**Hướng dẫn thực nghiệm Phát hiện DDos trên SDN**

1. **Mở các máy ảo trên VM Virtual Box**

* Mở Ubuntu (nơi chứa [ryu-controller](https://ryu.readthedocs.io/en/latest/getting_started.html))
* Mở Mininet VM [mininet](https://github.com/mininet/mininet/releases/)
* Connect ssh 2 máy ảo trên trên mobaXterm

1. **Clone source từ github**
   1. Trên máy Ubuntu ryu

* cd ryu/ryu/controller
* git clone <https://github.com/tranthanhhuy19032001/DACNTT2_DDos_ML.git>

username: tranthanhhuy19032001

password: ghp\_dJ13ANgAhoPo1DMLIQECFZGixaRluE1VT6Vc

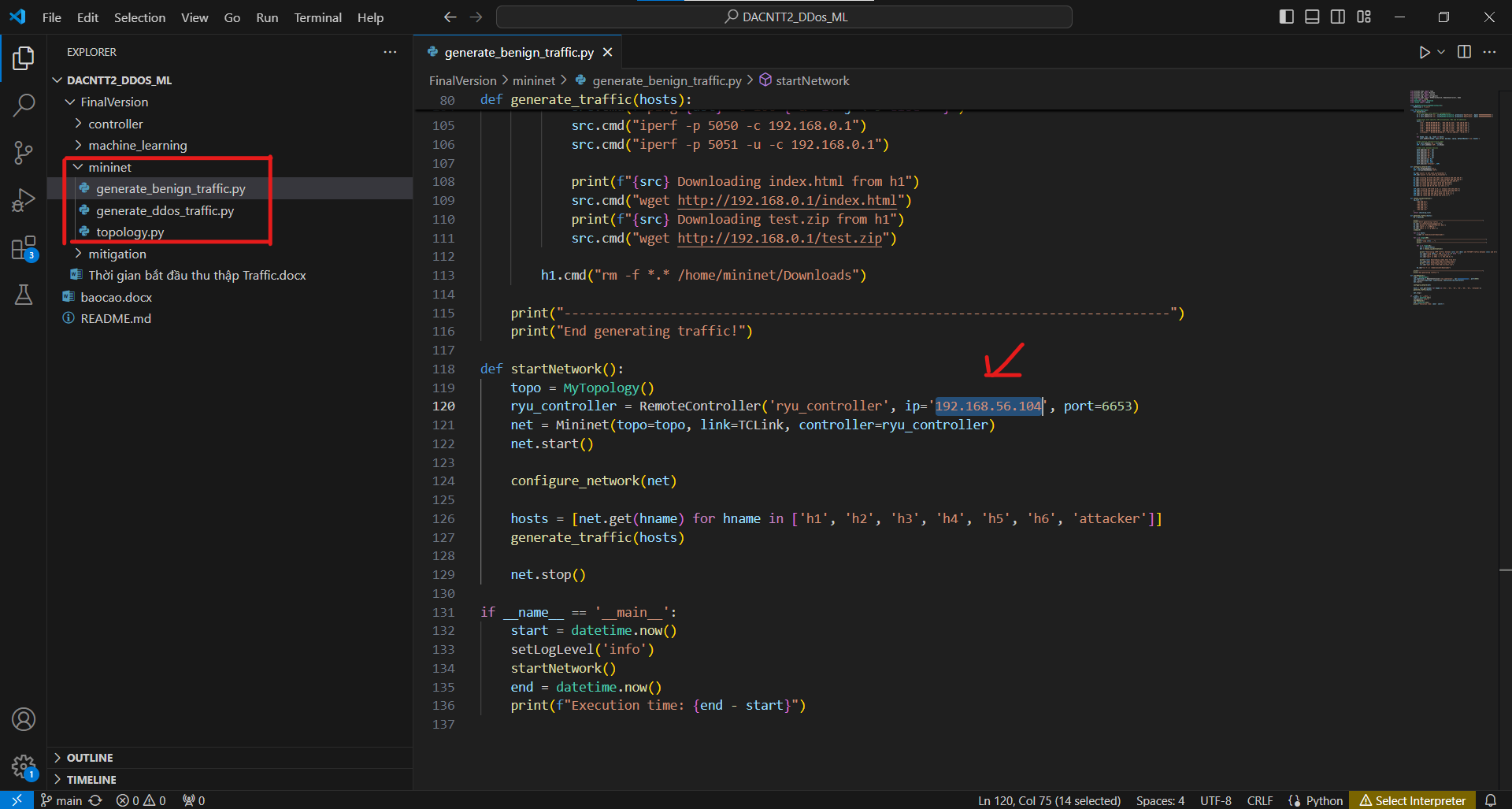
* cd DACNTT2\_DDos\_ML/FinalVersion/controller
  1. Trên Mininet VM
* cd mininet/mininet
* git clone <https://github.com/tranthanhhuy19032001/DACNTT2_DDos_ML.git>

username: tranthanhhuy19032001

password: ghp\_dJ13ANgAhoPo1DMLIQECFZGixaRluE1VT6Vc

* cd DACNTT2\_DDos\_ML/FinalVersion/mininet

Đổi địa chỉ ip trong 3 file generate\_benign\_traffic.py, generate\_benign\_traffic.py, topology.py thành ip máy ryu của bạn



* **Lệnh để mở được xterm trển mobaXterm**
* sudo -i
* export DISPLAY=localhost:10.0
* xauth add $(xauth -f ~mininet/.Xauthority list|tail -1)

