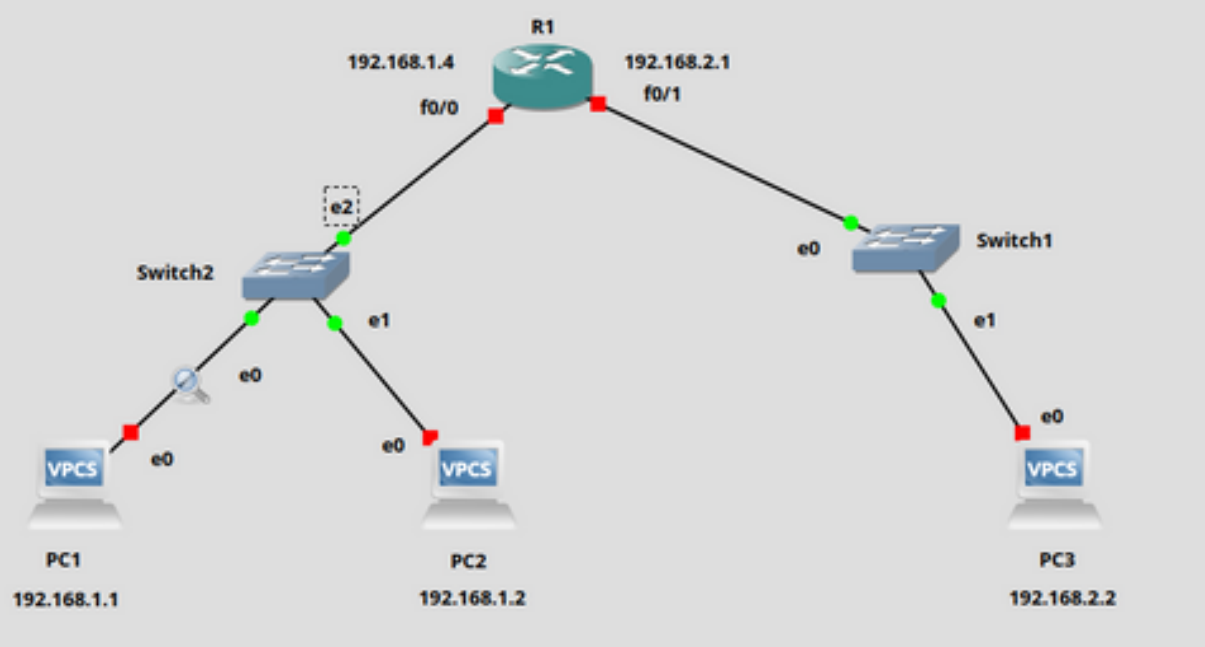
**3. TCP/UDP Intersection Module: Simulate coexistence, monitoring,**

**and analysis of TCP and UDP traffic in the network.**

**# Background Research for the problem statement:**

- Understood TCP and UDP protocol and the fundamental differences between them (connection-oriented and connectionless).
- Understood the TCP and UDP packet structure.
- How Wireshark can dissect and interpret packet headers for both protocols.
- Identified well-known ports for TCP and UDP services (eg. HTTPS, FTP)
- Learned how to set up filters and search for specific packets.




**# Observations:**

- **TCP and UDP Traffic Identification:**

  - **Protocol Differentiation**:

