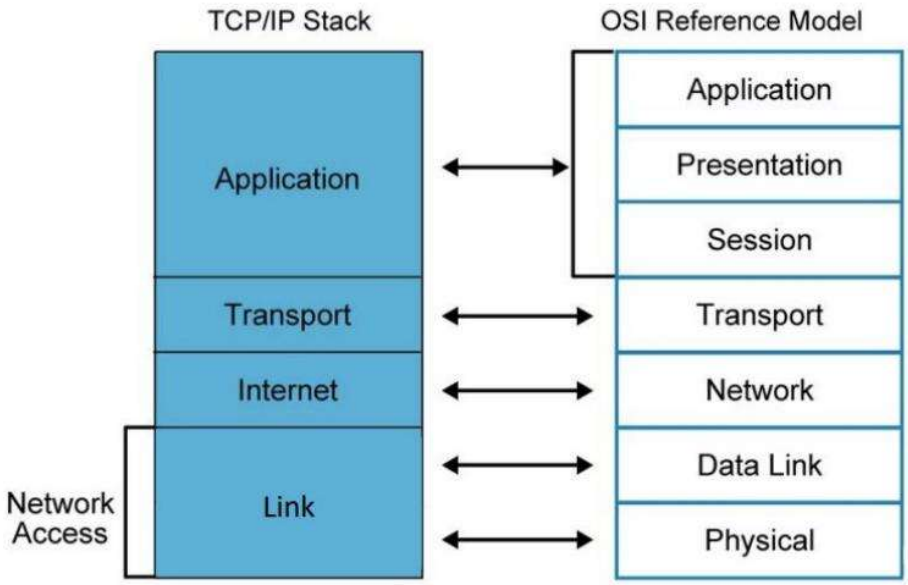
This project focuses on network packet analysis and understanding fundamental networking concepts using tools like Wireshark and TCPDump. Here's a summary of the key components and steps:

TCP (Transmission Control Protocol)
Three-way handshake: SYN, SYN/ACK, ACK
UDP (User Datagram Protocol)
ICMP (Internet Control Message Protocol)
ARP (Address Resolution Protocol)

OSI Model and TCP/IP Stack

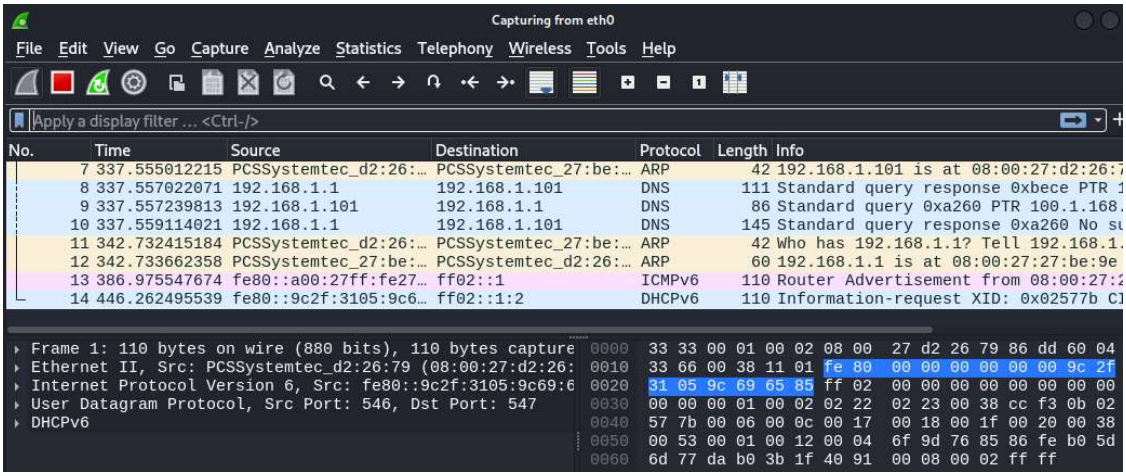


IP Addressing
IPv4 and IPv6 formats
Subnets and CIDR notation

```
┌──(kali㉿kali)-[~]
└─$ sudo arp -a
[sudo] password for kali:
pfSense.home.arpa (192.168.1.1) at 08:00:27:27:be:9e [ether] on eth0
? (192.168.1.100) at 08:00:27:3c:05:2e [ether] on eth0
```

Port Numbers
Common port numbers and their associated services
Packet Analysis Steps
Install and launch Wireshark:
bash

sudo Wireshark



Select network interface (e.g., eth0) and start capture

Capture specific protocol traffic:

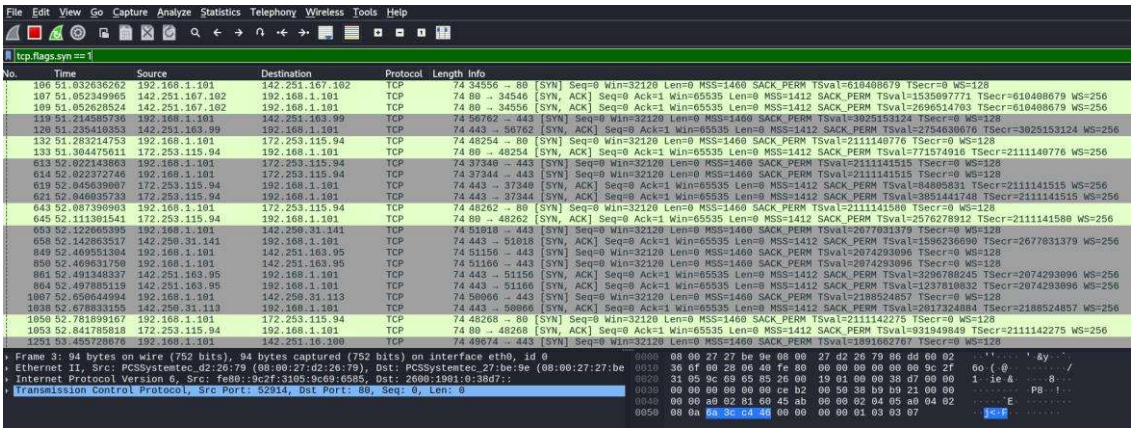
TCP handshake

ICMP (ping)

ARP requests/responses

Apply filters in Wireshark:

tcp.flags.syn == 1



Arp