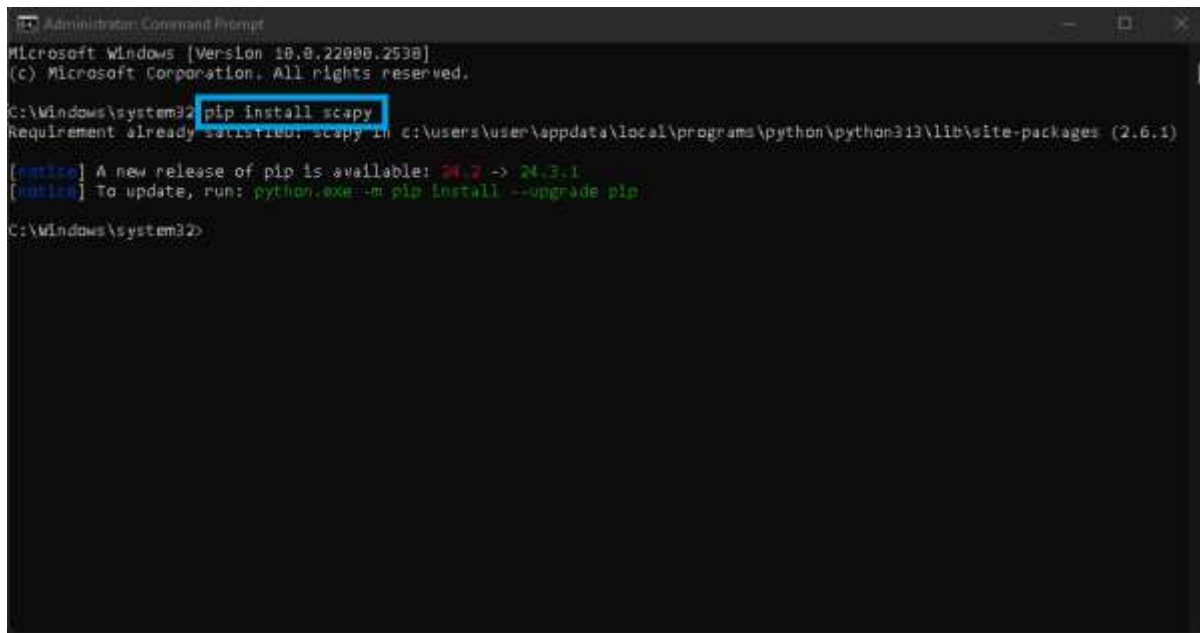


USING THE TOOL



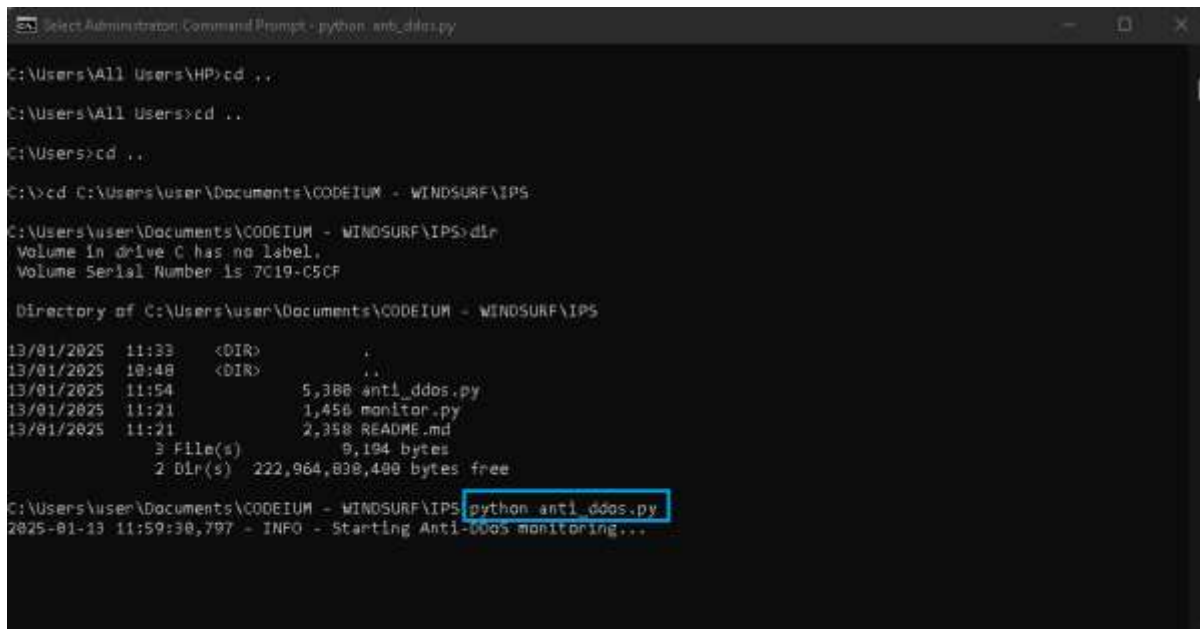
```
Administration Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> pip install scapy
Requirement already satisfied: scapy in c:\users\user\appdata\local\programs\python\python313\lib\site-packages (2.6.1)

[notice] A new release of pip is available: 24.2 -> 24.3.1
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Windows\system32>
```

