**Lab 05: Assignment: Tracert Utility Analysis & Advanced Scapy Tracert Utility**

Objective:

In this assignment, you will analyze the tracert utility, a fundamental network diagnostic tool. You will explore its functionality, usage, and output, and demonstrate your understanding through a series of tasks.

Tasks:

1. Tracert Basics

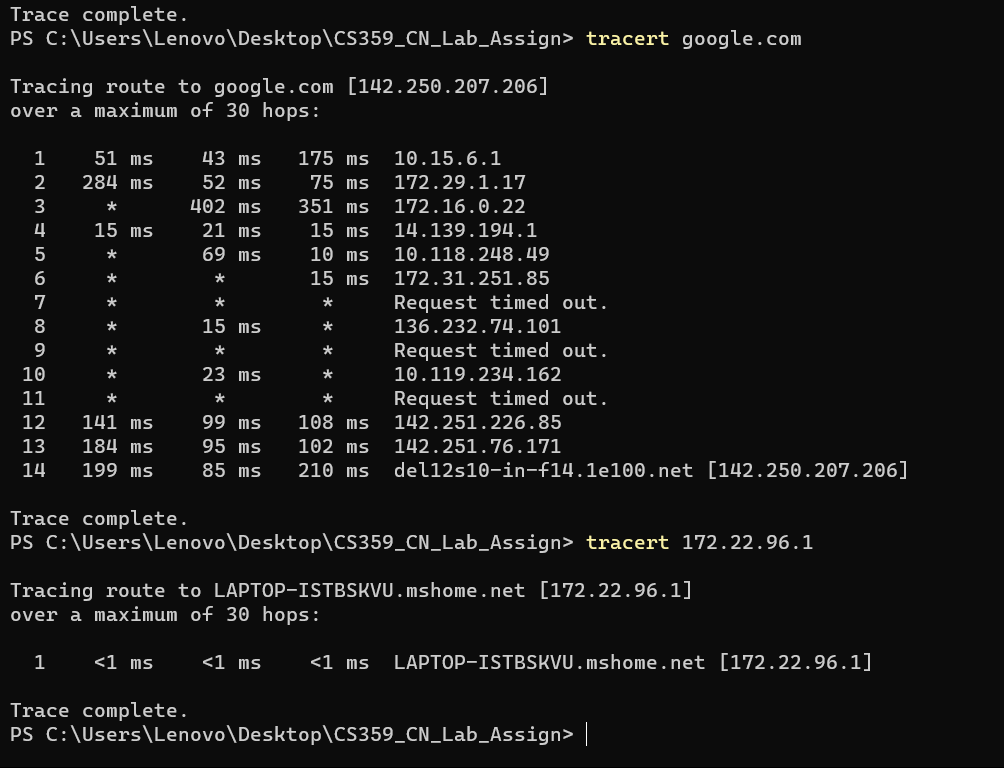
- Explain the purpose of the tracert utility and its basic syntax.

- Provide examples of how to use tracert to trace the route to a website and a local host.

**Purpose of the tracert Utility**

The tracert (short for **trace route**) utility is a network diagnostic tool used to track the path that data packets take from a source (your computer) to a destination (e.g., a website server). It helps identify where network bottlenecks, delays, or failures occur along the route. Each "hop" represents a router or device the packet passes through on its way to the destination.

* **Key Purpose**: To identify the intermediate hops or routers between the source and the target destination.



2. Tracert Output Analysis

- Run the command tracert (link unavailable) and capture the output.

- Analyze the output, explaining each line and its significance (e.g., hop number, IP address, RTT, etc.).

- Repeat the process for a local host (e.g., tracert 127.0.0.1).

**Hop Number**: The number on the left (e.g., 1, 2, 3...) shows the order of hops or routers the packet passes through.

**Round-Trip Time (RTT)**: The numbers next to each hop show how long it took for the packet to reach the hop and return (in milliseconds, ms).

**IP Address / Hostname**: Each hop will display either the IP address or hostname (if DNS resolution is enabled) of the router or network device.

**Timeouts or Unreachable Nodes**: Sometimes a hop will show \* \* \* instead of times, indicating the router did not respond or is blocking ICMP requests.

**Final Destination**: The final line shows the target server's IP address (142.250.182.206 in this case, which is a Google server), and the last RTT measurement indicates the total round-trip time to reach it.

3. Tracert Options

- Research and explain the following tracert options:

--d (do not resolve hostnames)

--h (maximum number of hops)

--w (timeout in milliseconds)

- Provide examples of how to use each option.

