

**Politecnico di Milano**

Wireless Internet Project

**Python Scapy Tutorial**

Giuseppe Maria Fiorentino

Professor: Redondi Alessandro Enrico Cesare

**1 - Introduction:**

Scapy is a Python interpreter that enables the user to send,sinff, dissect and forge networks packets. It is possible to say that with this tool you can perform some powerful network attacks, just writing few lines of code. Scapy has become really popular because of its semplicity. For instance, by writing the command to the terminal:

>>>send(IP(dst="192.168.1.1")/ICMP()/"ICMP packet")

We have created an ICMP packet and we have sent it to the IP address 192.168.1.1 just with one line of code. Among all these things, an other reason why Scapy is popular,is that it can sobstitute some networks programs such as: nmap, hping, arpscan, and tshark (the command line of wireshark). There are two ways of using scapy. The first one is more dynamic because the thing to do is to write commands on the “command prompt” and look at what is going to happen. The second way, is to use it in combination with Pycharm. “Scapy” is an extention of the python language, consequently you can create really powerful programms that will show all the potentialities of this tool.

**2 - Technical background**

In order to fully understand the potential of this tool it is necessary a good knowledge about Networks and python programming language. Then you only need a laptop and Wireshark installed on your pc. Even tought the best way to discover “Scapy’s potentialities” is through Ubuntu, in this notes I am going to show them by using the most common operative system: Windows 10.

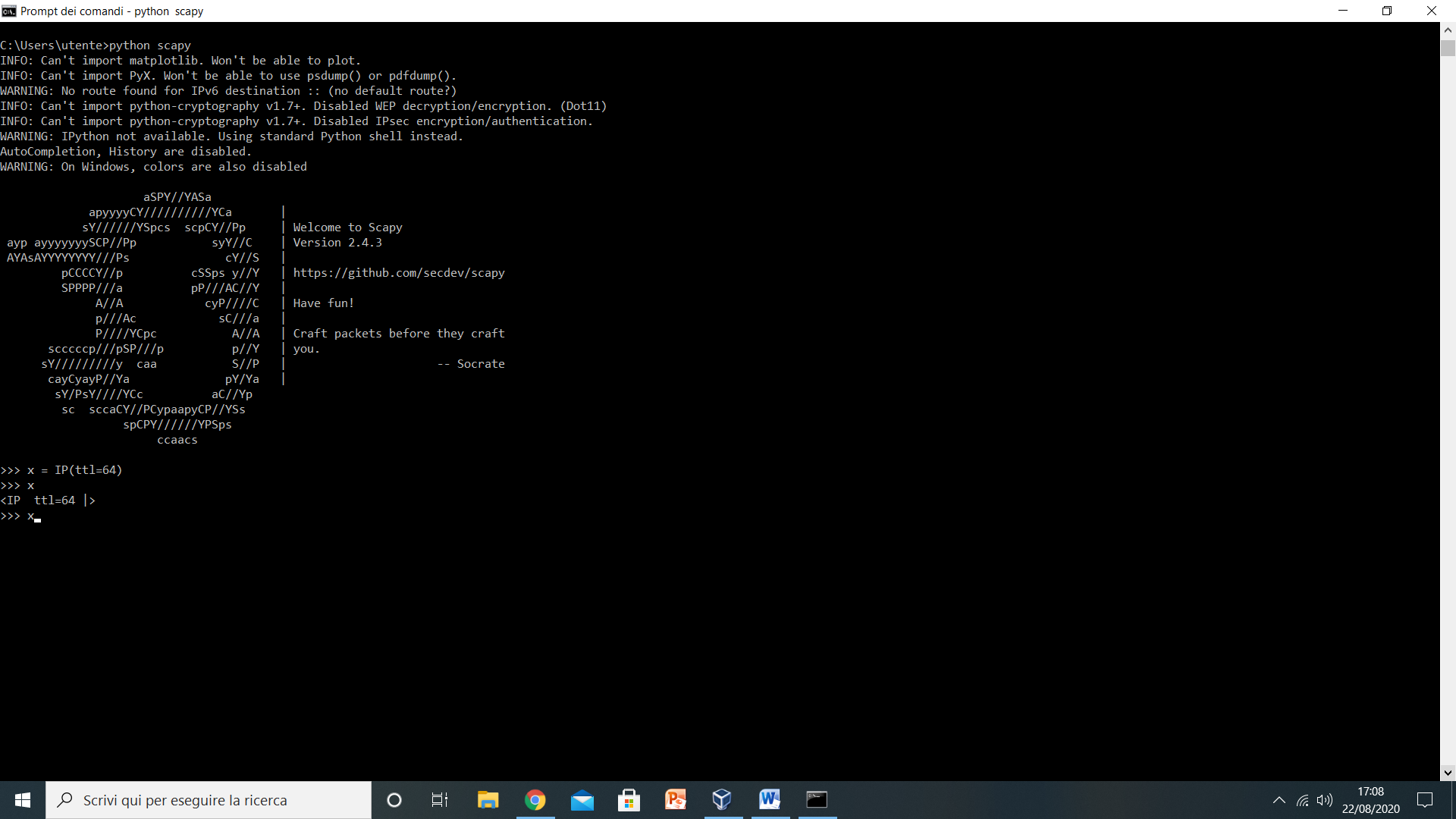
There are basically two steps two follow in order to get Scapy:

