

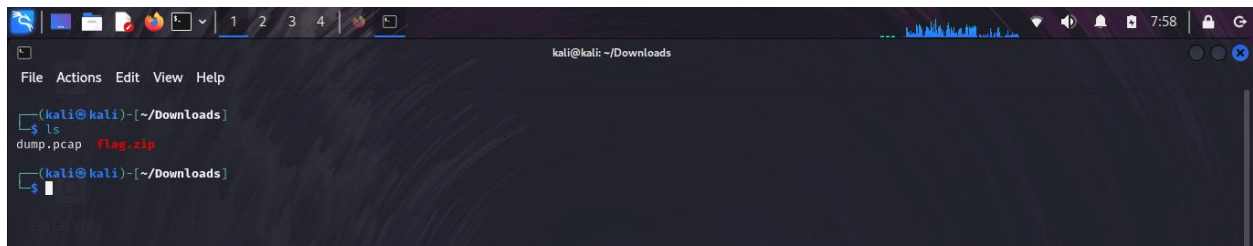
LinkedIn: [Kelvin Kimotho](#)

## Description

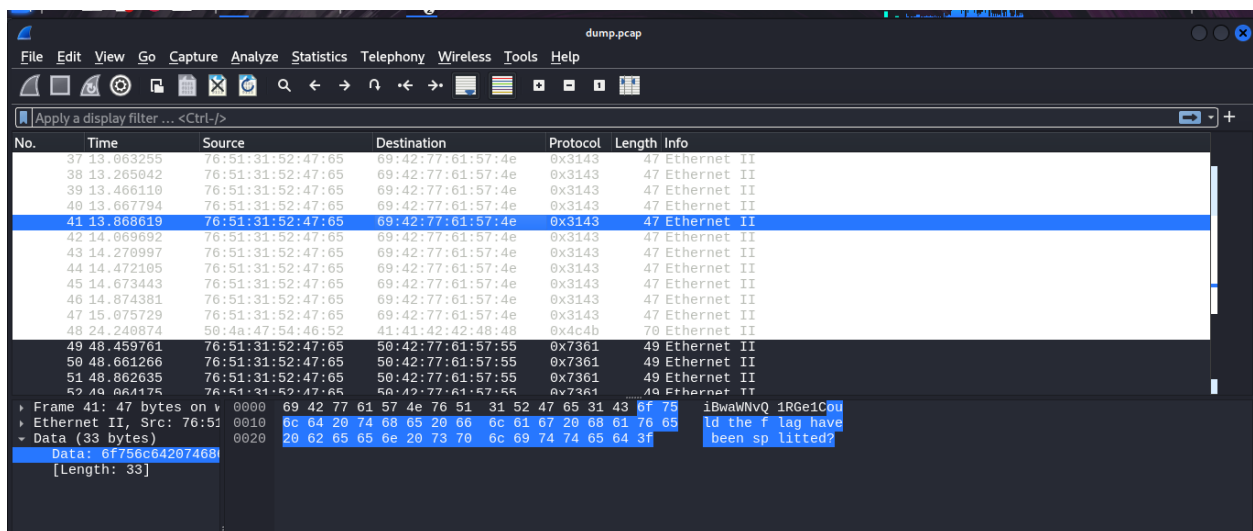
Someone might have hidden the password in the trace file. Find the key to unlock this file. This tracefile might be good to analyze.

