

**Submitted To:**

Mam Iqra Khan

**Submitted By:**

Rafia Tehseen (BSEF19M007)

Fatima Masood (BSEF19M020)

Toseeq Sarwar (BSEF19M041)

**Subject:**

Information Security

**Last Date of Submission:**

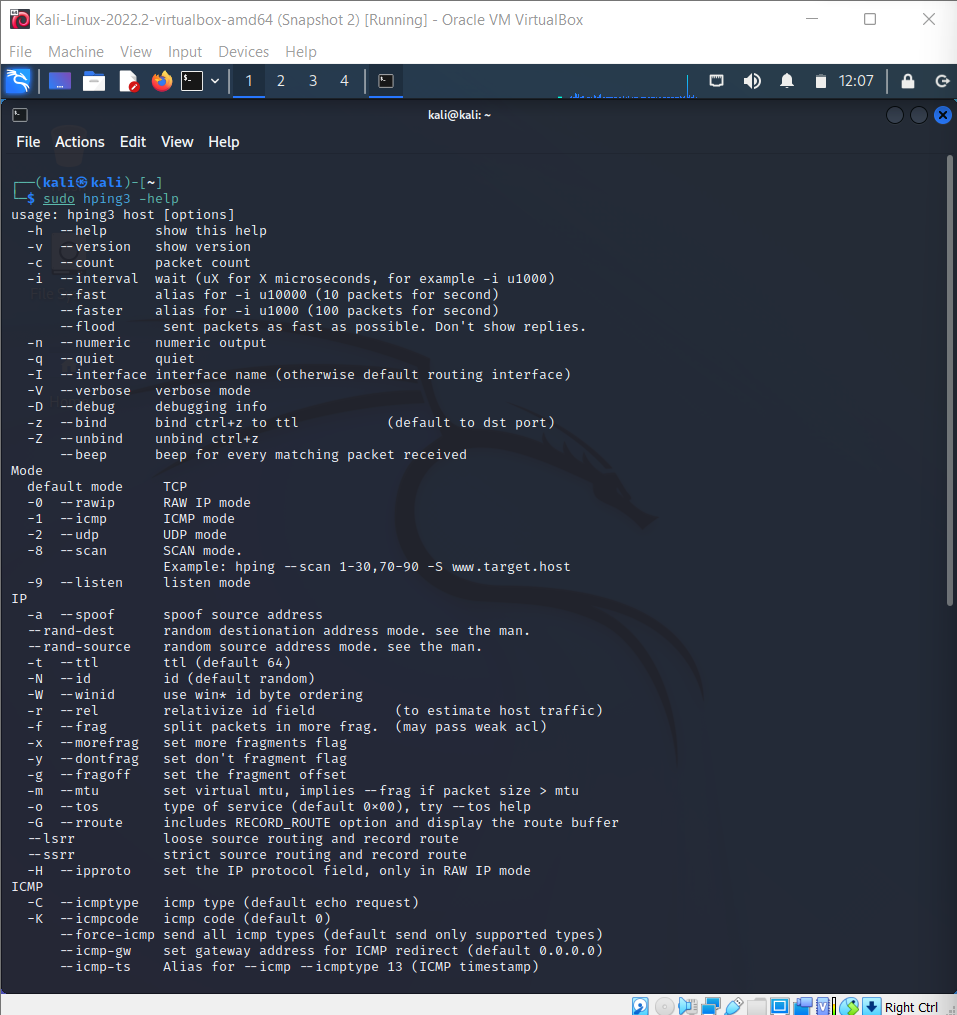
Monday, June 06, 2020

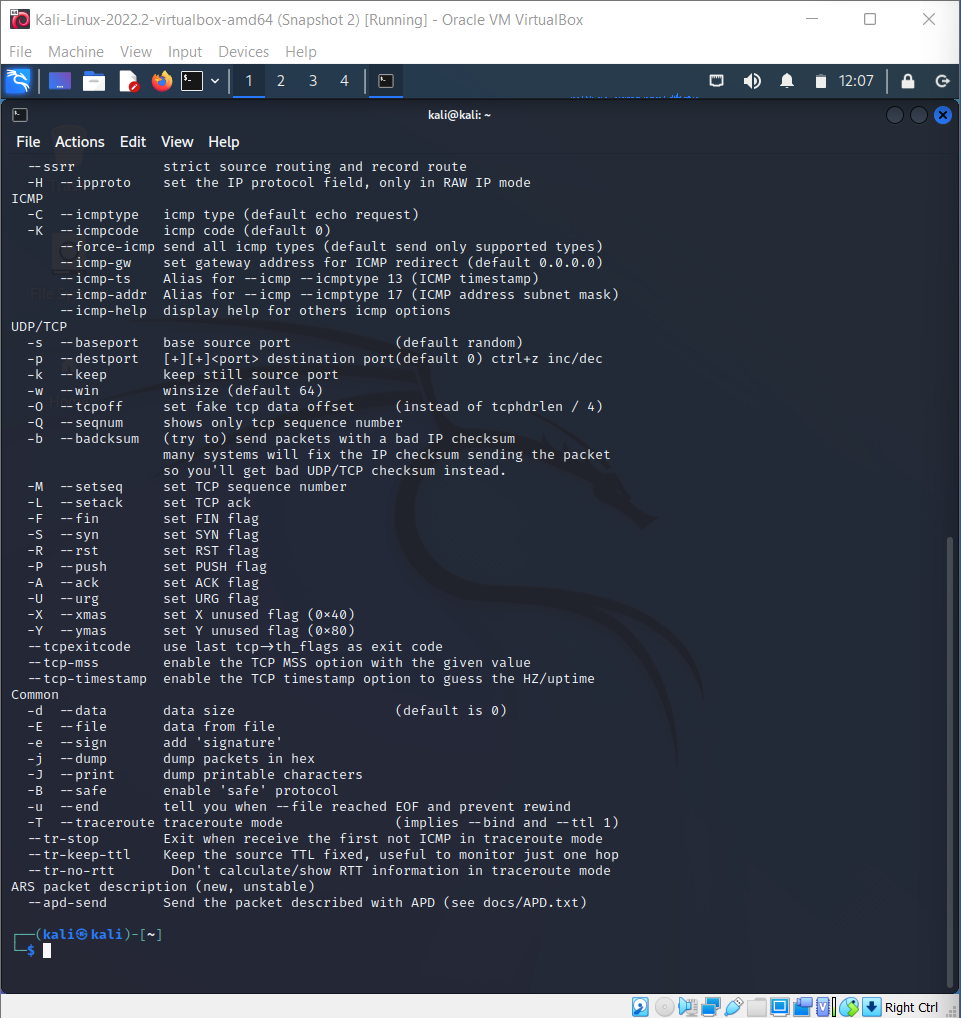
**Department:**

CS & IT Department

# DOS (Denial of service) Attack

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. We have implemented DOS attack using an “hping3”, a kali Linux tools. Hping3 is an open-source packet generator and analyzer for the TCP/IP protocol. hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP (Internet Control Message Protocol) replies. All the options available for hping3 is given below:

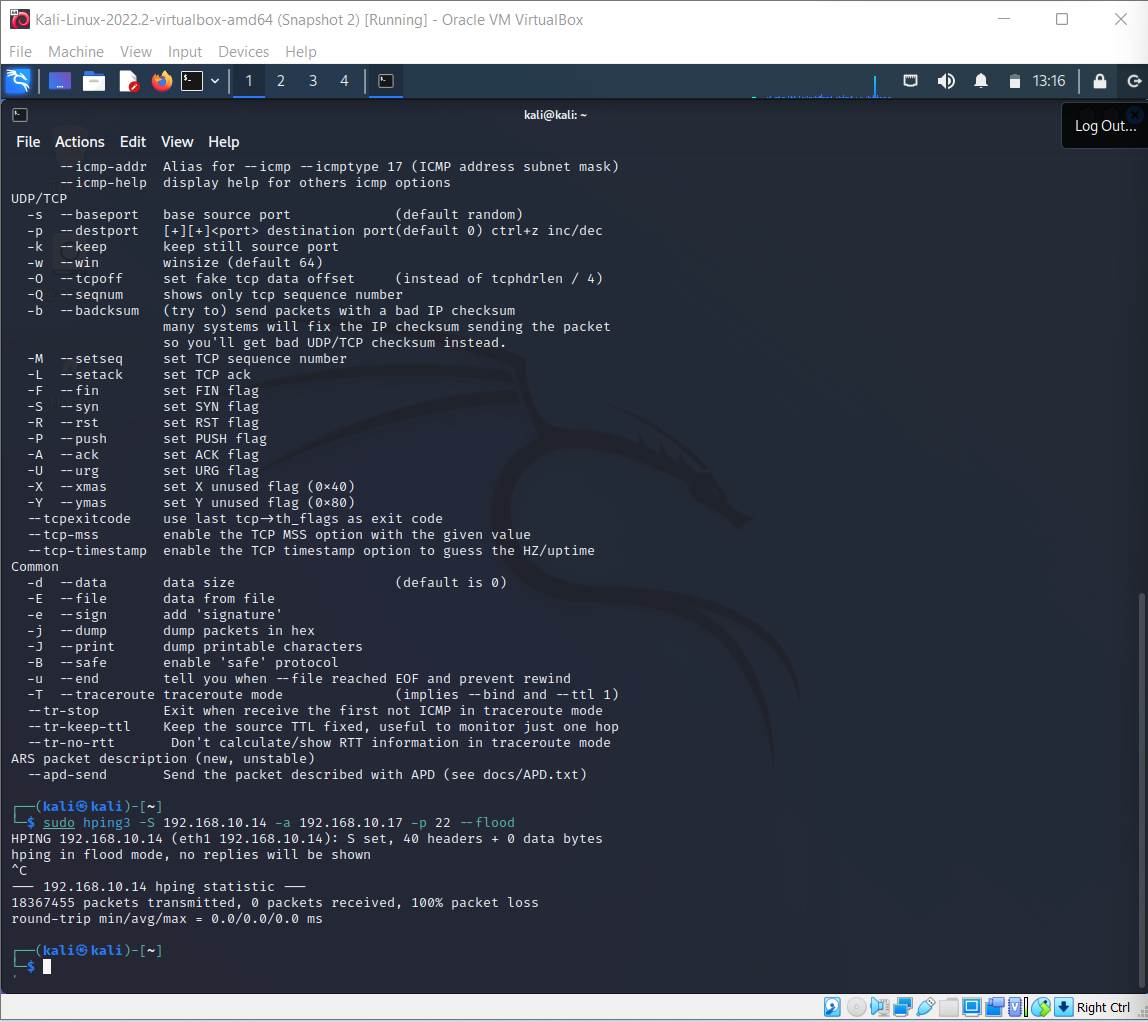




Command we use to launch DOS attack on target match is given below

sudo hping3 -S 192.168.10.14 -a 192.168.10.17 -p 22 –flood

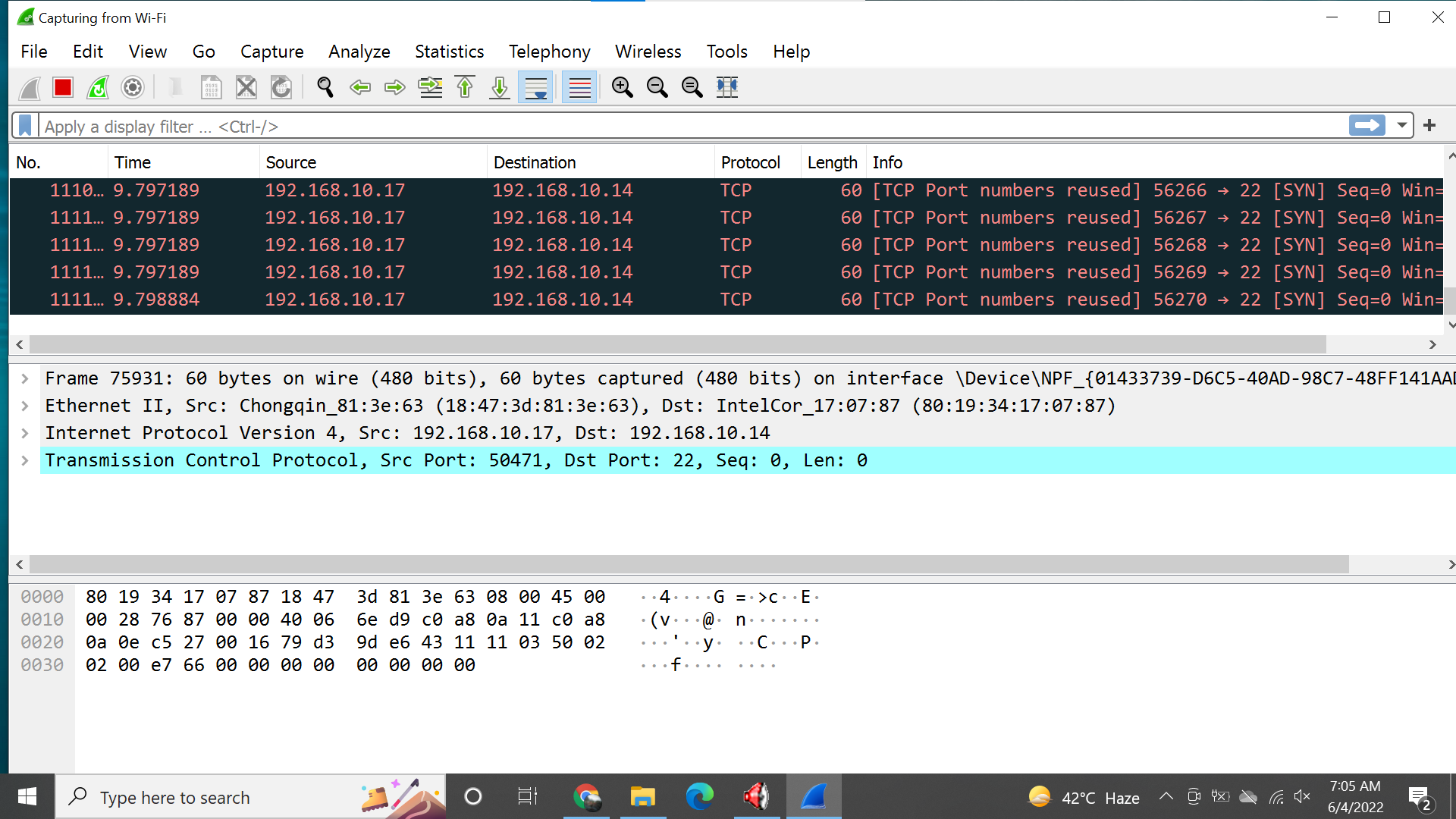
* -S indicate that hping3 will sent SYN flags to the target system
* 192.168.10.14 is the IP address of target machine
* -a indicate that it is the IP address of source machine which is going to send packet to target machine
* -p indicate the port number which is going to receive SYN flags/packets
* --flood indicate that source need to send packets as fast as possible but don’t show replies because if source machine begin receiving responses that there is a high chance that it will possibly crash source machine

