Operation Brutus (HACKTORIA)

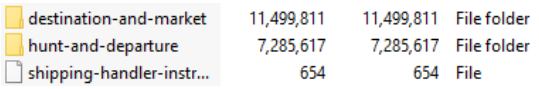
TABLE OF CONTENTS

Introduction

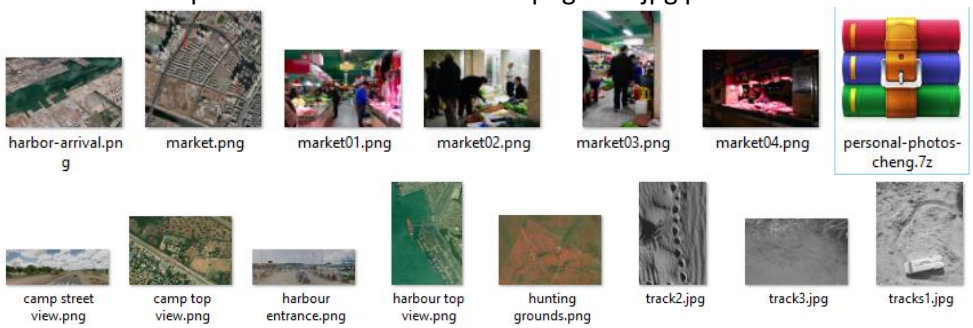
Back in the Operation Runner, Hacktoria's agents were able to catch Maksim Kotova and interrogate him. Besides other pieces of information, he offered some details about a wildlife smuggling operation and a "handler file" (a collection of information intended for the person in charge of the whole operation, from where the animals were hunted to wherever people bought them) plus some personal files in an encrypted folder.

In this monthly CTF organized by Hacktoria I had to map the entire operation, searching for lots of names, locations and other objectives that you can find below.

I got a .zip file containing two folders named "destination-and-market", "hunt-and-departure" and a file named "shipping-handler-instructions".



Further, the folder "destination-and-market" contained 6 .png photos and a zipped file named "personal-photos-cheng.7z" (which was encrypted) and the folder "hunt-and-departure" which contained 8 .png and .jpg photos.



Based on those files and images I had to find out these 14 pieces of information:

1.	Scientific name of the animal and subspecies
2.	Location of the hunter camp
3.	Location of the hunting grounds
4.	Harbor location the shipment leaves from
5.	Harbor location the shipment arrives in
6.	Location of the market
7.	Date and time of arrival
8.	Shipment ID
9.	Name of the ship
10.	Shipment handler full name
11.	Shipment handler personal phone number
12.	Shipment handler personal e-mail
13.	Name of contact at the market
14.	Description of contact at the market (visual)

Part 1. Translating, WEBINT & cracking passwords

The file "shipping-handler-instructions" didn't have an extension, so I opened it up with **notepad++**. You can see its contents below:

panderoshipping.cf

您好， 这是本月狩猎和装运的快速说明。 **通常的狩**猎场和动物，这次可能会带一个Sheng语翻译，如果需要，请拨打 +254 41 555 555 0。 **一旦您**获得 200 **只**动物，请安排发货，并确保在网站上已为客户准备了追踪的详细信息。 **您的市**场联系人是 Wendy Liu， **她会**带上ID证件并在码头等候。 **在某些**时候，她可能会通过电子邮件向您发送有关货件 ID **的信息。不用担心她会**说中文，这次不会使用英文。 **她在当地有交通安排会将**货物运往市场。 **她将穿着一件**蓝色雨衣和红色围巾，以供识别。

I extracted the data that I was able to understand: *panderoshipping.cf*, *Sheng*, *+254 41 555 555 0* – a phone number with a Kenyan prefix (+254), so I got a location, *ID* and *Wendy Liu* (see the full translation below).

I translated the full text with **Google Translate** (sometimes I do this piece by piece to get better results).

panderoshipping.cf Hi, here's a quick note on hunting and shipping this month. **The usual hunting grounds and animals**, this time may bring a **Sheng language interpreter**, **call +254 41 555 555 0** if needed. Once you have **200 animals**, schedule the shipment and make sure you have the **tracking details** ready for the customer on the **website**. Your **marketing contact** is **Wendy Liu** who will bring her ID and wait at **the dock**. At some point, she may **email you information about the shipment ID**. Don't worry she can speak **Chinese**, not English this time. She has **local transportation arrangements** to transport the goods to the market. She will be wearing a **blue raincoat** and **red scarf** for identification.

I took them piece by piece.
A. What was panderoshipping.cf? Initially, I thought that .cf was an extension and I kept reading about it, but it didn't make sense at all (something about SMTP protocol configuration). What could it be? A website? Yeah, WEBINT time. 😎

The first step I did was getting its IP and whois details. For IP one can use **ping**, **nslookup** (for command-line) or simpler online tools like **DNS Lookup**. In this particular case, I found two IPv4 addresses both of them located in San Francisco (USA) and the website wasn't registered, so that didn't help me very much.

