

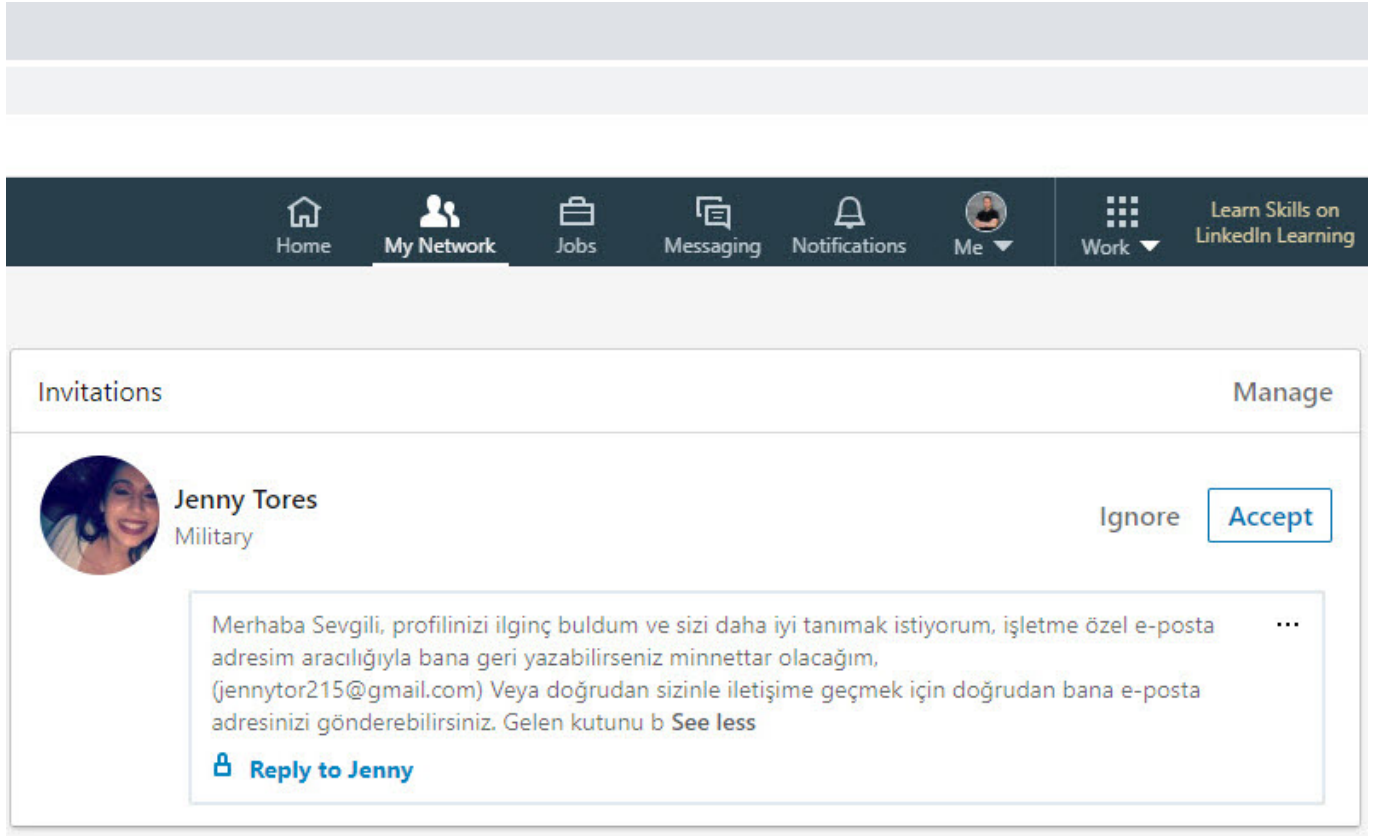
LinkedIn Dolandırıcıları

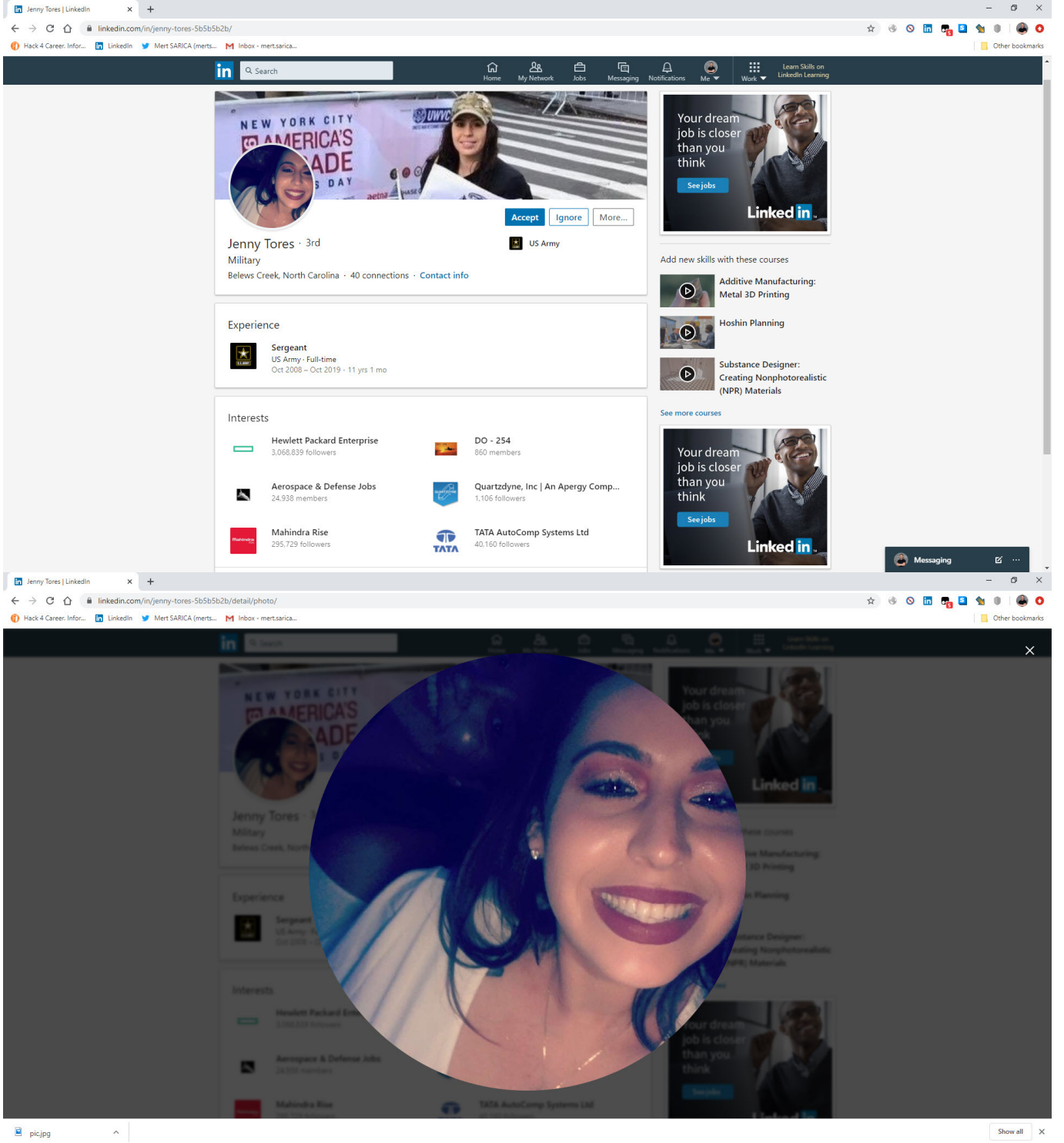
written by Mert SARICA | 28 March 2020

If you are looking for an English version of this article, please visit [here](#).

