PCAP Analysis refers to traffic analysis using the traffic stored traffic captures (packets/frames) in a PCAP file. In this section, we will cover the exercises that deal with analyzing WiFi, HTTP, and VoIP traffic using Scapy and PyShark Python libraries.

What will you learn?

- Analyze/process traffic stored in a PCAP file with Scapy and PyShark Python library

References:

1. Scapy documentation (https://scapy.readthedocs.io/en/latest/introduction.html)
2. Pyshark library (https://github.com/KimiNewt/pyshark)

Labs Covered:

- Wi-Fi layers: Scapy
  In this lab, you will learn to interpret and analyze the WiFi traffic stored in a PCAP using Scapy Python library.
- Analyzing HTTP: PyShark
  In this lab, you will learn to interpret and analyze the HTTP traffic stored in a PCAP using the PyShark Python library.
- Getting Started: Scapy Basics
  In this lab, you will learn to interpret and analyze the captured network traffic using the Scapy Python library.
- WiFi Kung Fu: Scapy
  In this lab, you will learn to interpret and analyze the WiFi traffic stored in a PCAP using Scapy Python library.
- Wi-Fi Traffic: Pyshark and Scapy
  In this lab, you will learn to interpret and analyze the WiFi traffic stored in a PCAP using Scapy and Pyshark Python libraries.
- Analyzing VoIP: PyShark
  In this lab, you will learn to interpret and analyze the VoIP traffic stored in a PCAP using the PyShark Python library.

Wi-Fi layers: Scapy

Start

Analyzing HTTP: PyShark

Start

Getting Started: Scapy Basics

WiFi Kung Fu: Scapy

Start

Wi-Fi Traffic: Pyshark and Scapy

Start

Analyzing VoIP: PyShark

Start