MIDTERM PROJECT REPORT

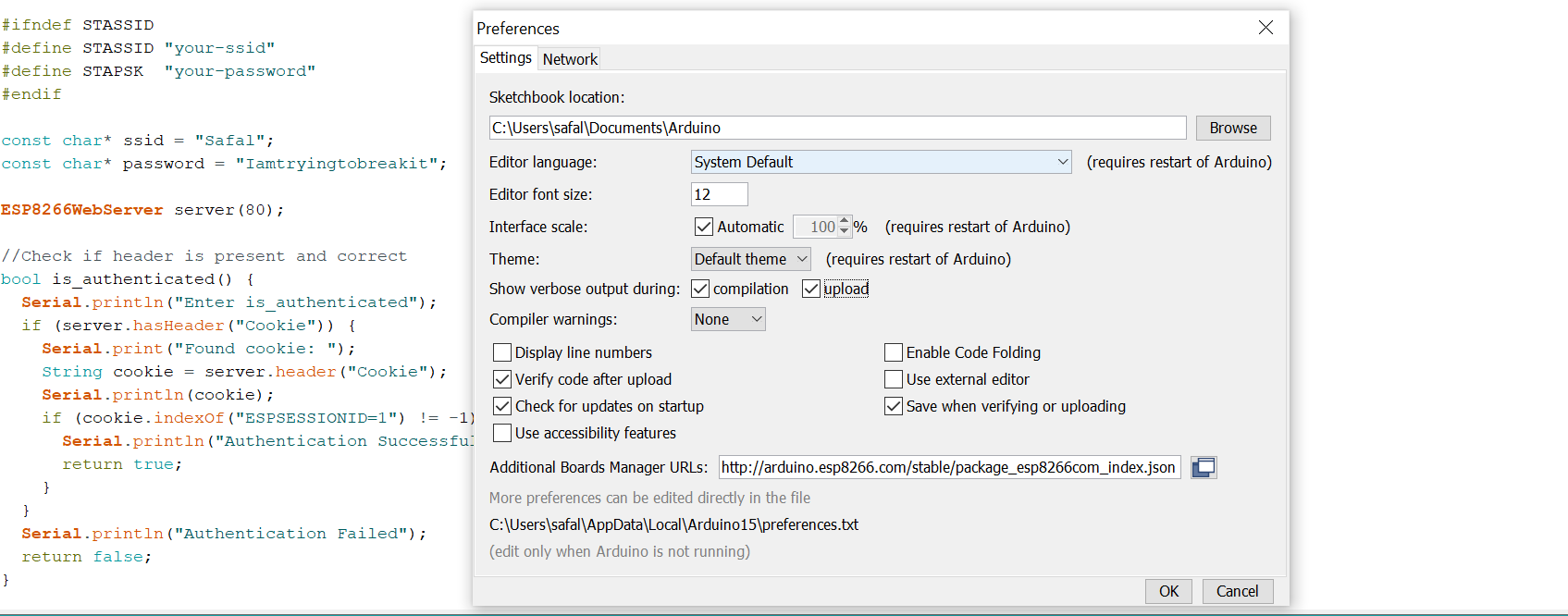
TO: Dr.Li

Steps:

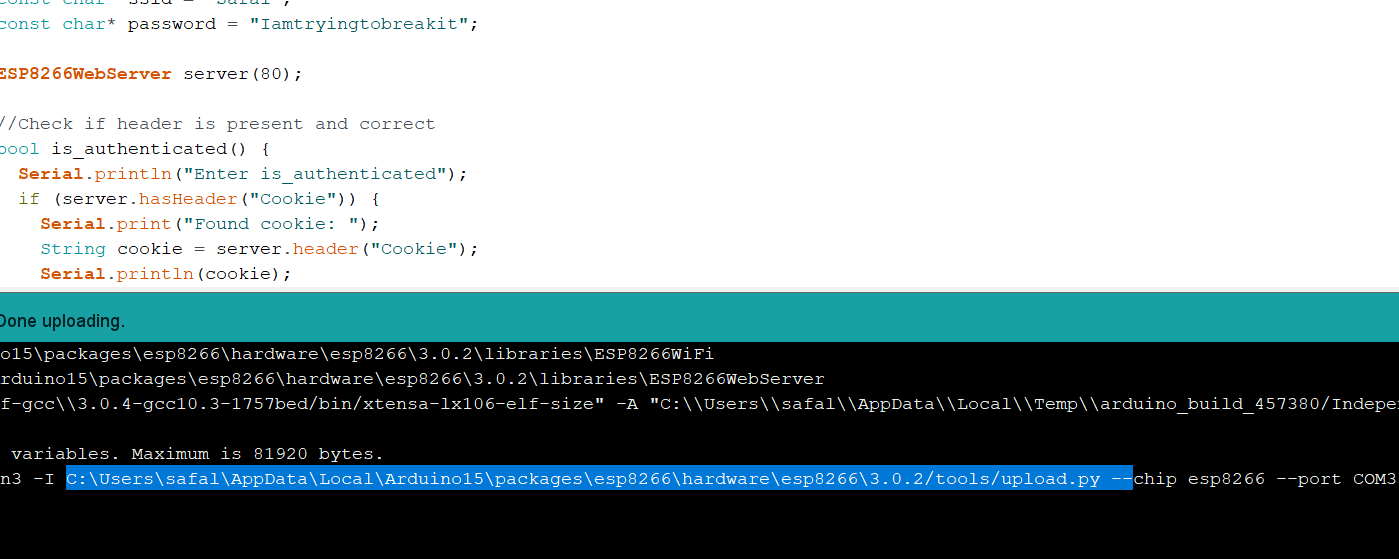
Step 1:

Get the binary code to exploit the physical interface

* Goto Arduino IDE – file – preference, check on ‘show verbose output during’ while compiling and upload options



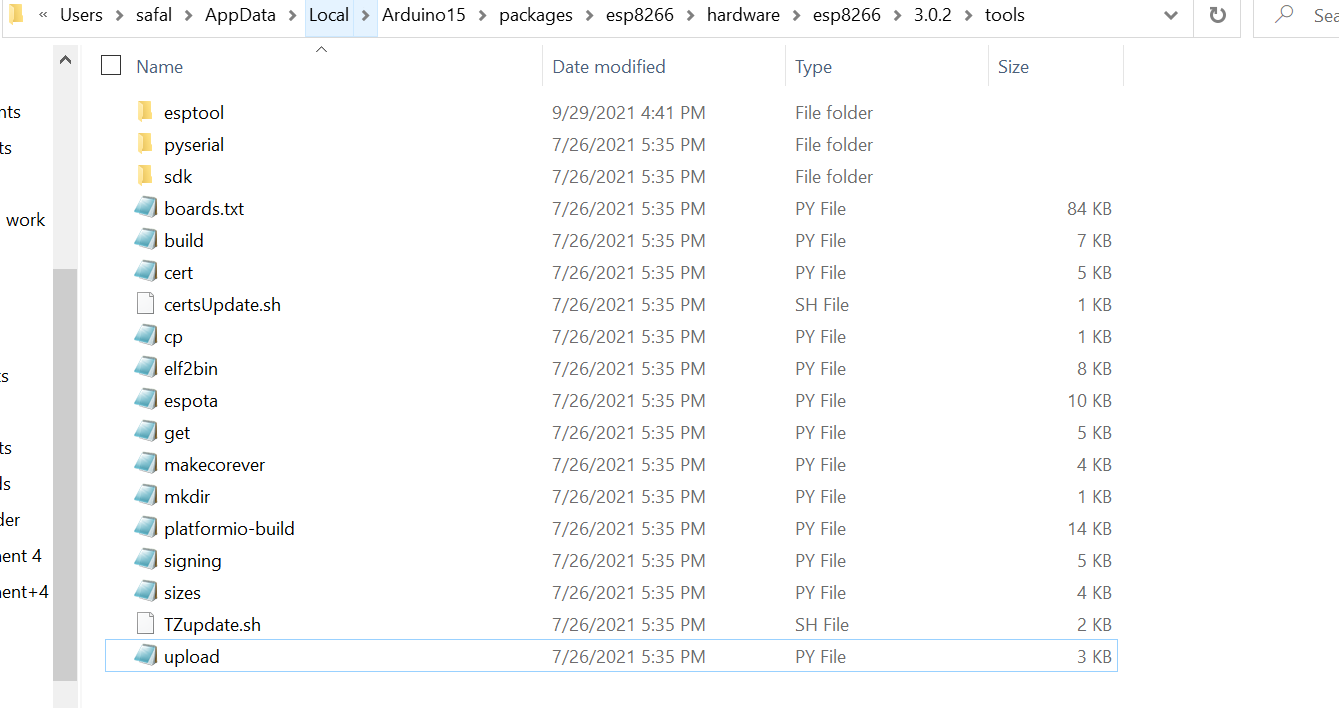
* Compile and upload our program to check the tools that are called when they were installed to trace and perform attack