**1. -d Option (Do Not Resolve Hostnames)**

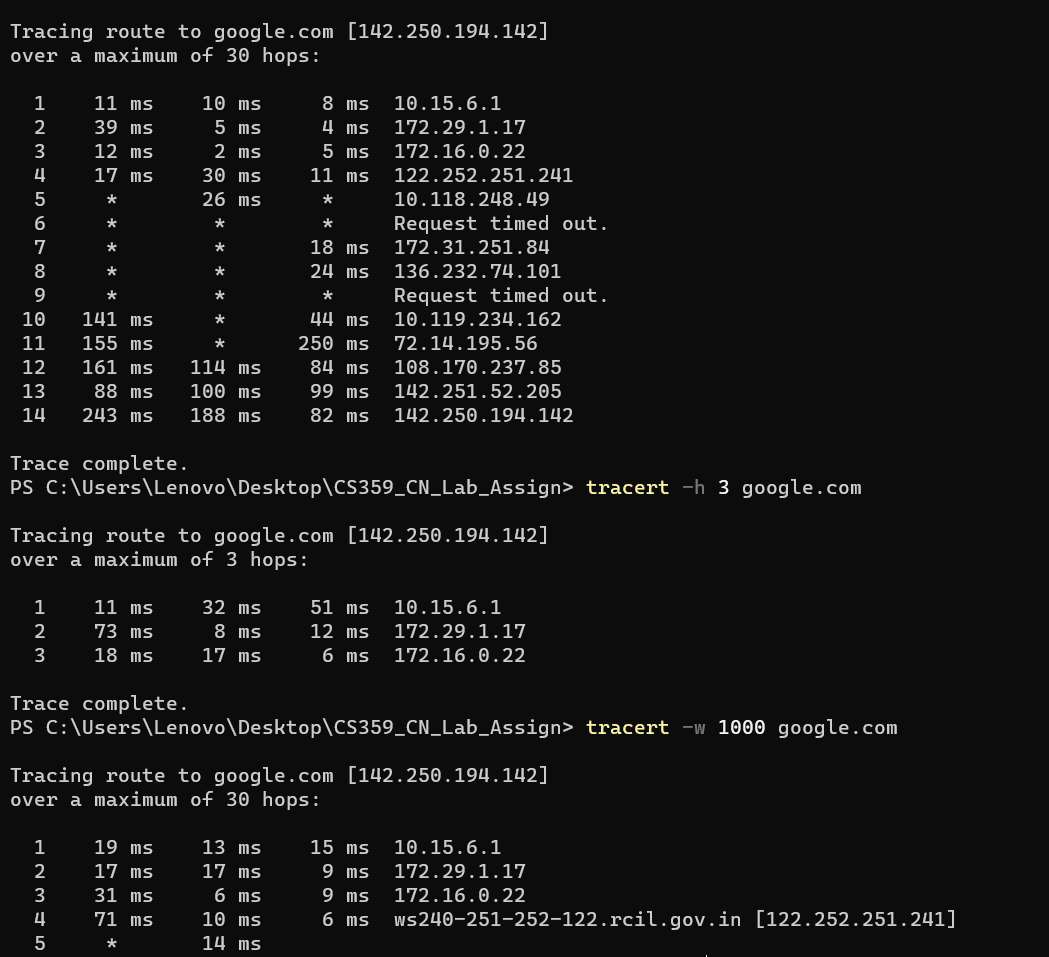
The -d option prevents tracert from attempting to resolve the IP addresses of routers to their corresponding hostnames. This can speed up the trace process because tracert won’t wait for DNS name resolution for each hop.

**2. -h Option (Maximum Number of Hops)**

The -h option allows you to specify the maximum number of hops tracert should attempt before stopping. By default, tracert will attempt up to 30 hops, but you can reduce this limit with -h.

**3 -w Option (Timeout in Milliseconds)**

The -w option allows you to set a timeout period (in milliseconds) for each hop. If a router does not respond within the specified time, tracert moves on to the next hop. By default, the timeout is 4000 milliseconds (4 seconds), but this can be adjusted with -w.



4. Troubleshooting with Tracert

- Describe a scenario where tracert would be used for network troubleshooting (e.g., connectivity issues, slow network speeds).

- Explain how to use tracert to diagnose the issue, including which options to use and why.

**Example: Troubleshooting Slow Connectivity**

1. **User Complaint**: You're experiencing slow access to a company server (www.example.com), while other websites load fine.
2. **Running Basic Tracert**:

tracert www.example.com

1. **Analyzing Output**:
   * You notice that most hops have reasonable RTTs, but there is a large spike in response time at hop 5.
   * Hop 5 consistently shows RTTs of 500 ms while other hops show 50 ms.
2. **Next Step**:
   * Use the -d option for quicker tracing:

tracert -d www.example.com

* + If the issue is still present at hop 5, it likely points to a problem with the router or connection at that hop.

