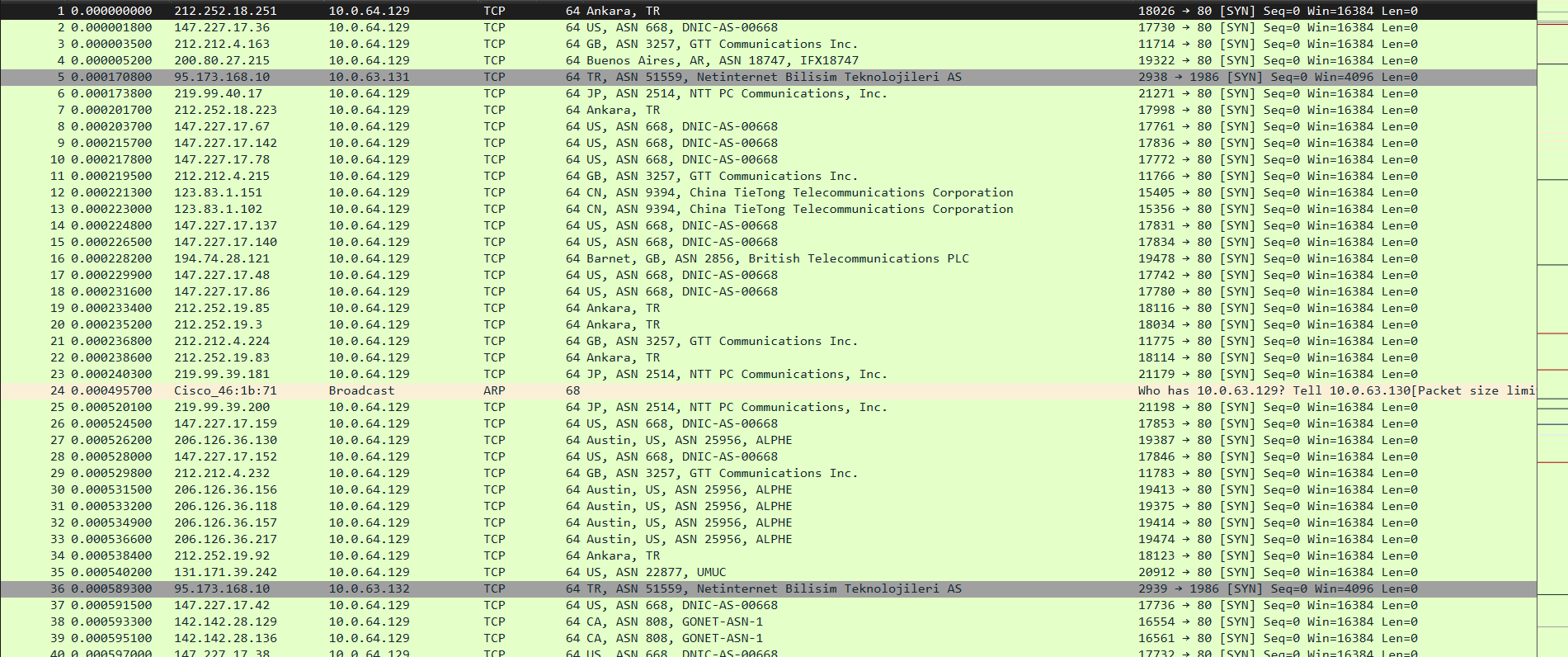
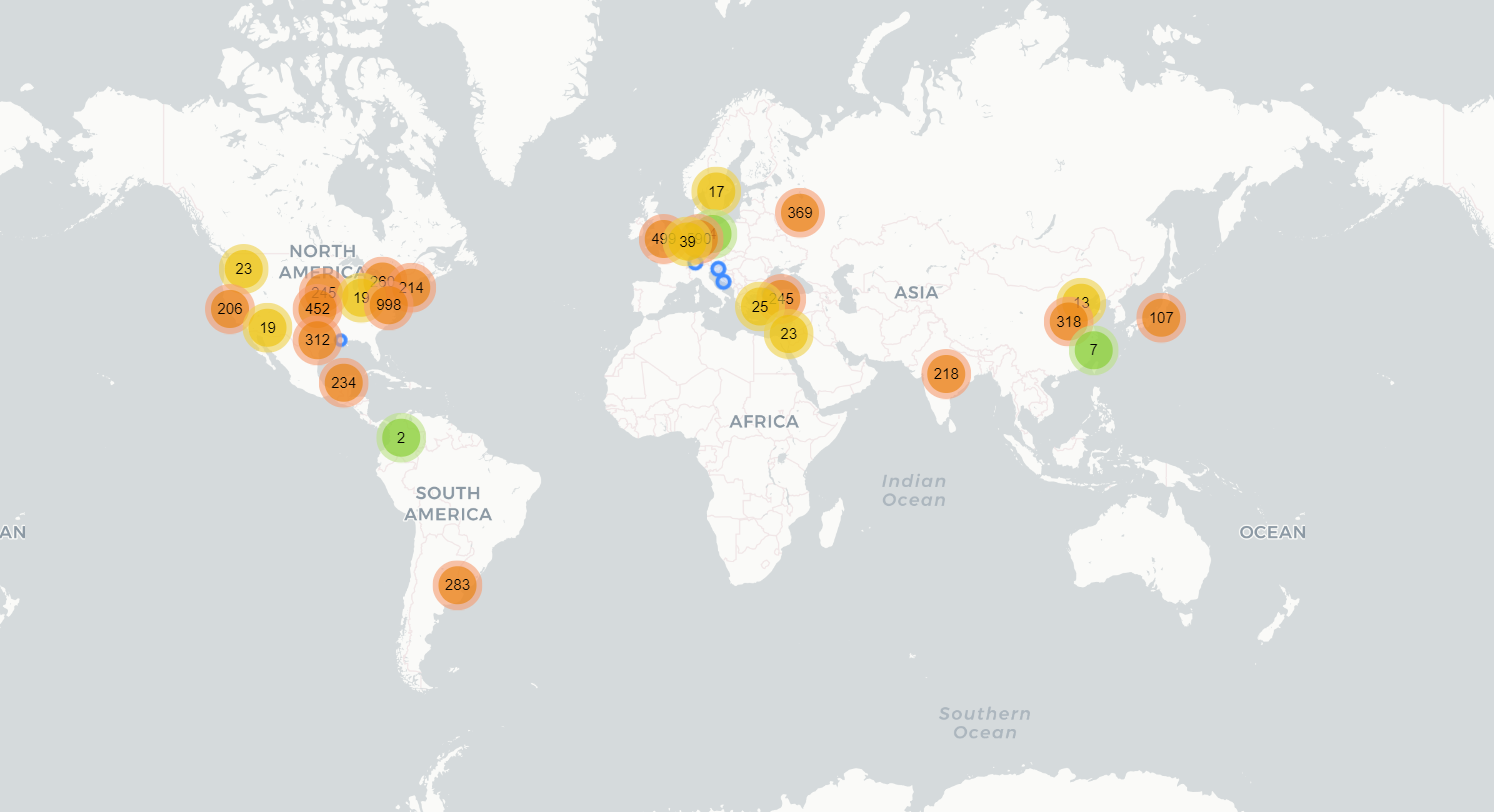
**Network Analysis task**

