

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:

The screenshot shows the TryHackMe interface for the 'OhSINT' room. At the top, there's a navigation bar with 'Try Hack Me' logo, user stats (1110 points, 29 solves, 30% streak), and links for Dashboard, Learn, Compete, and Other. On the right are buttons for 'Access Machines', 'Go Premium', notifications, and a profile icon. Below the nav is a globe map with network nodes. The main area has a dark background with a green progress bar at the bottom indicating 'Room completed (100%)'. A sub-header 'Learn > OhSINT' is followed by the room title 'OhSINT'. It asks 'Are you able to use open source intelligence to solve this challenge?' and shows difficulty level 'Easy' and time '60 min'. Below are buttons for 'Share your achievement', 'Start AttackBox', 'Badge', 'Help', 'Save Room', '4490 likes', and 'Options'. A task card for 'Task 1' is shown with a green checkmark and the name 'OhSINT'. At the bottom, a survey asks 'How likely are you to recommend this room to others?' with a scale from 1 to 10 and a 'Submit now' button.

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:

The screenshot shows two overlapping windows. The top window is titled 'ExifTool' and displays metadata from a file named 'aperisolve.com/49e91584068dd192c849496cba8e2883'. The 'XMP-TIFF' section contains a 'Copyright' field with the value '0Woodflint', which is highlighted with a red border. The bottom window is titled 'Binwalk' and shows the byte content of the file. It has three tabs: 'DECIMAL', 'HEXADECIMAL', and 'DESCRIPTION'. The 'DESCRIPTION' tab shows the string 'Copyright string: "Copyright>"'. The background of the entire screen is a dark image of a person's face.

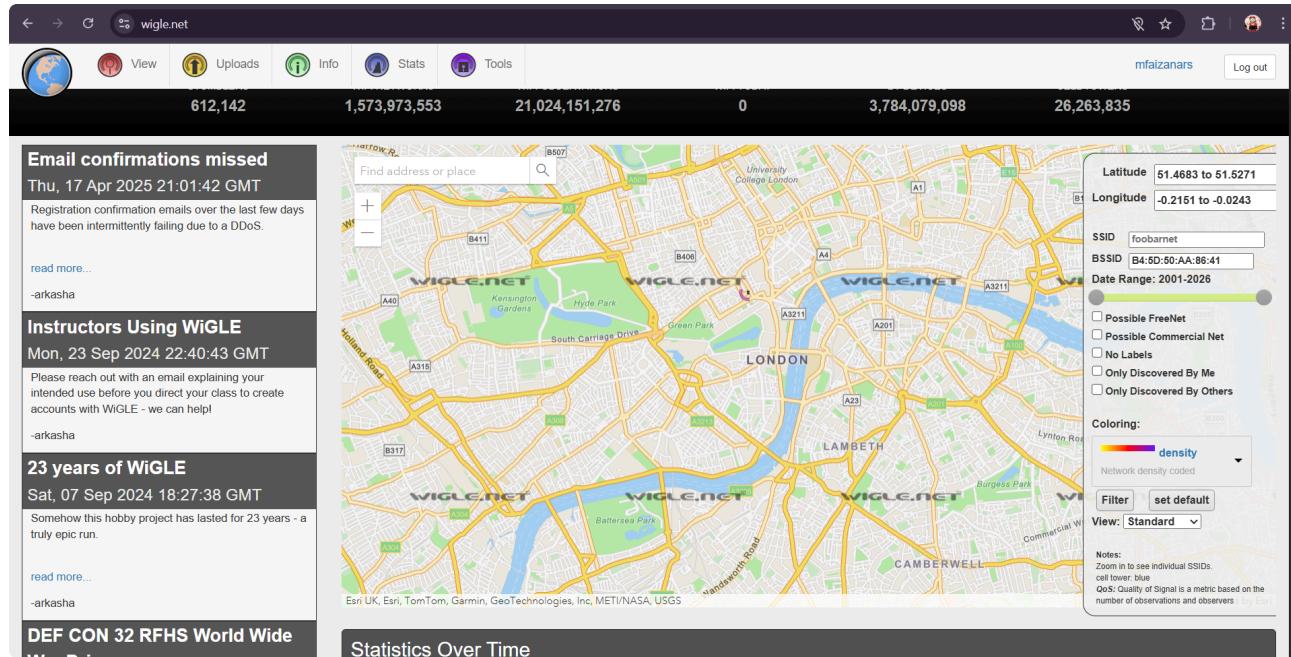
Searching this username on the browser led to a Twitter page, given as:

The screenshot shows a Twitter profile for the user '0x00000000000000000000000000000000' (@0Woodflint). The profile picture is a cat. The bio reads: 'I like taking photos and open source projects.' The user joined in February 2019. They have 6 Following and 651 Followers. There is one post visible: 'From my house I can get free wifi ;D'. The footer of the page includes a 'Don't miss what's happening' message, 'Log in', and 'Sign up' buttons.

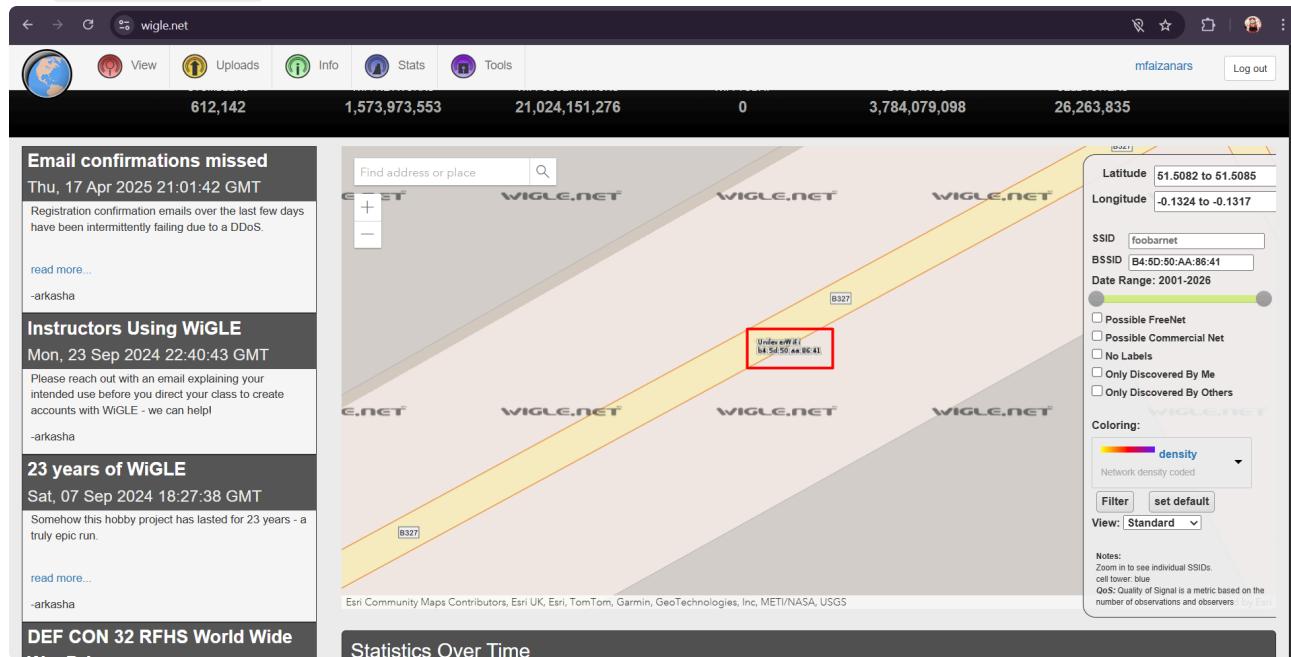
As we can see, the profile picture is of a cat !

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 `Wigle.net` to filter out the complete location of the user. The process is given as follows:



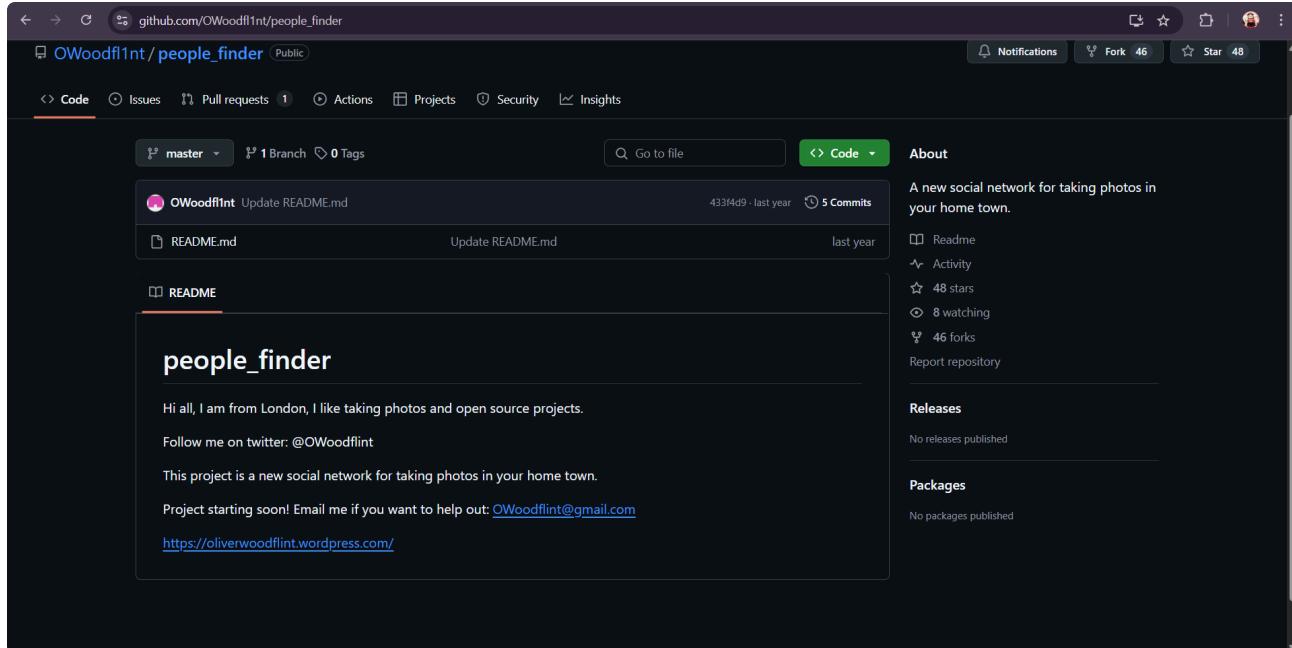
The location is found to be `London`. Upon zooming in, the SSID of the WAP is uncovered as `UnileverWIFI`. The screenshot is given as:



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 `0Woodflint@gmail.com`.

The details are given as:



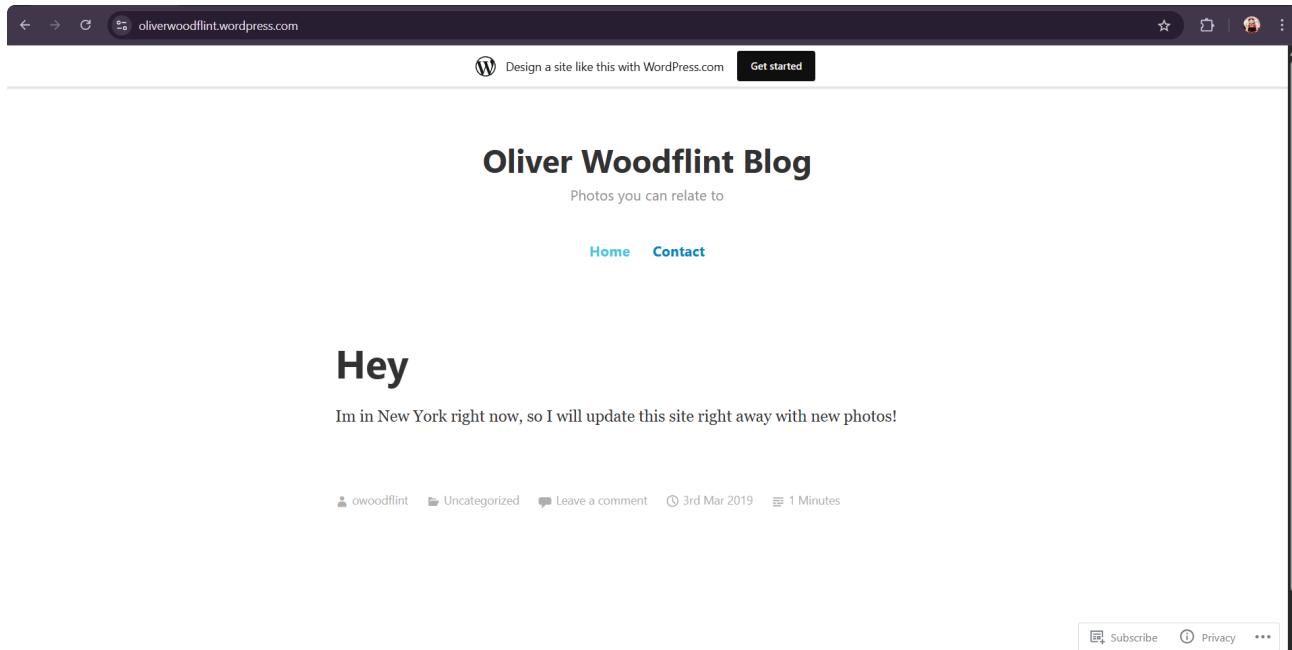
A screenshot of a GitHub repository page for 'OWoodflint/people_finder'. The repository has 1 branch and 0 tags. The README.md file contains the following content:

```
Hi all, I am from London, I like taking photos and open source projects.  
Follow me on twitter: @OWoodflint  
This project is a new social network for taking photos in your home town.  
Project starting soon! Email me if you want to help out: OWoodflint@gmail.com  
https://oliverwoodflint.wordpress.com/
```

