**Network Visualization Analysis**

**Protocol vs. Frequency**

From the sample data, there were 12 protocols found:

1. IGMP - Internet Group Management Protocol
2. EGP - Exterior Gateway Protocol
3. OSPFIGP - Open Shortest Path First Interior Gateway Protocol
4. ICMP - Internet Control Message Protocol
5. UDP - User Datagram Protocol
6. TCP - Transmission Control Protocol
7. PIM - Protocol Independent Multicast
8. ESP - Encapsulating Security Payload
9. VRRP - Virtual Router Redundancy Protocol
10. IGP - Interior gateway protocol
11. GRE - Generic Routing Encapsulation
12. SCPS - Space Communications Protocol Specifications

Any rows with any empty field in the protocol column was considered to have an unassigned protocol network. From the data gathered, the TCP protocol was the most prevalent at the time the data was captured, with nearly half a million exchanges using that protocol (666,096 exactly).

**ICMP vs. Others**

Based on the sample data, approximately 4.38% of the used protocols were ICMP. ICMP is “used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts” 1. Although this seems like a low percentage, from the Protocol vs. Frequency analysis, it is the fourth most used protocol in the sample data.

**Size vs. Frequency**

Based on the sample data, the largest packet size transferred is 1500 bytes. The most common packet size is 40 bytes, with 178,207 exchanges using this packet size. The second most common is the largest packet size, with 153,290 exchanges using this packet size.

**Reset vs. Time**

A reset is the third most significant bit in a flag that determines whether a connection is reset. Based on the sample data, the number of reset connections was greatest at time 204.2572, with 1150 reset connections.

**New Connections vs. Time**

A new connection is identified by the SYN bit in the flag (the fourth most significant bit). Based on the sample data, the number of new connections was greatest at time 297.1162, with 493 new connections.

**Closed Connections vs. Time**

A closed connection is identified by the FIN bit in the flag (the fifth most significant bit). Based on the sample data, the number of closed connections was greatest at time 249.4205, with 1279 closed connections.