Stage 1

Opening up the zip file and trying to extract it will yield you a nice password prompt, which means we really have to crack the password for this zip file.

Thankfully, the question text has provided and narrowed down the list of passwords to a decent size, so we first generate the password list based on the rules provided:

```
#!/usr/bin/python3

with open('pwlist.txt', 'w+') as f:
    for i in range(0, 0xffffff + 1):
        f.write('{:06x}\n'.format(i))
```

From there, we can use `zip2john` to get the password:

```
kali@kali:~/Downloads$ sudo zip2john b1ed57b7cf34d91e7dd1301597ff9101.zip >
./hash.txt; xxd ./hash.txt | head
ver 2.0 b1ed57b7cf34d91e7dd1301597ff9101.zip/temp.mess PKZIP Encr: cmplen=89166,
decmplen=155774, crc=5FA60D93
00000000: 6231 6564 3537 6237 6366 3334 6439 3165  b1ed57b7cf34d91e
00000010: 3764 6431 3330 3135 3937 6666 3931 3031  7dd1301597ff9101
00000020: 2e7a 6970 2f74 656d 702e 6d65 7373 3a24  .zip/temp.mess:$
00000030: 706b 7a69 7032 2431 2a31 2a32 2a30 2a31  pkzip2$1*1*2*0*1
00000040: 3563 3465 2a32 3630 3765 2a35 6661 3630  5c4e*2607e*5fa60
00000050: 6439 332a 302a 3237 2a38 2a31 3563 3465  d93*0*27*8*15c4e
00000060: 2a35 6661 362a 3962 3430 2a31 3433 3563  *5fa6*9b40*1435c
00000070: 6361 3233 3530 3730 6333 3533 3365 3238  ca235070c3533e28
00000080: 3965 3731 6331 3639 3963 6239 3863 6161  9e71c1699cb98caa
00000090: 3262 3937 3566 3038 3530 3766 3931 3064  2b975f08507f910d
```

Then we use `john` to crack the password itself with the wordlist we made:

```
kali@kali:~/Downloads$ sudo john --wordlist=pwlist.txt ./hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)
kali@kali:~/Downloads$ sudo john --show ./hash.txt
b1ed57b7cf34d91e7dd1301597ff9101.zip/temp.mess:362459:temp.mess:b1ed57b7cf34d91e7d
d1301597ff9101.zip::b1ed57b7cf34d91e7dd1301597ff9101.zip

1 password hash cracked, 0 left
```

We can finally unzip the encrypted file with the password `362459`, only to find that it is a mess.

```
kali@kali:~/Downloads$ unzip b1ed57b7cf34d91e7dd1301597ff9101.zip
Archive:  b1ed57b7cf34d91e7dd1301597ff9101.zip
[b1ed57b7cf34d91e7dd1301597ff9101.zip] temp.mess password:
(line too long--try again)
[b1ed57b7cf34d91e7dd1301597ff9101.zip] temp.mess password:
replace temp.mess? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: temp.mess
kali@kali:~/Downloads$ file temp.mess
temp.mess: ASCII text, with very long lines, with no line terminators
kali@kali:~/Downloads$ xxd temp.mess | head
00000000: 3166 3862 3038 3030 3439 3937 3261 3566  1f8b080049972a5f
00000010: 3032 6666 3030 3037 3430 6638 6266 6664  02ff000740f8bffd
00000020: 3337 3761 3538 3561 3030 3030 3034 6536  377a585a000004e6
00000030: 6436 6234 3436 3032 3030 3231 3031 3136  d6b4460200210116
00000040: 3030 3030 3030 3734 3266 6535 6133 6531  000000742fe5a3e1
00000050: 6365 3364 6566 6665 3564 3030 3333 3139  ce3deffe5d003319
00000060: 3032 3631 6533 3666 6635 3662 6534 3066  0261e36ff56be40f
00000070: 3932 6637 6437 3831 3830 6361 6331 3431  92f7d78180cac141
00000080: 6633 6335 6131 3833 3832 3239 3136 3465  f3c5a1838229164e
00000090: 3037 6138 6539 3732 6638 3962 3966 6639  07a8e972f89b9ff9
```

From the file, we can see they probably use hex to encode the file, which means we have to unhexlify it and store it as a binary.

```
kali@kali:~/Downloads$ xxd -r -p temp.mess > 0
kali@kali:~/Downloads$ file 0
0: gzip compressed data, last modified: Wed Aug  5 11:26:01 2020, max compression,
original size modulo 2^32 77844
```

Unfortunately, it appears that the challenge creator has decided to use tons of compression libraries to obfuscate the final file.

