Notes from OSINT Course

- The intelligence cycle
  - Planning and direction
  - Collection
  - Processing and exploitation
  - Analysis and production
  - Dissemination and integration
  - Feedback
- Add ons
  - Multi- Account Containers: Allows you to open tabs completely isolated from one another and dont share the same cookies, session data, or other information.
  - uBlock Origin: enhances the security of your browser. It mainly blocks ads, malware, and trackers.
  - ScrapBee: allows you to save entire webpages for offline access. Also allows you to add notes and edit the offline copy.
  - FireShot: Takes screenshots of webpages. Allows you to capture the visible area, the part selected or the entire webpage including parts that are not visible.
  - DownThemAll: Allows you to download all media like videos and images from a website and save them to your computer. It also saves the metadata.
- Database and Web Searches
  - Opencorporates: open database of companies worldwide. Search for business name or officers
  - Crunchbase: Information on public and private companies on a global scale.
  - Refinitiv: Organizations and people connected to organizations searchable by names.
  - Dun & Bradstreet: Us companies searchable by business name, Us state required.
- Refining a google search
  - You can put a phrase in quotation marks to make sure that the search engine only returns results with that phrase not just with one word or irrelevant phrases
  - You can also add the operator - in order to exclude entire phrases from your search e.g. -“football club” make sure you dont put a space between the minus and the first word of your phrase - football won’t work -football is correct
  - You can also force google to include phrases by using AND or OR

  they have to be capitalized tho
  - You can use the operator "site:.mos" to limit the search to websites for the imaginary country Mossaman, you can also use the "site" operator to show all the pages that google has indexed for a specific domain
- DNS Records
  - DNS Services like "viewers.info" provide valuable tools to explore domain information
  - DNS stands for Domain name system
  - On Viewdns.info there are other tools that may be of interest other than the ones we used which were: Domain/ IP whois, Reverse IP lookup, and IP history
  - Others of interest are:
    - Reverse whois lookup: you can enter the name of an individual or a company to find other websites owned by them
    - IP location finder: Enter the IP you retrieved from the reverse IP lookup and get the location of the server- country, region, longitude, latitude.
    - Port Scanner: different ports are used for different services, you use this to check if common ports are open on a server, ports 80 and 443 are used for websites, other ports may indicate other services e.g. and FTP server to download data
  - WHOXY: a service that provides historic entries on previous owners of a domain.
- Cached pages: a function offered by the major search engines, you click on the three dots by the website address and click cached, this is a snapshot of the page as it appeared on a certain date, the current page could have changed in the meantime.
  - archive.today allows anyone to archive websites, so this service would retrieve a copy of the website only if someone archived it previously. You would enter the address of the website here to search for it
- Social Media
  - Similar to other content you find during collection you should keep a local copy of an instagram profile, however saving each post can be cumbersome. Therefore using a tool that automates the process can save you time there are several different ones you can use
  - You can use a browser extension when you visit the page (e.g. Instagram downloader for Firefox)
  - Online services allow you the enter the address for the profile and do the job for you (e.g. snapinsta.app) since these programs run on third party servers this may not be the best option
  - Specialized applications run as a program on your computer (e.g.

Instaloader) and provide the most advanced features

- Other social media platforms that could be relevant
    - VK is a popular social network in Russia and other Russian speaking countries
    - QQ is an instant messaging software service and web portal used in China
    - Taringa! Is an Argentine based social networking site geared toward Hispanophone users
- Image information
    - There are two types of information contained in images: visual- meaning buildings, landscapes, street signs, advertisements, other visual information can help you find the location and other information, the second is meta data- this can reveal the camera model e.g could be a smartphone, the date the picture was taken, and the location
    - Most social networks strip all metadata from images uploaded
    - Exif: Exchangeable Image File Format, a standard for embedding metadata into image and sound files primarily used by digital cameras and smartphones
    - Other reverse image search providers:
        - TinEye: its strength is to find duplicates of images however it might also show similar images
        - Baidu also offers an image search which is in general not as powerful as the other options
        - In some occasions of a reverse image search it could be helpful to crop the image to the main content you are searching for
- Online communities, dark web, and virtual currencies
    - The dark web actually refers the TOR network (The Onion Router)- Tor is a network of servers. Using a specific browser, the request is sent via a random route, making use of the network. Tor allows for an encrypted and anonymous connection and helps you access the unindexed part of the internet. It was first developed by the US Navy and is used by journalists, activists, and others for a secure and private communication and to bypass censorship however due to the anonymity illegal activities are conducted through it
        - The use of random intermediary servers disconnects the requesters computer from the requested computer therefore making the connection anonymous
        - You can enjoy the anonymous access however because your traffic is being routed over various servers your browsing experience will most likely be slower than normal
    - The course talks about what a transaction through bitcoin would look

like

    - Blockchain.com or blockchair.com allows you to explore all transactions conducted via bitcoin. You can also search for addresses to see all incoming and outgoing transactions
    - You can search for blockchain payments sent from the receiving bitcoin address to see whether they are sent to an exchange (Virtual Asset Service Provider VASP) if, so the VASP can be subpoenaed to reveal the name of the account owner.
  - Tips on bitcoin
    - Investigating how traditional currency was converted to Bitcoin and then back to traditional currency will help you identify the owner
    - Websites like Bitcoin Who’s who or Bitcoin Abuse offer directories of known bitcoin address that have been used in scams and might even link these to known social media accounts
    - Most bitcoin wallets contain multiple addresses. Some users might make use of advanced tools like so called mixers to disguise the traces left on the blockchain
    - A search for a bitcoin address on google might reveal known addresses like exchanges or addresses used by shops
- Reporting
  - For structuring a report it’s a good idea to start with an initial fact sheet of the most important findings.
    - Our entity investigated in this case would be Mossaman Commodities and the Vessel FV Malaga
    - Summary
      - You took a screenshot of the summary but use it to check yours and make sure there wasn’t anything you missed but write it urself
    - Details of the findings
      - Main body of the report. You tell the story about the case, you might go along the chronological timeline or you might organize it in a way that you found the intelligence
    - Recommendations
      - You could do a section that indicates what information would be of interest but it is not available as OSINT. You could present ideas of how and where to father this information.