Cyber Clinic

Session 4: OSINT and Operational Security

WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES
1,717,287,530	22,808,107,946	127,140	4,488,798,178

Wigle.net and Wardriving

What is WiGLE?

- Stands for **Wireless Geographic Logging Engine**
- "Maps and database of 802.11 wireless networks, with statistics, submitted by wardrivers, netstumblers, and net huggers."

How does it work?

- Wigle exists as a mobile app
- As a user moves around with the app on, it tracks nearby Wi-Fi networks and Bluetooth devices and links them to GPS coordinates
- The data is then uploaded to the Wigle database, making Wi-Fi networks and Bluetooth devices like headphones searchable by name to find their exact GPS location.
- The process of gathering this data while in a car is called **Wardriving**.

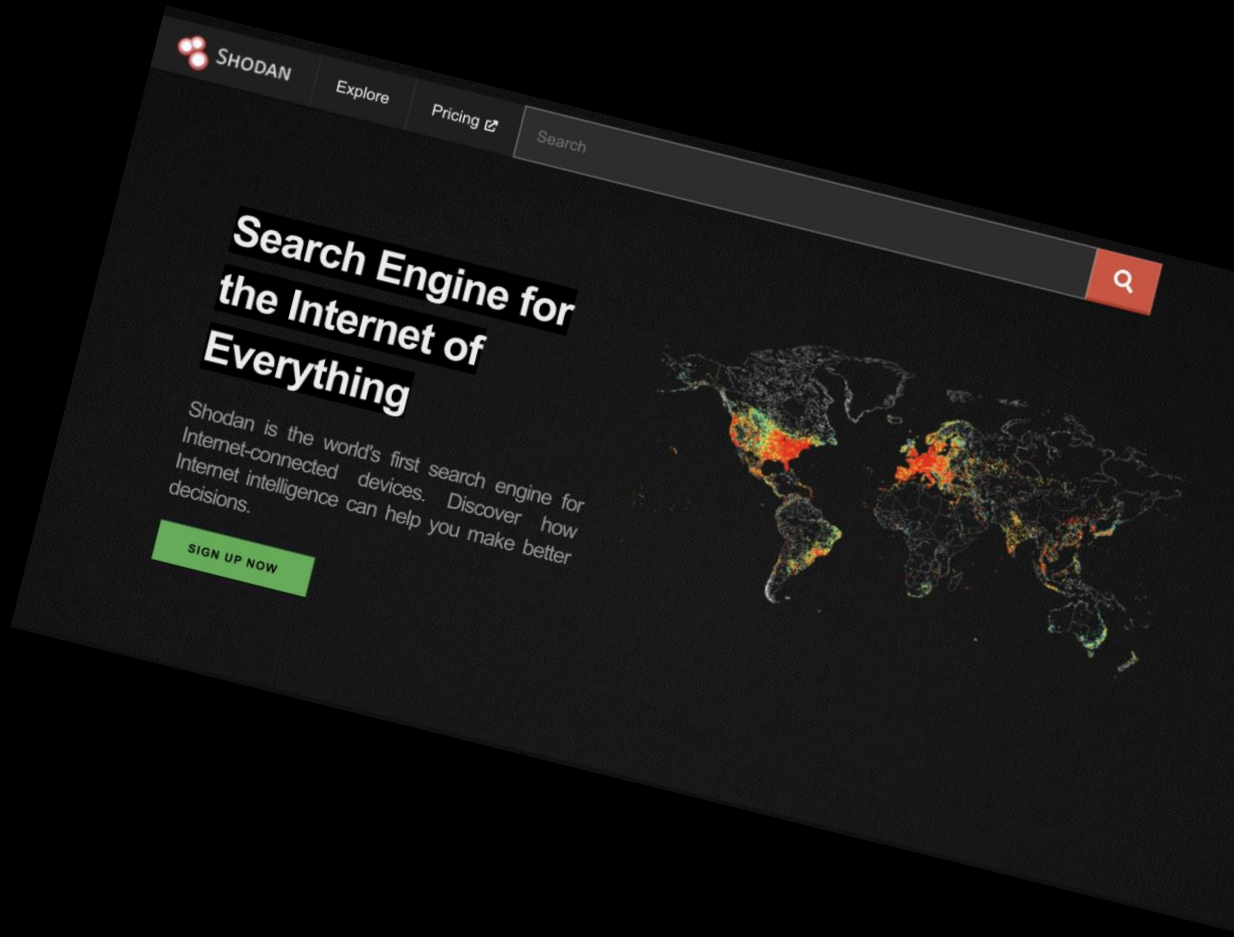
How can it be used?

