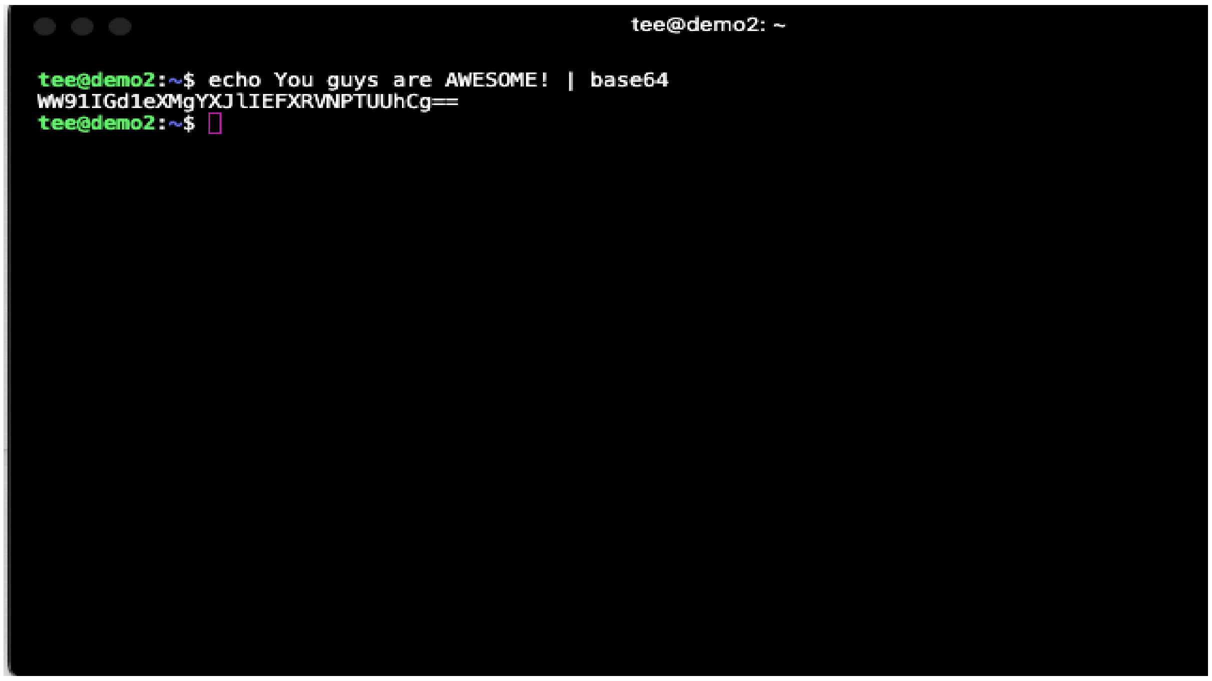
Encoding v. Hashing Assignment

Step 1

Type in ‘echo You guys are AWESOME! | base64’ in the Linux interface

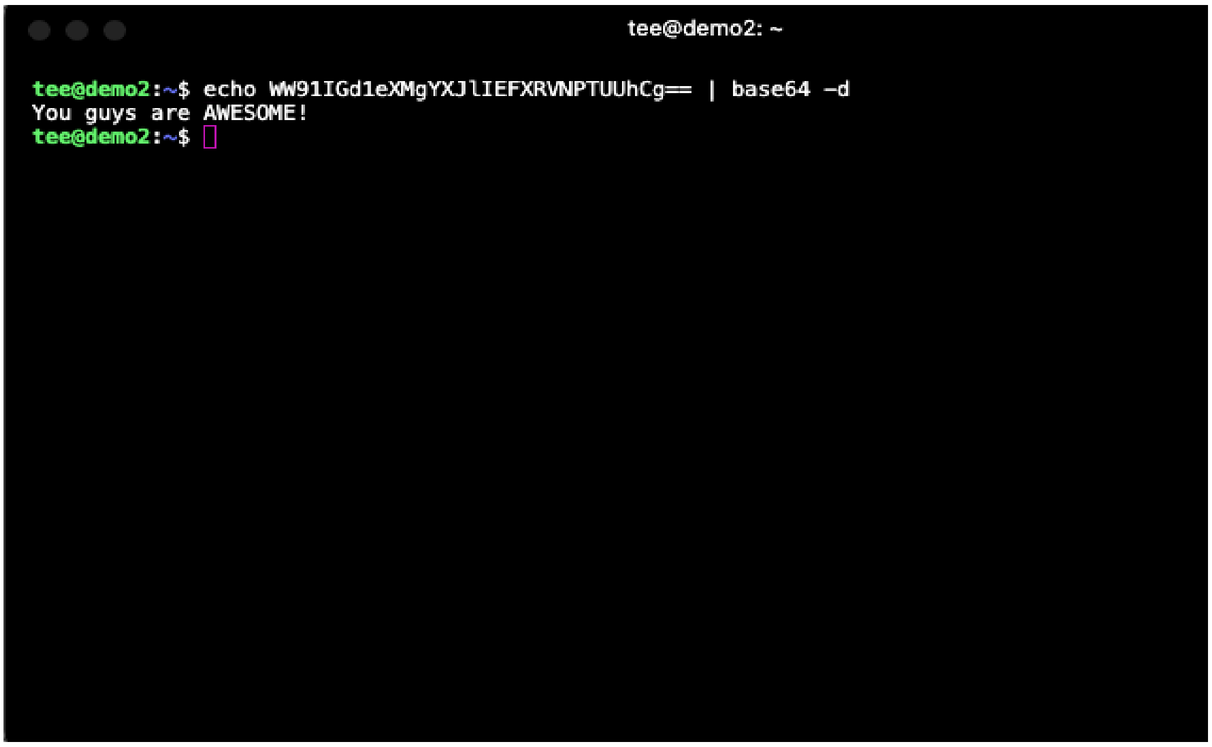


```
tee@demo2:~$ echo You guys are AWESOME! | base64
WW91IGd1eXMgYXJlIEFXRVNPTUUhCg==
tee@demo2:~$ 
```

