Networking Reconnaissance and Analysis

Course	CSN
Done?	☑

Task 1: Wireshark

1. Download this pcap file and try to investigate the traffic flow and extract any artifact that is inside the pcap file.

> 💡 the goal is to find an image that is been transferred in the pcap file

2. Try to do a networking activity (for example, pinging Google DNS) and then use Wireshark filters to show only that activity.

Task 2: Nmap

Do an Nmap scan of your localhost or any virtual machine **that you are allowed to scan**, what can you see?

1. Do an all-port scan.
2. Do a version enumeration scan.
3. When scanning a Windows system Nmap will stop the scan and report that the host is **down**, what can you do to solve this issue?
4. **IF YOU ARE IN INNOPOLIS AND YOU HAVE A 10.1.1.X IP ADDRESS**, then do a scan for the whole network (10.1.1.0/24)

Task 3: Reconnaissance

There are two types of reconnaissance, active and passive. What are the differences between them? which one would you use? Can you do a passive scan of the local

subnet that is connected to your PC? (Make sure you are connected to the 10.1.1.X subnet or your own local subnet, for example home router)