- If someone reveals the name of their Wi-Fi network or Bluetooth device (even the phone itself, if it has a distinguishable name), for example unknowingly within a screenshot, you will be able to find it on Wigle.

LEWIS

Shodan.io

- Shodan allows you to find anything exposed to the internet
- You can use simple search queries to find cool stuff
- CCTV, Industrial Control systems, Electronic Billboards etc etc etc



Remember It's illegal to access any computer system without The permission of the owner Under the Computer Misuse Act 1990

People Search Sites

- BeenVerified – background checks
- TruePeopleSearch – reverse lookup
- Spokeo – Identity Resolution
- PeekYou – Social media lookup
- WhitePages – Contact and fraud screening
- Maltego – visual link analysis for people, domains and infrastructure
- SpiderFoot – OSINT scanner for emails, users, IP, numbers
- Dehashed/LeakLookup - find leaked credentials from breaches
- DNS Dumpster – DNS mapping and subdomain discovery
- Censys – real time visibility into exposed infrastructure
- Shodan – search engine for internet connected devices
- FOCA – extract metadata from images, documents. Media and hidden data extraction
- Imgops (https://imgops.com/) – Multiple engine reverse image search

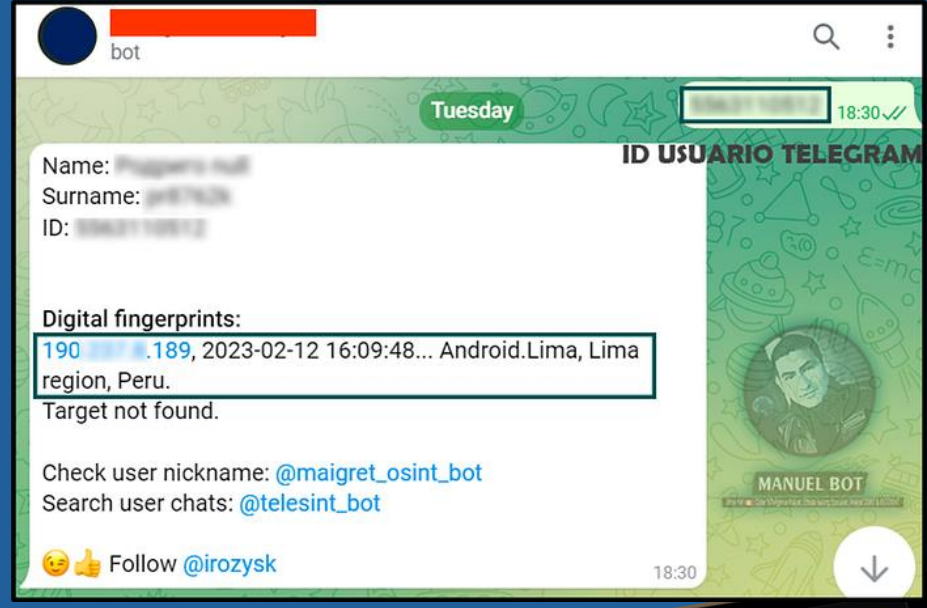
OSINT Industries and Telegram Bots

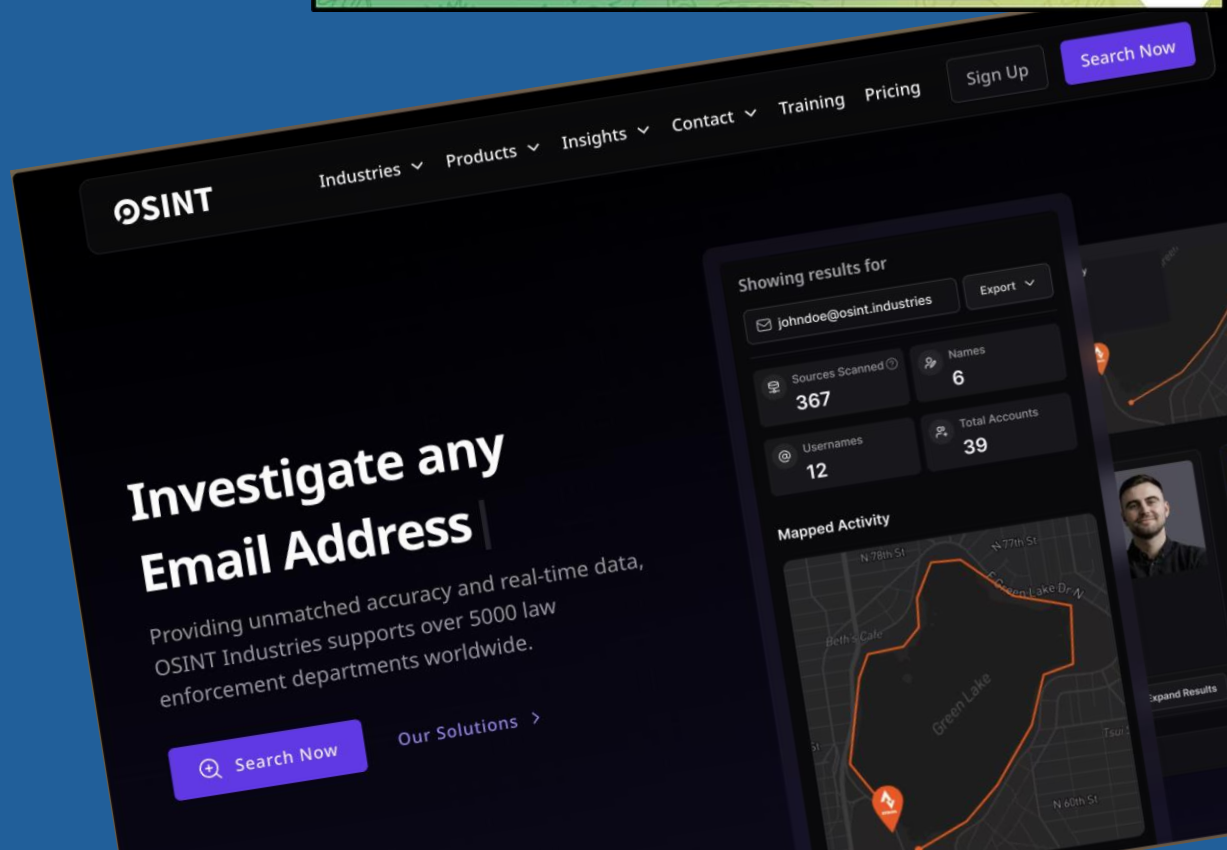
Instead of manually looking through database leaks and different people-search engines, you can let someone else do the work for you.

Telegram bots exist that, when provided with any piece of identifiable information, will check their own database to find related info.

Example Inputs (and outputs):

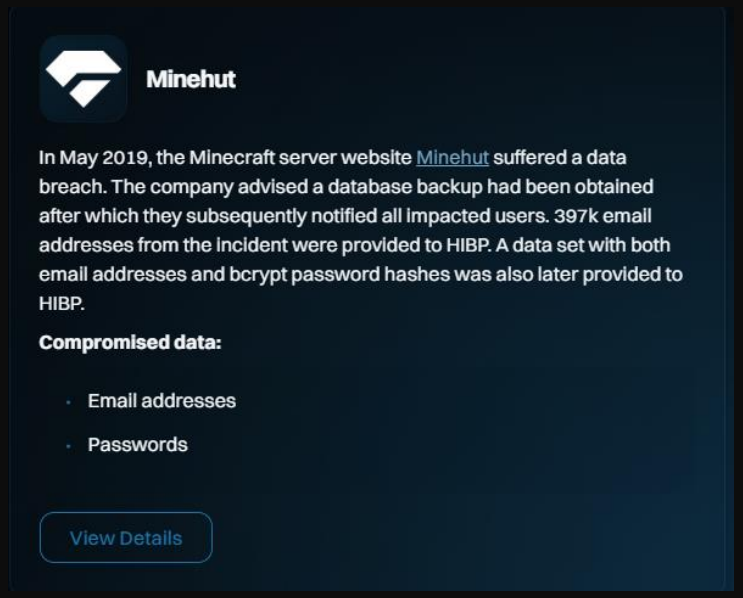
- Vehicle license plate
- Full name
- Username
- Phone number
- IP Address





Database leaks like LeakForums

- Both the darknet and clearnet will have websites where people post 'dumps' (e.g. database leaks). Sometimes for free, sometimes paid.
- This can be used in conjunction with HaveIBeenPwned.com to find the leak an email address is in, then get access to that leak to expose the related password.



