times q$ ve $\varphi(n) = (p-1) \times (q-1)$ eşitlikleri ile n *ve* $\varphi(n)$ sayılarını hesapladığımızı hatırlayanız. Zaten (e, n) sayıları açık anahtar, herkes tarafından bilinen sayılar. Asıl gizliliği sağlayan ve şifreli mesajları çözen ise $d \times e \equiv 1\ mod\ \varphi(n)$ eşitliği ile hesapladığımız d sayısıdır. Eğer saldırgan $n = p \times q$ eşitliğindeki p, q sayılarını, n sayısını asal çarpanlarına ayırmayı başarıp p, q sayılarını elde edebilirse, $\varphi(n) = (p-1) \times (q-1)$ sayısını ve ardından e sayısının $mod\ \varphi(n)$ 'ye göre tersini alıp d sayısını hesapladığımız gibi d sayısını hesaplaması çok kolay olur. Sonrada orta şekerli kahvesi eşliğinde zevkle mesajlarımızı okuyacaktır. Bu zevki ona yaşatmak istemeyiz değil mi !?



Görsel 2 Örnek uygulama ekran görüntüsü

Örnek uygulama VS2012 C# dili ile yazıldı. İnternetteki kaynaklardan oldukça faydalandım. Dünyayı yeniden keşfetmek zorunda değiliz. Ama olanı da anlamak gibi bir zorunluluğumuz var. Bu uygulama profesyonel olmaktan uzak, yazı içeriği ile uyumlu eğitim amacıyla hazırlanmıştır. NET mimarisi içerisinde kullanıma hazır RSA ve Kriptoloji sınıfları vardır.Doğrudan bu sınıfları kullanarak daha performanslı ve birkaç satır koda sahip şifreleme uygulaması yazmanız mümkündür. Uygulama içerisinde rastgele sayı üreteci ve diğer bazı yordamlar 64 bitlik tam sayı ile sınırlandırılmıştır. Kendiniz bu sınırlandırmayı kaldırıp, veri tipilerini *Biginteger* sınıfına uyarlayabilir ve daha yüksek (1024 bit) basamaklı anahtarlar ile şifreleme yapabilirsiniz. Ancak daha yüksek basamaklık anahtarlar ile işlem yapabilmek için asal sayı testinin daha performanslı bir yöntem ile değiştirilmesi önerilir.

Yazının yayına hazırlanmasında düzelti, öneri ve katkıları için Halit İnce hocamıza teşekkür ederim. Birinci sayıdan itibaren Kriptoloji serisi haline gelen yazıları kesintisiz Arka Kapı dersinde yer veren dergi yönetimine minnettarım.

---

[1] www.wikipedia.org , "Leonhard Euler" , https://tr.wikipedia.org/wiki/Leonhard_Euler
[2] www.wikipedia.org , "Eratosten kalburu" , https://tr.0wikipedia.org/wiki/Eratosten_kalburu
[3] www.wikipedia.org , "Asal Sayı" , https://tr.0wikipedia.org/wiki/Asal_sayı
[4] "Factorization of a 768-bit RSA modulus", https://eprint.iacr.org/2010/006.pdf
[5] www.wikipedia.org , "Fields Madalyası" , https://tr.0wikipedia.org/wiki/Fields_Madalyası
[6] www.wikipedia.org , "Riemann hipotezi" , https://tr.0wikipedia.org/wiki/Riemann_hipotezi
[7] http://www.matematikdunyasi.org , "İkiz Asal Sayılar üzerine"
http://www.matematikdunyasi.org/arsiv/PDF_eskisayilar/2002_4_6_12_IKIZ.pdf, Matematik Dünyası C:11-S:4-2002
[8] Khan Academy Türkçe , "Aritmetiğin Temel Teoremi (Bilgisayar Bilimi / Kriptografiye Yolculuk)",
https://www.youtube.com/watch?v=78My9Z6Mu9Y
[9] www.matematikdunasi.org, "Euler phi Fonksiyonu", www.matematikdunyasi.org/arsiv/PDF/04_1_39_41_EULER.pdf
[10] www.wikipedia.org , "Euclidean algorithm", https://en.0wikipedia.org/wiki/Euclidean_algorithm
[11] "The Euclidean Algorithm and Multiplicative Inverses",
https://www.math.utah.edu/~fguevara/ACCESS2013/Euclid.pdf
[12] Öklid Algoritması https://www.youtube.com/watch?v=CG7ECG3e7vQ
[13] Uzatılmış Öklid Algoritması, https://www.youtube.com/watch?v=BBiRu7S6SKQ
[14] Online Big Number Calculator, https://defuse.ca/big-number-calculator.htm

Örnek uygulama bağlantısına QR kod üzerinden de ulaşabilirsiniz **https://bit.ly/2UiRGLR**

Murat Kaygısız - TA1IHE@arkakapidergi.com

FREKANS – SWR – ANTEN UYUMU NEDİR?

Değerli arkadaşlar, bir önceki yazımızda işlediğimiz frekans, saykıl (cycle) ve bazı elektronik devre elemanları gibi temel konulardan sonra, sıra geldi telsiz haberleşmesinde oldukça önem taşıyan ve bilinmediği takdirde yılların, bilgisiz şekilde, sadece telsiz taşıma ötesine geçemeyeceği hobimizin olmazsa olmaz konularına.

Telsiz haberleşmesinde temel olan, frekans bilgisi ve bu frekanslar üzerinde doğru haberleşme yapılabilmesi için gerekli teknik donanım uyumudur. Elimizde hangi cihaz olursa olsun, bu cihazın hangi frekans aralıkları için uygun olduğunu bilmemiz ve buna uygun altyapı ile doğru ve verimli şekilde bu cihazı kullanabilmemiz esastır. Daha önceleri de bahsi geçtiği üzere, haberleşme dünyası içerisinde sonsuz yapıda frekans aralıkları kullanılmakta ve buna paralel olarak her ayrı frekans için aynı şekilde uygun bir düzeneğimizin olması gerekmektedir.

UHF – VHF – HF dediğimiz geniş aralıklar için her biri aynı şekilde farklılıklar gösteren anten yapıları ve güç beslemesi hatta doğru kablolama çok önemlidir. Elimizde bulunan imkânlar doğrultusunda kullanabileceğimiz en doğru malzemeyi temin etmemiz ve bunların arasındaki ilişkilere tam olarak hâkim olmamız gereklidir. Aksi hâlde elimizde tüm frekanslarda çalışabilme özelliğine sahip bir telsiz cihazı bulunsa dahi hiçbir frekans aralığında haberleşme sağlanması mümkün değildir.

Biraz daha konuyu açmak gerekirse, şu ana kadar anlatımlarımızda geçen frekans tanımı için bir de metre veya cm olarak ifade edilen bir ölçüden bahsetmemiz gerekli. Her frekans için bir dalga boyu vardır. Bununla ilgili bir tabloyu sizlerle paylaşmak istiyorum.