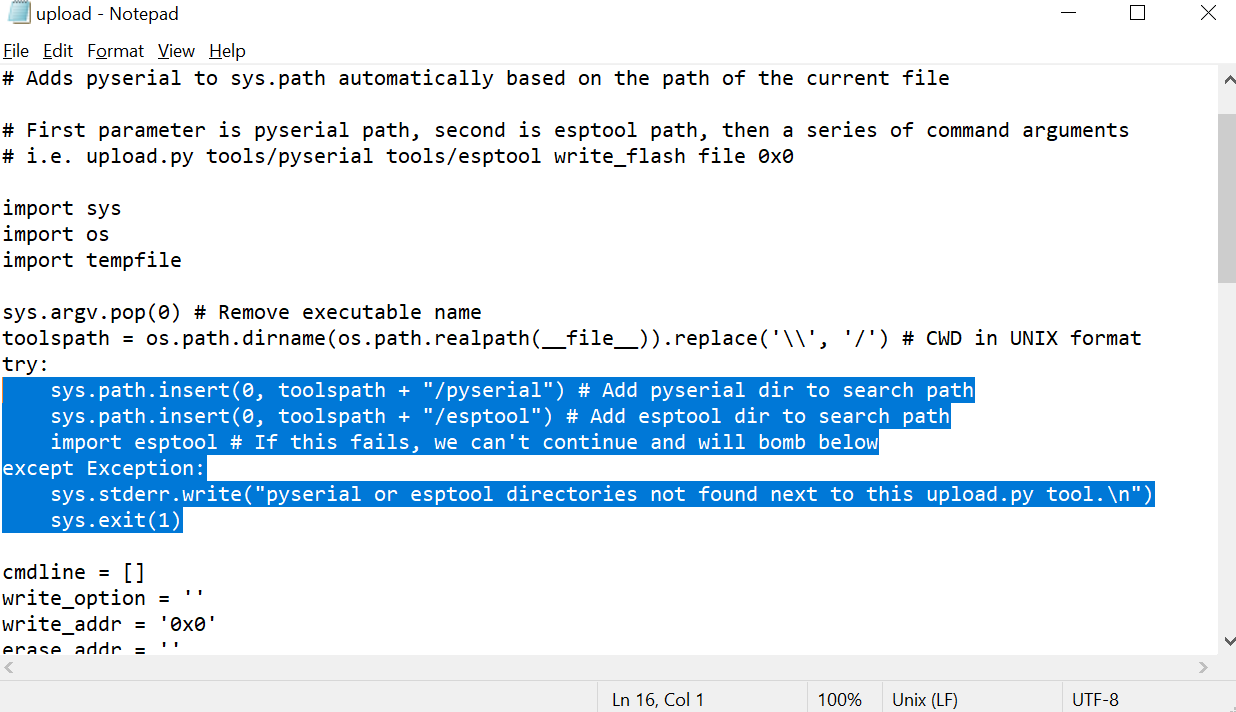
SSID- Safal

Password – Iamtryingtobreakit

* Goto upload.py source file

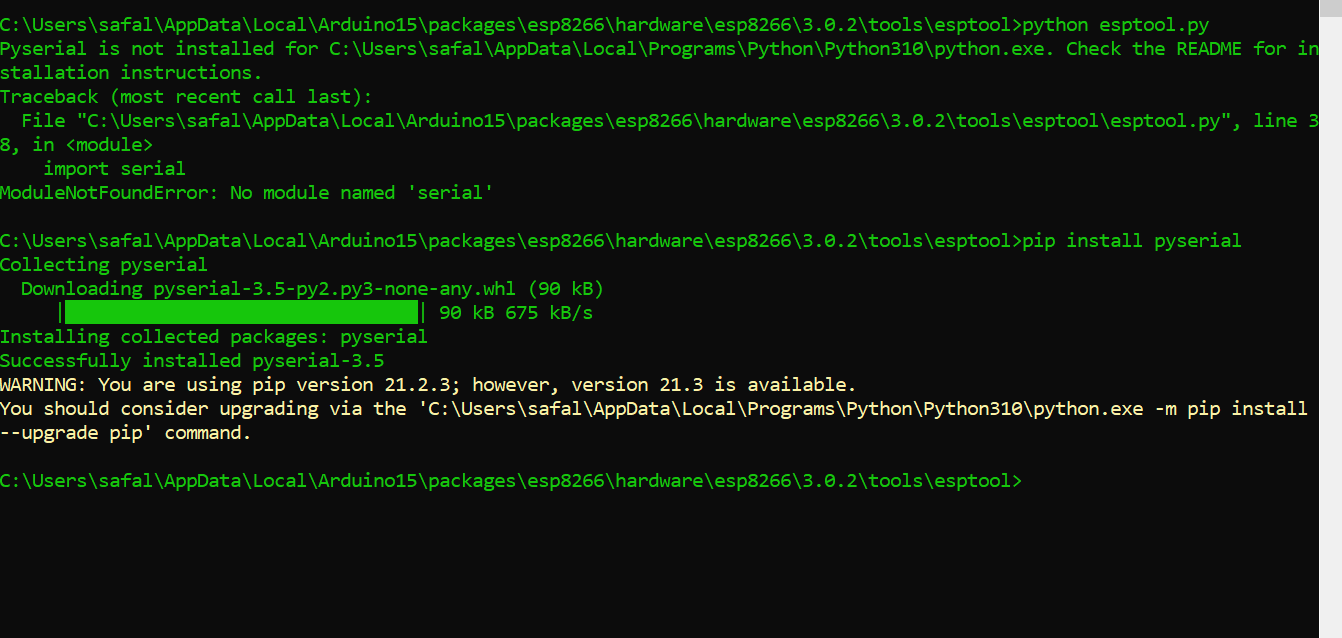


OPEN IT

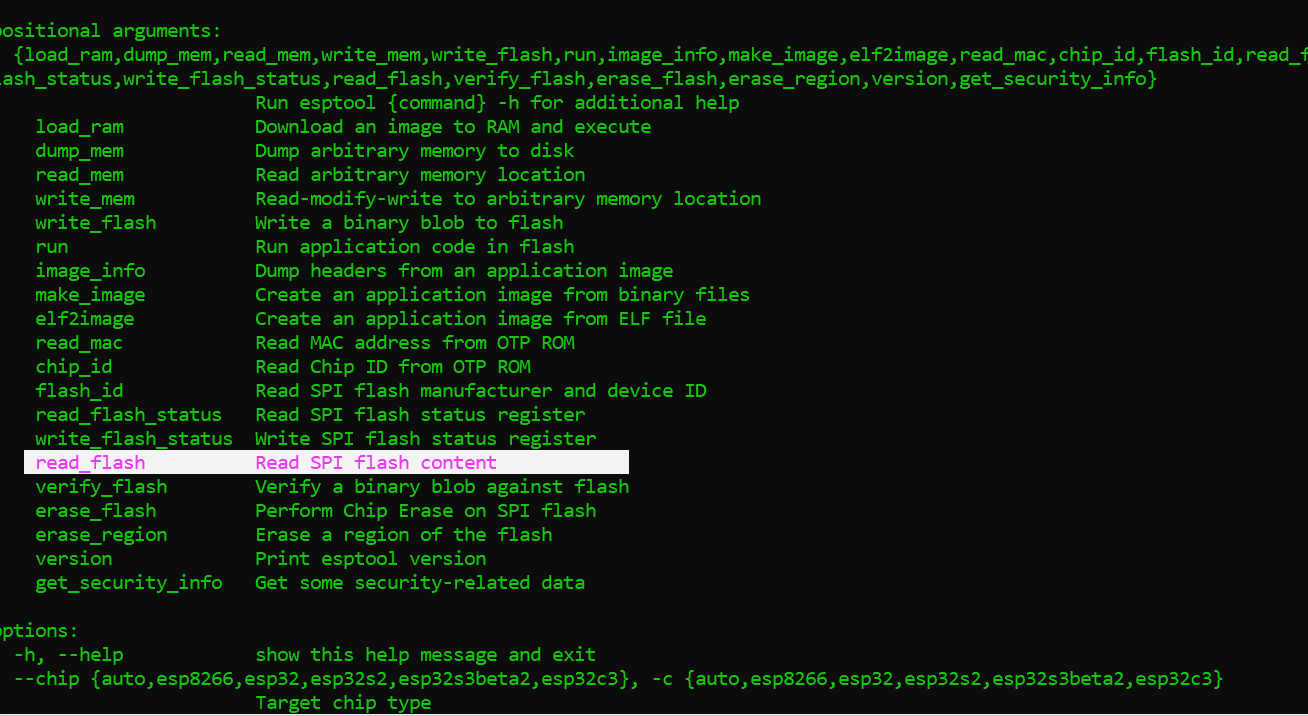