Fig 1.0 – Installing scapy



```
Select Administrator Command Prompt - python_anti_ddos.py

C:\Users\All Users\HP>cd ..
C:\Users\All Users>cd ..
C:\Users>cd ..
C:\>cd C:\Users\user\Documents\CODEIUM - WINDSURF\IPS
C:\Users\user\Documents\CODEIUM - WINDSURF\IPS>dir
Volume in drive C has no label.
Volume Serial Number is 7C19-C5CF

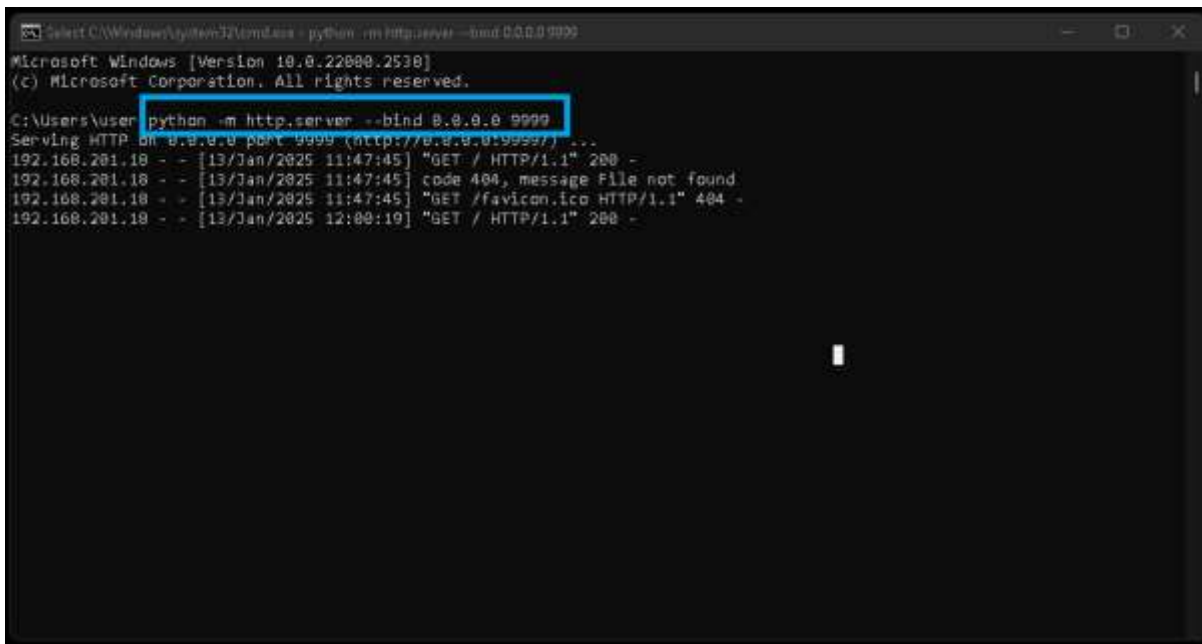
Directory of C:\Users\user\Documents\CODEIUM - WINDSURF\IPS

13/01/2025  11:33    <DIR>          .
13/01/2025  10:48    <DIR>          ..
13/01/2025  11:54             5,388 anti_ddos.py
13/01/2025  11:21             1,456 monitor.py
13/01/2025  11:21             2,358 README.md
               3 File(s)              9,194 bytes
               2 Dir(s)  222,964,838,400 bytes free

C:\Users\user\Documents\CODEIUM - WINDSURF\IPS>python anti_ddos.py
2025-01-13 11:59:30,797 - INFO - Starting Anti-DDoS monitoring...
```

