Title: Simulated Packet Sniffer in Python

Introduction:

This Python script demonstrates a simulated packet sniffer suitable for online compilers where live packet capture is not allowed. Traditional packet sniffing requires raw socket access, which online environments restrict. Therefore, we simulate packets to showcase packet analysis.

Components of the Script:

1. Packet Class:

Represents a network packet with source/destination IP, protocol (TCP/UDP), source/destination ports, and payload.

Enables simulation of network traffic in environments without raw socket access.

2. analyze_packet Function:

Takes a Packet object and prints its details.

Prints timestamp, IP addresses, protocol info, and first 50 characters of payload.

3. main Function:

Prints a message indicating simulated packet capture.

Creates a list of simulated Packet objects.

Loops through each packet and calls analyze_packet.

4. Execution:

Ensures the main() function runs when the script is executed.

Key Points:

- Works in any online Python compiler.
- Demonstrates packet capture and analysis logic without requiring raw network access.
- Can be extended by adding more simulated packets or user input.
- Maintains the same output format as a real packet sniffer for learning purposes.

Conclusion:

This script serves as a learning tool for understanding packet sniffing in Python. While it does not capture real network traffic, it effectively demonstrates how to analyze packet information such as IP addresses, protocol, ports, and payloads.