The repository has 5 commits, 48 stars, 8 watching, 46 forks, and 46 contributors. It also includes sections for About, Releases, and Packages.

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:



A screenshot of a WordPress blog titled 'Oliver Woodflint Blog'. The post is titled 'Hey' and contains the text: 'Im in New York right now, so I will update this site right away with new photos!'. The post was made by 'owoodflint' on 3rd Mar 2019, and it took 1 Minutes to read. There are links for Home and Contact at the bottom of the post.

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

```
316
317     <header class="page-header">
318         <h1 class="page-title">Category: <span>Uncategorized</span></h1>           </header><!-- .page-header -->
319
320
321
322 <article id="post-3" class="post-3 post type-post status-publish format-standard hentry category-uncategorised">
323     <header class="entry-header">
324         <h1 class="entry-title"><a href="https://oliverwoodflint.wordpress.com/2019/03/03/the-journey-begins/" rel="bookmark">Hey</a></h1>           </header><!-- .entry-header -->
325     <div class="entry-content">
326
327     <p>Im in New York right now, so I will update this site right away with new photos!</p>
328
329
330
331
332     <p style="color:#ffffff;" class="has-text-color">pennYDropper!</p>
333
334
335 <footer class="entry-footer">
336
337     <div class="entry-meta">
338         <span class="byline">
339             <a href="https://oliverwoodflint.wordpress.com/author/owoodflint/" title="Posts by owoodflint" rel="author">owoodflint</a>           </span>
340
341             <span class="cat-links">
342                 <a href="https://oliverwoodflint.wordpress.com/category/uncategorised/" rel="category tag">Uncategorized</a>           </span><!-- .cat-links -->
343
344         <span class="comments-link"><a href="https://oliverwoodflint.wordpress.com/2019/03/03/the-journey-begins/#respond">Leave a comment</a></span><!-- .comments-link -->
345         <span class="published-on">
346             <a href="https://oliverwoodflint.wordpress.com/2019/03/03/the-journey-begins/" rel="bookmark"><time class="entry-date published" datetime="2019-03-03T15:14:10+00:00">3rd Ma
347
348             <span class="word-count">1 Minutes</span>           </div><!-- .entry-meta -->
349
350 </footer><!-- .entry-footer -->
351
352
353
354
355     </main><!-- #main -->
356 </div><!-- #primary -->
357
358
359 </div><!-- #content -->
360
361 <footer id="colophon" class="site-footer" role="contentinfo">
362     <div class="site-info">
```

oliverwoodflint.wordpress.com/category/uncategorised/

 Design a site like this with WordPress.com [Get started](#)

[Home](#) [Contact](#)

Category: Uncategorized

Hey

Im in New York right now, so I will update this site right away with new photos!

[pennYDropper!](#)

 owoodflint  Uncategorized  Leave a comment  3rd Mar 2019  1 Minutes

Blog at WordPress.com.