Frekans	İsmi		Dalga Boyu
10-30 kHz	Very Low F.	VLF	300-10 km
30-300 kHz	Low F.	LF	10 – 1 km
0.3-3.0 Mhz	Medium F.	MF	1,000-100 m
3-30 MHz	High F.	HF	100-10 m
30-300 MHz	Very High F.	VHF	10-1 m
300-3,000 MHz	Ultra High F.	UHF	1-0.1 m
3-30 GHz	Super High F.	SHF	100 – 10 cm
30-300 GHz	Extremely High	EHF	10 – 1 cm
300GHz-400THz	Infrared light		1mm-.0008mm

Tabloda görüldüğü üzere örneğin, VHF frekans aralığı 30-300 Mhz olmakla beraber dalga boyu konuşulduğunda 10 ile 1m ölçüsü görülmektedir. Frekansla orantılı dalga boyu, buradan da anlaşıldığı üzere değişmektedir. Dalga boyunu daha iyi anlayabilmeniz için şöyle bir çizim daha paylaşalım isterim.

Bu çizimde gördüğümüz gibi frekans ne olursa olsun dalganın iki tepe noktası arasında aldığı mesafe dalga boyunu verir. Yani bir diğer deyişle dalga; frekansa göre tam bir boy yol alması içerisinde farklı mesafeler gösterir. Örneğin 140Mhz bir frekansta dalga boyu 2m iken, 430Mhz frekansta 70cm yol almaktadır dersek herhalde konu daha anlaşılır bir hâl alacaktır.

Buradan konuyu kavrarsak şunu rahatlıkla söyleyebiliriz; frekans faktörü dalga boyuna göre farklılıklar gösterir. Yani sinyalimizin aldığı yol her frekans aralığında farklılıklar gösterir. Dolayısıyla frekanslar değiştikçe kullanılacak antenler de değişiklik göstermelidir. Dalga boyuna uygun sinyal yayılımı ve duyulabilmesi için antenler ana etkenlerdir. Bu sebeple VHF bandında yer alan 144 Mhz bir sinyal duyumu ve gönderimi için, UHF frekans anteni işimize yarar hâlde değildir. Her frekans kendi dalga boyuna uygun anten yapısı gerektirmektedir.

Telsiz kullanmaya başlayacak her operatörün temelinde hâkim olması gereken ana öğe frekans ve dalga boyu ikilisi olmadıkça sağlıklı haberleşme ve cihaz kullanımından bahsedilemez. Her farklı bant aynı şekilde kendi dalga boyuna uygun bir antenle birleştirilmediği sürece ortaya kayıplar çıkacaktır. Anten yapıları çok çeşitli şekillerde karşımıza çıkabilmektedir. Mono Bant olarak ifade edilen tek bant için üretilmiş antenler, örneğin VHF Mono Band bir anten, sadece 144-146 Mhz arası

olabildiği gibi, 140-170Mhz aralığı olarak da farklı modellerde karşımıza çıkabilmektedir. Bu tip bir durumda 160 Mhz de çalışma yapılacak ise tabii ki 140-170 Mhz aralığa sahip anten tercih edilmelidir. Diğer durumda 144-146 Mhz aralığa uygun yapıdaki anten tercih edilmek zorunda kalınırsa da burada bilinmesi gereken şudur ki, anten yapımız cihazımızın ürettiği 160 Mhz sinyalimizi havaya yayılımı için düzgün şekli ile atamayacağı için normalde örnek olarak 5W bir güç ile 50 km alanda duyulabilecek iken belki de 3 km içerisinde ancak anlaşılır olabilecektir.

Anten yapısından dolayı, kendi frekansına uygun atılamayan sinyaller hem yapısal olarak dağınık olacak hem de cihazımız çıkış katında, tam olarak atılamamasından ötürü geri dönüş yapan güce sebep vererek ısınmaya, ayrıca aynı zorladığımız frekansta atış yaptığı şekilde duyum aşamasında da yeterli uygunlukta olmadığından, duyum gücü de aynı oranda oldukça düşük kalacaktır. Burada cihazımız da zarar görebilmektedir. Bu tip detaylar haberleşmede oldukça önemlidir. Amatör telsiz cihazları arasında daha çok yeni bir seçim yapmış ve özellikle bu hobiye yeni başlamış, hevesli biri için Dual Band olarak ifade edilen bir el cihazı örneğin VHF Mono Band cihazı alarak kullanmaya başladığı takdirde en üretken zamanlarında UHF bantta haberleşme sağlamaya çalıştığında ya cihazı zarar görecek ya da verim alamadığı için hobiden soğuyabilecektir. Başka bir örnek olarak, yeterli telsiz teknik bilgisine ulaşmamış bir arkadaşımızın almış olduğu özel eğitimler sonrasında tam donanımlı bir Arama kurtarma personeli olmuş olması ve sahada herhangi bir vaka içerisinde ekip arkadaşları veyahut kriz merkezi ile haberleşme sağlayamaması gibi konular kötü sonuçların yaşanmasına sebep olabilecektir.

SWR denen ve birçok yerde duyduğumuz dengeden de bu aşamada bahsetmeden geçmeyelim. SWR ve anten dalga boyu uyumuna bir sonraki yazımız içerisinde daha detaylı örnek anlatımlarla yer vereceğimizi belirterek SWR, yani Duran Dalga Oranı'nı kısaca tarif ederek bu yazımızı sonlandırmak isterim.

Duran Dalga Oranı (SWR) anten yapısında olduğu gibi, ölçümü yapılacak frekans aralığına uygun bir SWR Metre ile uygun şartlarda ölçülmelidir. Bir diğer deyişle 400-520 Mhz arası ölçüm yapabilen bir SWR Metre ile 144 Mhz aralığı ölçümü yapılamaz. Uygun frekans aralığı ölçümüne sahip bir SWR Metre cihazımızın anten çıkış konektörü üzerine yerleştirilerek, cihazdan antene kadar olan hattın başına bağlanır ve cihazımızdan çıkan sinyal ile anten ucu arasında bir terazi ölçümü yapılır. Burada esas olan Ohm cinsinden verilen daha önce de bahsettiğimiz 50Ohm dengesi ölçümüdür. Yani cihazdan anten yayılımı noktasına kadar olan hat üzerinde Ohm dengesizliği olup olmadığına bakmak için kullanılır.

Şimdi ileride işleyeceğimiz konular esnasında pekiştireceğimiz ancak şimdi belirtilmesini önemli gördüğüm konunun altını çizerek bu yazımı sonlandırmak isterim; SWR Metre cihazı Ohm dengesi kontrolü sağlar, anten yapısının çalışma yapılan frekansa uyumunu göstermez, gösteremez. SWR ve Frekans Dalga Boyu uyumu Anten Analizör cihazı gerektirir.

