Network Topology Visualization

Michel de Boer - s1011542
Lorenzo Casini - s1062069
Onno de Gouw - s1025613
Stefan Popa - s1027672

Group 4 | Advanced Network Security
Radboud University
13-12-2021

BGP Network Topology

- **Goals**
  - Define and measure nodes of interest
  - Gather data with the right tools
  - Visualize results

Tools

Data Gathering

- Icmplib
- Ipinfo
- Aslookup

Visualization

- Django
- Jquery
- Chart.js
- Openlayers

Debugging

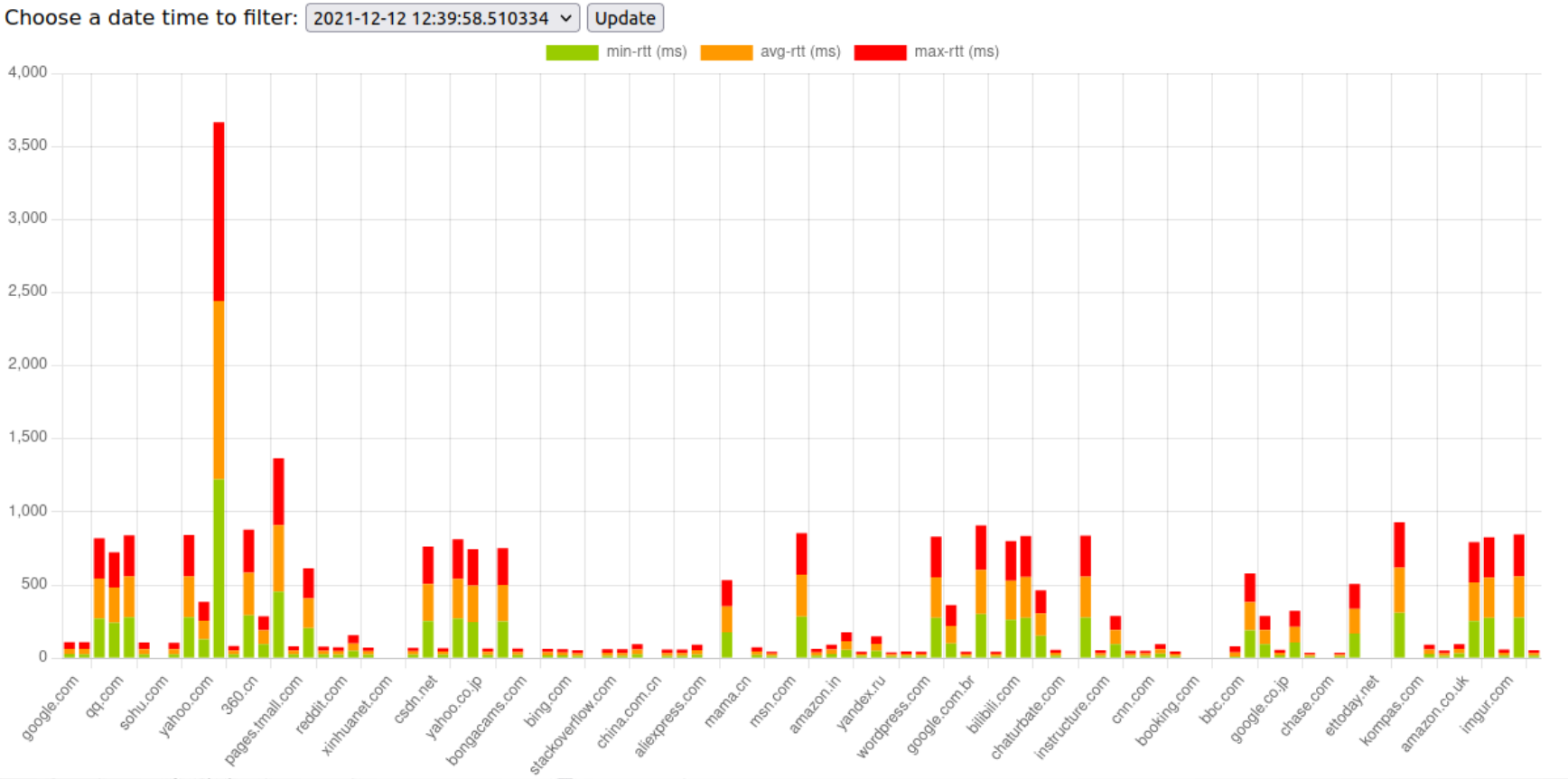
- Wireshark
- Dropwatch

Measurements & Data

- Measurements:
  - Parsing handled by packages
  - Stored using Django database model
    - SQL access and insertion
  - Data extracted and converted to JSON
- Data:
  - Top 100 websites
  - Newspaper websites + social media
  - VPN