After many hours of trying, I have decided to install `pigz` to handle `zlib` files, and just running a python script to handle ripping apart the data (the source code for rip.py is at stage1/rip.py)

```
kali@kali:~/Downloads/tisc1new$ python3 rip.py 0
0 is a gzip file
1 is a XZ file
2 is a hex ASCII file
3 is a XZ file
4 is a zlib file
5 is a bzip file
6 is a gzip file
7 is a gzip file
8 is a gzip file
9 is a hex ASCII file
...
152 is a hex ASCII file
```

```
153 is a zlib file
154 is a base 64 ASCII file
155 is a gzip file
156 is a zlib file
Could not decode: JSON
JSON data


kali@kali:~/Downloads/tisc1new$ ls 15*
150  152  154  155  157
kali@kali:~/Downloads/tisc1new$ cat 157
{"anoroc": "v1.320", "secret": "TISC20{q1_9ae08ad36fa3b76e9716fa22616ef610}",
"desc": "Submit this.secret to the TISC grader to complete challenge",
"constants": [1116352408, 1899447441, 3049323471, 3921009573, 961987163,
1508970993, 2453635748, 2870763221], "sign":
"j8QhSantw08"}kali@kali:~/Downloads/tisc1new$
```

Then finally I just submit the secret to the connection and volia! The flag is there:

```
kali@kali:~/Downloads/tisc1new$ nc fqybysahpvift1nqtwywevlr7n50zdzp.ctf.sg 31081


$$$$$$$$\ $$$$$$\  $$$$$$\   $$$$$$\
\__$$  __|\_$$  _|$$  __$$\ $$  __$$\
   $$ |     $$ |  $$ /  \__|$$ /  \__|
   $$ |     $$ |  \$$$$$$\  $$ |
   $$ |     $$ |   \____$$\ $$ |
   $$ |     $$ |  $$\   $$ |$$ |  $$\
   $$ |   $$$$$$\ \$$$$$$  |\$$$$$$  |
   \__|   \______| \______/  \______/

CSIT's The Infosecurity Challenge 2020
https://play.tisc.csit-events.sg/

CHALLENGE 1: What is this thing?
=======================================

SUBMISSION_TOKEN? SPBcjgOrbENajUzGKexGlcNTDYbUHwbDjMDVyTZBsTGDnPrOJgUIIVZpktlbeJjE

We noticed unusually network activity around the time that the user reported being
ransomware-d.
There were files being sent and recieved, some of which we were unable to inspect.
Could you try to decode this?

Reminder! SAVE ANY CODE YOU WROTE / TAKE SCREENSHOTS OF YOUR WORK, THIS WILL NEED
TO BE SUBMITTED IN YOUR WRITEUP!
CLARITY OF DOCUMENTATION WILL CONTRIBUTE TO A BETTER EVALUATION OF YOUR WRITEUP.

The file is hosted at
http://fqybysahpvift1nqtwywevlr7n50zdzp.ctf.sg:31080/b1ed57b7cf34d91e7dd1301597ff9
101.zip .
```

```
Flag? TISC20{q1_9ae08ad36fa3b76e9716fa22616ef610}

Reminder! SAVE ANY CODE YOU WROTE / TAKE SCREENSHOTS OF YOUR WORK, THIS WILL NEED
TO BE SUBMITTED IN YOUR WRITEUP!
Winner Winner Vegan Dinner 🎉🎊🎁🥳
{"submission":"failed","error":"Already solved!"}kali@kali:~/Downloads/tisc1new$
```