Classification and attribution for reflected Denial of Service traffic

Lauren Rudman
Supervised by Prof Barry Irwin

What is a DDoS attack?

- Attempt to make a machine or network resource unavailable to its intended users

- Takes advantage of compromised computers to attack a victim

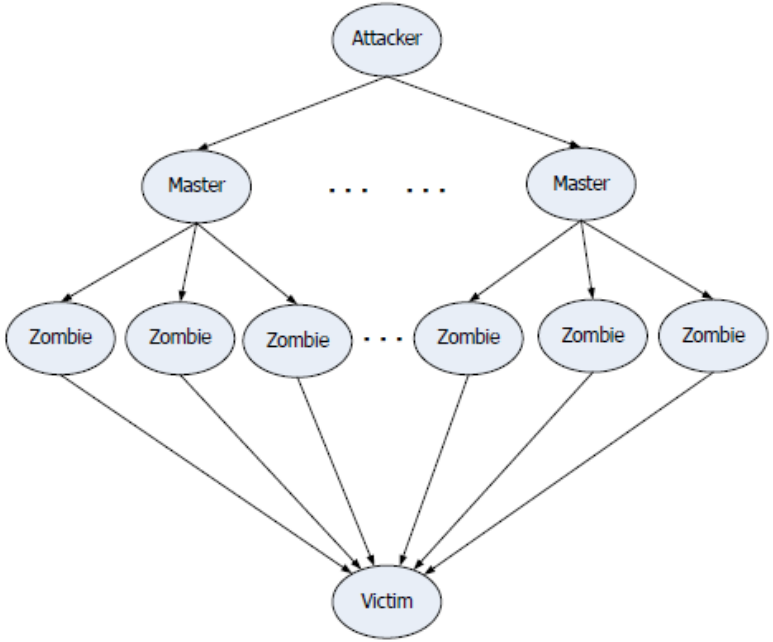


Figure 1. The structure of DDoS attack

Why are they a problem?

- Prevents users from accessing information or services
- Inconvenient
- Can have significant economic damage
- Widespread impact on users as ‘collateral damage’

Objectives

- A tool to process capture file (packets)
- The tool must indicate the probability that certain traffic is spoofed
- Potentially find the source of spoofed the traffic

What I have done so far…

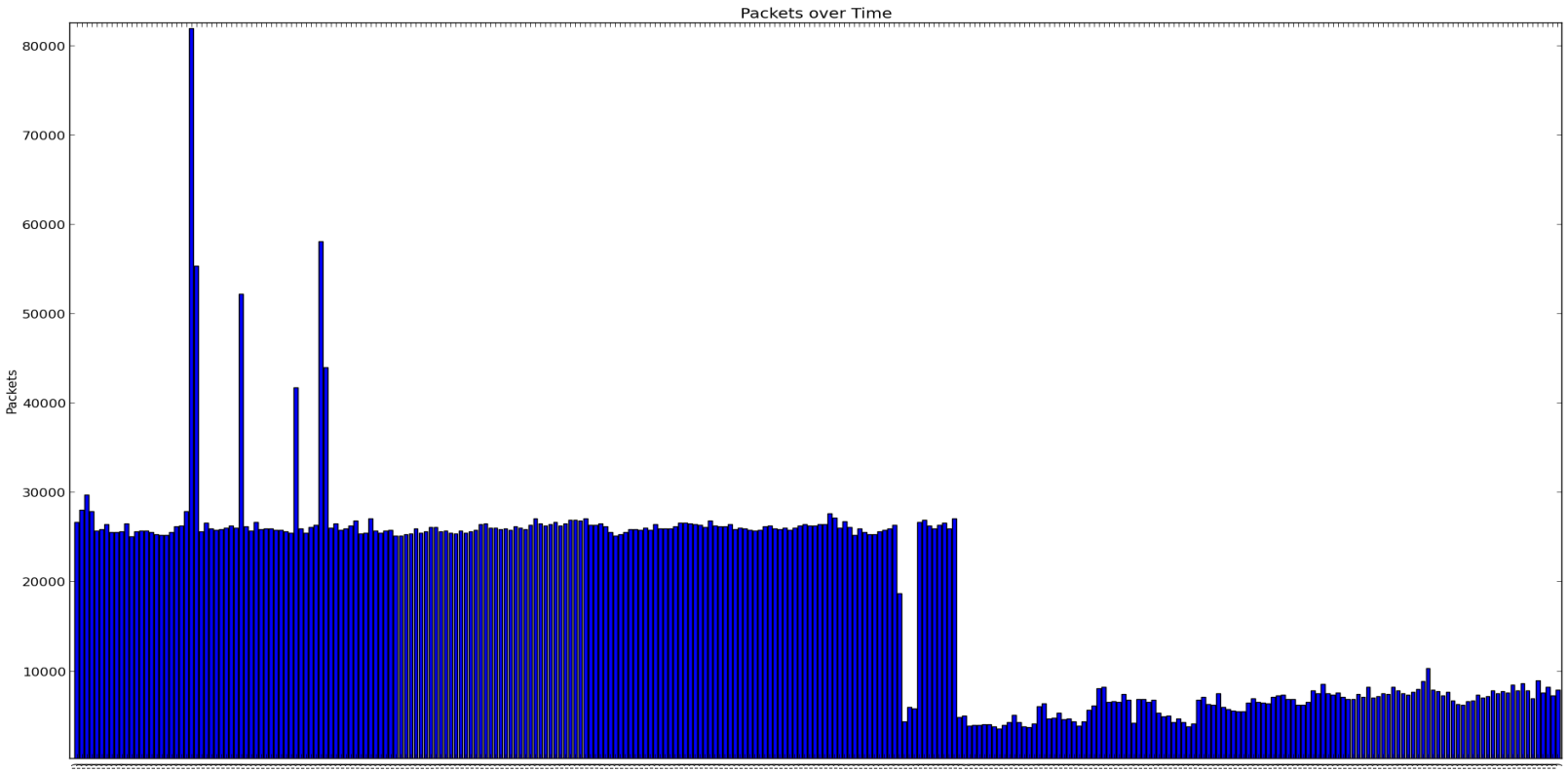
- Literature review
- Read papers
- Developed a Python framework to read in .pcap files and create graphs