Fig 2.0 -Starting the anti_ddos tool

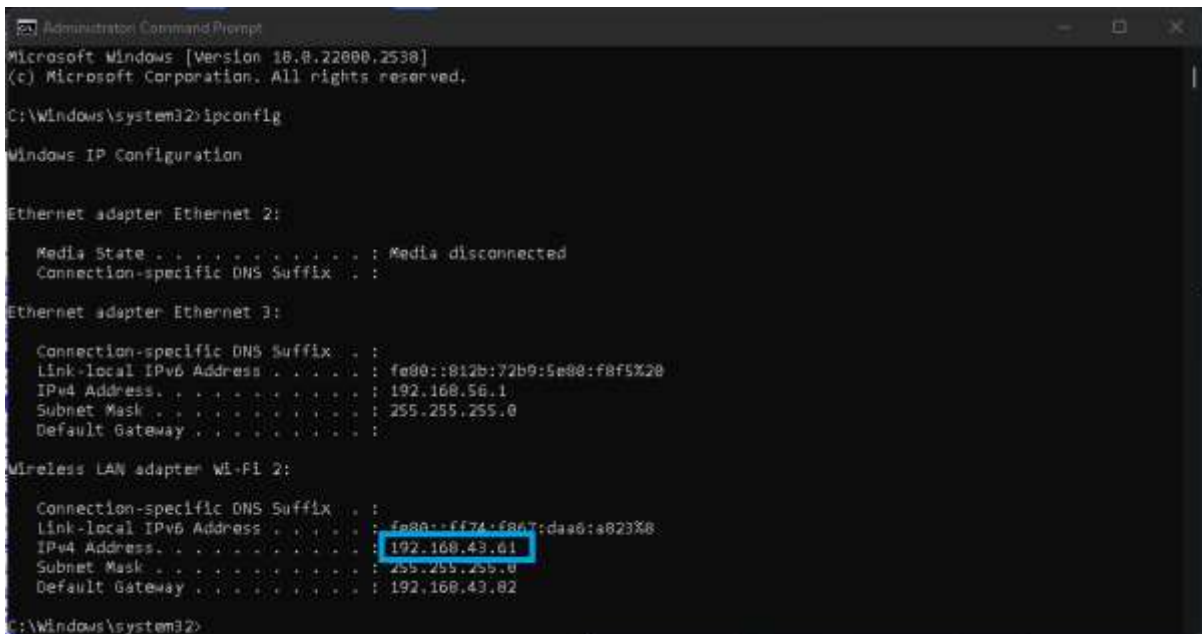
TESTING THE TOOL



```
Select C:\Windows\system32\cmd.exe - python -m http.server --bind 0.0.0.0 9999
Microsoft Windows [Version 10.0.22000.2530]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user> python -m http.server --bind 0.0.0.0 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
192.168.201.10 - - [13/Jan/2025 11:47:45] "GET / HTTP/1.1" 200 -
192.168.201.10 - - [13/Jan/2025 11:47:45] code 404, message File not found
192.168.201.10 - - [13/Jan/2025 11:47:45] "GET /favicon.ico HTTP/1.1" 404 -
192.168.201.10 - - [13/Jan/2025 12:00:19] "GET / HTTP/1.1" 200 -
```

