

1. What is the purpose of the UDP Psuedo-Header? Does it contain any information unique to the other headers of the packet in the OSI model?
2. Recall that in a WireGuard Handshake, peers employ not only a set key-pair of statically generated keys, but also a set of ephemeral keys that persist only for the duration of the connection, and are changed on each re-key. What is the point of these ephemeral keys?
3. Advertisements for commercial VPN services often tout that they provided military grade encryption, such that nobody can see your network activity. The `main` application emulates this sort of relationship, where peers connect to the commercial VPN's servers before being routed to their destination. In both these schemes, at what point is the packet encrypted? At what point is it plaintext? Who can see the network activity of the client?