Bir sonraki yazımızda telsizcilik hobisi konusunda hevesli ve öğrenme gayreti içerisinde bulunan arkadaşlarla görüşmek dileklerimle güzel bir bahar başlangıcı diliyorum,

Saygılarımla...

Ilgın Müftüoğlu - ilginmuf@gmail.com

YAPAY ZEKÂYA HAWKING BAKIŞI

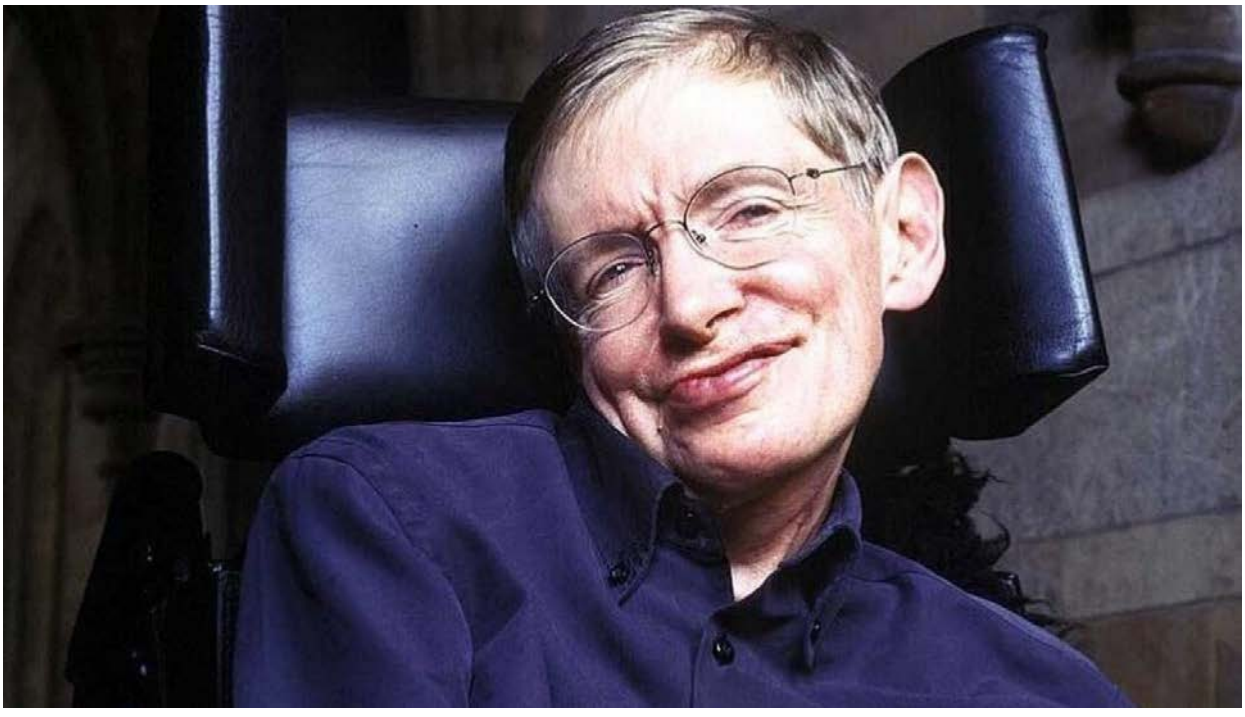
Stephen Hawking son anına kadar, insanlığın yapay zekâdan nasıl faydalanabileceği konusundaki tartışmaların en öncü sesiydi. Kendi kendine düşünerek gelişme kabiliyetindeki bu makinelerin bir gün kontrol altında tutulamayabileceği korkusunu hiç gizlemedi. Hatta açıkça, "yapay zekâ üzerindeki gelişmelerin geleceği, insan ırkının sonu olabilir" demek kadar da ileri gitti.

Çok satan kitaplarında veya en bilinen konuşmalarında evrenin ve insanın varoluşunu irdeleyen Hawking, 2014'te yine insan ürünü olan yapay zekâlarla ilgili bir konuşmasında ise; *"Yapay zekâ, kendisini geliştirmeyi sürdürebilir ve hatta kendisini yeniden biçimlendirebilir. Son derece yavaş bir biyolojik evrimle sınırlı olan insanlar, bu tür bir güçle yarışamaz."* ifadesiyle ise, insanoğlunun olası sonu ile ilgili de bir senaryo ortaya atmış oldu.

Hawking bundan bir sene sonra başka bir konuşmasında ise bilgisayarların yapay zekâ ile birlikte gelecek 100 yıl içinde insanları çoğu hususta geride bırakacağını dile getirirken, bu zaman geldiğinde bilgisayarların bizimkilerle aynı hedeflere sahip olduğundan emin olmalıyız diye de ekledi.

2017'de ise Hawking, potansiyel risklerin belirlenip gerekli önlemlerin alınmaması halinde, yapay zekânın uygarlık tarihindeki en kötü olay olabileceğini söylediği konuşmasında, yapay zekâ ile söz konusu olabilecek tehlikelerin ekonomiyi de sarsacağına değinmiş; bu potansiyel gerçeklikten korunmak için, yapay zekâ yaratıcılarının olası bütün riskleri belirleyerek en etkili yönetimleri kullanması gerektiğini ifade etmişti.

Hawking bütün bu süreçte özetle düşünebilen makinelerinin kendi başlarına hareket edecekleri, kendilerini geliştirip değiştirecekleri ve insanlardan bağımsız olarak daha yetenekli



sistemler tasarlayıp inşa edecekleri, bugün belki hayal edilemeyen bir yapay zekâ türüne karşı uyarıda bulunmuştu. **Ona göre biyolojik evrimin yavaş akışına bağlı insanların, makinaların bu hızla gelişen dünyasından trajik bir şekilde dışlanmaları kaçınılmazdı**.

Tehlike unsuru bir yana bırakılırsa Hawking, henüz insanüstü bir seviyede olmayan günümüzdeki yapay zekâ sistemlerinin; savaşları, yoksulluğu ve hastalıları yok edeceğine inanıyordu. İfade ettiği derin kaygılar, yapay zekâ sistemlerinin yalnızca insan zekâsı süreçlerini algılayarak çoğaltmakla kalmayıp, aynı zamanda insan desteği olmadan bunları geliştirmeye devam ettiği nokta olan insan üstü yapay zekâ ile ilgiliydi. Yapay zekâların birkaç on yıl sonra bu seviyeye geleceklerini dile getiriyordu.