Fig 1.0. Starting an http web server



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.2530]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::812b:72b9:5e00:f8f5%20
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ff74:f867:d4a6:a823%8
    IPv4 Address. . . . . : 192.168.43.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.82

C:\Windows\system32>
```

Fig. 2.0: Confirming the Network IP address of the Target System

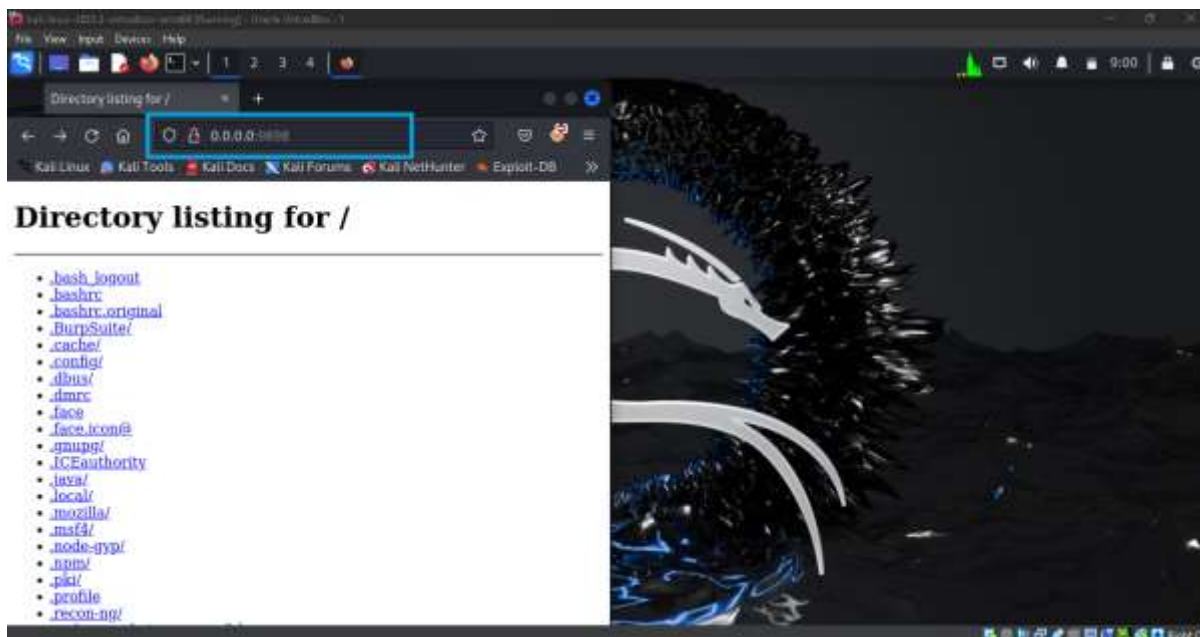


