Forensics

Week 9 – OSINT Framework

Date: 14th Oct 2025

Course Code: TU856 / TU857 / TU858 yr 4.

TU Dublin – Grangegorman Campus

School of Computer Science

Seoladh Cláraithe / Registered Address
OT Baile Átha Cliath - Teach na Páirce Ghráinseach Ghormáin
191 An Cuarbhóthar Thuaidh, D07 EWV4, Éire

TU Dublin - Park House Grangegorman
191 North Circular Road, D07 EWV4, Ireland

OT Baile Átha Cliath
Gráinseach Ghormáin
D07 H6K8, Éire

TU Dublin
Grangegorman
D07 H6K8, Ireland

~ +353 1 220500
~ tudublin.ie

Overview

Intro to OSINT

Tools

Process to follow

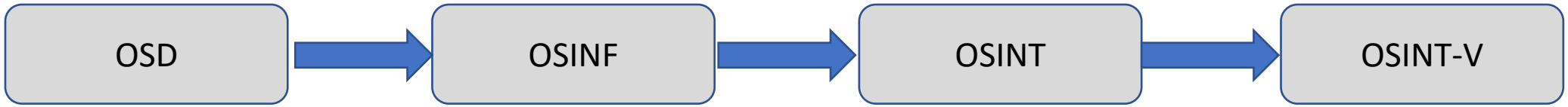
OSINT – Open Source Intelligence

OSD – Open Source Data

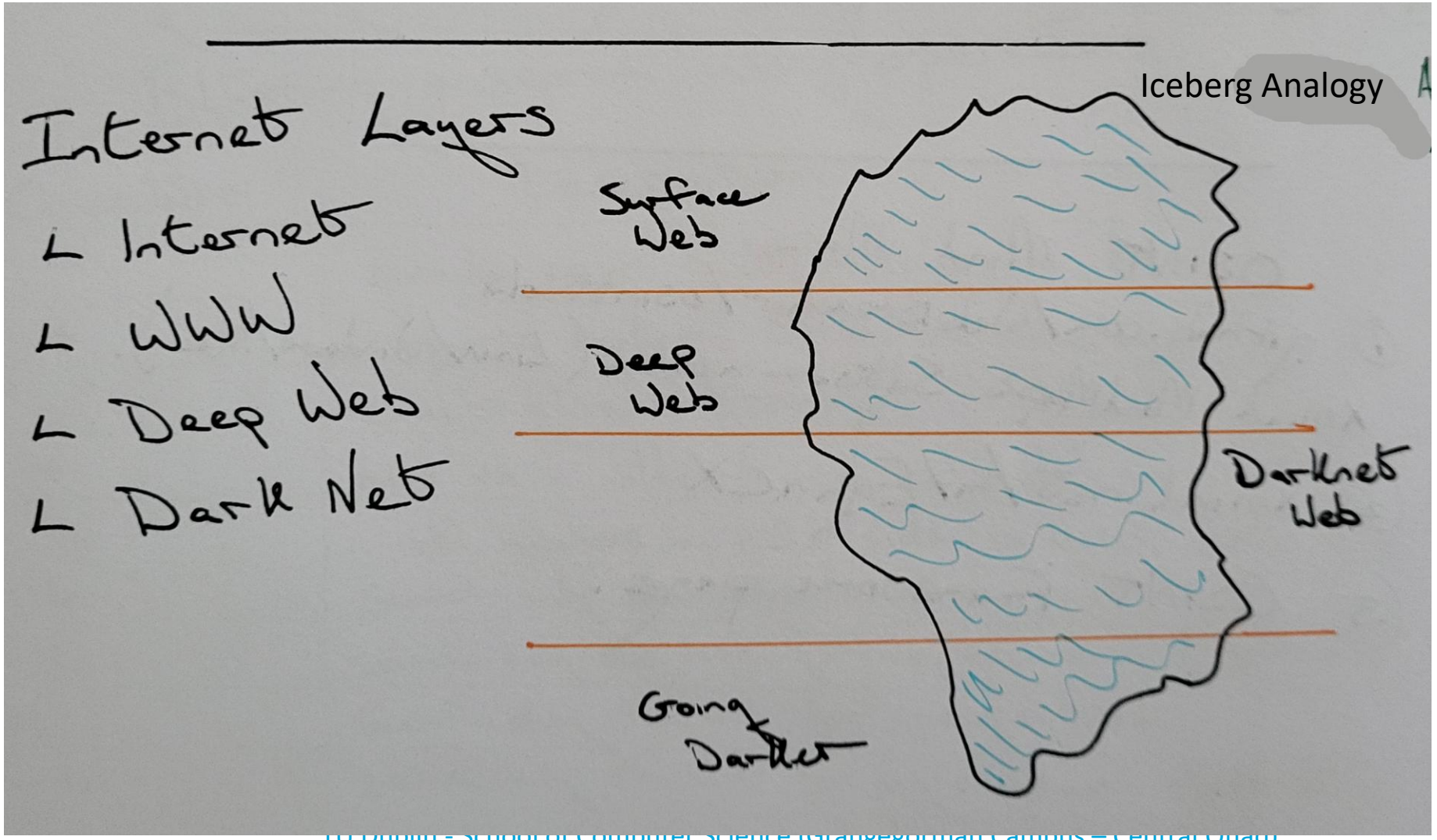
OSINT can be thought of as the process of processing OSD material.

