TCP

SYN FLOOD DOS ATTACK

Mushfiqur Rahman (StudentID:2005107)
Arnab Dey Kabya (StudentID:2005112)

OVERVIEW

- Introduction
- Workflow
- Attack
- Methodology
- Result
- Conclusion

INTRODUCTION

- What is TCP SYN Flood?

A Denial-of-Service attack exploiting TCP’s connection establishment process.

- Goal of Project

Create a custom tool to demonstrate attack impact in a controlled environment.

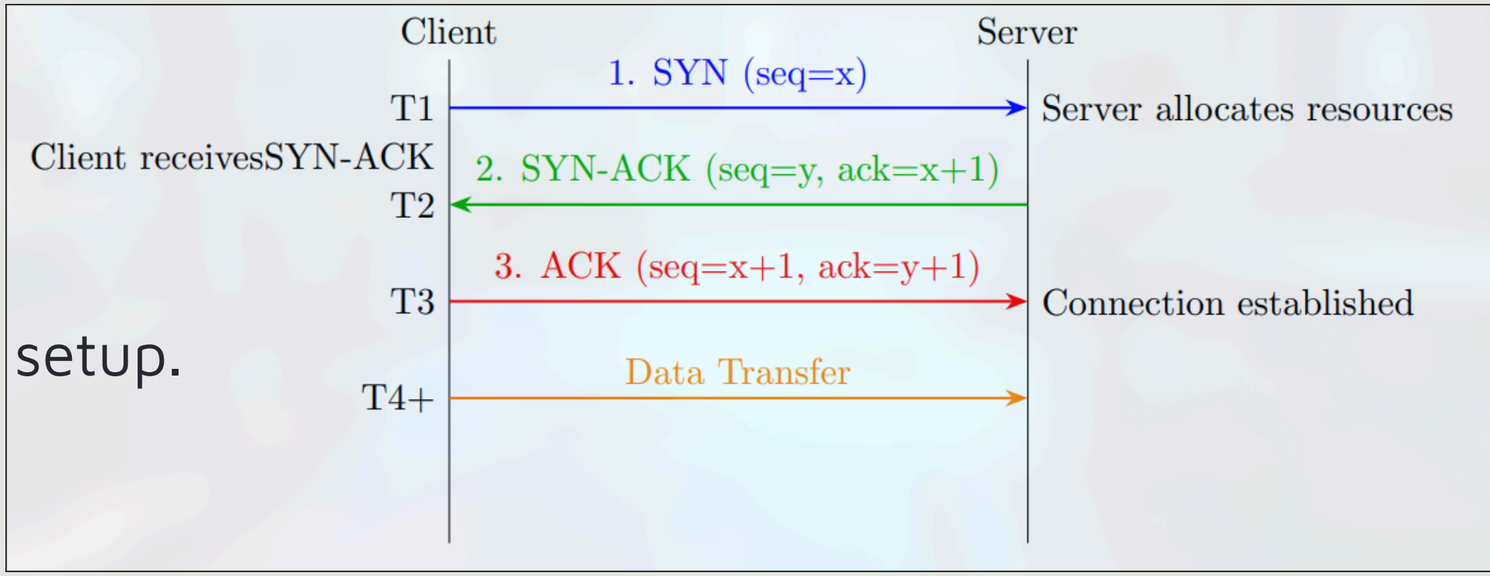
TCP THREEWAY HANDSHAKE

- Steps

SYN → SYN-ACK → ACK

- Purpose

Ensures reliable connection setup.