1. **Use the -h Option**:
   * If you suspect the issue is within the first 10 hops, limit the trace:

tracert -h 10 www.example.com

1. **Use the -w Option**:
   * If the network seems to have high latency overall, increase the timeout:

tracert -w 5000 www.example.com

1. **Conclusion**:
   * After analyzing the output, you find the problem consistently occurs at hop 5, which is a router belonging to your ISP. You can now report the issue to your ISP, providing them with the tracert output to demonstrate the latency problem.

5. Conclusion

- Summarize your understanding of the tracert utility and its applications.

- Discuss any limitations or potential issues with using tracert for network diagnostics.

**Summary**

* tracert can be a powerful tool for diagnosing network issues such as slow connectivity or routing problems.
* By using different options (-d, -h, -w), you can optimize the tracing process and focus on specific aspects of the network route.
* The key to successful troubleshooting is analyzing the output, identifying any latency spikes or timeouts, and narrowing down the problem to a specific hop or network segment.

Submission:

Please submit a written report (PDF or Word document) containing your answers to the tasks above. Include screenshots or output captures where relevant.

**Objective 2 :**

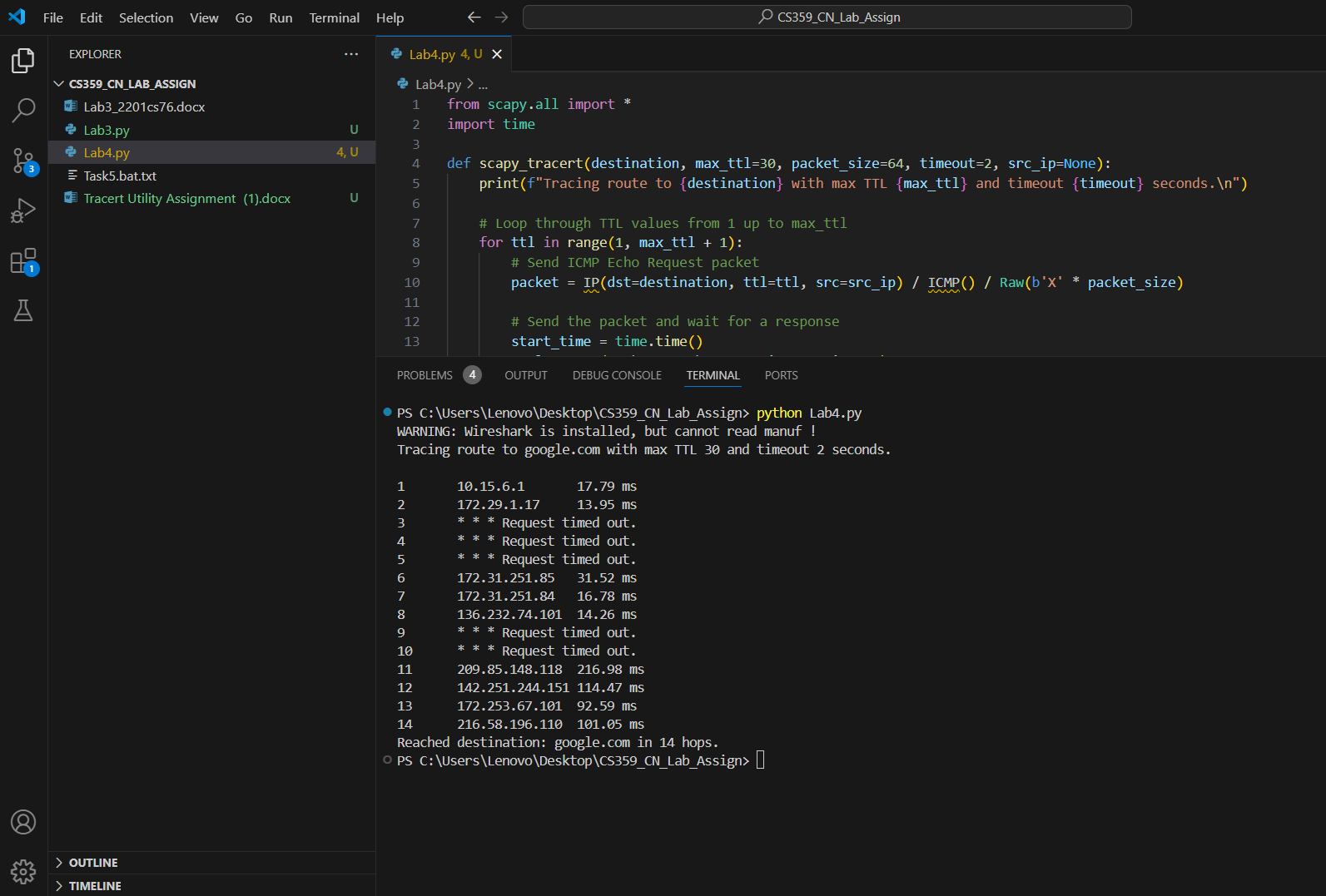
In this assignment, you will code a Scapy-based tracert utility to include additional features and functionality.