* We can see that the tool is esptool.py

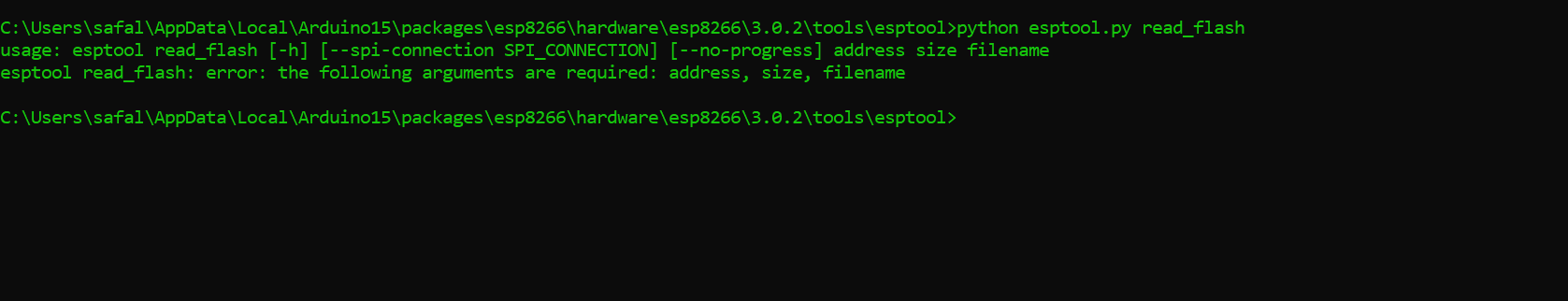
See esptool.py what options does it support.



After Installing package, we can see that read\_flash is used to read the contents