1. **Generate Dataset**

Chạy các lệnh sau:

* Trên máy ryu

ryu-manager collect\_traffic.py

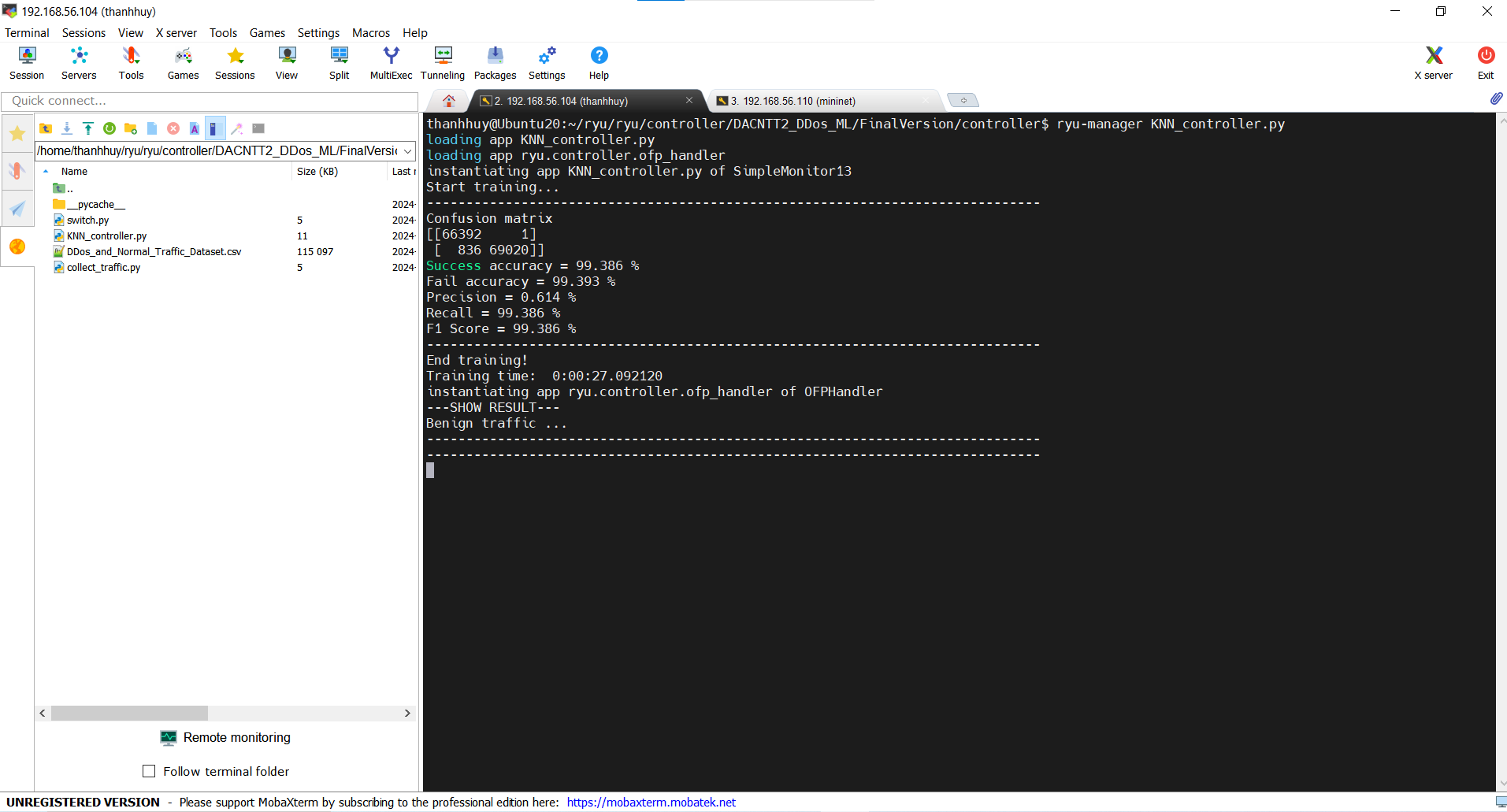
* Trên máy Mininet

sudo python generate\_benign\_traffic.py (tạo normal traffic)

sudo python generate\_ddos\_traffic.py (tạo DDos traffic)