Fig 3.0: Loading the Web server on your pentest machine after connecting to the same network

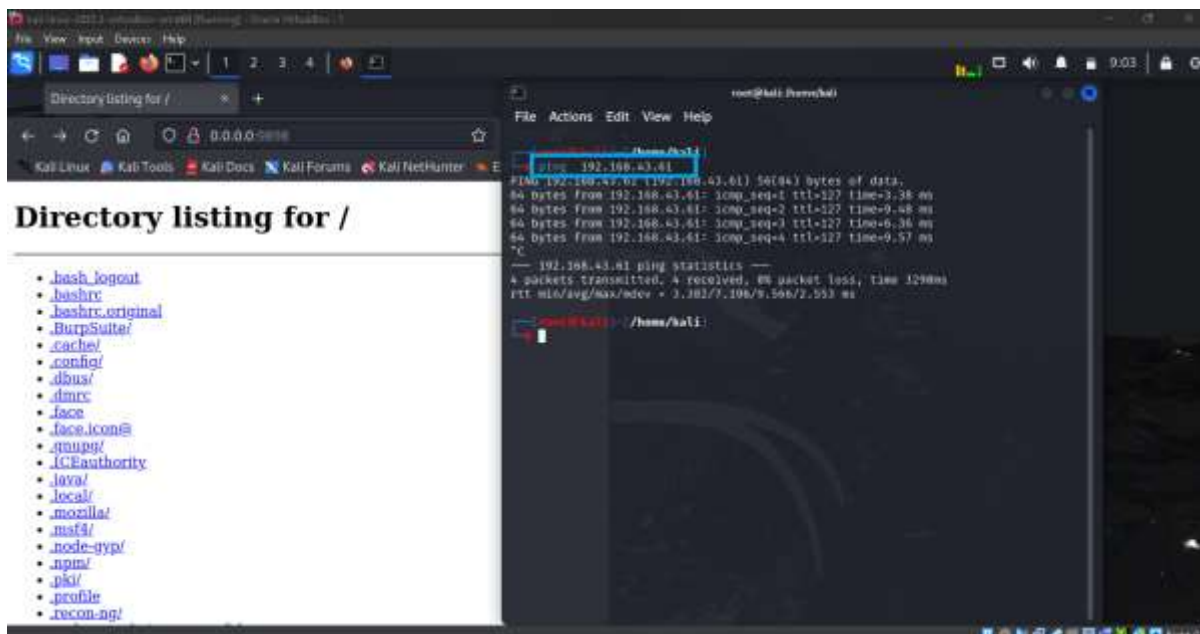


Fig. 4.0: Pinging the Target IP to confirm connection

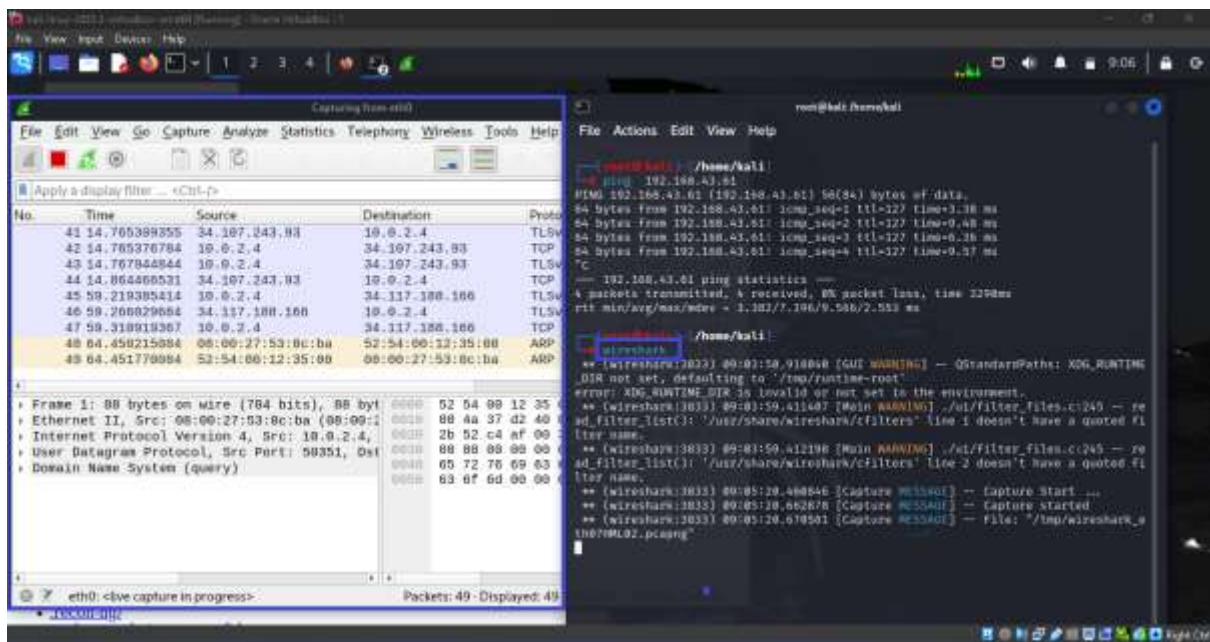


Fig 5.0: Launching Wireshark to enable you monitor the network while running the DDOS/DOS attack

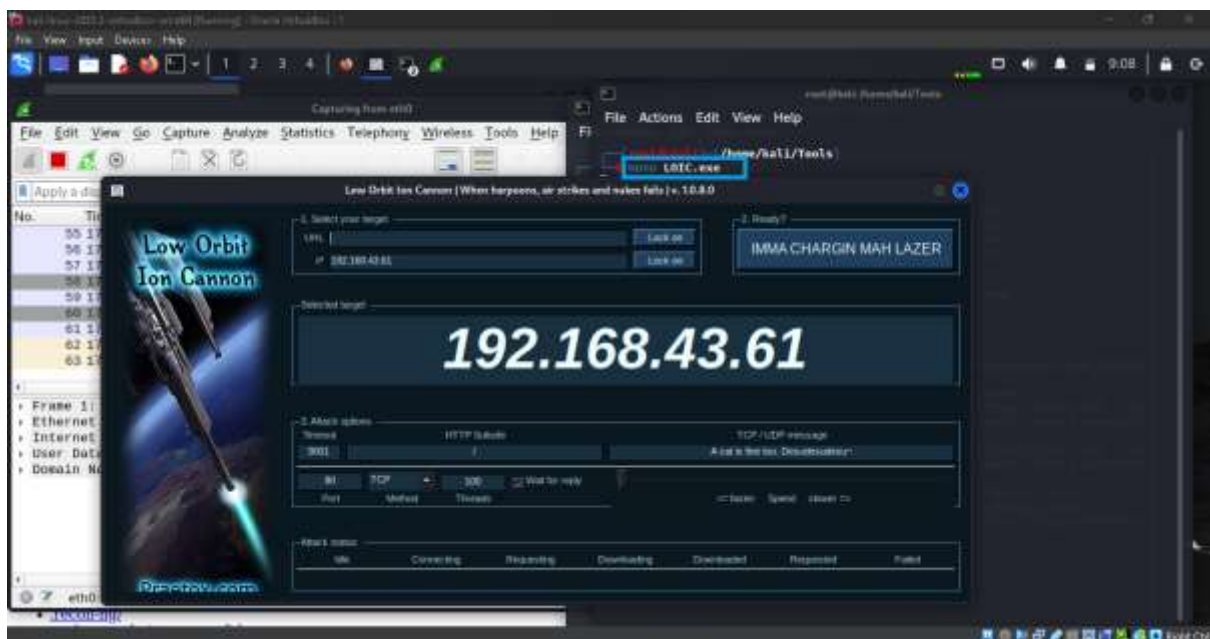


Fig 6.0: Launching LOIC tool for a DDOS attack. The Low Orbit Ion Cannon is a user-friendly tool that launches DoS and DDoS attacks