### Solution

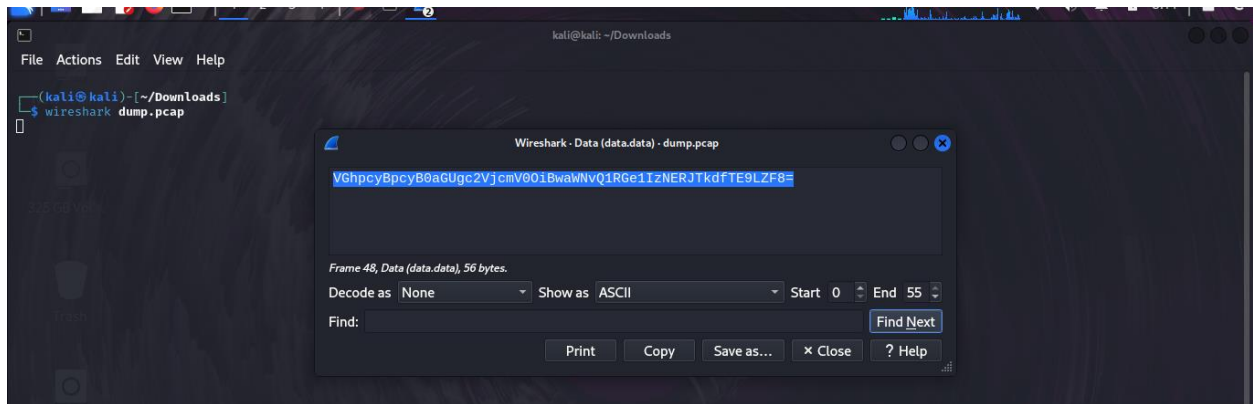
I first downloaded two files: dump.pcap, which appeared to be a network trace file, and flag.zip, a password-protected ZIP archive. My goal was to analyze the trace file (dump.pcap) to uncover any hidden password or key that could unlock the flag.zip file.



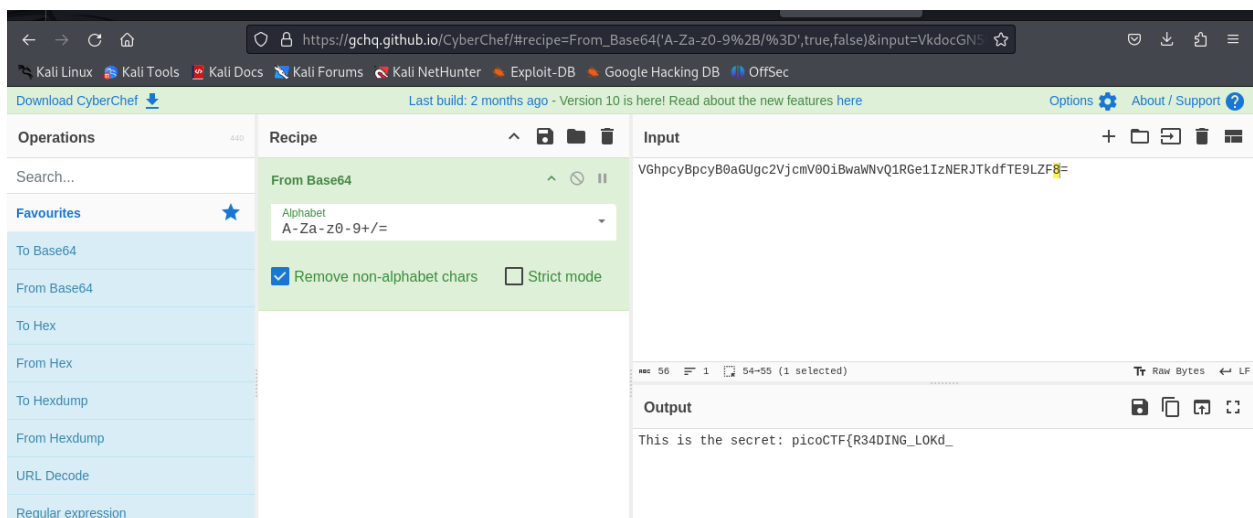
To begin, I used Wireshark, a powerful network protocol analyzer, to inspect the contents of the dump.pcap file. My objective was to carefully examine the packets for any suspicious patterns, plaintext credentials, or hidden clues that could reveal the password.



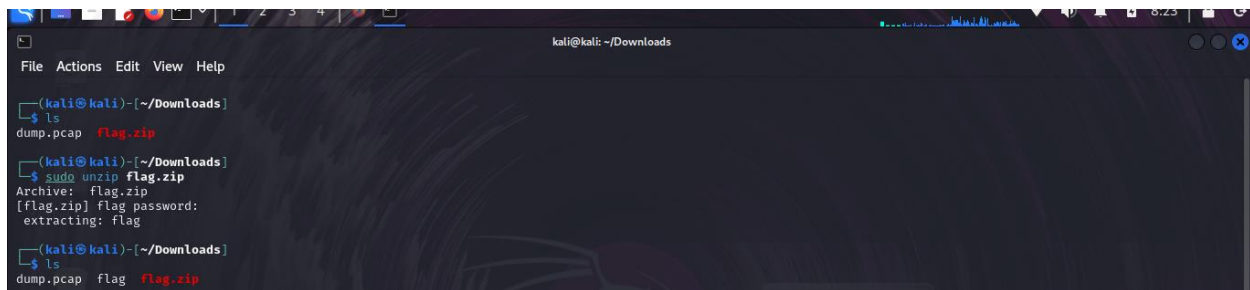
After some thorough analysis of the dump.pcap file in Wireshark, I came across a packet that caught my attention. Upon closer inspection, the payload contained what appeared to be Base64-encoded data. "VGhpncyBpcyB0aGUgc2VjcmV0OiBwaWNvQ1RGe1IzNERJTkdfTE9LZF8="



