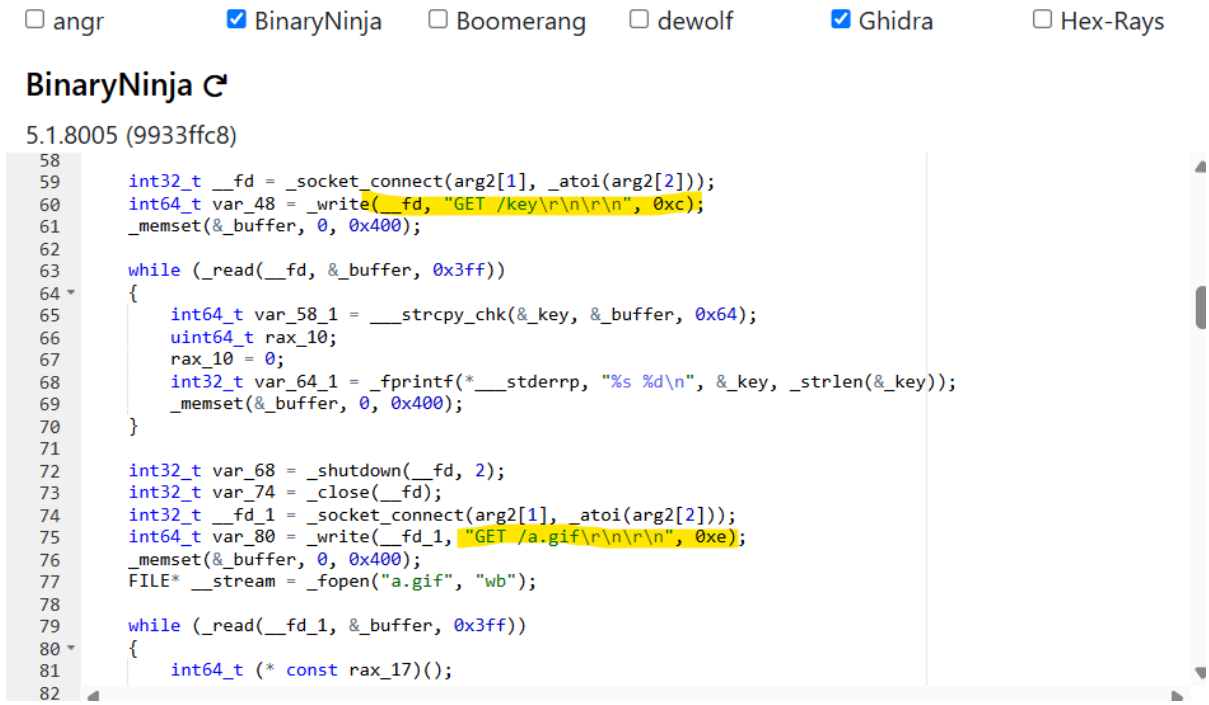
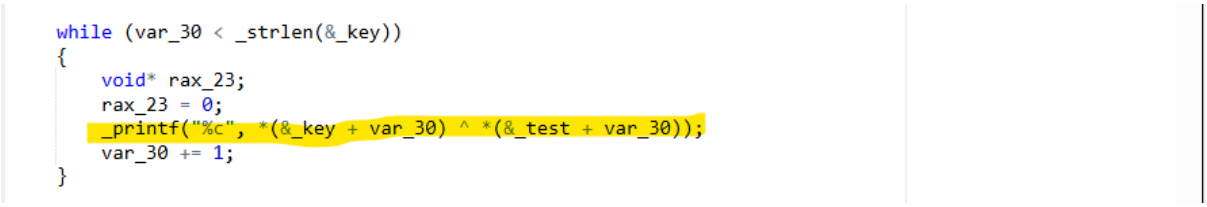
Looking through Wireshark at conversations, we can see a lot of TCP streams (**172**). I ran the following shell script to export all the TCP outputs in a single file (**tcp.sh**)

```
for stream in $(tshark -r chall.pcapng -Y "tcp.stream" -T fields -e tcp.stream | sort -n | uniq); do
  echo "=== TCP Stream $stream ==="
  tshark -r chall.pcapng -q -z follow,tcp,ascii,$stream
  echo
done
```

chmod +x tcp.sh
./tcp.sh > file.txt

And I found nothing special. I started to inspect the second file (**a.out**) and I found out that it is an executable. And because I cannot run it, I decompiled it with an online tool and I found some hints.I found 2 “files” and a XOR function :





Looking through **file.txt,** I found the 2 files ne needed (stream 43 and 78) :

```
===================================================================

=== TCP Stream 43 ===

===================================================================
Follow: tcp,ascii
Filter: tcp.stream eq 43
Node 0: 192.168.1.12:50587
Node 1: 161.35.16.97:31337
12
GET /key


        70
AAAAAA85783cc847fb84e7ba9c1c727099c9040fe086fab96857227bedc4b3967ec978
===================================================================
```

```
===================================================================

=== TCP Stream 78 ===

===================================================================
Follow: tcp,ascii
Filter: tcp.stream eq 78
Node 0: 192.168.1.12:50622
Node 1: 161.35.16.97:31337
14
GET /a.gif


        70
....:x.S.Y
W....U...S.SX
TT.S.Q..
W
RP...SY..UTZR[..WPQRU..
.UZ..PR[TE
```

Now I copied the content as **raw** (hex) and I wrote a Python script to use the key to XOR the GIF. You cannot open the GIF because it's just text. So, when the script ends, just cat the gif. And I forgot, remove the **AAAAAA** from the key

The Python code :

```
def hex_to_bytes(hex_string):
    return bytes.fromhex(hex_string)

def xor_decrypt(data, key):
    return bytes(data[i] ^ key[i % len(key)] for i in range(len(data)))

def main():
    key_data =
hex_to_bytes("414141414141383537383363633834376662383465376261396331633732373039396339303430666530383666616239363835373232376265646334623339363765633937 38")
```

```
    gif_data =
hex_to_bytes("040212023a78085300590a570608040f55030101530053580d54540253015
109080d570d525006070753590005555 45a525b040f575051525500050d01555a030f50525
b5445")

    decrypted_data = xor_decrypt(gif_data, key_data)

    with open("decoded.gif", "wb") as f:
        f.write(decrypted_data)
    print("finish")

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

THE FLAG :
ECSC{90f7a94e0083a95671947ead3f91444bd6abca6c46cdc18ebf00df9cfc5851bc}
~Z4que