The program: important libraries

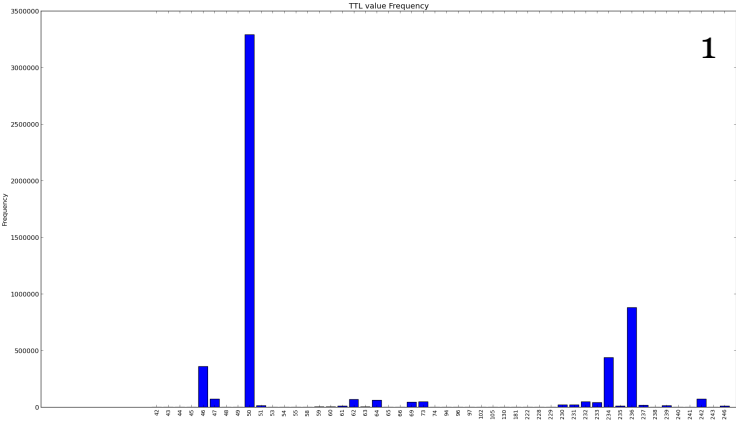
- dpkt
  - Used to parse the .pcap files

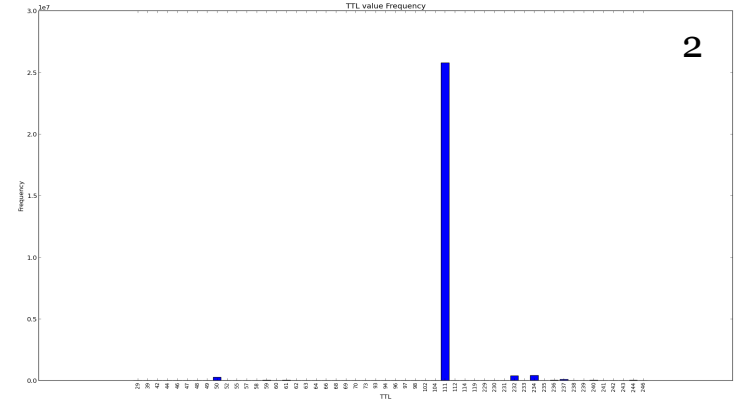
- matplotlib
  - Similar to Matlab
  - Used to plot the graphs