The second step was extracting information that the website provided in the contact section:

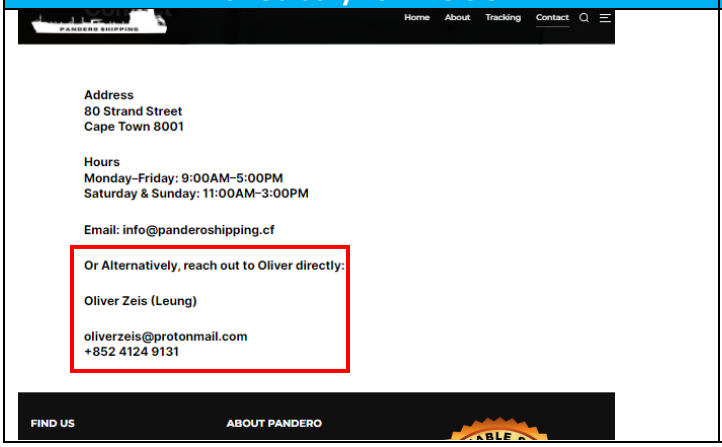
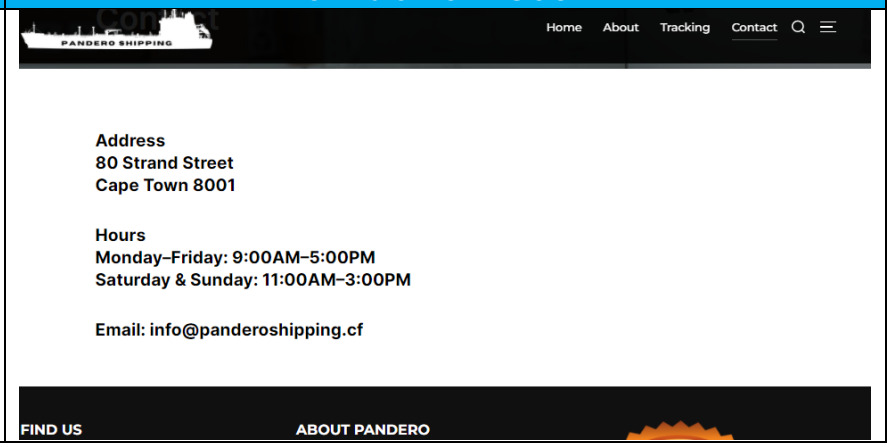
- Address: *80 Strand Street Cape Town 8001* (an office center located right in the center of Cape Town); I thought about searching all the companies that were registered with that address, but based on the fact that it was an office center, definitely there would have been too many results and false leads;

- E-mail: info@panderoshipping.cf (I googled it a little bit, but nothing relevant at first sight);
- I also inspected the website's source code, but I didn't find anything useful.

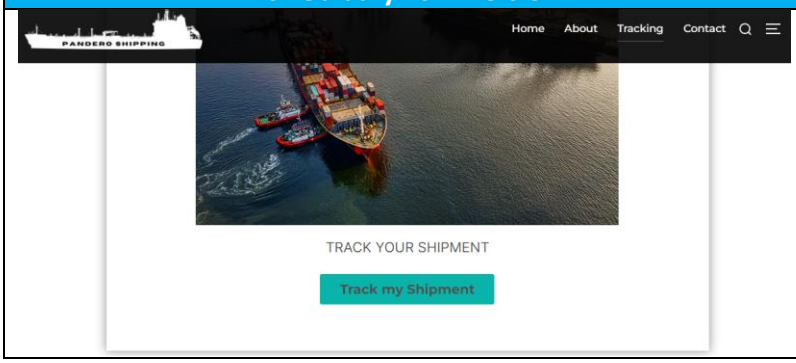
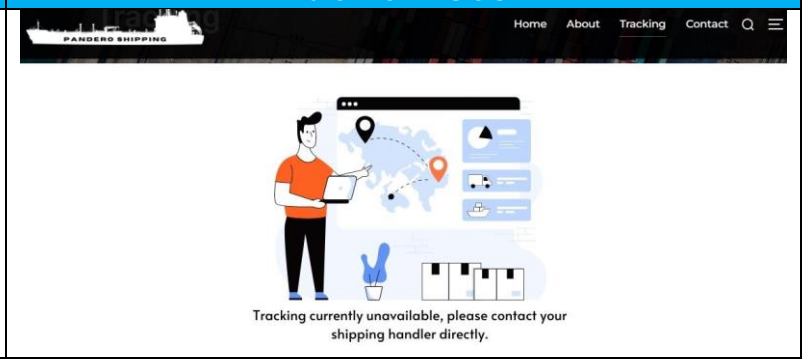
The third step was using **WayBackMachine** to see if there was any snapshot of an older version of the website. Well, it was saved two times: on 10.02.2022 and 04.03.2022.