1) open the command prompt;

2) write the following statements:

*-pip install scapy* (a command used to install scapy)

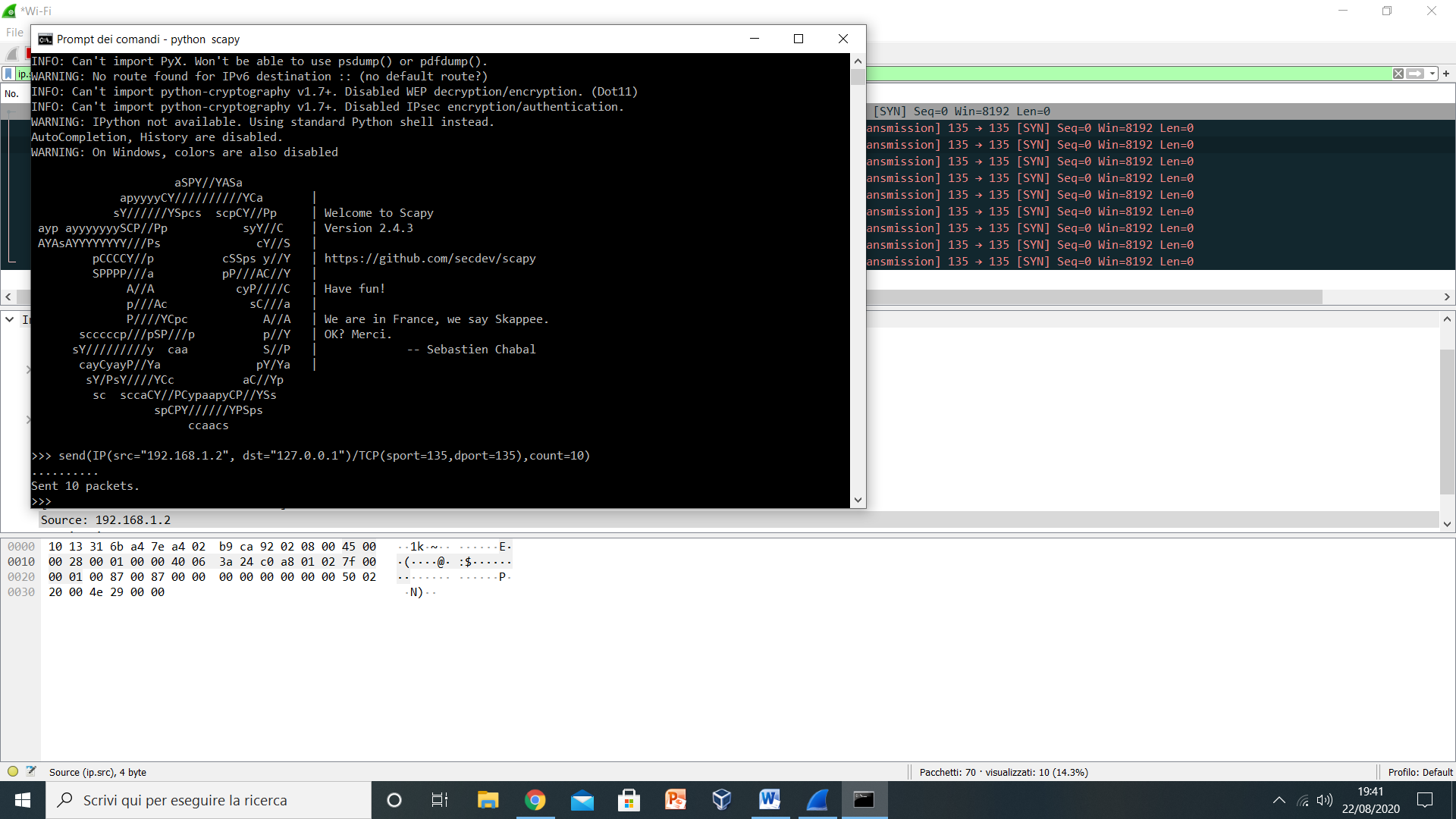
*-python scapy*(a command to launch scapy)