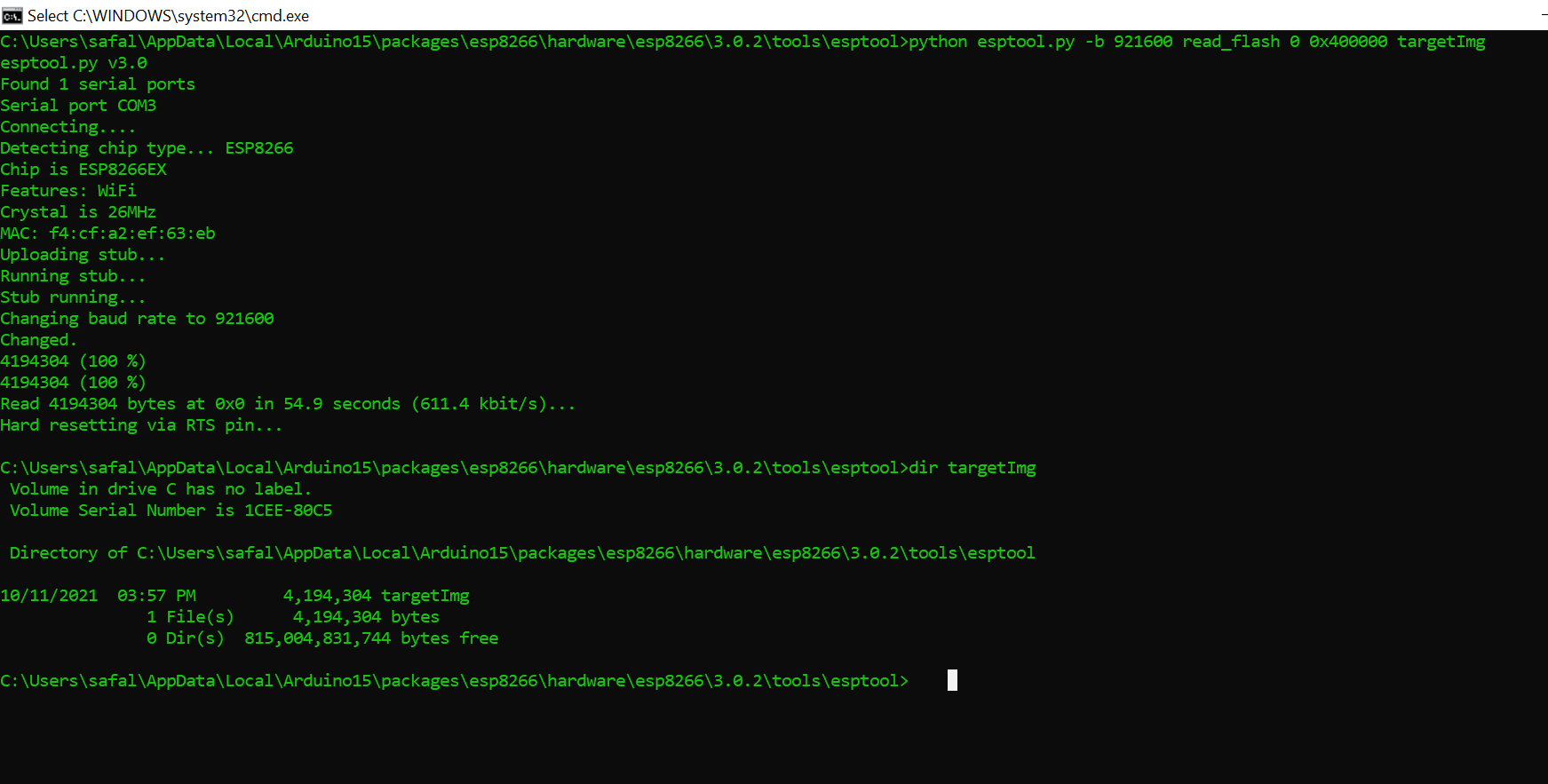


Try read\_flash option to check what does it support

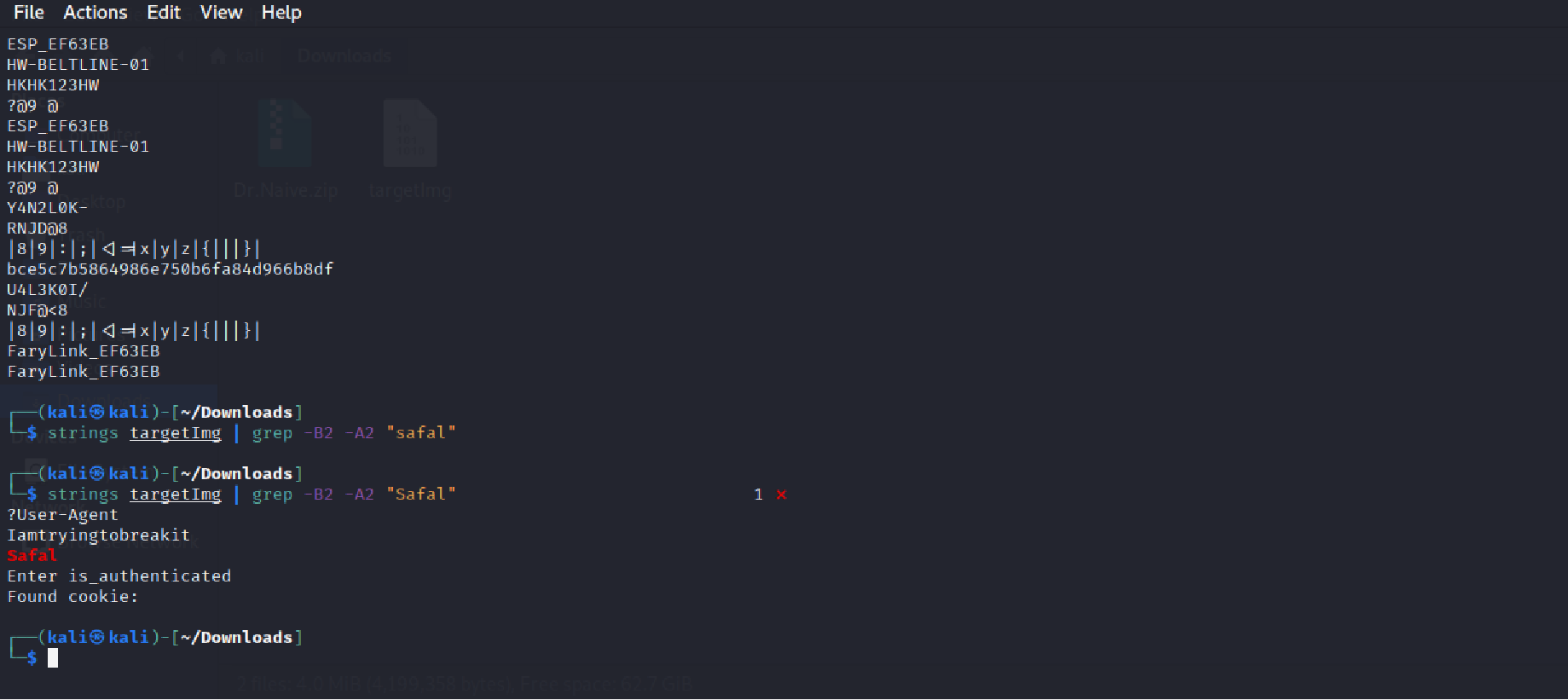


So, first let’s download the binary code from the target and verify the image file

