# OSINT Assignment

## Part 1 - Reading and Response (30 pts.)

Answer the following questions using the reading: "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence" Hassan and Hijazi (2018).

1. Suppose you are doing an open-source investigation, and you find a database posted online from a hack from last year. What is this information called? (5 pts.)
    a. OSINT
2. Why would a government use OSINT intelligence? (5 pts.)
    a. Governments need these types of sources for different purposes such as national security, cybertracking of terrorists, counterterrorism, understanding domestic and foreign public views on different subjects, policy making, and the exploitation of foreign media.
3. Why would an independent citizen use OSINT intelligence? (5 pts.)
    a. An individual can use OSINT to fight identity theft as an example. OSINT can also help individuals in hiding their own digital footprint while also protecting themselves from other cyber threats and breaches.
4. What is the difference between passive and semi-passive data collection? (5 pts.)
    a. Passive data collection is considered highly anonymous and should be done secretly. Passive data collection does not involve sending traffic over a network or server.
    b. Semipassive data collection is different as it sends limited traffic, meant to resemble standard internet traffic to avoid detection, to target servers to acquire general information about people.
5. Describe two benefits of OSINT. (5 pts.)

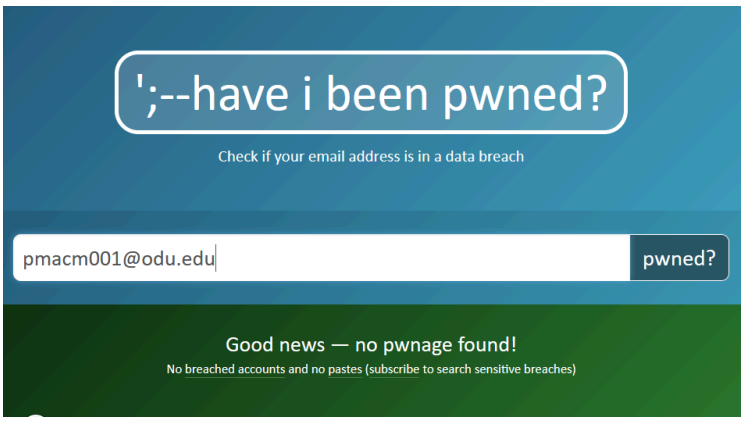
a. OSINT is considered to be less risky when compared to other ways of information gathering. OSINT uses publicly available information to collect any intelligence people or organizations may be after.
b. OSINT also helps in the fight against online counterfeiting. These techniques can be used to find false goods and services and report them to the proper authorities as a means to close the website or send warnings to users.

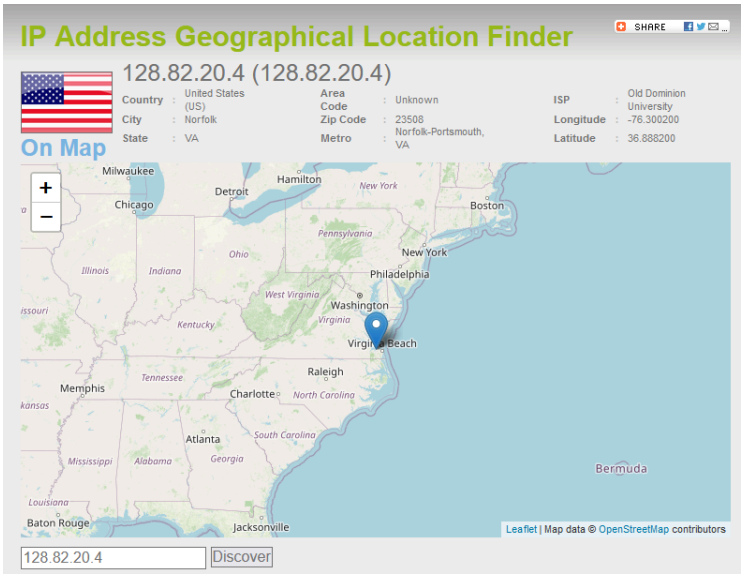
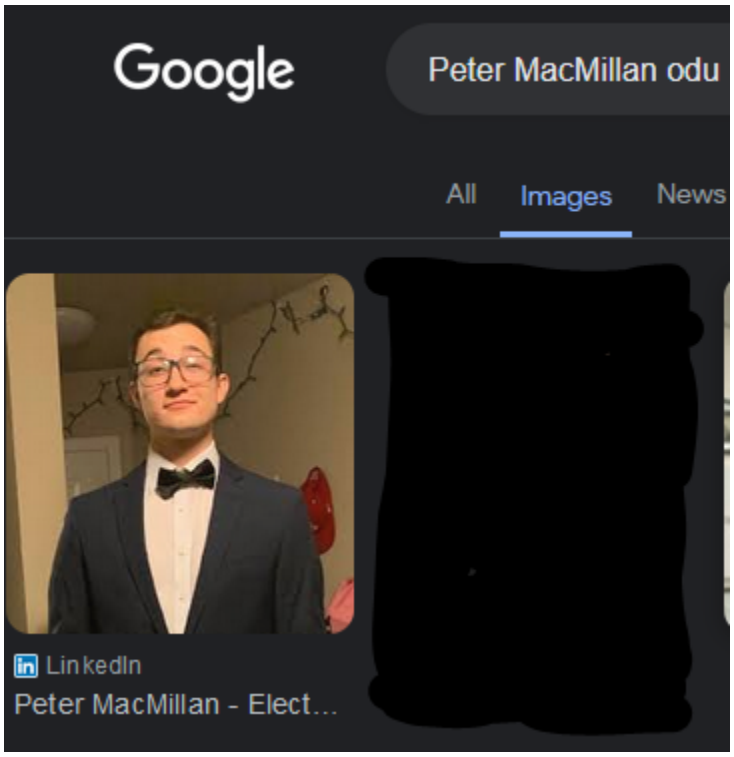
6. What is the difference between OSINF and OSD? (5 pts.)
    a. OSD is raw information and data. OSINF has been filtered to meet specific criteria or needs of individuals or organizations.