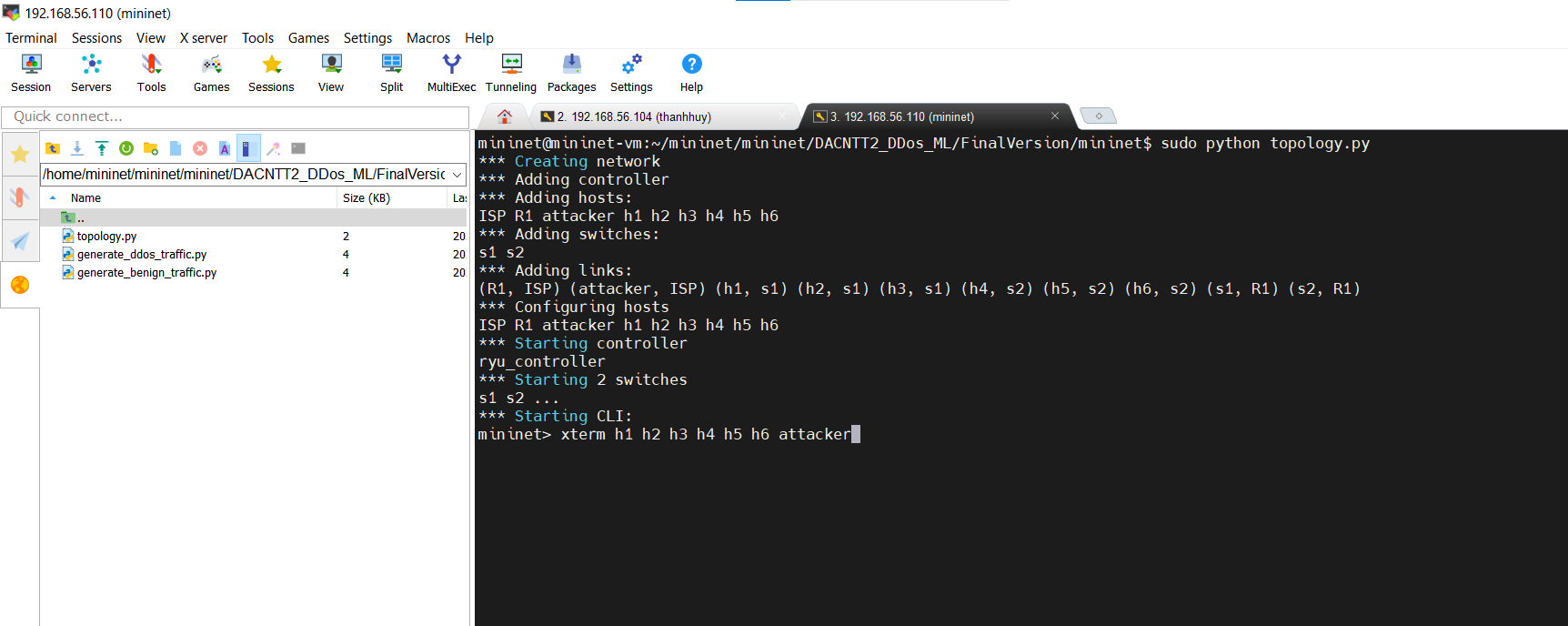
1. **Thực nghiệm phát hiện DDos**
   1. Trên máy RYU

