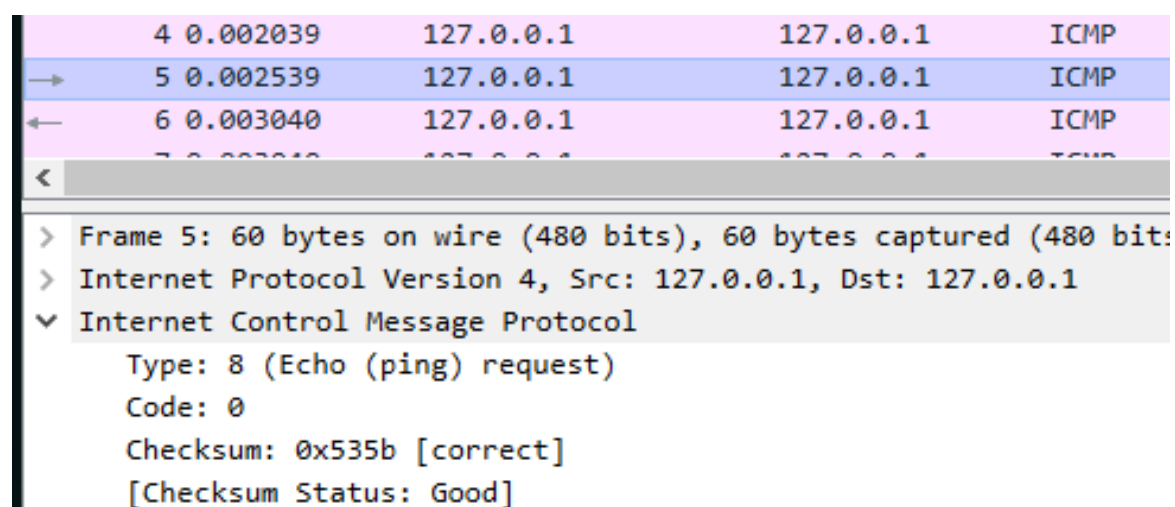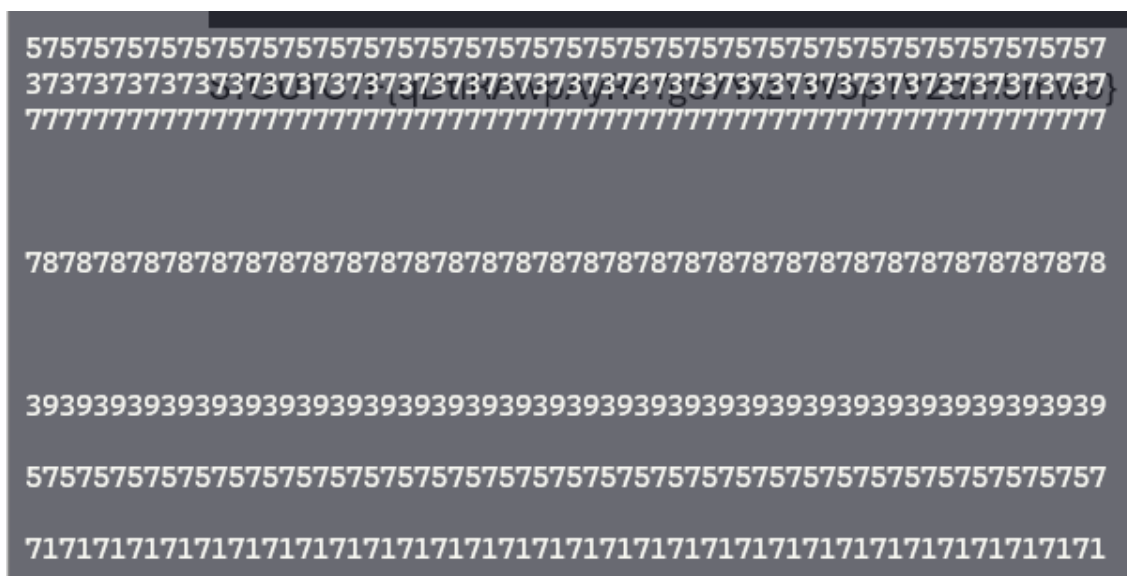# The echo

When opening the wireshark file. We can see strings in every packet. We can use tshark to extract data from wireshark via linux terminal. After understanding about the data in wireshark, I know we need to extract the data field. This solve is one liner so I apologise because it's not so beginner friendly. But I'll give the visualisation on why I use this command.

```
tshark -r TheEchos.pcap -Y "icmp.type == 8" -T fields -e data | cut -c 1-2 | tr -d '\n'
```

Baically, -r is we reading the file. We need the data in icmp because theres only icmp packet. If you take a look at one of the packet, there is type 8 mentioned.

Then -e data is just extracting data. Using | (pipe) command to use multiple command. Using tshark -r TheEchos.pcap -Y "icmp.type == 8" -T fields -e data we get below

Add the cut -c 1-2 to get below.

57
37
77

78

39
57
71

Add tr -d '\n' to get concatenate all of them


```
┌──(zeqzoq㉿zeqzoq)-[/mnt/c/Users/hzqzz/Downloads]
└─$ tshark -r TheEchos.pcap -Y "icmp.type == 8" -T fields -e data | cut -c 1-2 | tr -d '\n'
Warning: program compiled against libxml 212 using older 209
```

394a414a79356669755433716577684241524c575352754b7a5248387070656b3575457336656d d7a354c54324b70367055467a424c56675671336f42
647979306156696d d556d396d70685651594349695363553763625a72767430414b5a6468545873306d d7a6e6b726555574a595863494923657334774546a
694d615066695a53417339586c c553172716130547539357976706e24e7078776766555565907356393541142585348416361664667707179714c4e3165
575936736e4d376747555541723471646464744f56654856656e66e6161434e464a565255315371634d476c784e38343354e506d61576c654c724445
36776c73775777794a47587845727207664755634e7832683861766a54426566953727076b747a777652634c72664c62315a304c493938433955796e
38536333331305676775778764e77697267664a706f4b416d54526769384f72515a6c665a4c6e544c684369706d4d766664e477a4c31504A4257707268
6635674e426872412415241306f444d636369950376a4f434277786c446c44e4d4a5226b33794335766e6777726f38686d6f71507733c324f77
4862526847545a77417a5a3756764e70574b754d6c7379474f77423758634d306d5a6a5877743167671034686e30627835686574546c c3347c526616442
336c33427a6d d68356b7853384d7a4376364b6751756d614d63707367545424261361671f5032523646534741674950716536673136744236b71564e6b
726f4855662504416f4d70676976704c45414d64a7a77637635441366616f654e52373743546f56664e6383b5771745976474f46331574075051544d7a3643
4331624c57576e46594d743773705550310315686674c596f666693651c6a34737a44344365323764483706f333177747043644c387846e5846345a6d6f465835
51794c525525871322384e77357178534958443156c6c79354c6a533975654447324b6335c5387a69514d5069796b6e7650544438623177d47534b624657
```

We know wireshark use hex. So go to cyberchef and find flag



STOUTCTF{fZtPEj720e1OKFrQPqouICBdgVAtD14N}