Stephen Hawking'in, yapay zekânın insanlığı alt edeceği korkusu ile aynı zamanda sağlayacağı faydalarıyla ilgili olumlu olan çelişkili görüşleri ise muhtemelen kendi hayat hikâyesinden kaynaklanıyordu. Hawking'in dünyayla iletişim kurabilmesi için bir yapay zekâyla yaşaması gerekiyordu. 1985'ten itibaren konuşamayan Hawking, konuşmasına ve yazmasına yardımcı olan ve sağ yanağındaki bir kas tarafından işletilen o efsanevi bilgisayar üzerinden çözümlenen bir dizi farklı iletişim sistemi kullandı. Yalnızca kendisi için geliştirilen bu yazılım programlarıyla kendini ifade edebiliyordu. Son olarak ise Intel tarafından geliştirilen yeni bir yazılımla hayatı yakalaması hızlandı. En önemlisi ise bu yazılım Hawking'in kelimelerini analiz ederek edindiği bilgileri kullanarak, onun yeni fikirlerini dile getirmesini kolaylıkla sağlayan bir yapay zekâ kullanıyordu. Öyle ki bu sistem Hawking'in kitaplarını, makalelerini ve ders notlarını analiz ederek o kadar iyi bir hâl aldı ki, Hawking ile en çok örtüşmüş olan "kara delik" terimini hiçbir tuşlama yapmadan kendiliğinden uygun şekilde kullanabiliyordu. Yapay zekâ teknolojisinden bizzat faydalanan Hawking yapay zekâ kullanan bir yazılım üzerinden, bu teknolojinin insan neslinin sonunu da getirebileceğini ifade ediyordu.

Yine de Hawking'in yapay zekâ hakkındaki görüşleri, bizlerin öngörebildiklerine nispeten daha az endişe verici. Bu konudaki konuşmalarının bizi ürküten tarafı ise muhtemelen, takdir görmüş olduğu önceki yaklaşımlarından farklı olarak sergilediği tedirgin duruşu ve uyarıları. Önceki görüşlerinde samimiyetle, gelişmekte olan teknolojileri anlamak, sindirmek ve bu teknolojileri uygun şekilde yönetmek gerektiğini açıklayan Hawking, yapay zekâ ile ilgili olarak ise sürekli ve çok fazla araştırma yapılması çağrısında bulunmuş ve sıklıkla endişelerini dile getirmiştir.

Yazılımcılar için Okuma Listesi

Merhabalar. Arka Kapı Dergisi'nde üçüncü defa huzurlarınızdayım. Yine bol ve güzel makaleler derledim. Umarım istifade edersiniz. Buyursunlar:

Boca: Blockchain Uygulaması Geliştirme

Son dönemin hype; hype olduğu kadar da büyük potansiyele sahip teknolojilerinden biri Blockchain. Şahsi düşünceme göre her yazılımcının en azından temellerini bilmesi ve uzaktan da olsa takip etmesi gereken bir teknoloji. Hatta belki elimizi kirletmenin vakti de gelmiştir. Bu sayıda farklı dil ve platformlar üzerinde Blockchain uygulaması geliştirmeye yönelik, rast geldiğim kaynakları üzerinize boca ediyorum:

Blokchain 101: Ahmet Usta ve Serkan Doğantekin'in yazdığı -ücretsiz- e-kitapta adından anlaşılacağı üzere Blockchain'in temelleri, üzerinde geliştirilen platformlar ve uygulamalar anlatılıyor.

PHP ile Blockchain (Blokzinciri) yazıyoruz: Ulugbek Miniyarov, PHP ile Blockchain oluşturmayı anlatan 4 yazılık (Prototip, Proof of Work, Saklama ve Komut Satırı, Transactions) İngilizce serinin çevirisini yapmış.

.Net Core ile Blockchain İnşa Etme: Hasan Denli, .Net Core üzerinde bir Blockchain oluşturmayı anlattığı 3 yazılık (Temel Altyapıyı Oluşturma, Proof of Work, Wallet Transaction) bir seri kaleme almış.

Python ile Blockchain Oluşturma: Evrim Dönmezgel de Python ile detaylıca adım adım Blockchain oluşturmayı anlatmış.

Blockchain Yapısı ve Ethereum: Engin Ünal, Blockchain yapısı ve Ethereum'la ilgili bir dizi yazı yazmış. İlkinde Bitcoin ve Blockchain'in çalışması, ikinci yazıda Ethereum ve akıllı kontratlar, akabinde Ethereum Blockchain'i oluşturma ve son olarak da Solidity ile Ethereum'da akıllı kontrat yazmayı anlatmış.

Yine yukarıda bahsettiğim kitabın yazarlarından Serkan Doğantekin, 15'er dakika Ethereum ağı oluşturmayı ve akıllı sözleşme yazmayı anlatmış.

Bunların dışında Deniz Özgür, dev bir amme hizmetine imza atarak Ethereum'da akıllı sözleşme geliştirmek için kullanılan Solidity dilinin dokümanlarını Türkçeye çevirmiş.

Son olarak Mert Susur'un ve Onur Aykaç'ın Blockchain temelleri, Ethereum&Solidity ve Ethereum webinar serisi eğitim videolarını da buraya bırakayım.

Yeni Bir Blockchain Protokolü

10 yıl önce Bitcoin'in açtığı yolda insanlar farklı rotalar üzerinden yürümeye devam ediyor. En son 15 Ocak'ta Bitcoin'in eksik kaldığı noktalara odaklanan yeni bir teknoloji açıklanmış: MimbleWimble(şu an kopyala yapıştır yapmadan, tek seferde doğru yazmanın gururunu yaşıyorum). Özellikle mahremiyeti koruma ve hafiflik üzerine yoğunlaşılarak tasarlanmış. Bu teknoloji üzerine şimdiden bazı uygulamalar geliştirilmiş. Hatta bunlardan Grin, geleceğin ödeme aracı olacağı iddiasında imiş. Bitcoin'in rakibi ve onun aksine her sene aynı oranda üretilebilecek bir kripto para. Turan Sert, ilkinde MimbleWimble'ı diğerlerinde Grin'i detaylarıyla anlattığı 3 yazı kaleme almış.

HTTP ve Güvenlik

Gökhan Şengün, önceki haftalarda http isteklerinde kimlik doğrulama işlemlerini anlattığı bir seriye başlamıştı. Geçtiğimiz hafta da ücretsiz SSL/TLS sertifikası sağlayan Let's Encrypt servisinden bahsetmiş.

Diğer yandan Buse Kalkavan da aynı günlerde yayımladığı yazısında SSL sertifikasını ve SSL/TLS protokolünün çalışma prensibini anlatmış.

Cumartesi Geceleri

Ekosistemin en istikrarlı ve üretken bloggerlarından biri şüphesiz Burak Selim Şenyurt. 2003 yılında yazmaya başlamış ve kaba hesapla 1000'e (yazıyla bin) yakın nitelikli makale yazmış. Yazmaya da devam ediyor. Çiçeği burnunda bir öğrenci edasıyla da okumaya, araştırmaya devam ediyor (Medium'da okuduğum hemen her yazıda onun izlerine/vurgulamalarına rastlıyorum).

Birkaç aydır geçtiğimiz yıllara nisbeten blogunda daha az yazı yayımlıyordu. Meğer bu arada Github'da büyük bir hazine meydana getirmekle meşgulmüş. Oluşturduğu repoda cumartesi geceleri çalışmalarından çıkardığı notları derlemiş. An itibariyle Angular'dan React'e Vue'ye, TypeScript'ten Python'a, Blazor'dan GraphQL'e 29 farklı konuda makale ve örnek var. Şuradan hazineye ulaşıp, hunharca tüketip, "star"ınızı bırakabilirsiniz.