EWAN

Documentation

Documentation guide for incident response:

1. Report Title – Use a clear title
2. Report ID – alphanumeric code for identity
3. Date and Time of Incident
4. Report Author - your name, position and contact details
5. Time of Submission – when you filed the report
6. Report Reviewer – normally a senior/team leads details confirming the incident
7. Incident Type – use ISO standard categories
8. Impact Summary – business functions, data types, systems affected
9. Severity Rating – based on internal matrix
10. Action Taken - containment, resets, notifications, forensics
11. Technical breakdown – what did you do, what happened, how did it happen, how was it discovered – SIEM, Affected Assets, Timeline, Data Involved, Attack Vector, provide evidence such as logs/images
12. Review and Formalize – signatures and details from security lead, sponsor and compliance officer
13. Align with standards such as ISO2700, GDPR, NIST, HIPAA, DPA, CFAA

NEW PASSWORD STANDARDS 2025

12 char

Avoid symbols, upper/lower mix, numerical

Use a paraphrase

No periodic resets unless breached

Use MFA/FIDO2

Doxing Tutorial

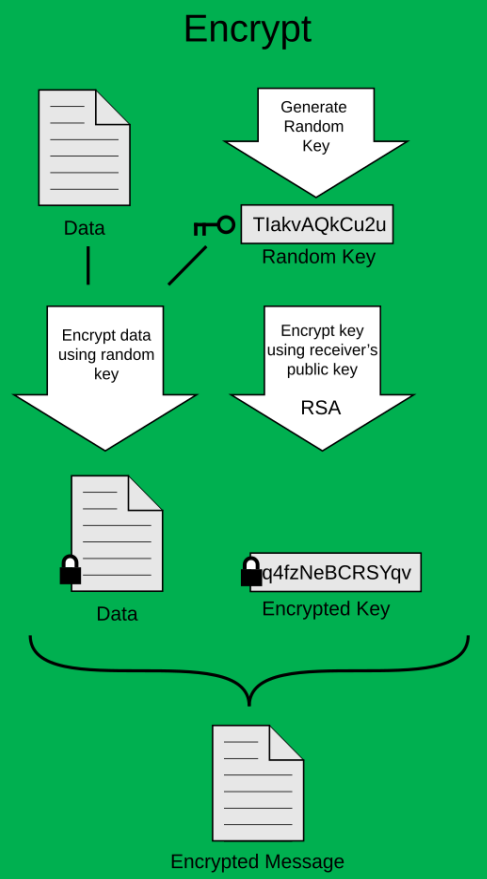
- Get your first piece of information (name, email, username)
- Name: Enter into Google, 192.com/Whitepages, Facebook, **Havelbeenpwned.com**
  - This could give you useful information like city, friends, phone number and **especially other usernames**
  - Location not shown? Try their friend list – their family members might.
  - LinkedIn will show you their city as well as previous employers.
- Email: Enter into your list of websites.
  - See previous slides.
- Leverage the information that just gave you.
  - IP: Insert into Shodan
  - Pictures: Reverse image search (https://imgops.com/)

