**Assignment 02**

**Reconnaissance**

**CS4061**

**Ethical Hacking Concepts and Practices**

**Submitted by:** Faizan Pervaz

**Roll number:** 20I-0565.

**Date:** 17-02-2024

**Table of Contents**

[ **Introduction** 3](#_Toc143364655)

[ **Steps** 3](#_Toc143364656)

[ **Summary** 21](#_Toc143364657)

[ **References** 22](#_Toc143364658)

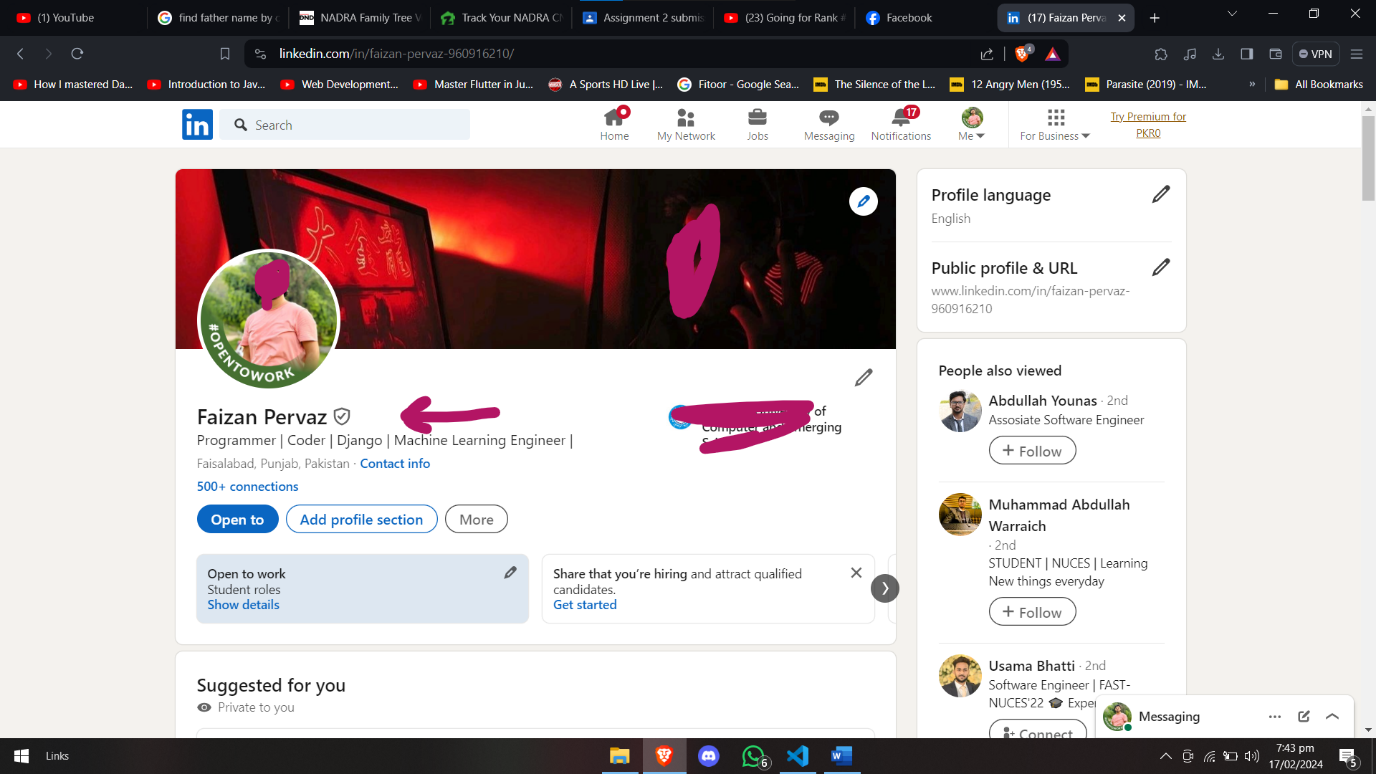
# **Introduction**

# For this assignment, we need to start with the first step of the cyber kill chain, which is reconnaissance, and we'll be focusing on gathering information about our own systems. There are 17 specific pieces of information we're tasked with uncovering, and it's crucial that we gather all of them during the reconnaissance process.

# **Steps**

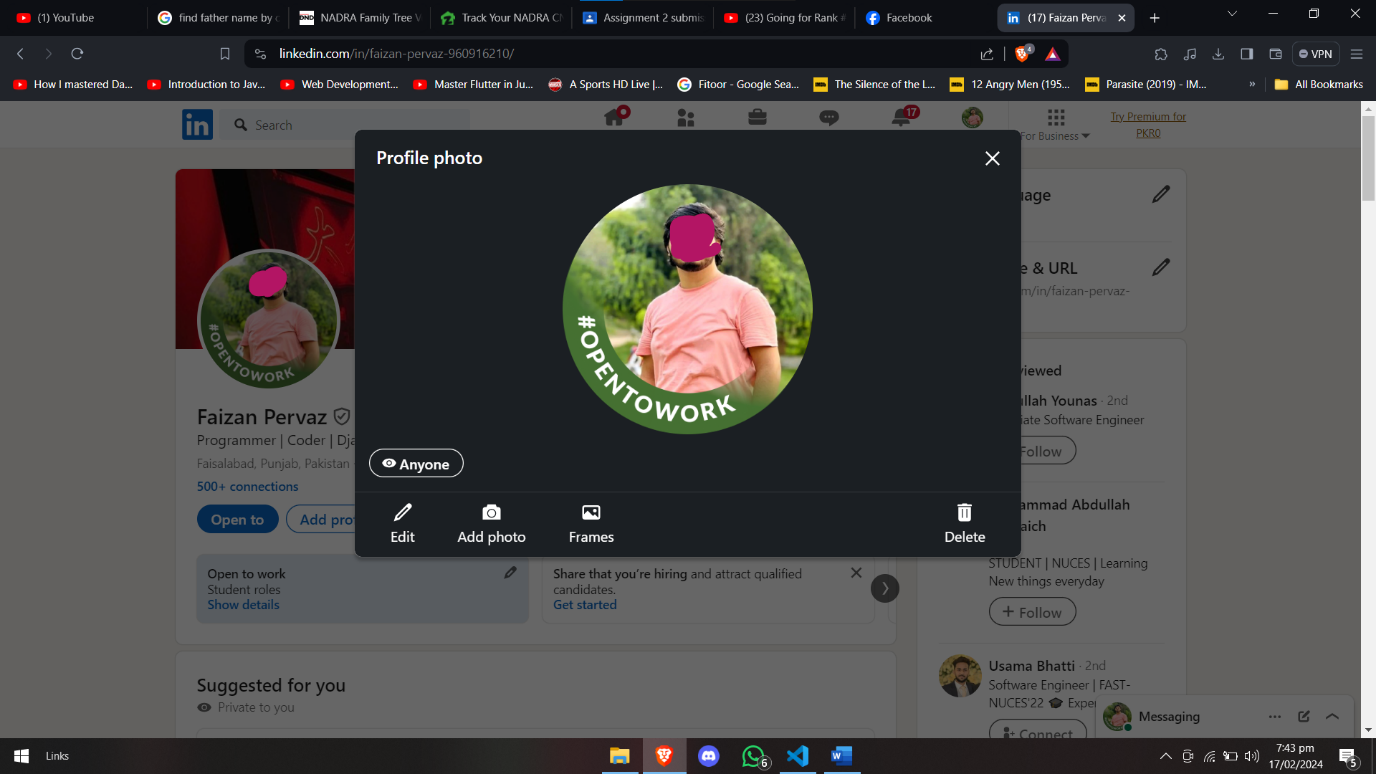
1. **Full Name:**

Initially, we must find the full name of the person. LinkedIn is an optimal platform for this kind of service, as compared to other media platforms such as Instagram or Facebook where people use Nicknames or short names. As LinkedIn is recognized as professional social platforms where people use their authentic names. Hence it is a reliable source for obtaining full names accurately.



