**PICOCTF**

**Spoof Proof – 60**

The police have retrieved a network trace of some suspicious activity. Most of the traffic is users viewing their own profiles on a social networking website, but one of the users on the network downloaded a file from the Thyrin Labs VPN and spoofed their IP address in order to hide their identity. Can you figure out the last name of person that accessed the Thyrin files, and the two source IP addresses they used?

Ans.

Analysing pcap file we can see:

Secret file **source ip** address 192.168.50.4 MAC address **08:00:27:2b:f7:02**

Claudio.drake **source ip** address 192.168.50.4 MAC address 08:00:27:e6:02:37

John.Johnson **source ip** address 192.168.50.3 MAC address **08:00:27:2b:f7:02**

As we can see at first we find claudio.drake suspicious because his source ip address is same as the secret file source ip address which indicates that he requested that file.

However, When cross-checking his mac address with the secret file mac address we can see that it DO NOT match.

We can also see the mac address of the secret file matches with the john’s mac address. This means that john has spoofed his ip address with the ip address of claudio to hide his identity.