Digital forensics project – Question 1

As a forensic examiner, you are required to analyze the given capture file using Wireshark and answer the following questions in your report: <https://drive.google.com/file/d/16GR5hpLa-Jlo7HcJiN2BFAIMLO0I3IG5/view?usp=sharing>

* 1. Is this an Att­ack? Justify your answer.

**Yes, it is a Distributed Denial of Service attack (DDoS)**

**Justification**:

* Different source IPs are sending to the same destination IP (attempt to overwhelm a target system or network with a flood of traffic).
* [Packet size limited during capture] -- Was repeated multiple times which indicates a big traffic of data was being forced into transmission.
* Distinct/unexpected protocol (ARP) repeated multiple times which might indicate for ARP spoofing or cache poisoning which is an attack. – **What is ARP???????**A screenshot of a computer

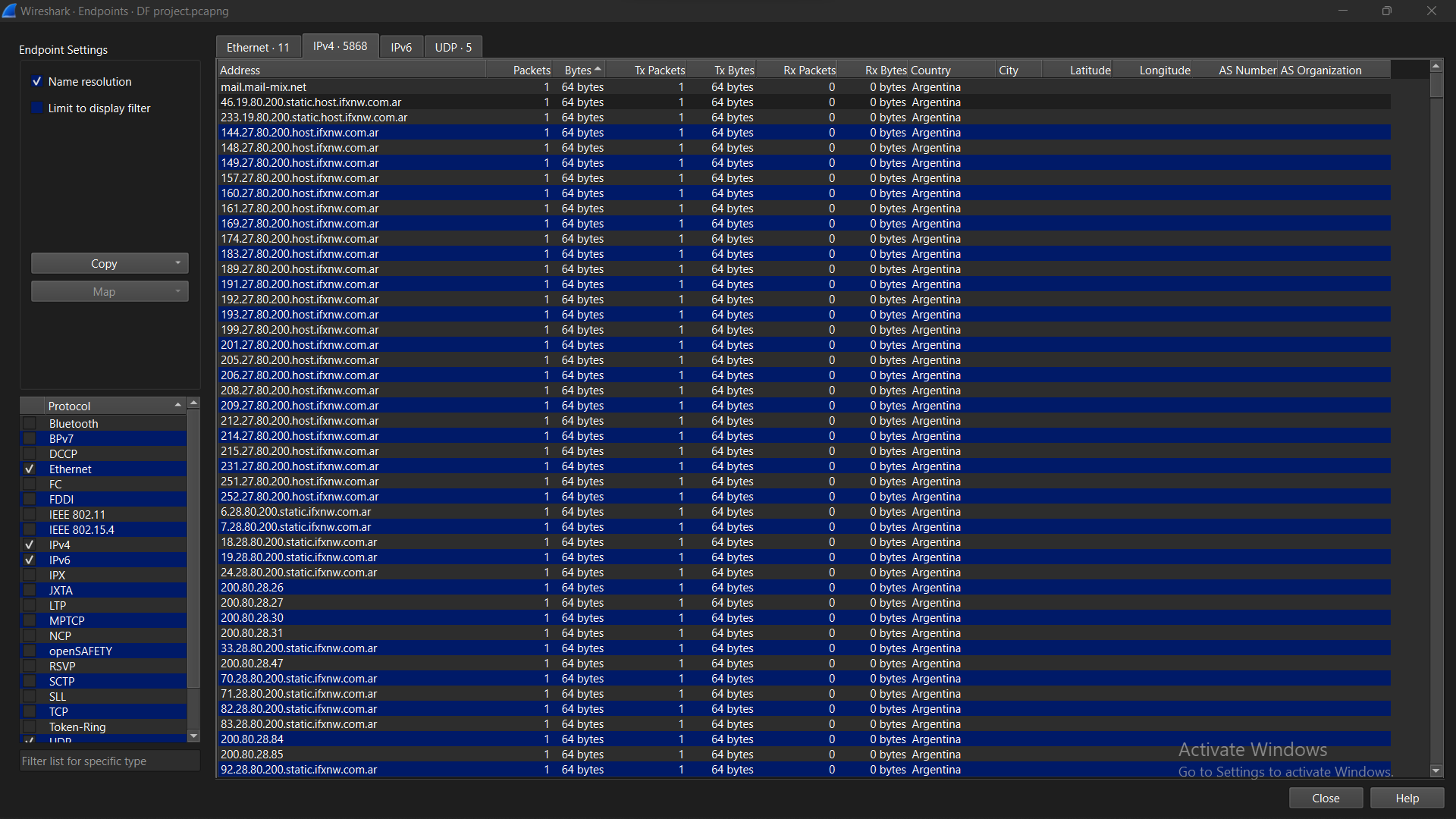
  Description automatically generated
* Unusual source/destination ports (Greater than 1024)*A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generated*
  1. Discover the source geo IP country? (do your own research)

**Argentina**.

Sorting by "Bytes" displayed IP addresses based on the number of Bytes sent:



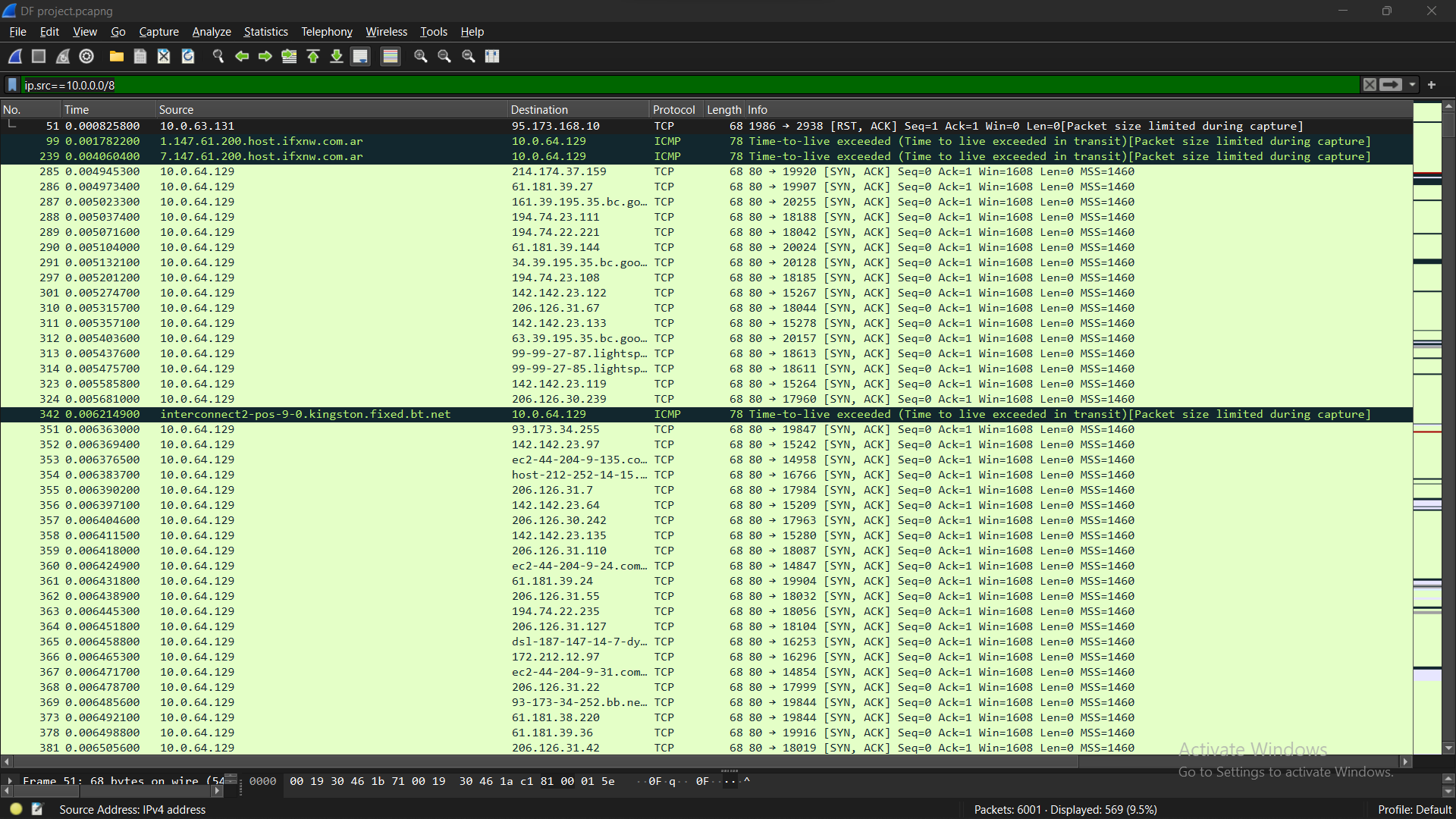
* 1. How many countries are involved?

**19 countries**.

* Argentina, Canada, China, Germany, India, Japan, Mexico, Russia, Turkey, UK, US, Belgium, Australia, Sweden, Switzerland, Colombia, Slovenia, Netherlands
  1. Choose any of the identified locations in Question 2, how many packets come from the location you choose? Mention the location and the number of packets.

I choose the **United States (US).**

Number of packets: **569**



* 1. Are these packets made by a pot or normal devices?

Packets are made by normal devices.

* (Most of them are with source /destination MAC addresses from Cisco.
* No environmental metrics were shown.
* Looked for protocols that might indicate IoT devices communication and there were none.
  1. Extract the TTL of the packets and show how it can be used in discovering attacks.

**TTLs of the US packets:**

* **255 – “**The maximum TTL value”. It could suggest potential packet spoofing, as the packet might have originated from nearby or directly from the source rather than going through multiple network hops.
* **254 – “**A common initial TTL value set by many operating systems”. Might indicate altered routing paths or attempts to blend in with normal traffic by setting TTL to a commonly expected value.
* **248, 247, 246, 245 and 243** – Might indicate a typical number of hops for certain types of traffic. Could indicate route manipulation, altered traffic paths, or potential attacks like packet injection.
* **127, 126, 63 and 62** – “Intermediate TTL values”. Sudden changes in TTL values compared to the normal for specific traffic could indicate anomalies, route manipulation, or traffic redirection attempts.
* **52 and 47** - Unexpectedly low TTL values for specific traffic might suggest potential spoofing or route alteration.