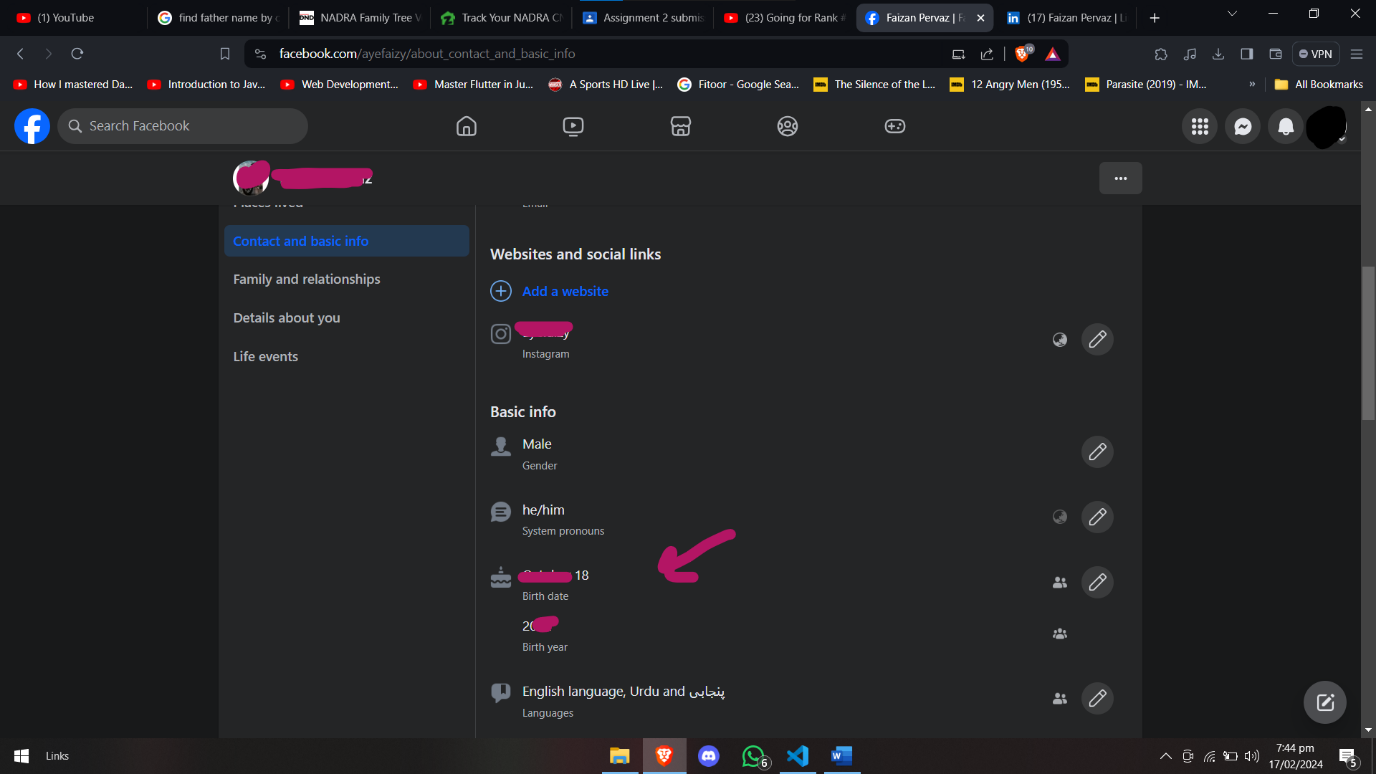
1. **Picture:**

For the picture, we found it on the LinkedIn profile easily, also we observe that that the picture on the LinkedIn should be accurate as LinkedIn is recognized as a leading professional social networking platform where users typically employ their authentic pictures too. Therefore, it presents a reliable option for obtaining accurate pictures.



1. **Date of Birth:**

When seeking the date of birth, social media platforms, particularly Facebook, can be instrumental. Individuals commonly display their date of birth on Facebook profiles, rendering it a viable source for extracting this information.



1. Place of Birth:

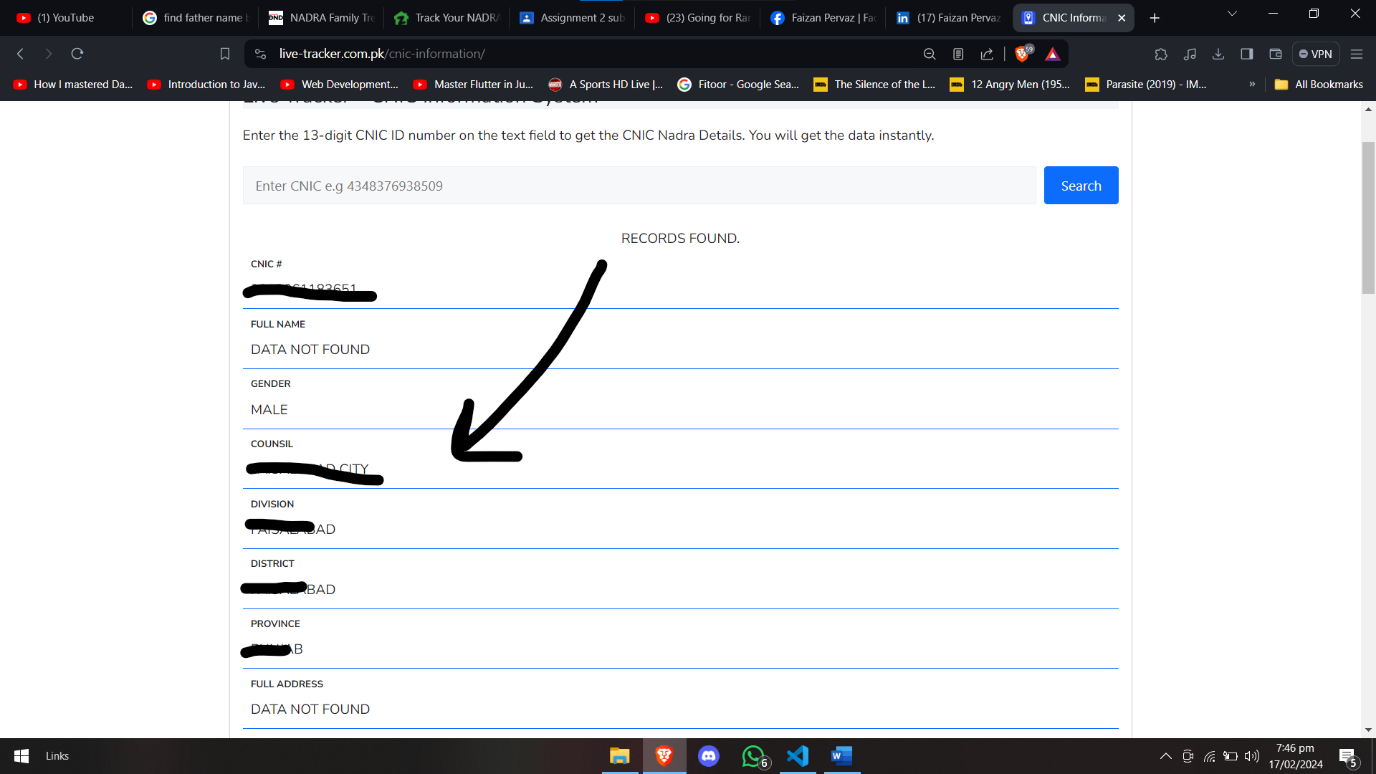
We cannot find such information easily through individual’s social media platforms as mentioned earlier because that only tells where do they belong but that doesn’t mean that, were they were born there.