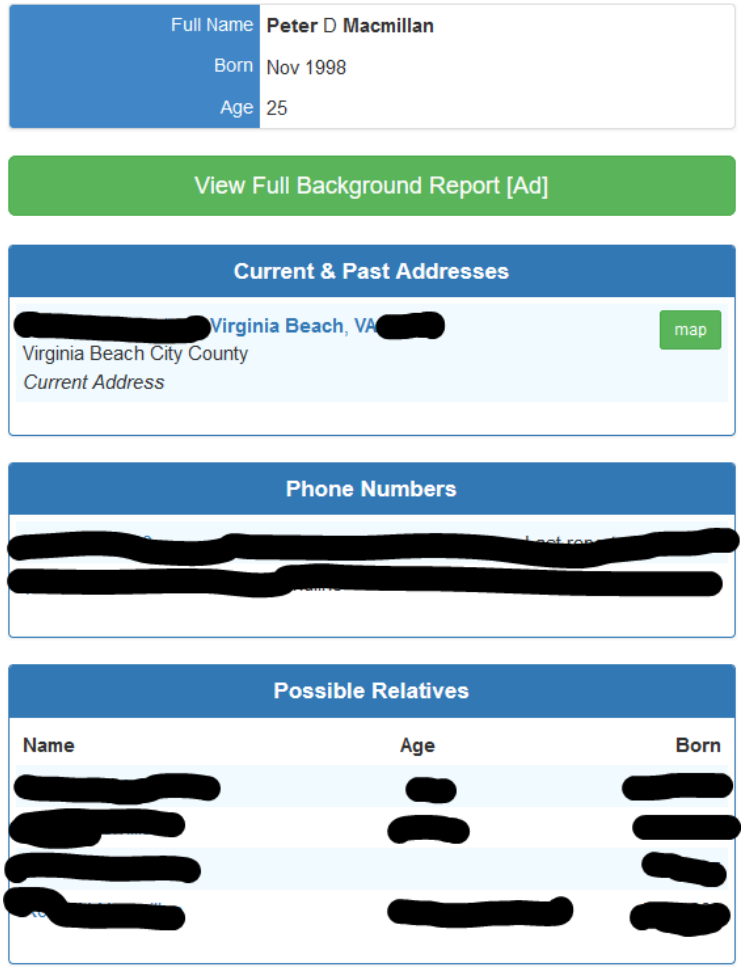
## Part 2 - Using OSINT Tools to Collect Data (50 pts)

Now you will discover what OSINT is available online about you. Watch the video tutorial and use the OSINT framework to complete the chart below. Using the tool but not finding info does not count (I looked but couldn't find anything). Remember, you can only use tools from the same root node twice (they must provide different pieces of information), and you must use at least three root nodes.

Feel free to blur info if you like.

| 10 Pts. Each | Root Node | Tool | Data Collected | Screenshot |
|---|---|---|---|---|
| | Business Records | Open Corporates | The year I started my corporation and where it was registered. |  |
| 1 | Email Address | Have I been pwned? | This tool allows you to see if any of your emails have been part of a data breach or the subject of a data breach. |  |

| | | | | |
|---|---|---|---|---|
| 2 | IP & MAC Address | IP Fingerprints | This tool uses an IP address in order to geolocate a user. |  |
| 3 | Public Records | Voter Records | This tool allowed me to see my own voting status and when I registered to vote. | **Voter Name** PETER DANIEL MACMILLAN<br>**Voter Number** 208657680<br>**Status** Active<br>**Date of Status** 2/6/2017 |
| 4 | Images/Videos /Docs | Google Images | Did search on myself and was able to find my LinkedIn page |  |

| | | | | |
|---|---|---|---|---|
| 5 | People Search Engines | Family Tree Now | Searching for your name populates results for possibly family tree creation. It pulls from public records and census data. |  |

## Part 3 - Critical Thinking (20 pts.)

Suppose a company was highly skilled at OSINT investigations. They are able to find all available OSINT (including NOSINT) on a person or organization.

They do this legally.

They then create “digital profiles” of the person or organization describing addresses, contact information, estimated net worth or profits, family members (or for businesses who work in the company), their tech stack (for businesses), and so on.

They offer to sell these profiles to anyone at a cost of $100.00 per profile. In two paragraphs, state whether or not the company *should* be allowed to sell these digital profiles, and give your reasons.

Note: That it is legal is not a reason why someone *should* be able to do something.

While the company may be operating within the bounds of legality, the ethical implications of their actions raise significant concerns. Selling detailed digital profiles compiled through extensive OSINT investigations without the consent of the individuals or organizations involved raises serious privacy and security issues. Individuals have a reasonable expectation of privacy regarding their personal information, and organizations likewise have proprietary interests in their internal workings, such as their tech stack or financial data. By commodifying and selling this information, the company is essentially monetizing the exploitation of others' privacy and potentially exposing them to various risks, including identity theft, harassment, and targeted cyber attacks.

Allowing the sale of such digital profiles sets a dangerous precedent that undermines individuals' rights to privacy and data protection. It fosters a culture where personal information is treated as a commodity to be bought and sold without regard for the consent or well-being of the individuals concerned. Moreover, it creates an asymmetry of power, where those with the resources and technical capabilities can exploit and profit from the personal data of others, further exacerbating existing inequalities. Instead, there should be robust legal frameworks in place to regulate the collection, use, and sale of personal information, ensuring that individuals have control over their own data and that it is used responsibly and ethically.