**Stage 1: SMTP Communication and Packet Analysis**

**Objective:** Build a client to communicate with an SMTP server provided as an executable file. The client should handle the SMTP protocol to receive an email containing a packet capture file (PCAP). Analyze this PCAP using Wireshark to extract critical information needed for the next stage.

**Details:**

1. **Client Functionality:**
   * Establish a connection to the SMTP server using Python’s smtplib.
   * Handle email retrieval and download the attached PCAP file.
   * Ensure the client handles different types of email content and attachments.
2. **Packet Capture Analysis:**
   * Use Wireshark to analyze the PCAP file.
   * Look for specific hints or encoded data in the packet streams.
   * Extract and save any files or messages found in the PCAP.

**Stage 2: TCP Stream and AES-256 Decryption**

**Objective:** Decode a TCP stream to extract an encrypted message. The TCP stream will include an audio file with hidden data. Use the symmetric key found within the audio file to decrypt the hidden message, which will contain latitude coordinates.

**Details:**

1. **Audio File Analysis:**
   * Extract the audio file from the TCP stream.
   * The audio will contain an embedded key and encoded data for decryption.
2. **AES-256 Decryption:**
   * Locate the symmetric key within the audio file.
   * Use this key to decrypt the hidden message encoded in AES-256.
   * The decrypted message should reveal three latitude coordinates.

**Stage 3: DNS Coordinates and Triangulation**

**Objective:** Decode longitude coordinates hidden in DNS server MAC addresses. Use the latitude coordinates obtained in Stage 2 and the longitude coordinates to triangulate the point of interest. Input the final coordinates into a provided program to verify correctness.

**Details:**

1. **DNS Server Analysis:**
   * Analyze DNS responses to extract MAC addresses.
   * Each MAC address encodes a longitude coordinate. Determine the encoding scheme used.
2. **Triangulation:**
   * Combine the latitude coordinates from Stage 2 with the longitude coordinates from the DNS server.
   * Use a suitable triangulation method, the player will need to figure it out using hints and proper hashing methods, to compute the final coordinates.
3. **Verification:**
   * Input the computed coordinates into the provided program.
   * The program will confirm the correctness and display a win message if the coordinates are accurate.

**Technical Requirements:**

* **Wireshark**: For analyzing the PCAP file from Stage 1.
* **Socket Programming**: To build the SMTP client.
* **SMTP Protocol**: Used for communication with the email server.
* **Encryption**: AES-256 for decrypting the hidden message.
* **DNS Protocol**: For encoding and decoding longitude coordinates.
* **Scapy**: To extract and reconstruct the executable from UDP packet headers.
* **Python**: For building the client, handling encryption, and performing triangulation.