

# I filtered the packets by **length**, and in **tcp.stream eq 1** I found this hint :

The left pane shows a list of network packets from a traffic.pcapng file. The right pane shows a detailed view of a specific TCP stream (tcp.stream eq 1). The stream details the exchange between two hosts, with various messages like Key Exchange Init, Elliptic Curve Diffie-Hellman, and OPEN messages. Several messages contain encrypted data blocks, some of which are highlighted with red or blue boxes. A red circle highlights the word 'ke' in one message, and a blue circle highlights 'd ere' in another. A blue arrow points to a message containing 'd is t'. A red circle highlights 'd 4C95', and a blue circle highlights 'd he v'. A blue box highlights 'd ecto'. A red box highlights 'd r: 8'. A blue box highlights 'd BF46'. A red box highlights 'd C25D'. A blue box highlights 'd 9BAD'. A red box highlights 'd 98ED'. A blue box highlights 'd 8EAE'. A red box highlights 'd 6C1F'. A blue box highlights 'd 7AD2'.

# There is a hidden message in **tcp.stream eq 1**. I filtered the packets for each client. There were 2 messages :

Two separate Wireshark windows show the hidden messages for each client. The left window shows messages for client 1, and the right window shows messages for client 2. Both windows display a series of messages with their content partially obscured by dots. Red and blue boxes highlight specific words in these messages, such as 'd 11', 'd ere', 'd is t', 'd he v', 'd ecto', 'd r: 8', 'd BF46', 'd C25D', 'd 9BAD', 'd 98ED', 'd 8EAE', 'd 6C1F', and 'd 7AD2'.

# I copied them manually and I got the following encrypted data :

```
vector = 8BF46C25D9BAD98ED8EAE6C1F7AD2D04
key = 74C95604043427F0BEE1D0E16BFA53AFD537F736AD0073C4CC4E1CCB3A82B5DC
secret1 = uWyYTCYqBTy9afI69to3eK0ScCA3SIPDEzBsWBnR9D8Ro7aI0qihGMPXwu/Z+HLn
secret2 = KQ6R50gkQLYCKY90yIBDHdznHRUyMaTijWmHO30UXjwftOMIGgZJhKh2xli7Sqln
```

# This is an AES CBC. Run the following script to decrypt the flag :

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import base64

def aes_cbc_decrypt(ciphertext, key, iv):
    cipher = AES.new(key, AES.MODE_CBC, iv)
    plaintext = cipher.decrypt(ciphertext)
    return unpad(plaintext, AES.block_size)

def try_decrypt_flag(ciphertext, key, iv) :
    try:
        pt = aes_cbc_decrypt(ciphertext, key, iv)
        print(pt.decode(errors="ignore"))
    except Exception as e:
        print("error : ", e)

def main() :
    key_hex =
"74C95604043427F0BEE1D0E16BFA53AFD537F736AD0073C4CC4E1CCB3A82B5DC"
    iv_hex = "8BF46C25D9BAD98ED8EAE6C1F7AD2D04"
    secret1_b64 =
"uWYTCYqBTy9afI69t03eK0ScCA3S1PDEzBsWBnR9D8Ro7aIOqihGMPXwu/Z+HLn"
    secret2_b64 =
"KQ6R50gkQLYckY90yIBDHdznHRUyMaTijWmHO30UXjwftOMIGgZJhKh2xli7Sqln"

    key = bytes.fromhex(key_hex)
    iv = bytes.fromhex(iv_hex)
    ciphertext1 = base64.b64decode(secret1_b64)
    ciphertext2 = base64.b64decode(secret2_b64)

    try_decrypt_flag(ciphertext2, key, iv)
    try_decrypt_flag(ciphertext1, key, iv)

if __name__ == "__main__":
    main()
```

THE FLAG :

CTF{25B24F21A9B698C026A7FF6D911B252414260C11A4A7F46DD6885C9BAA0A5386}  
~Z4que