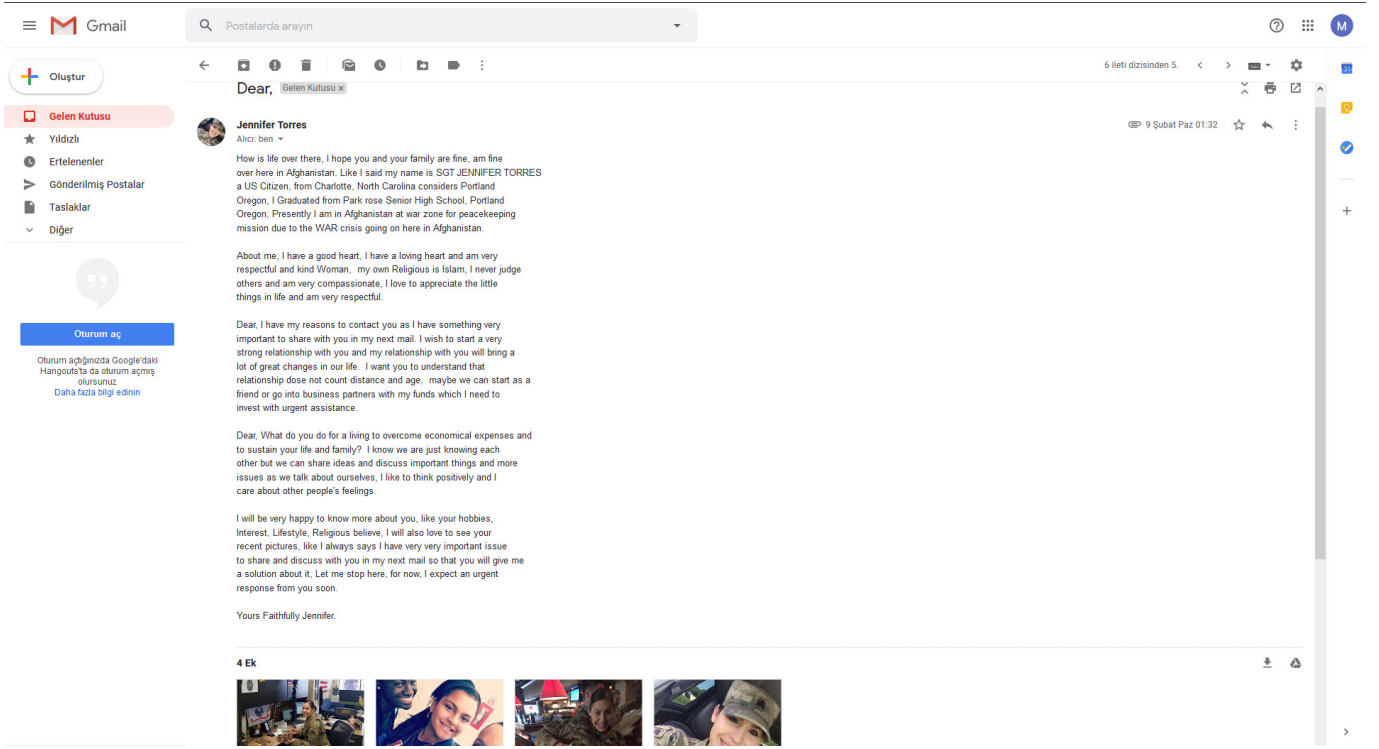
Uzun yıllardan beri sosyal ağları ve medyayı etkin kullanan bir siber güvenlik araştırmacısı olarak bağlantılarım arasında yer alanlarınız özellikle hafta içi LinkedIn ve Twitter üzerinden okuduğum ve beğendiğim siber güvenlik makalelerini, haberleri paylaştıklarımı farkediyorlardır. Twitter hesabımın korumalı olması sebebiyle LinkedIn paylaşımlarımın Twitter'a kıyasla çok daha fazla kişiye ulaşması beraberinde art niyetli kişilerin, dolandırıcıların da radarına girmeme ve ilginç mesajlar almama yol açabiliyor.

Günlerden bir gün LinkedIn üzerinden Jenny Tores isimli bir kişiden özel bir mesaj aldım. Google Çeviri ile hazırlanmış bir metinden hallice olan mesajında, profilimi çok ilginç bulduğunu ve benimle iletişime geçmek istediğinden bahsediyordu. Haber peşinde koşan bir gazeteci edasıyla ayağıma gelen bu fırsatı değerlendirerek bu kişiyle iletişim kurmaya karar verdim.

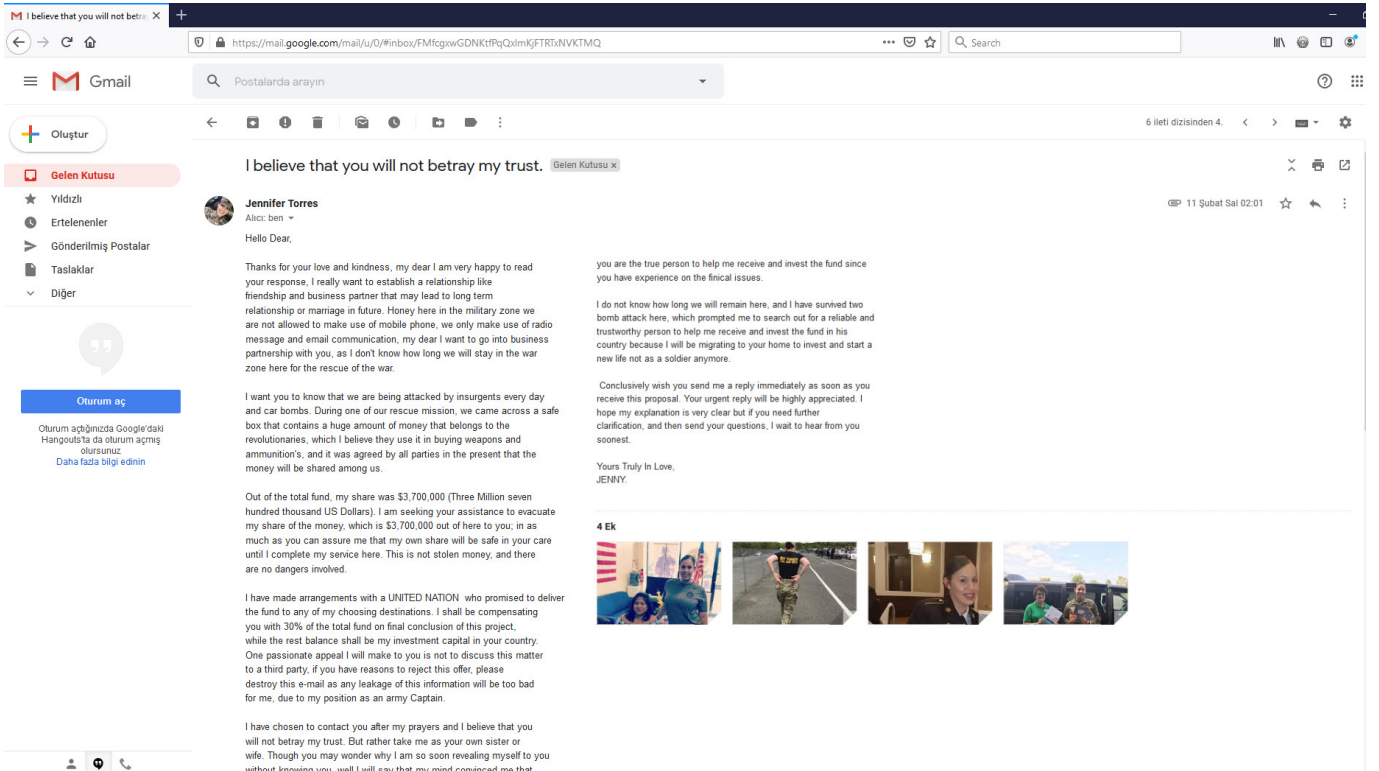




Kendisine e-posta gönderdikten sonra gelen yanıtta hanım ablamız, Afganistan'da ABD vatandaşı bir asker olduğundan, yeni bir ilişkiye başlamak istediğinden, yaşın ve mesafenin önemli olmadığından ve asıl konuşmak istediği önemli konuyu bir sonraki e-postasında belirteceğinden bahsediyordu. Sosyal mühendislik girişiminin gerçekçi olabilmesi adına da sağolsun bana 4 tane fotoğrafını da göndermeyi ihmal etmemişti. Devrik cümleli LinkedIn mesajına kıyasla e-postasındaki yazı dili ise şaşırtıcı derecede iyiydi.