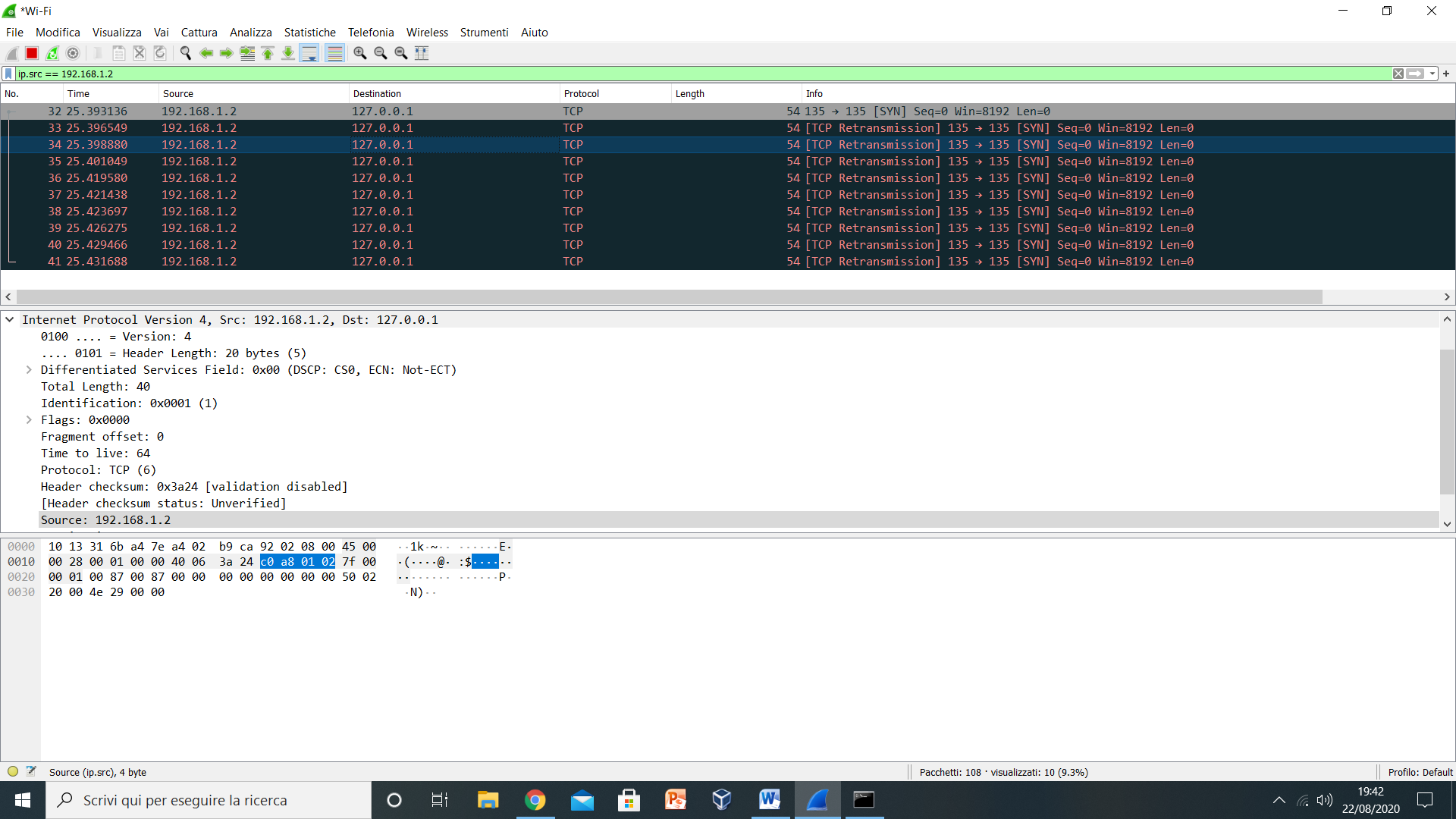
At this point it is possibile to see that Scapy is installed and now we can create and manipulate our packets.The best way to put your hands on scapy is in combination with an other really important tool : ‘Wireshark’ . It is a packet analyzer that will show us with its graphical interface what we are doing with Scapy.

