SECTALKS CTF 0x04 Solution

swarley, kronicd

 $\mathrm{May}\ 21,\ 2014$

0.1 START

We have a 128 byte file named 'key' and a 4 MB file named 'mail'. After messing around thinking the key was the actual AES encryption key kronicd realised it was the password.

From there it was a matter of stripping the mail headers from the mail file, and decrypting it with the keyfile.

```
{\tt swarley@Pro: openssl \ enc \ -d \ -aes-128-cbc \ -kfile \ key \ -in \ mail \ -out \ decrypt}
```

Open decrypt in texteditor and strip the header and footer to leave a nice block of base64'd data (which is likely an mp4 given the name of the "attachment")

```
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="W1EBFwEcSaQ.mp4"
Content-Transfer-Encoding: base64
```

Then it was a case of decoding the base64'd data into our mp4 file thusly:

```
swarley@Pro: base64 -D -i decrypt2 -o fuckyou.mp4
```

0.2 FIN

```
<flag>
flag: the radio is playing some sort of.. rick roll
</flag>
```

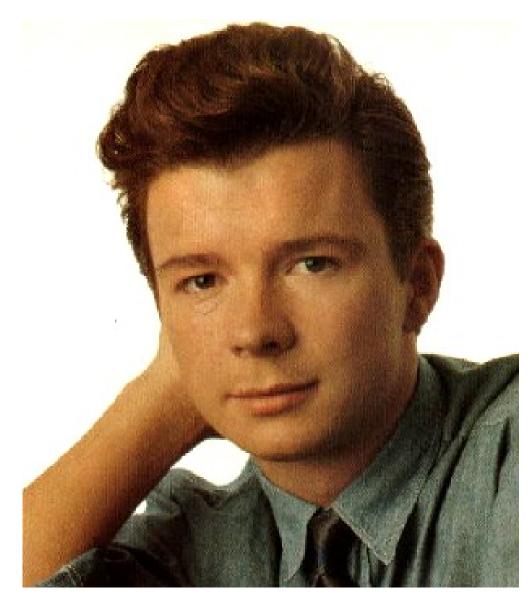


Figure 1: A mad wicked sick image of the man himself.