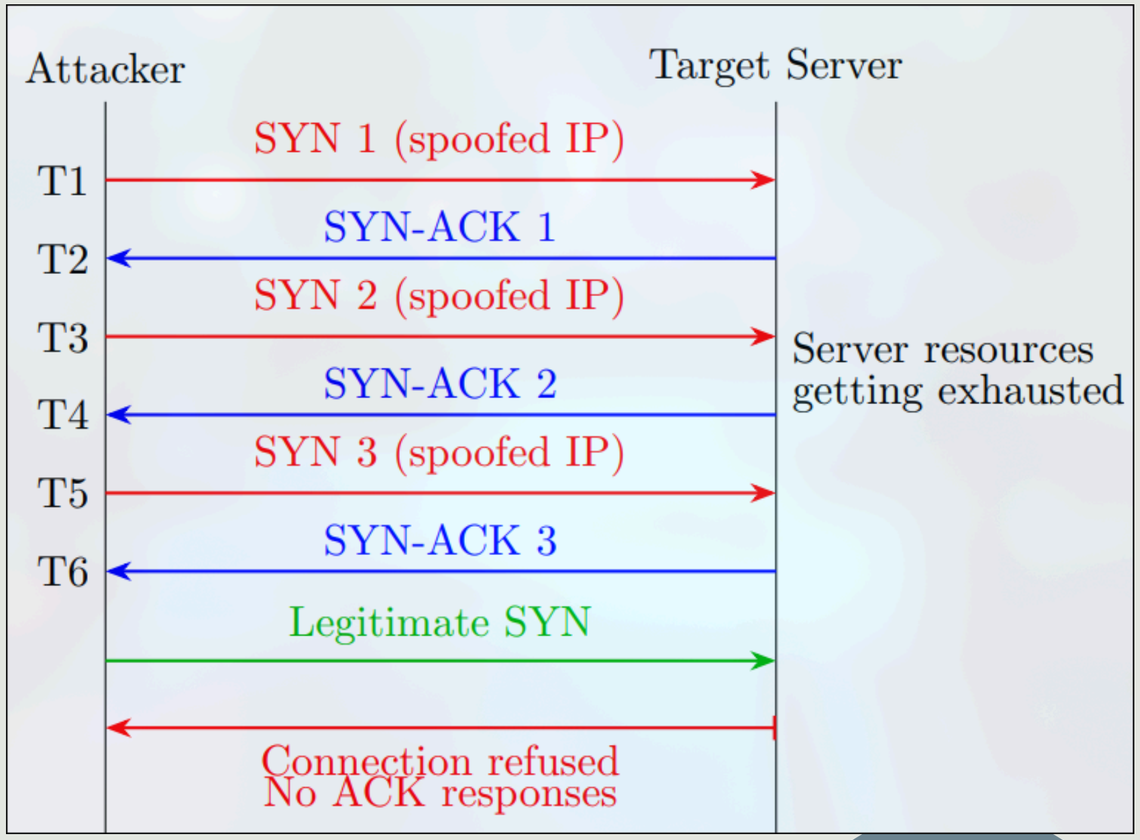


- Vulnerability

Server allocates resources after receiving the first SYN, even before handshake completes.