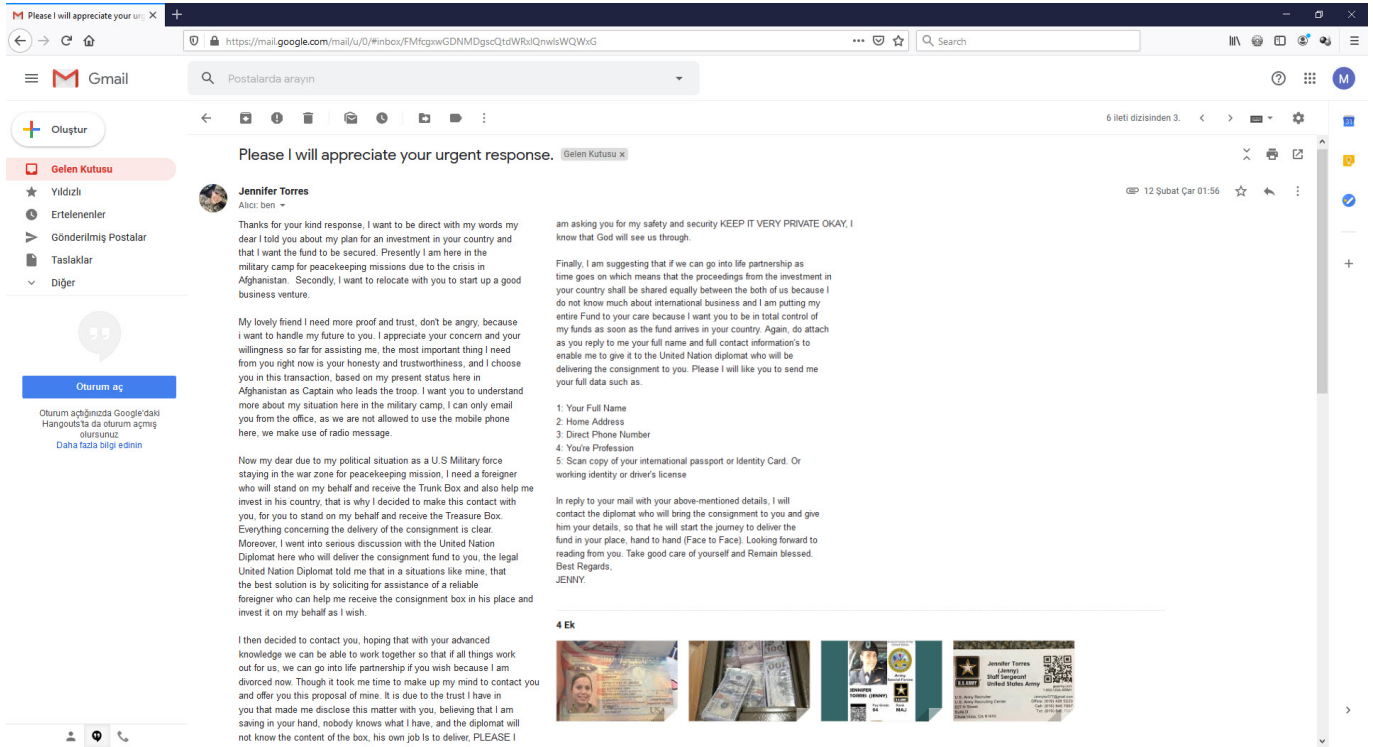


Gönderdiği ikinci e-postada hanım ablamız gerçekleştirdiği bir kurtarma operasyonunda içinde yüklü miktarda para bulunan bir kutu bulunduğunu, kendisine düşen payın tam tamına 3.7 milyon dolar olduğunu, bu parayı görevini tamamlayana kadar başka bir ülkeye çıkarmak istediğinden ve tabii ki benim yardımına ihtiyacı olduğundan bahsediyordu. :) Yine bu e-postasında da yeni resimler göndermeyi ihmal etmemişti.



Üçüncü e-postasında ise bir yandan güvenini kazanabilmek bir yandan da

sevkiyatı gerçekleştirebilmek için Birleşmiş Milletler diplomatını devreye sokacağı için kişisel bilgilerime, telefon numarama, pasaportumun veya kimliğimin o da olmazsa ehliyetimin taratılmış halini göndermemi istiyordu. Garanti olsun diye e-devletten ikametgahımı da hazır ettikten sonra gönderdiği yeni fotoğrafları incelemeye başladım. Kutu içinde yer alan 100'lük banknotları ve hanım ablamızın pasaportunu da gördükten sonra artık benden istediği tüm bilgilerimi göndermeye iyice ikna olmuşum. :)



“Vay efendim sen bana nasıl güvenmezsin” diye hanım ablamıza çıkıştıktan sonra gelen son e-postada hanım ablamız “Geçmişe bir sünger çekelim ama bir yandan da bilgilerini alayım” dedikten sonra yazışmayı sonlandırmaya ve epostalarda yer alan bilgileri incelemeye koyuldum.

Hello dear Gelen Kutusu x



Jennifer Torres

Alici: ben ▼

Please I mean no offense dear.

I'm only trying to be careful that's all, I would like to proceed with you on this so please let's move on

To proceed, dear, I will need some of your info so that I can register it with the cargo company that will deliver the box to you without any mistakes

Please I will need your info as follows

- 1: Your Full Name
- 2: Home Address
- 3: Direct Phone Number
- 4: You're Profession
- 5: Scan copy of your international passport or Identity Card. Or working identity or driver's license

In reply to your mail with your above-mentioned details, I will contact the diplomat who will bring the consignment to you and give him your details, so that he will start the journey to deliver the fund in your place, hand to hand (Face to Face). Looking forward to reading from you. Take good care of yourself and Remain blessed.
Best Regards,
JENNY.

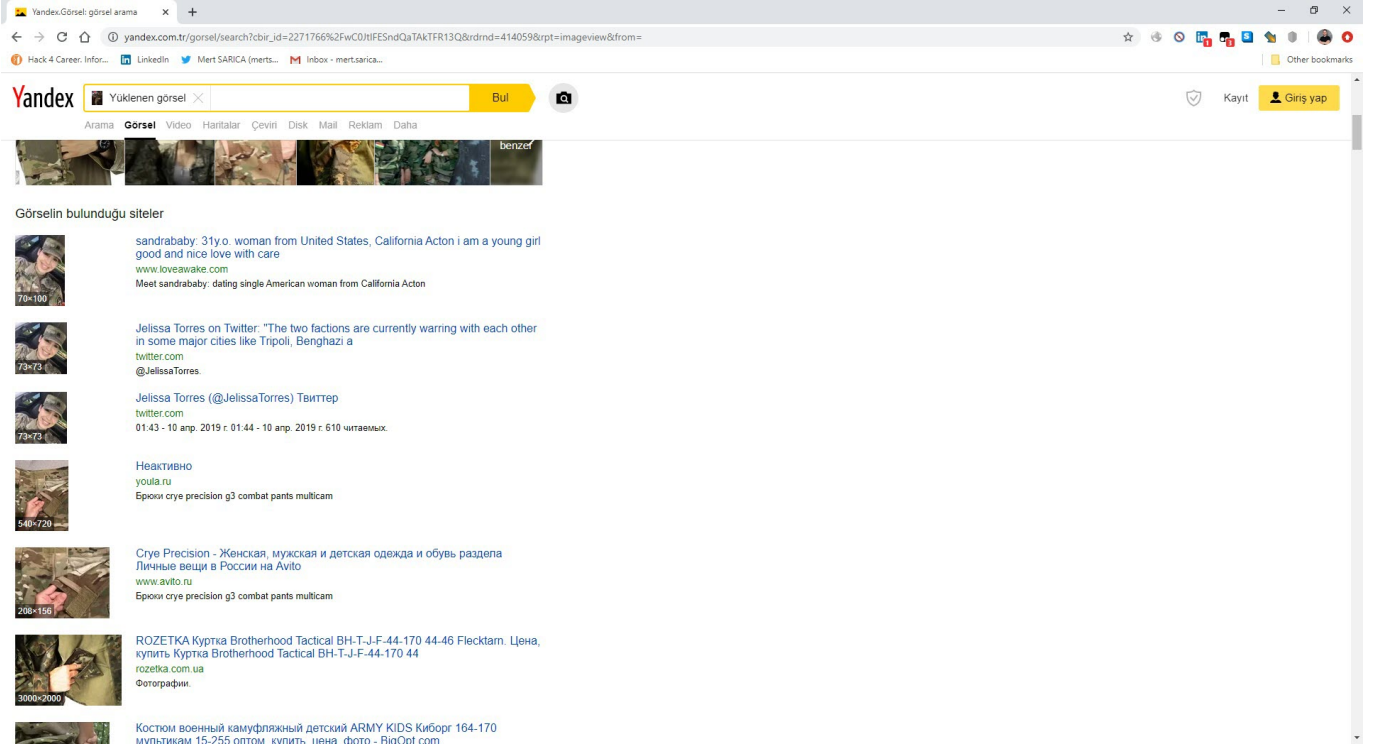
[Yes, I am interested.](#)

