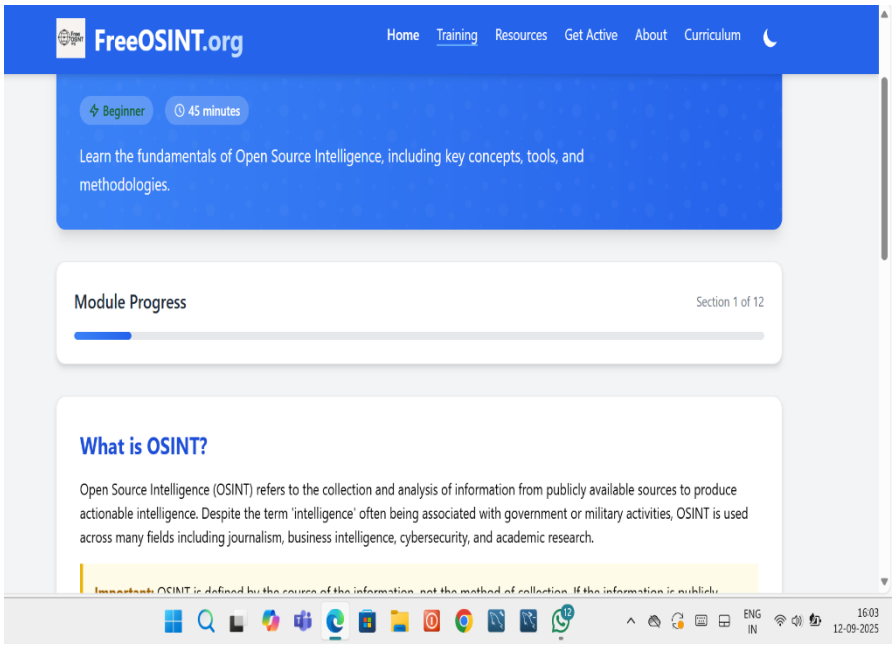
1. Module Completion (Intro to OSINT):

- Access the OSINT training module at:



- **<u>Definition of OSINT</u>**

Open-Source Intelligence (OSINT) is the collection and analysis of publicly available information to produce actionable intelligence.

- It's used in **cybersecurity, journalism, law enforcement, and military operations**.
- The key idea is that the data comes from **legally and openly accessible sources**.

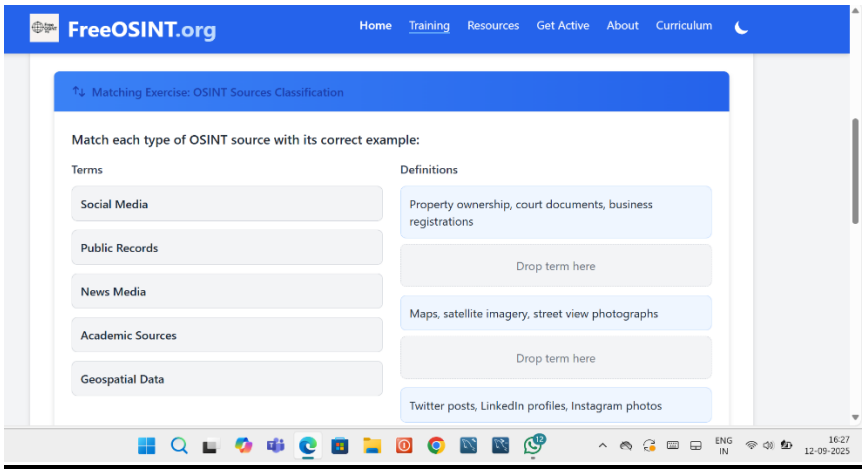
- **<u>Why Timestamps Matter</u>**

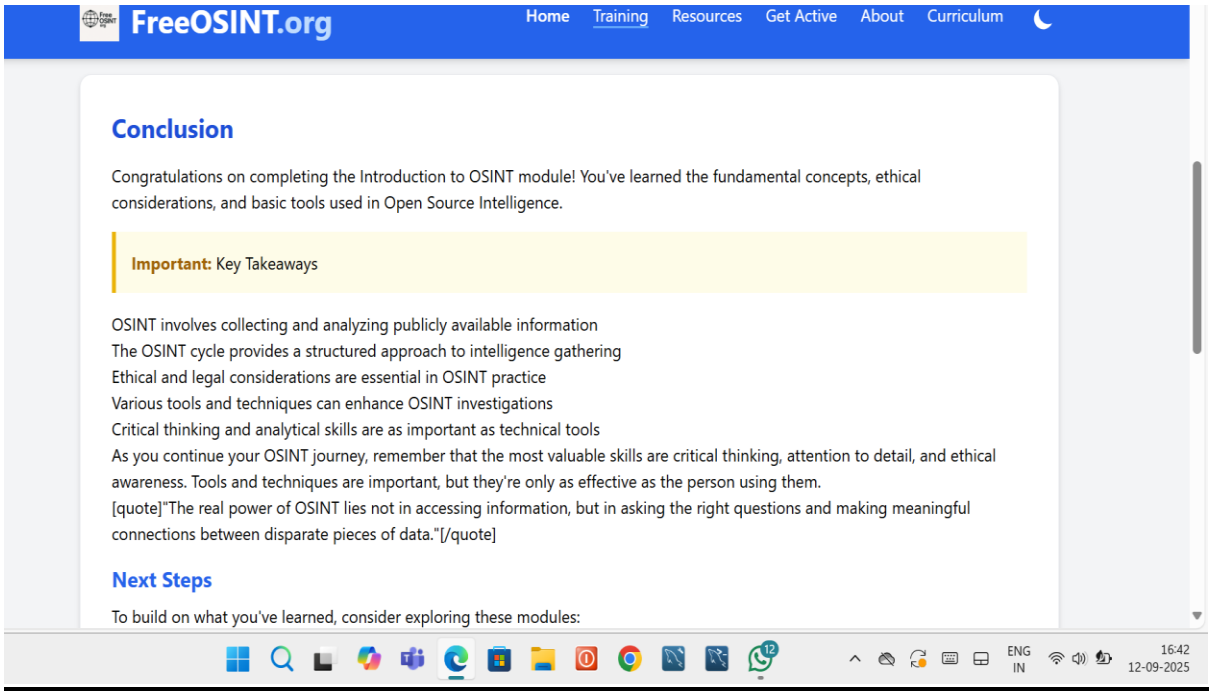
Timestamps are essential in OSINT because they:

- **Verify authenticity** → Check whether a document, photo, or post is consistent with its claimed origin.
- **Establish chronology** → Build accurate timelines of events.
- **Correlate across sources** → Match information from different platforms (e.g., matching a social media post timestamp with satellite imagery metadata).
- **Detect manipulation** → Inconsistencies in timestamps may suggest tampering or disinformation.

- **Examples of Open Sources for OSINT**

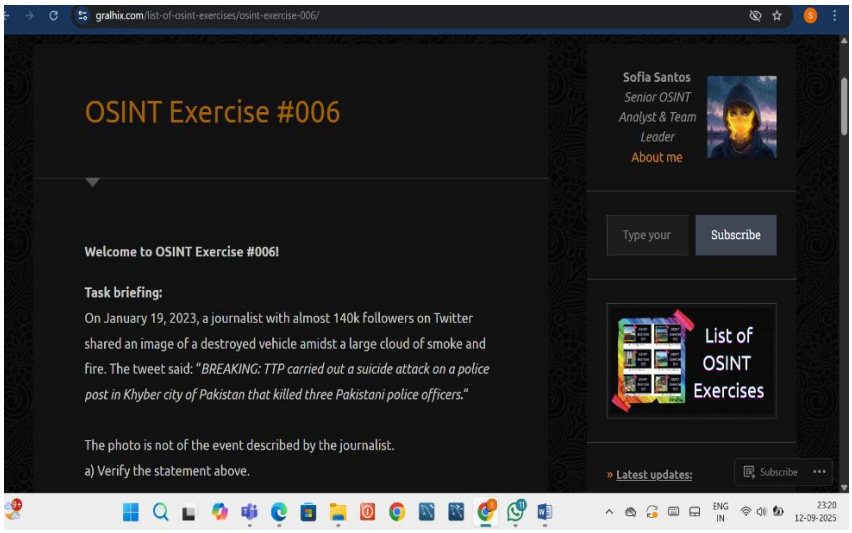
1. **Media** – TV, radio, newspapers, online news sites.
2. **Internet** – Social media (Twitter/X, Facebook, TikTok), blogs, forums, websites.
3. **Public Government Data** – Census info, press releases, hearings, regulations.
4. **Academic Publications** – Journals, research papers, theses.
5. **Commercial Data** – Market research, trade publications.
6. **Grey Literature** – White papers, technical reports, think tank publications.





2. Practical Lab (Sofia Santos)

Choose any one lab from the OSINT exercises collection:



Lab Name: OSINT Exercise #006

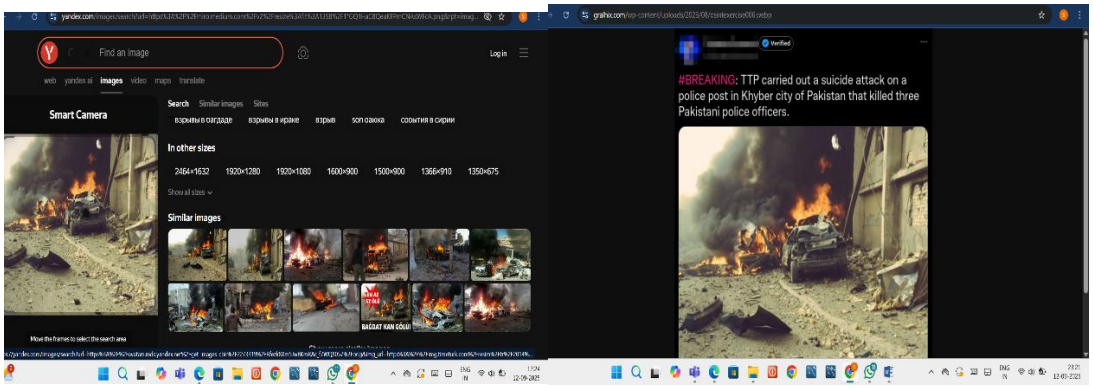
Objective: To verify the authenticity of a journalist's claim regarding a suicide attack in Khyber, Pakistan by analysing whether the shared image accurately represents the reported event.

