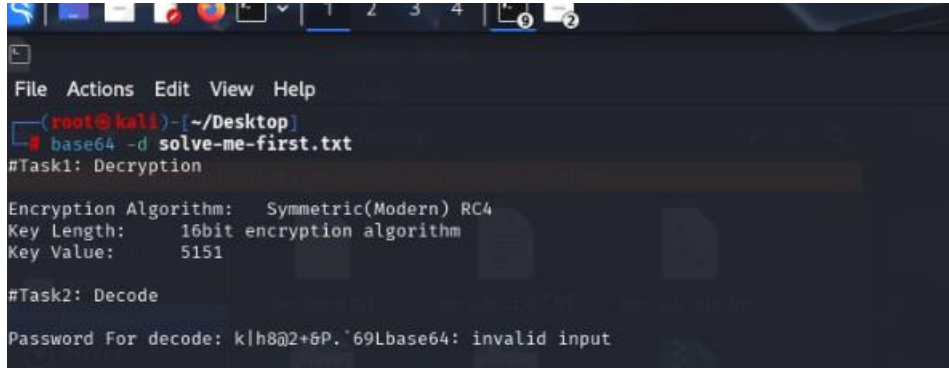


# 1. Decoding text using base64

The content of the file is encoded in **Base64**, a common method for transmitting binary data in text format. On decoding, it reveals task instructions in plain text.

A terminal window with a dark background and light-colored text. The prompt is '(root@kali) ~/Desktop'. The command 'base64 -d solve-me-first.txt' has been entered. The output shows task instructions for decryption and decoding, including encryption details and a password for decoding.

```
(root@kali) ~/Desktop
base64 -d solve-me-first.txt
#Task1: Decryption

Encryption Algorithm:  Symmetric(Modern) RC4
Key Length:           16bit encryption algorithm
Key Value:             5151

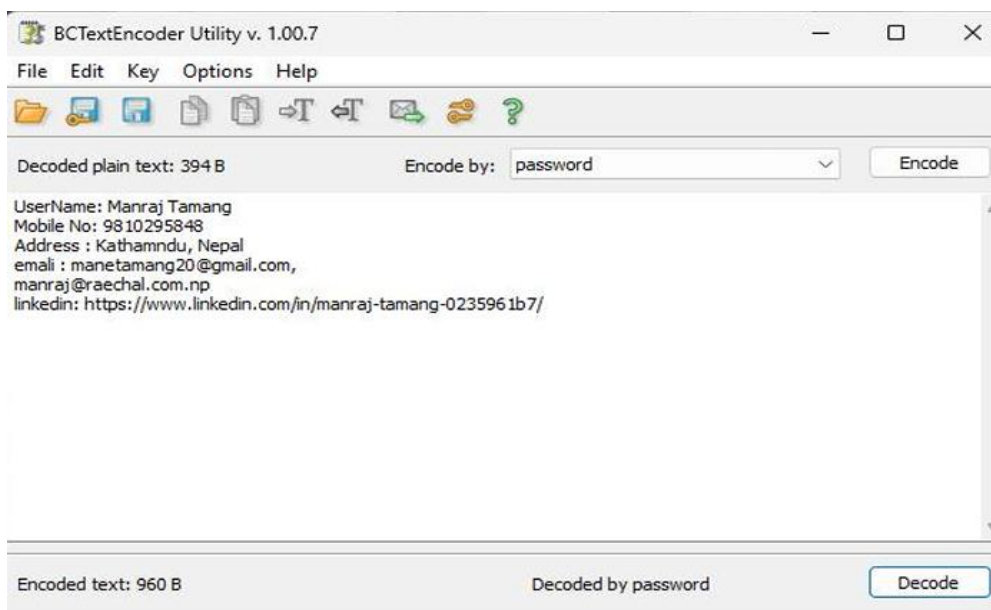
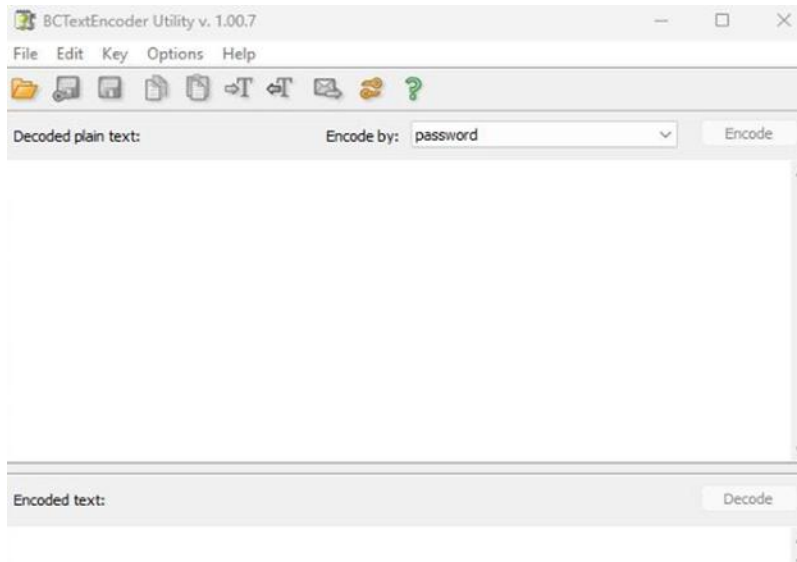
#Task2: Decode

Password For decode: k|h8@2+6P.'69Lbase64: invalid input
```