Tasks:

1. Basic Functionality

- Ensure the provided code works correctly.

- Test with different destination IPs, max TTL values, packet sizes, timeouts, and source IPs.



2. Additional Features

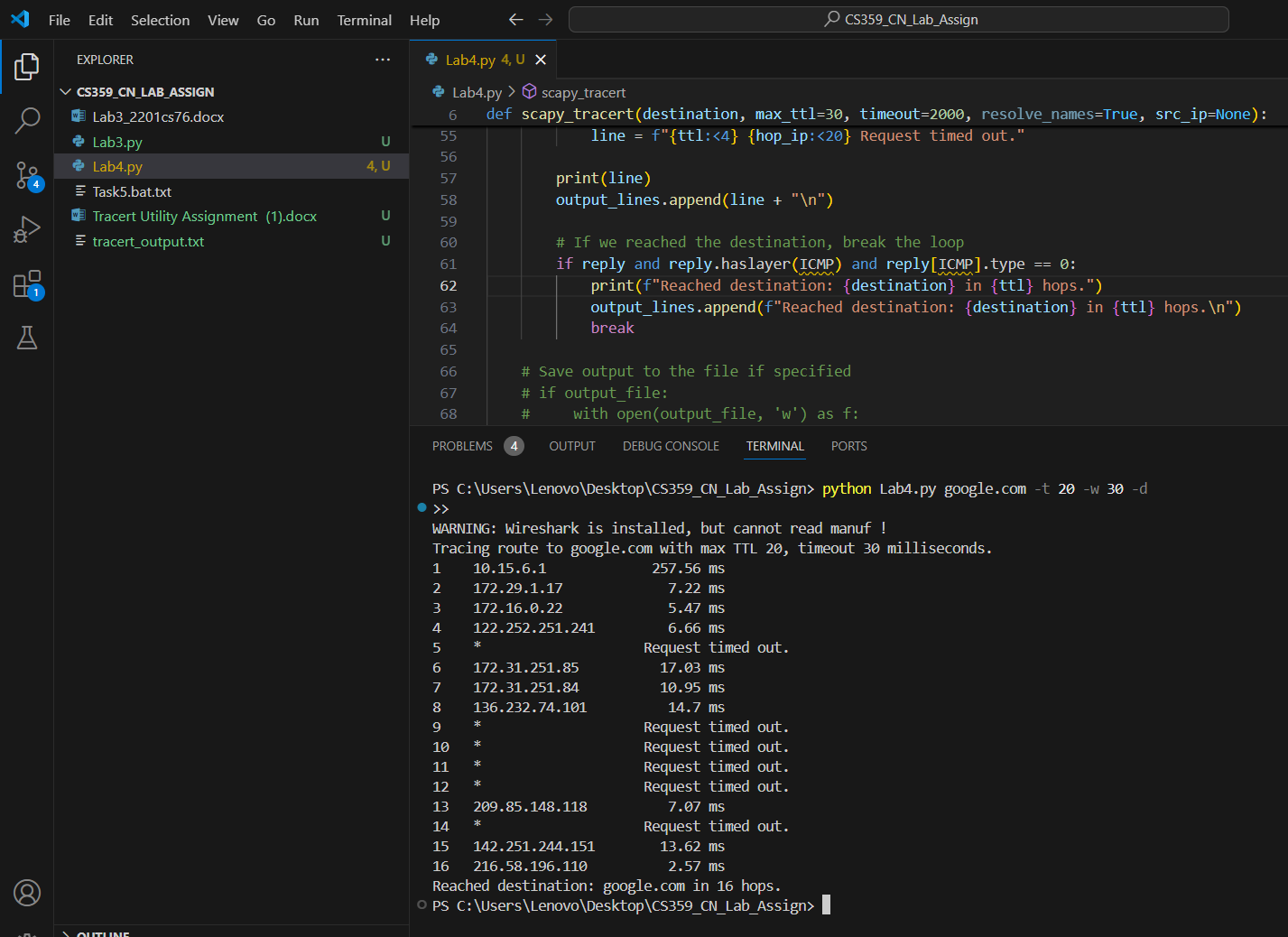
- Implement the following features:

- Option to specify the number of pings per hop

- Option to specify the delay between pings

- Option to save the output to a file

- Use Scapy's built-in functions to implement these features.