On 10.02.2022 the website's contact section looked different and it had additional information (contact for shipment and a tracking system):

- Contact for shipment: name *Oliver Zeis (Leung)*, e-mail *oliverzeis@protonmail.com* and a phone number *+852 4124 9131* with a Hong Kong prefix (at this point I had two contacts: one from Kenya and one from Hong Kong).
  3/14 ☑
  Shipment handler full name: Oliver Zeis (Leung)
  Shipment handler personal phone number: +852 4124 9131
  Shipment handler personal e-mail: oliverzeis@protonmail.com

10 February 2022 version	04 March 2022 version
	

- A tracking system for shipment ID, which looked unavailable on the current website.

10 February 2022 version	March 2022 version
	

B. Continuing with the information from the Chinese text:

- *"the usual hunting grounds and animals"*: so the operation did happen at least once in the past;
- a phone number *+254 41 555 555 0* for a Sheng language interpreter if needed: as mentioned above, the prefix of the number was specific to Kenya (I didn't insist very much on the number because at first look there was no public information about it);
- *"a marketing contact named Wendy Liu who will be waiting at the dock wearing a blue raincoat and a red scarf"* (also, she might have provided the smuggler a shipment ID via e-mail): 5/14 ☑
  Name of contact at the market: Wendy Liu
  Description of contact at the market (visual): wearing a blue raincoat and a red scarf

I didn't like the fact that I had a password-protected file that might have had something important there. *(Yeah, that "personal-photos-cheng.7z" file)*. I'd never cracked a password before so I started to read about the encryption method used by 7-zip and similar ways of cracking it. The encryption method is AES-256 and it's one of the most secure because of its key length size. To crack the password, one has two methods at hand: *brute force* (guessing based on multiple combinations of characters) or *dictionary attack* (guessing based on a list of passwords). I spent a few hours on researching various cracking methods and I came across **7z2hashcat** (a tool, written in Perl, that can convert password-protected .7z files into hashes) and **hashcat** for resolving the hash. Fair enough, I downloaded the **7z2hashcat** Perl script, Strawberry Perl (a perl environment for Windows to run the script) and **hashcat 6.2.0** (I had some GPU problems with 6.2.5 version).

One line code in the Windows PowerShell and I got the hash. The next step was to pass it to **hashcat** to resolve it (*hashcat has a specific hash mode for .7z which is 11600*). Brute force or dictionary? I chose the latter (thinking that it would be simpler) and I used one of the well-known password databases (rockyou.txt) which contained around 14m passwords. After a couple of hours, the hashcat was exhausted (which meant that there was no match). I tried with brute force, too, but it got to a point where it would've taken a couple of days to crack it because I had no clue about it (I didn't know if the password contained only lowercase letters or if it contained some numbers/symbols so I wasn't able to narrow down the number of possibilities).

I tried a lot of combinations on google with different dorks, hoping that there might be some information about the file, but nothing. I also checked some passwords that came up in my mind, but nothing again.

Part 2. GEOINT

So, I moved to those images from the abovementioned folders.

HUNTER CAMP

Camp Street View

Camp Top View

Initial reconnaissance (I already knew that if the smuggler needed a Sheng translator, he had to call a Kenyan phone number, based on the Chinese text extracted from *shipping-handler-instructions* file):

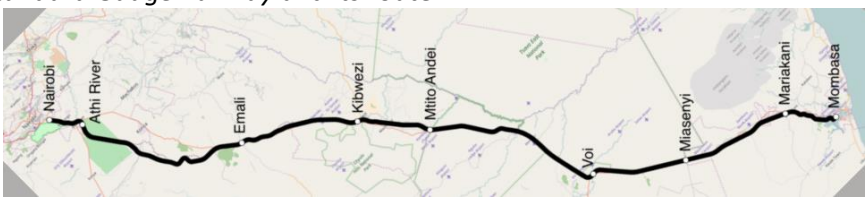
- the driving side was on the left (according to google, in Kenya people drive on the left side of the road);
- the other part of the road seemed to be under construction;
- a building that looked like a local mosque right in the center of the image (statistically, according to Wikipedia, Christianity is the predominant religion in Kenya with 85.52% of the total population, being followed by Islam with 10.91% percent of the total population);

- a gas station in the right with a "feng-shui" looking logo.

Initially, I wanted to OCR that name out of the roof of the gas station but I left it as the ultimate solution. I started to search for some gas/oil/kerosene stations in Kenya, but none of them seemed to have that logo. Also, I looked for some mosques but that particular one didn't show up.

If you look at the top view of the location, you can see that it is a rural-like area so there are small chances that something related to it will show up in search engines results. But, if you look closely at that top view image, in the top right corner you can see something special. A railway.

Researching the railway infrastructure in Kenya, I found that China planned to invest in its restoration to link the dock of Mombasa to Uganda. I was interested to see where the railway starts from and where it ends. I found on Wikipedia information about *Mombasa–Nairobi Standard Gauge Railway* and its route:



So, I started from the Kenya Railway station Shimanzi in Mombasa and I went along the railway until I found the target located in **Mackinnon Road** (95km from city Mombasa).