This command encodes the text “You guys are AWESOME” using base64 as displayed above. The output of the coded text can also be seen above.

Step 2

Type in ‘echo <encoded output> | base64 -d’ to decode the previously encoded text line. This is illustrated below:

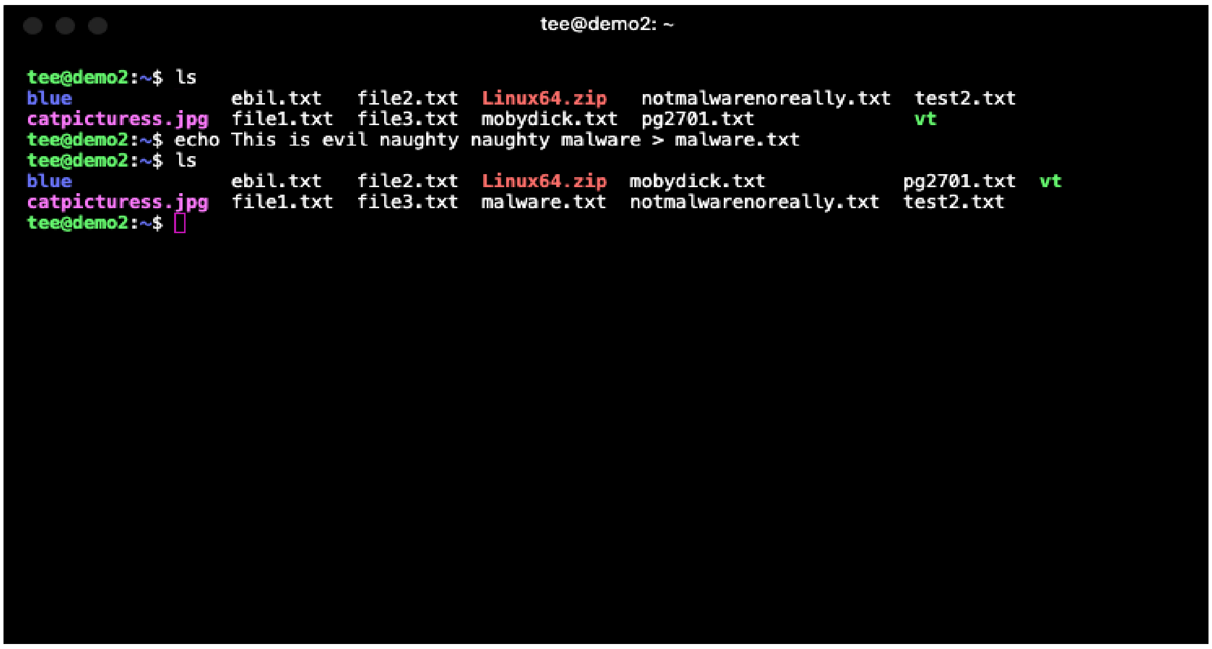


```
tee@demo2:~$ echo WW91IGd1eXMgYXJlIEFXRVNPTUUhCg== | base64 -d
You guys are AWESOME!
tee@demo2:~$ 
```

This shows that an encoded text can be decoded to reveal the plaintext format.

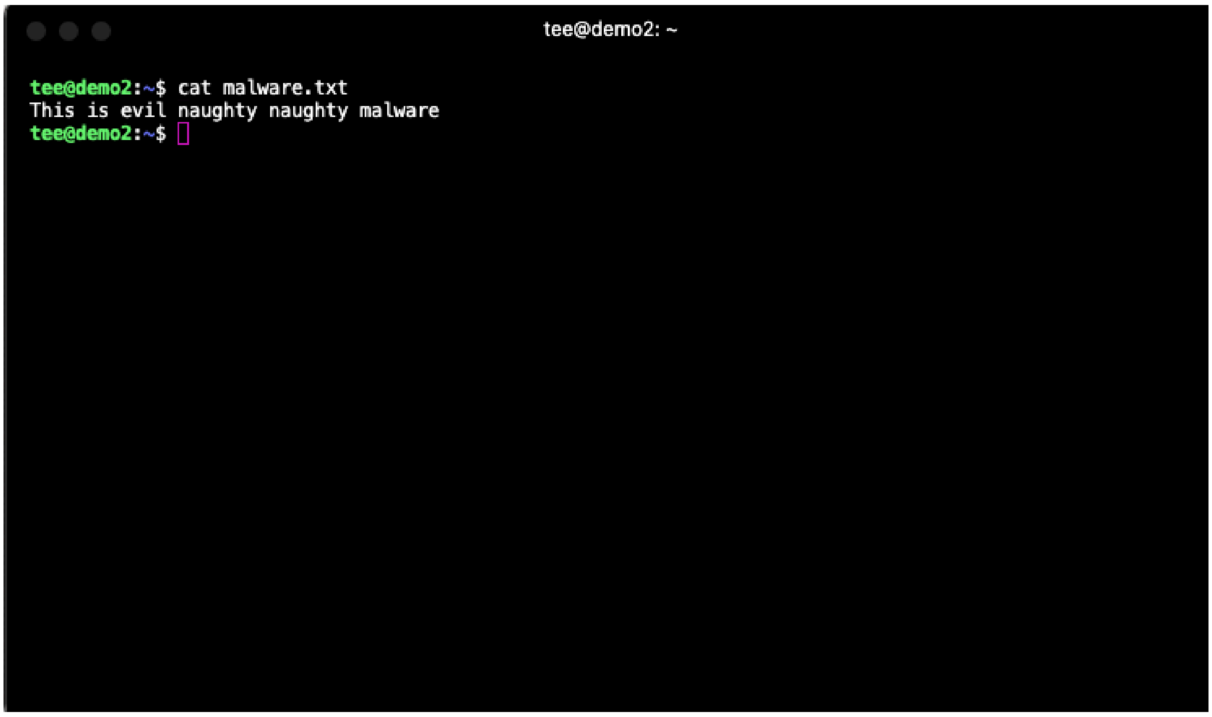
Step 3

Type ‘echo This is evil naughty naughty malware > malware.txt’



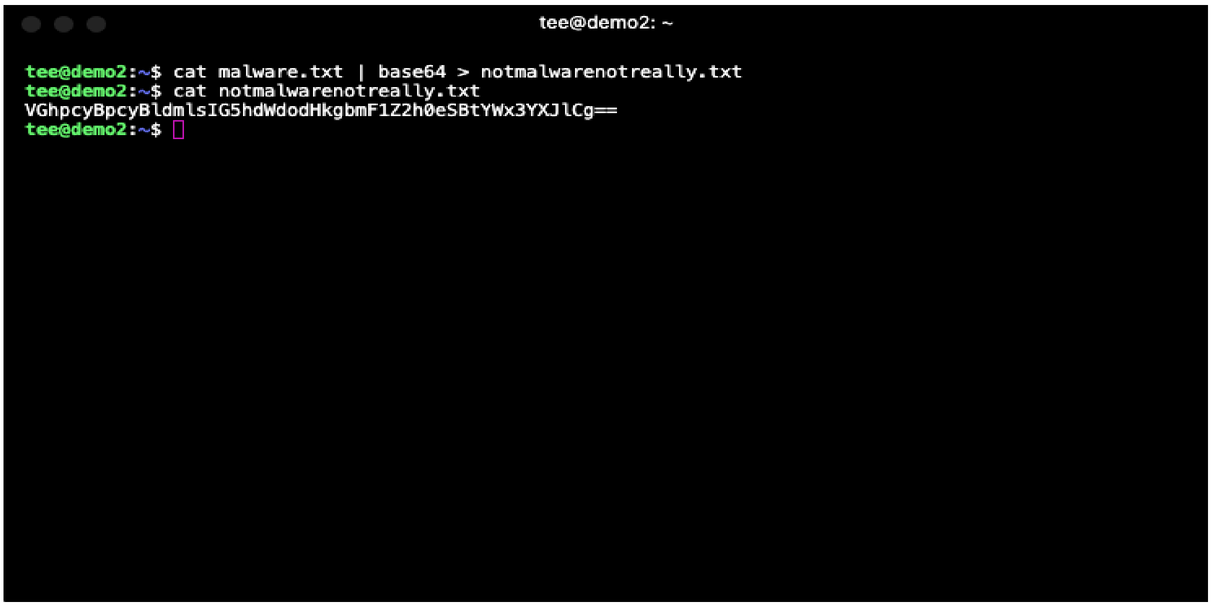
```
tee@demo2:~$ ls
blue             ebil.txt   file2.txt  Linux64.zip   notmalwarenoreally.txt  test2.txt
catpicturess.jpg file1.txt  file3.txt  mobydick.txt  pg2701.txt              vt
tee@demo2:~$ echo This is evil naughty naughty malware > malware.txt
tee@demo2:~$ ls
blue             ebil.txt   file2.txt  Linux64.zip  mobydick.txt            pg2701.txt  vt
catpicturess.jpg file1.txt  file3.txt  malware.txt  notmalwarenoreally.txt  test2.txt
tee@demo2:~$
```