Here is a solid plan to verify the journalist's claim in OSINT Exercise #006:

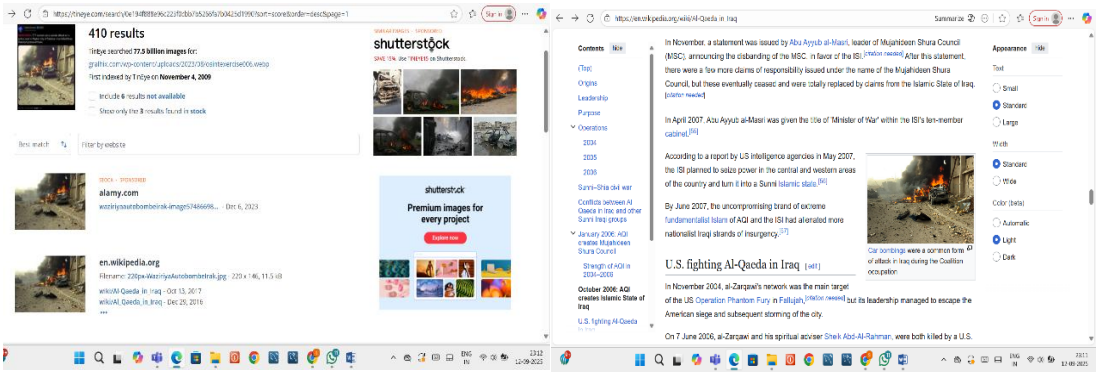
Multiple investigative attempts were made to verify the authenticity of the image shared by the journalist. These included:

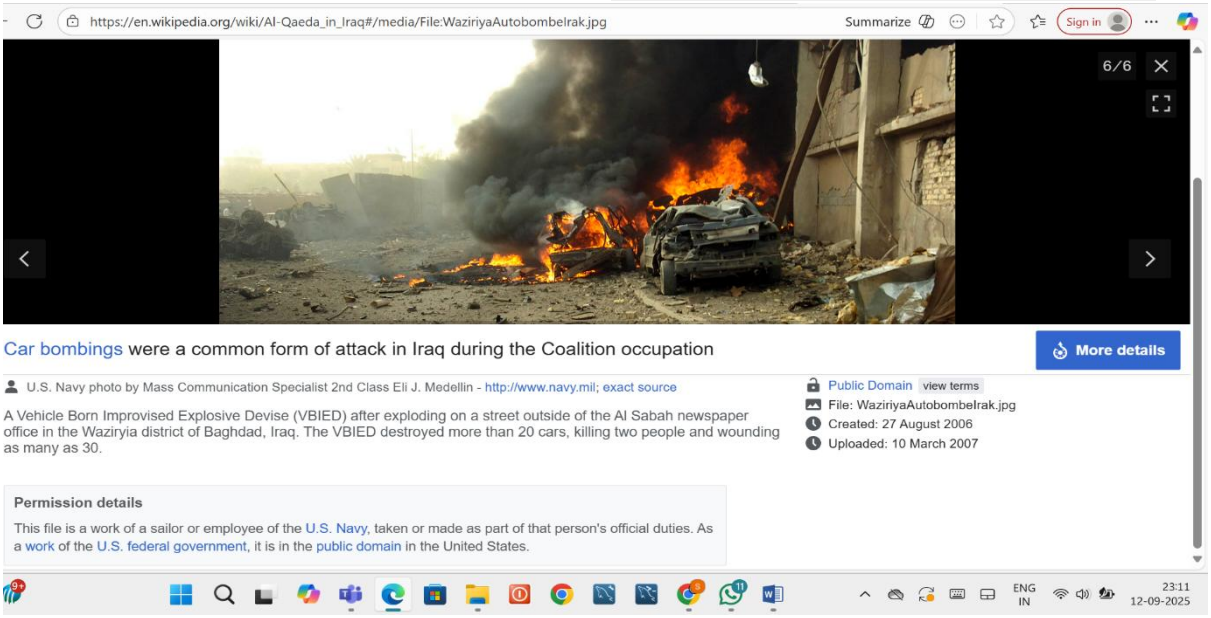
- Exploring various online sources and media outlets for coverage of the alleged incident.
- Reviewing social media discussions and fact-checking platforms for commentary or contradictions.

  Searching for visual matches and contextual clues across publicly available databases.



Through these efforts, the image was ultimately traced to a Wikipedia article that provided clear and accurate context. It was confirmed that the image depicted a different event, unrelated to the reported suicide attack in Khyber, Pakistan.