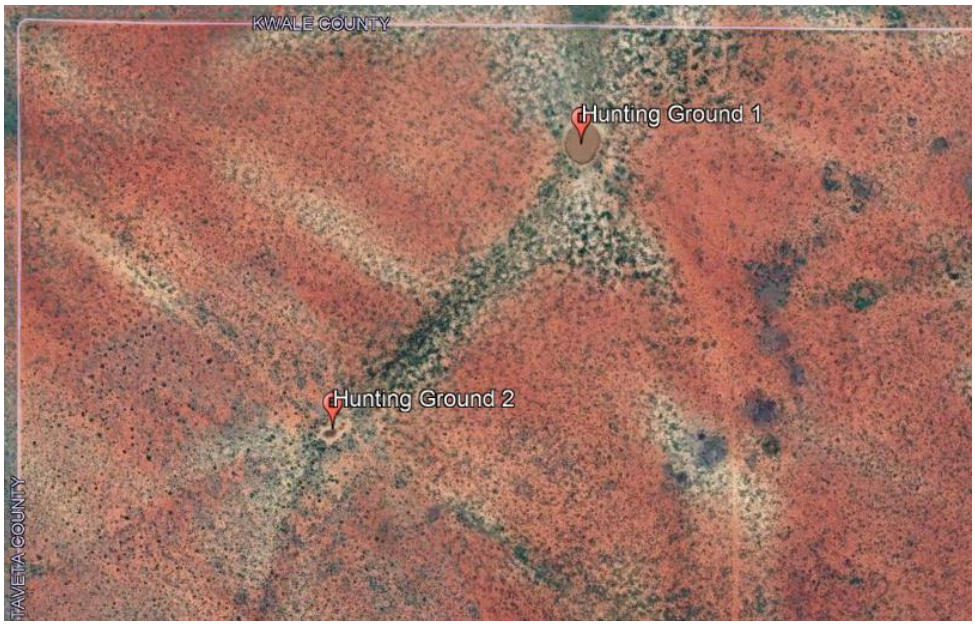
The gas station and the mosque (images taken from Google Maps Street View):

6/14 ☑

Location of the hunter camp: 3°43'14.89"S 39° 1'46.34"E near Ebagh Ali Shah Mosque (Mackinon Road)

HUNTING GROUNDS

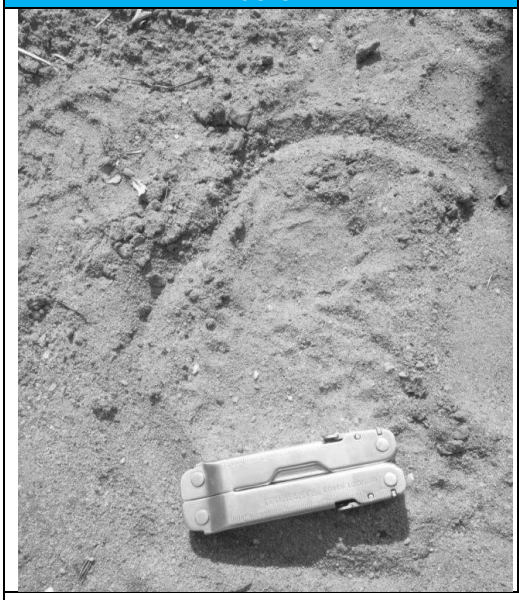
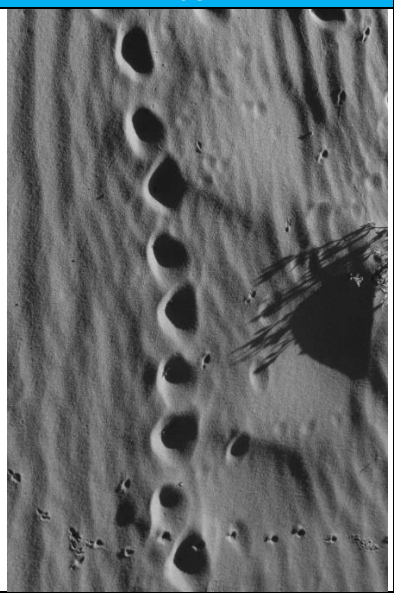
I thought that the hunting grounds couldn't be far away from the hunter camp because of OPEX reasons. At the same time, the terrain around that zone seemed to be semi-arid which matched the image. It took only a couple of minutes of grid-searching to find it.



7/14 ☑

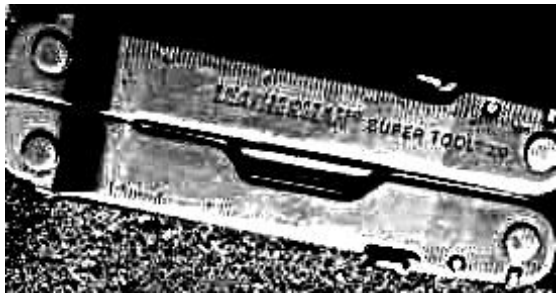
Location of the hunter grounds: 3°38'58.22"S 38°59'3.29"E and 3°39'13.49"S 38°58'17.83"E

I also had to find the scientific name of the animal that was hunted and its subspecies. For that I had those tracks below.

