Notes on OSINT investigation

- Blue- investigation details
- Purple- OSINT details
- Premise
  - You are an investigator in a mock investigation working for the National Criminal Investigations Division (CID) in a country called "Fair Islands"
  - You get a request from the Coast Guard to support in regard to a shark fin seizure that took place on 09/20/2024
  - The routine patrol in our territorial waters spotted and boarded a fishing vessel FV Malaga sailing under the fiction country Mossaman.
  - The officers found shark fins that upon inspection was listed in CITES and classified as "near threatened" by the International Union for Conservation of Nature IUCN
  - Along with the illicit goods there was also a camera on board is deemed to contain further evidence of the illicit catch
  - The boats fishing license was requested through Mossaman Commodities, a company that has been significantly reducing its operations in our waters in the past years but has recently filed for an additional fishing license for another ship.
  - Fair Islands conservationists have long pointed at the ships operating company for repeatedly falsifying fishing licenses using trans shipment vessels and making efforts to bribe officials involved in the fish landing to turn a blind eye.
  - Two months ago authorities seizes a container ready to leave the fair islands full of shark fins.
  - Hypothesis: Mossaman Commodities (MC) is involved in illegal fishing activities in the territorial waters of the Fair Islands and traffics illegal, highly profitable animal products using containers most likely shipped to Auslandia. MC might bribe public officials to hide their activities. One vessel utilized has been identified as the FV Malaga. This activity seems to have started at least on year ago and appears to be ongoing. Indications are that MC is seeking to intensify its criminal activities.
- Collection
  - Central business registry
    - You look up Mossaman Commodities
    - Address: 312 Ragati Road 34670 Bigare
    - You see that 01/2016 total starting capital 40,000 100% shares owned by Musa Umar

    - 12/2023 company files for insolvency and creditor protection
    - 03/2024 the company Alpha Imports registered in the Isle of Don acquires 80% of company shares for a total of 126,450
- Google search of Mossaman Commodities
    - Founded in 2016
- Search for FV malaga, the ship that had the illicit good on it
    - Turned up no relevant information
- Now searching the deep web
    - We go onto GISIS (Global Integrated Shipping Information System) then ship and company particulars
        - We search up the FV Malaga
        - We get the MMSI (maritime mobile service identity) which is a nine digit number that uniquely identifies ships and other maritime related stations
        - We also confirm that the boat is owned by Mossaman Commodities
        - We see the in service summary and we can see that another boat is owned by Mossaman Commodities
    - Now on Marine Traffic
        - We look up the FV Malaga, the latest position of the ship was Tuca fair islands
        - The summary for these finds is that the boat sails under Mossaman
        - The MMSI 4232561205
        - Built 2007-01
        - Gross tonnage is 54
        - Last voyage is Arendisa de mar to tuna pearl Gulf
        - Second unknown boat registered to Mossaman commodities
- We are looking at DNS
    - We go to Viewdns.info
        - The first took we use is the domain/ IP Whois, here you enter the domain name youre searching for in this case it is mossaman-commodities.mos
        - Here we find that the domain was registered in 2016 but then the registration information was updated in 2024 (04/07)
        - It seems that the website is registered by a company in Auslandia, this company is a professional hoster and is different from the owner of the domain
        - The website was registered on behalf of the Auslandian company Turnbull Enterprises
    - Next we are still on the same page and go back to use the reverse IP lookup tool. This will show other websites hosted on the same

server. We enter the same domain name as before.
    - We see that another domain is hosted on the same server, its domain is allegro-supplies.aus
    - This might indicate that its connected to Mossaman Commodities
    - We look at allegros website and we get the CEO name which is Suzana Torres, we also get an address (allegro Supplies Lot. Main Street 87 89898 Balil, Auslandia
    - Looking at both domains we can see that both are registered by the same company Turnbull Enterprises
- Now we look at the IP history tool to check if the domain name was used on different servers before, we look up mossaman-commodities.mos
    - The domain was hosted in Mossaman and was transferred to Auslandia in April 2024
- We gathered the information on Turnbull Enterprises from the Business Center Auslandia
    - The director is Natsumi Petunia Turnbull
- We will now search for more information on Turnbull Enterprises
    - Upon first google search the first thing that comes up is that Turnbull was involved in illegal fishing activities between 2010 and 2012.
    - We look at the official website, its offline
    - We use a google search operator “site”
    - We get other results that reveal Suzana terries as the president of the board
- We go back to Viewdns.info
    - We look up the domain turnbull.aus to look up turnbull enterprises
    - We see that the registrant name is withheld for Privacy purposes
- We now use WHOXY
    - We can see who owned turnbull.aus in the past
        - Suzana torres owned it in March 2010
        - We get her professional email suzanatorres@turnbull.aus and her personal email suzanna79@gmail.com
- Archived and cached pages
    - We are now going to try to find more information about Alpha imports. They are the majority owner of Mossaman Commodities and registered in the Isle of Don. The company register is not publicly available and a web search for alpha imports did not result in any relevant information

- We notice that the time between December 2023 and january 2024 is an interesting time because Alpha Imports acquired Mossaman Commodities during that period.
- We go to the wayback machine and enter mossaman-commodities.mos
  - The website was saved several times in 2016, we go to 2024 to check if there is any useful information on Alpha Imports investment in Mossaman Commodities
  - We see there is a version of the website from January 6 2024, we also find a twitter handle (@MossComm)
  - On the about us page we do fine the name of the second vessel that was registered with Mossaman Commodities, FV Rider
- We now go to the twitter webpage
  - The latest post on the page is Nov 7 2023, this is before the acquisition with Alpha Imports
- We go back to the Wayback machine to see if there are any archived pages of Mossaman Commodities twitter page
  - Type in twitter.com/MossComm
  - There is an archived post here from 8 January 2024 that states that Gabriel Tran and Linda Shibuya are owners of Alpha Imports
- Now we look at cached pages
  - We look at a cached page of mossaman commodities website and nothing relevant