- After conducting a reverse image search using TinEye, I reviewed multiple sources and ultimately traced the image to a Wikipedia article, where I studied the case in detail and confirmed the original context and accurate information about the incident.
- 

- 

Findings:

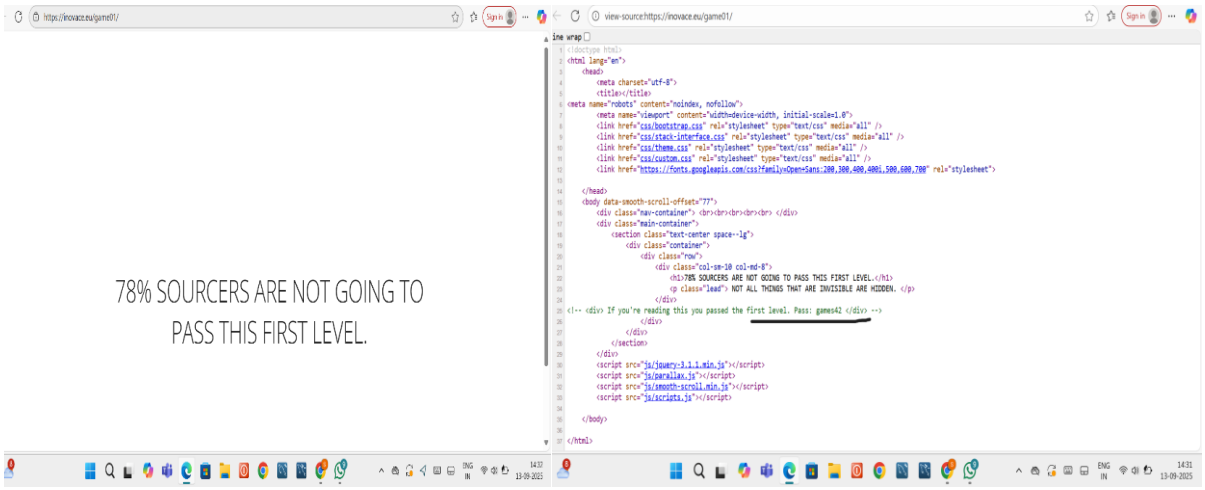
- Through these efforts, the image was conclusively traced to a **car bomb attack in Baghdad, Iraq**, which occurred on **August 27, 2006**, outside the **Al Sabah newspaper office in the Waziryia district**. The explosion, caused by a **Vehicle-Borne Improvised Explosive Device (VBIED)**, destroyed over 20 cars, killed **two people**, and injured **up to 30 others**.
- The image was taken by **U.S. Navy Mass Communication Specialist 2nd Class Eli J. Medellin** and is part of the public domain as an official work of the U.S. federal government. It was later uploaded to Wikimedia Commons on **March 10, 2007**.
- This confirms that the image is **not** related to the alleged TTP suicide attack in Khyber, Pakistan, and was misattributed in the journalist's tweet.

- **Conclusion:**

  The image shared by the journalist does **not** depict the suicide attack in Khyber city on January 19, 2023. It was misattributed and reused from a previous, unrelated incident. This confirms the task statement: ***"The photo is not of the event described by the journalist."***

3.OSINT Sourcing Game 1 – First Finding Report

- **Level 1 Discovery Summary** :
- To uncover hidden clues embedded in the webpage of Game 1 hosted at as part of an OSINT sourcing challenge.



Finding Summary:

Upon accessing the game page, the visible message stated: **"78% SOURCERS ARE NOT GOING TO PASS THIS FIRST LEVEL."** This suggested a high failure rate and hinted at a hidden clue.

By inspecting the **HTML source code** of the page, a hidden message was discovered inside a `<div>` element:

"If you are reading this you passed the first level. Pass: game01"

Additional embedded text included cryptic lines such as:

"CLASS CLUEBIRDS ARE NOT GOING TO PASS THIS FIRST LEVEL." "CLASS CLUEBIRDS ARE NOT ALL THINKING THAT SOME ANSWERS ARE HIDDEN."

These clues confirmed that viewing the source code was essential to progressing past Level 1. The passcode **"game01"** was revealed only through this inspection.

Notes :