**Question and reasons of the investigation**

Why the server response time is high and it drops some requests ?  
  
**Report**



After analysing the network capture , there is definetly a Distributed Denial of service (DDOS) attack on server 10.0.64.129 in order to overwhelm the server with request because I see multiple IP Addresses from different location sending requests to the server.



And after tracking the packets source countries and cities using ip geolocation we discovered there is 19 countries involved in this attack , and the following countries and cities are involved in the attack

1-Argentina in city of Buenos Aires

2-Belgium in city of Brussels

3-Canada

4-China in both cities Wenzhou Tianjin and others

5- Colombia

6- Croatia in city of Split and others

7- Germany in cities of Dusseldorf ,Bonn ,Frechen ,Noerten-Hardenberg ,Nassenfels,Berlin,Cologne,Wesseling,Remagen,Stuttgart,Berlin,Bad Freienwalde ,Golzow,Bad Oeynhausen,Bergisch Gladbach,Rhede,Karlsruhe,Düsseldorf, Dortmund,Werl,Frankfurt am Main,Erlangen,Ludwigshafen am Rhein,Gaggenau and others

8-India

9-Israel in cites of Tel Aviv,Ramat Gan , Ness Ziona and others

10- Jaban in city Tokyo and others

11- Mexico in cites Campeche and Solidaridad

12- Russia

13- Slovenia

14-Sweden in city of Degerfors

15- Switzerland in city of Adliswil

16- The Netherlands

17-Turkey in cities of Guzelbahce , Ankara and others

18-United Kingdom in cities of London ,Acton ,Willenhall ,Barnet and others

19-United States in cities of Chandler,Baton Rouge,San Antonio,Ashburn,Baton Rouge,Charlottesville,Vinita,Omaha,Muncie,Oakland,Indianapolis,Southborough, Tappahannock,Walla Walla,Benton City,Austin,Dallas

After analyzing the network capture, I suspect that it is a coordinated botnet attack because we observed a large number of requests coming from a limited set of IP addresses. This indicates a coordinated attack from a botnet.

**Future detection**

I have noticed that all packets have TTL with value 254

Normal TTL Behavior: Every packet has a TTL value, which represents the maximum number of hops it can traverse. As the packet moves through routers, the TTL decreases by one at each hop.

Baseline Establishment : Create a baseline or normal range of TTL values for your network under regular conditions. This baseline reflects the typical number of hops between different parts of your network.

Anomaly Detection: Monitor TTL values in real-time. Sudden deviations from the established baseline could indicate a problem.

TTL Exhaustion: In a DDoS attack, attackers may flood the network with packets, deliberately setting TTL values to very low numbers. This causes routers to quickly discard the packets, generating a large number of ICMP Time Exceeded messages.

Detection of Unusual Patterns: Look for unusual patterns, such as a flood of packets with TTL values outside the normal range. This could suggest an attack.

Thresholds and Rate Limiting: Implement thresholds for acceptable TTL values and consider rate limiting. If incoming packets exceed expected limits or if TTL values fall outside predefined thresholds, it may indicate a DDoS attack.