Hence, for this purpose CNIC, which is identity card plays major role.

As shown in example below, it tells information about province, gender, tehsil, and district, etc. As, this CNIC is basically b-form of a child which is registered and created where a child is born.



There is a website <https://live-tracker.com.pk/cnic-information/> through which if you enter the 13 digit CNIC number You will get the CNIC details of Counsil, District, Division, Province, etc. from where you can find the information that where was the place of birth of this individual.



1. Family Information:

If an individual sends his CNIC number to 7000 then CNIC holder and his father name is received in that response, through that we can find about the information of family.

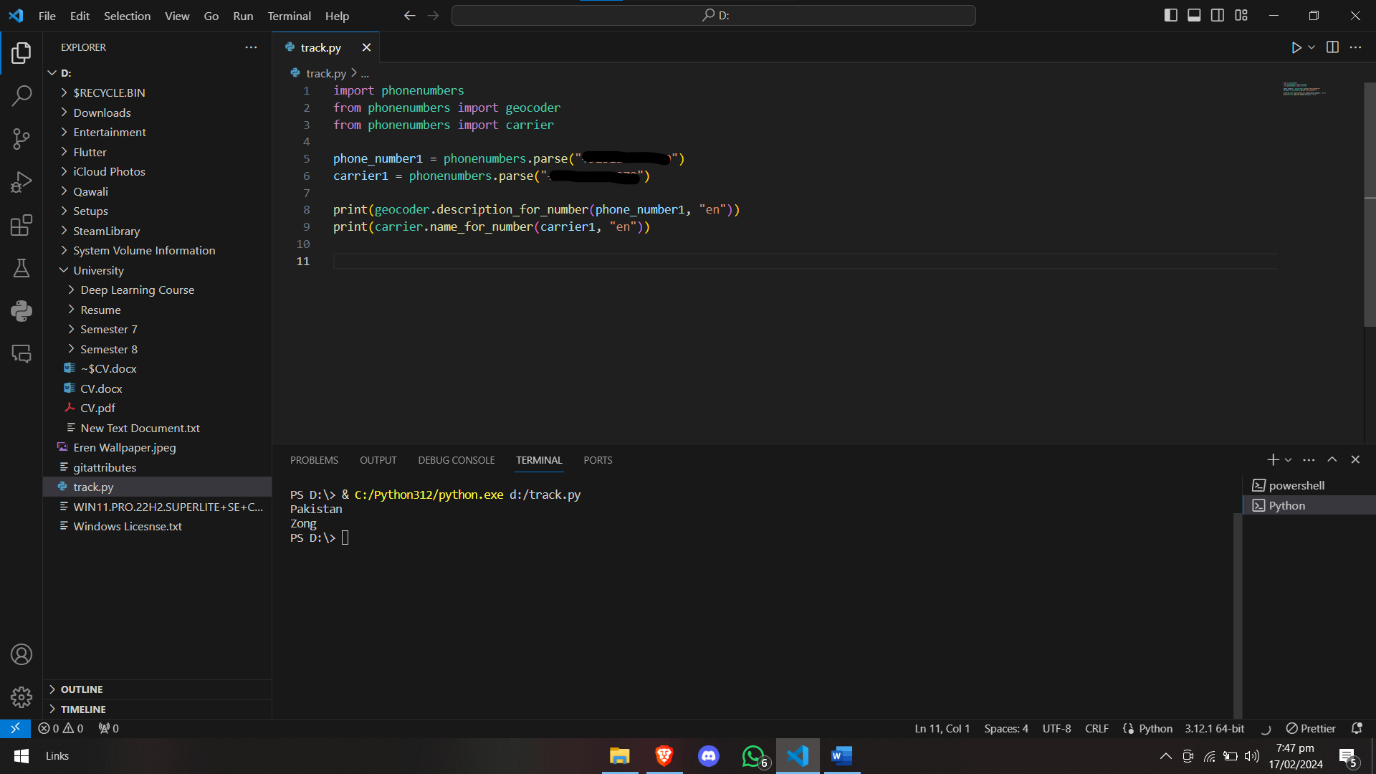
1. **Permanent And Temporary Address:**

If an individual sends his CNIC number to 8300, one can get the information of the election polling station mainly where one needs to cast his vote, which gives the election address based on permanent address of his CNIC.

From that, you can get an idea of his permanent address.



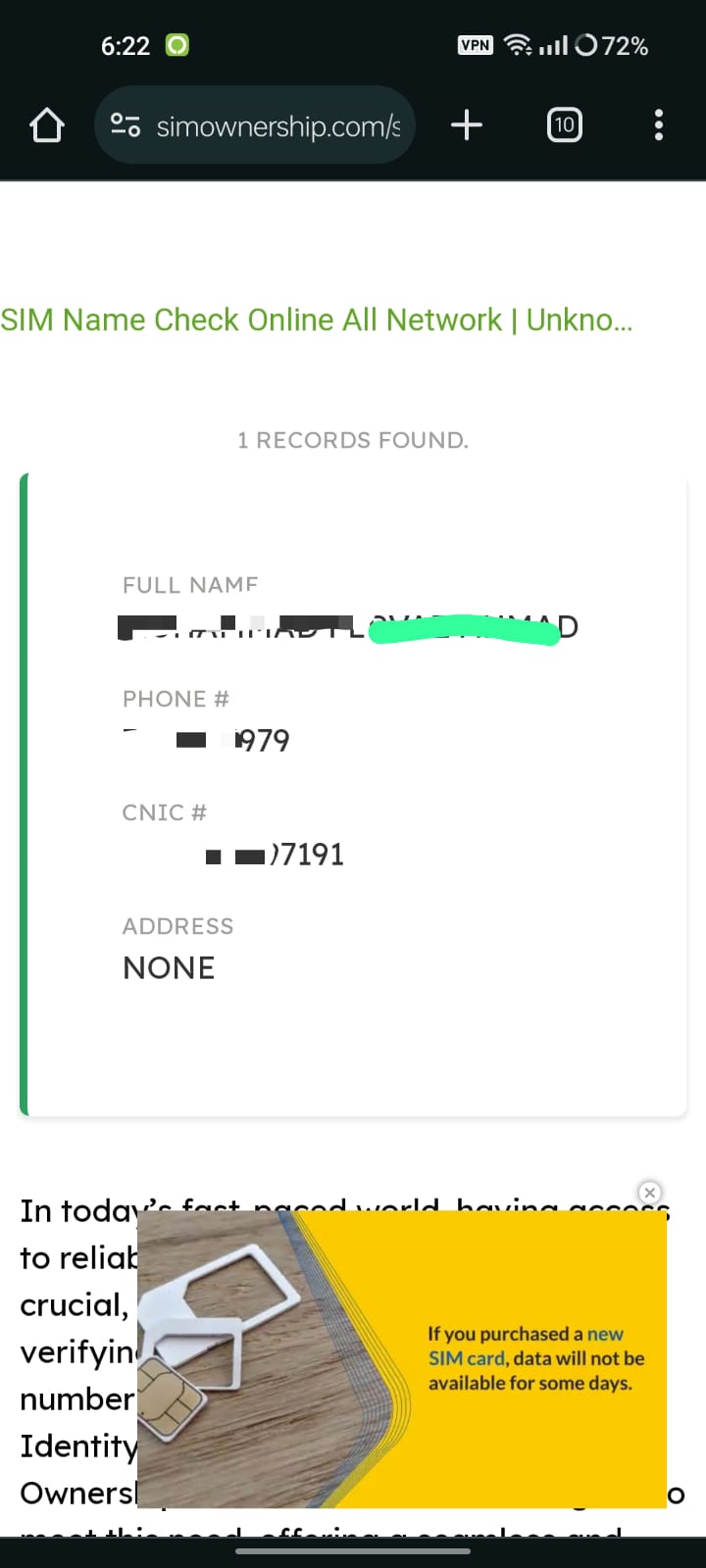
Also, I have written a python script which tells about the sim location as well as the carrier.