As we know we have used baud rate 921600 and NodeMCU is connected, so download the code using that



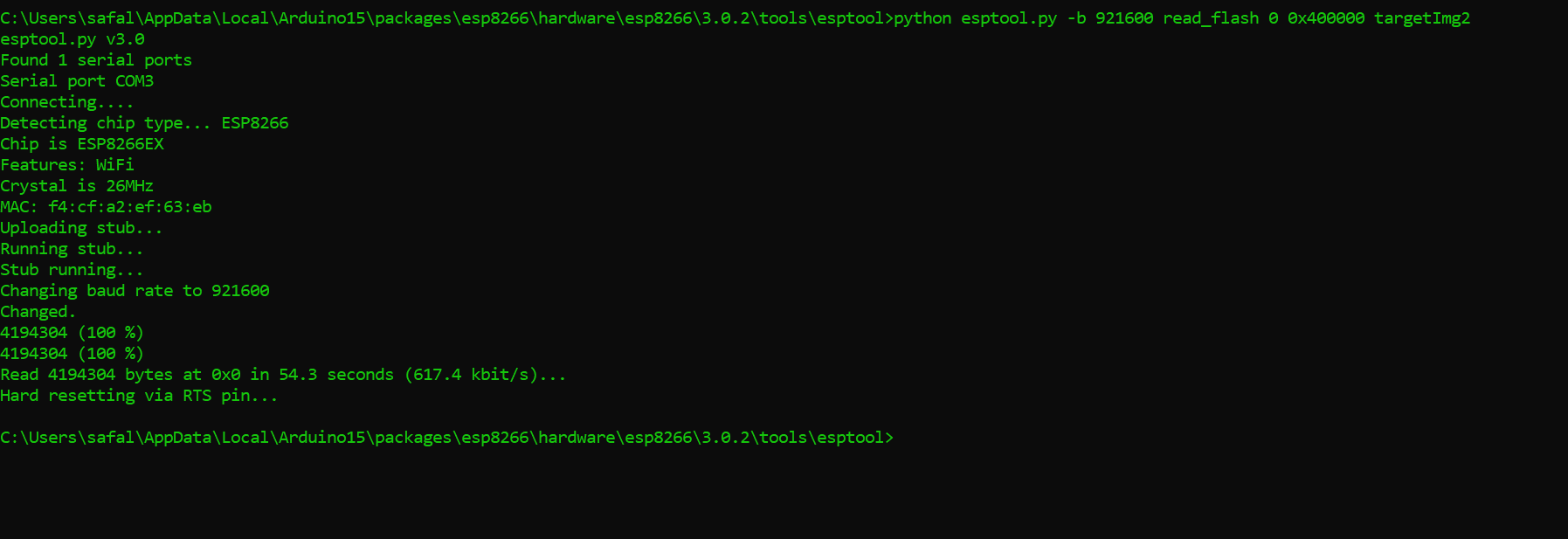
Use Strings Command to analyze the file. CMD doesn’t support so We use Kali Linux. There are too many Strings, so we have used the filtering options BY using greg. We know the username of the network so we the username.