The above command creates and writes the text “This is evil naughty naughty malware” to a file named malware.txt file. To confirm this, cat the malware.txt file as illustrated below:



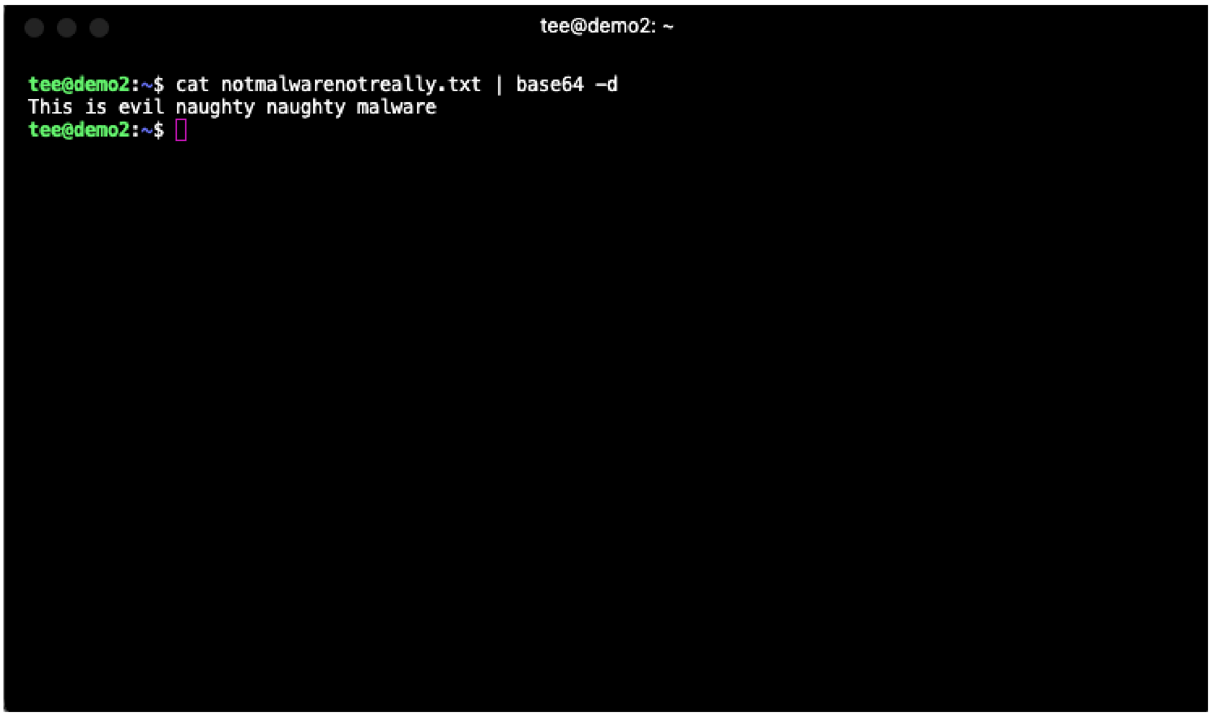
```
tee@demo2:~$ cat malware.txt
This is evil naughty naughty malware
tee@demo2:~$
```