[I am not interested.](#)

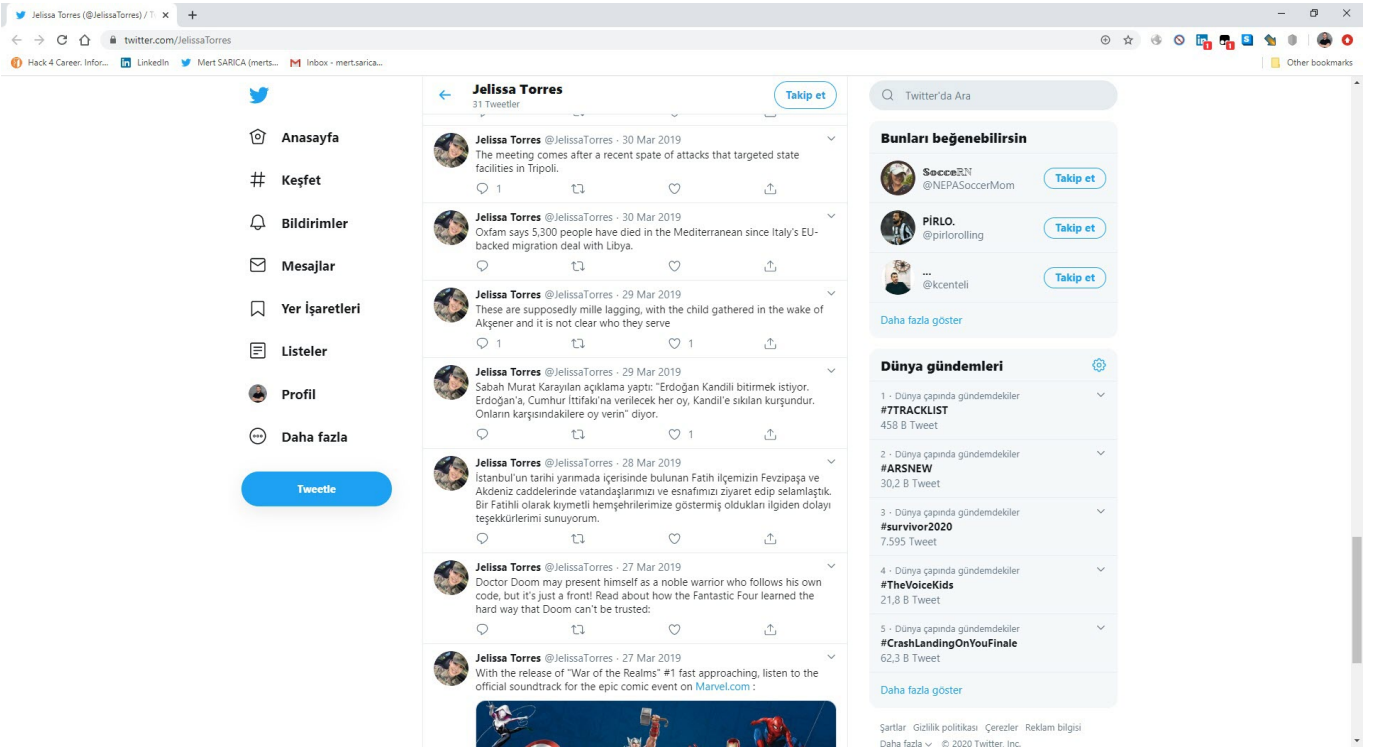
[Where are you from?](#)

Geçtiğimiz aylarda görsel arama motorlarının geldiği son noktayı konu alan faydalı bir yazı okuduktan sonra hanım ablamızın göndermiş olduğu e-postalara yakından göz atmaya karar verdim.

Üniformalı fotoğraflardan birini Yandex.Images arama motorunda arattığımda bu fotoğrafın kullanıldığı başka web siteleri olduğunu ve farklı bir isim (Jelissa Torres) altında sosyal medya hesabı olduğunu öğrendim.



@JelissaTorres Twitter hesabına göz attığımda Mayıs 2019 yılına kadar gönderdiği tweetler arasında Türkçe mesajlar da olması dikkatimi çekti. Bu mesajları Twitter'da arattığımda başka hesaplardan kopyala yapıştır yapılan mesajlar olduğunu öğrendim.



Twitter search results for "İstanbul'un tarihi yarımada içerisinde bulunan Fatih ilçesi".

Search filters:

- Kişiler: Herhangi birinden (checked), Takip ettiğin kişiler (unchecked)
- Konum: Herhangi bir yerde (checked), Yakınlarında (unchecked)

World trends:

- 1 · Dünya çapında gündemdekiler #ARSNEW 63,9 B Tweet
- 2 · Dünya çapında gündemdekiler #survivor2020 19,1 B Tweet
- 3 · Dünya çapında gündemdekiler #7TRACKLIST 505 B Tweet
- 4 · Dünya çapında gündemdekiler #GSVMS 25,6 B Tweet
- 5 · Dünya çapında gündemdekiler Saka 56,3 B Tweet

Who to follow:

John Opendakker @j_o_pendakker (Takip et)

Search results:

Popüler En Son Kişiler Fotoğraflar Videolar

Numan KURTULMUŞ @NumanKurtulmus · 27 Mar 2019
İstanbul'un tarihi yarımada içerisinde bulunan Fatih ilçemizin Fevzipaşa ve Akdeniz caddelerinde vatandaşlarımızı ve esnafımızı ziyaret edip selamlaştık. Bir Fatihli olarak kıymetli hemşehrilerimize göstermiş oldukları ilgiden dolayı teşekkürlerimi sunuyorum.

Jelissa Torres @JelissaTorres · 28 Mar 2019
İstanbul'un tarihi yarımada içerisinde bulunan Fatih ilçemizin Fevzipaşa ve Akdeniz caddelerinde vatandaşlarımızı ve esnafımızı ziyaret edip selamlaştık. Bir Fatihli olarak kıymetli hemşehrilerimize göstermiş oldukları ilgiden dolayı teşekkürlerimi sunuyorum.

Twitter search results for "The talks enter second week raising expectations that there could be some progress towards ending the Afghan war".