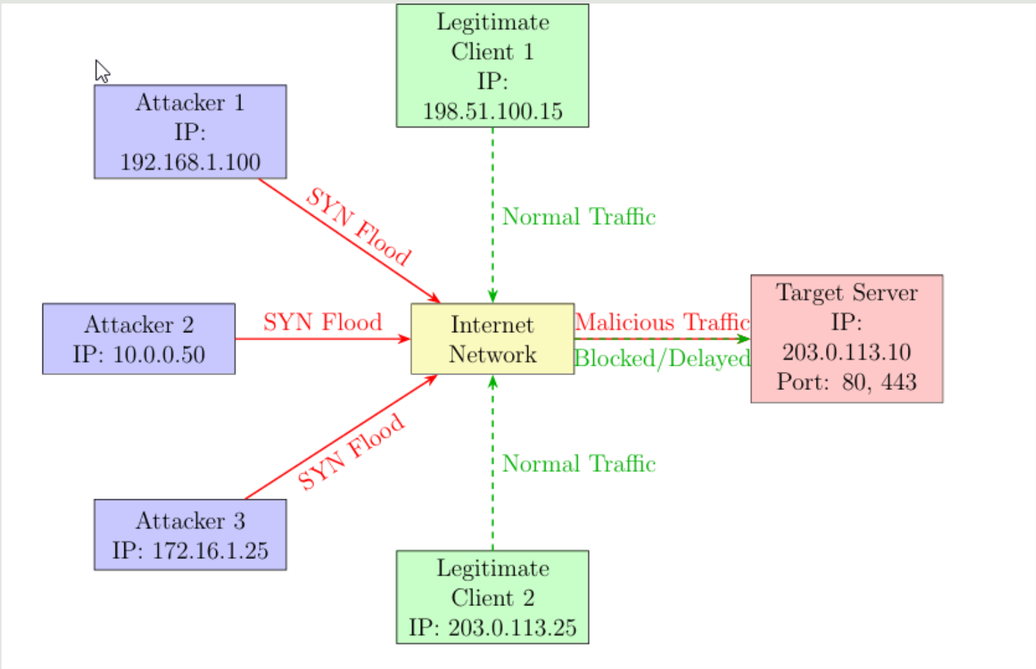
HALF OPEN ATTACK

- **Concept:** Send SYN packets but never complete the handshake
- **Impact:** Server's connection table fills, blocking legitimate users.



ATTACK TOPOLOGY

Attacker → Internet → Victim Server → Legitimate Clients



Spoofed source IP ensures SYN-ACK goes nowhere.

ATTACK TIMING

Normal Flow: SYN → SYN-ACK → ACK → Data Transfer

Attack Flow: SYN (fake IP) → SYN-ACK (lost) → backlog fills → service denied

PACKET CONSTRUCTION

- **Custom Packet Crafting**: Using Python raw sockets
- **Headers:**

1. **IP Header:** Spoofed source IP, manual checksum
2. **TCP Header:** SYN flag, random port & sequence number