ryu-manager KNN\_controller.py



* 1. Trên Mininet VM

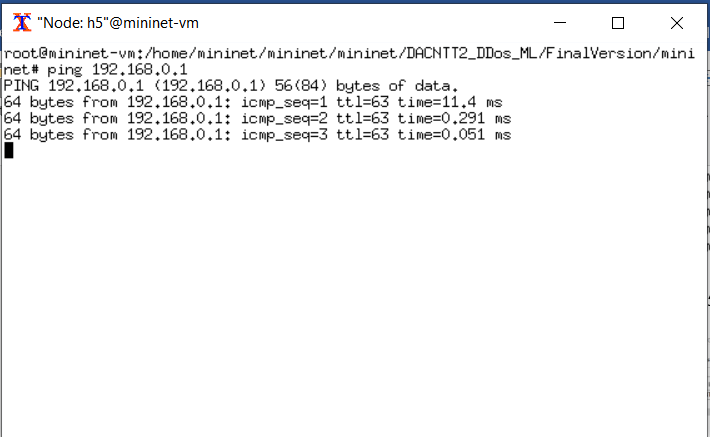
sudo python topology.py



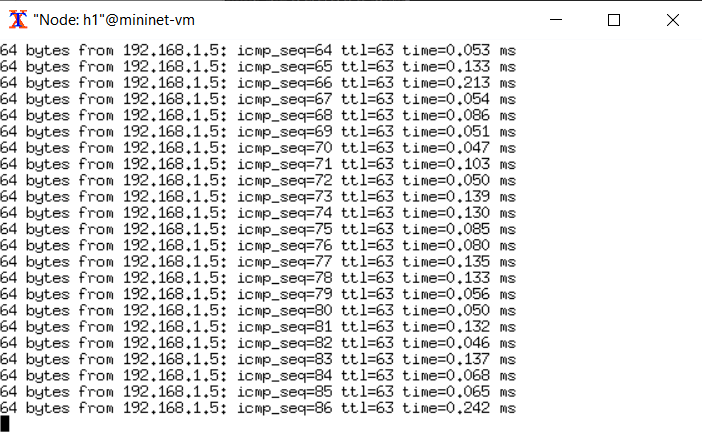
xterm h1 h2 h3 h4 h5 attacker

