Assumptions :

1. TCP timeout

UDP Timeout

2. Packets without ports are ignored

3.

Data Unexpected values:

1. IP flags – comma separated, blanks

2. TTL – comma separated multiple values

Conversations in Wireshark:

1. Have packets from A to B and B to A both in 1 record

2. 30 repeated flows were identified in TCP convos

3. Duration of A->B and B->A flows same or different as convo duration?