- **Firewall Adjustment**: Prevent RST packets from attacker OS

ATTACK VARIANTS

No Spoof

IP Spoofing

IP NO SPOOF

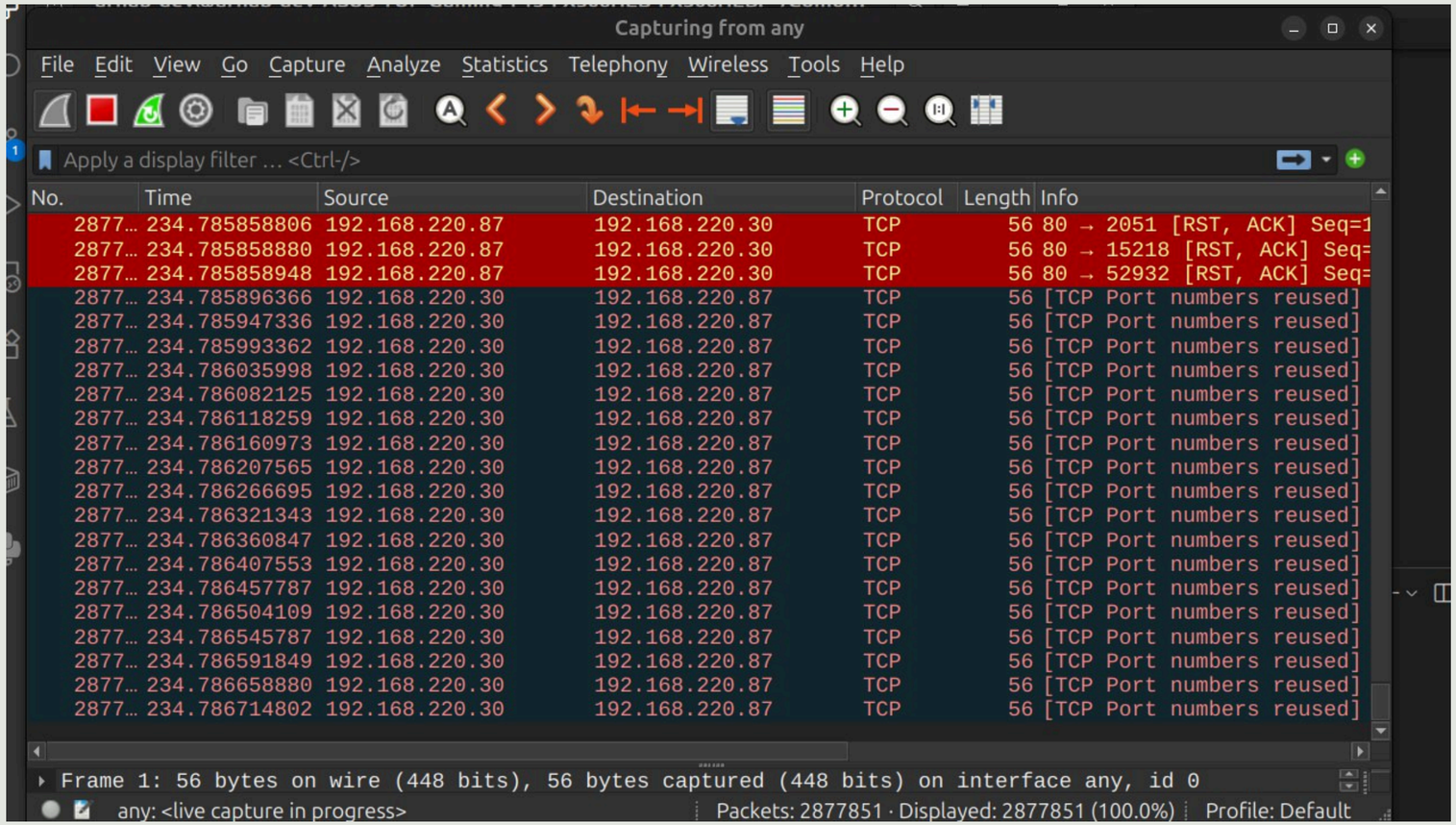


