Part A code high level view

The 'analysis_pcap_tcp.py' is mainly to get tcp packets from a given pcap file and find relevant information from its header and data. The arrival time and packet (in byte format) pair are stored in a list called ‘bufList. Then from the bufList, different flows are recognized by reading the source port part in the packet header. These flows are stored in a directory call 'flows' in the program. In this way, every flow could be analyzed independent. Besides dptk, some other libraries are also used in this 'analysis_pcap_tcp.py', such as 'datetime', 'struct', 'sys', and 'math'. These libraries help read strings, transform times, etc.