Programming network project

In this project, we intend to get acquainted with low-level programming with the help of implementing several network tools.

Phase 0 : Research and preparation

I choose python for network programming because Python allows you to build scripts to automate complex network configuration and it is the most widely used programming language for software-defined networking and also python has a lot of library which helps to program faster.
A packet analyzer or packet sniffer is a computer program or computer hardware such as a packet capture appliance, that can intercept and log traffic that passes over a computer network or part of a network Packet capture is the process of intercepting and logging traffic. As data streams flow across the network, the analyzer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications. A packet analyzer used for intercepting traffic on wireless networks is known as a wireless analyzer or WiFi analyzer. A packet analyzer can also be referred to as a network analyzer or protocol analyzer though these terms

Packet sniffing:

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender’s node called data packets and reassembled at receiver’s node in original format. It is the smallest unit of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called packet sniffing. It is a form wherein, we can “tap phone wires” and get to know the conversation. It is also called wiretapping and can be applied to the computer networks.
Sniffing can be either Active or Passive in nature. In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with the Hub devices. In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack.

Packet analyzing:

Packet analysis is a primary traceback technique in network forensics, which, providing that the packet details captured are sufficiently detailed, can play back even the entire network traffic for a particular point in time. This can be used to find traces of nefarious online behavior, data breaches, unauthorized website access, malware infection,etc.

Useful library and tools:

For implementing packet sniffing we use some basic module like binascii ,struct ,socket and etc.

Wireshark is a network packet analysis tool that captures packets in real time and displays them in a graphic interface.
We can use the pyshark library to analyze the network traffic in Python, since everything Wireshark decodes in each packet is made available as a variable.

References:

https://www.lynda.com/Python-tutorials/Python-Theory-Network-Engineers/772337-2.html
https://en.wikipedia.org/wiki/Packet_analyzer
https://www.tutorialspoint.com/python_penetration_testing/python_penetration_testing_network_packet_sniffing.htm
https://www.geeksforgeeks.org/what-is-packet-sniffing/
https://www.paessler.com/it-explained/packet-sniffing
https://www.sciencedirect.com/science/article/pii/S1742287619302002
https://subscription.packtpub.com/book/networking_and_servers/9781789958096/1/ch01lvl1sec15/interacting-with-wireshark-with-pyshark