To decode the Base64-encoded string, I used CyberChef, a versatile tool for data analysis and decoding. After pasting the string  
VGhpcyBpcyB0aGUgc2VjcmV0OiBwaWNvQ1RGe1IzNERJTkdTE9LZF8= into CyberChef and selecting the "From Base64" operation, the decoded output revealed.



With the decoded secret in hand, I proceeded to use picoCTF{R34DING\_L0Kd\_ as the password to unlock the flag.zip file. I ran the following command to extract the contents of the ZIP archive.

A terminal window on a Kali Linux system. The user is in the ~/Downloads directory. They run 'ls' and see 'dump.pcap' and 'flag.zip'. Then they run 'sudo unzip flag.zip'. The terminal shows the password prompt, the password 'flag', and the extraction progress. Finally, they run 'ls' again and see 'dump.pcap', 'flag', and 'flag.zip'.

```
kali@kali: ~/Downloads
File Actions Edit View Help

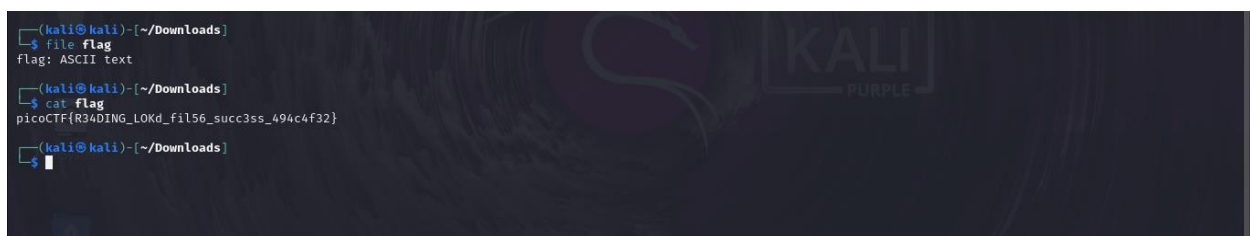
(kali@kali)-[~/Downloads]
$ ls
dump.pcap  flag.zip

(kali@kali)-[~/Downloads]
$ sudo unzip flag.zip
Archive:  flag.zip
[flag.zip] flag password:
extracting: flag

(kali@kali)-[~/Downloads]
$ ls
dump.pcap  flag  flag.zip
```

The password worked successfully, and the contents of the archive were extracted. This confirmed that the Base64-encoded string found in the packet contained the correct key to access the flag.

After successfully extracting the contents of the flag.zip file, I found a file named flag. To determine its type, I ran the file command. The output indicated that it was an ASCII text file. To view its contents, I used the cat command. This revealed the final flag.

A terminal window on a Kali Linux system. The user runs 'file flag' and gets 'flag: ASCII text'. Then they run 'cat flag' and see the flag 'picoCTF{R34DING\_LOKd\_fil56\_succ3ss\_494c4f32}'.

```
(kali@kali)-[~/Downloads]
$ file flag
flag: ASCII text

(kali@kali)-[~/Downloads]
$ cat flag
picoCTF{R34DING_LOKd_fil56_succ3ss_494c4f32}

(kali@kali)-[~/Downloads]
$
```

With that, I successfully captured the flag and completed the challenge.

## Conclusion

By systematically analyzing the dump.pcap file using Wireshark, I was able to identify a Base64-encoded string embedded in a packet. Decoding this string with CyberChef provided the password necessary to unlock the flag.zip archive. Finally, by using simple commands like file and cat, I accessed the extracted flag and completed the challenge.