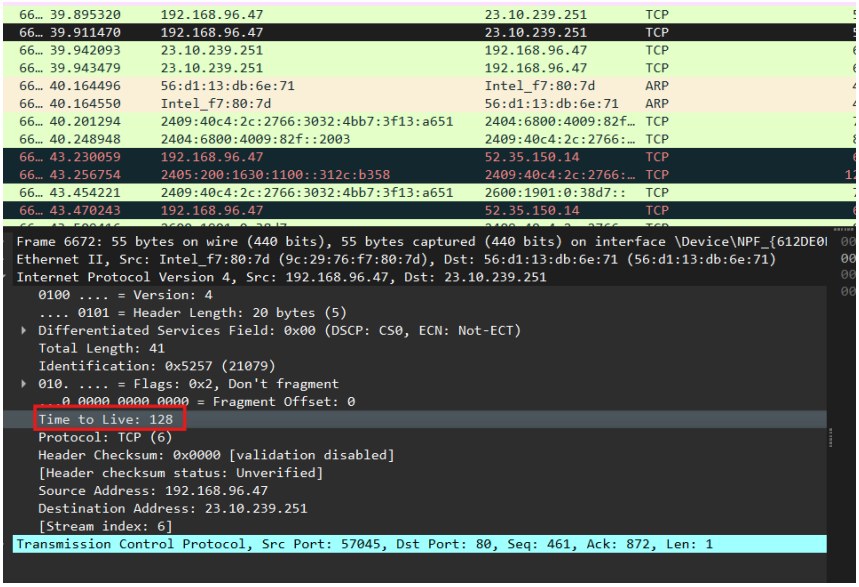
OS Fingerprinting

Using TTL (Time to Live) to fingerprint operating system on a network :



In this figure we used Wireshark on Windows to see inside a IPv4 traffic from a source to a destination that is 192.168.96.47 to 23.10.239.251, where TTL is 128, which we can infer that 128 TTL is a default value for a Windows OS.

Next, using Nmap to fingerprint operating system on a network :

```
└─$ nmap -v -O -Pn 10.10.10.245
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 00:44 IST
Initiating Parallel DNS resolution of 1 host. at 00:44
Completed Parallel DNS resolution of 1 host. at 00:44, 0.01s elapsed
Initiating SYN Stealth Scan at 00:44
Scanning 10.10.10.245 [1000 ports]
Discovered open port 22/tcp on 10.10.10.245
Discovered open port 80/tcp on 10.10.10.245
Discovered open port 21/tcp on 10.10.10.245
Completed SYN Stealth Scan at 00:44, 2.21s elapsed (1000 total ports)
Initiating OS detection (try #1) against 10.10.10.245
Nmap scan report for 10.10.10.245
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Uptime guess: 29.359 days (since Wed Feb 26 16:06:51 2025)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

Here we can clearly see on IP, 10.10.10.245, we have discovered that there is a Linux Machine running of any version from 4.15 to 5.19, with ports for ftp, ssh, http open on a network.