1. **Phone Number (SIM Records):**

There is a website name simownership.com which can be used to find the sim records phone numbers which are registered on your CNIC number. You just must input CNIC number and then sim records will be shown.

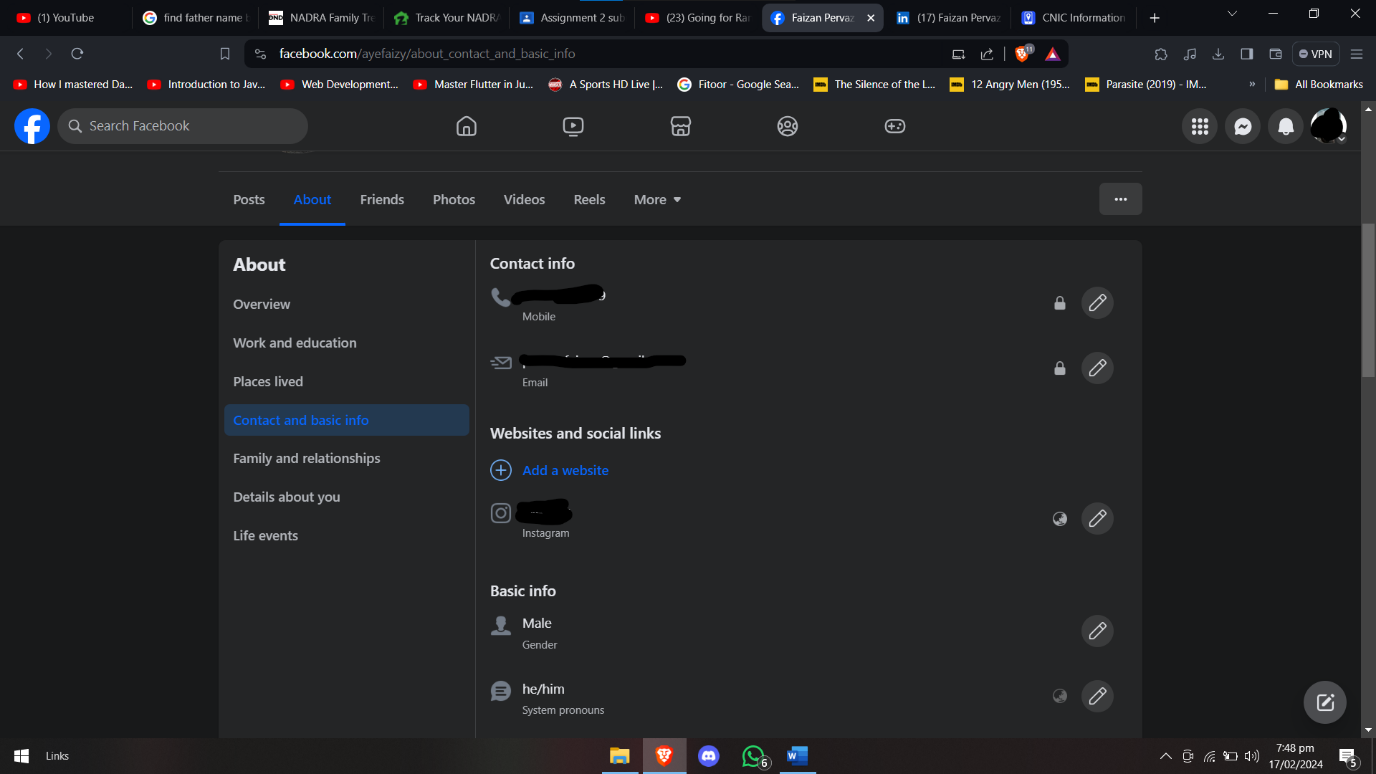
simownership.com can be used to find the information about the sim records phone numbers which are registered against the CNIC number. Someone just has to add his CNIC 13 digits to find out about the phone number.

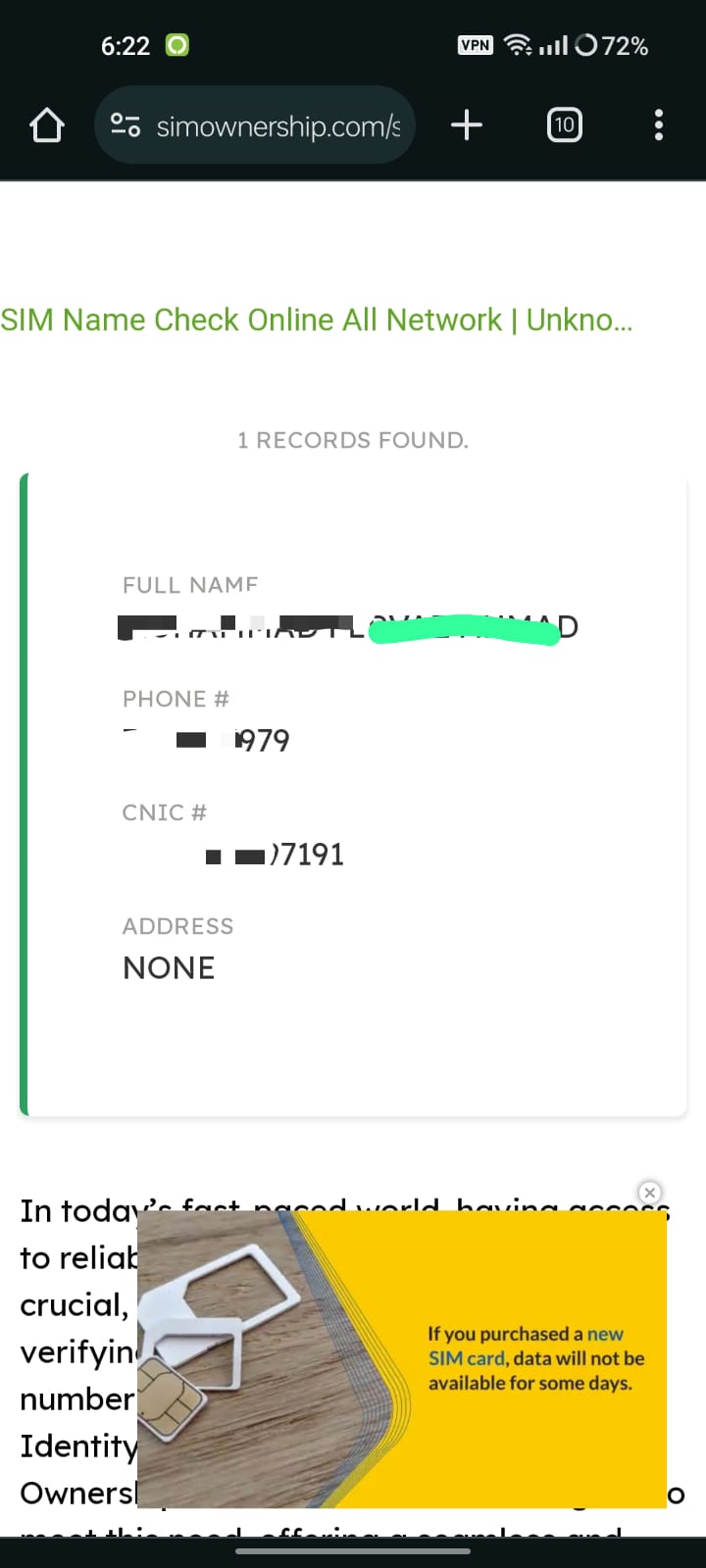


1. **CNIC:**

Similarly, CNIC number also can be found using just the phone number.

simownership.com can be used to find the information about the CNIC number which are registered against the phone number. Someone has just to add his phone number to get the CNIC number.