Yazılımcının Kamçısı

Geliştirdiğimiz yazılımlardaki teknik borçlar hayatımız gerçeği. Yüzde yüz kendi yağında kavrulan bir yazılım geliştirmek neredeyse imkansız. Ama ne kadar az borçla ilerlersek yarınlarımızı o kadar az ipotek ederiz ve başımız o kadar az ağrır. Burak Selim Şenyurt, geçtiğimiz haftalarda yayımladığı yazısında genişçe teknik borçlardan bahsetmiş; nasıl kaçınacağımızı ve önceden birikmiş borçları nasıl ödeyeceğimizi anlatmış.

TOR

TOR, internetin derinlerindeki gizli saklı köşelere erişim için kullanılan bir yapı. Bir nevi giriş kapısı. Anonim ve kimi zaman illegal hayatların velinimeti. Ziyahan Albeniz, TOR servislerinin tarihini ve çalışma prensibini anlatmış.

Eğlenceli Algoritmalar

İbrahim Kürce, İngilizce teknik kitapların Türkçe özetini çıkarmaya devam ediyor. Son olarak Grokking Algorithms kitabını özetlemeye başlamış. Kitabın (ve dolayısıyla özetin) anlatımı tek kelime ile harikulade. Tabii kelime sınırı gibi bir derdimiz olmadığı için övmeye devam edebiliriz. Evet, en son harikulade demiştik. Genel itibariyle problemler ve onları çözen algoritmalar eğlenceli bir şekilde hikâyeleştirilerek anlatılmış. Ayrıca bol ve yine eğlenceli çizimlerle bezenmiş. Henüz linke gitmediyseniz övmeye devam edeceğim. Haydi gidin, okuyup gelin. Burada bekliyorum.

Evet, okuduğunuza göre devam edebiliriz. Kitap özeti demişken, henüz bir üniversite öğrencisi olan Ege Alpay da Clean Code kitabını okumuş ve anladıklarını not alıp blog olarak yayımlamaya başlamış. Gayet de başarılı iş çıkarmış. Maşallah deyip başarılarının ve dahi paylaşımlarının devamını dileyelim.

Yazılımcıların Bilmesi Gereken Anahtar Kavramlar

Yazılım dünyasına ilk adımını atan veya buna niyet eden hemen herkesin merak ettiği ilk meseleler "nereden başlamalıyım, neleri öğrenmeliyim" vb. sorular. Mehmet Cem Yücel, Twitter'da yazdığı floodda 15 madde halinde yazılımcının bilmesi, aşina olması gereken kavramlardan bahsetmişti. Bunu blog yazısı olarak paylaşması talebimizi geri çevirmeyerek kendi blogunda ve Medium'da da yayımladı. Başta bahsettiğim konu için başucunda yer alması gereken bir makale.

Bu arada yakın zamanda kişisel blogundaki mevcut yazıları Medium'da da yayımlamaya başlamış. Son yazısı Heroku'nun bulut tabanlı yazılım geliştirme süreci için yayımladığı manifesto "12 Factor App" hakkında. Bulut tabanlı uygulama geliştirmeseniz bile yönetilebilir ve ölçeklenebilir bir uygulama geliştirme noktasında herkesin istifade edebileceği bir yazı.

Twelve Factor App demişken, Erkan Erol'un konu hakkındaki güzel sunumunun videosunu da istifadenize sunayım.

Veri Bilimi Uygulaması Geliştirme

Fatma Gülcan Ertop, tam sektörün ihtiyaç duyduğu türde bir yazı kaleme almeş: "Gerçek Hayatta Bir Veri Bilimi Projesi Nasıl İnşaa Edilir?". Oldukça detaylı bir şekilde fikrin ortaya çıkmasından ürüne dönüşmesine kadar olan süreci ve hatta sonrasını adım adım anlatmış.

Veri bilimi ile ilgili yayımlanan bir başka yazı ise Merve Bayram Durna'nın Python'daki veri bilimi için kullanılan kütüphanelerden Pandas'ı anlattığı makale.

Yapay Zekâ Alemi

Yapay zekâ hızla gelişse de önünde daha uzunca bir yol var. Hâlâ önünde önemli zorluklar bulunan dallarından biri bilgisayarla görme. Hacettepe Üniversitesi öğretim üyelerinden Aykut Erdem ve Erkut Erdem, "Bilgisayarlar Düşünebilir mi?" başlıklı bir yazı dizisine başlamışlar. İlk yazıda yapay zekanın ve bilgisayarla görmenin tarihinden bahsetmiş; bilgisayarla görmenin neden zor olduğunu irdelemişler. Oldukça detaylı ve okuması keyifli bir yazı kaleme almışlar. Sonraki yazılarda ise asıl konuya doğru ilerlemişler.

Mert Çobanoğlu, Keras ile nesne tanıma uygulaması geliştirmeyi anlatmış.

Okan Yıldız, Andrew Ng'nin ilk yapay zeka projesini gerçekleştirirken dikkat edilmesi gerekenleri anlattığı makalesinden notlarını paylaşmış.

Ömer Koçbil, bilisim.io'da "yapay zeka nedir?"den "dünyada yapay zekanın durumu"na an itibariyle 6 yazıya ulaşan bir seri yayımlaya başlamış.

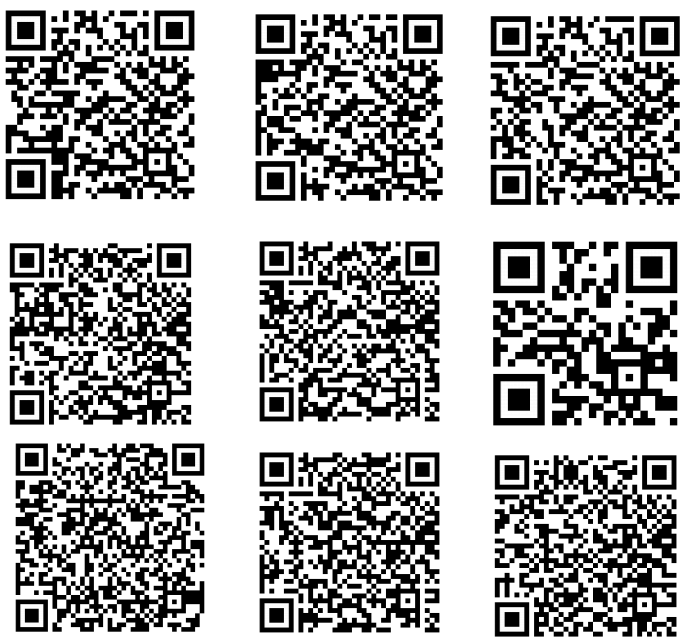
Yapay zekâ pek çok farklı alt dalı ile beraber geliştirilmeye devam ediyor. Bu alt dallardan biri de bir görseldeki nesneleri tanımaya yarayan bilgisayarlı görü. Görseli verdikten sonra "Burada kaç çocuk var, hava güneşli mi, çiçekler ne renk?" vs. sorularının cevabını aramaya ise "görsel soru cevaplama" deniyormuş. Başak Buluz, bu konudaki çalışmalarda kullanılan yaklaşımları ve veri kümelerini anlattığı detaylı bir yazı yayımlamış.