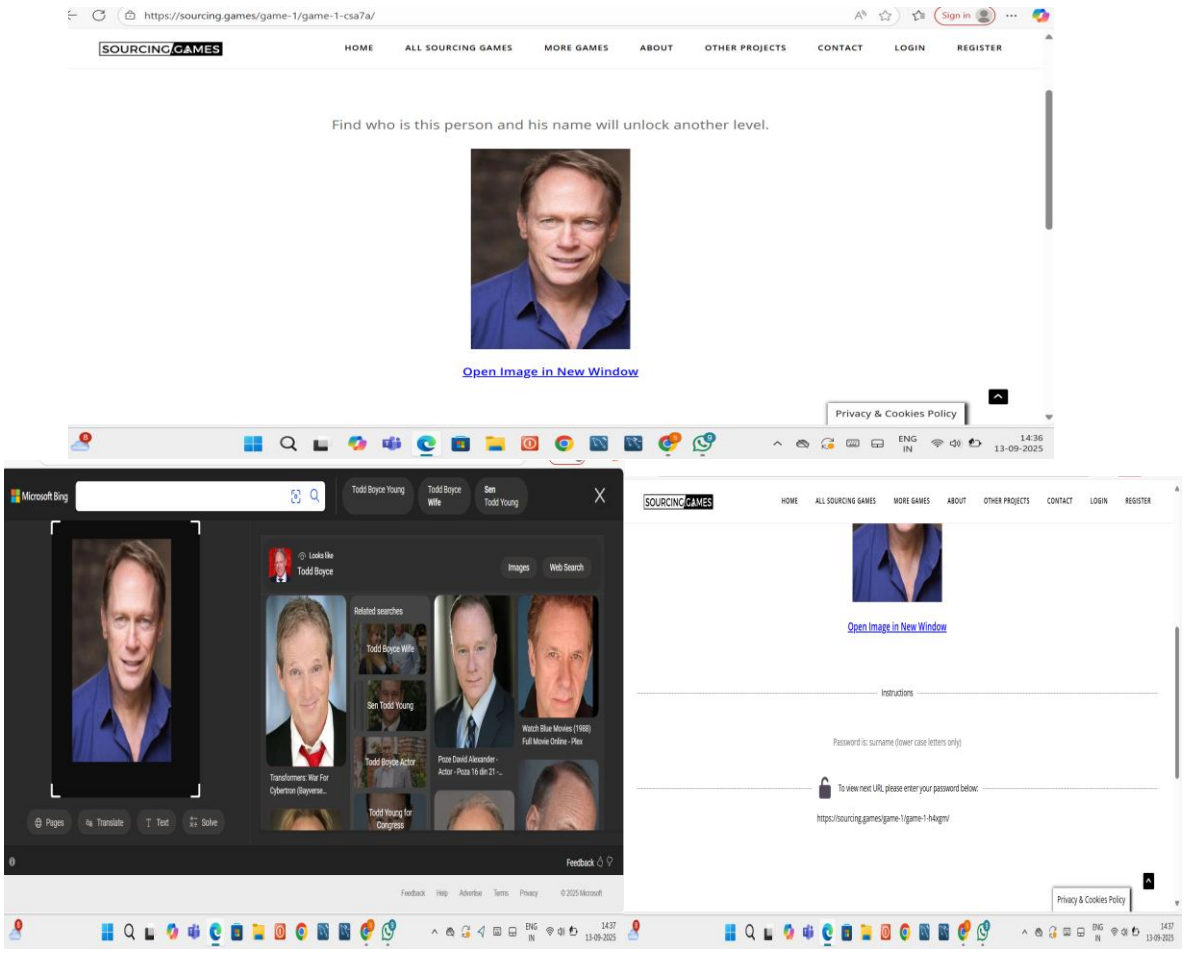
- The challenge emphasizes the importance of **source code analysis** in OSINT work.
- Hidden clues were not visible on the surface page, reinforcing the need for technical curiosity and thoroughness.

- **Level 2 Discovery Summary**

To solve the **second level** of Game , I used **Google Lens** to perform a reverse image search of the photograph provided.

This led me to identify the individual as **Todd Boyce**.

Once I confirmed his full name, I followed the game's instructions to use his **surname ("boyce") in lowercase** as the password to unlock the next level.

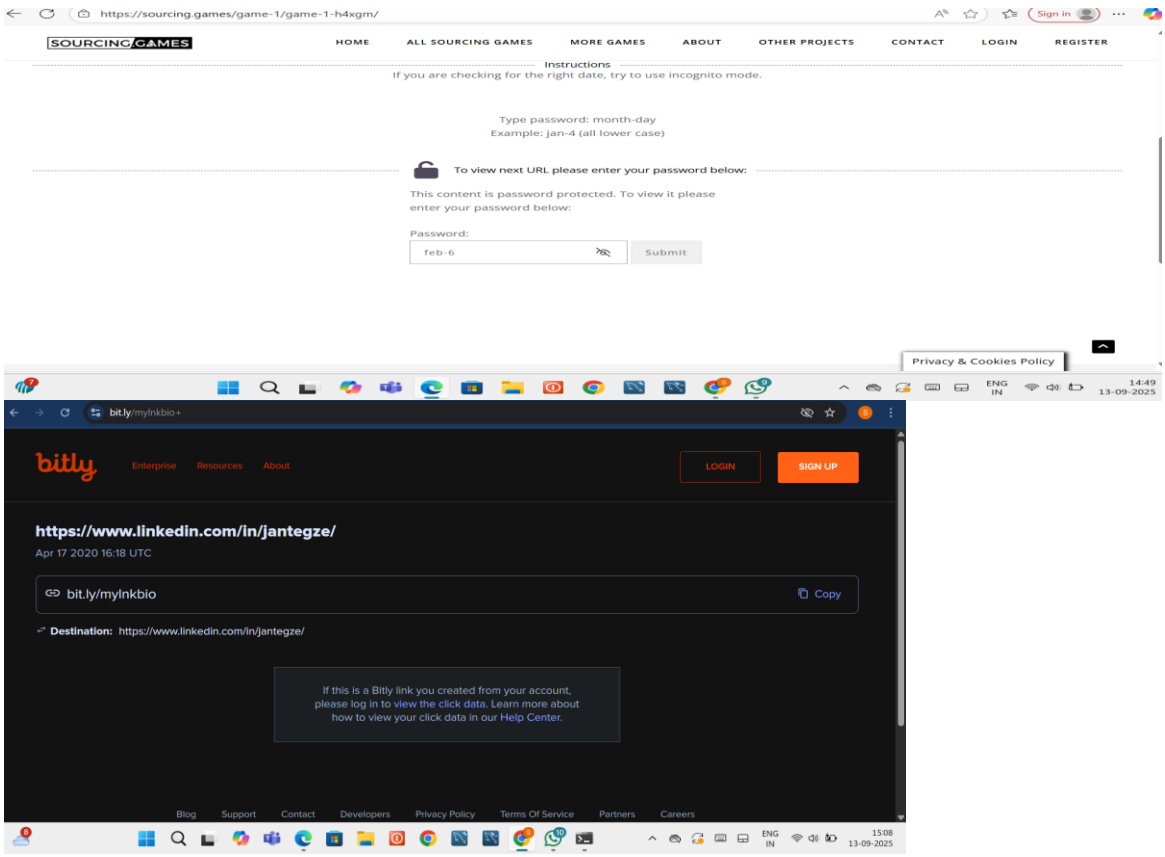


Outcome:

- Successfully cleared the second level using the correct surname.
- Progressed to the next stage of the game.