Fig. 7.0: Copying the web application url, replacing the **0.0.0.0** with the ip of the target server I got from **Fig 2.0**, setting the method of the flood to be a **TCP** request, setting the **Threads** (Amount of request) to 100 the clicking on the **IMMA CHARGIN MAHLAZER** to start the flood.

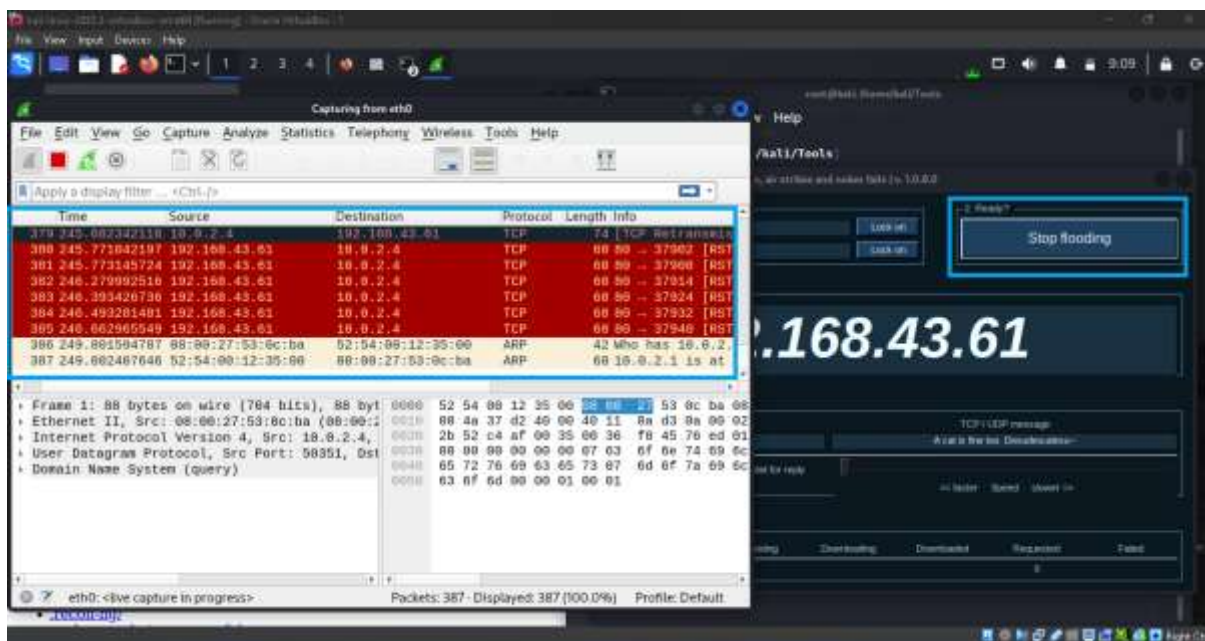


Fig. 8.0: The Flooding has started but it is being dropped by the **anti_ddos** tool, you can see this display on **wireshark**. You can click on **Stop flooding** to stop this attack.


