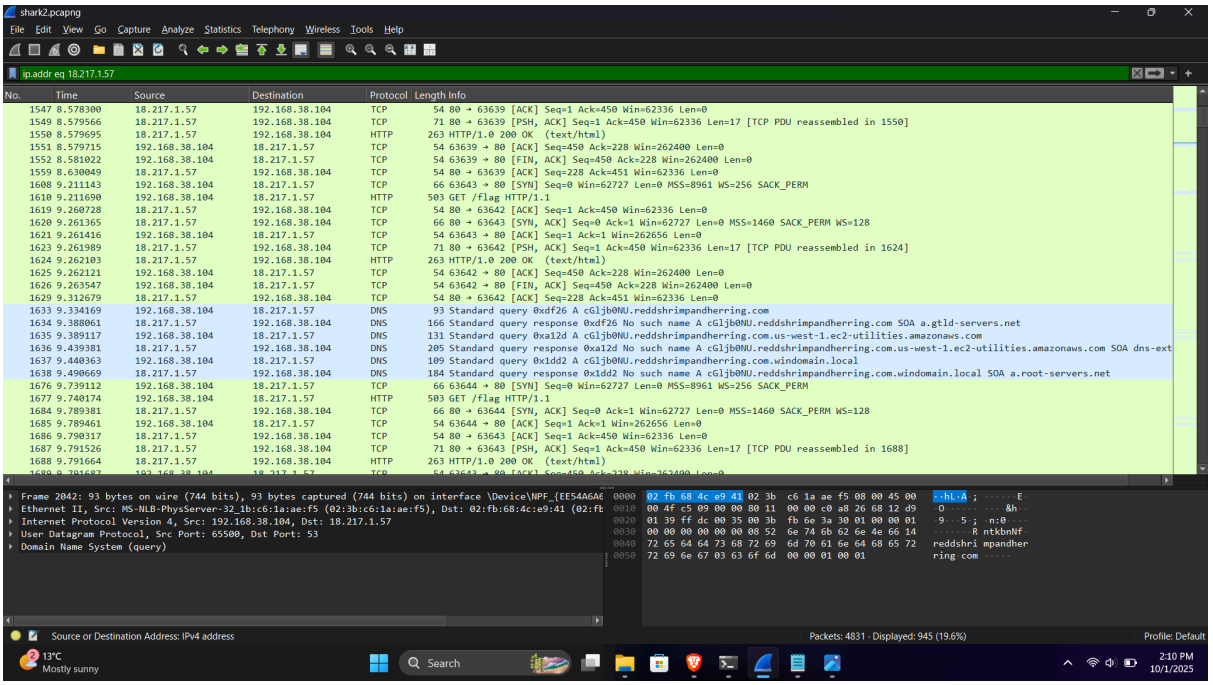
Looking through the files I exported with HTTP, we can see a bunch of fake picoCTF flags :

