OSINT Challenge Lab

# lesson

**Warm Up:** Show students a short presentation on some OSINT techniques and resources that can be used.

**Lesson:**

1. What is OSINT?
   * OSINT stands for Open Source Intelligence.
   * It involves collecting information from publicly available sources, such as websites, social media platforms, public records, and more.
   * OSINT aims to gather insights, knowledge, and data about individuals, organizations, or specific topics of interest.
2. Importance of OSINT:
   * OSINT plays a vital role in various fields, including cybersecurity, law enforcement, journalism, and competitive intelligence.
   * It helps in understanding potential risks, identifying vulnerabilities, and uncovering valuable information that can aid decision-making.
   * OSINT is used to gather information about individuals for background checks, investigate online threats, assess the security of systems, and much more.
3. Common OSINT Techniques:
   * Web Search: Conducting targeted searches using search engines like Google, Bing, or specialized search engines to find relevant information.
   * Social Media Analysis: Examining social media profiles, posts, and connections to gather insights about individuals or organizations.
   * Public Records: Accessing public databases, government records, court filings, and other publicly available documents to find relevant information.
   * Website Analysis: Investigating websites, analyzing their content, WHOIS data, and any publicly available information.
   * Online Forums and Groups: Participating in or monitoring relevant online communities and forums to gather insights and opinions.
4. Ethical Considerations:
   * It is important to use OSINT techniques ethically and responsibly.
   * Respect privacy laws and terms of service when collecting information.
   * Do not engage in activities that could harm individuals or violate their rights.
   * Ensure the information collected is relevant and used for legitimate purposes.
   * Always verify the accuracy of information obtained through multiple sources.

Some example resources:

Google

WHOIS Lookups

OSINT Framework

DNS Dumpster

Every Social Media Site

County Records/GIS Systems

News Sites

Local Paper Sites

**CHALLENGES:**

**Target: Lsc.edu Domain**

What is the IP address of appointment.lsc.edu?

What is the name of the server on 134.29.189.5?

Who is the administrative contact and what is their email address?

How many name servers are listed on the WHOIS lookup?

**Target: image in Wednesday folder of the LSC Github**

What lake is featured in the picture?

When was the picture taken?

What brand and model of camera was used?

What altitude was this taken at?

CHALLENGING: Using what you know so far about this picture, and knowing that this was taken on “Day 5”…can you find a blog detailing more information about this?

**Target: St. Louis County, MN Parcel ID 010-1370-07230 (hint Google the “Land Explorer” for the county)**

What is the owner name of this property?

What is the square footage of “Building 2”?

What was the total value of the property in 2019?

What was the total value of the property in 2023?

What is the full taxpayer address for this property?

**Target: Unknown Building**

Using the two following pictures, determine the **full address** of the building that is circled:

A metal structure next to a road

Description automatically generated with low confidence

A picture containing outdoor, sky, road, asphalt

Description automatically generated

Hint…look for “gold” (clues) in the photos and try to use Google Maps to get a similar view.