Search filters:

- Kişiler: Herhangi birinden (checked), Takip ettiğin kişiler (unchecked)
- Konum: Herhangi bir yerde (checked), Yakınlarında (unchecked)

World trends:

- 1 · Dünya çapında gündemdekiler #ARSNEW 64,1 B Tweet
- 2 · Dünya çapında gündemdekiler #survivor2020 19,1 B Tweet
- 3 · Dünya çapında gündemdekiler #7TRACKLIST 505 B Tweet
- 4 · Dünya çapında gündemdekiler #GSVMS 25,6 B Tweet
- 5 · Dünya çapında gündemdekiler Saka 56,3 B Tweet

Who to follow:

John Opendakker @j_o_pendakker (Takip et)

Search results:

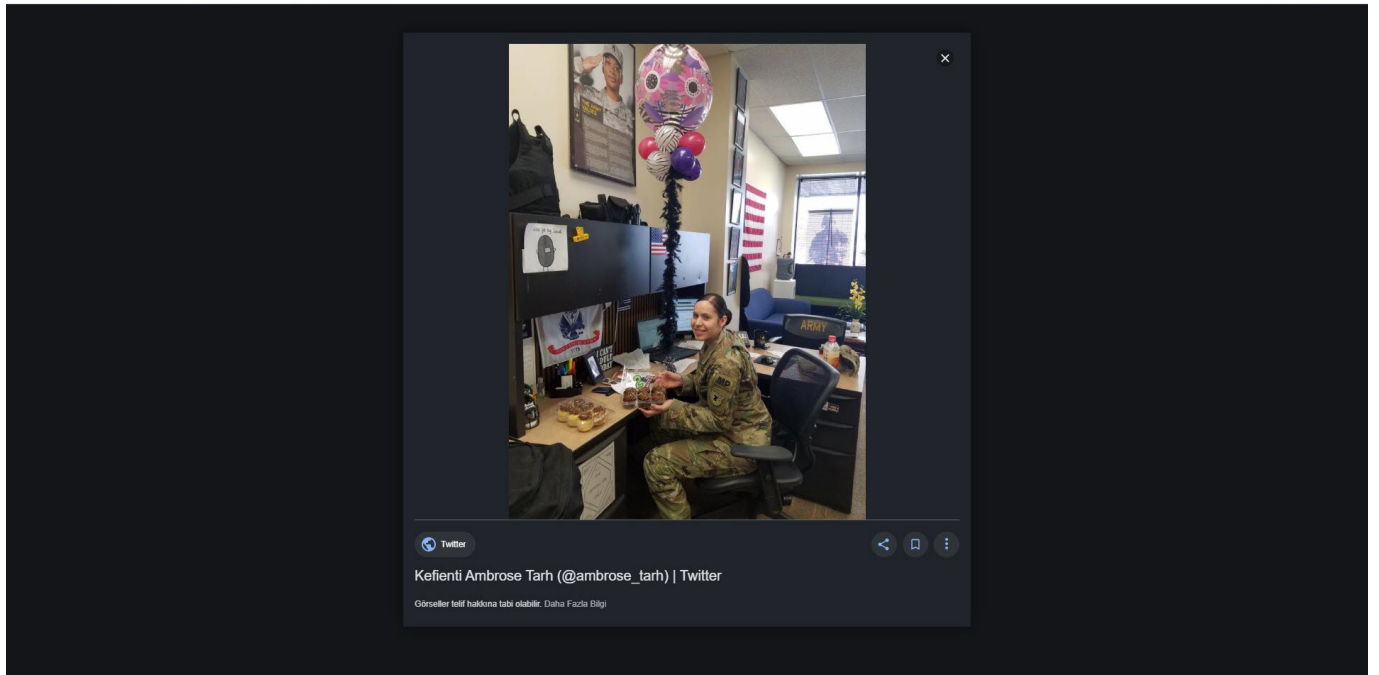
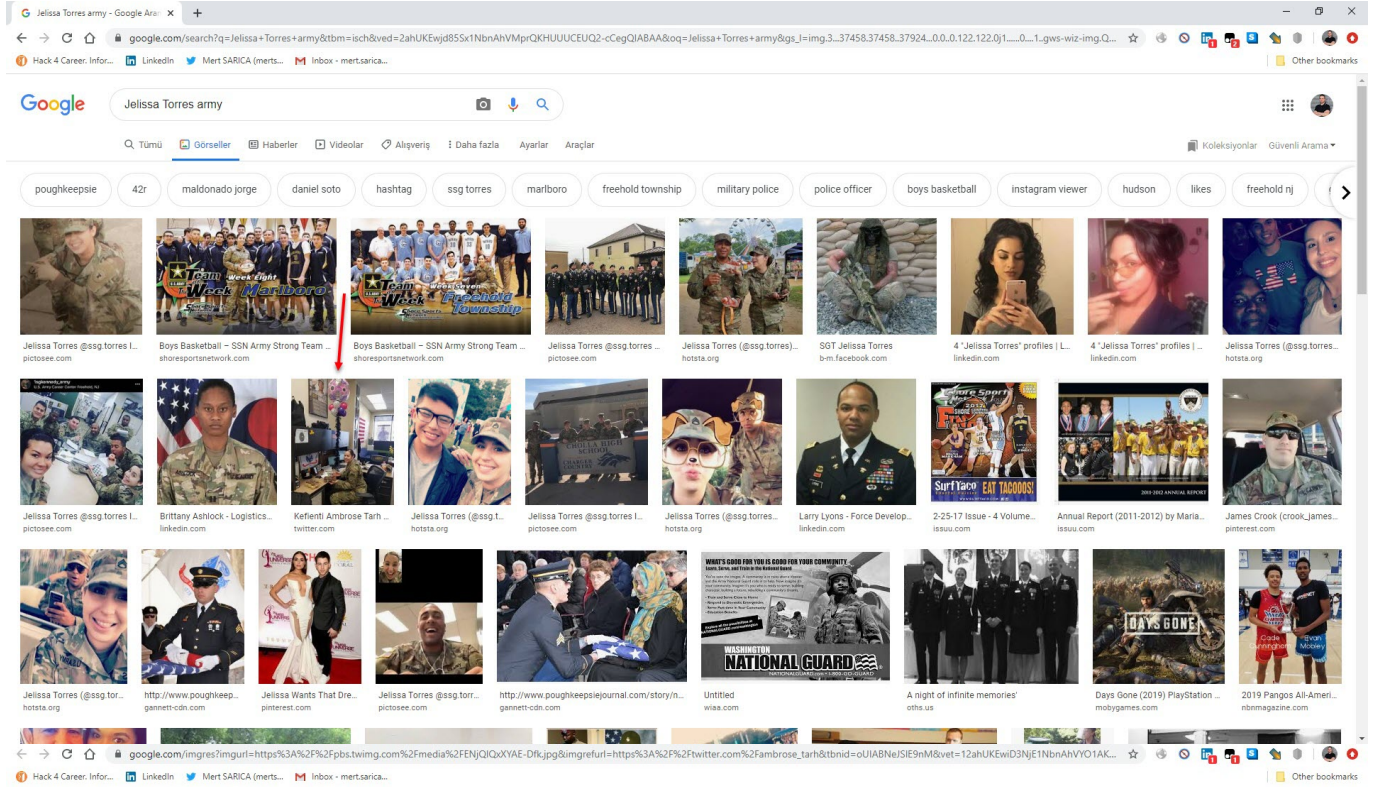
Popüler En Son Kişiler Fotoğraflar Videolar

