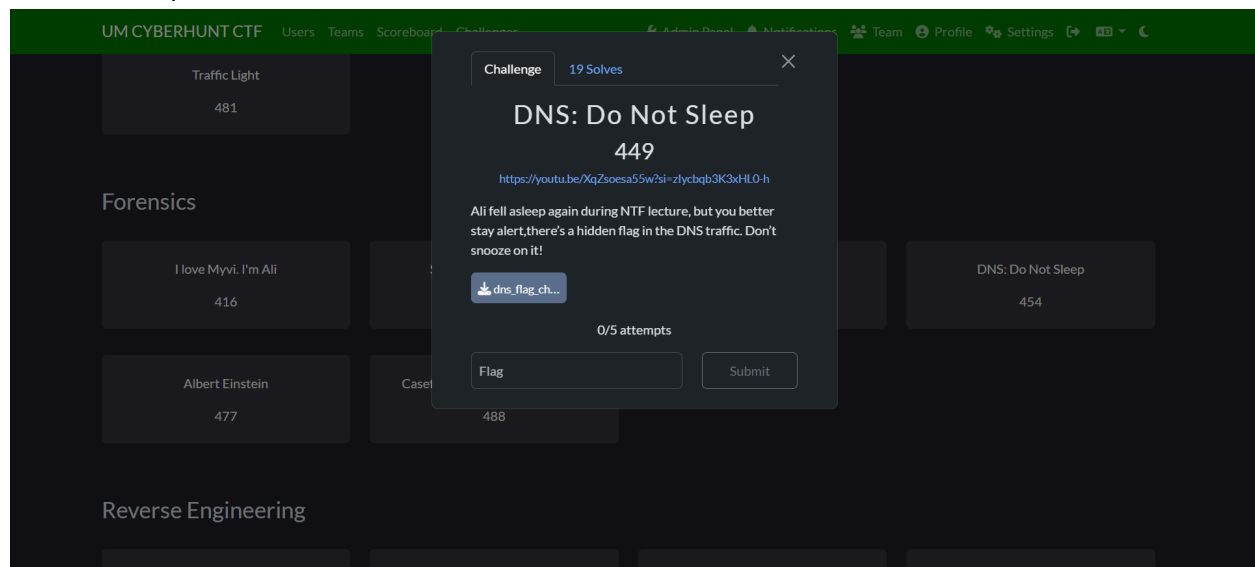


This is how question looks :



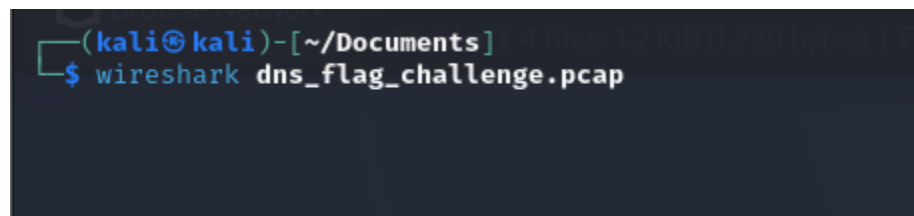
What we get:

- Youtube link direct to baby shark (babyshark actually means wireshark)
- Flag in DNS traffic, so need to inspect the DNS packet in pcap file

*BYcfFwTkOfSHVudHs0RE41XzN4Zmk0bHRyYTR0aTBufQ==*

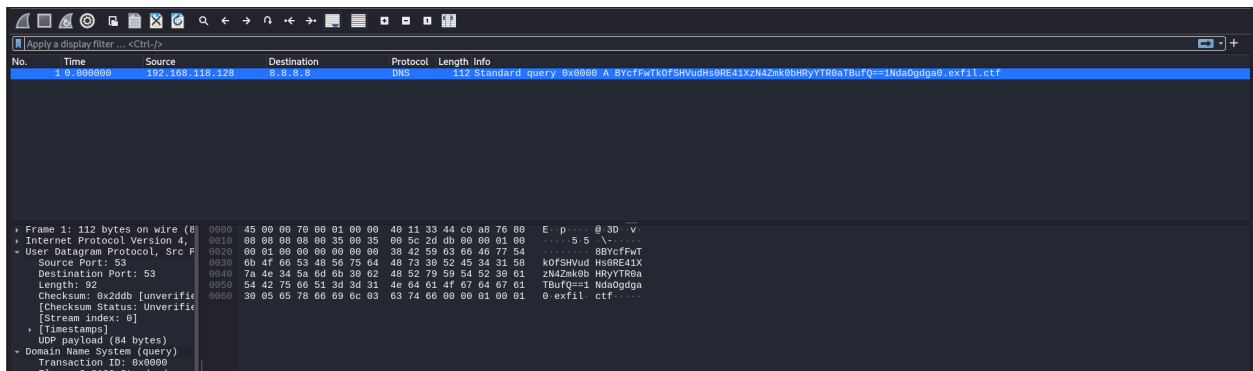
Use wireshark to open the pcap file

In Linux:



Or u may install wireshark on your window.

<https://www.wireshark.org/download.html>



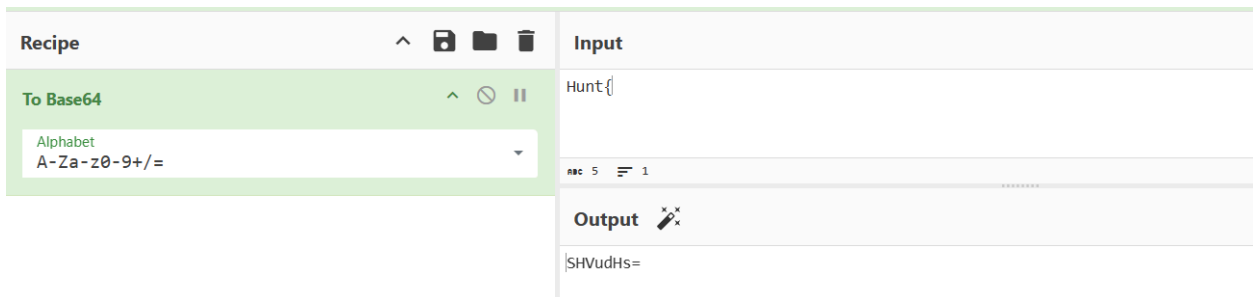
Then we found a string :

*BYcfFwTkOfSHVudHs0RE41XzN4Zmk0bHRyYTR0aTBufQ==1NdaOgdga0.exfil.ctf==*

- The == end is a common indicator of base64 encoding, hence flag might be

*BYcfFwTkOfSHVudHs0RE41XzN4Zmk0bHRyYTR0aTBufQ==*

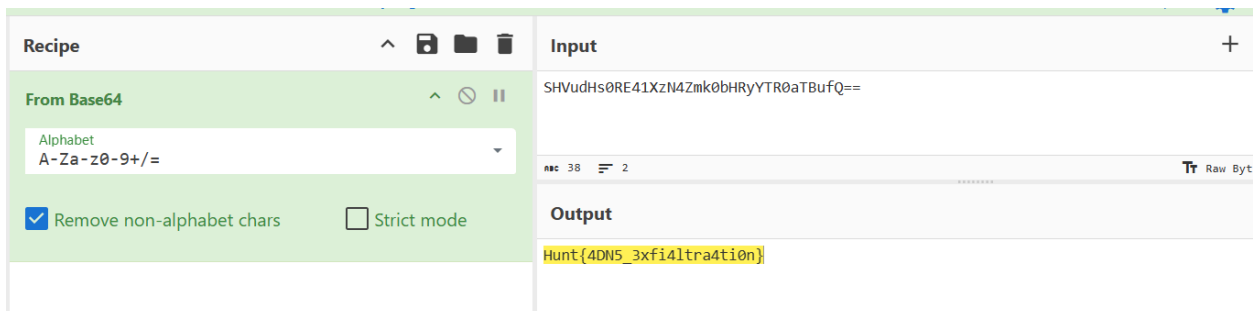
- but when we try to decode this string from base 64, we got invalid input, so u think you r not on the right track? Nono, as we know, the format for flag is Hunt{.....}. So now try to check what it's in base 64 form.



Cool, so the base 64 strings will start with SHVudHs, hence, the strings that we need:

*BYcfFwTkOfSHVudHs0RE41XzN4Zmk0bHRyYTR0aTBufQ==*

Now, decode it from base 64



Then, you will get the flag!

Website: <https://gchq.github.io/CyberChef/>