fig: attacker sends SYN packet

IP NO SPOOF

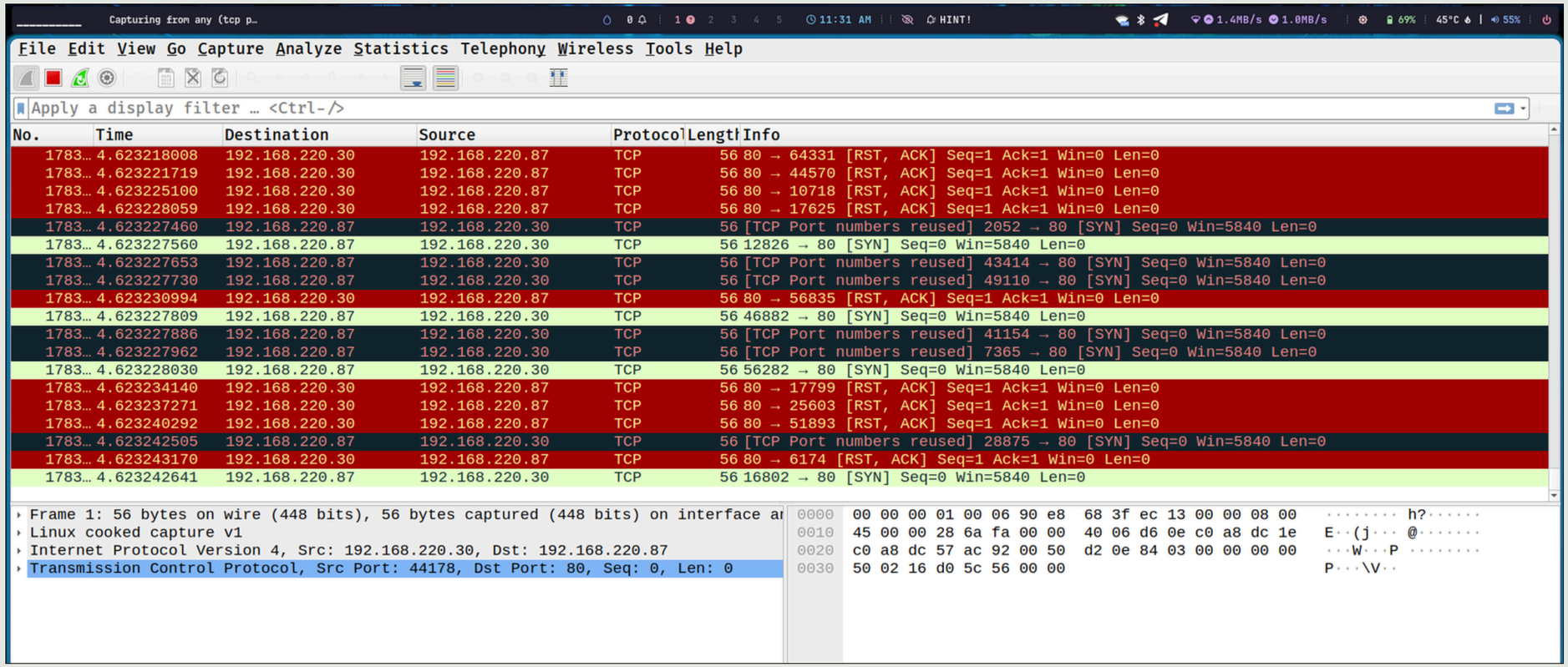


fig: victim receives SYN and sends SYN-ACK back

IP SPOOF

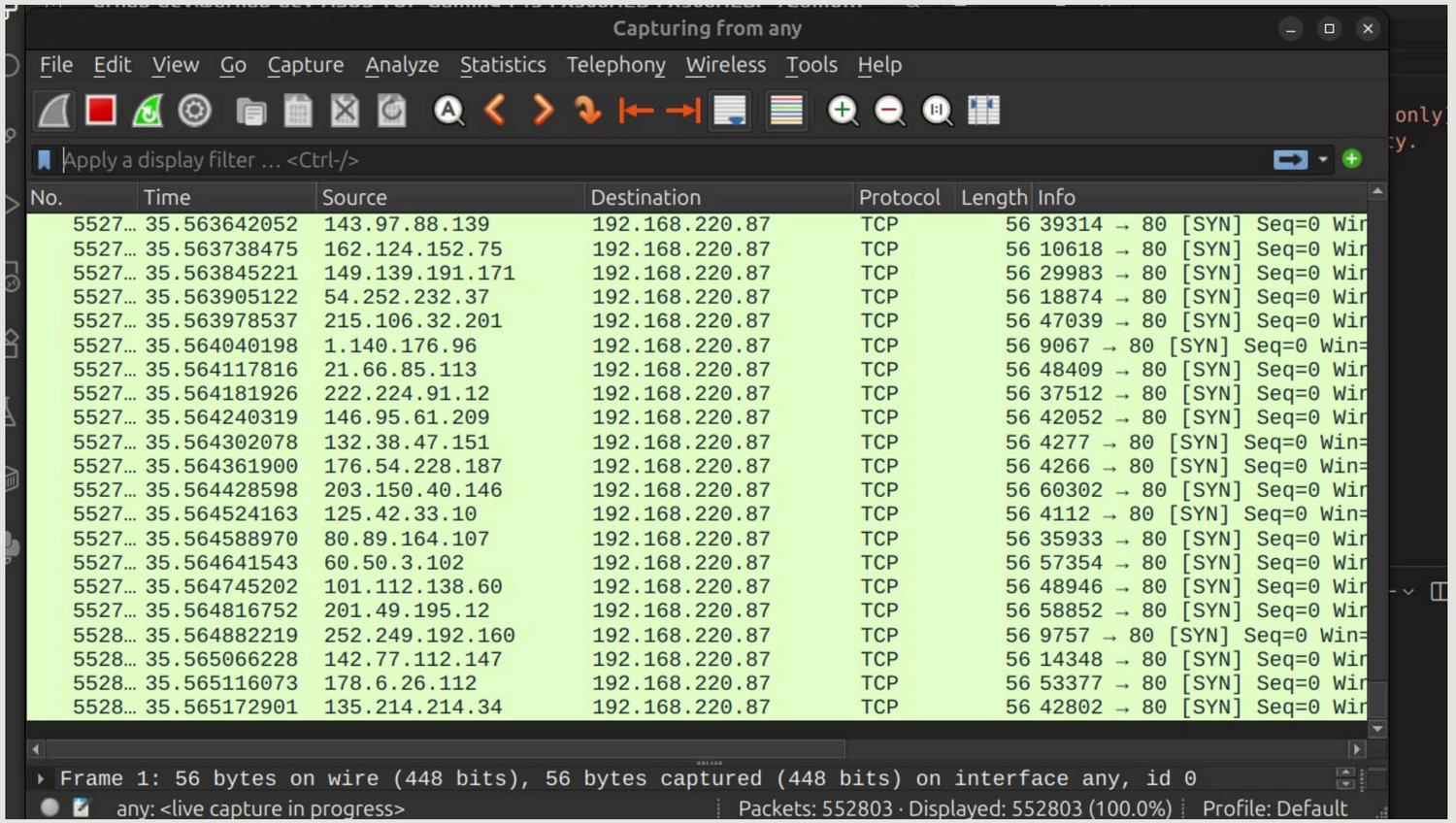