**3 – Introduction to the Scapy Language**

Among all the documentation that can be found on the internet, it is really useful the scapy function : “*lsc()”* . It lists all possible commands that can be used with this powerful tool. I found really interesting the ‘*wrpcap’* and the *‘rdpcap’* commands, that have allows the user to respectively, write in a .pcap file a list of packets and read a .pcap file. A way to fully understand what we can really do with scapy is keeping on running a wireshark session. I am going to show how simple can be to perform a potential network attack. Writing this simple line of code on the terminal we can notice on wireshark that:



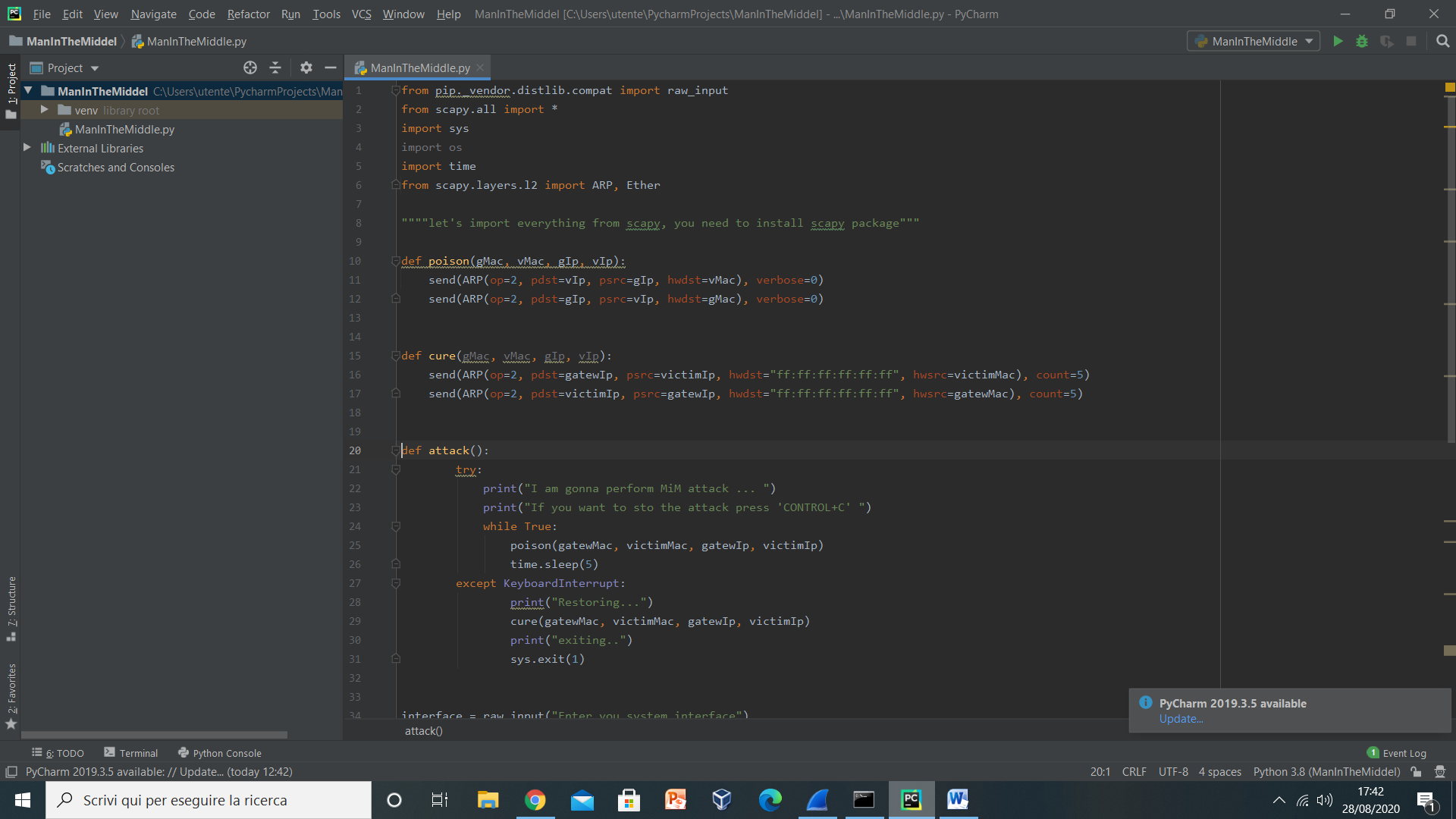
Are sent 10 packets(the parameter *count*), from the source address 192.168.1.2 to the destination address 127.0.0.1,using TCP protocol from the source port ‘135’ to destination port ‘135’. In order to show the proof of this command I kept on running a Wireshark session.With the filter: ip.src = 192.168.1.2, these packets have been captured :



