Muhammad Faizan Arshad - 221577

Digital Forensics - Lab Task #6

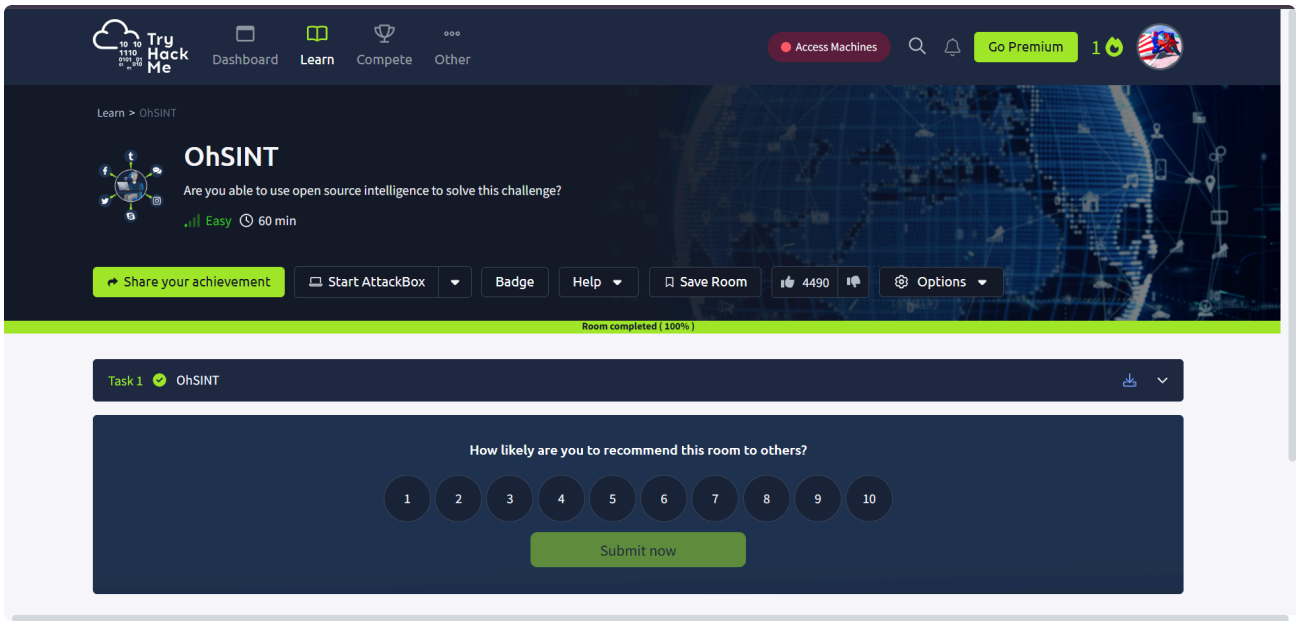
Task #1: TryHackMe OSINT Challenge

In this challenge, the most amount of information is extracted from a single image file using the technique of Open Source Intelligence (`OSINT`).

What is OSINT?

Open-source intelligence, or OSINT, refers to the process of gathering information from public, legal data sources to serve a specific function. Some open sources might include social media, blogs, news, and the dark web.

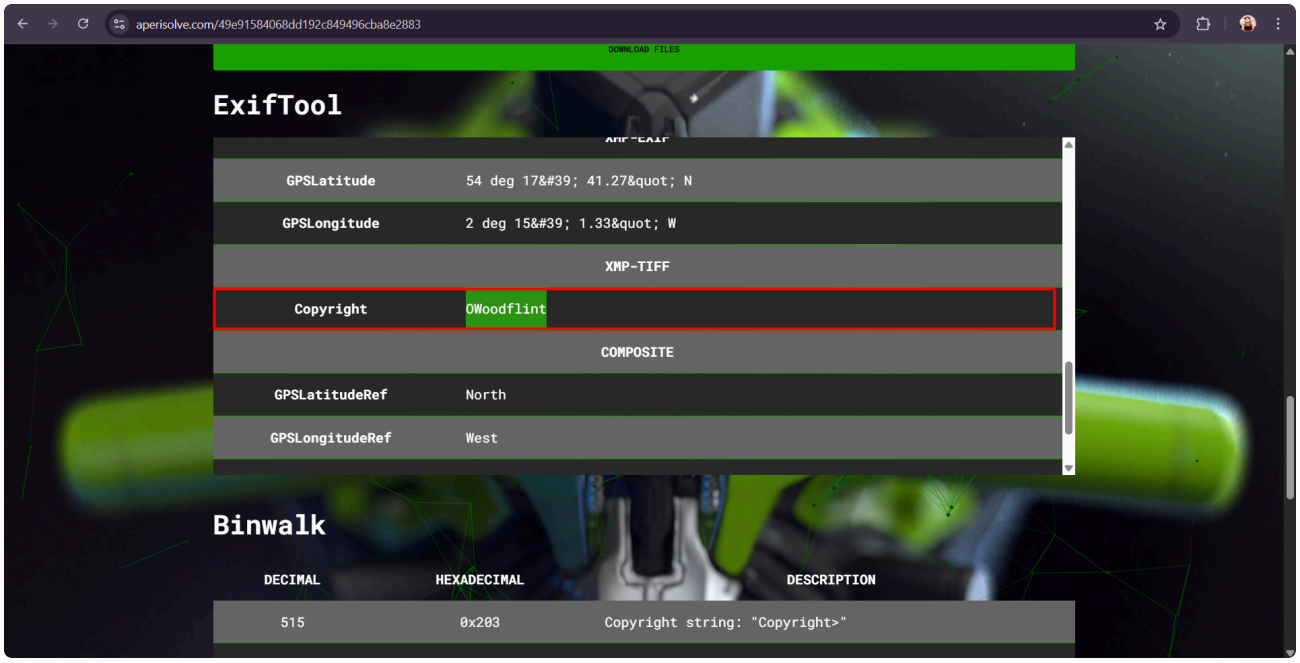
Room Overview:



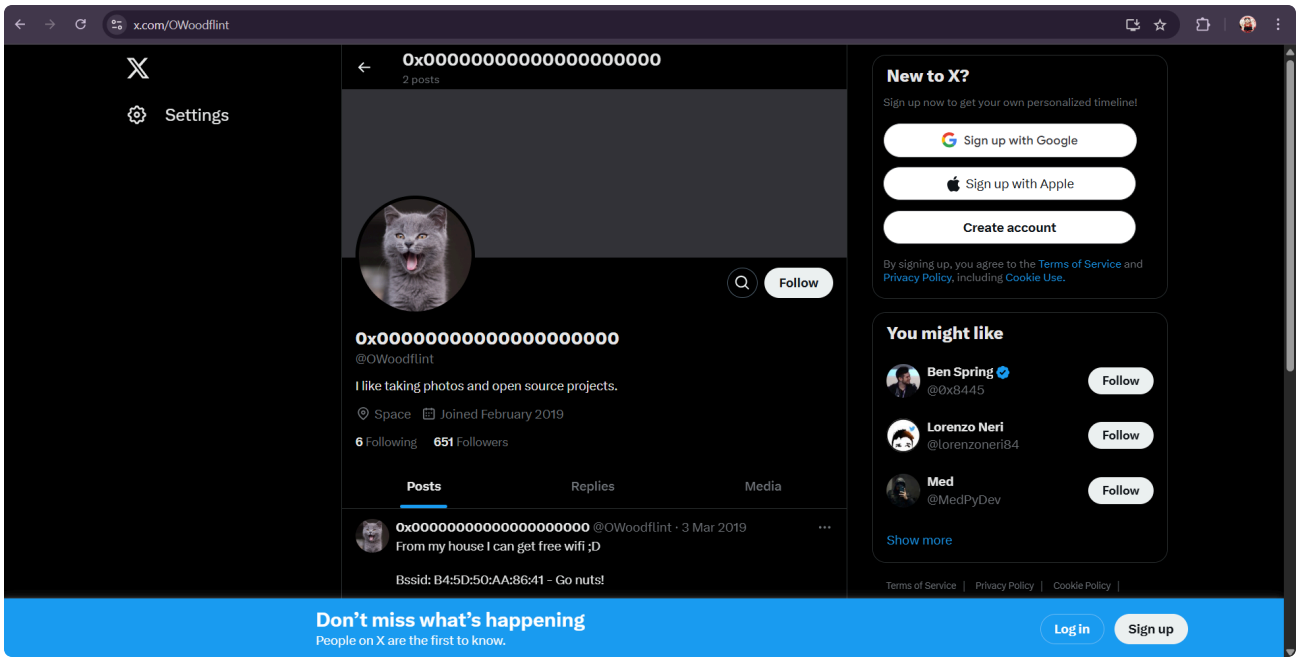
Question #1: What is this user's avatar of?

First of all, the image was downloaded and pasted on `Exiftool` to get a clue on who uploaded the image in the first place, prompting the need of Social Media Intelligence. The

`Exiftool` gives us the following findings:



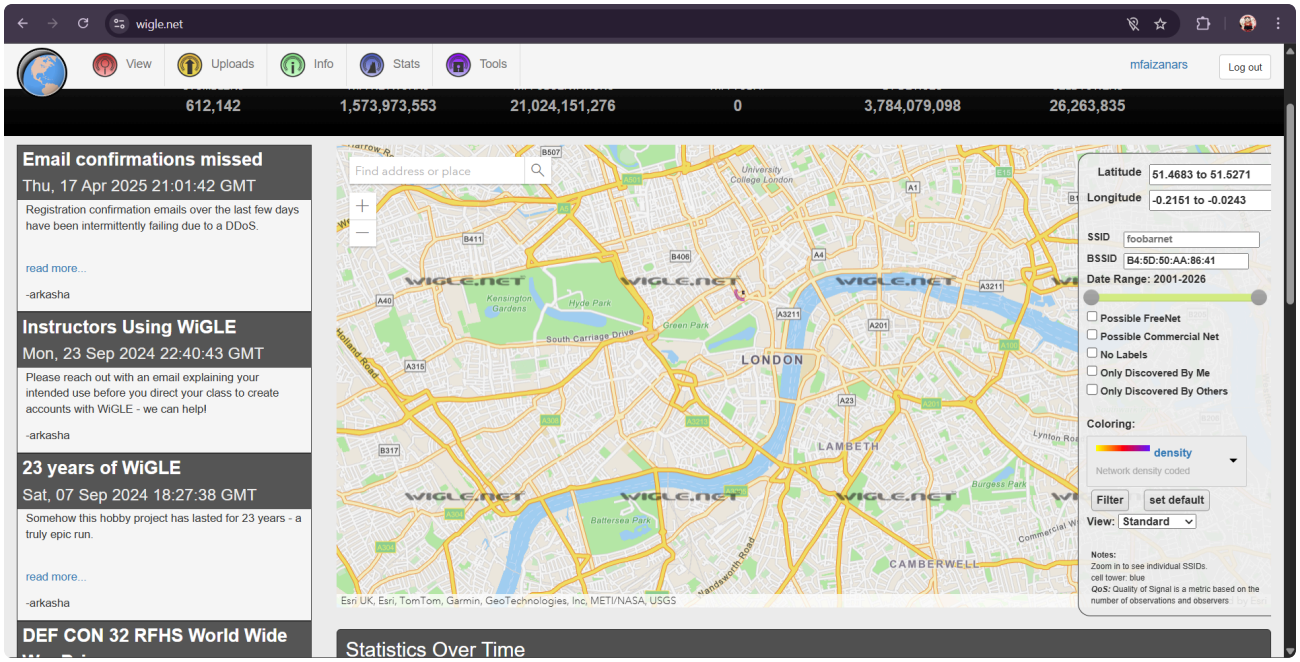
Searching this username on the browser led to a Twitter page, given as:



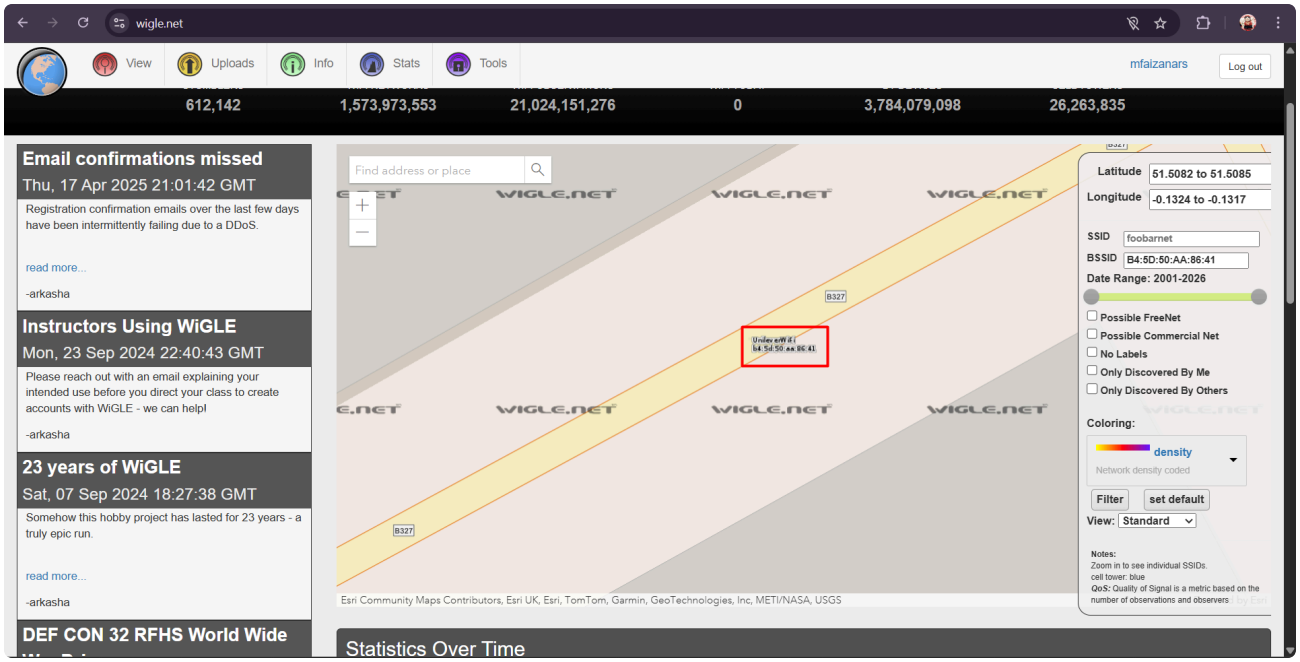
As we can see, the profile picture is of a `cat`!

Question #2 - #3: What city is this person in? What is the SSID of the WAP he connected to?

The hint of this question says: `BSSID + Wigle.net` and hence, the `BSSID` was pasted on `Wiggle.net` to filter out the complete location of the user. The process is given as follows:



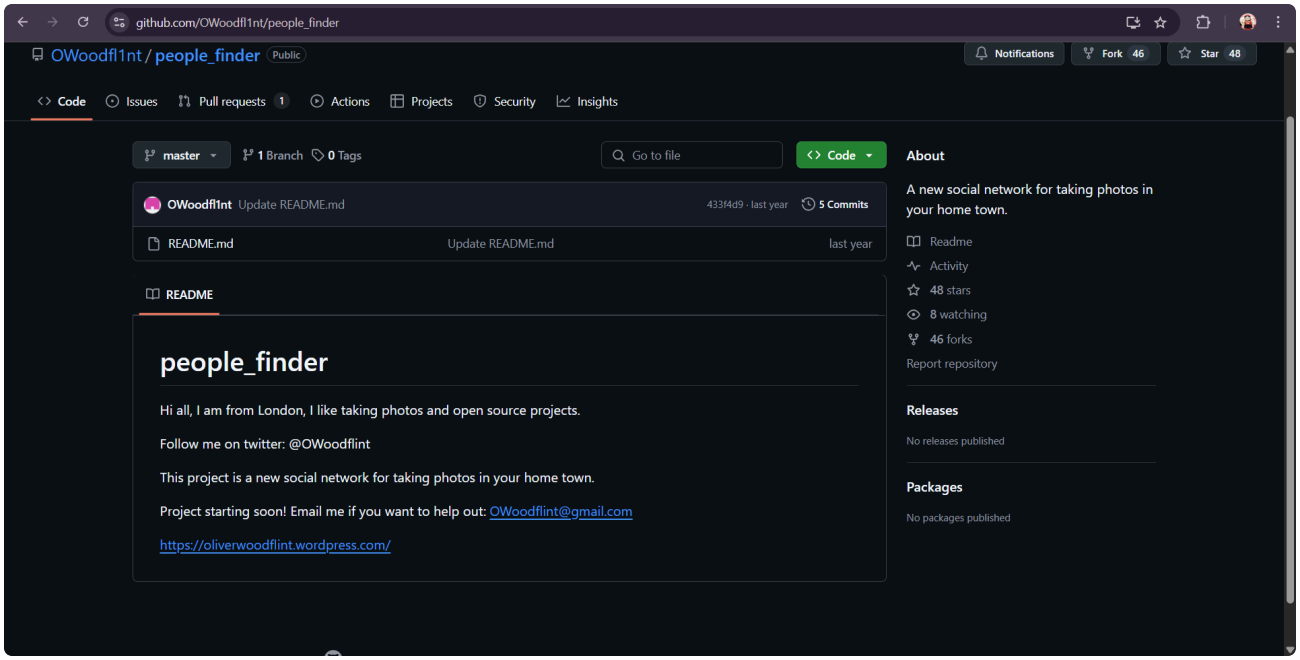
The location is found to be `London`. Upon zooming in, the SSID of the WAP is uncovered as `UnileverWIFI`. The screenshot is given as:



Question #4 - #5: What is his personal email address? What site did you find his email address on?