Graphs: packets per hour



Graphs: TTL frequency





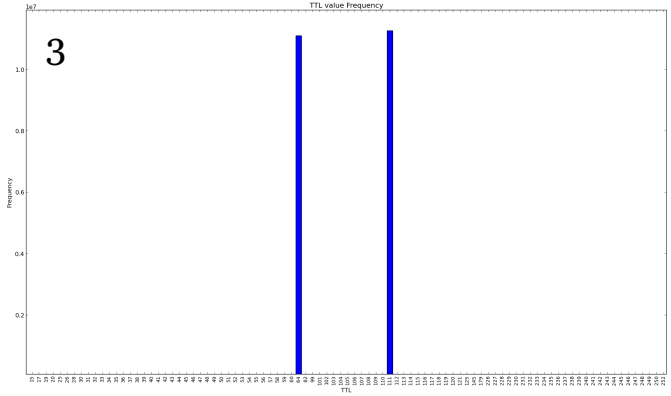
Always seems to be values that stand out

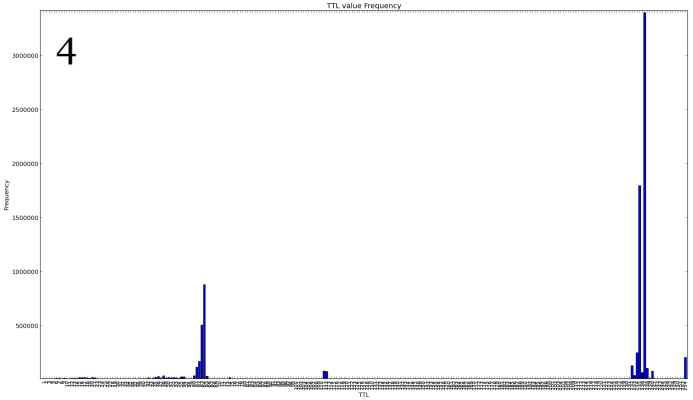
1. 50

2. 111

3. 64 and 111

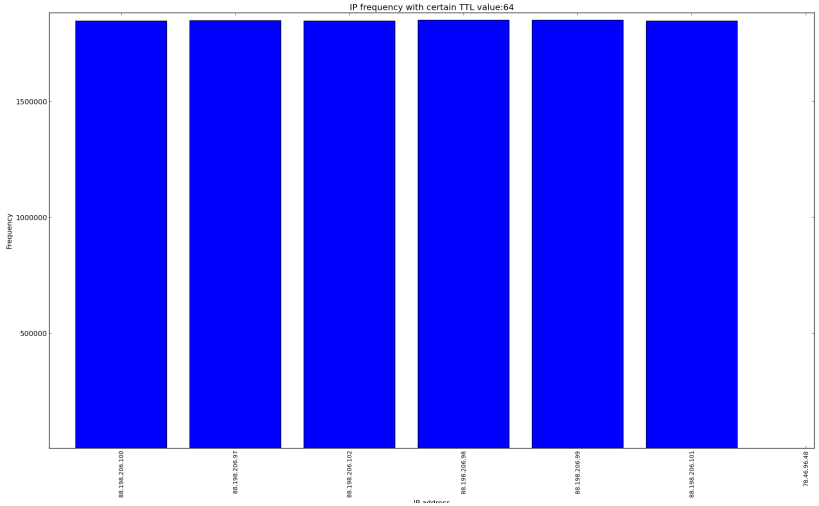
4. 237





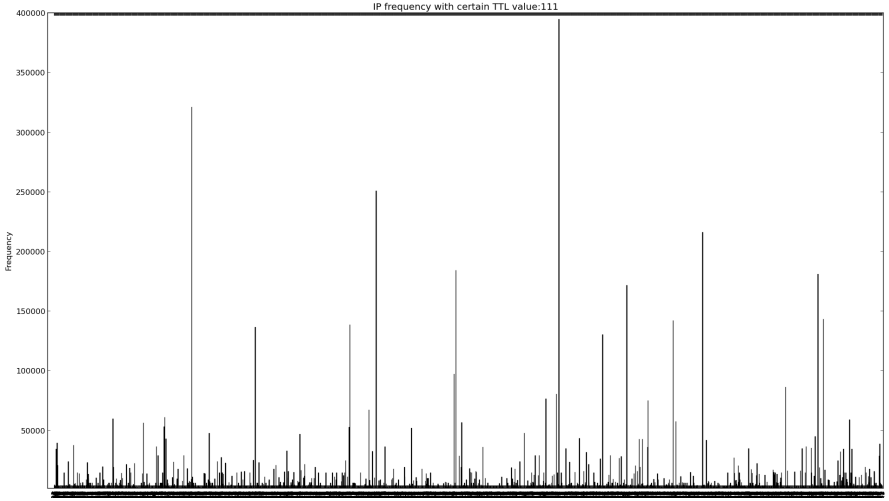
Graph 3: IP frequency for a TTL

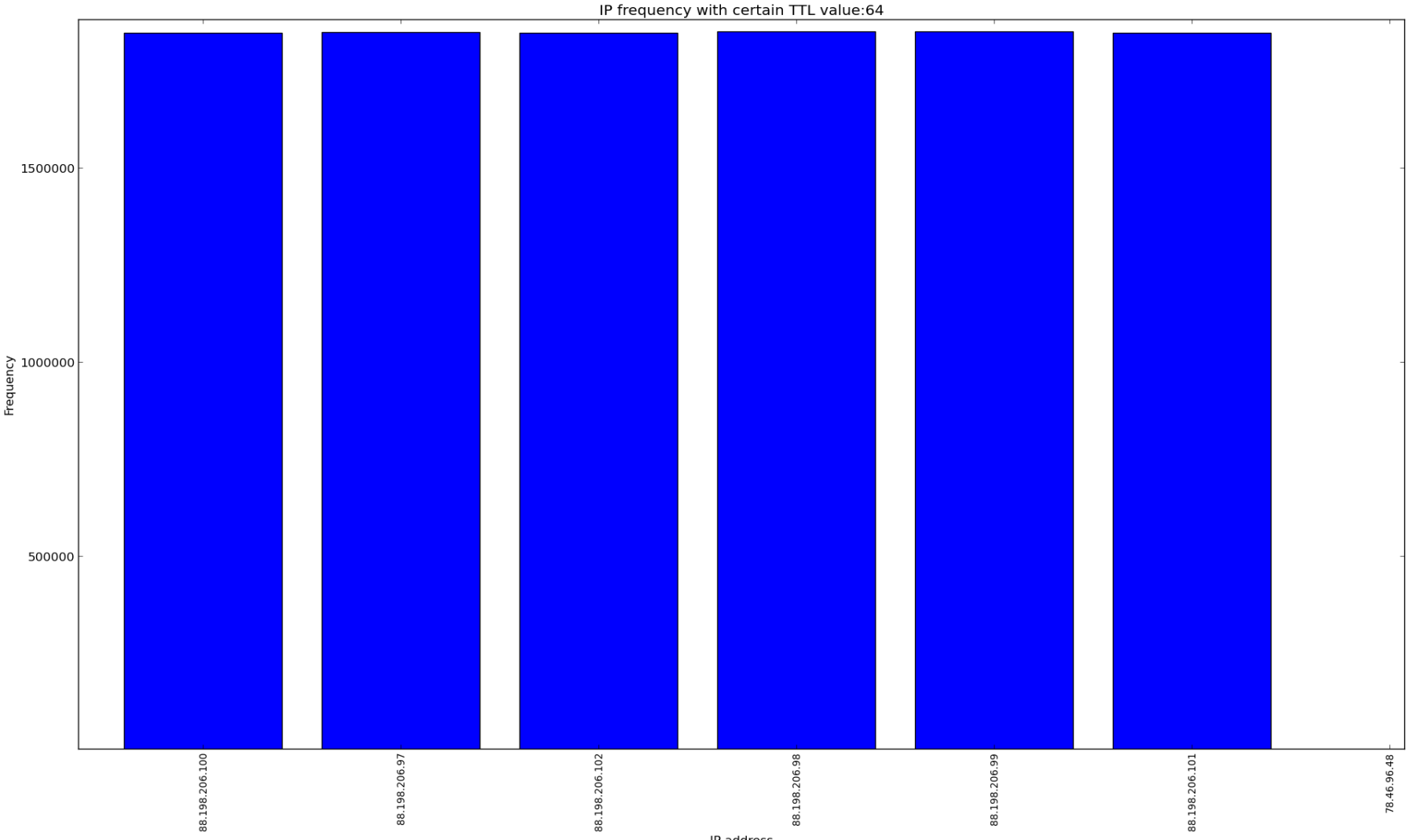