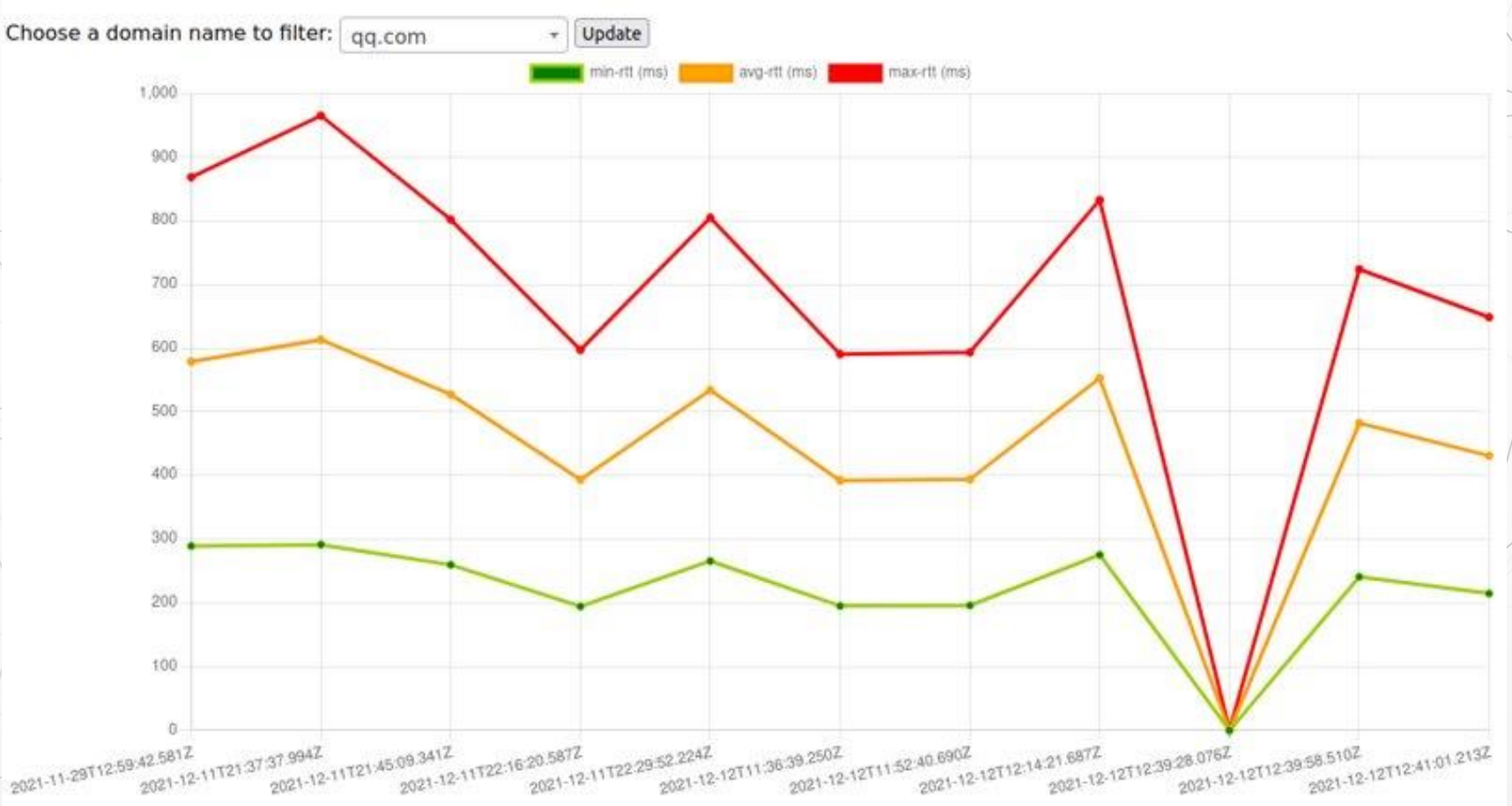
Ping Visualization

- Min-rtt, average, max



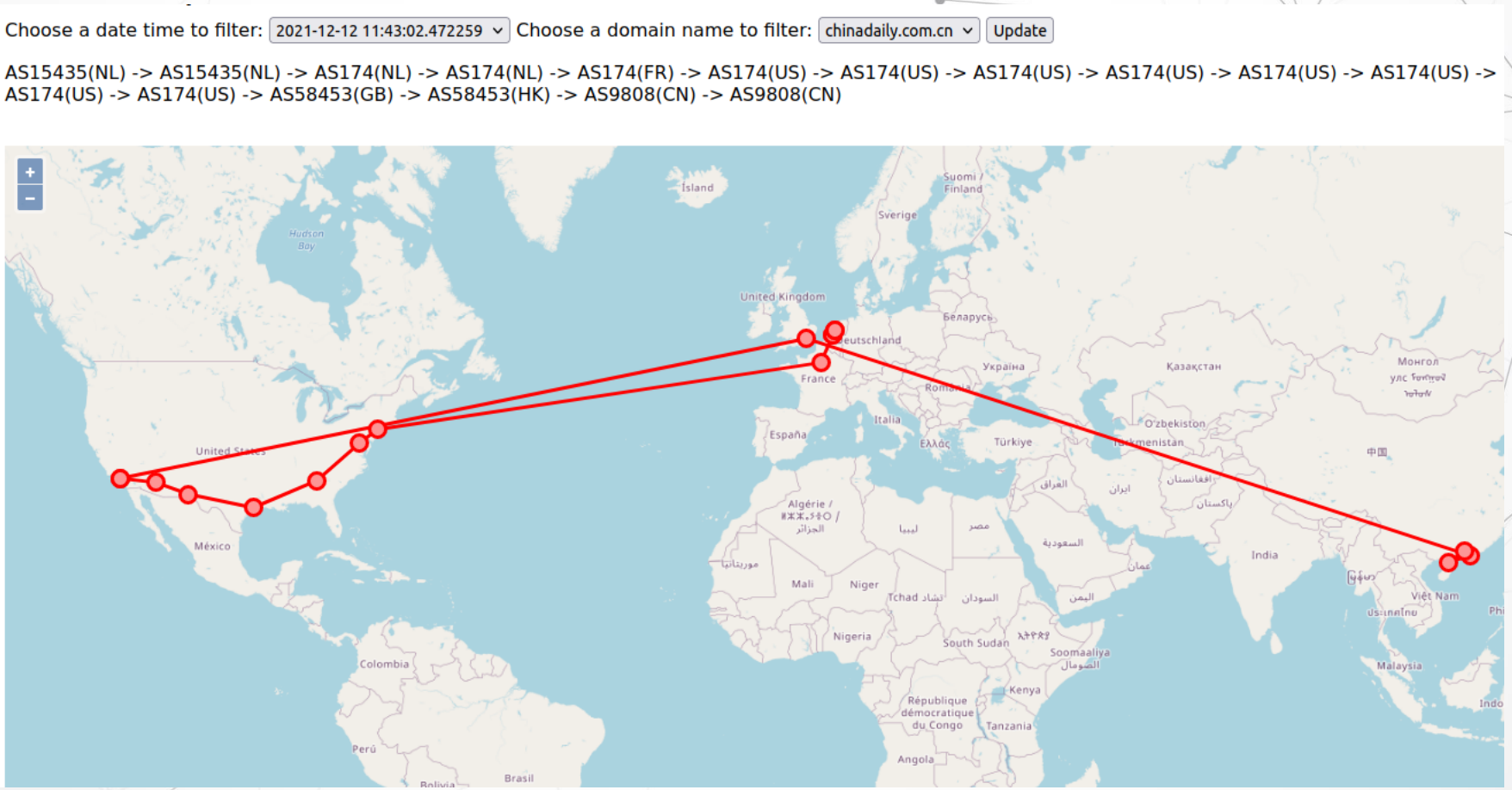
Ping Visualization

- Timeline visualization for host



Traceroute Visualization

- AS number + Countrycode path and Map (geolocation)