 [Subscribe](#)  [Privacy](#) 

Proof of Answers

tryhackme.com/room/ohsint

Rooms completed (100%)

Download Task Files

What information can you possibly get with just one image file?

Note: This challenge was updated on 2024-02-01. If you are following any older walkthroughs, expect a small change. Additionally, the file is also available on the AttackBox, under the `/Rooms/OHSINT` directory.

Answer the questions below

What is this user's avatar of?
cat ✓ Correct Answer 💡 Hint

What city is this person in?
London ✓ Correct Answer 💡 Hint

What is the SSID of the WAP he connected to?
UnileverWiFi ✓ Correct Answer

What is his personal email address?
OWoodflint@gmail.com ✓ Correct Answer

What site did you find his email address on?
Github ✓ Correct Answer

Where has he gone on holiday?
New York ✓ Correct Answer 💡 Hint

What is the person's password?
pennYDr0pper! ✓ Correct Answer

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/

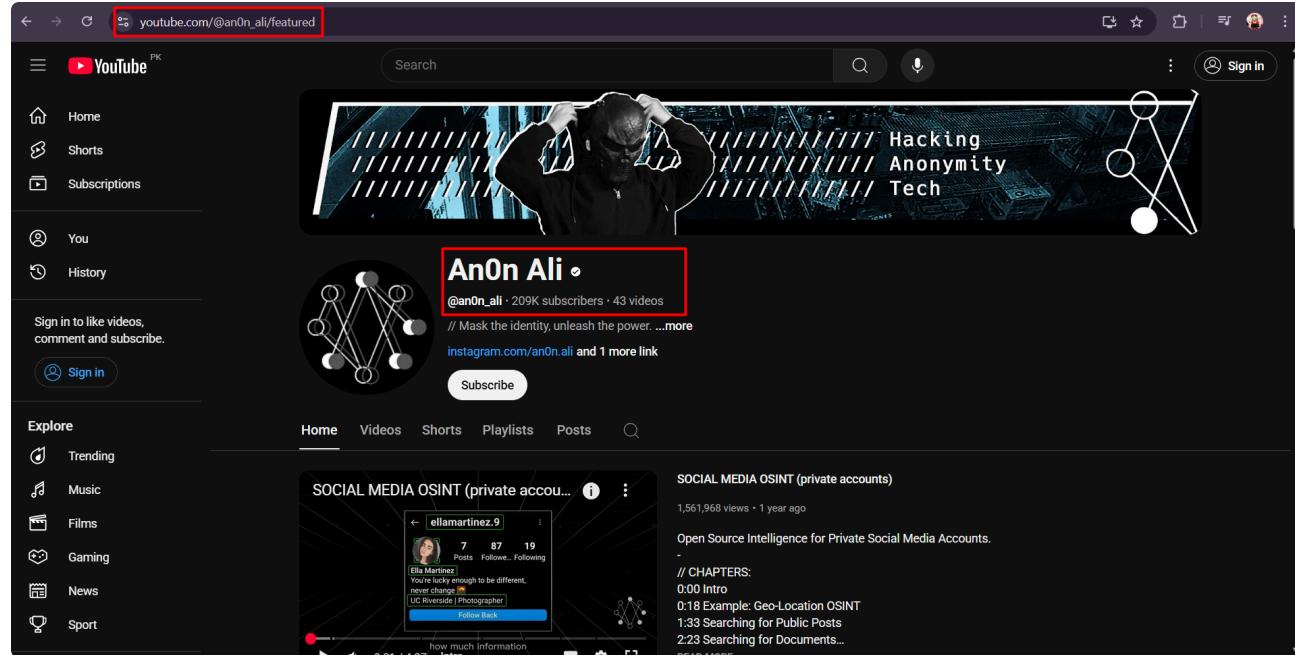
Number of Subscribers: 209K

Join date: 28 June, 2023

Country: United States

Type of content uploaded: Ethical Hacking, Informational, Educational

Screenshots:



The image consists of two screenshots of a YouTube channel named 'AnOn Ali'.
The top screenshot shows the channel's profile page. It features a banner with the text 'Hacking', 'Anonymity', and 'Tech'. Below the banner, there is a 'More info' section with a red box highlighting the location 'United States' and the joining date 'Joined 28 Jun 2023'.
The bottom screenshot shows a grid of video thumbnails. The videos include topics such as 'How Hackers Target Power Plants (SCADA Explained)', '3 INSANE Mr. Robot Hacks (That Actually Work)', 'Payloads? Shells? Exploits? (System Hacking Explained)', 'HACK Radio Devices! (SDR Basics)', 'What are PROTOCOLS? (in Networking) PT. 2 NETWORKING BASICS', 'Python Basics For HACKERS!', 'DISCOVER THE TRUTH', 'How to Hack (almost) Anything?', 'How to Use AI for OSINT?', 'EVIDENCE', 'facebook', and '[MALWARE ANALYSIS]'. Each thumbnail includes a play button and a timestamp.

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:

This BrandYourself profile is automatically optimized to show up high in Google [CREATE YOUR FREE PROFILE](#)

AnOn Ali
Pakistan

[Facebook](#) [Twitter](#)

PROFILE **MY LINKS**

ANON ALI

CONTENT CREATOR | GREY HAT HACKER, INTERNET

AnOn Ali - Content Creator | YouTuber | Grey Hat Hacker

ANON ALI'S BIO:

-Skills- AnOn Ali Is A- Hacker Video Editor Graphics Designer Article Writer -Introduction- AnOn Ali Is Mostly Known For Posting Hacking Tutorials On His YouTube Channel And Hacking Articles On His Blogger Blog. The Introduction He Has Given on His Website Is: * Introduction: Look Around, Technology Is All Around Us. We Use It In Every Aspects Of Our Lives. It Enables Us To Do Fascinating And Unbelievable Things! But What If We Could Go Further? What If We Have The Ability And Power To Control And Hack The World Using Laptops On Our Laps And Mobiles In Our Palms. I'm AnOn Ali [A Gray Hat Hacker] From Pakistan, Teaching You How To Hack And Crack Into Codes And Passwords To Compromise Computer Security To Perform Powerful Actions And Activities. These Activities May Be Ethical Or Un-Ethical, I'm Just Creating A Society Full Of Hackers. Nobody Has Seen His Full Face Till Now Because He Wears A Mask To Hide His Face While Making Videos. He Has Also Given A Reason Behind It Which Is: "A lot of people ask me why I wear a mask. The mask is

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

AnOn Ali

Description
// Mask the identity, unleash the power.

Links

- [Instagram](#) instagram.com/an0n.ali
- [Uncensored Content](#) odysee.com/@an0n.ali:8

More info

- an0n@an0n.network
- www.youtube.com/@an0n_ali
- United States
- Joined Jun 28, 2023
- 209K subscribers
- 43 videos

Home **Videos** **Shorts**

// HACKING FUNDAMENTALS
Everything you need to begin your hacking journey.

NETWORK BASICS FOR HACKERS
6:05

What are PROTOCOLS? (In 10:15 **HACK Radio Devices! (SDR** 6:49 **Payloads? Shells? Exploits?** 7:46 **Introduction to WEBSITE**

The channel has Twitter, and Facebook presence as well.

Part C: Behavioral Analysis

Is the content educational or 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:

A screenshot of a YouTube video page. The main video thumbnail on the right is titled "LEARN HACKING 2025 - a Practical Guide" by CyberFlow, with 282K views. Below it are several recommended video thumbnails, each with a title, creator, and view count. On the left, a red box highlights a portion of the comment section. The comments are as follows:

- @AaronFord-7q 5 days ago: How about ring cameras can you give us insights on that
- @theRogMick 5 months ago: Can you tell me what voice changer you use?
- @aspirant-uy8lv 6 months ago: Hey Ali, I recently started watching your videos. Though they all are very great but I'm still confused as to where to start. Can you pls give a step by step guide on from where and how should I start learning hacking so that I can start doing bug bounties asap. Plsss reply ❤️
- @nojoys 6 months ago: how about cyber security? do you think its become future job. I'm already interested and do you recommend i study in university to cybersecurity
- @archangel5723 5 months ago: A hacker is someone with resources , you have to develop a specific mindset to find answers in the unknown.
- A locksmith won't find knew ways to open a door if he doesn't know how the lock works to begin with.
- @WebDeveloperAgent1 3 months ago

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.