To encode the content of the file malware.txt and save them in a new file, use the following command: cat malware.txt | base64 > notmalwarenotreally.txt. This is illustrated below:


tee@demo2: ~

```
tee@demo2:~$ cat malware.txt | base64 > notmalwarenotreally.txt
tee@demo2:~$ cat notmalwarenotreally.txt
VGhpcyBpcyBldmlsIG5hdWdodHkgbmF1Z2h0eSBtYWx3YXJlCg==
tee@demo2:~$ 
```

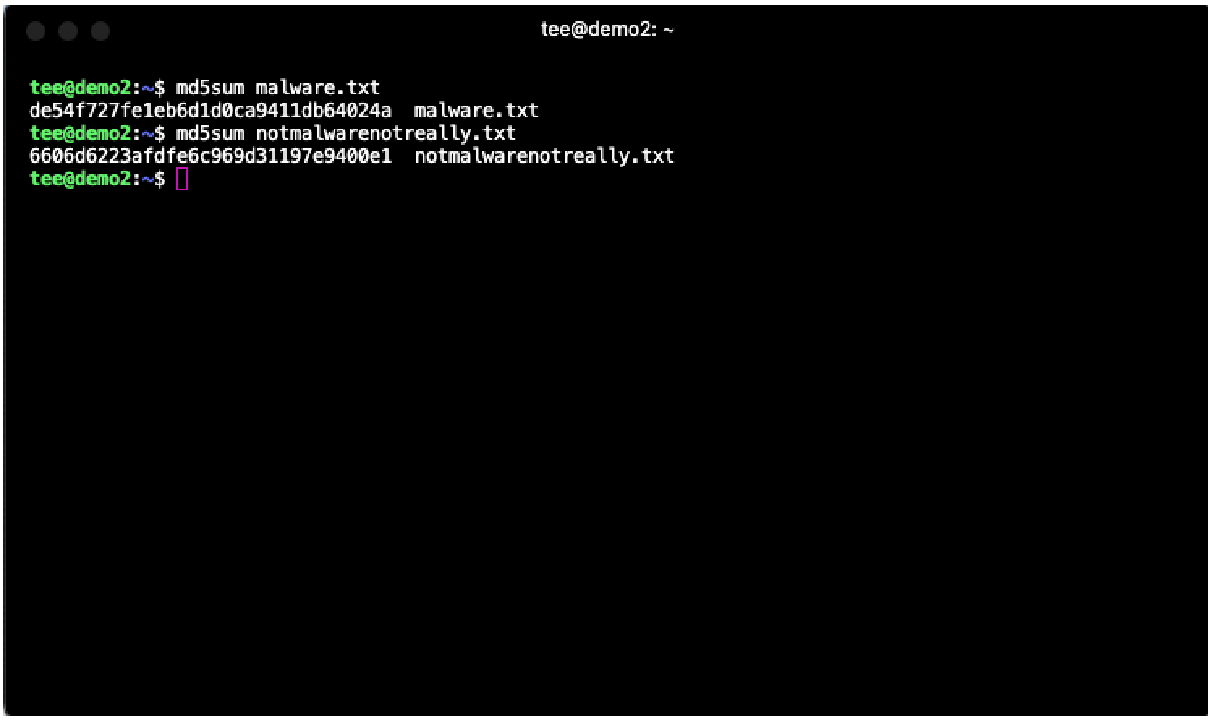
As shown above, catting the new file notmalwarenotreally.txt reveals the coded content of the file. It is encoded and NOT human readable. To decode the content of this file, the following command will be used: cat notmalwarenotreally.txt | base64 -d as illustrated below:


tee@demo2: ~

```
tee@demo2:~$ cat notmalwarenotreally.txt | base64 -d
This is evil naughty naughty malware
tee@demo2:~$ 
```

This confirms that the encoding and decoding was successful.

Step 4
Finally, both files (malware.txt and notmalwarenotreally.txt) will be hashed to establish that even though they carry the same content, the plaintext version will carry a different hash compared to the encoded version. To achieve this, both files will be hashed using the 'md5sum' command as shown below:



```
tee@demo2:~$ md5sum malware.txt
de54f727fe1eb6d1d0ca9411db64024a  malware.txt
tee@demo2:~$ md5sum notmalwarenotreally.txt
6606d6223afdfe6c969d31197e9400e1  notmalwarenotreally.txt
tee@demo2:~$ 
```

This is an example of how attackers can use encoding to disguise malicious files in order to bypass signature based antivirus systems.