* Thực hiện các lệnh ping bình thường để kiểm tra traffic bình thường

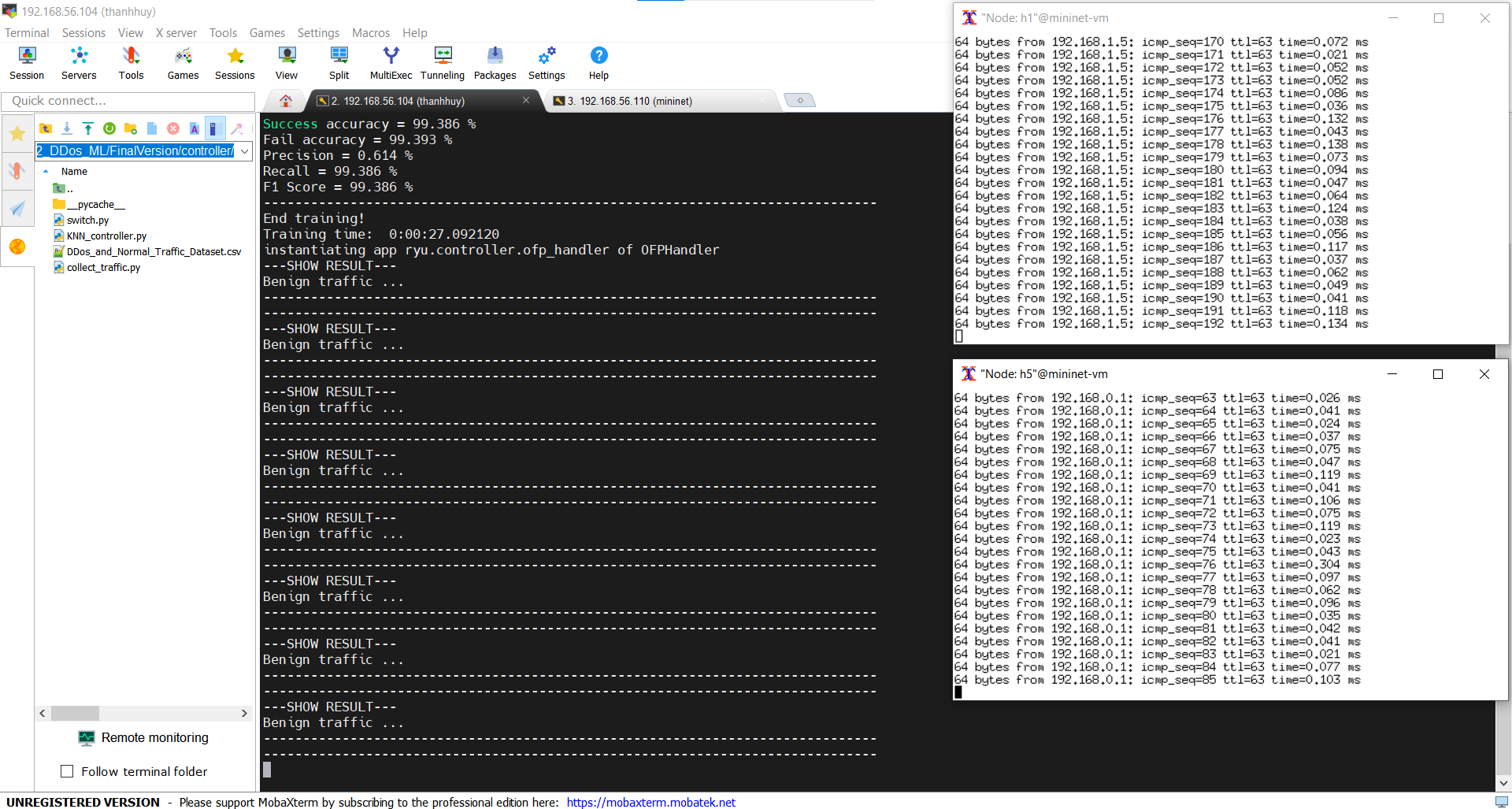
ping 192.168.0.1



ping 192.168.1.5



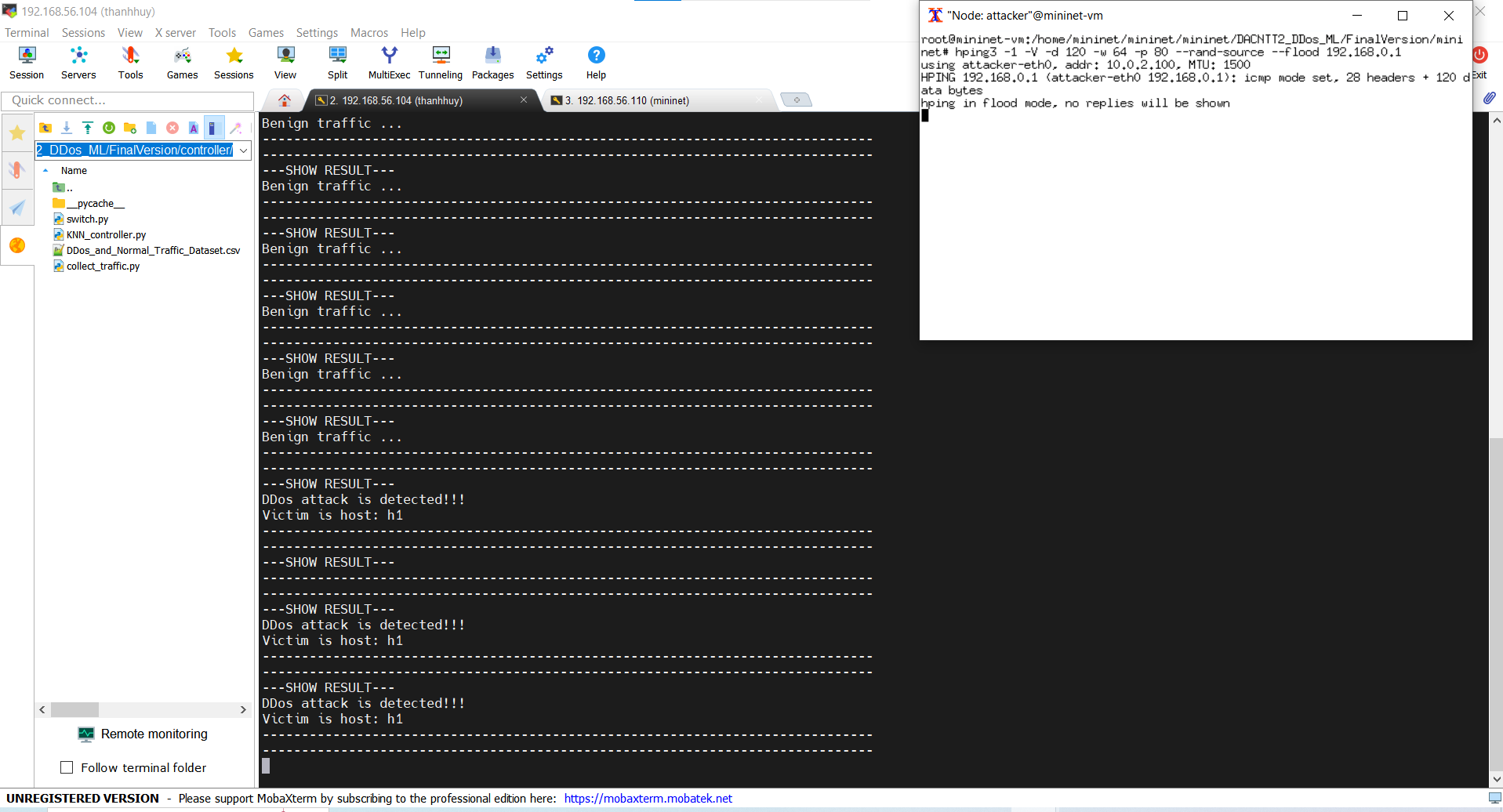
Kết quả predict