Level 3 Discovery Summary

After numerous trial-and-error attempts, I successfully uncovered the next clue by modifying the URL structure. I added a **"+" symbol** to the shortened Bitly link provided in the game, which redirected me to a **Bitly analytics page**. This page revealed the **destination URL**—a LinkedIn profile belonging to **Jan Tegze**—and clearly displayed the **creation date** of the Bitly link: **April 17, 2020, at 16:18 UTC**.



Outcome:

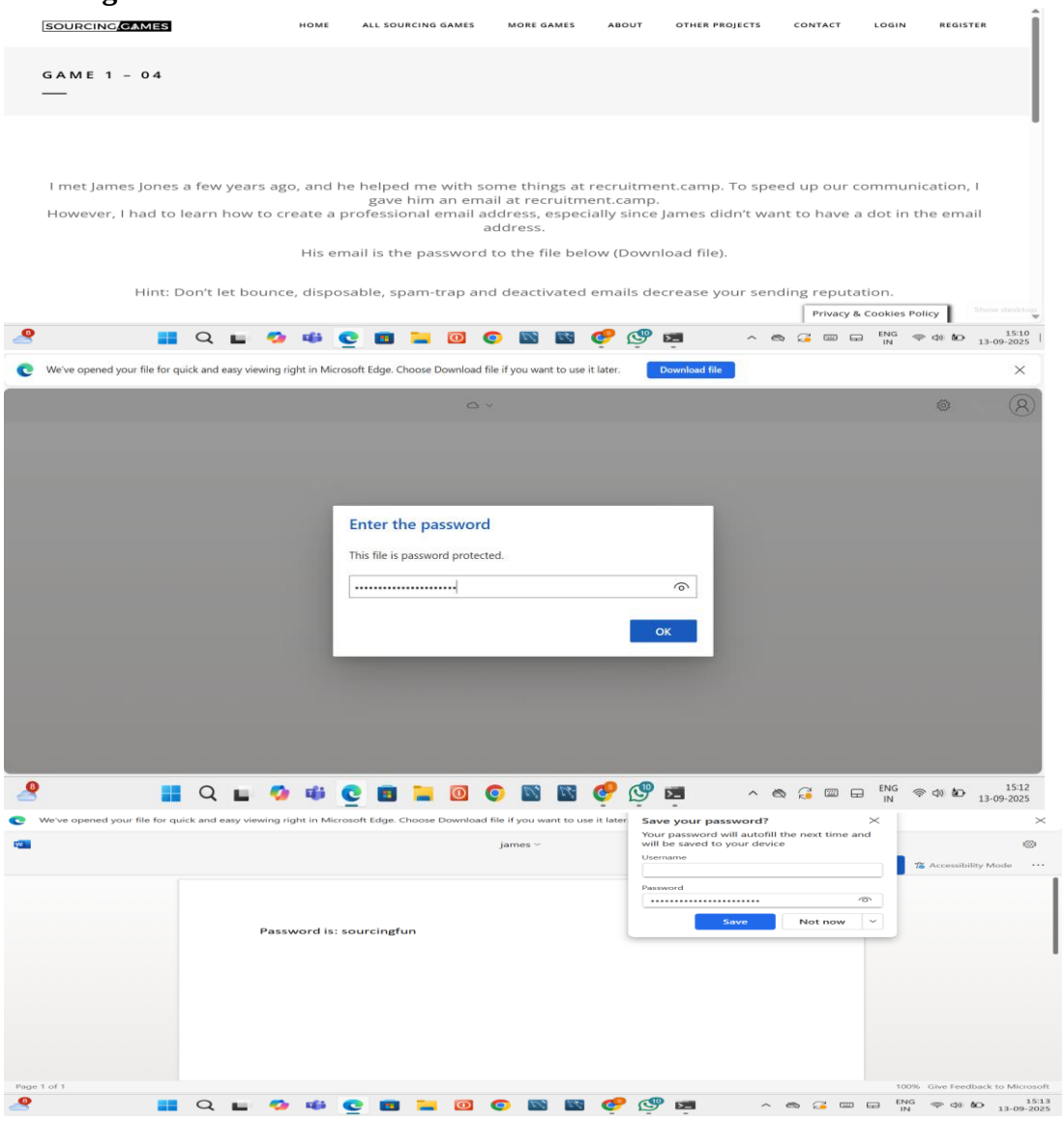
- Identified the correct person and relevant date
- Used the date in the required format (`month-day`, e.g., `apr-17`) to unlock the next level

Challenges Faced:

- Initial confusion over password format
- Multiple incorrect attempts before discovering the Bitly trick
- Required persistence and creative thinking to decode the clue