Daron Yöndem de görüntü tanıma ile alakalı yazısında Azure Cognitive Services ile yüz tanıma uygulaması oluşturmayı anlatmış.

Özkan Doğan ise özellikle eldeki veri miktarının az olması gibi farklı senaryolarda başarılı sonuçlar veren öğrenme algoritması "Pekiştirmeli Öğrenme" hakkında bir giriş yazısı yazmış.

Ayyüce Kızrak ve Deep Learning Türkiye ekibinden bir grup arkadaş, yapay zekanın kullanım alanlarını ve senaryolarını derlemişler. Sektör bazlı olarak ayırdıkları emek dolu bu uzun ve kapsamlı derleme de 12 farklı sektörde 100'den fazla kullanım alanından bahsetmişler.

Deniz Kılınç da yapay zeka çalışırken karşılaşılan problem ve zorluklardan; aynı zamanda bunları aşma yöntemlerinden bahseden devamlı güncellemeyi planladığı bir yazı kaleme almış.



10 Yaşında Bir Çocuğa Yapay Zekâ Çalıştırmak

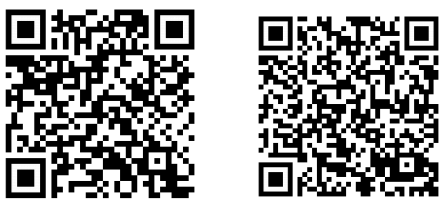
Son haftalarda okuduğum en güzel yazılardan birinden bahsetmek istiyorum: "10 Yaşındaki Oğlumla Nasıl 'Yapay Zekâ' Çalışıyorum?". Zafer Demirkol, yapay zekâ çağında 10 yaşındaki oğlunun bunun dışında kalmaması için seviyesine göre yapay zekâ öğretmeye karar vermiş. İlk başta temel seviyede bildiği Excel'i geliştirmesi için yardım etmiş. Misal futbol merakından faydalanarak Fenerbahçeli futbolcuların bilgilerini pek çok detayıyla bir Excel dosyasına girmesini sağlamış. Akabinde PowerBI ile bu verileri yine seviyesine uygun şekilde görselleştirmiş. Daha sonra yaz tatilinde Dünya Kupası'nın olmasından istifadeyle Dünya Kupası'ndaki futbolcuların verilerini oluşturmasını sağlayıp, bunların bir kısmı ile IBM Watson'ı eğitmiş, kalanları ile de test etmişler. Elhâsılı, pek çok konuda ders çıkarabileceğimiz müthiş bir yazı serisi.

Yeni Teknolojiler ve Hukuk

Yapay zekâ, robotik ve otonom araçlar gelişip yaşamımızın içine girdikçe etik ve hukuki tartışmalar da artıyor. Olayın sevindirici tarafı azar azar da olsa ülkemizde bu tartışmaların dillendiriliyor olması. Geçtiğimiz haftalarda bu konuda 2 makaleye denk geldim.

Bunlardan ilki Avukat Burçak Ünsal'ın Baro Dergisi için kaleme aldığı makale.

Diğeri ise Betül Çolak'ın otonom araçların yasal sorumluluğu hakkında yazdığı makale.



Verilerimiz Talan Edilirken Biz

Facebook, durmaksızın veri skandallarına imza atmaya devam ediyor. En son ortaya çıkan olayda bir firma üzerinden Facebook Research diye bir uygulama için ücret mukabili denekler bulmuşlar. Ama bu arkadaşlara söylediklerinden daha fazla verilerini toplamışlar. İsmail Hakkı Polat, bu örnek üzerinden giderek biraz da "Atı alan Üsküdar'ı geçti." nevinden düşüncelerle olayı normal görmeye başlayan yorumlara karşı çıkarak yapılması gerekenlerden bahsetmiş.

Geçtiğimiz haftalarda yayımladığı diğer bir yazısında ise Ticaret Bakanlığı'nın dış ticaret işlemlerinde Blockchain kullanma kararını irdeleyerek, üzerinde enine boyuna konuşulması gereken hususlardan bahsetmiş.


İş Görüşmesinde İşverene Sorulacaklar

Ülkemizdeki iş görüşmelerinde genelde maaş, terfi vb. kozlara sahip olduğu için işveren tarafı yukarıda, kendisine beğenilmesi gereken pozisyonda; çalışan adayı ise talep eden, kendini beğendirmek mecburiyetinde olan pozisyonda algılanıyor. (Ben de geçmişte yaşadım bu psikolojiyi.) Ne var ki bir şirkette çalışma dediğimiz eylem esasında bir efendi-köle ilişkisi değil bir alışveriş. Hatta emek-sermaye ortaklığı da diyebiliriz. İşveren, çalışanına lütufta bulunmuyor bilakis satın aldığı emeğin karşılığını veriyor. Dolayısıyla ideal bir dünyada görüşmede de aynı pozisyona ve aynı değerde kartlara sahip olmalılar.

Gökhan Topçu, yayımlandığında en çok paylaşılan yazılardan biri olan ve kuvvetle muhtemel sizin de denk geldiğiniz uzun yazısında, bahsettiğim bakış açısıyla işverene ait bir hak gibi görülen soru sorarak karşı tarafı değerlendirme meselesini, çalışan adayının nasıl kullanabileceğini anlatmış. Bu vesileyle, kaliteli sunumlarıyla da tanıdığımız Sayın Topçu gibi dolu dolu insanların daha fazla Türkçe blog üretmeleri için buradan talepte bulunalım.

Mühendisler vs İK'cılar

Mühendisler (diplomadan bağımsız, yaptığı iş mühendislik içerenler) olarak hobilerimiz arasında yer alan faaliyetlerden biri İK'cıları (İnsan Kaynakları çalışanları) gömmek. Bunun için de elimizde bolca malzeme var. Peki bu yaptığımız pragmatik olarak ne kadar doğru? Veya bu durumu, şikâyet ettiğimiz konuları nasıl düzeltebiliriz, düzeltirsek neler elde ederiz? İşte bütün bu soruların cevabını Bilgem Cakir, geçtiğimiz haftalarda yayımladığı yazıda irdelemiş. İK birimlerinin kuruluş nedenlerinden, mühendislik takımlarını başarılı oluşturmak için sahip olmaları gereken organizasyondan ve mühendislik ekiplerinin neden iş birliği içinde olması gerektiğinden objektif bir şekilde bahsetmiş.