OSINF – Open Source Information. Secondary and processed data is in the public domain and is legally obtainable.

OSINT-V – validated. High degree of certainty + trustworthy source



Internet Layers



OSINT Framework

- The OSINT framework focuses on gathering information from free tools or resources.
  - https://osintframework.com
- The intention is to help people find free OSINT resources.
- Some of the sites included might require registration or offer more data for payment
- It should be possible to get some of the required information for no cost.

Who can benefit from using OSINT?

- OSINT is a Cybersecurity Intel Gathering Tool
- It was created to offer a central location to find tools that can be used to gather intel and reconnaissance as part of cybersecurity research
- There are no shortage of free tools that can be used to gather public data, OSINT is a collection of tools to make intel and data collection tasks easier. (Can we name some tools/sources?)
- Used by security researchers and penetration testers for digital footprints/intelligence gathering/reconnaissance.

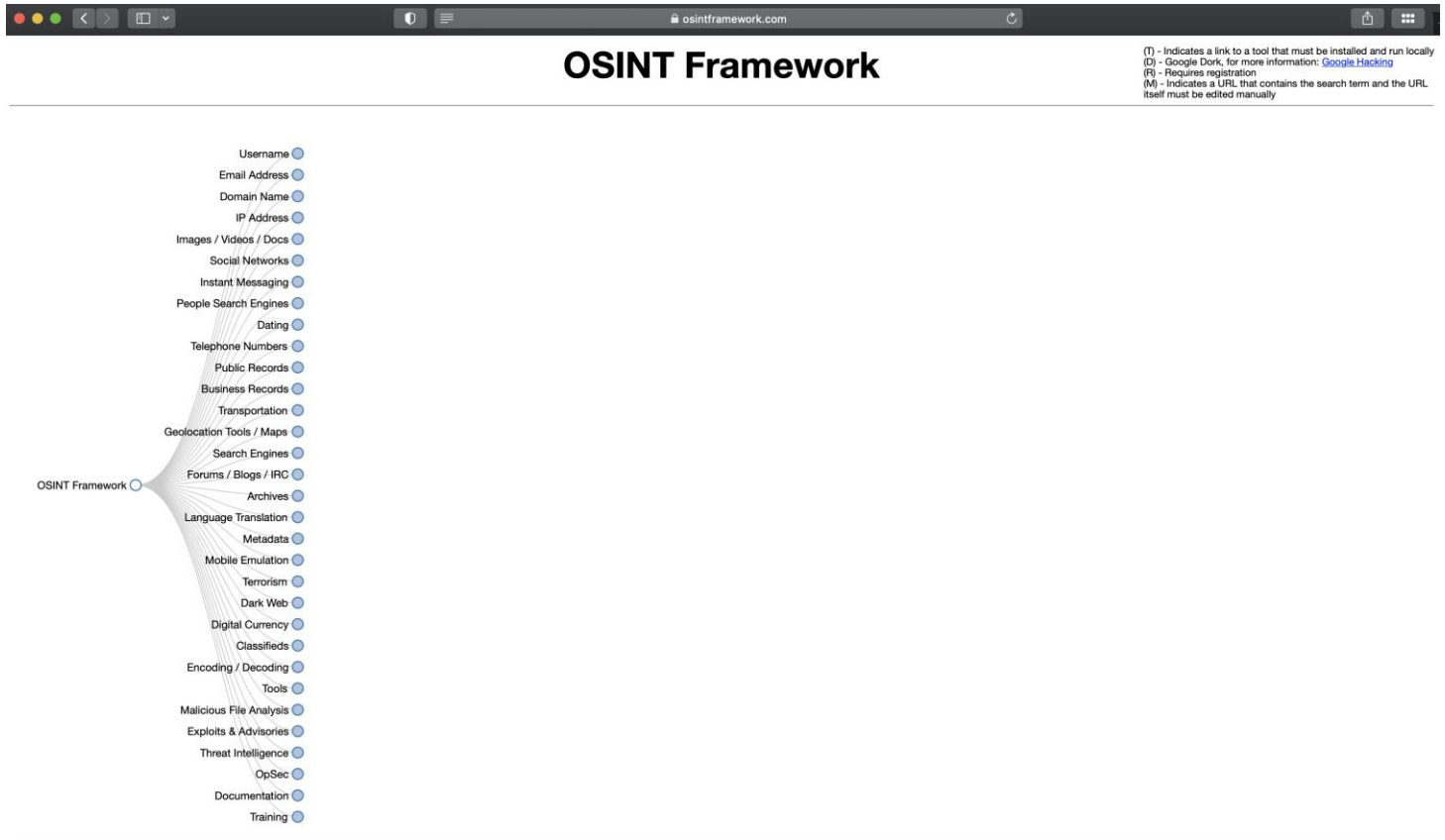
Digital Forensics with OSINT

- “The amount of data generated by the current interconnected world is immeasurable, and a large part of such data is publicly available, which means that it is accessible by any user, at any time, from anywhere in the Internet. In this respect, Open Source Intelligence (OSINT) is a type of intelligence that actually benefits from that open nature by