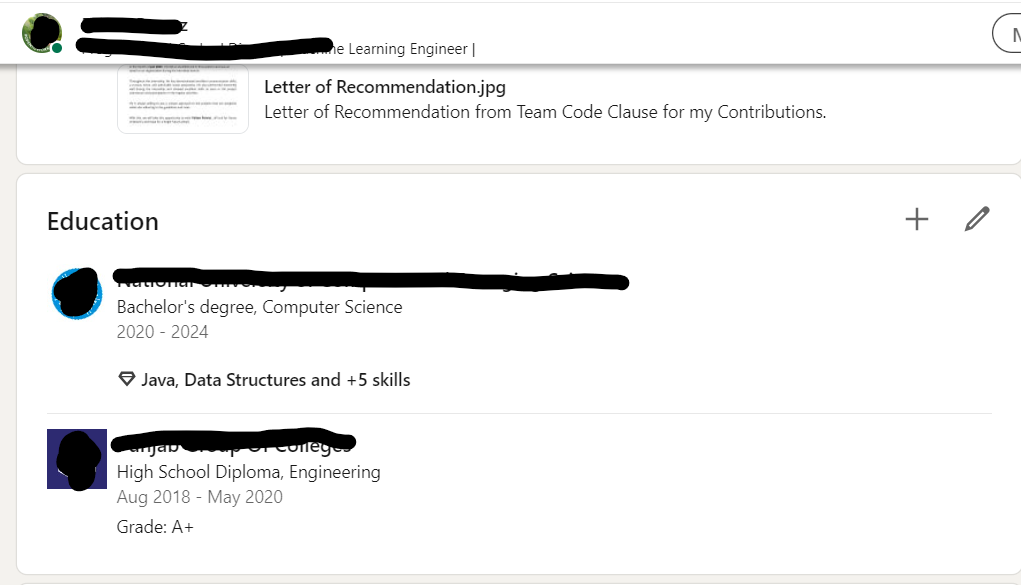
1. Passport and Driving License**:**

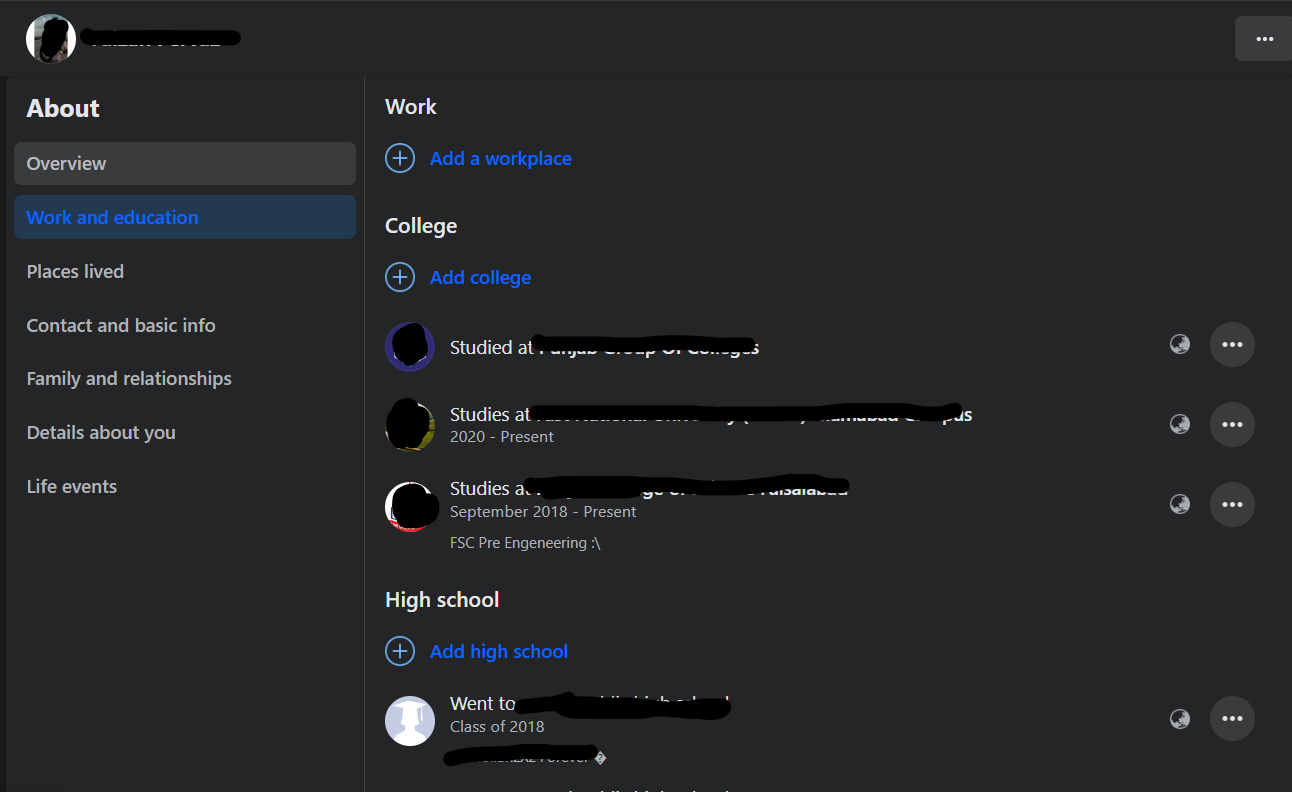
NOT FOUND

1. **EDUCATION RECORDS:**

Using Facebook and LinkedIn, we can find the educational records easily.

For this, I used both Facebook and LinkedIn.





1. Medical Records:

NOT Found

1. Bank Accounts:

Not Found

1. **Device Information:**

Finding device information is very challenging. Through social media, it is very difficult to find which devices the person is using unless we do an attempt to attack him electronically. Through his social media pictures, we can observe that in his previous pictures he was using some LG phone, can be LG G6

