**Lab 04: Assignment: Tracert Utility Analysis & Advanced Scapy Tracert Utility**

**Vishwas S**

**2201CS78**

1. Purpose of ping:

The tracert (or traceroute on Unix-based systems) utility traces the route packets take to reach a network host. It identifies each hop between routers and measures the time taken for the round trip.

Basic syntax:  **tracert [options] destination**

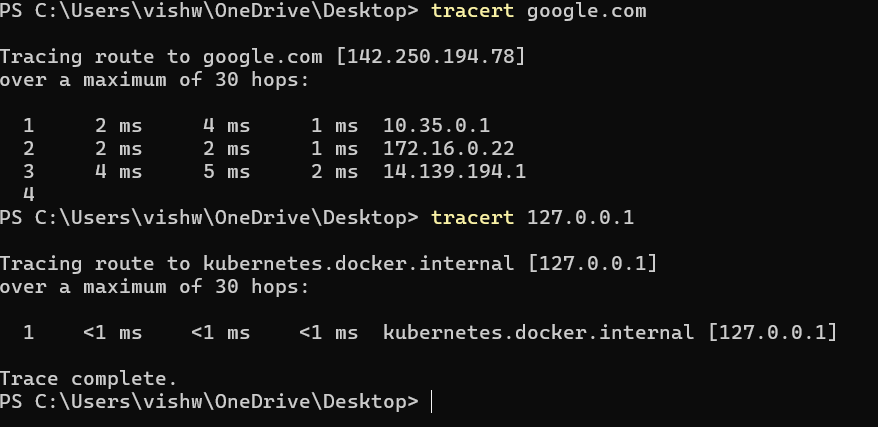
destination can be an IP address or a hostname.

Examples:

To test connectivity to a website: **tracert google.com**

To test connectivity to a local host: **tracert 127.0.0.1**





**Analysis:**

tracert to a website:

* **Tracing route to google.com [142.250.194.78] over a maximum of 30 hops:**: The tracert command is tracing the route to Google's IP address with a maximum of 30 hops.
* **Hop number**: The sequence of routers between your machine and the destination.
* **RTT**: The round-trip time for packets to reach each router and return.
* **IP Address**: The address of the router at each hop.

tracert to a website:

The tracert command traces the route to the local host, which is the same as the source IP.

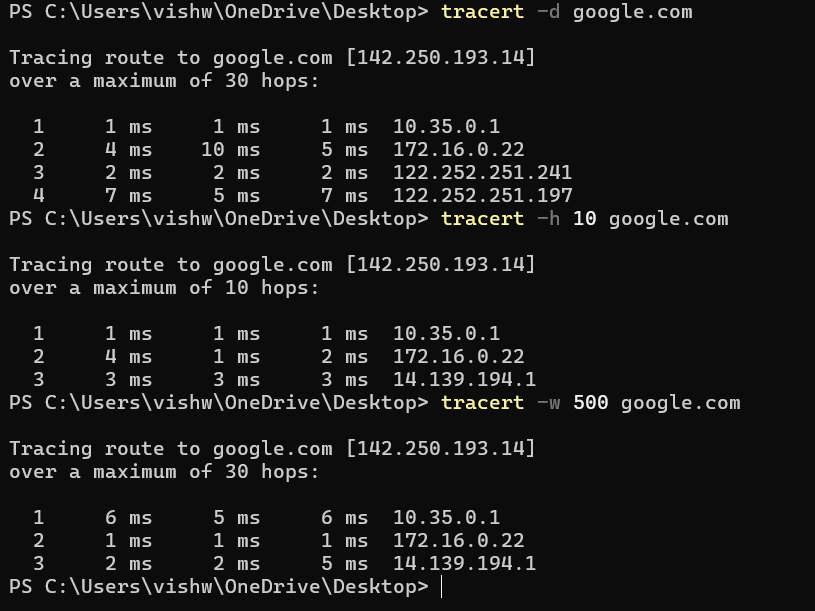
3.

* **-d** (do not resolve hostnames): Disable name resolution for IP addresses.