- Social Media
  - We did an initial open web search on Gabriel Tran and Linda Shibuya but could not find any relevant results
  - We now will go look at LinkedIn
    - We first change the privacy settings on our covert LinkedIn account, using private mode my identity won't be disclosed to other LinkedIn members if I visit their profile, and I won't be able to see the identity of the people that visit my profile however not a problem as this is a covert account
    - We look up Gabriel Tran on LinkedIn and refine our search to "Gabriel Tran" as to only get results that have Gabriel tran as a name and doesn't have Gabriel in a location like San Gabriel etc.
    - We further limit our search to only include those from Auslandia, then we see there is a Gabriel Tran that is a sales representative at Allegro Supplies which was the other website we saw hosted on the same server as Mossaman

Commodities.
    - We see that Linda Shibuya is also an employee of Allegro Supplies in Auslandia and her profile has much more information
        - She has a picture and it says that she's an administrative assistant at allegro supplies
        - She has contact info on her profile
        - There is a link to allegro supplies page which can give us more colleagues and connections
        - There is a link to the University Balili Auslandia, which can link us to former or current friends and connections
        - In the featured section there is a link to a personal twitter page
- Now we look at instagram
    - We look up #fvmalaga because looking up the peoples name does not yield anything interesting
    - There is one post of a picture of the FV Malaga
    - The post was uploaded 47 weeks ago meaning the end of October 2023
    - The hashtags on the post confirm the locations the boat has been
    - Isabel Umar seems to have commented on this post saying "been on that boat!"
        - We look at Isabel Umar's profile
        - We see there is a post of what looks like Musa Umar the owner of Mossaman Commodities and it seems Musa is the father of Isabel
- We go back to twitter to see if Isabel Umar uses the same username on other social media accounts
    - We find Isabels account
    - Her account is pretty active considering how many tweets she has
    - We want to use twitters advanced search to look for tweets that happened during the target time period we type search-advanced into the URL
        - We type in Oct 28- nov 2nd 2023 into the dates
        - On Nov 2nd 2023 Isabel states that she is about to fly back to Mossaman
        - On oct 30 2023, her hashtags are #pearlgulf #HartbronGorge #TheBayofLourlet
- We look up the hashtag locations on the internet
    - We see that they indicate a natural reserve area with strictly

limited fishing activities such as only fishing to feed ones family or the Pearl Gulf economic Zone that favors vessels registered in that specific zone

- Image Information
  - We are going to use googles image search function to find more information about an image on Isabels instagram
    - We find nothing of significance
  - We now are going to use Yandex, a popular search engine in Russia
    - We upload the image and we find the mountain on the photo in another photo. It is "plagan Hill, Colcouche Islands," an area located in a national park of the Fair Islands
  - We now are using protected planet an internet database that allows us to search for protected areas
    - It shows that Colcouche Islands are a marine protected area and further research reveals that fishing is not allowed in this area
  - Useful resource to track fishing vessels is the website Global Fishing Watch. It combines tracking data from different sources to show current and historical positions of commercial fishing boats
    - We type in FV Malaga
    - Click on the entry, type in the data 10/29/2023-10/31/2023
    - According to our previous findings the Colcouche Islands is a protected marine area and using this website we confirm that the FV Malaga was in this protected area fishing on October 30
  - Moving through the investigation the Coast Guard sent you a copy of the photos found on the camera that was seized on the FV Malaga
    - We look at the pictures on the SD card and there is a selfie of a young woman with fish in a net in the background
      - We use a metadata viewer on this photo such as Jeffreys Image Metadata Viewer and upload the selfie
      - The most important information apart from the content of the image is the date and location extracted from the data
      - The date October 30 2023 refers to the same day as the posts on the social media we already found
      - There is also latitude and longitude and this confirms that the photo was taken close to Plagan Hill, Colcouche Islands
    - A second picture is of interest which is one of a container
      - The Exif (Exchangeable Image File Format) analysis shows

the photo was taken on nov 5 2023, in Oaksby landing the main harbor of the Fair Islands
    - We will use a site that allows us to track containers this site is SEARATES
        - We input the container number we got from the photo
        - The container is owned and rented out by Hapag-Lloyd
        - At the time of investigation the container is on its way from Oaksby landing fair islands to scarcola piers auslandia
        - We see that the container is loaded on the Vessel HMM Balil
    - We now go to GISIS to get information on HHM Balil
        - The registered owner is the MA Tauria
        - The entry shows the full address of the owner of the vessel, which would allow us to contact them to obtain more information about the use of the container in Oct/ Nov 2023
- Online Communities, dark web, and virtual currencies
    - We go on reddit
        - We searched for names of other assets but none reveal relevant information
        - we search for the website mossaman-commodities.mos
            - A post comes up by the user ramuasum, he is requesting feedback for the mossaman website he launched, this post is 5 years old
            - We click on the users profile
                - We find a link on a post from a year ago that is advertising a ship for "traditional Auslandian food" the address on this post ends in the domain .onion meaning its hosted on the TOR network
                - We paste the link into the TOR browser and find that the link leads to an online shop that offers various maritime delicacies and offers parts of endangered animals.
                - The website says that payments will be made via bitcoin
            - We type the address for the bitcoin payments in blockchain to look at the transaction history on the address
                - The summary at the top shows that the address was used 1225 times for transactions. You also see the total amount received in BTC and $ and the total amount

sent from the address

- Reporting
  -