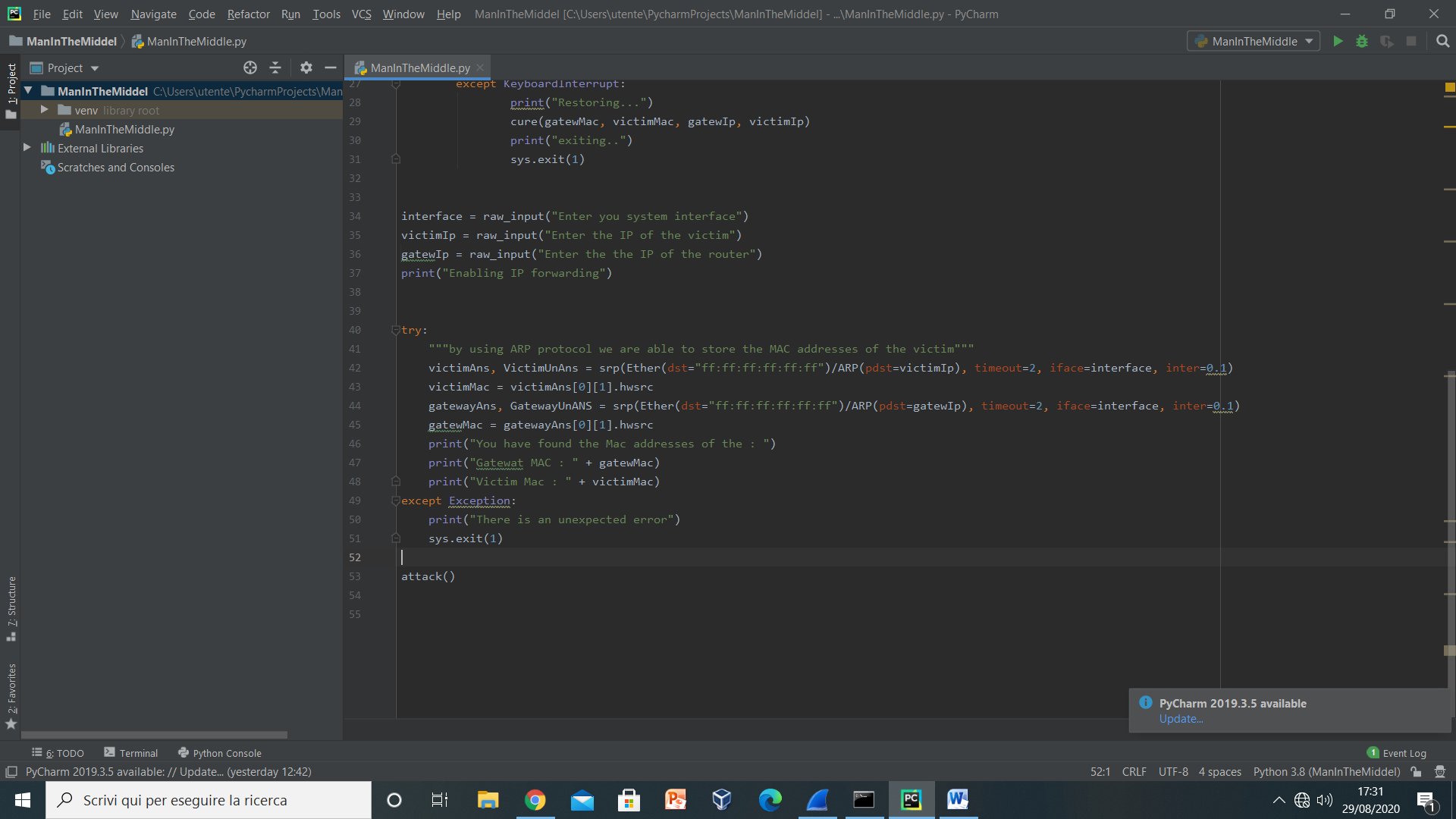
Now with the knowledge from The Wireless Internet course it is intuitive to say that: if we modify the destination IP(to the one of an AP) and sobstituted the parameter count with an other one really big we can perform a flooding attack. Consequently with one line of code we have performed a network attack.