collecting, processing and correlating points of the whole cyberspace to generate knowledge. In fact, recent advances in technology are causing OSINT to currently evolve at a dizzying rate, providing innovative data-driven and AI-powered applications for politics, economy or society, but also offering new lines of action against cyberthreats and cybercrime.” source: https://ieeexplore.ieee.org/abstract/document/8954668

Usage in an Investigation

- What question are you trying to answer?
- After identifying a user profile, is this a potential catfish?
- Is there any data or metadata we can gather from this platform
- Based on usernames, is this user on other platforms?
- There are a lot of ways to get data about any target you're investigating.
- Reverse image lookup for images found etc.
- By using the OSINT website(framework) this can be a good checklist to see what areas you have left to explore while analyzing any individual or company.

OSINT Overview



Source: https://osintframework.com

OSINT Content Categories

OSINT Framework			
Username	Dating	Archives	Encoding / Decoding
Email Address	Telephone Numbers	Language Translation	Tools
Domain Name	Public Records	Metadata	Malicious File Analysis
IP Address	Business Records	Mobile Emulation	Exploits & Advisories
Images / Videos / Docs	Transportation	Terrorism	Threat Intelligence
Social Networks	Geolocation Tools / Maps	Dark Web	OpSec
Instant Messaging	Search Engines	Digital Currency	Documentation
People Search Engines	Forums / Blogs / IRC	Classifieds	Training