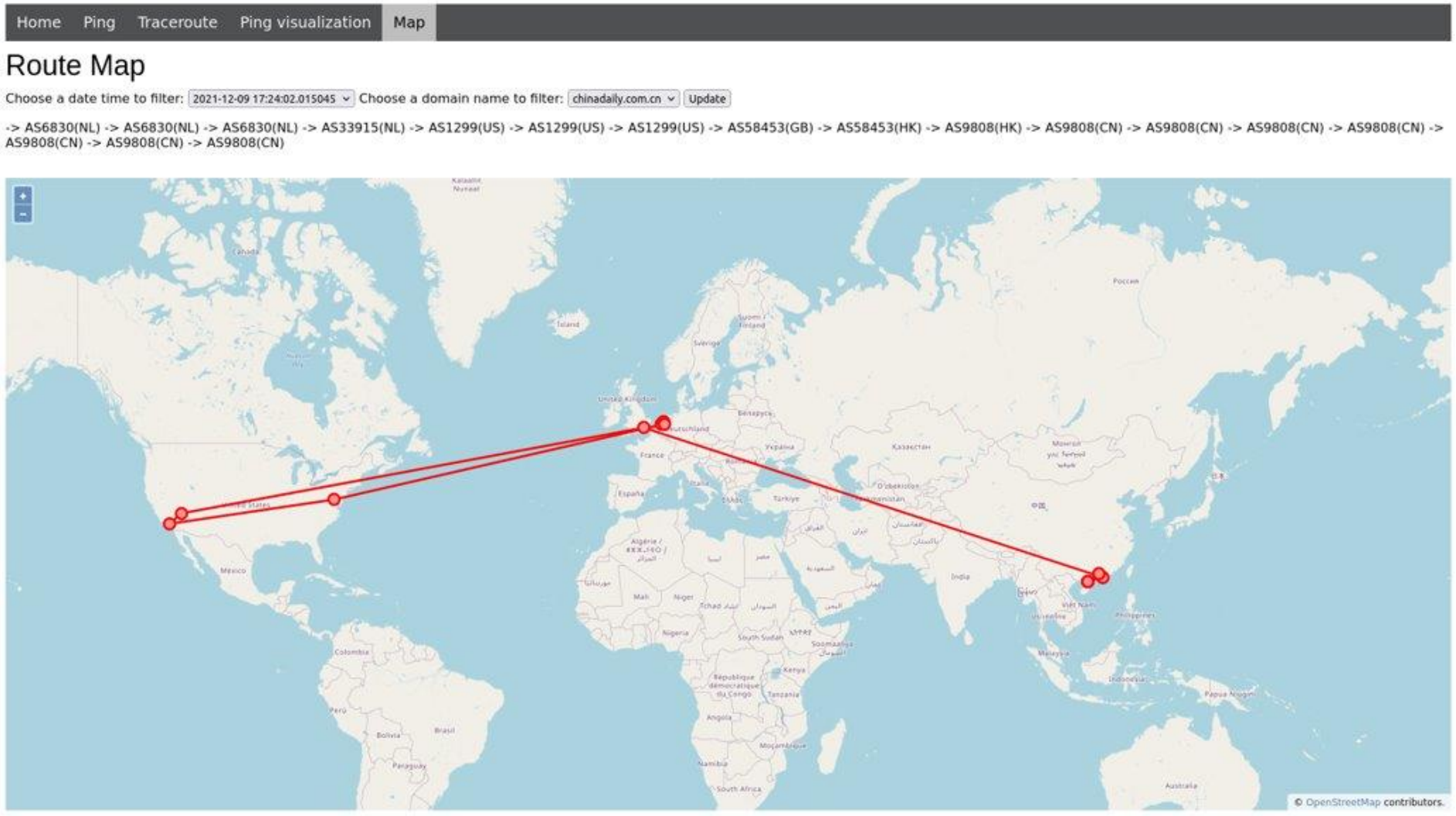


DEMO

Results

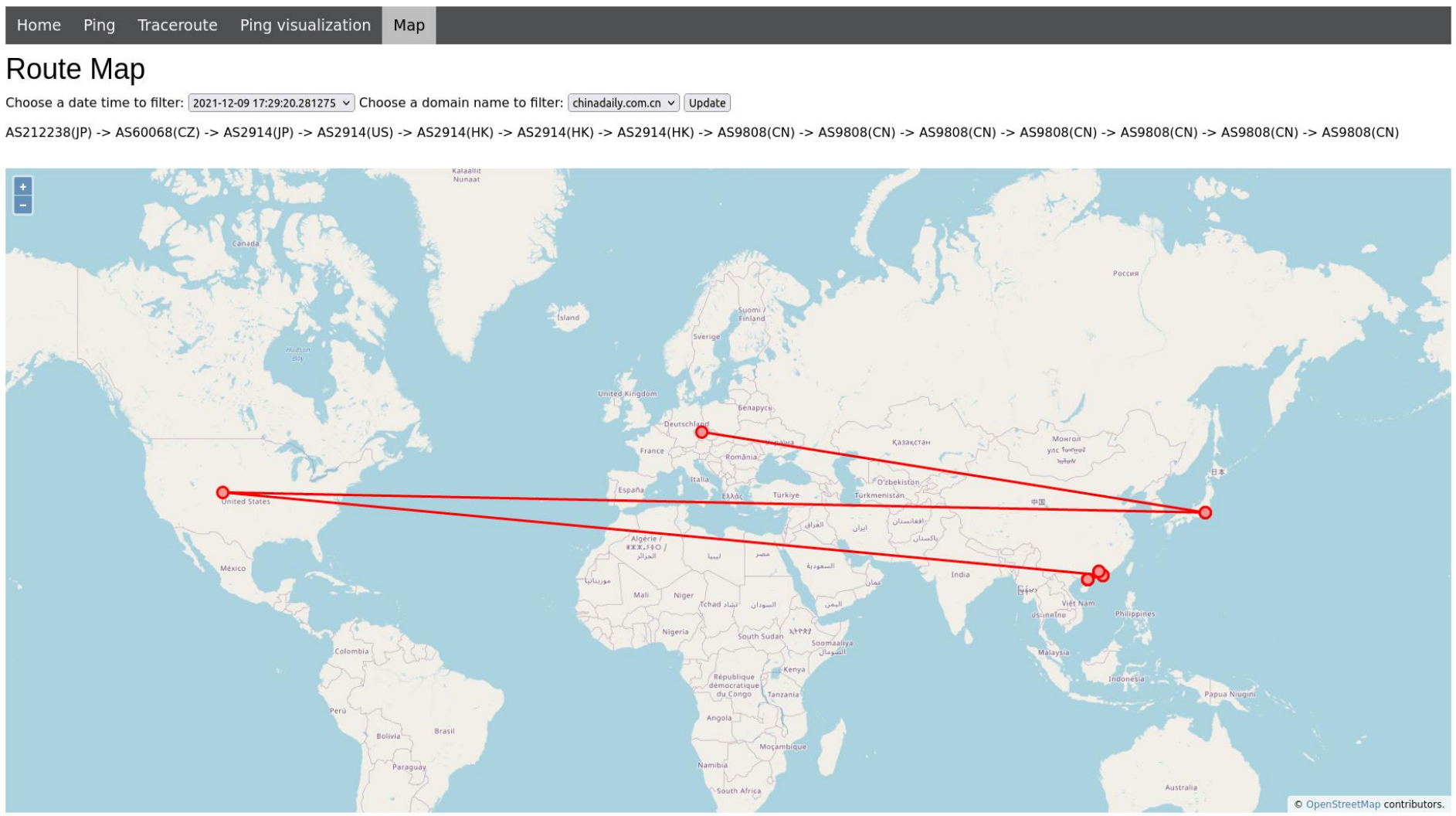
- Chinadaily.com.cn
- No VPN vs. VPN

Chinadaily.com.cn (No VPN)



Chinadaily.com.cn (Japan: VPN)

Note: Starting point is visited twice sometimes!



Limitations

- Corelation ping & traceroute
  - Possibly different paths
- Use 1 specific API/database for the GeoIP lookup
  - Different API's might return different locations
- Difficult to explain routing decisions
  - No ground-truth
- Network unreliable
  - Packet drop by kernel if hugely parallel
  - Debugging can be difficult and time consuming (dropwatch, wireshark)

QUESTIONS?