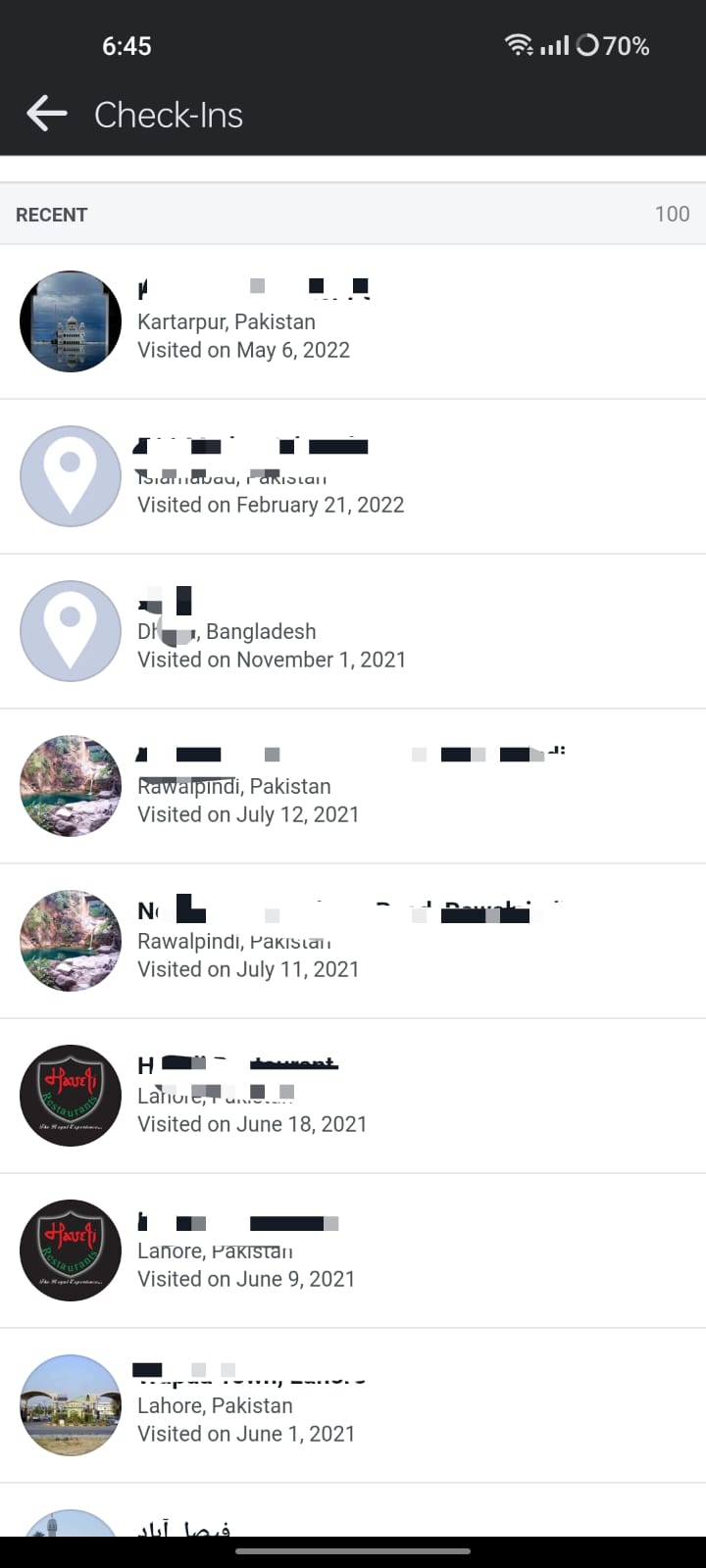


But his last recent year post shows he is using OnePlus brand mobile, from seeing it looking like OnePlus 8, I cannot find any photo of him with his laptop.



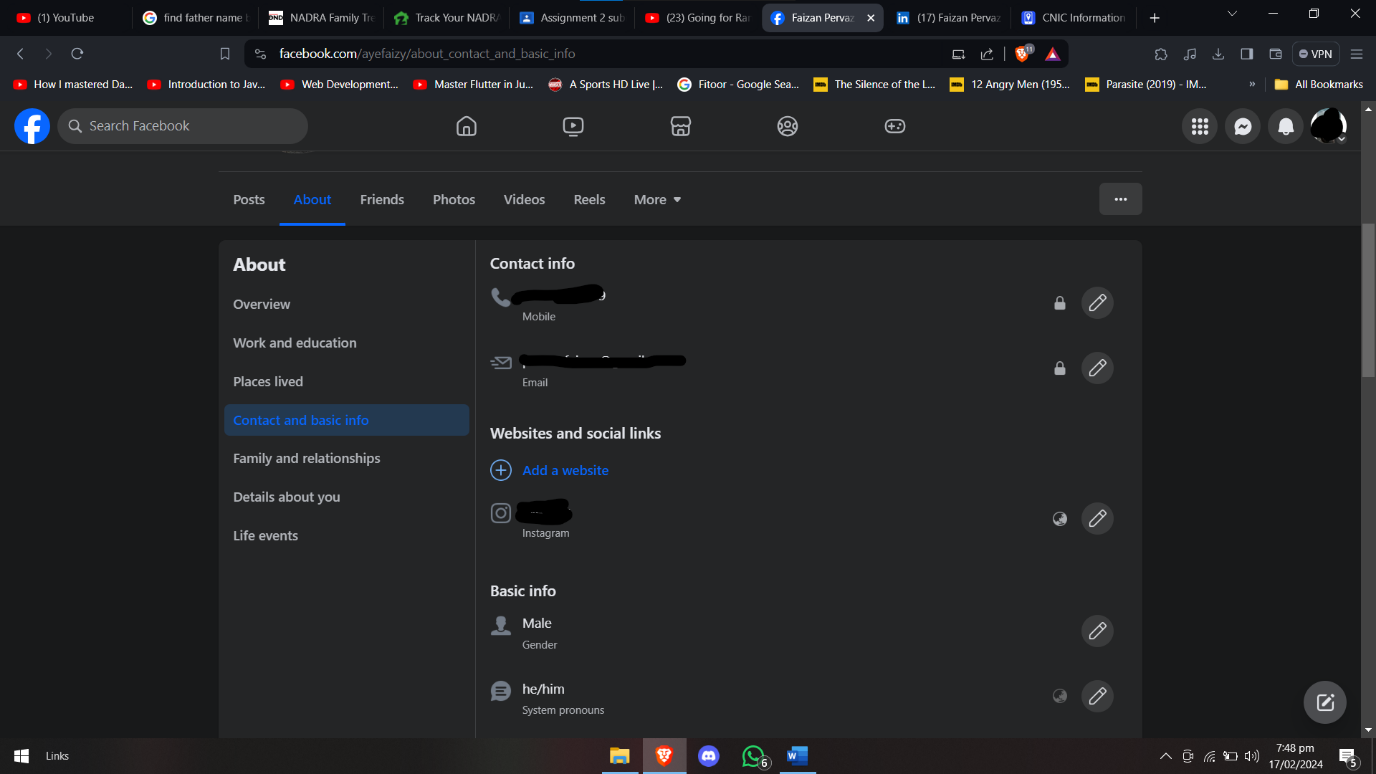
1. **Geographical Information:**

For this type of info social media sites are the best option. I used Facebook for this information. The life events only included the educational history.



1. **Email Accounts:**

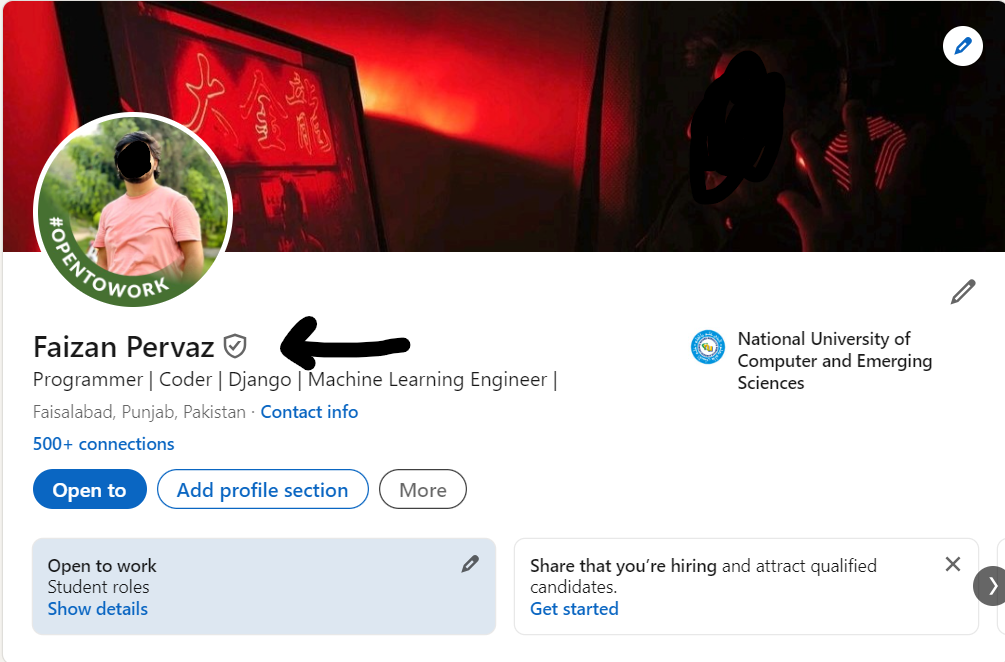
For extracting email information, I used Facebook, a social media account, as people will be using their email addresses with that.