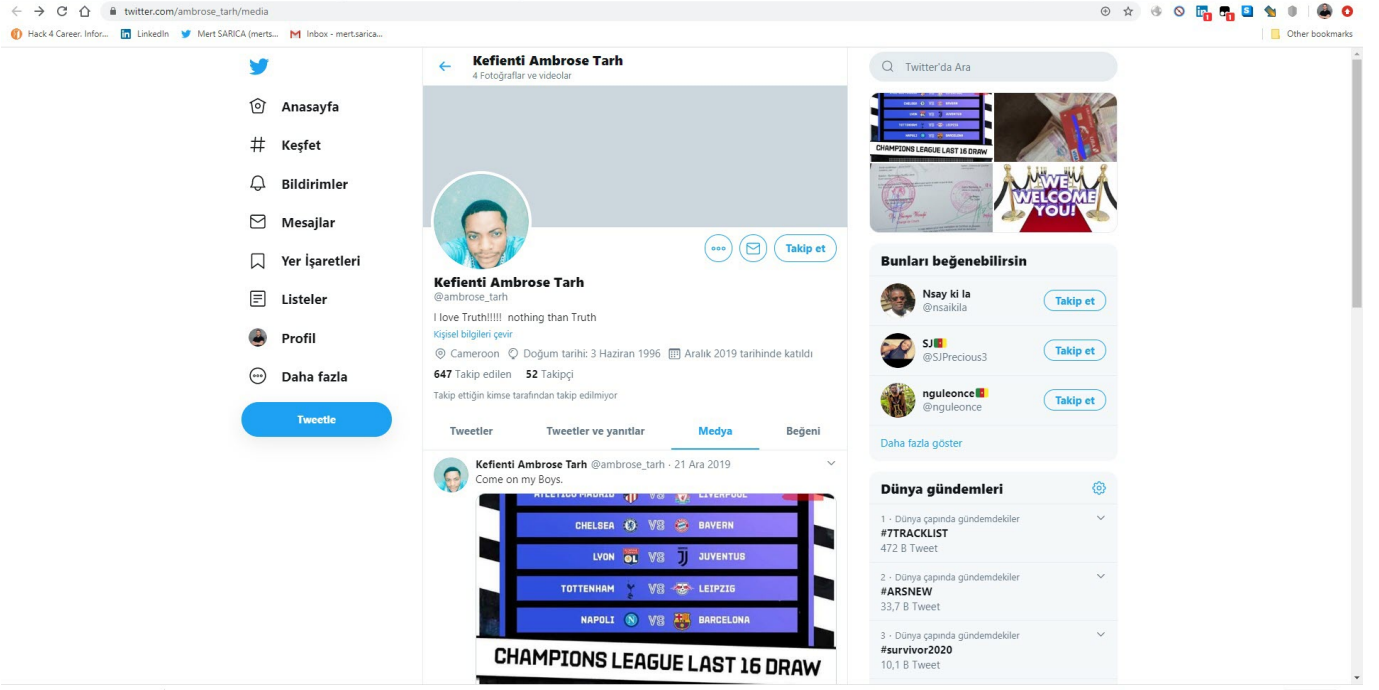
Jelissa Torres @JelissaTorres · 10 Nis 2019
The talks enter second week raising expectations that there could be some progress towards ending the Afghan war.

Ultrascan HUMINT @ultrascanhumint · 8 Mar 2019
US-Taliban talks: Two sides take a break amid bid for peace: The talks enter second week raising expectations that there could be some progress towards ending the Afghan war.

"Jelissa Torres army" anahtar kelimesi ile Google arama motorunda arama yaptığımda ise Kamerun'da bulunan bir kişinin bana gönderilen fotoğraflardan birini @ambrose_tarh Twitter hesabında paylaştığını daha sonrasında ise sildiğini farkettim. (OPSEC fail ?) Jelissa tarafından gönderilen e-postaların başlık bilgilerini kontrol ettiğimde gönderilen e-postaların saatleri ile Türkiye saati arasında -3 saat zaman farkı olduğunu gördüm. Kamerun'a komşu olan Senegal, Gana ve Gine ile Türkiye arasında 3 saat zaman farkı olduğunu göz önünde bulundurduğumda, bu e-postaların bu ülkelerin birinden Kamerunlu bu kişi veya bu kişi ile bağlantılı başka kişiler

tarafından gönderilmiş olma ihtimalinin yüksek olduğunu düşünmeye başladım.





From: Jennifer Torres <jennytor215@gmail.com>
Date: Tue, 11 Feb 2020 22:57:20 +0000
Message-ID: <CAKDKUFGecJAnYjFxsQ6H+hzK+WA5m8XL9Wmb42hA7dq+=Ai9xg@mail.gmail.com>
From: Jennifer Torres <jennytor215@gmail.com>
Date: Wed, 12 Feb 2020 22:06:14 +0000
Message-ID: <CAKDKUFGjz2XXchumc3YBN+hQvJqW=mfKtUHzyj8g__eN+JM=hg@mail.gmail.com>
From: Jennifer Torres <jennytor215@gmail.com>
Date: Mon, 10 Feb 2020 23:02:39 +0000
Message-ID: <CAKDKUFH12uHAujpzP9hePbaPLTLnBmkPqWqAUuDsRc=1W35AJQ@mail.gmail.com>
From: Jennifer Torres <jennytor215@gmail.com>
Date: Sat, 8 Feb 2020 22:33:09 +0000
Message-ID: <CAKDKUFFkNVdYTDkkyWHZ8RUX+r38qWC9Jz-rUqe0pYCuH4-DQ@mail.gmail.com>

J.T: 9 Şubat 01:32 (mesaj alındı)
M.S: 10 Şubat 22:18 (yanıt gönderildi)
J.T: 11 Şubat 02:01 (mesaj alındı)
M.S: 11 Şubat 22:45 (yanıt gönderildi)
J.T: 12 Şubat 01:56 (mesaj alındı)
M.S: 12 Şubat 20:44 (yanıt gönderildi)
J.T: 13 Şubat 01:05 (mesaj alındı)

World Clock interface showing a grid of cities and their current times. The interface is in Turkish and includes a sidebar with navigation options and a calendar on the right.

ARAÇLAR

Sayfanın yüklediği andaki mevcut zaman

24 saat moduna çevir

Abidjan	Per 6:09 OS	Akra	Per 6:09 OS	Addis Ababa	Per 9:09 OS
Ahmedabad	Per 11:39 OS	Basra	Per 9:09 OS	Al Başrat al Qadimah	Per 9:09 OS
Al Jizah	Per 8:09 OS	Al Mawşil al Jadidiah	Per 9:09 OS	Halep	Per 8:09 OS
İskenderiye	Per 8:09 OS	Algiers	Per 7:09 OS	Almatı	Cum 12:09 OS
Ankara	Per 8:09 OS	Asuncion	Per 3:09 OS	Bağdat	Per 9:09 OS
Bandung	Cum 1:09 OS	Bandung	Cum 1:09 OS	Bangkok	Cum 1:09 OS
Barcelona	Per 7:09 OS	Pekin	Cum 2:09 OS	Beyrut	Per 8:09 OS
Bekasi	Cum 1:09 OS	Belo Horizonte	Per 3:09 OS	Bangalore	Per 11:39 OS
Berlin	Per 7:09 OS	Bhopal	Per 11:39 OS	Bogota	Per 1:09 OS
Brasilia	Per 3:09 OS	Brooklyn	Per 2:09 OS	Bükreş	Per 8:09 OS
Budapeşte	Per 7:09 OS	Buenos Aires	Per 3:09 OS	Kahire	Per 8:09 OS
Calı	Per 1:09 OS	Camayenne	Per 6:09 OS	Cape Town	Per 8:09 OS
Karakas	Per 1:39 OS	Casablanca	Per 6:09 OS	Changchun	Cum 2:09 OS
Changsha	Cum 2:09 OS	Chengdu	Cum 2:09 OS	Chennai	Per 11:39 OS
Şikago	Per 1:09 OS	Chittagong	Cum 12:09 OS	Chongqing	Cum 2:09 OS
Ciudad Juárez	Per 12:09 OS	Conakry	Per 6:09 OS	Curtiba	Per 3:09 OS
Dakar	Per 6:09 OS	Dallan	Cum 2:09 OS	Şam	Per 8:09 OS
Dar es Salaam	Per 9:09 OS	Delhi	Per 11:39 OS	Dakka	Cum 12:09 OS
Durban	Per 8:09 OS	Ecatepec	Per 12:09 OS	Eşfahan	Per 9:39 OS
Faialabad	Per 11:09 OS	Fortaleza	Per 3:09 OS	Grand Dakar	Per 6:09 OS
Guadalajara	Per 12:09 OS	Guangzhou	Cum 2:09 OS	Guayaquil	Per 1:09 OS

Dünya Saati
The Time Now dünyanın bütün şehirleri ile senkronize doğru (Amerikan seyyum saatleri) zaman hizmetleri sunan güvenilir bir araçtır.