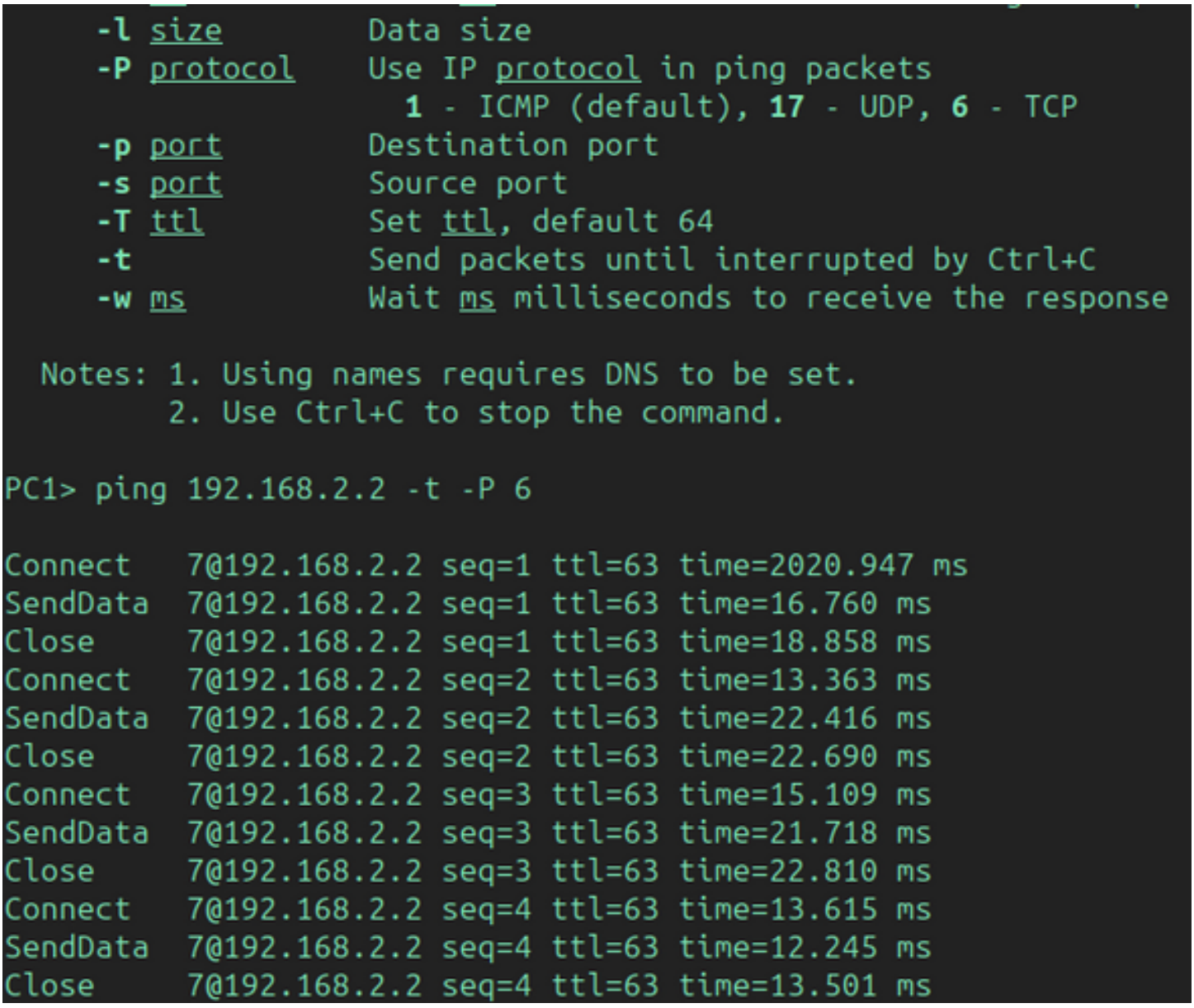
    Successfully identified and differentiated between TCP and UDP traffic in the Wireshark captures.

    Recognized the unique characteristics of TCP and UDP packets.

- **Port Numbers:**

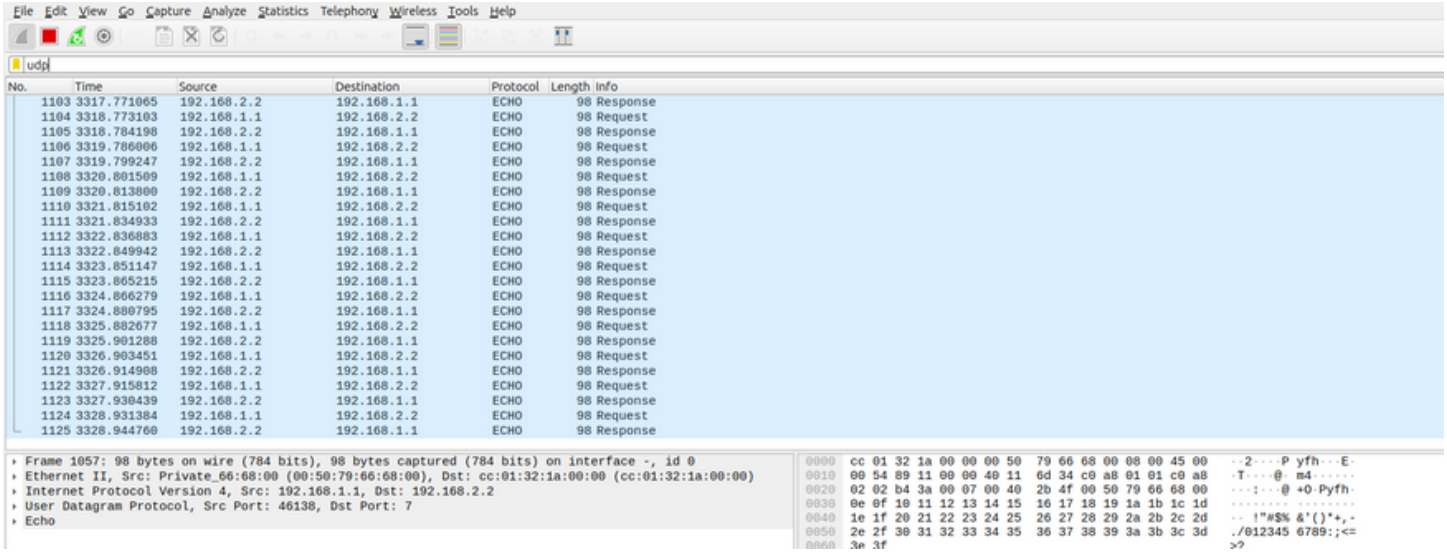
  Associated port numbers with specific protocols to understand the nature of the traffic.