Tracks1	Track2	Track3
		

- The object from the first image had an inscription on it:

- I added some darken effects, lowered the gamma bright, added some contrast, flipped the image, sharpened it and I got these results:



- A **LEATHERMAN SUPER TOOL 100**

SUPER TOOL®

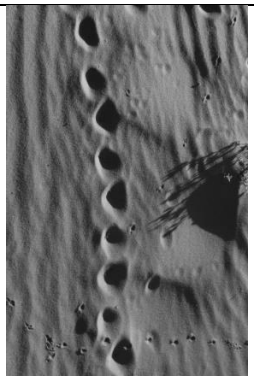
The Super Tool® is the biggest, strongest multi-purpose tool in our line. All blades have a unique locking mechanism, which is the toughest, most precise locking mechanism available on any multi-purpose tool. Its heavy-duty capabilities make the Super Tool® especially useful for the professional, but anyone who needs the extra safety of ten locking blades will be glad to have this workhorse at their fingertips.

SPECS
Primary Blade Length: 3 in | 7.62 cm
Closed Length: 4.5 in | 11.5 cm
Weight: 9 oz | 260 g

MATERIALS
Stainless Steel

TOOLS
Needlenose Pliers, Regular Pliers, Hard-wire Cutters, Wire Cutters, Electrical Crimper, Wire Stripper, 420HC Blade, 420HC Serrated Knife, Saw, Awl, Ruler (9 in | 22 cm), Can Opener, Bottle Opener, Wood/Metal File, Phillips Screwdriver, Large Screwdriver, Medium Screwdriver, Small Screwdriver

- Well, you don't need that to hunt birds.
- I researched the subject a little bit and I came across an INTERPOL article where this matter was discussed. Elephants, asian tigers and pangolins were the most hunted animals in Africa, including Kenya (https://www.interpol.int/News-and-Events/News/2021/The-Kenyan-officers-on-the-front-lines-against-wildlife-crime).
- I searched for elephants, tigers and pangolins footprints and I found a reddit post about pangolins' distinct footprints with an image from ©Pangolin Research Mundulea 2012 which was identical with those from the track2 image.

vs


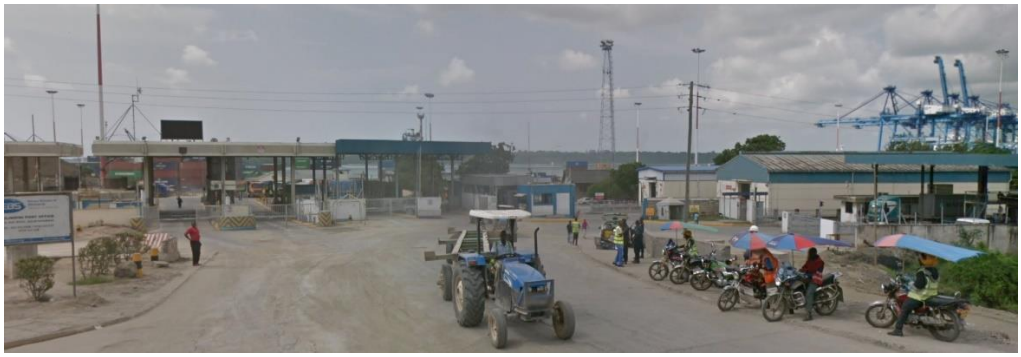
- Further, I had to find its scientific name and subspecies. According to Wikipedia, the scientific name of pangolin is *Pholidota* and according to this article (https://www.worldwildlife.org/species/pangolin) four species live in Africa: Black-bellied pangolin (Phataginus tetradactyla), White-bellied pangolin (Phataginus tricuspis), Giant Ground pangolin (Smutsia gigantea) and Temminck's Ground pangolin (Smutsia temminckii).

8/14 ☑

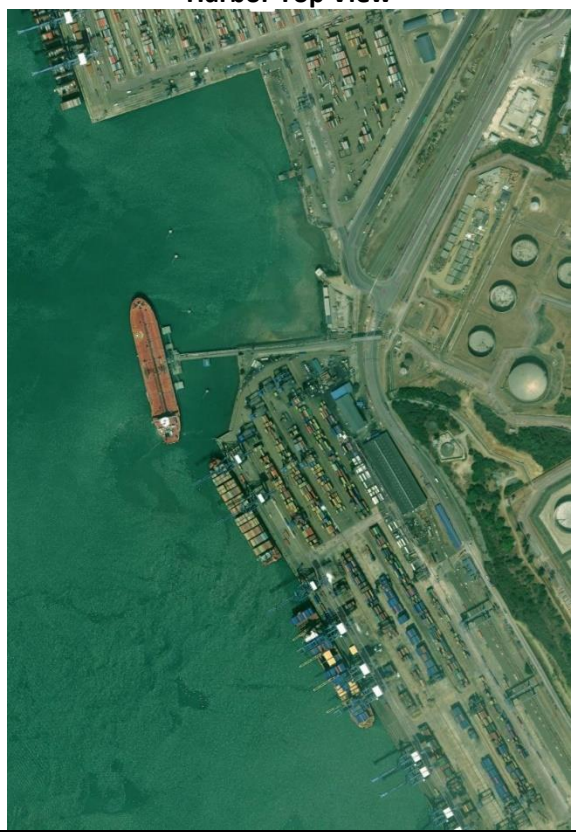
Scientific name of the animal and subspecies: Pholidota (subspecies: Phataginus tetradactyla, Phataginus tricuspis, Smutsia gigantea, Smutsia temminckii.