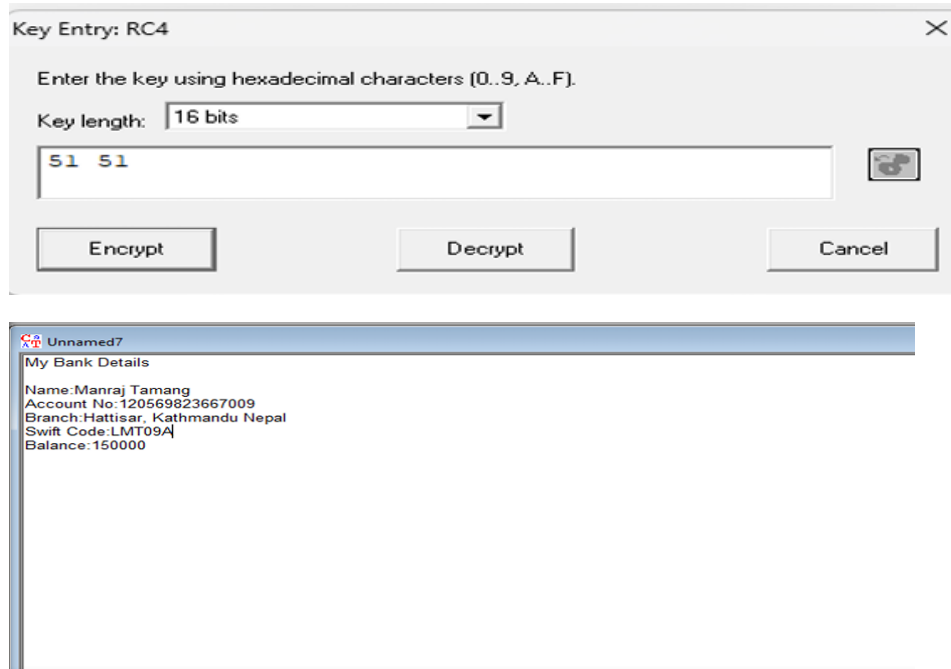
The information obtained is:

- Algorithm: Symmetric(modern)RC4
- Key value is 5151
- Key length is 16 bit
- Password for decode k|h802+6P.'69L

## 2. Decoding text using BCTextEncoder



### 3. Decryption using RC4 algorithm



This file contains **encrypted data represented in hexadecimal format**. It's a common representation for binary ciphertext when transmitting or storing data in a text-based medium. According to the hints from `solve-me-first.txt`, this file is encrypted using the **RC4 symmetric stream cipher** with the key 5151.

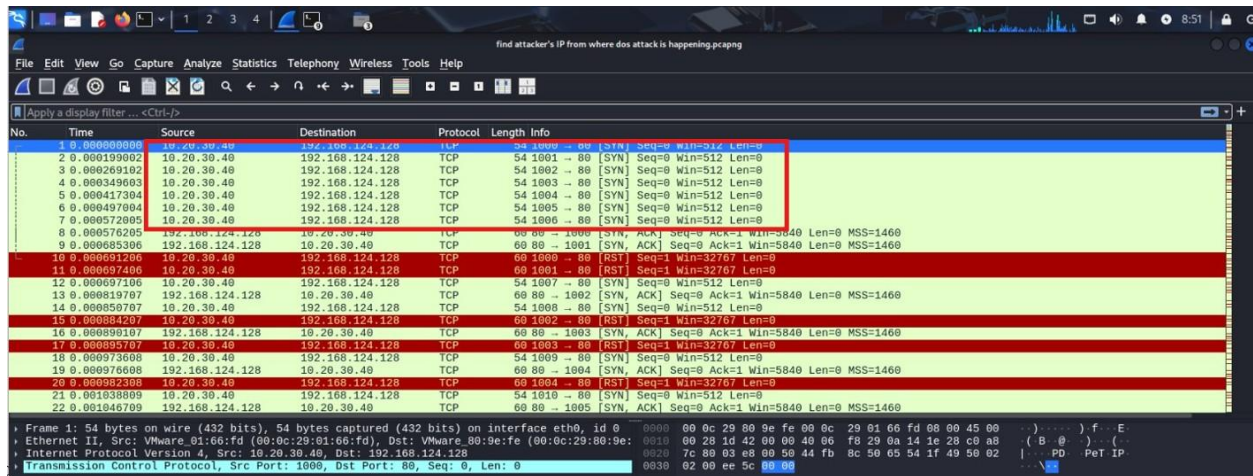
The information includes private banking information “My Bank Details”:

- Account Holder: Manraj Tamang
- Account Number: 120569823667009
- Branch: Hattisar, Kathmandu, Nepal
- Swift Code: LMT09A
- Account Balance :150,000

## 4. Finding attackers IP from where DOS attack is happening using Wireshark:

**Wireshark** is a free and open-source network protocol analyzer. It lets you capture, inspect, and analyze network traffic in real time or from saved packet capture files (e.g., .pcap, .pcapng).

Using tool called Wireshark to look at DOS attack:

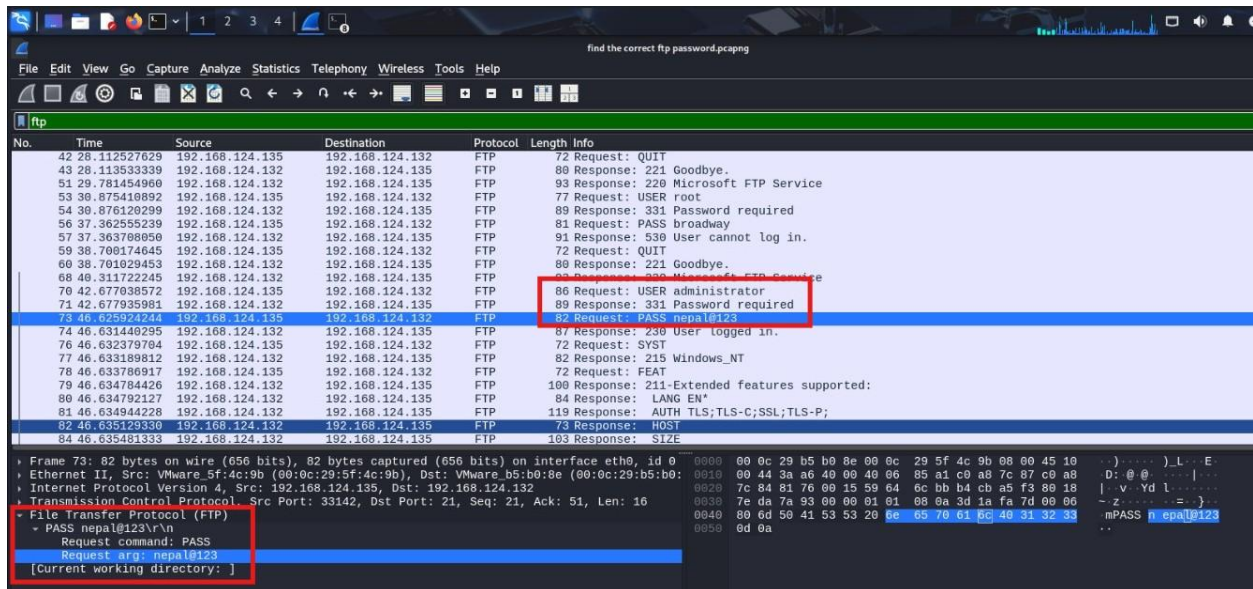


The highlighted parts show many connection requests (TCP SYN packets) coming from the **IP address 10.20.30.40** to port 80 on the **IP 192.168.124.128**.

This repeated is a sign of a SYN flood attack where someone tries to overload a server by sending too many fake connection requests.

## 5. Finding the correct ftp password using Wireshark:

Using tool called Wireshark to look at Network traffic:



It shows an FTP session where I found the login details sent in plain text.

- Username: “administrator”
- Password: “nepal@123”

“230 User logged in” confirm that the login was successful. This shows how using unencrypted protocols like FTP.