OSINT Usage

- Usage Warning

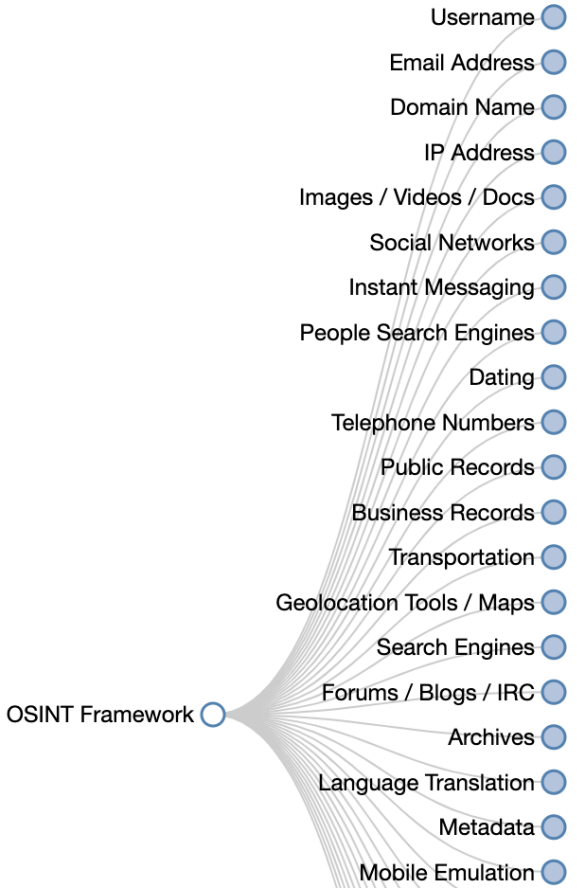
Steps to Perform OSINT

- Use basic attributes to build a profile
- Define your requirements
- Use OSINT tools and techniques to gather as much info as possible
- Analyse the required info
- Pivot, if needed (if investigative solutions break down)
- Validate the assumptions
- Create the complete profile / report.

OSINT Mind Map

- https://github.com/WebBreacher/osinttools
- https://www.xmind.net/

- https://osintframework.com/



The power of search engines

- Google
- Yahoo
- Bing
- Badiu (China)
- Shodan (IoT)
- Ahmia
- Yandex (Russia)
- Etc……..

Google Dorking

- Google Dorking is a hacking technique that makes use of Googles advanced search services to locate data or difficult to find content.
- This is also referred to as Google Hacking.
- This is basically filtering a search using operators.

Google Dorking - Operators

-	Avoid pages that match a term
+	Match exactly
“ “	Specific phrase
*	Wildcard to match any word
#..#	Numbers on either side to match a range
intitle:” ”	In the title
allintitle:” “	Specific phrase
inurl:” “	In the url
allinurl: “ “	Specific phrase
intext:” “	In the text
allintext:” “	Specific phrase
filetype:	By filetype
OR	Logical OR in search. Default in AND

Google Hacking Database (GHDB)

- The GHDB is a collection of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications.
- This was launched in 2000 by Johnny Long to serve pen testers.
- Google allows pen testers to query its search engine to help reveal sensitive data.
- https://www.exploit-db.com/google-hacking-database

- Tutorial:
- https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

Shodan

- Search engine for servers, hardware devices in the Internet
- It is the search engine for the Internet of Everything
- Site: https://www.shodan.io/

Reverse Image Lookup

- Google reverse image search, officially called Google Search by Image, is a service provided by Google that allows a user to search for images using an image as the starting point

- https://images.google.com/
- Yandex Search (Russia)

WiGLE.net

- WiGLE (or Wireless Geographic Logging Engine) is a website for collecting information about the different wireless hotspots around the world. Users can register on the website and upload hotspot data like GPS coordinates, SSID, MAC address and the encryption type used on the hotspots discovered. In addition, cell tower data is uploaded and displayed.

- Site: https://wigle.net/

Tor (darknet)

- Tor is a web browser that has a strong focus on privacy.
- It aims to defend users against tracking and surveillance and strengthens your right to publish and your freedom of speech.
- The easiest way to access the dark web is through the Tor Browser.
- It is free to download and install.

- Note: some people hide their Tor Browser download using a VPN
- Some countries have also banned the Tor browser and network. Using Tor in these countries could also land you in trouble.

Source: https://vpnoverview.com/privacy/anonymous-browsing/is-tor-legal/

Web Snapshots

Archive.org

- Way Back Machine

Search and view content on past versions of websites.

Bellingcat

Bellingcat is a Netherlands-based investigative journalism group that specialises in fact-checking and open-source intelligence (OSINT). Bellingcat publishes the findings of both professional and citizen journalist investigations into war zones, human rights abuses, and the criminal underworld. The site's contributors also publish guides to their techniques, as well as case studies.

Site: https://www.bellingcat.com/

Property Search

Land Registry

Local Authority Planning Records

Social Media Profiles

- Facebook
- Twitter
- Instagram
- YouTube
- LinkedIn
- Snapchat
- TikTok
- Etc…..

Example 1

https://tryhackme.com/room/ohsint

Questions