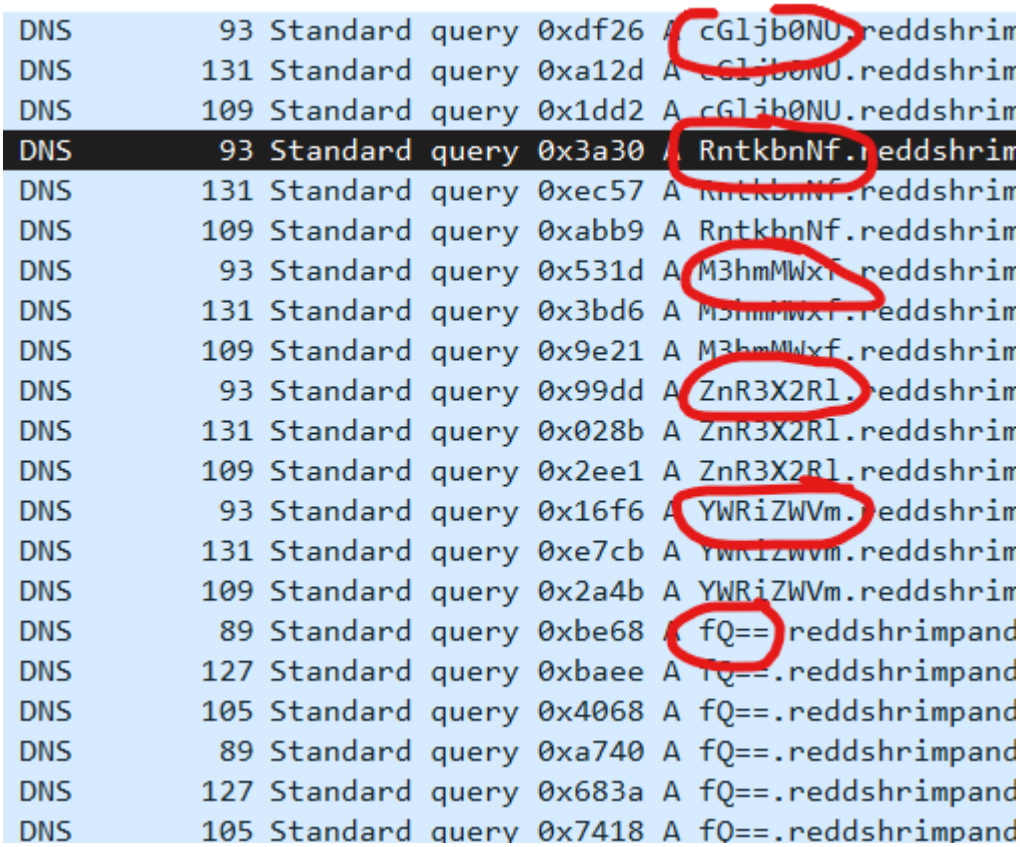
```
z4que@z4que /m/c/U/z/D/aici> strings * | grep "picoCTF"
picoCTF{bfe48e8500c454d647c55a4471985e776a07b26cba64526713f43758599aa98b}
picoCTF{bda69bdf8f570a9aaab0e4108a0fa5f64cb26ba7d2269bb63f68af5d98b98245}
picoCTF{fe83bcb6cfd43d3b79392f6a4232685f6ed4e7a789c2ce559cf3c1ab6adbe34b}
picoCTF{711d3893d90f100c15e10ef4842abeed3a830f8237c1257cd47389646da97810}
picoCTF{3cf1e22d489fcfb6bb312a34f46c8699989ed0434061343314 52d11ce73cd59e}
picoCTF{b4cc138bb0f7f9da7e35085e349555aa6d00bdca3b021c1fe8663c0a422ce0d7}
picoCTF{41b8a1a796bd8d202016f75bc5b38889e9ea06007e6b22fc856d380fb7573133}
picoCTF{9812bc4be04e6f9c803152313db3da53b3dfb799bdb05aac46fa0dd0045d2fc2}
picoCTF{64cf3ede3736a340fdf2954be5151ce53bec291c5e48cbccb44faa529946e249}
picoCTF{c50d259a4e172fcb2eddbabeebd272473e4882b76c9efcd12c03ac04429d884a}
```

After some failed tries, where I applied operations in CyberChef and the only flag remained was picoCTF{3fe0b2788f30d9cb9f77d3b2752f13c554fe7f0e7a2883e57c8a44b34f35675c} (also not good) I started again to look in our PCAP file.

The first thing I noticed was the only public IP, 18.217.1.57, so I used filters :
(**ip.addr eq 18.217.1.57**)



Again, looking through packets, we can see some DNS packets. I filtered them again, using **dns && ip.dst eq 18.217.1.57 (** I was curious about the packet destination with the public IP **).** And now, you can see a Base64 code :



THE FLAG : picoCTF{dns_3xf1l_ftw_deadbeef}
~Z4que