Example: **tracert -d google.com**

* **-h** (maximum number of hops): Specify the maximum number of hops to trace. Example: **tracert -h 10 google.com**
* **-w** (timeout in milliseconds): Specify the timeout for each hop.

Example: **tracert -w 500 google.com**



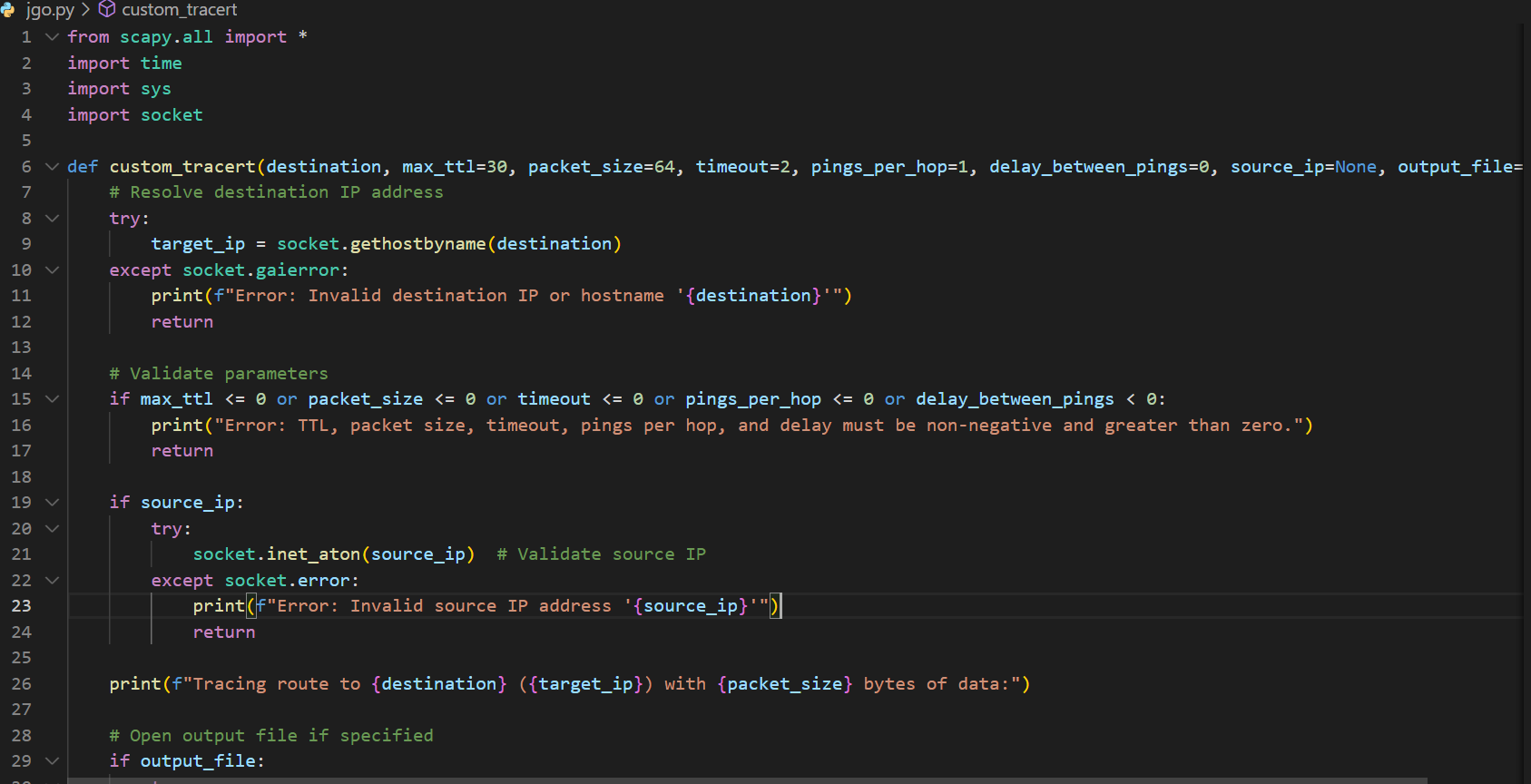
4. **Scenario**: You are experiencing slow network performance and suspect a problem with one of the routers on the path.

