This document explains how to set up and operate the UDP communication system using `udp_client.py`, `udp_server.py`, and `extract_packets.py`. The setup involves two nodes: a Windows machine (server) and a Kali Linux machine (client). The instructions cover the entire process, from capturing packets to replaying them and extracting the data.

Table of Contents

1. Setup and Prerequisites
2. Running the Server
3. Running the Client
4. Capturing Packets
5. Changing IP Address and Replaying Packets
6. Extracting Packets
7. Full Process

Setup and Prerequisites

1. **Install Python**: Ensure Python is installed on both machines.
2. **Install Necessary Packages**:
   - On Windows: `pip install prettytable`
   - On Kali Linux: `pip install scapy prettytable`
3. **Install Wireshark**: Install Wireshark on both machines for packet capturing.
4. **Install tcpreplay and tcprewrite** (Kali Linux):

   ```
   bash
   Copy code
   sudo apt-get update
   sudo apt-get install tcpreplay tcprewrite
   ```

Running the Server

1. Open Wireshark on the Windows machine and start a new capture.
2. Run `udp_server.py`:

   ```
   python udp_server.py
   ```

   This script will listen on ports `12345` for normal messages and `12346` for replay messages.

Running the Client

1. Open Wireshark on the Kali Linux machine and start a new capture.
2. Run `udp_client.py`:

   ```
   bash
   Copy code
   python udp_client.py
   ```

   This script sends student details to the server.

Capturing Packets

1. After running the client and server scripts, stop the Wireshark capture on both machines.
2. Filter the captured packets in Wireshark using the filter `udp.port == 12345`.
3. Save the filtered packets into a file named `communication.pcap` on both machines.

Changing IP Address and Replaying Packets

1. On Kali Linux, change the IP address:

   ```
   sudo ip addr del 192.168.0.103/24 dev eth0  #Deleting old IP
   sudo ip addr add 192.169.0.104/24 dev eth0  #Adding new IP
   ```

2. Rewrite the pcap file:

   ```
   sudo tcprewrite --infile=communication.pcap --outfile=output.pcap --
   srcipmap=192.168.0.103:192.169.0.104 --portmap=12345:12346
   ```

3. Open Wireshark on Windows and start a new capture.
4. Replay the packets on Kali Linux:

   ```
   sudo tcpreplay --intf1=eth0 output.pcap
   ```

5. Filter the packets in Wireshark using `udp.port == 12346` and save this into a file named `two.pcap`.

Extracting Packets

1. On the Windows machine, run `extract_packets.py` to process and display the captured packets:

   ```
   python extract_packets.py
   ```

   This script will read `two.pcap`, sort the packets by sequence number and timestamp, and display them in a tabular format.

Full Process

1. **Setup the Environment**:
   - Ensure all prerequisites are installed.
   - Start Wireshark on both machines.
2. **Run Server and Client**:
   - Start the server on Windows.
   - Start the client on Kali Linux.
3. **Capture Packets**:
   - Stop the capture on both machines.
   - Save the filtered packets.
4. **IP Address Change and Replay**:

   - Change IP on Kali Linux.
   - Rewrite the pcap file.
   - Start a new capture on Windows.
   - Replay packets from Kali Linux.
   - Save the filtered packets.
5. **Extract Packets**:
   - Run `extract_packets.py` on Windows to display the extracted data.