  Used port numbers to identify common applications or services.

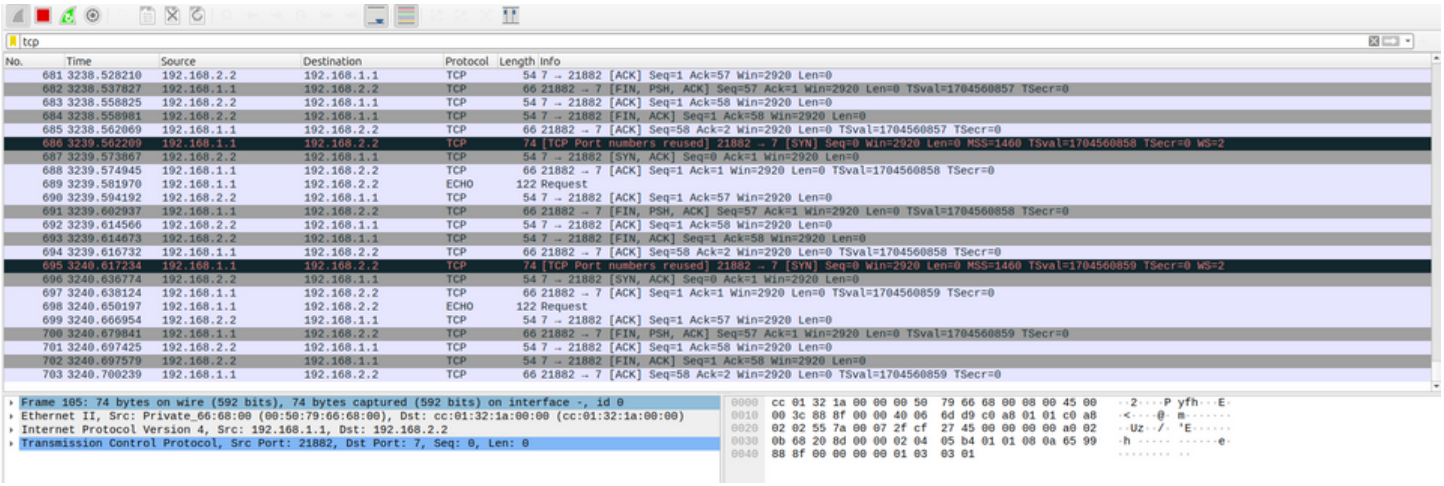


```
     -P protocol    Use IP protocol in ping packets
                      1 - ICMP (default), 17 - UDP, 6 - TCP
     -p port        Destination port
     -s port        Source port
     -T ttl         Set ttl, default 64
     -t             Send packets until interrupted by Ctrl+C
     -w ms          Wait ms milliseconds to receive the response

  Notes: 1. Using names requires DNS to be set.
         2. Use Ctrl+C to stop the command.

PC1> ping 192.168.2.2 -t -P 17

84 bytes from 192.168.2.2 udp_seq=1 ttl=63 time=29.744 ms
84 bytes from 192.168.2.2 udp_seq=2 ttl=63 time=13.978 ms
84 bytes from 192.168.2.2 udp_seq=3 ttl=63 time=13.718 ms
84 bytes from 192.168.2.2 udp_seq=4 ttl=63 time=13.171 ms
84 bytes from 192.168.2.2 udp_seq=5 ttl=63 time=13.392 ms
84 bytes from 192.168.2.2 udp_seq=6 ttl=63 time=14.303 ms
```

**UDP**




**TCP**




- **Traffic Patterns:**

  - Pattern Analysis:

    Observed traffic patterns for both TCP and UDP.

    Identified characteristics such as connection-oriented behavior in TCP and connectionless nature in UDP.

  - **Wireshark Filters:**

    Successfully applied capture filters to focus on capturing only TCP or UDP traffic.

    Explored the effectiveness of filters in isolating specific types of traffic.