HARBOR WHERE THE SHIPMENT LEAVES FROM

Harbor Entrance

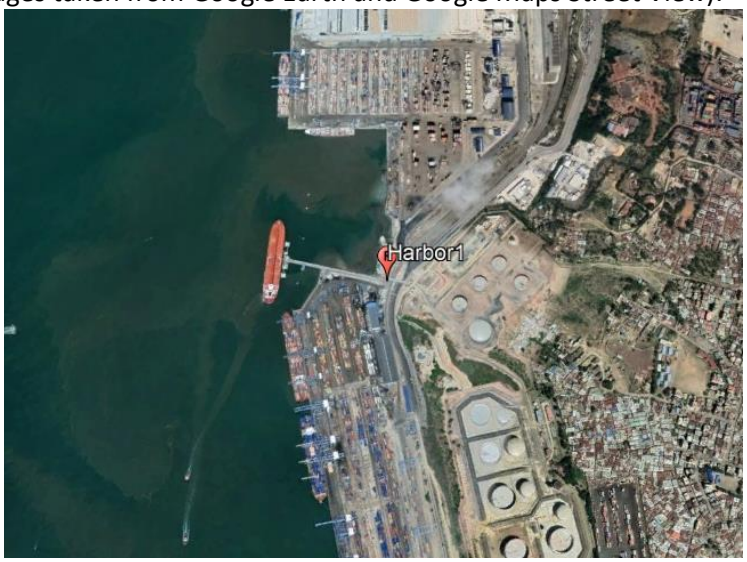


Harbor Top View



I didn't spend too much time on this one. When I was searching for the hunter camp I read about the railway infrastructure starting from the dock of Mombasa, so that was the first location that I checked based on the fact that a smuggler will take in consideration OPEX optimization.

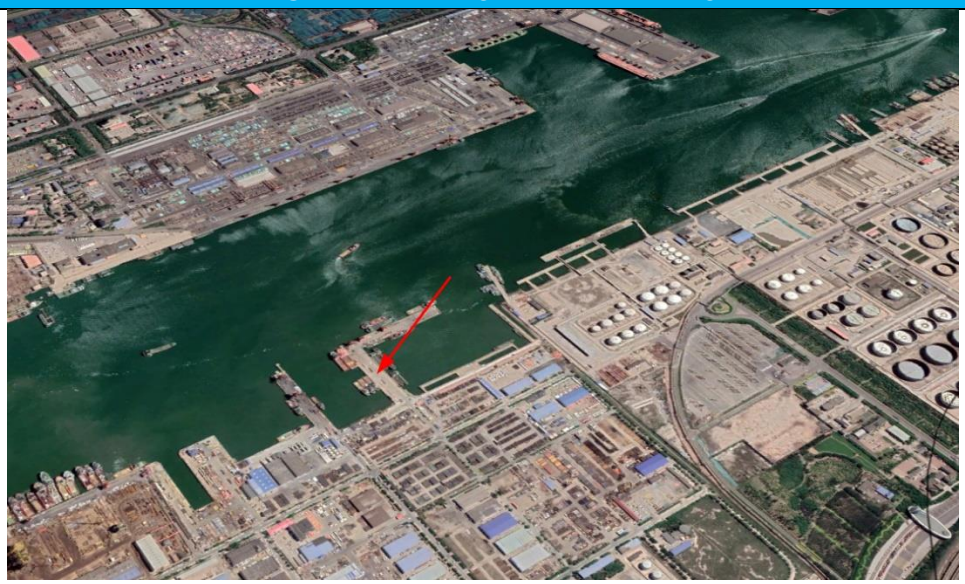
The harbor and its entrance (images taken from Google Earth and Google Maps Street View):



9/14 ☑

Harbor location the shipment leaves from: Kilindini Harbour/Mombasa Port 4° 2'31.57"S 39°37'57.35"E (address: Old Mombasa Port, Sir Mbarak Hinawy Road, Mombasa, Kenya)

HARBOR WHERE THE SHIPMENT ARRIVES IN



I assumed the harbor where the shipment arrives in was in China or Hong Kong based on the phone number of the shipment handler, the name of the contact at the market, the images from the market (located in "destination-and-market" folder) where Chinese inscriptions can be seen and also from panderoshipping's presentation page where it was mentioned that they were specialized in Africa – Asia shipments.