**4 - Man in the middle attack**

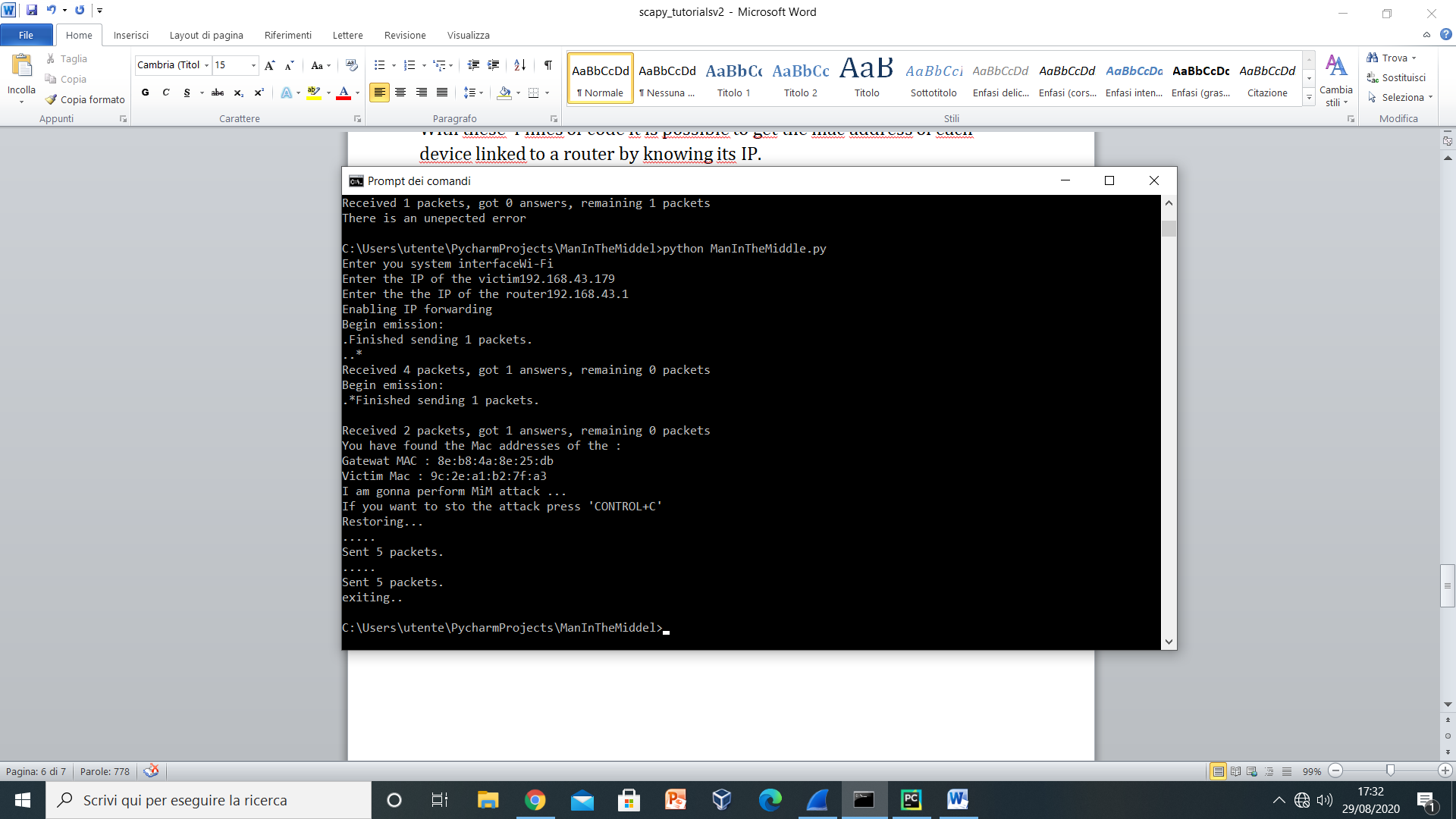
I want to conclude this tutorial with a program, implemented to perform a network attack named as: “Man in the middle”. A MIM attack is part of the attacks on WLANs, where the attacker puts himself in the middle of the communication. The goal of this attack is to secretly relay or alter the communication between the two parties. In order to perform this attack you need a laptop, an internet connection, and in case you are not using a Virtual Machine, an other device linked to an Access Point. By looking at the program implemented on Pycharm, it is possible to notice that the programm is divided into two parts. The first one defines the functions *Poison* and *Cure* . The Poison function is particularly interesting, because it will manipulate the ARP protocol in order to get a spoofed Mac address.