Sektörde Çalışma Koşulları

Ülkemizin kanayan yaralarından biri -her- sektördeki çalışma koşulları. Yukarıda bu konuyla dolaylı yoldan alakalı olan yazılımcı iş görüşmelerinden ve İK & mühendis ilişkisinden söz eden makalelerden bahsettim. Bunlardan sonraki hafta direkt bilişim sektöründeki çalışma koşulları ile ilgili bir yazı yayımlandı. Hem de çalışanların gözünden. Oğuz Kılıç, internet üzerinden konu ile ilgili görüştüğü kişilerin söylediklerini, kendi yorumlarıyla harmanlayarak yazmış.

Yazılımcılara Tavsiyeler

Bilgem Çakır üstad, yine döktürmüş ve dolu dolu bir yazı yayımlamış. Üzerinden haftalar geçtiği için çoktan okuduğunuzu tahmin ediyorum. Konu, yazılıma nasıl başlayacağını ve başladıktan sonra kendini nasıl geliştireceğini soranlara tavsiyeler. Yazıya girişte yine itinayla fikri temeli oluşturmuş ve bilgi, olgu, yeti kavramlarını irdelemiş. Akabinde yol haritasının nasıl çizilmesi gerektiğinden bahsedip tavsiyelerini sıralamış.

Legacy Code Maceraları

Bir yazılımcının hayatındaki en büyük gerçekliklerden biri legacy code (miras kod) diye nitelendirdiğimiz, uzun süredir çalışan ama eskimiş, kokmaya başlamış, üzerinde değişiklik yapması yürek isteyen yapılar. Bir nevi statüko. (Hatırlayacağınız üzere geçen sayıda bu kokuları refactoring marifetiyle nasıl giderebileceğimize dair muazzam bir Türkçe kaynak paylaşmıştım.)

Burak Altın, Avustralya'da yeni başladığı işinde fevkalade bir legacy code hazinesiyle karşılaşmış. Anlatımına göre hemen her nevi kötü kodu muhtevi, düzeltmesi zor bir yapı. İşin güzel tarafı bu mücadelesini bir yazı dizisi halinde paylaşmaya

başlamış. İlk yazısında durumu rapor ettikten sonra ikinci yazıda ufaktan canavarı dürtüklemeye, ortalığı toparlamaya başlamış.

Söz Legacy Code'dan açılmışken, İbrahim Kürce, konu hakkındaki kült eser "Beyond Legacy Code" kitabının Türkçe özetini çıkarmış.



Refactoring

Yazılım geliştirme hayatımızın her evresinde mücadele ettiğimiz bir kişi var: önceki yazılımcı. Saçma sapan bir yazılım tasarımı yapar, gereksiz bir ton kod yazar, doğru düzgün null kontrolü yapmaz… Bu listenin sonu yok. Ama işin acı tarafı her birimiz birer önceki yazılımcıyız. Üstelik hiç kimsenin olmasa bile kendimizin. 3-5 ay önce yazdığınız kodları inceleyin mutlaka düzenleyeceğiniz bir şeyler çıkacaktır. Dolayısıyla kim yazarsa yazsın hemen hemen tüm yazılımlar zamanla düzenlenmeye muhtaçtır. Bu düzenleme işlemine "refactoring" diyoruz.

Ali Rıza Adıyahşi, refactoring için Github'da oldukça detaylı ve güzel bir Türkçe rehber hazırlamış. İlk etapta temiz kod, teknik borç gibi konularla giriş yaparak "kokan kod"dan bahsetmiş ve tek tek tüm kötü kokuları irdelemiş. Son olarak da bunları çözmek için kullanılan refactoring yöntemlerini anlatmış. Her yazılımcının okuması gereken bu rehbere siz de katkı ve star verebilirsiniz.

Black Friday Tecrübeleri

Geçtiğimiz aylarda Iyzico'nun Black Friday tecrübesini anlattığı yazıdan bahsetmiştim ve benzerlerinin artmasını temenni etmiştim. O dönem gözümden kaçan daha detaylı ve teknik bir yazı da yayımlanmış: cimri.com'un BF tecrübeleri. İlim Turan, yazının başında uygulamaların mimarisini anlatarak başlamış ve bir nevi antrenman sayılan 11.11 kampanya dönemini anlatmış. Akabinde Black Friday'e hazırlık için tekrar tekrar yapılan testleri, başarısızlıkları, problemleri, çözümleri ve uygulamayı ölçeklemelerini anlatmış. Finalde de asıl kampanya döneminde yaşananları anlatarak bitirmiş. Yine örneklerinin artmasını temenni ederek bu bahsi geçelim.

CORS Sezonu

CORS, ucundan kıyısından web geliştirmeye bulaşan hemen herkesin -yüksek ihtimalle de aldığı hata sonucu- yüzleşeceği bir kavram. Gökhan Şengün haftalık yazılarından son 2'sinde bu kavramı anlatmış. İlk yazısında genel bir giriş yapmış, ikinci yazıda ise pratik kullanım senaryolarından ve bypass etme yöntemlerinden bahsetmiş.

CORS hakkında Ziyahan Albeniz de geçtiğimiz senelerde oldukça kapsamlı bir yazı yayımlamıştı.

Diğer yandan Doğan Aydın, kısa bir web tarihinden başlayarak kapsamlı bir şekilde Same Origin Policy'yi anlatmış. Hangi sebeplerden/kısıtlardan dolayı değiştirildiğini/esnetildiğini detaylı bir şekilde anlatmış. Alt başlıklarda doğal olarak CORS'a da yer vermiş.

Son olarak ise Zafer Ayan'ın direkt CORS'u anlattığı Devnot'ta yayımlanan yazısı.





Sesli Asistan Yazmak

Veri bilimi alanında nitelikli içerikler üreten genç bloggerlardan Yunus Emre Gündoğmuş, bu kez Python ile bir sesli asistanın nasıl yazılabileceğini anlatmış. Yazının sonunda ise kendi yazdığı açık kaynak bir asistan olan Kavi'den bahsedip kod deposunu paylaşmış.

Yılan Hikayesi

Fatih Erikli, Python'ı anlattığı "yılan hikayesi" isimli bir seriye başlamış ve geçtiğimiz haftalarda ilk bölümünü yayımlamış. Kendine has üslubuyla anlattığı, hikaye tadında, akıp giden, enfes bir yazı olmuş.

GPU Mimarisi ve CUDA

Python son zamanların en popüler dili. Özellikle yapay zekâ ve veri biliminin gelişmesiyle altın çağlarını yaşıyor. Ama muadilleri ile yapılan kıyaslamalarda 2 ila 10 kat daha yavaş olduğu ortaya çıkmış. Tahir Özdemir, İngilizce bir makaleden yararlanarak bu yavaşlığın sebeplerini anlatmış.