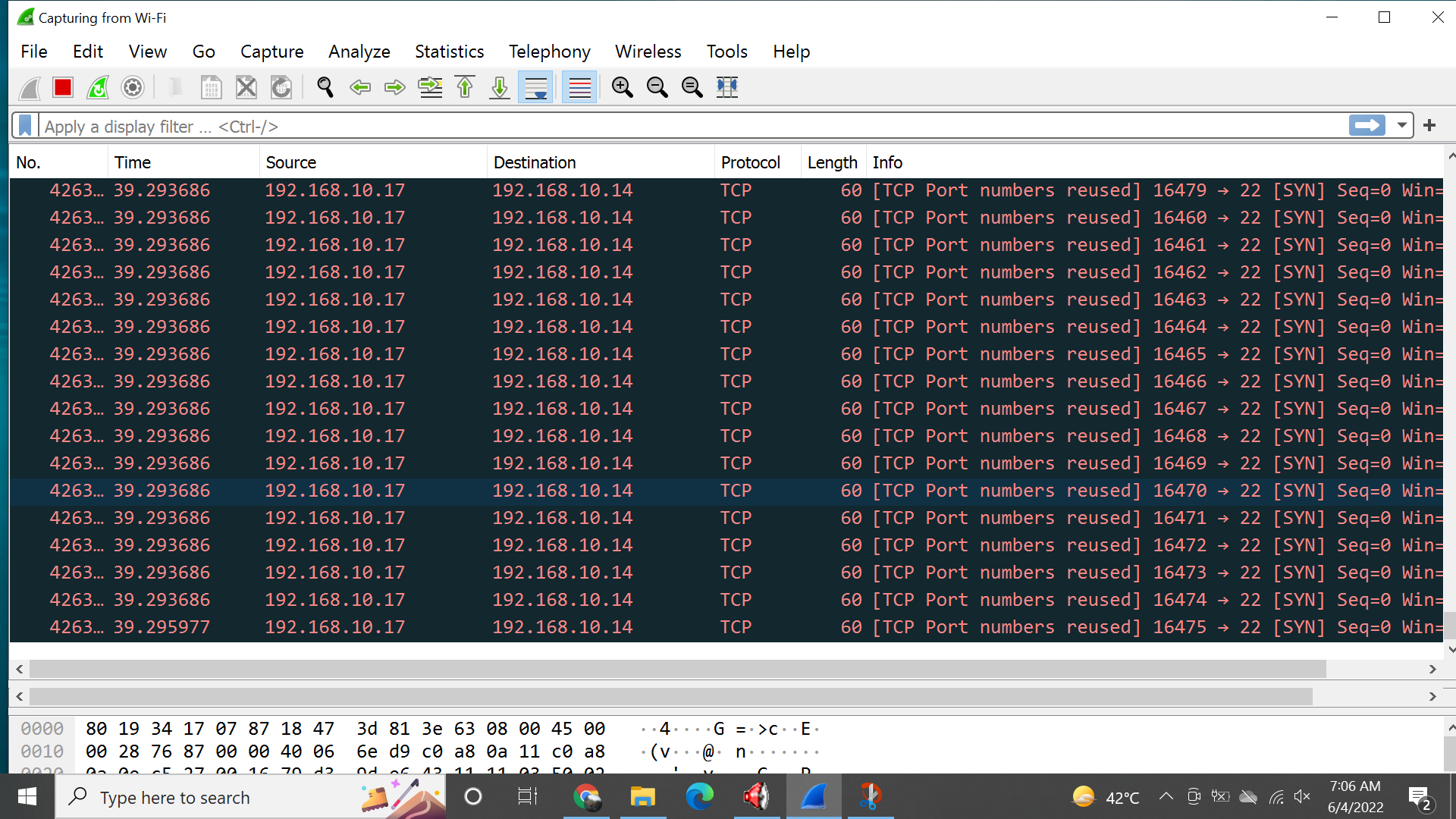


# Attack Detection on Targeted Machine

## Packet Sniffer:

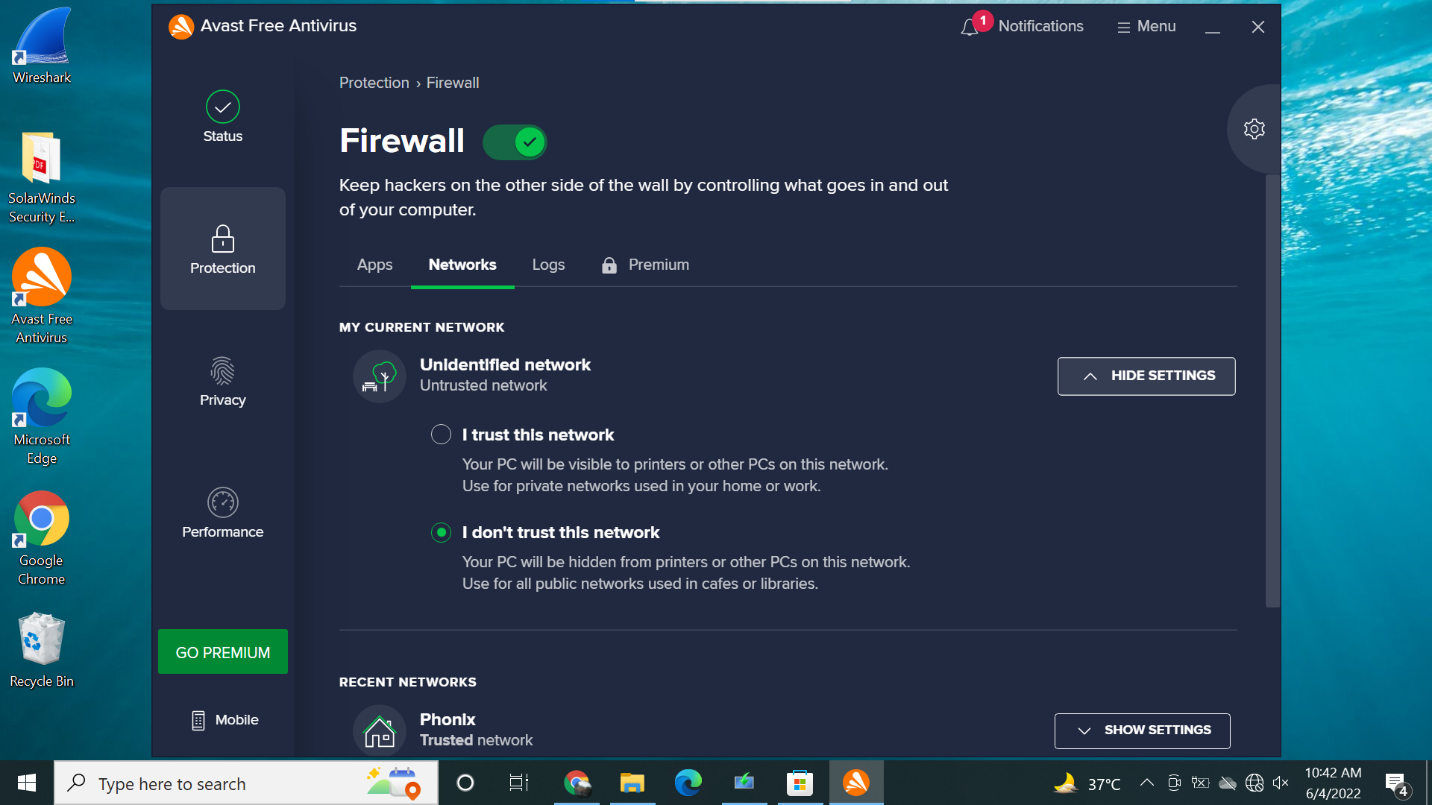
We have used Wireshark to catch packets being received on the targeted device. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark was able to catch SYN packets that were received by target machine.