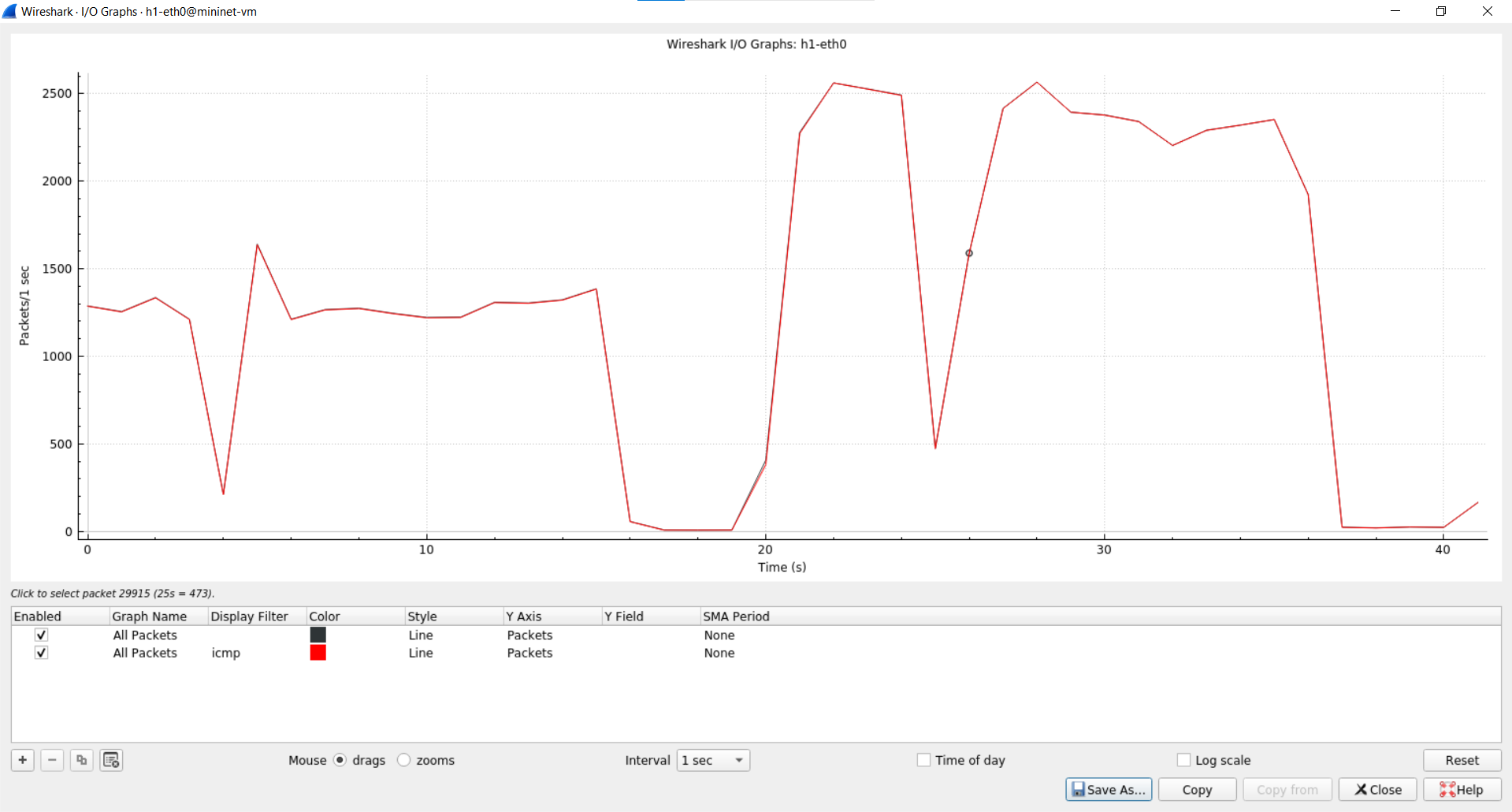


…

* Thực hiện tấn cống ICMP Flood tới h1

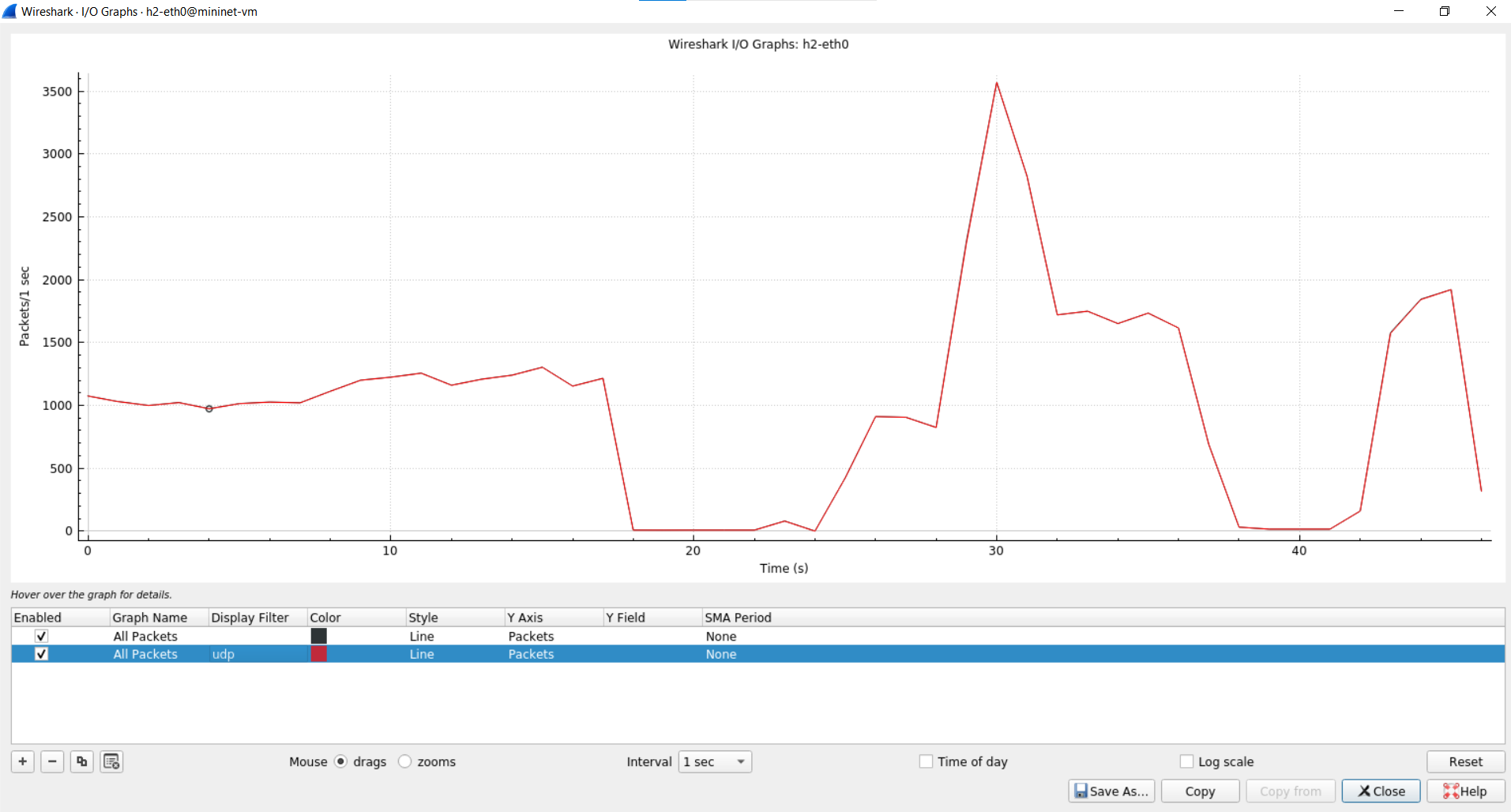
hping3 -1 -V -d 120 -w 64 -p 80 --rand-source –flood 192.168.0.1