```
Administrative Command Prompt - python url_ddos.py

2025-01-13 15:22:22,605 - INFO - Blocked IP: 192.168.43.61
2025-01-13 15:22:22,606 - WARNING - Rate limit exceeded for IP: 192.168.43.61

Deleted 1 rule(s).
Ok.

2025-01-13 15:27:30,014 - INFO - Unblocked IP: 192.168.43.61
Ok.

2025-01-13 15:28:17,802 - INFO - Blocked IP: 192.168.43.61
2025-01-13 15:28:17,802 - WARNING - Rate limit exceeded for IP: 192.168.43.61

Deleted 1 rule(s).
Ok.

2025-01-13 15:33:30,471 - INFO - Unblocked IP: 192.168.43.61
Ok.

2025-01-13 15:34:25,425 - INFO - Blocked IP: 192.168.43.61
2025-01-13 15:34:25,426 - WARNING - Rate limit exceeded for IP: 192.168.43.61
Ok.

2025-01-13 15:35:30,764 - INFO - Blocked IP: 192.168.153.18
2025-01-13 15:35:30,767 - WARNING - Rate limit exceeded for IP: 192.168.153.18
Ok.

2025-01-13 15:35:35,977 - INFO - Blocked IP: 35.186.224.26
2025-01-13 15:35:35,977 - WARNING - Rate limit exceeded for IP: 35.186.224.26
```

Fig 9.0: This is the results you will be getting from the tool when you are under this kind of attack.