fig: attacker sends SYN packet

IP SPOOF

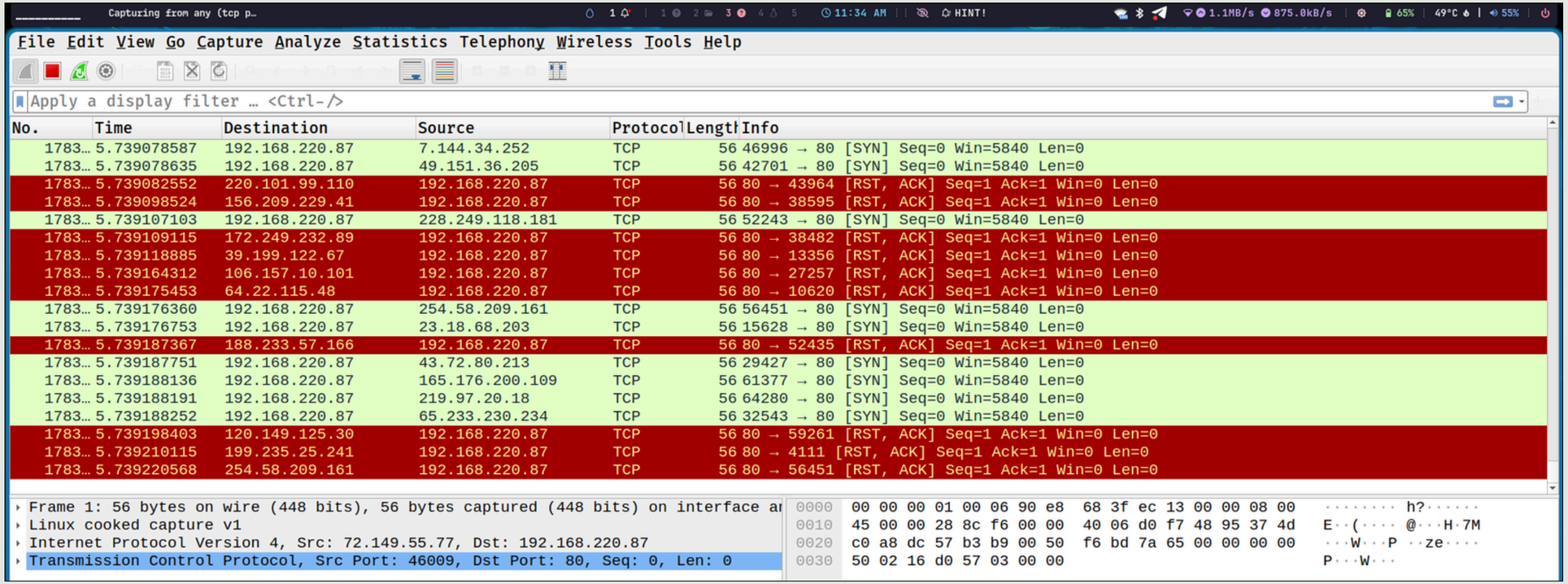


fig: victim receives SYN and sends SYN-ACK back

Thank You

For your attention