3. Error Handling

- Add error handling for cases like:

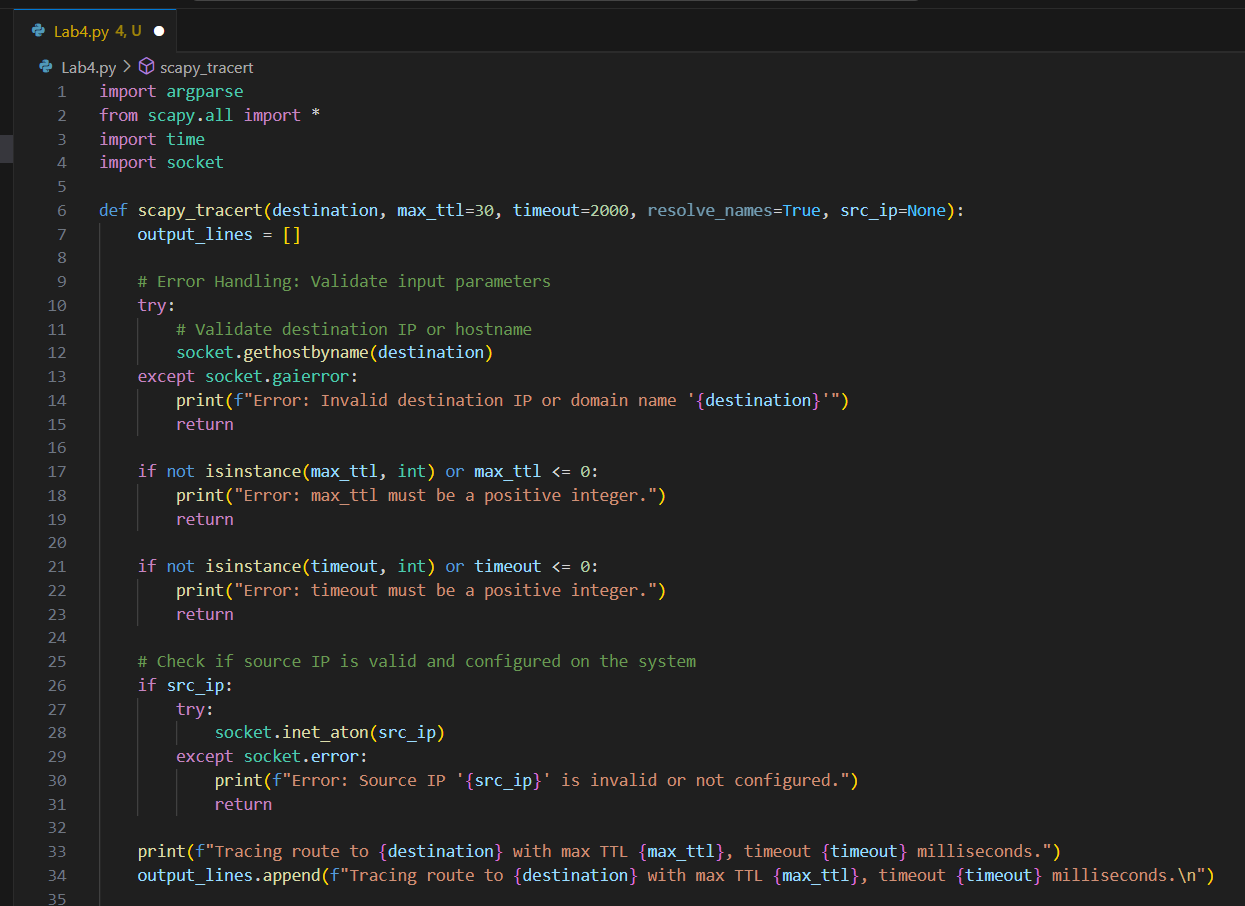
- Invalid destination IP

- Invalid max TTL value

- Invalid packet size or timeout value

- Source IP not configured on the system

- Use try-except blocks to catch and handle exceptions.



4. Output Formatting

- Improve the output formatting to include:

- Hop number

- IP address of each hop

- RTT (Round-Trip Time) for each hop

- Packet loss percentage for each hop

- Use Python's built-in formatting options to create a clean output.