For TTL of 64: 7 IPs

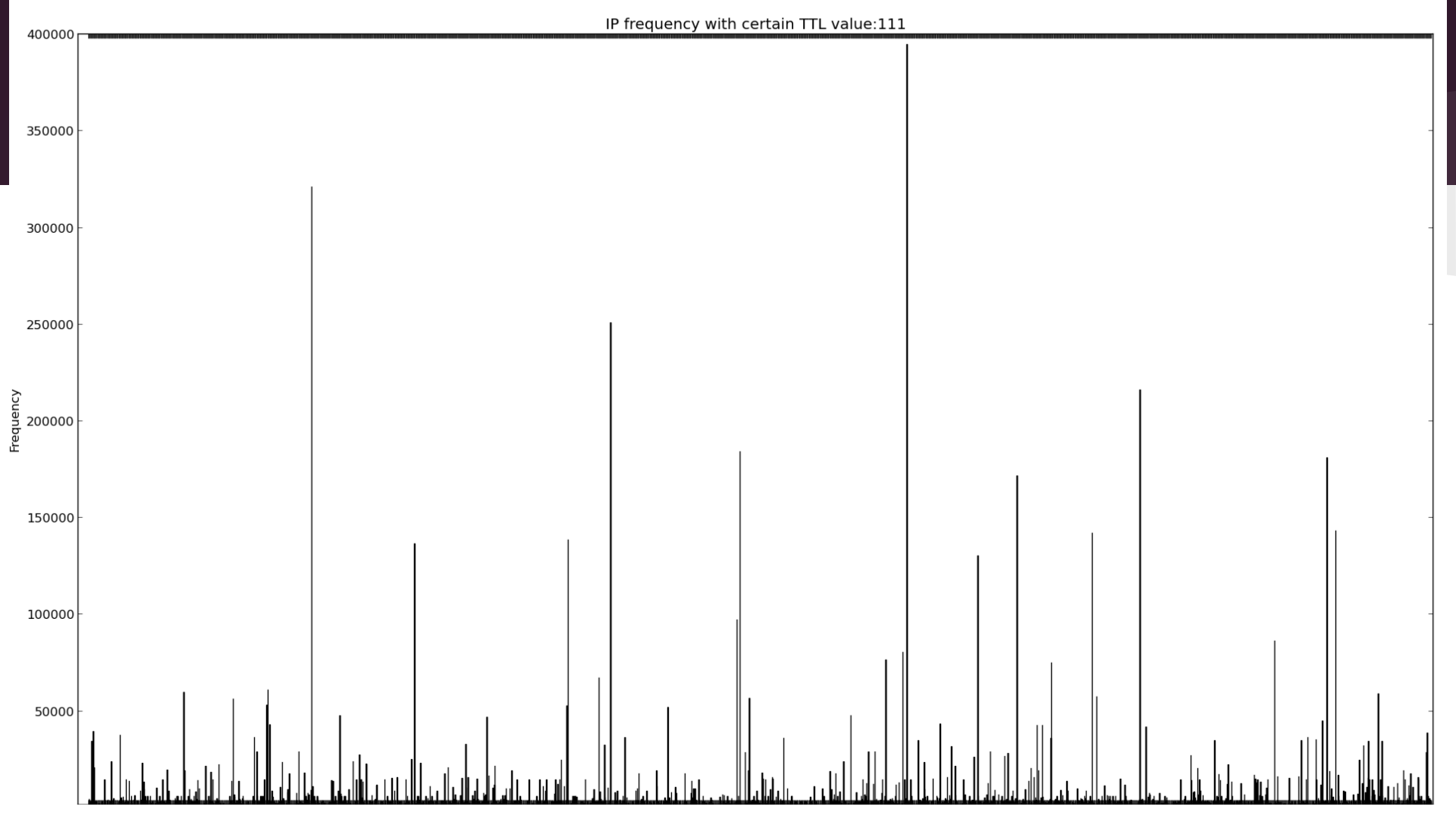


6 consecutive IP addresses

For TTL of 111: 2889 IPs




IP frequency with certain TTL value:64
Frequency
1500000
1000000
500000
88.198.206.100
88.198.206.97
88.198.206.102
88.198.206.98
88.198.206.99
88.198.206.101
78.46.96.48
IP address


IP frequency with certain TTL value:111
Frequency
400000
350000
300000
250000
200000
150000
100000
50000

Next steps

- Find the IP addresses with low frequencies that occurred before and during the attack
  - Could lead to the source
  - Matching TTL
  - Matching packet payload
- Draw more graphs comparing packet size distribution
- Analyse the traffic further
  - Use knowledge derived from graphs to build analysis program

Questions?