Level 4 Discovery Summary

In this stage, the challenge involved deducing a professional email address used by **James Jones** at the domain **recruitment.camp**. The hint specified that the email should not contain a dot, and that the correct email would serve as the password to unlock a protected file.Initially, I attempted various combinations using the name "James" and common email formats, but none were successful. After multiple failed attempts, I began experimenting with **initials**.Eventually, I discovered that the format **jamesj@recruitment.camp** was accepted and successfully unlocked the file.Inside the file, I found the password for the next level: **sourcingfun**



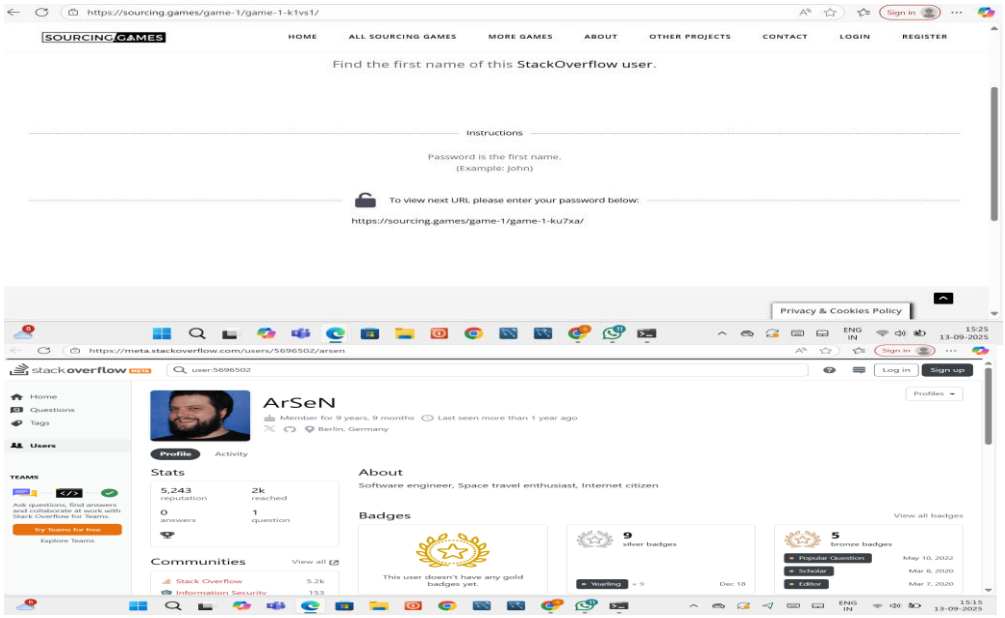
Challenges Faced

- Blank page with no feedback or error message
- Required creative thinking and URL structure analysis
- Time-consuming trial-and-error process

Level 5 Discovery Summary

In this stage, I encountered a challenge involving a person's image and a misleading username. The image was linked to a profile under the name **"ArSeN"** on Stack Overflow. Initially, I assumed this was the individual's real name. However, after deeper investigation and using **Google Lens**, I discovered that "ArSeN" was just a username.

By reverse searching the image, I was able to locate the person's **professional profile on Xing**, which revealed his actual name: **Kolja Zuelsdorf**, a Software Security Engineer based in Berlin, Germany.



Challenges Faced:

- Misleading username created initial confusion
- Required cross-platform verification to confirm identity
- Needed persistence and image-based search skills

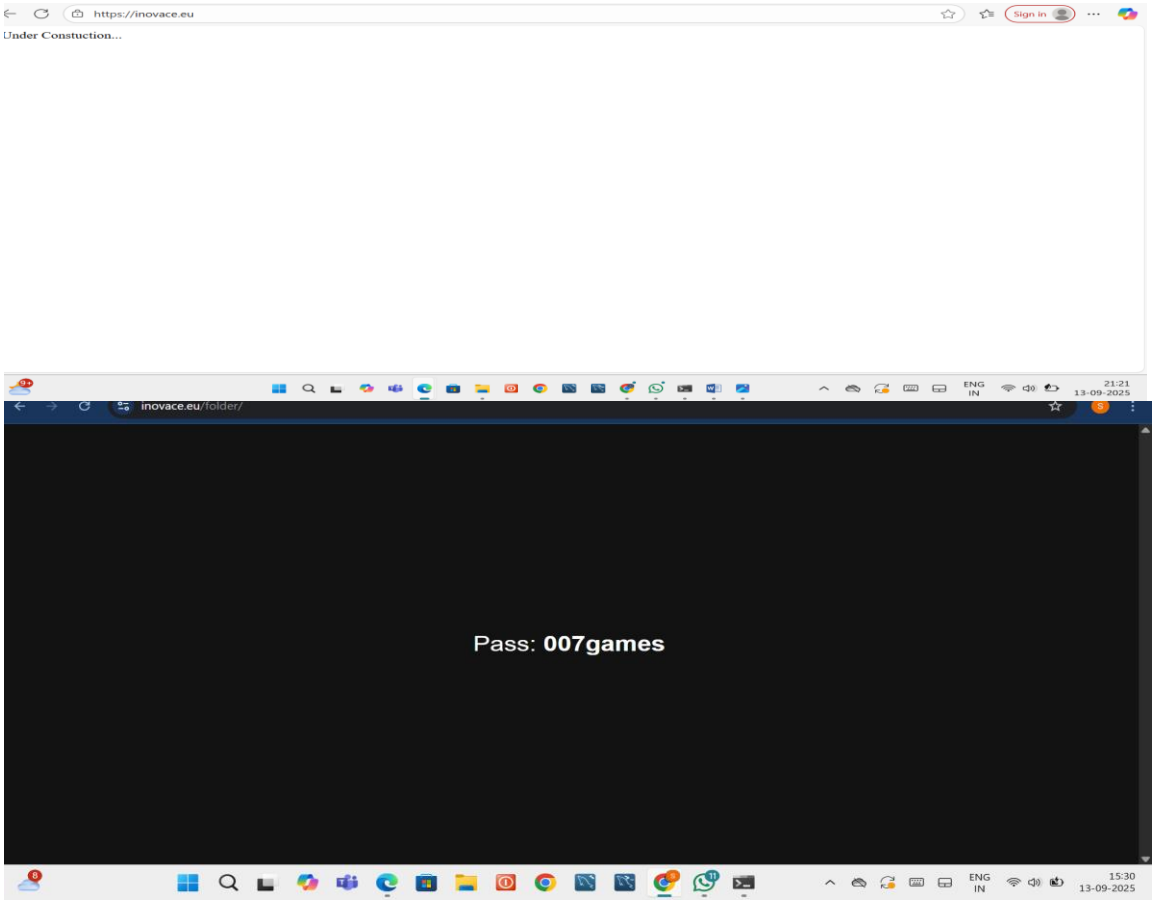
Outcome:

- Correctly identified the person behind the alias "ArSeN"
- Retrieved the real name needed to progress in the game

Level 6 Discovery Summary:

In this stage, I encountered a dead-end while attempting to access a linked website. The page consistently loaded as blank, offering no clues or interactive elements. After extensive research and experimentation, I discovered that appending "**/folder**" to the base URL successfully redirected me to a new page containing the next clue.

This breakthrough revealed a password: **007games**, which was displayed prominently on the newly accessed page. This password was then used to unlock the next level of the game.

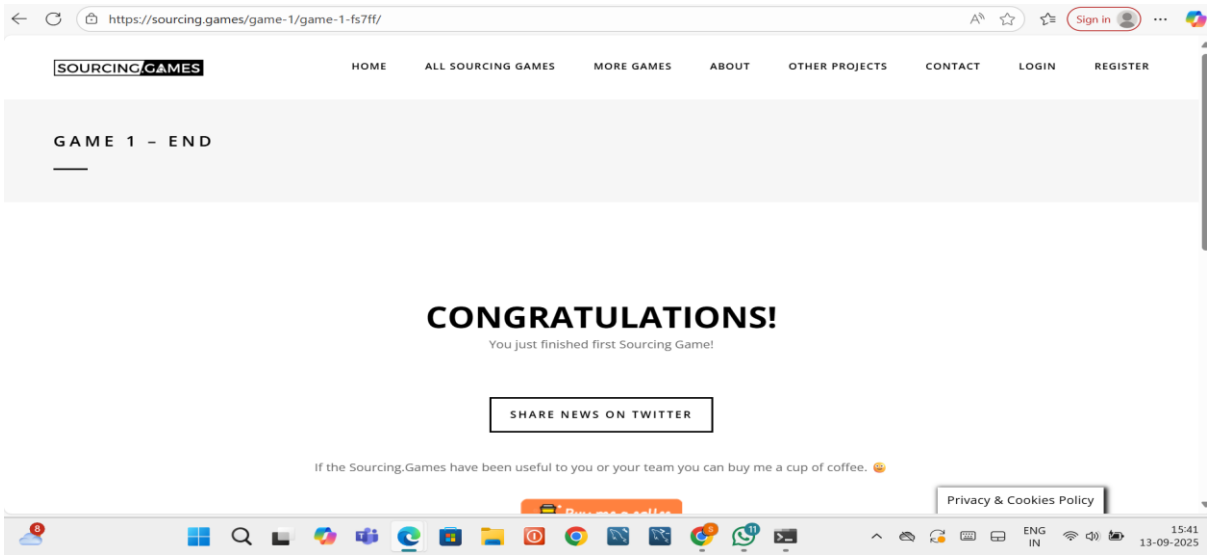


Challenges Faced

- Blank page with no feedback or error message
- Required creative thinking and URL structure analysis
- Time-consuming trial-and-error process

Outcome

- Bypassed a blank page by adding `/folder` to the URL
- Retrieved the password `007games` to proceed



4. Reflection (Short Write-Up):

- This week, I learned how to effectively use reverse image search tools like Google Lens to identify individuals, how to manipulate URLs to uncover hidden pages, and how to decode password formats based on contextual clues.I also gained experience in verifying identities across platforms such as LinkedIn, Xing, and Stack Overflow. One technique I want to explore further is Bitly link analysis, especially how metadata can reveal critical timestamps and redirect paths.
- A major challenge I faced was dealing with blank or misleading web pages; I overcame this by experimenting with URL extensions like "/folder" to access hidden content. These skills have sharpened my ability to think creatively and critically—essential traits for future OSINT tasks where uncovering hidden information and verifying sources are key to success.