Zaman Dilimi Dönüştürme:
CST » EST
EST » GMT

21:09:43
12 Mart 2020 Perşembe

Mart 2020

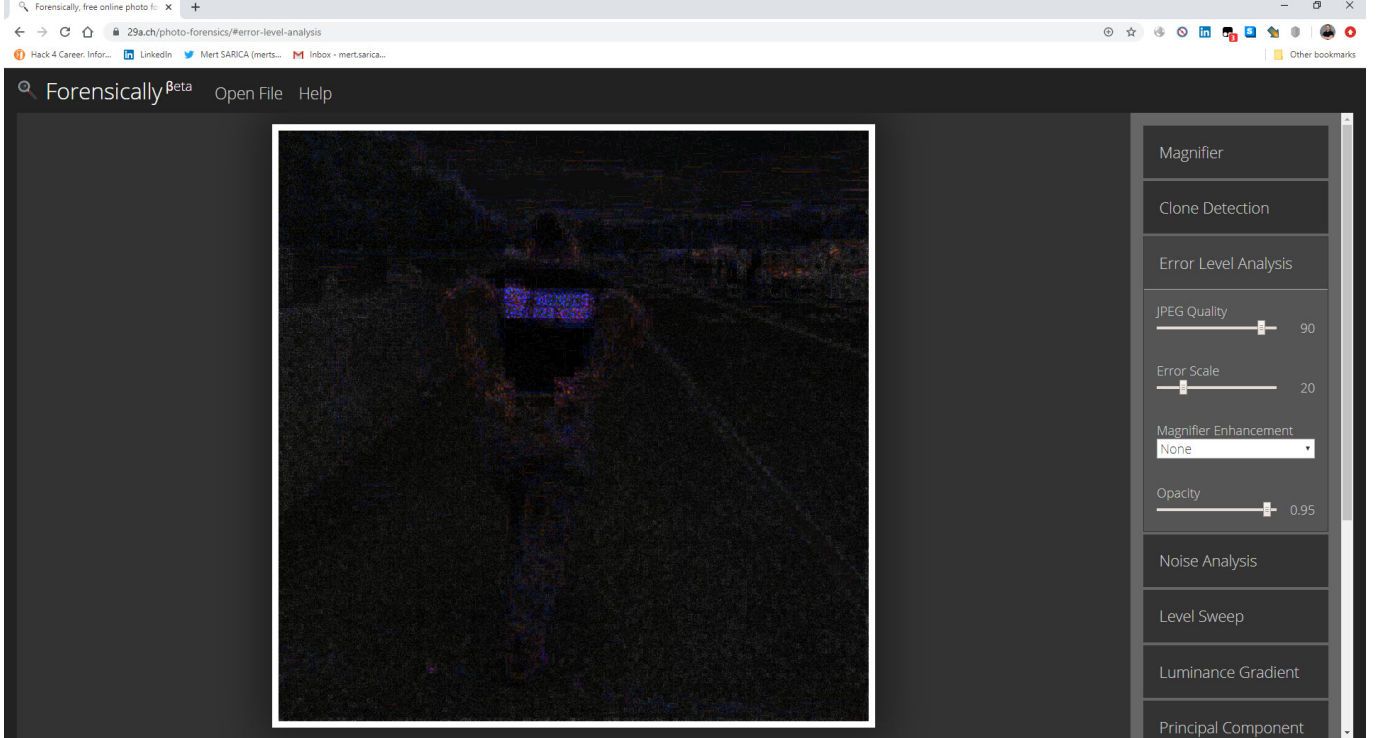
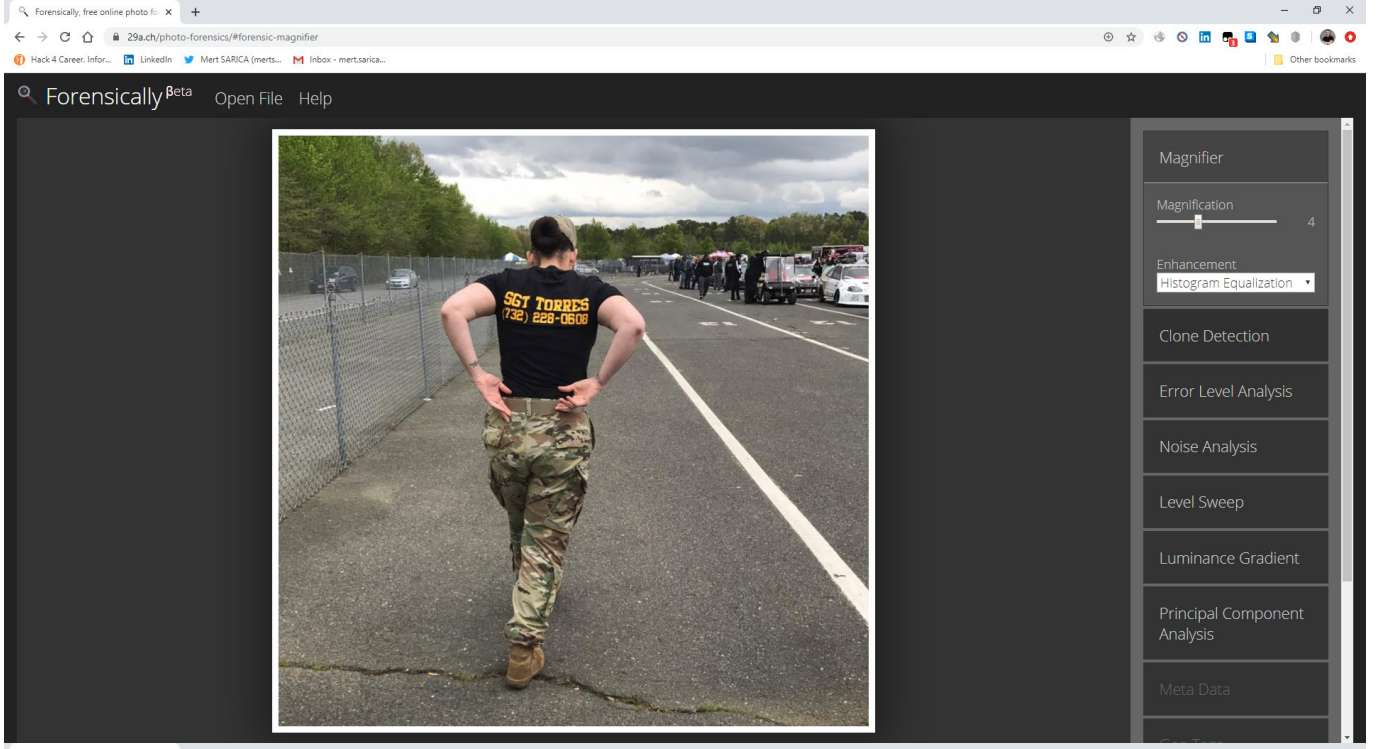
Pt	Sa	Ça	Pe	Cu	Ot	Pa
24	25	26	27	28	29	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today
No events