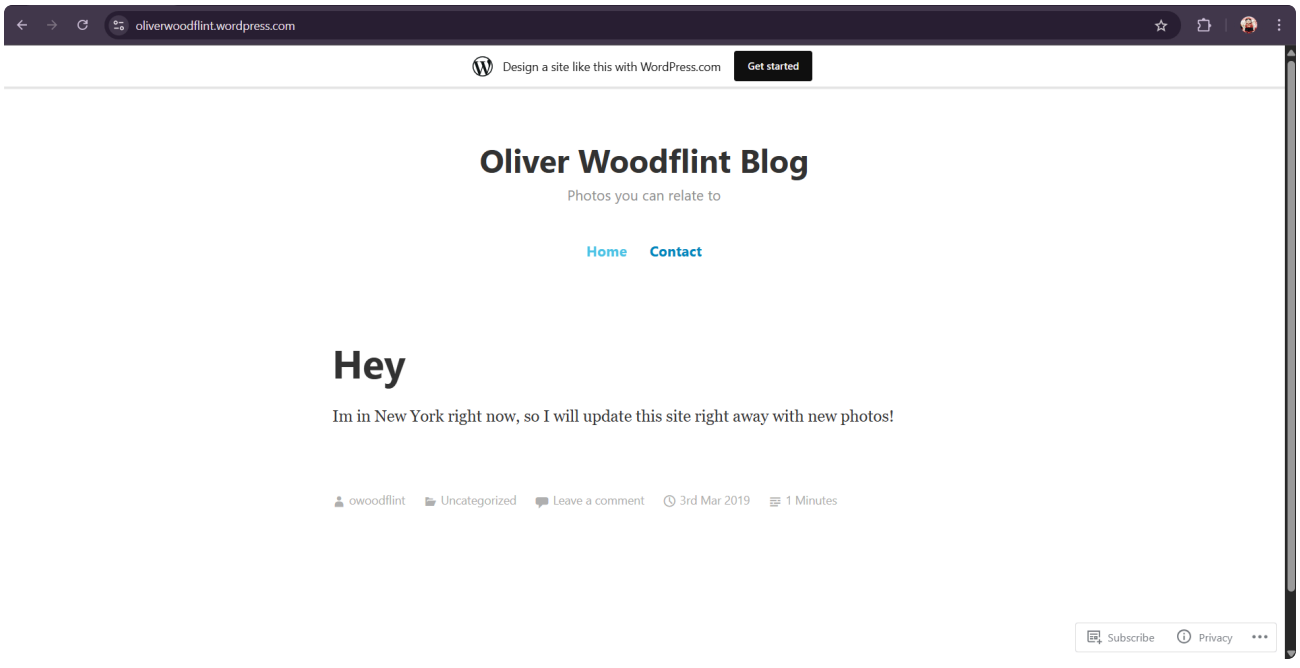
Upon further search, the email address of the username was found on `GitHub` under their personal project of `people_finder` as `OWoodflint@gmail.com`.

The details are given as:

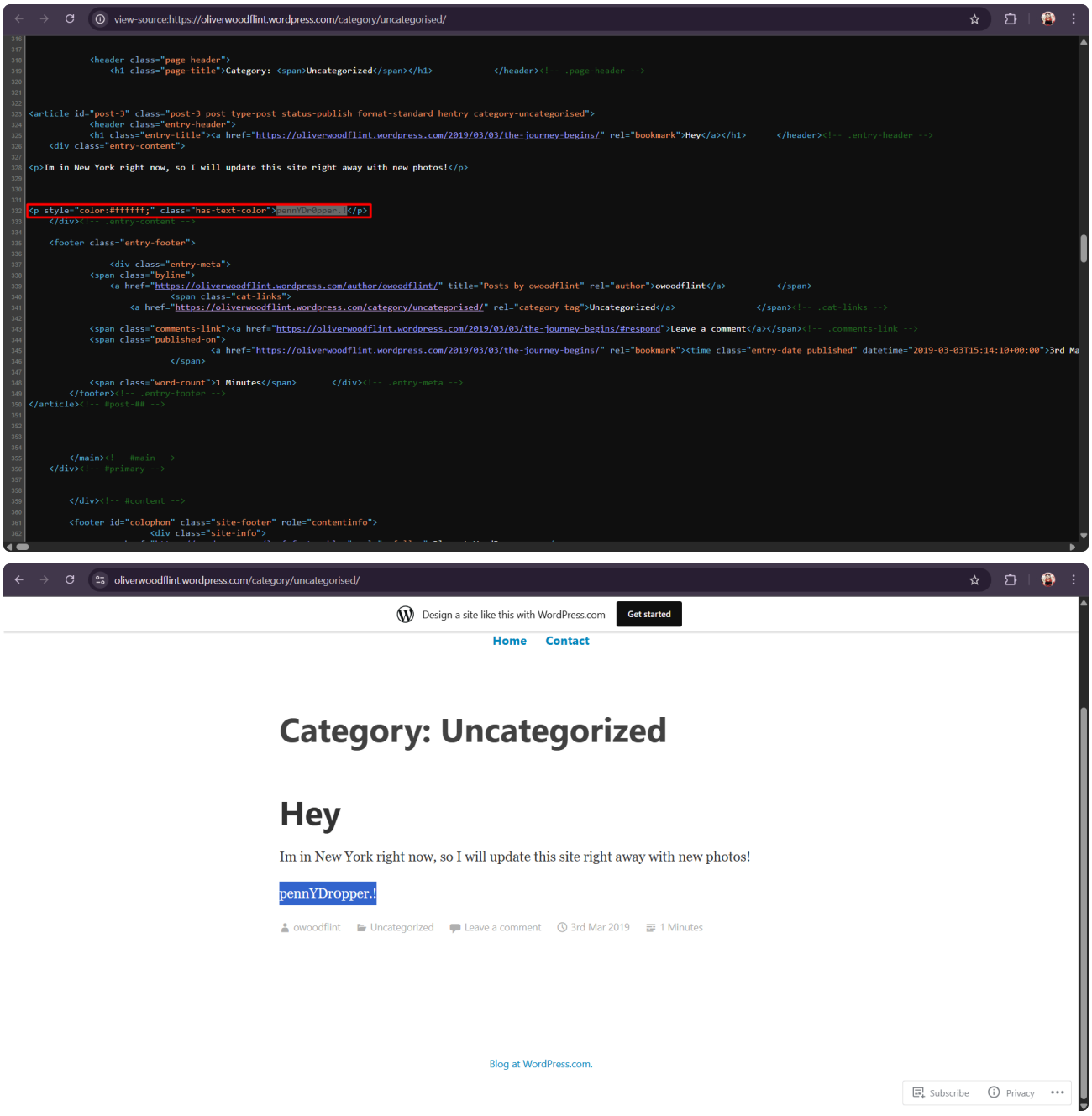


Question #6 - #7: Where has he gone on holiday? What is the person's password?

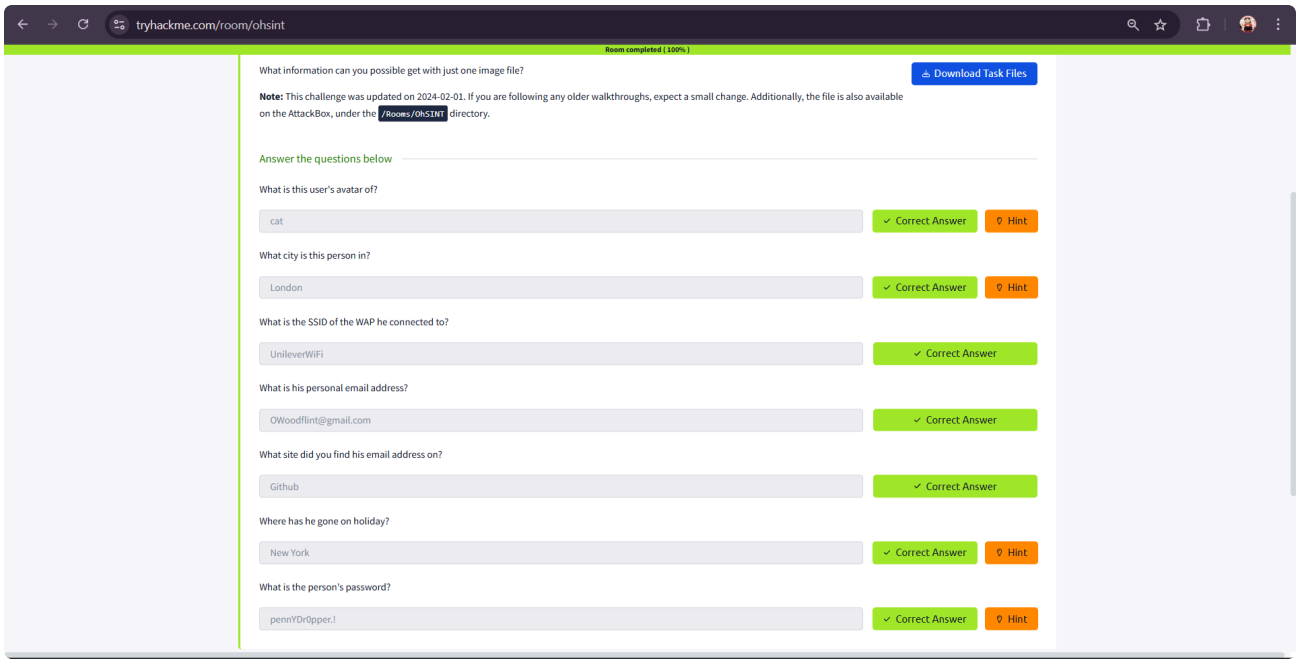
User had taken a holiday to `New York`, and this was found from this WordPress website as follows:



The password was also found as `pennYDr0pper.!` by viewing the source code of the website as follows:



Proof of Answers

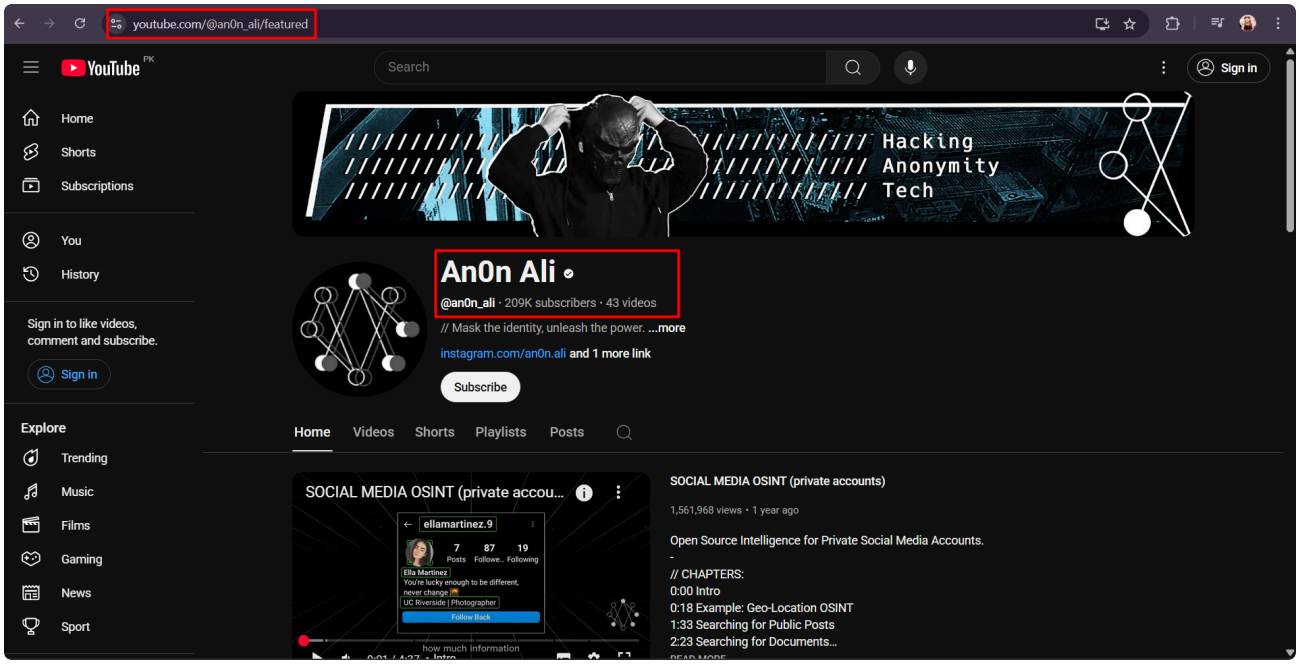


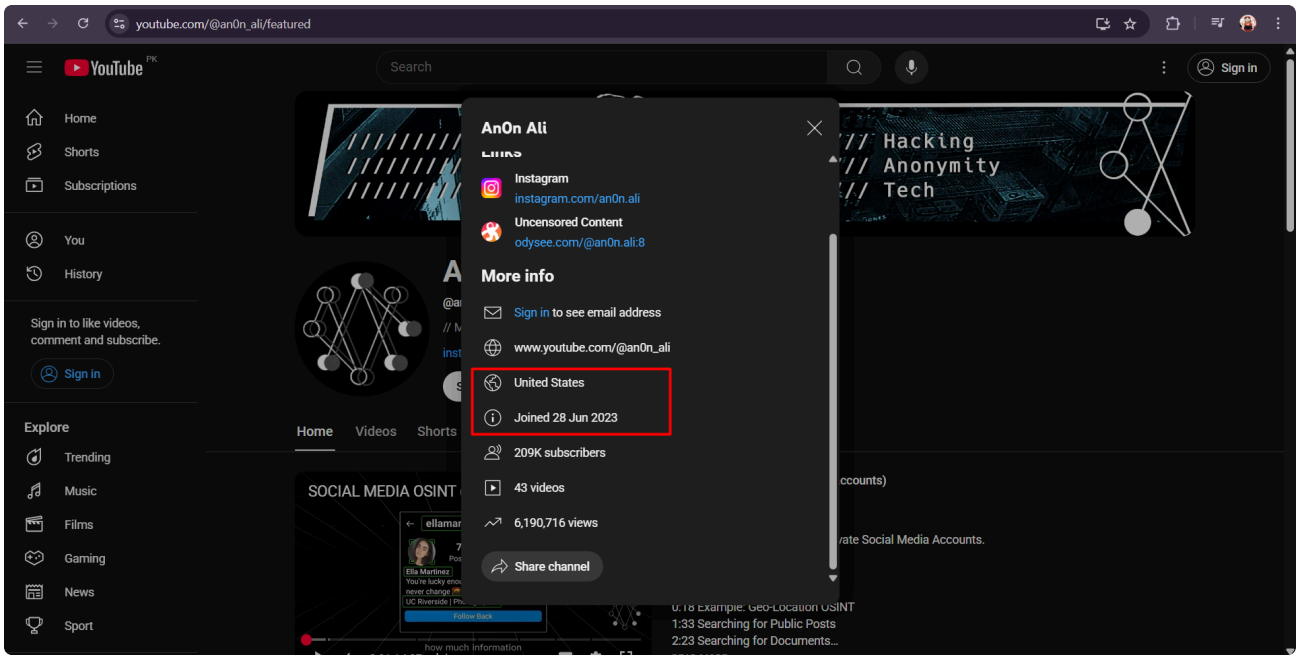
Task #2: Investigate a YouTube Channel using OSINT Techniques