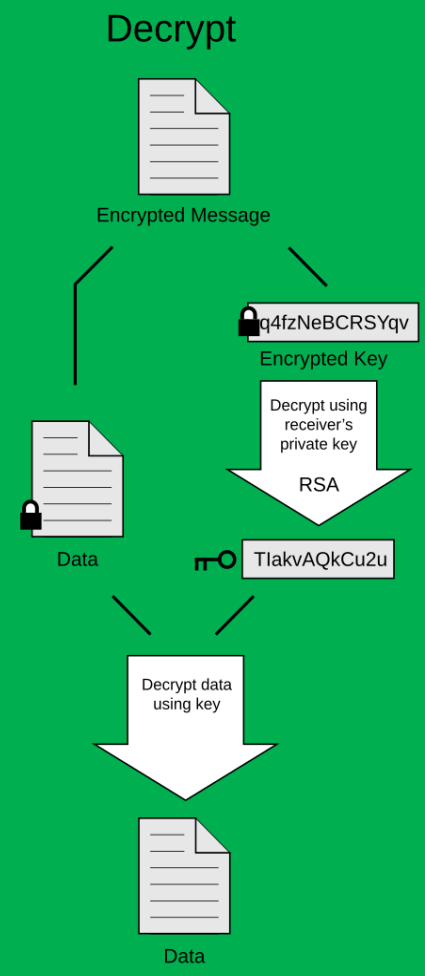
Task 1: Dox yourself

- Use what you have learnt on yourself

PGP – What is it

Pretty Good Privacy: a encryption program that uses CIA for digital communication.
Asymmetric Encryption: a pair of keys, public key for encryption and private key for decryption that ensures only the intended recipient can read the messages.
Symmetric Encryption: A session key which is encrypted by the public key.
Digital Signatures: Signing a message with a private key which is used as authentication to confirm the identity of the sender.
Certificates: A digital document which verify the identity of the user, organization or device they often contain names and email addresses of the owner, a digital certificate which is signed by the CA and a expiry date.
Web of Trust: Instead of a CA it relies on a decentralized system where users validate each others keys





PGP Task

- Ubuntu: Create a PGP encrypted message using GNUPG
- Windows: Create a PGP encrypted message using Kleopatra

Task Setup – Gnupg on Ubuntu

Update System

sudo apt update && sudo apt upgrade –y

- Install

sudo apt install gnupg -y gpg —full-generate-key

-Select key type, size, exp-date, userID, passphrase

- List your keys

gpg —list-keys

-Export keys

gpg—armor —export your-email@expample.com > public key.asc

-This will save your key to a file named public key.asc

-Import a key

gpg —importreceived public key.asc

- Encrypt message

nano message.txt

-To encrypt using recipients public key

gpg —armor —encrypt —recipient(recipientemail).com message.txt

-This creates the file

Message.txt.asc

-to sign a message

gpg —armor —signmessage.txt.asc

-Send the email

Attach both the message.txt.asc and the signature to your email client to send

- Decrypt the email

Save incoming email as incoming.ascgpg —decrypt incoming.asc

-Do not use any real details, any questions you may raise your hand after attempting setup

All commands are in a red font

Task 2: Email another person with PGP keys

- Find a partner
- Exchange public keys
- Encrypt your message using your partner's public key
- Decrypt your partner's message with your private key

Task 3: Phishing (Task)

- Create an email account on e.g. Mail.com (or use your own) and craft a phishing email as one of the following:
  - Employer
  - Royal Mail
- Or craft a text message as one of the following:
  - Parking fine
  - Klarna

Share your phishing attempt on the following Excalidraw board:

https://excalidraw.com/#room=bc15fcacd86ae649e239,S5JHsuN2N2EYR7A9Y0g9sQ

Prevention

- You can obtain a domain for £10/year
  - This can give you unlimited email addresses which you can use for each service you sign up to (e.g. Gmail@mydomain.com)
  - You can make them all forward to your normal email, keeping convenience and increasing security
  - Searching for 'name@gmail.com' won't display any of your public accounts
- Secure passwords (three words, completely different for each site, password managers)
  - Teach how to use Bitwarden
- Keep your social media private. Be aware of what you share as things might not be as fine as you think
  - Example: Plane tickets.
  - Example: LifeLock
    - https://www.wired.com/2010/05/lifelock-identity-theft/

Prevention 2

- “I deleted my Facebook, I’ll be fine”
  - Wrong
  - http://web.archive.org/
- Check if your details show up in any leaks.
  - Haveibeenpwned.com
  - If your details show up, you better have different passwords for each service you use, otherwise you are at high risk of being hacked.

What is TOR?

- The Onion Router is a free open source network which allows for anonymous communication and protects users privacy however it is widely used by journalists, activists and professionals to find information, solve cases or oppress regimes.

- There have been instances of criminals being caught even though they were using Tor.
  - This happened because government bodies hosted their own Tor nodes
- I2P (Invisible Internet Project) is a lesser known alternative to Tor, using peer-to-peer connections like a BitTorrent client where every user helps host the network as they use it.
  - "I2P hides the server from the user and the user from the server. All I2P traffic is internal to the I2P network. Traffic inside I2P does not interact with the Internet directly. It is a layer on top of the Internet. It uses encrypted unidirectional tunnels between you and your peers. No one can see where traffic is coming from, where it is going, or what the contents are"

TOR Guide

Not possible on uni computers :(

- Download TOR for Linux from the TOR website
- Extract file – tar –xvzf tor-browser-linux64 -*.tar.xz
- Change Directory – cd tor-browser-en-US/
- Execute - ./start-tor-browser
- Open, Connect then configure as necessary
- Adjust settings via the shield logo in the URL bar, adjust settings as needed
- See what you can find
- Do not use any personal details and do this on the VM