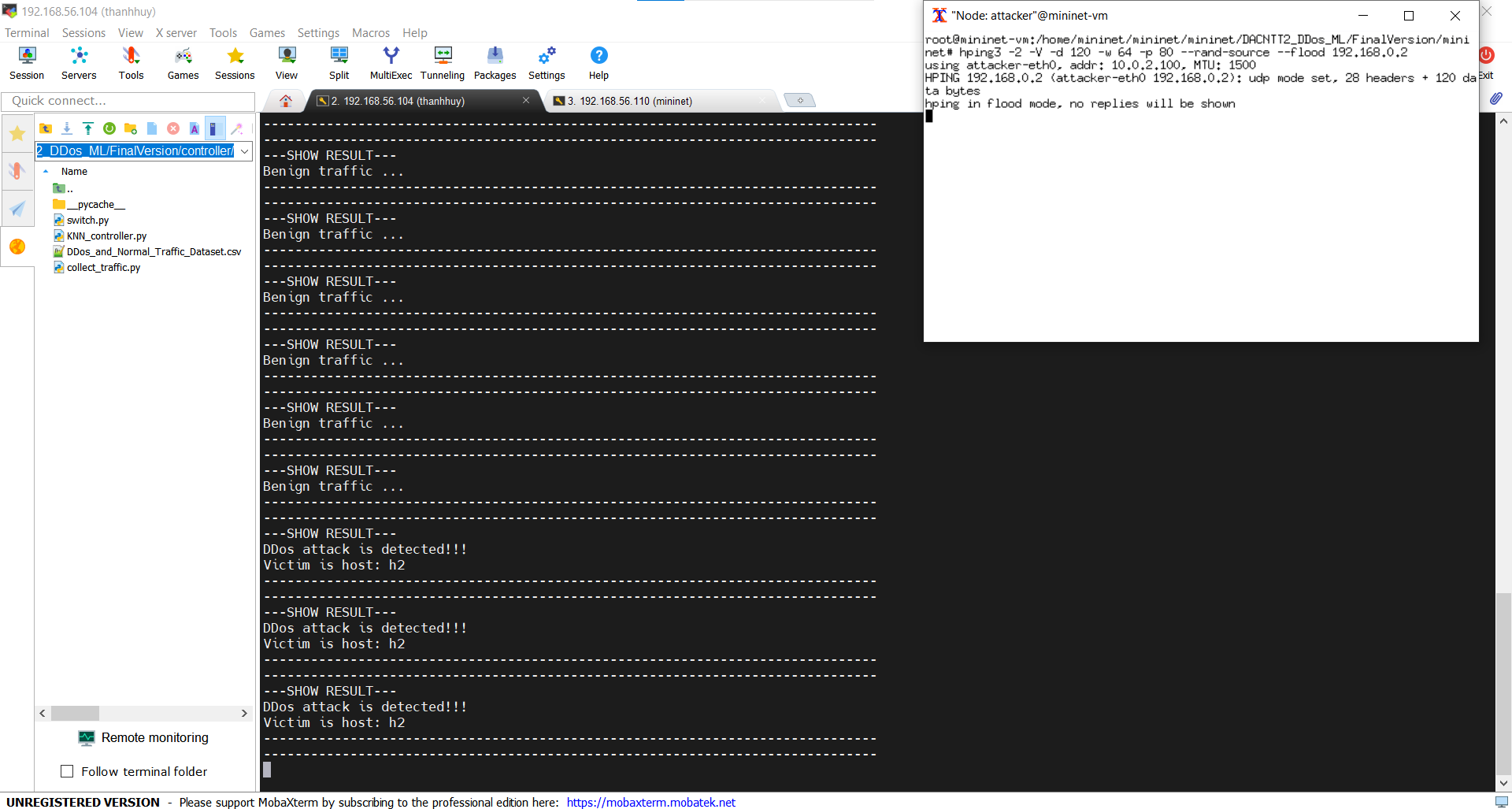




* Thực hiện tấn công UDP Flood tới h2

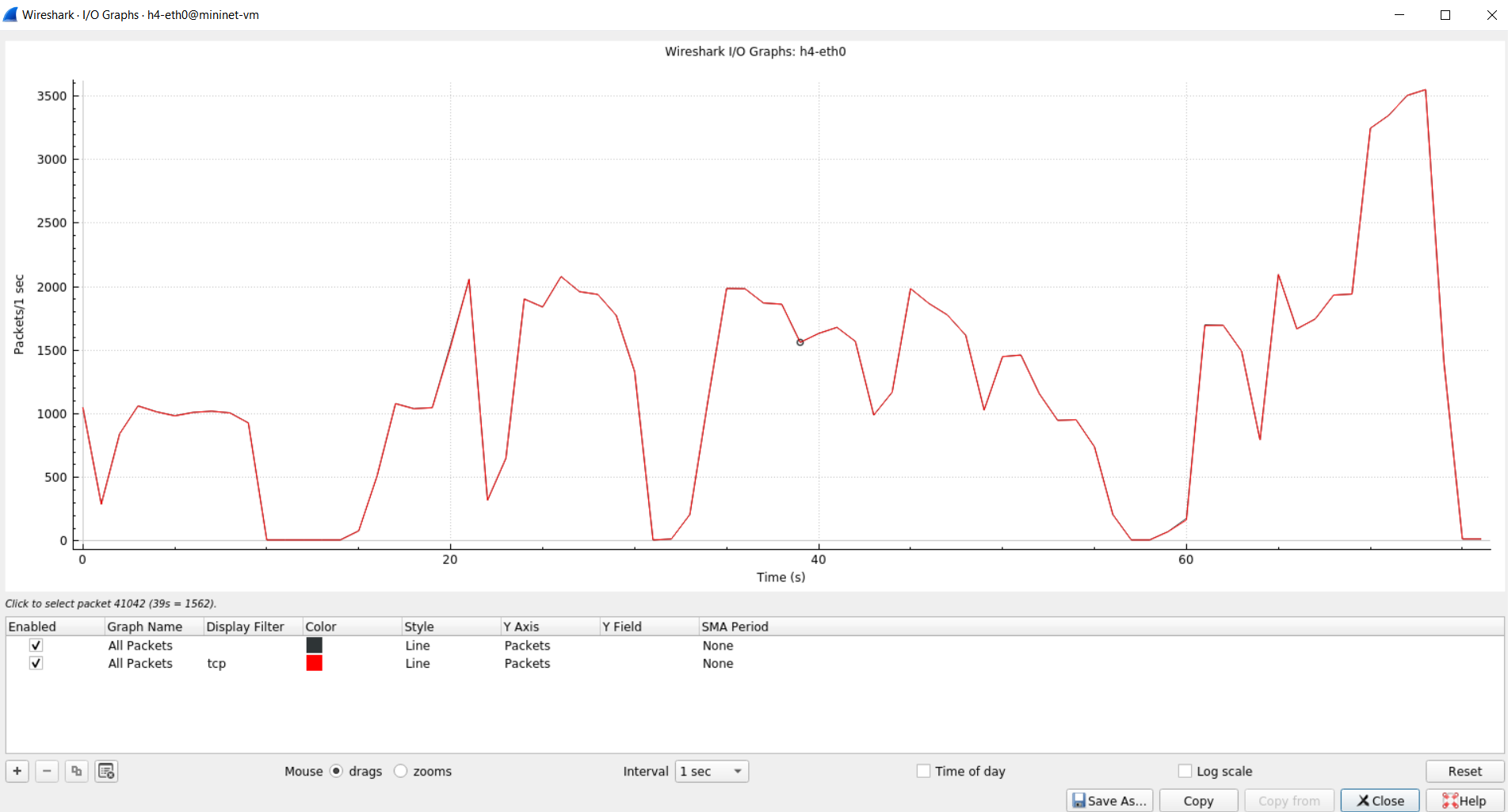
hping3 -2 -V -d 120 -w 64 -p 80 --rand-source –flood 192.168.0.2