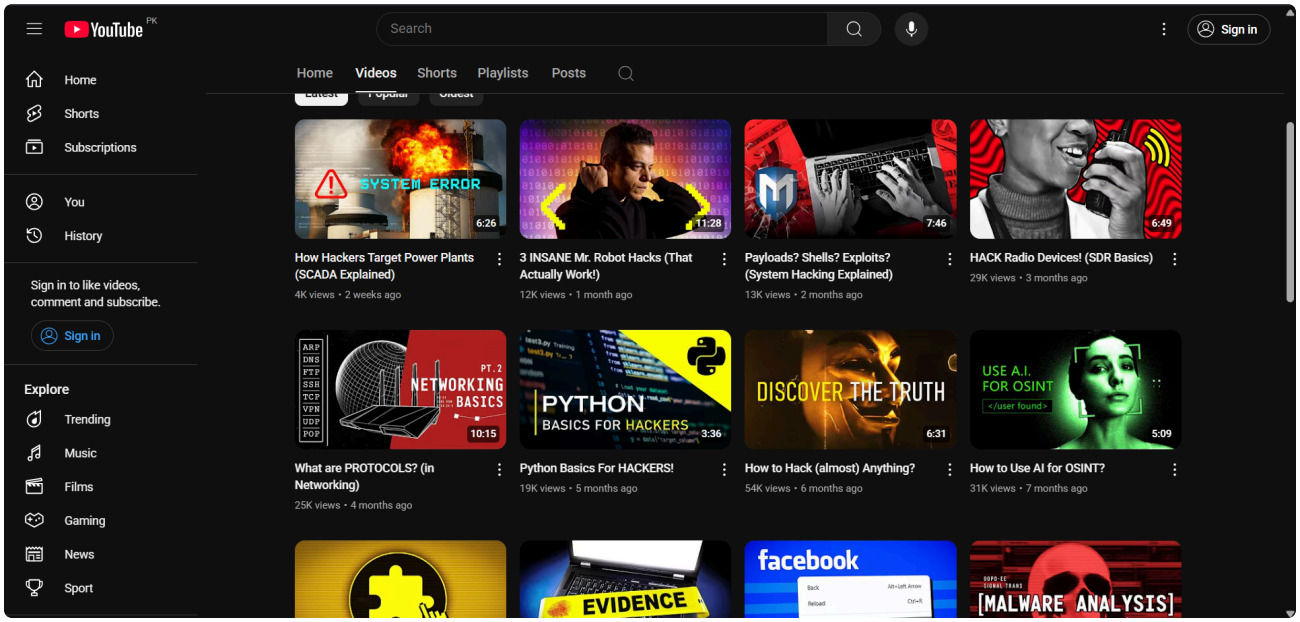
Part A: Channel Information

Username: `An0n Ali (@an0n_ali)`
URL: `https://www.youtube.com/@an0n_ali/`
Number of Subscribers: 209K
Join date: 28 June, 2023
Country: United States
Type of content uploaded: Ethical Hacking, Informational, Educational

Screenshots:



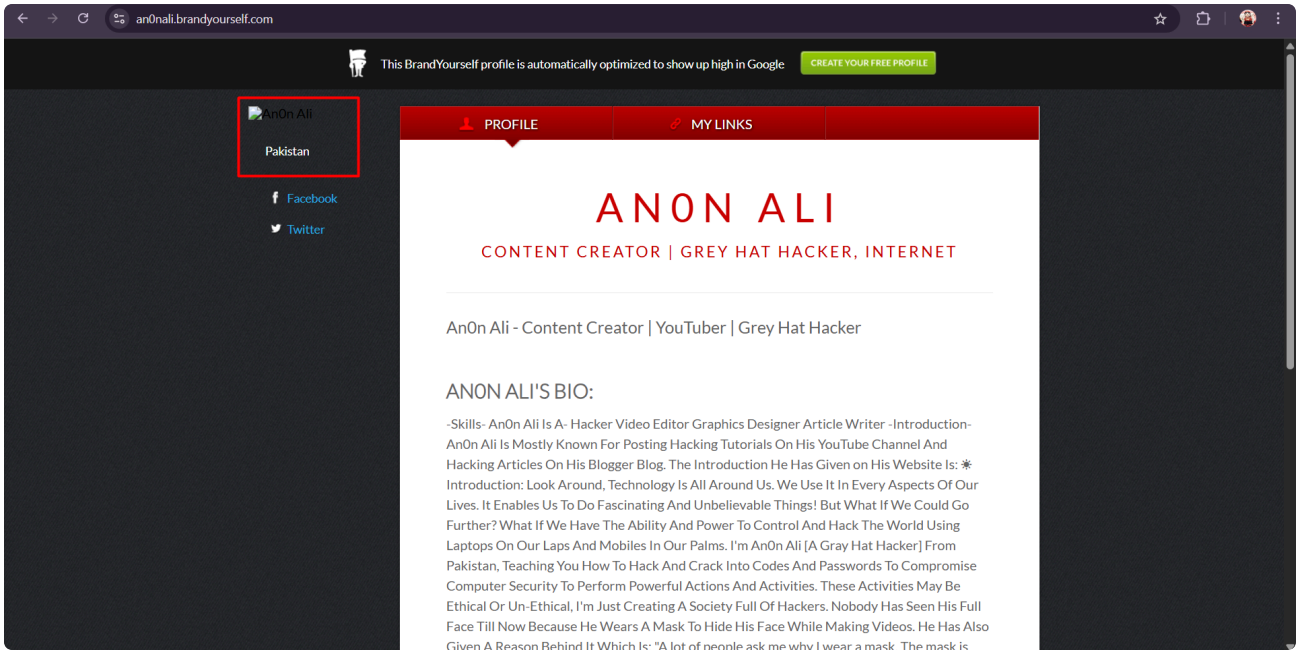




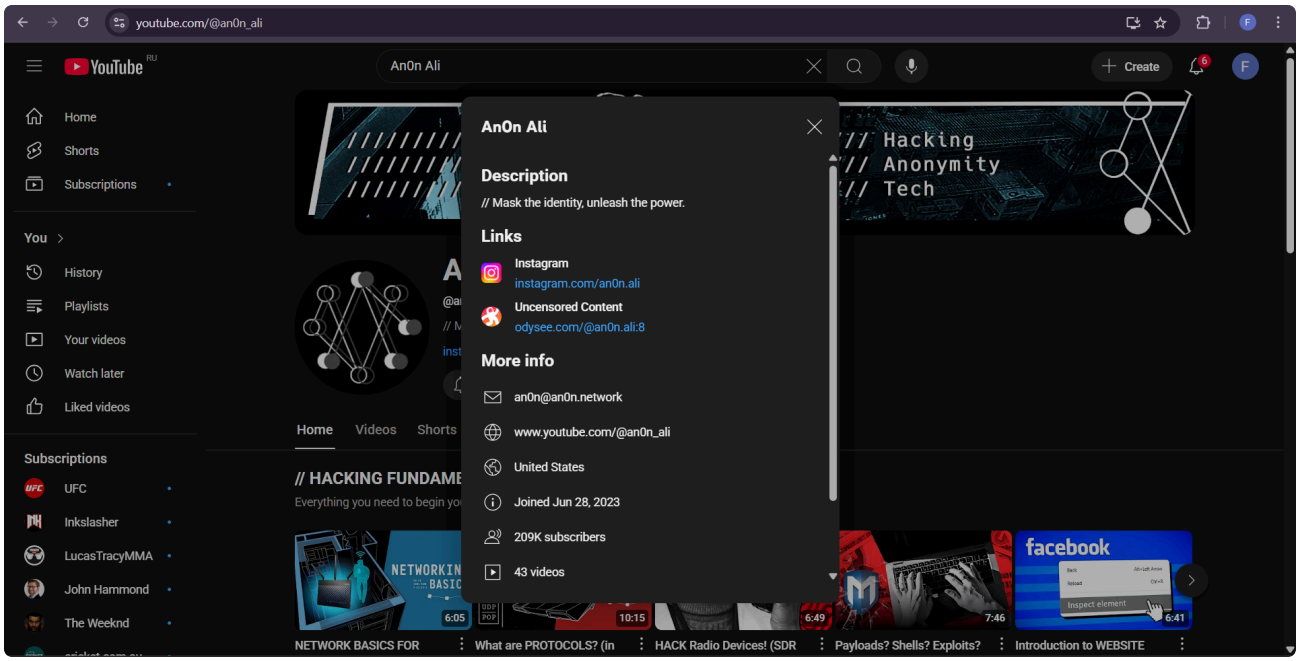
Part B: OSINT-Based Analysis

Upon searching online, it was found that although the channel is from `United States`, the channel owner is from `Pakistan`. This was found from the website

`https://an0nali.brandyourself.com/`, proof of which is given as:



Moreover, the links to external sites were found as well along with the email address, given as follows:



The channel has Twitter, and Facebook presence as well.

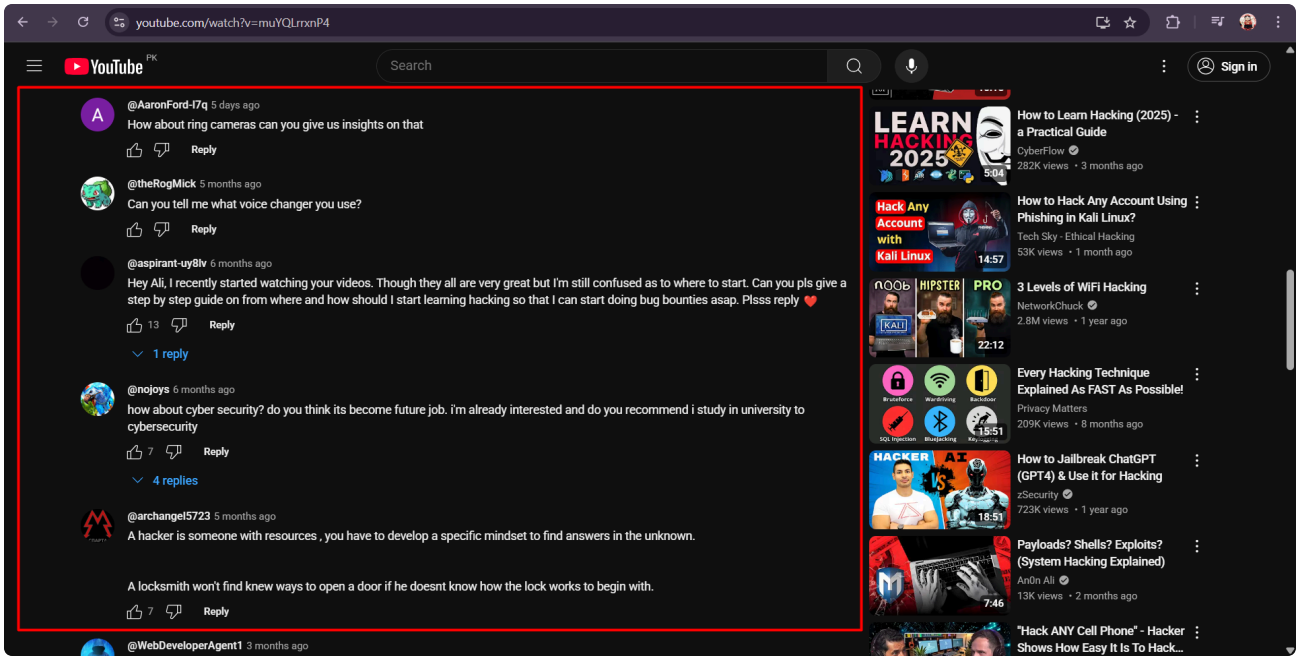
Part C: Behavioral Analysis

Is the content educational of suspicious?

The content is completely education as well as informative, as the channel spreads awareness online regarding cyber threats and instructs how to tackle with them. Moreover, the channel itself teaches ethical hacking as well. Moreover, every video contains a disclaimer that states that all the videos are completely educational.

Do the video comments contain links to illegal services?

No, not at all. Sample screenshot is given as:



Is there promotion of hacking tools or cracked software?

No, it does not. Not in any video.

Does the creator hide their identity or act anonymously?

Yes, the creator maintains anonymity by hiding their true identity and by changing their voice.

Conclusion

All the mentioned deliverables have been answered in detail, stating each and every answer with a solid proof.