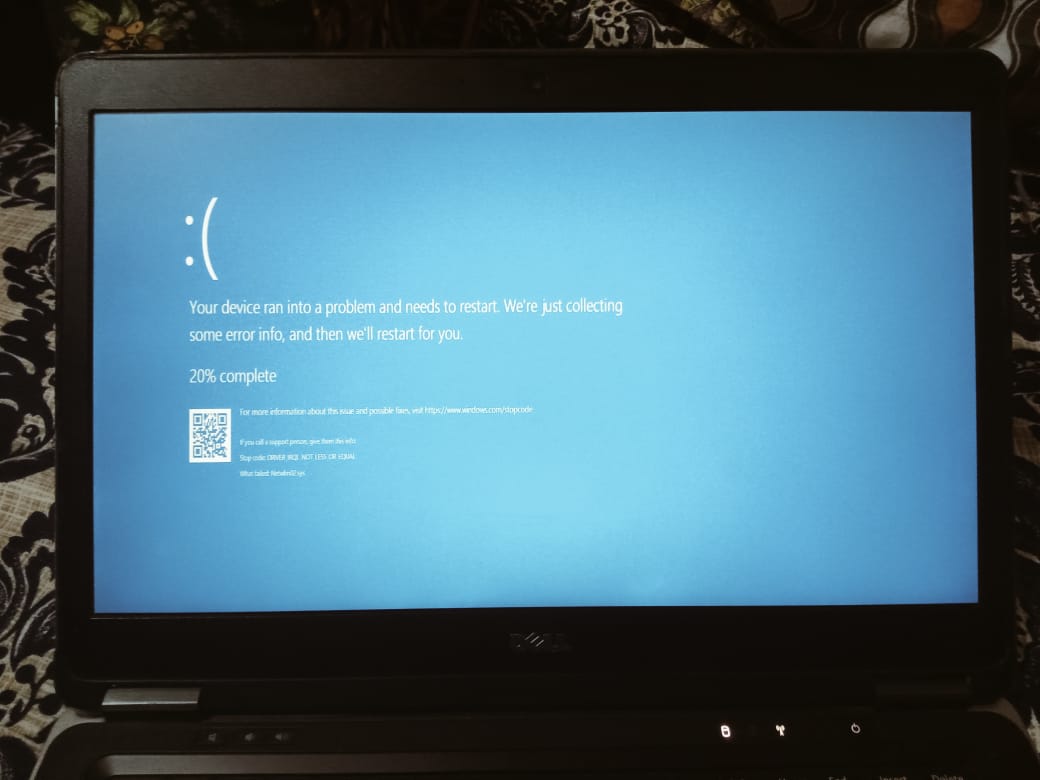




## Firewall:

We use Avast anti-virus firewall to resist the implementation of DOS attack. The Firewall reacted by immediately rebooting the target system after detection malicious activity.





## IDS and HoneyPot:

KfSensor is used to detect the attack which act as both intrusion detection system and HoneyPot. It was able to generate warning and point out malicious visitors of the targeted machine. It also catch the packets that were being send to implement the DOS attack.