Bu arada Medium profilini incelerken CUDA hakkında bir yazısını gördüm. Neymiş diye araştırınca şöyle bir tanıma denk geldim: "GPU'nun donanımsal hesaplama gücünden faydalanmak amacıyla sunduğu paralel hesaplama mimarisidir."

Bahsettiğim yazıda, CPU ve GPU'nun karşılaştırmasından başlayarak GPU'nun mimarisini ve çalışma prensibini anlatmış. Akabinde GPU'da çalışacak bir yazılım geliştirirken dikkat edilmesi gerekenlerden bahsetmiş. Henüz okuyamadığım bir devam yazısı da yazmış. CUDA'yı araştırırken denk geldiğim, Nezihe Sözen'e ait nispeten daha detaylı yazıyı da buraya bırakayım.

2018-2019 Değerlendirmeleri

2018'i bitirip 2019'a girmemiz hasebiyle bolca muhasebe ve değerlendirme yazısı yayımlandı.

Mesela Fırat İşbecer, "kendince" önemli gördüğü gelişmeleri bir flood haline getirip akabinde blog olarak yayımlamış.

Fırat Demirel, yeni yıla girmesini bahane ederek kendine yeni hedefler belirlemiş. Bunlardan biri çok yazmak olsa gerek ki ilk 15 günde 10 blog yazısı yayımlamış.

Baran Somaklı, 2018'in bir muhasebesini yapıp 2019 hedeflerinden bahsetmiş.

Benzer şekilde Hamza Üzümcü de 2018'in muhasebesini yapmış.

AvivaSA Dijital Garaj, Techcrunch'tan derlediği yazıda 2019'da halka arz edilmesi beklenen unicorndan bahsetmiş. MIT Tech Review'dan yaptıkları bir derlemede ise 2018 yılında yeni teknolojiler konusunda yaşanan gelişmeleri paylaşmışlar.

Fikri Türkel, 2019'da teknoloji dünyasında yaşanabilecek önemli gelişmelerden bahsetmiş.

Aynı şekilde Atıf Ünaldı da 2019 beklentilerini kaleme almış.

Bir diğer önemli derleme ise dijitalguvenlik.org'daki 2018'de yaşanan önemli veri sızıntılarını derlemiş. İstisnasız her ayda veri sıkıntısı yaşanması ve Facebook'un 3 farklı sızıntıyla başı çekmesi dikkat çekici.

Yine Selin Çetin de veri (veri skandalları, yapay zekâ) ağırlıklı olmak üzere 2018'de yaşanan önemli teknolojik gelişmeleri derlemiş.

Selin Arslanhan, "CBInsights'ın 2019'da dünyayı yeniden şekillendirebilecek girişimler" listelesinden bahsetmiş. Akabinde ülkemizden gelecek vaad eden bir girişimi anlatmış.

Soner Canko, teknoloji dünyasının gündemini belirleyen organizasyonlardan olan dünyanın en büyük teknoloji fuarı CES 2019'a katılmış ve izlenimlerini aktarmış.

Dünya Halleri ise öngörülerden ziyade 2019'da gerçekleşmesi planlanan/bu yönde açıklama yapılan önemli olayları derlemiş.

2019 Teknoloji Raporları

Softtech, geçtiğimiz haftalarda harika bir teknoloji raporu yayımlamış. 264 sayfalık raporda güncel teknolojiler hakkında 2018 yılında yaşanan gelişmeler, bu teknolojilerin çözdüğü problemler, önlerindeki zorluklar, geçmişi, bugünkü durumu ve geleceği anlatılmış. Bunun yanında Türkiye'nin bu bilgiler ışığında geleceği ve alması gereken aksiyonlar irdelenmiş. Bu dolu dolu ve doyurucu raporda emeği geçen herkesi tebrik ediyorum.

Rapor demişken, dünya çapında yıllık sosyal medya kullanımını derleyen We Are Social raporunun 2019 sayısı yayımlanmış. Gamze Nurluoğlu, 10 maddede 2018 ile karşılaştırmalı olarak raporu incelemiş.

Beyaz Yakadan Girişimciliğe

Kendi ifadesiyle "pinpon topu gibi bir kariyer"e sahip olan Umut Gökbayrak, 3 kez kurumsal dünyaya 4 kez de girişimcilik dünyasına göç etmiş. Aynı zamanda uzun yıllara yayılan bu süreçte edindiği tecrübeleri, "beyaz yakadan girişimciliğe geçiş" başlıklı her yönüyle enfes yazısında bize aktarmış.

Siber Sözlük

Siber Sözlük

[Whaling]

Whaling (Balina Avcılığı) şirketlerin kritik, hassas verilerine tam erişim yetkisi bulunan üst düzey şirket yöneticilerini hedefleyen bir kimlik avı şeklidir. CEO sahtekarlığı olarak da bilinen balina avcılığı, hedefi aldatarak hassas verileri açığa çıkarmak veya para transferi gibi belirli eylemleri gerçekleştirmek için e-posta ve spoofing gibi yöntemler kullandığı için oltalama saldırılarına (phishing) benzetilebilir.

[Steganography]

Bilgiyi gizleme bilimine verilen addır. Amaç; alıcı ve gönderenin dışında üçüncü kişilerin bilgiyi öğrenememesini sağlamaktır. Steganografi›nin şifrelemeye göre en büyük avantajı bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu fark edemiyor olmasıdır. "Gizlenmiş yazı" anlamına gelen Steganography kelimesi, Yunanca «örtülü, gizlenmiş veya korumalı» anlamına gelen steganos (στεγανός) ve "yazı" anlamına gelen graphein (γράφειν) kelimelerinin birleşiminden oluşur.

[Data Exfiltration]

Bir kişinin veya şirketin verileri, izinsiz/yetkisiz bir şekilde bilgisayardan, sunucudan veya herhangi bir cihazdan kopyalandığında, aktarıldığında meydana gelen bir güvenlik ihlali biçimidir. Geçmiş yıllarda yaşanan veri sızıntıları şirketlerin kurumsal değerini, fikri mülkiyetlerini ve dünyadaki hükümetlerin ulusal güvenliğini ciddi anlamda zedelemiştir.

[IP Spoofing]

Bir web sitesi, tarayıcı ya da sistemi aldatmak için başka bir bilgisayar sistemini taklit etmek amacıyla sahte bir kaynak IP adresine sahip İnternet Protokolü (IP) paketlerinin oluşturulması tekniğidir. IP spoofing yapabilmek için çeşitli ücretsiz, açık kaynak kod ve ticari yazılımlar bulunmaktadır. ***Hping3*** ve ***nmap*** bu uygulamaların başında gelir.

ÇOCUKLAR İÇİN GÜVENLİ İNTERNET SERİSİ

Çocuklar için Güvenli İnternet

abaküs

Türkiye'nin Bilişim Kaynağı

www.abakuskitap.com

"İki şey sınırsızdır. Evren ve insanoğlunun aptallığı.
İlkinden emin değilim."
Albert Einstein