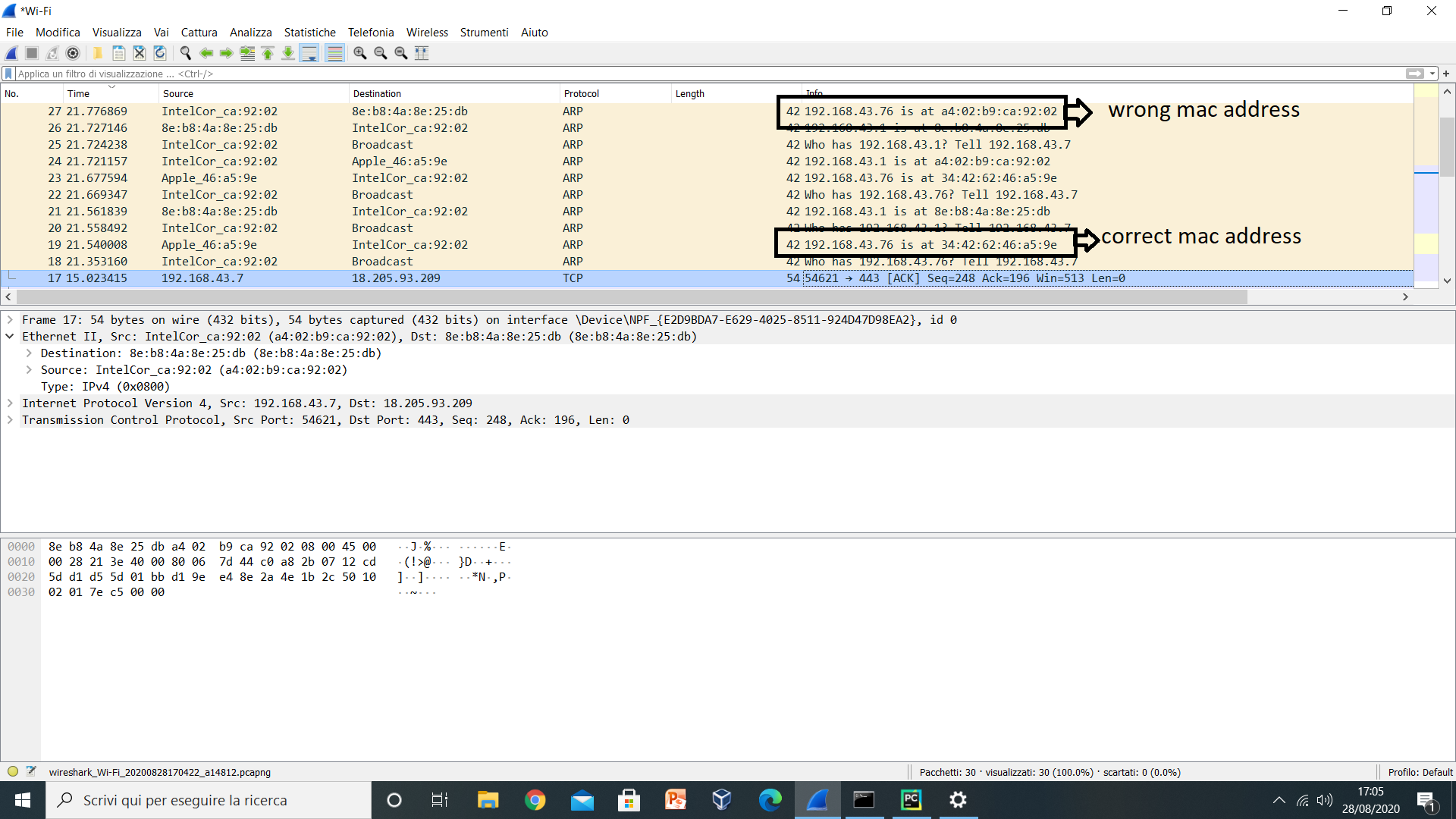
The second part of the code exploits the pontentialities of Scapy:



In practice, by only knowing the IP addresses of the router and the victim, it is possible both to get the respective mac addresses but also perform a Man in the middle attack. The thing to do is to launch the program by the command prompt,follow the instructions as reported in the follow screenshot and then by the help of wireshark look at what is happening.



In this particular case I have used my phone-device as router, as victim a tablet and a laptop to perform the attack. As it is possible to see in the picture the victim mac is : “9c:2e:a1:b2:7f:a3”. Let’s see now if Wireshark agrees with this assumption.

After I have launched the program, what Wireshark have found is that the IP address of the victim (192.168.43.76) is at the mac address: A4-02-B9-CA-92-02, that is the one of my laptop. In conclusion with 30 lines of code it is possible not only to perform a MiM attack but also to evaluate some issues of a really powerful program like Wireshark.

**5- Conclusions**

Just being only an extention of the python language,’Scapy’ is a really powerful tool that can make you exploit all the vulnerabilites of the networks. I think that in order to improve the strenght of a system is really important to firstly know its weaknesses, having the possibility to study this tool it is really useful. In particular it has helped me to put in practice concepts studied during lectures ( such as Attack on Wlans) and to better learn the python programming language.