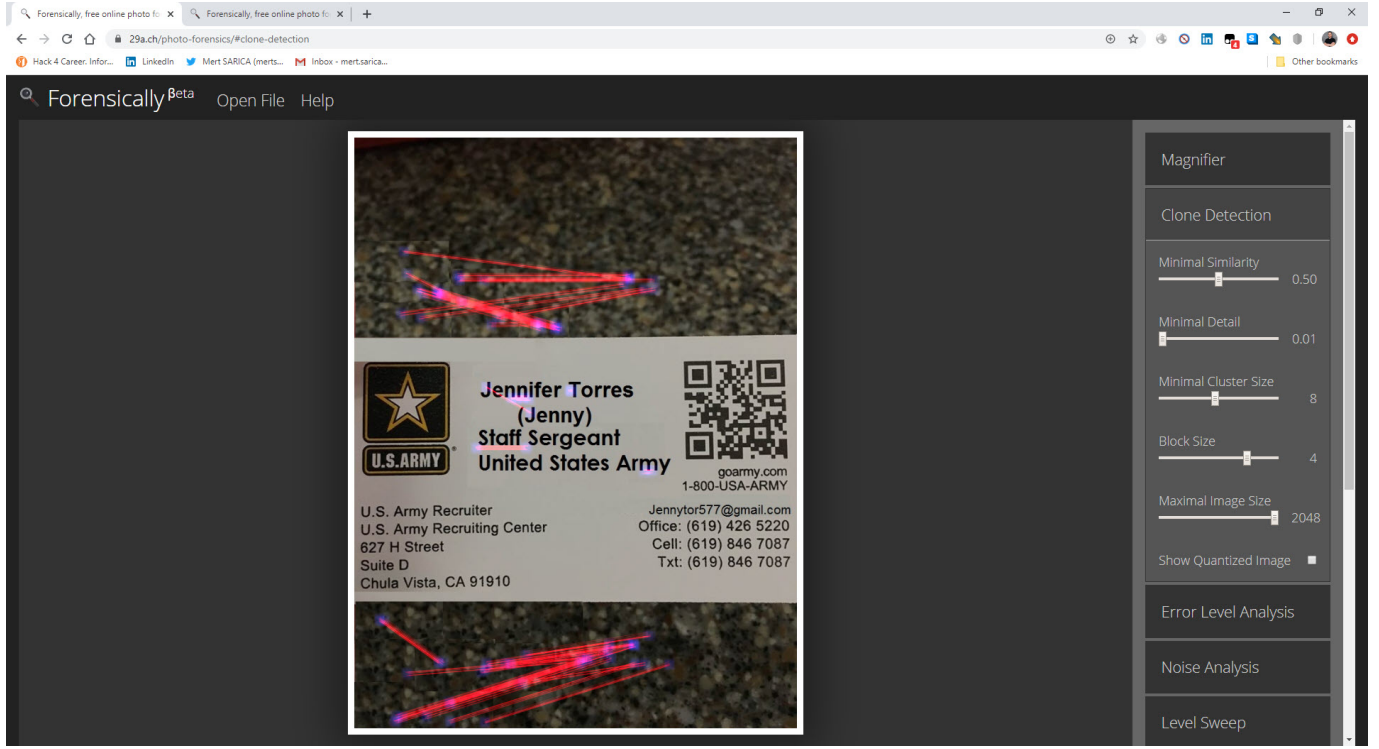
Hide agenda

Fotoğraflara hızlıca göz attığımda amatörce yapılan fotomontajlar hemen dikkatimi çekti. Bundan 7 yıl önce kaleme aldığım Manipüle Edilmiş Fotoğraf Analizi blog yazımda olduğu gibi fotoğrafları ELA tekniği ve Forensically web uygulamasında yer alan kopyalama tespiti tekniği ile analiz etmeye başladım.

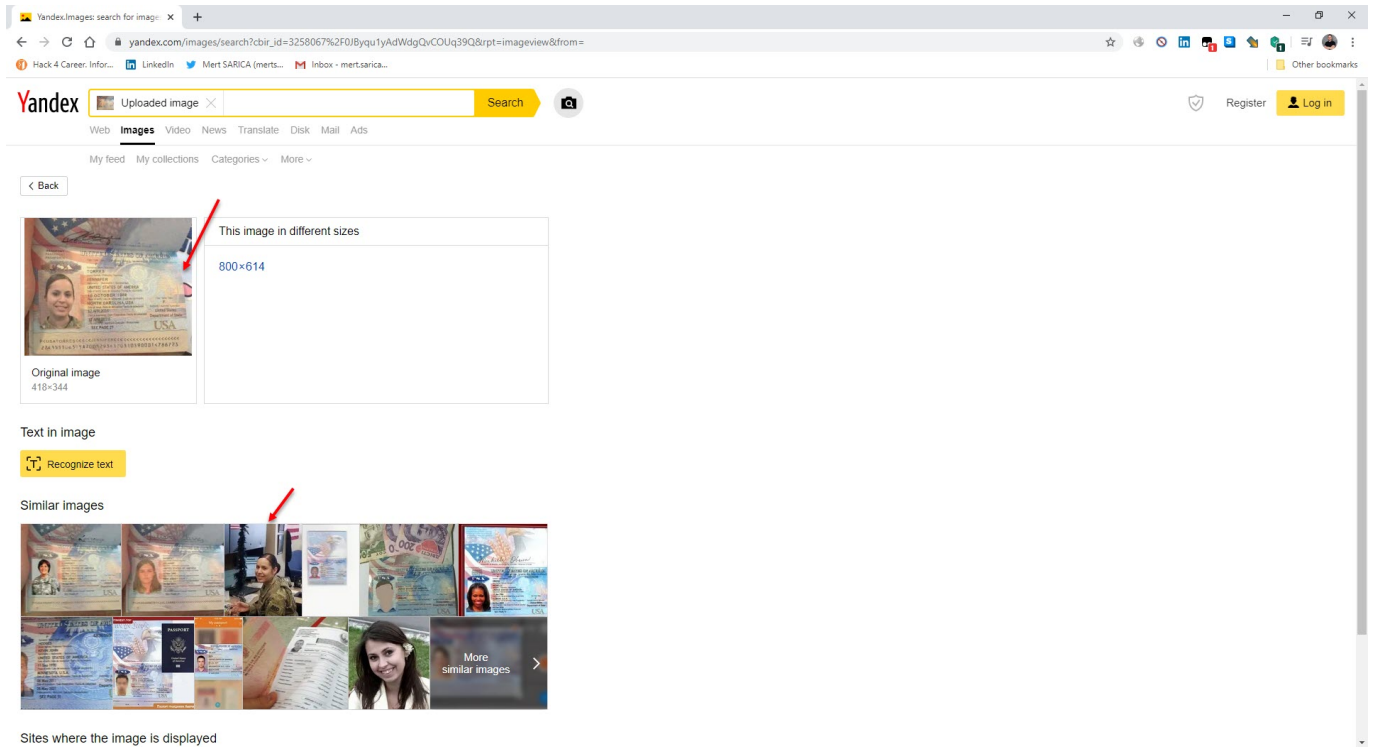
Kimsenin damgalı eşek gibi tişörtünün sırt kısmına adını ve telefon numarasını yazdırmayacağını düşünerek bu fotoğrafı ELA tekniği ile analiz ettiğimde, tahmin ettiğim üzere sırt kısmında yer alan isim ve telefon numarasının sonradan bu fotoğrafa eklendiğini tespit ettim.



Her ne kadar kartvizitinin yer aldığı fotoğrafta gözle görülür bir şekilde fotomontaj olduğu görülse de teyit etmek için Clone Detection sayfasından faydalanarak bu fotoğraf üzerinde çok sayıda kopyalama işlemi yapıldığını tespit ettim.



Son olarak pasaport fotoğrafını Yandex.Images üzerinde arattığımda ise arka plandaki pembe işaretin aynı olduğu benzer sahte pasaport fotoğraflarını bularak pasaportun da sahte olduğunu teyit etmiş oldum.





Jennifer ile yazışmayı kestikten sonra aç gözlü dolandırıcılar tabii ki peşimi bırakmayıp yeni mesajlar ile LinkedIn mesaj kutumu meşgul etmeye bir süre daha devam ettiler.

Home

My Network

Jobs

Messaging

Notifications

Me

Work

Reactivate Premium

Invitations

Manage



Niffer Pandey

Staff Sergeant at US Army

Muhammed Hacı Ahmet Özsarı and 2 others

Ignore

Accept

Profilinizi kontrol ettim ve ilginç buldum ve bana iş amaçlı özel e-posta adresimle (jenipher119@gmail.com) geri yazabiliyorsanız minnettar olacağım Veya bana e-posta adresinizi de gönderebilirsiniz doğrudan kendim sizinle temasa geç! Gelen kutunuzu bekliyorum. [See less](#)

Reply to Niffer

Görünen o ki bir zamanların oldukça popüler Nijeryalı Prens dolandırıcıları artık faaliyetlerine LinkedIn üzerinde devam etme kararı almışlar dolayısıyla dikkatli olmakta ve çevrenizdekileri uyarmakta fayda olacağına inanıyorum.

Ülke olarak COVID-19 salgınını geride bırakacağımız sağlıklı günlerde yeni bir yazı ile tekrar görüşmek dileğiyle herkese sağlıklı ve güvenli günler dilerim.