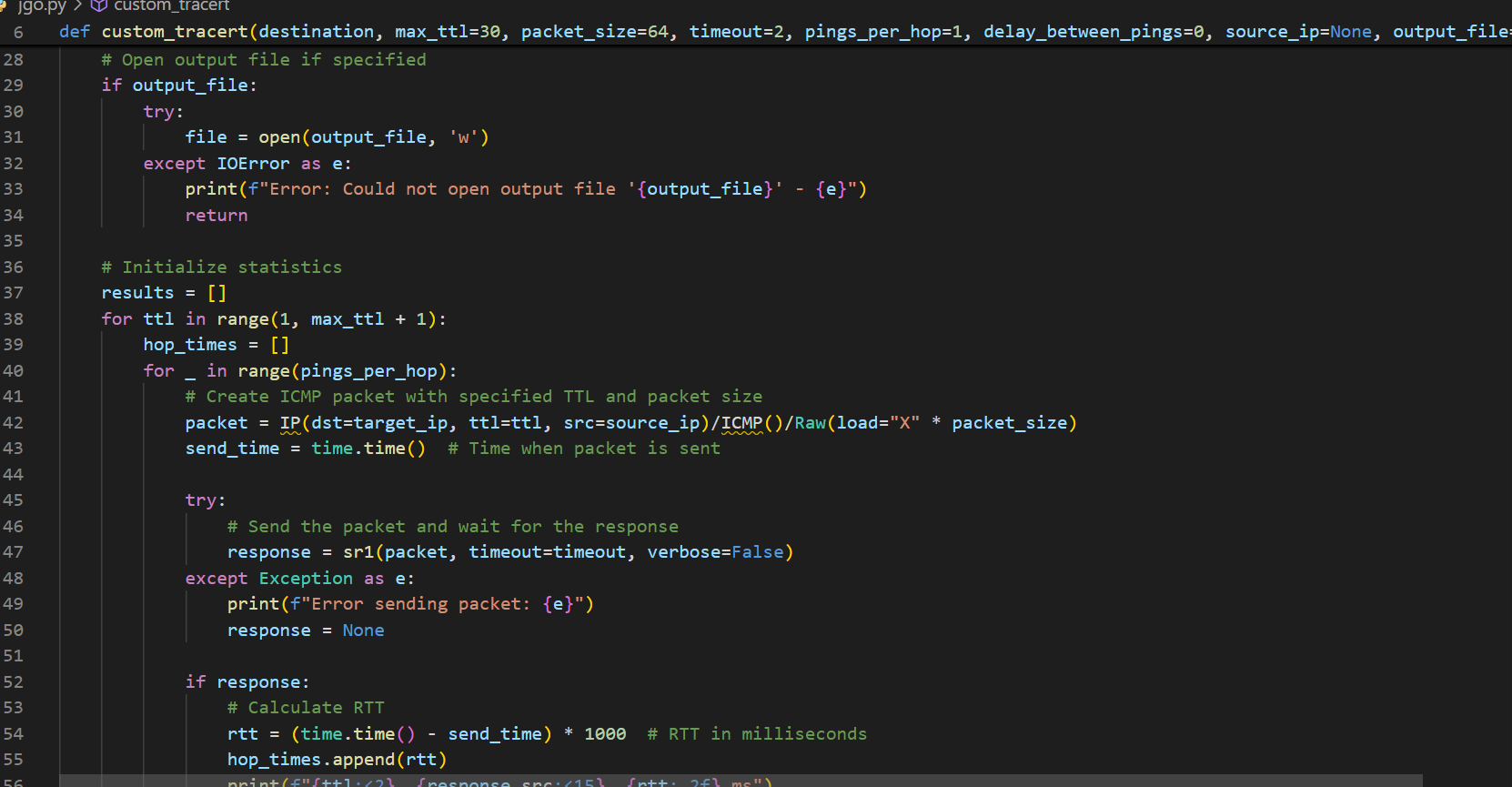
* **Diagnosis**: Use tracert to identify where the delay is occurring.
* **Commands**:

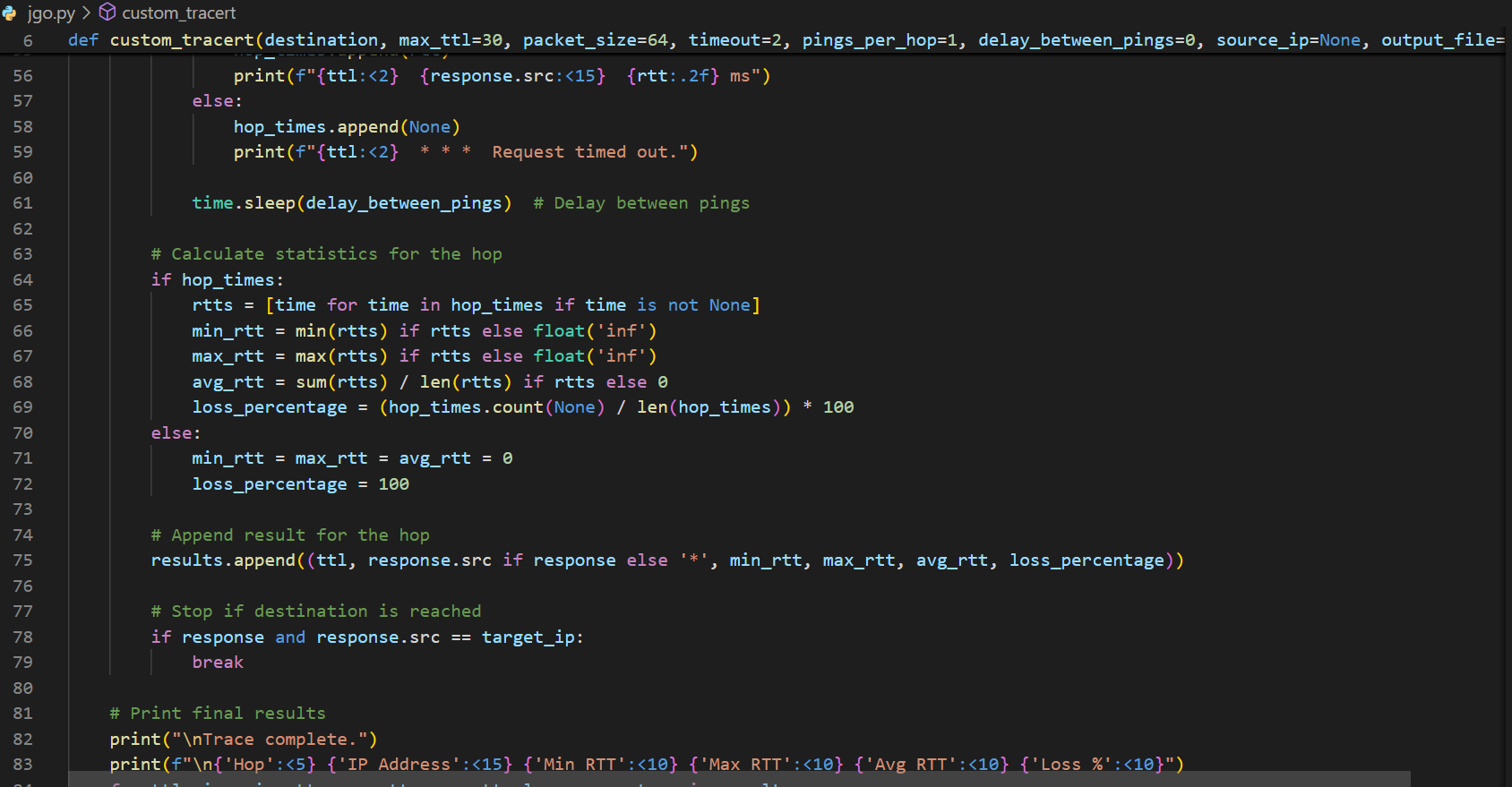
tracert www.google.com: Traces the route to identify the problematic hop.