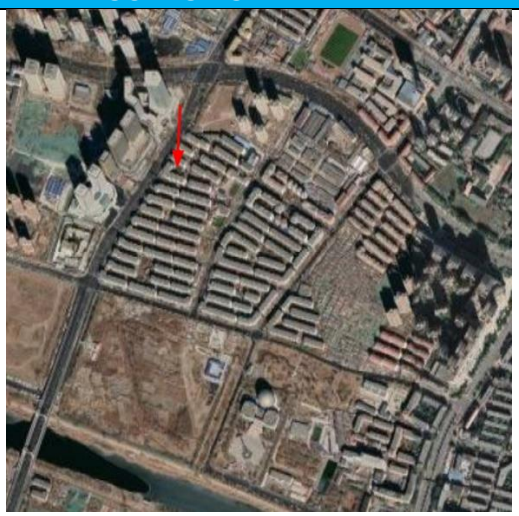
At Pandero we understand your logistical needs like no other. We're a fast and reliable partner who can get any type of cargo anywhere in the world. Although we ship anywhere, we specialize in Africa and Asia, working with local partners who we know we can trust.

I searched for all China's major ports and I started to take them one by one. It didn't take me long until I came across Tianjin(xin) Port.

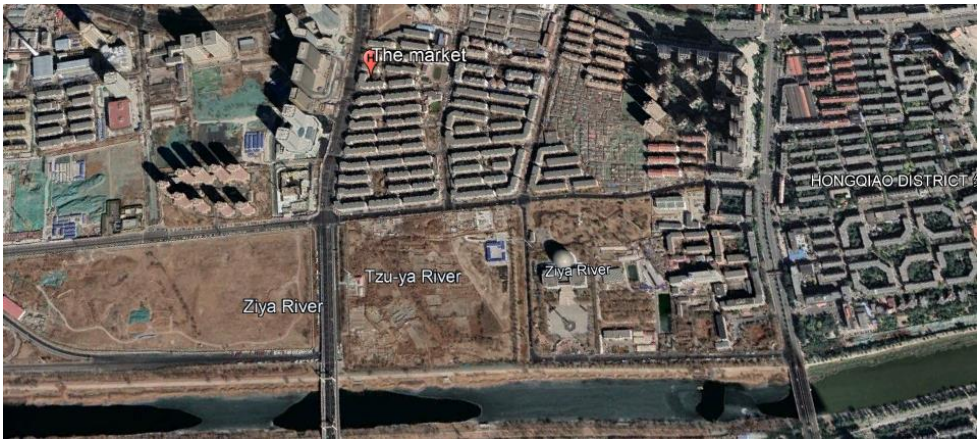
10/14 ☑

Harbor location the shipment arrives in: Tianjin(xin) Port 38°58'55.47"N 117°43'41.09"E (address: China, Tianjin, Bin Hai Xin Qu, 东五路 邮政编码: 300456)

LOCATION OF THE MARKET



I assumed that the market should've be around the harbor of Tianjin (OPEX again 😉) and I saw in the bottom left corner of the image that the location was near a river (a bridge can also be seen). The only river that flows into the Yellow See, passing through the Tianjin(xin) harbor, is Haihe River. So, I started to follow along the river until I found the location (at one moment the main river divided in in Xinkai River, Jinhang Yunhe and Tzu-ya River, but my gut told me to follow along the Tzu-ya River and that was it).



11/14 ☑

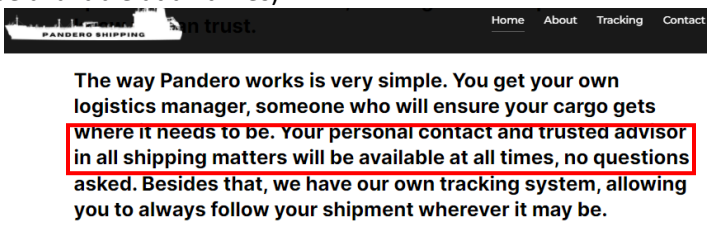
Location of the market: 39°10'29.04"N 117° 8'16.44"E (address: Hongqiao District, Tianjin, China, 300131)

Part 3. Social engineering

I still had to find the shipment ID, the name of the ship, the date and time of arrival. I spent some time scraping online maritime databases, searching for ships linked to Mombasa and Tianjin ports, but I didn't find anything conclusive. However, there was also that shipment ID that couldn't be found just using maritime OSINT.

I had to find something else.

On the panderoshipping's presentation page there was a mention about a logistics manager (a personal contact and trusted advisor in all shipping matters who would be available at all times).



Who was the logistics manager? Well, the one found above with the help of **waybackmachine** – Oliver Zeis (Leung). I had his phone number (+852 4124 9131) and his e-mail address (oliverzeis@protonmail.com). I used proton mail services to check if the address was valid (it was) and I created an ad-hoc e-mail address (I won't go into details about that). Of course, just creating the e-mail was not enough. I had to compose a message that looked genuine and take some OPSEC actions. I won't go into details about social engineering, but to give some authenticity to the message I took in account (i) what I knew about the target, (ii) what element(s) would give credibility, (iii) context, (iv) language, (v) title, (vi) formality/informality, (vii) OPSEC.

I sent the e-mail and I got back everything I needed. 14/14 ✅
Date and time of arrival: 25.03.2022 at 15:00 local time
Shipment ID: CN555701D10TWITT66
Name of the ship: Pangea

Part 4. EXIF (Exchangeable Image File Format)

The password that I tried to crack was killing me. What was in that folder and why was I able to find all the information without it? Was it just a bait to waste time on? I followed the community discussions and I found this hint: *"what can you find out about an image without looking at it?"*. Well, hidden/meta data… of course.

First, I took a look at the jpeg images using **HxD** to check if there was any steganography involved there (data can be hidden in a jpeg image by using hexadecimal notation between specific markers). There was nothing. (you can find at the end an article about hiding data in jpeg images)

Second, I used **ExifTool by Phil Harvey** to extract the EXIF out of those images. The market.png image had the following comment: *"The password is jf438r3PASSWORD940945345488"*. It would've taken haschat years to find it and I should've done this at the beginning 😣. Anyways, there was a folder with 25 not-so-interesting photos. Although I did it without them, the lesson has been learned.

```
exiftool market.png
ExifTool Version Number         : 12.40
File Name                       : market.png
Directory                       : .
File Size                       : 730 KiB
File Modification Date/Time     : 2022:02:26 17:06:22+02:00
File Access Date/Time           : 2022:03:21 12:54:57+02:00
File Creation Date/Time         : 2022:03:01 21:10:26+02:00
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 662
Image Height                    : 659
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 3780
Pixels Per Unit Y               : 3780
Pixel Units                     : meters
Comment                         : The password is jf438r3PASSWORD940945345488
Image Size                      : 662x659
Megapixels                      : 0.436
```

a.

FINAL ANSWERS		
1)	Scientific name of the animal and subspecies	*Pholidota (subspecies: Phataginus tetradactyla, Phataginus tricuspis, Smutsia gigantea, Smutsia temminckii)*
2)	Location of the hunter camp	*3°43'14.89"S 39° 1'46.34"E near Ebagh Ali Shah Mosque (Mackinon Road)*
3)	Location of the hunting grounds	*3°38'58.22"S 38°59'3.29"E and 3°39'13.49"S 38°58'17.83"E (MacKinnon Rd, Kenya)*
4)	Harbor location the shipment leaves from	*Mombasa Harbor 4° 2'31.57"S 39°37'57.35"E (address: Old Mombasa Port, Sir Mbarak Hinawy Road, Mombasa, Kenya)*
5)	Harbor location the shipment arrives in	*Tianjin(xin) Port 38°58'55.47"N 117°43'41.09"E (address: China, Tianjin, Bin Hai Xin Qu, 东五路 邮政编码: 300456)*
6)	Location of the market	*39°10'29.04"N 117° 8'16.44"E (address: Hongqiao District, Tianjin, China, 300131)*
7)	Date and time of arrival	*25.03.2022 at 15:00 local time*
8)	Shipment ID	*CN555701D10TWITT66*
9)	Name of the ship	*Pangea*
10)	Shipment handler full name	*Oliver Zeis (Leung)*
11)	Shipment handler personal phone number	*+852 4124 9131*
12)	Shipment handler personal e-mail	*oliverzeis@protonmail.com*
13)	Name of contact at the market	*Wendy Liu*
14)	Description of contact at the market (visual)	*Wearing a blue raincoat and a red scarf*

What I could've done better:

- I should've analyzed the EXIF data of those images (but I wouldn't have learned how to use haschat 😁).

Lessons learned:

- Certainly, the best way to learn is by doing.

Kudos to Hacktoria team for their work! 😎 https://hacktoria.com/monthly-ctf/operation-brutus/

@praetorius

Resources/tools:

- Google (Translate, Images, Lens, Earth Pro)
- Wikipedia
- https://hashcat.net/hashcat/ (+ this guide https://miloserdov.org/?p=953)
- https://github.com/philsmd/7z2hashcat
- Windows PowerShell and Perl
- https://archive.org/web/
- https://exiftool.org/
- https://blog.nviso.eu/2020/07/13/how-to-embed-secret-data-in-jpeg-files/

Some great articles that I found during researching EXIF/steganography:

- https://auth0.com/blog/read-edit-exif-metadata-in-photos-with-python/
- https://ctfs.github.io/resources/topics/steganography/invisible-text/README.html
- https://www.hackerfactor.com/blog/index.php?/archives/894-PNG-and-Hidden-Pixels.html
- https://infosecwriteups.com/beginners-ctf-guide-finding-hidden-data-in-images-e3be9e34ae0d

Disclaimer: *any mention of real locations, people, countries, organizations and such, are not affiliated with me or Hacktoria; they are incorporated into the stories to make them more immersive and relatable.*


FINISHER
OPERATION
BRUTUS
March 22, 2022
PRESENTED BY
HACKTORIA
CERTIFICATE
OF COMPLETION
PRESENTED TO - AGENT CALL-SIGN:
praetorius
Hacktoria monthly OSINT CTF Event
Operation Brutus
Frank Diepmaat
Frank Diepmaat
Founder & CTF Creator
Sofia Santos
Sofia Santos
CTF Creator & GEOINT Spcialist