1. **All Social Media Accounts:**

All available social media accounts are shown below.

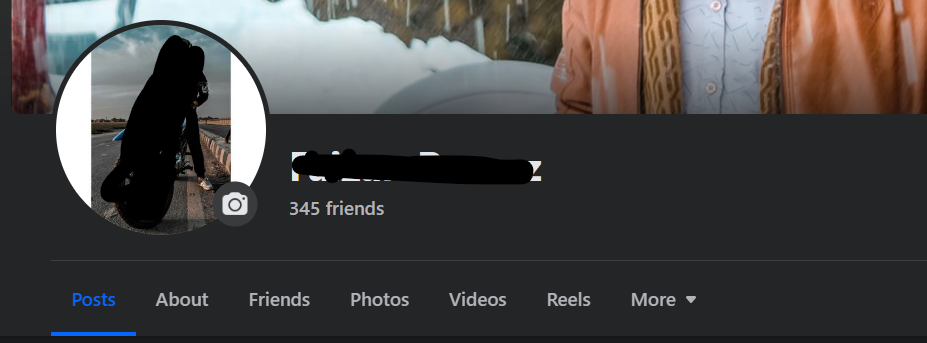
1. LinkedIn



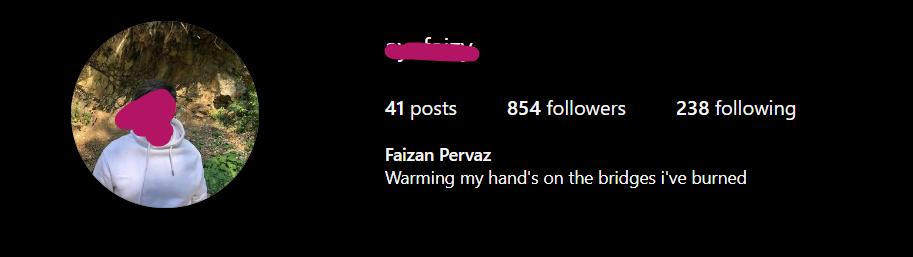
1. Twitter:



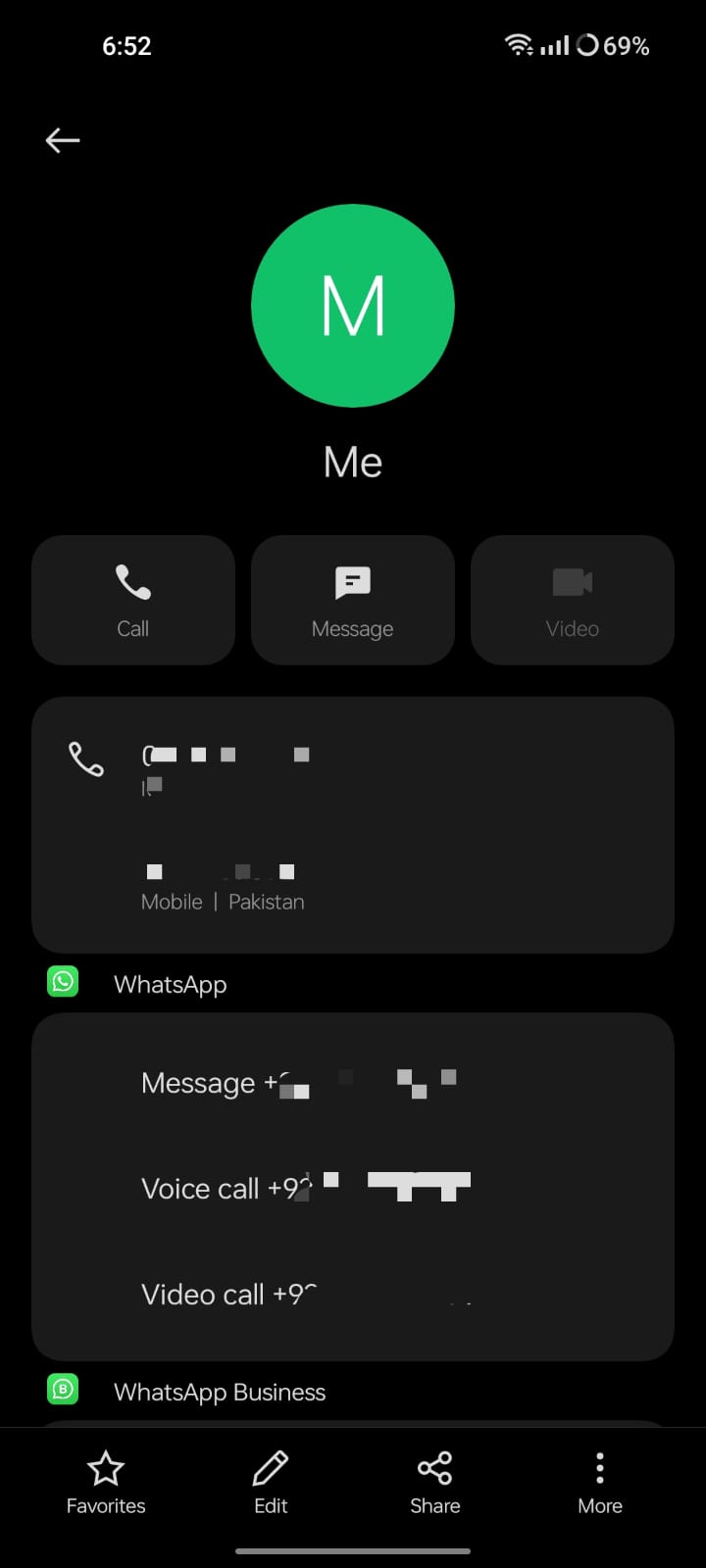
1. Facebook:



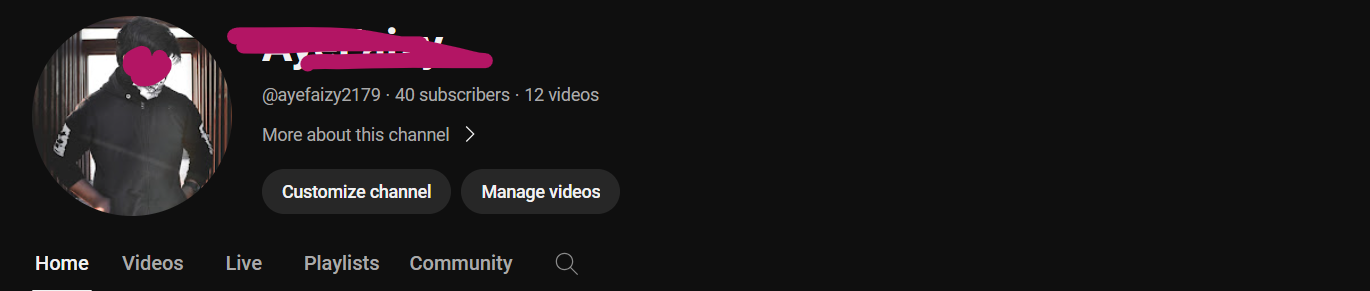
1. Instagram:



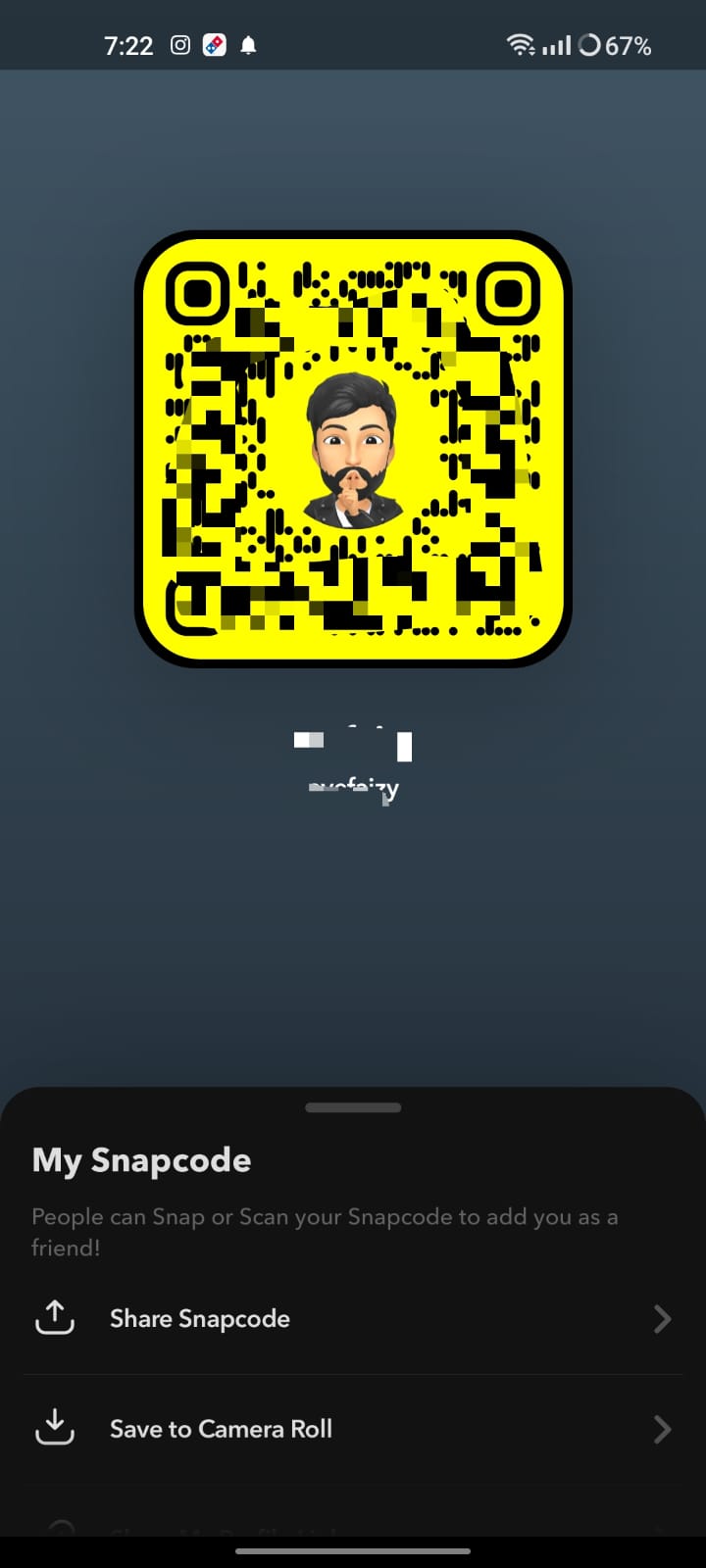
1. WhatsApp:



1. YouTube:

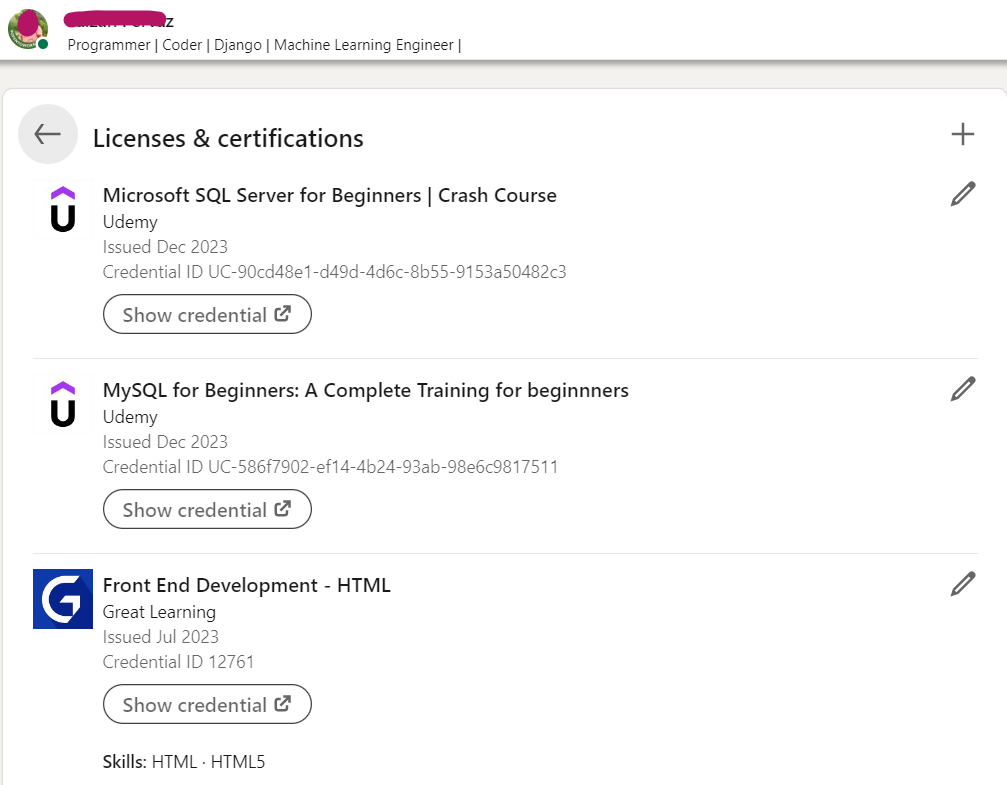


1. Snapchat



1. **Awards and Achievements:**

To get that kind of information, LinkedIn is the best source, The tab for awards and honors was not there but some information regarding achievements of certifications and licenses were available.



# **Summary**

Before obtaining the information listed above, we need to complete the reconnaissance step of the cyber kill chain. Each piece of information represents a step in this process, and it's important to understand how and where each of these details can be extracted.

# **References**

1. <https://simownership.com/>
2. https://www.linkedin.com/in/faizan-pervaz-960916210/
3. <https://www.facebook.com/ayefaizy/>
4. <https://www.instagram.com/ayefaizy/>
5. https://live-tracker.com.pk/cnic-information/
6. <https://twitter.com/ayefaizy1>
7. <https://www.youtube.com/channel/UCyawrkBr_V26sA2t6R3yWTA>