

CS-GY 6843

Wireshark Socket Programming 3

04/25/2022

Yibei Huang

```
Command Prompt
(c) Microsoft Corporation. All rights reserved.
C:\Users\huang>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::f4c6:a3fc:2281:4c2f%18
    IPv4 Address. . . . . : 192.168.31.230
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.31.1
```

```
#Fill in start
header = recPacket[20:28]
icmpType, code, mychecksum, packetID, sequence = struct.unpack("bbHHh", header)
```

Get ICMP header from the packet bit 160 to bit 224. Unpack the struct and store variables.

```
#Fetch the ICMP header from the IP packet
if packetID == ID:
    bytesinDb1 = struct.calcsize("d")
    timeSent = struct.unpack("d", recPacket[28:28 + bytesinDb1])[0]
    rtt = timeReceived - timeSent
    return (rtt*1000, icmpType, code, mychecksum, packetID, sequence, timeSent)
```

Check if ID matches. If match, get the data with double's size, start from bit 224 to 224+double's size.

Calculate the rtt by differencing the time received packet and time packet sent.

Finally return the tuple with format [(float, (integer, integer, integer, integer, integer, double))].

The extra credits Ping Statistics and Decoding Errors were completed in file <Exercises.py>.