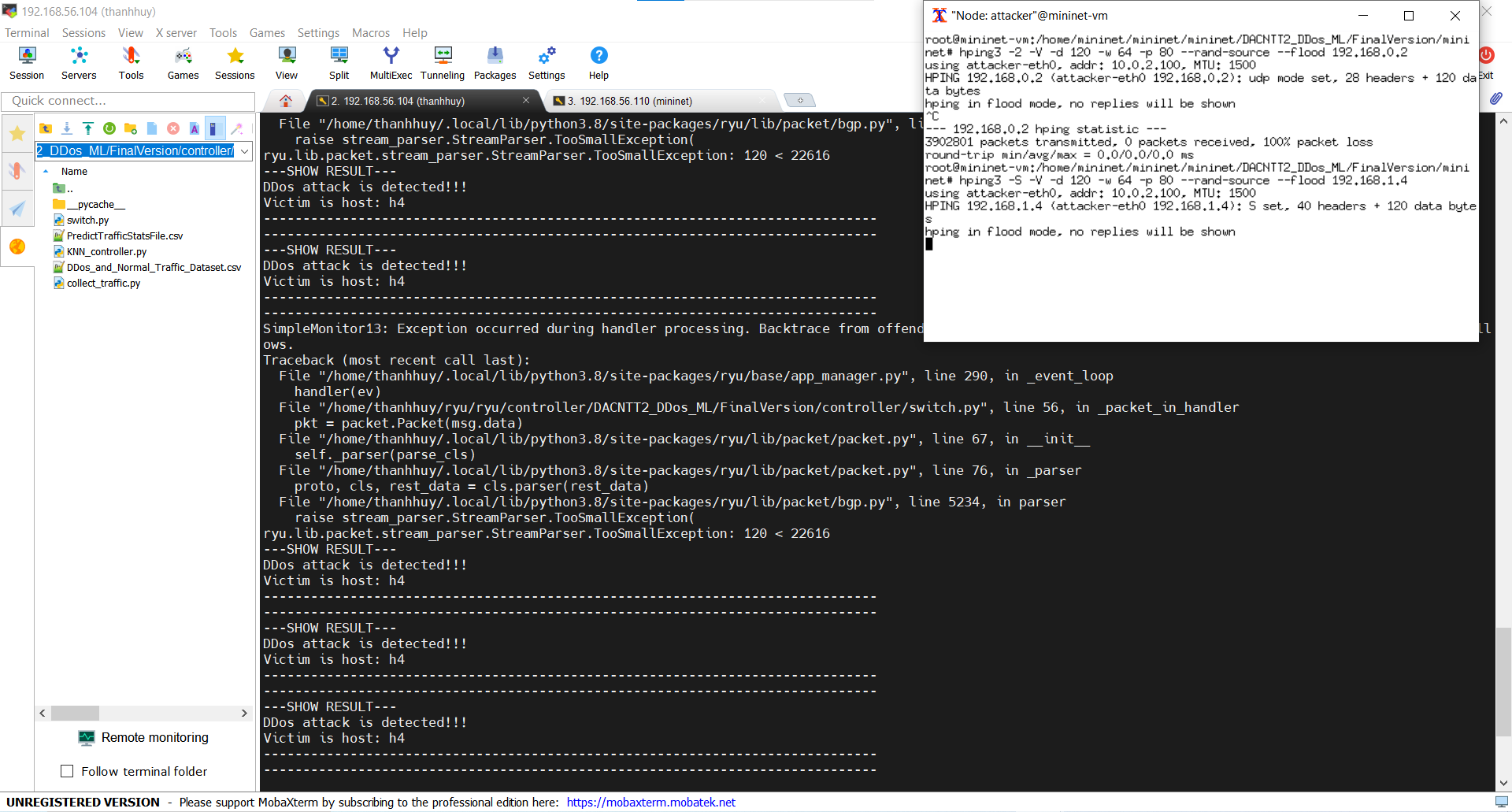




* Thực hiện tấn công TCP-SYN Flood tới h4

hping3 -S -V -d 120 -w 64 -p 80 --rand-source –flood 192.168.1.4





1. **Mitigation**
   1. Trên RYU

Cd tới path migitation

ryu-manager controller.py

* 1. Trên Mininet VM

sudo python topology

Chạy lại các lệnh tấn công ở phần 4 và kiểm tra sau khi phát hiện bị tấn công DDos thì port của host đó bị block.