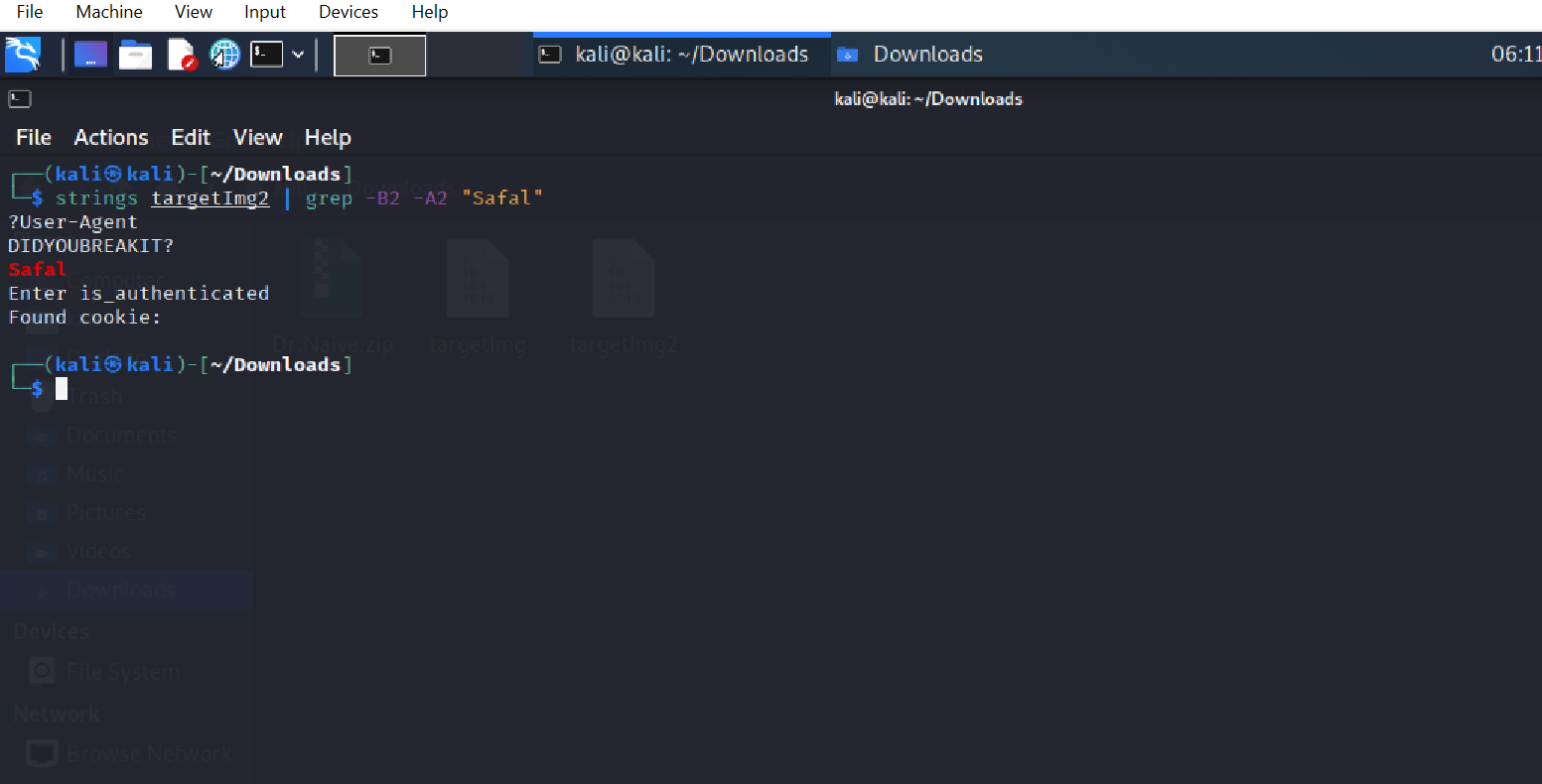


* Now Check if it this works on another PC with the same NodeMCU.
* Let’s change the password and for the SSID and upload the code from another PC.
* Then again, another PC is used to crack to check if it works where there is only device and no PC which was used to upload the source code.

Let’s retrieve the Password now. 😊

Remember to select correct board and port





SO, the password set from another PC was DIDYOUBREAKIT?

CONCLUSION:

We can get the password just by using NODEMCU, read the content in Flash where targetImage is generated.

Thankyou!!