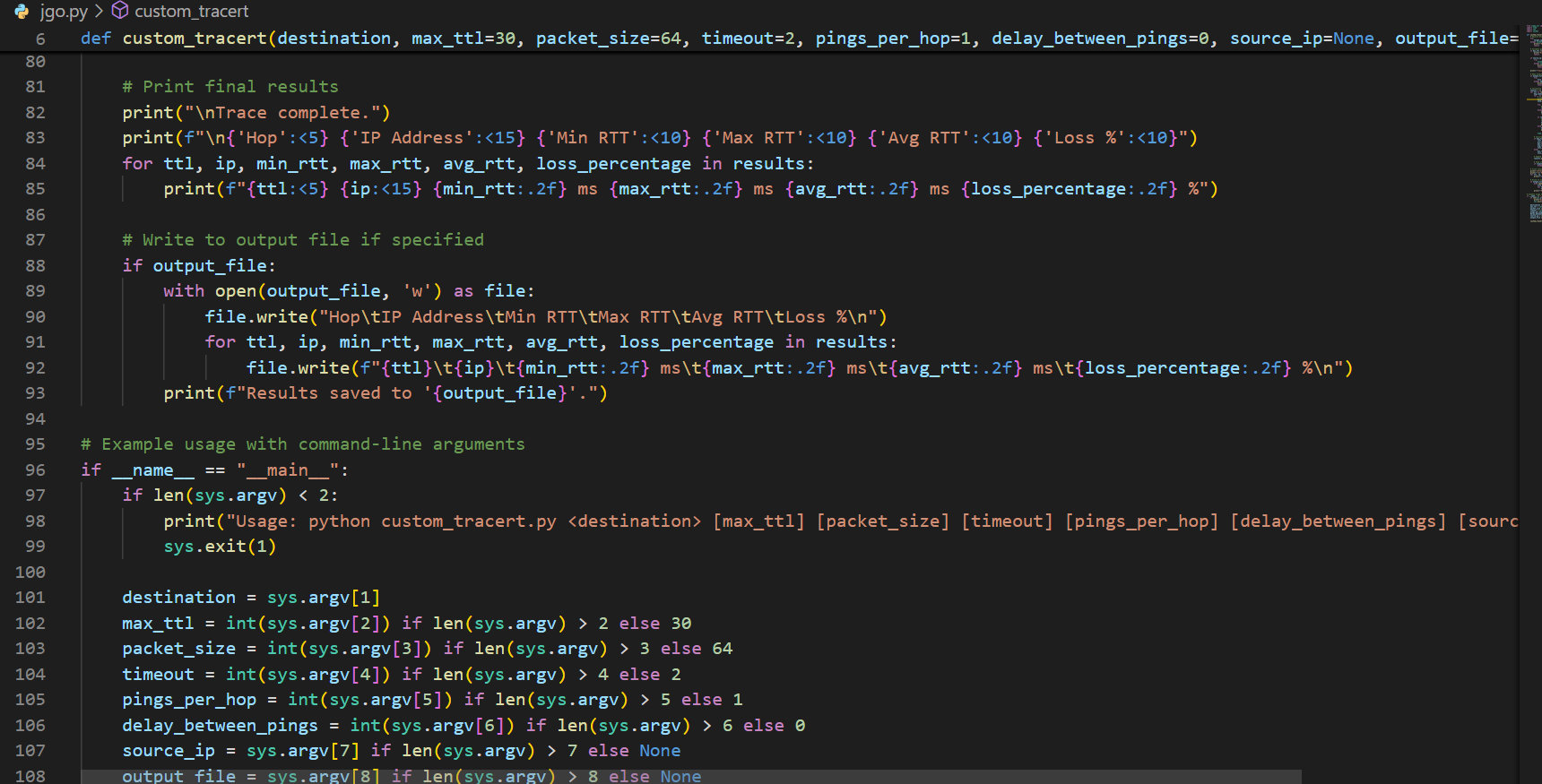
tracert -d www.google.com: Faster output by not resolving hostnames.

5. Code:









Output:

