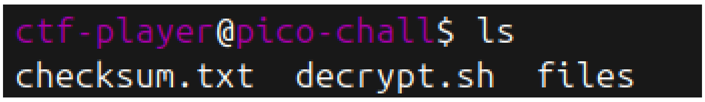
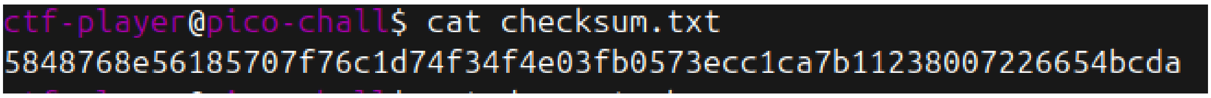
Verify

kami mengaksess sebuah server yang di dalamnya terdapat 2 file satu directory, dan kami menemukan sebuah check sum yang dimana terdapat string base64 di dalamnya

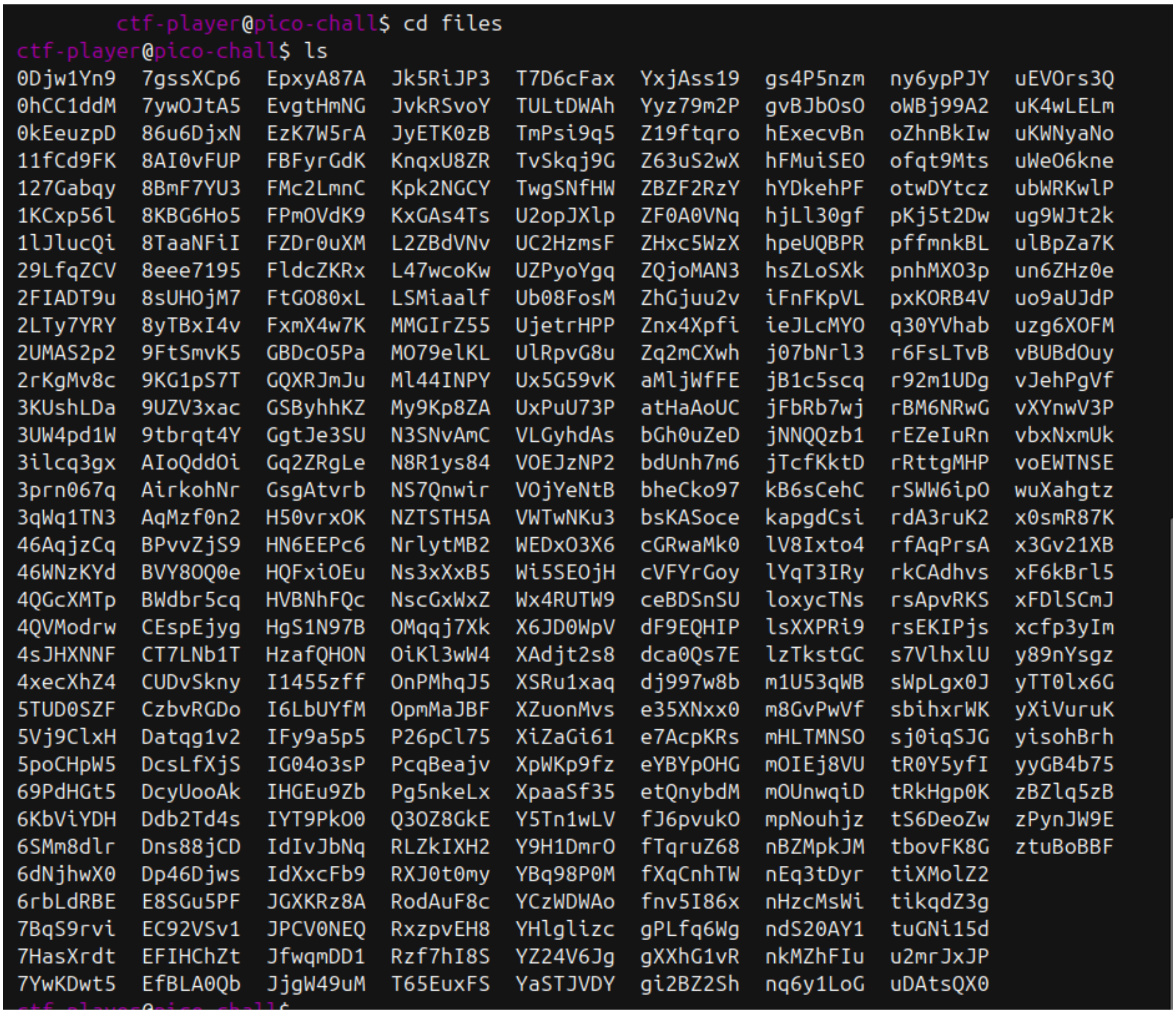


```
ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
```



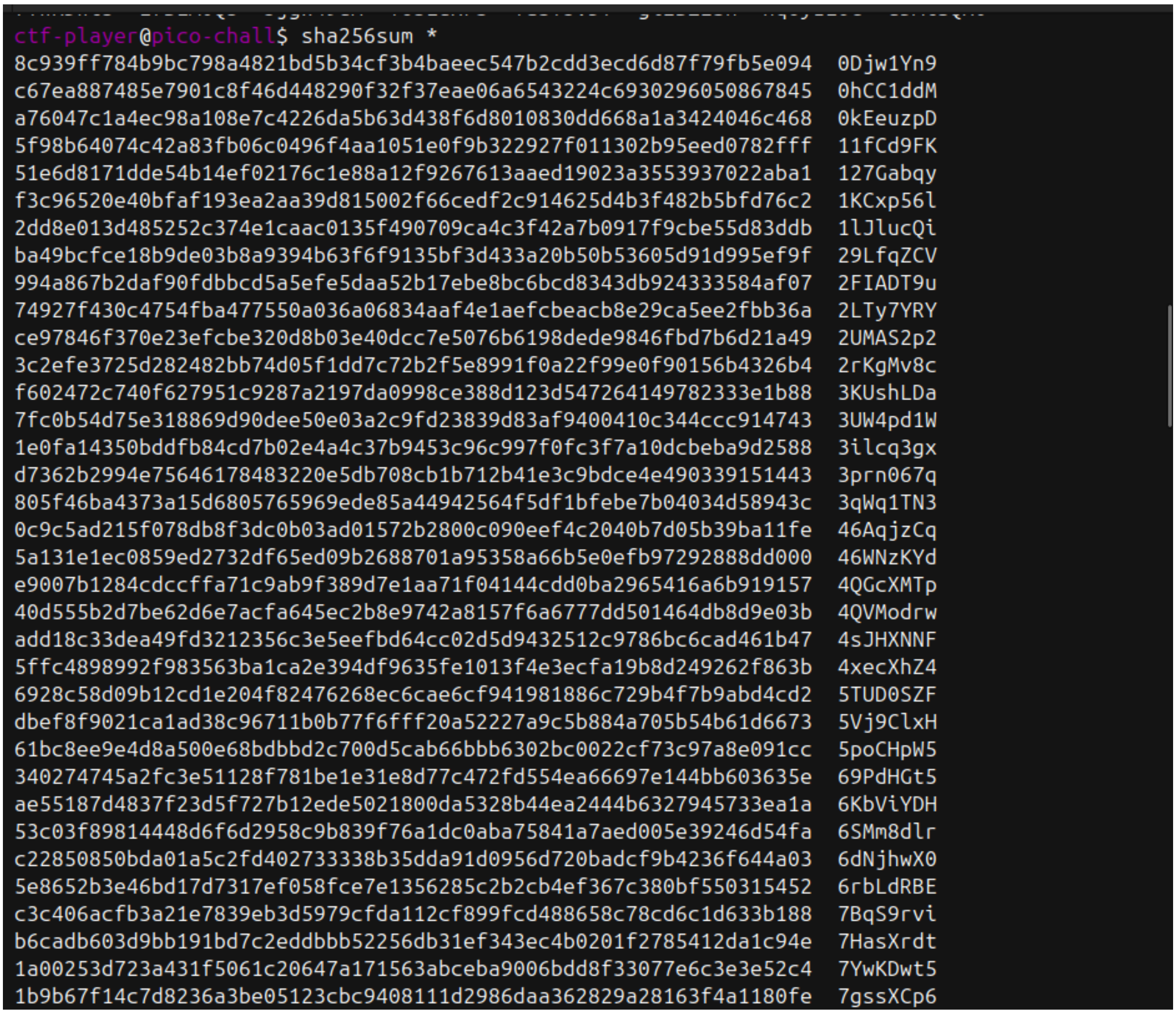
```
ctf-player@pico-chall$ cat checksum.txt
5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda
```

terdapat satu folder dengan nama files, yang kami temukan memiliki file dengan nama yang unik



```
        ctf-player@pico-chall$ cd files
ctf-player@pico-chall$ ls
0Djw1Yn9  7gssXCp6  EpxyA87A  Jk5RiJP3  T7D6cFax  YxjAss19  gs4P5nzm  ny6ypPJY  uEVOrs3Q
0hCC1ddM  7ywOJtA5  EvgtHmNG  JvkRSvoY  TULtDWAh  Yyz79m2P  gvBJbOsO  oWBj99A2  uK4wLELm
0kEeuzpD  86u6DjxN  EzK7W5rA  JyETK0zB  TmPsi9q5  Z19ftqro  hExecvBn  oZhnBkIw  uKWNyaNo
11fCd9FK  8AI0vFUP  FBFyrGdK  KnqxU8ZR  TvSkqj9G  Z63uS2wX  hFMuiSEO  ofqt9Mts  uWeO6kne
127Gabqy  8BmF7YU3  FMc2LmnC  Kpk2NGCY  TwgSNfHW  ZBZF2RzY  hYDkehPF  otwDYtcz  ubWRKwlP
1KCxp56l  8KBG6Ho5  FPmOVdK9  KxGAs4Ts  U2opJXlp  ZF0A0VNq  hjLl30gf  pKj5t2Dw  ug9WJt2k
1lJlucQi  8TaaNFiI  FZDr0uXM  L2ZBdVNv  UC2HzmsF  ZHxc5WzX  hpeUQBPR  pffmnkBL  ulBpZa7K
29LfqZCV  8eee7195  FldcZKRx  L47wcoKw  UZPyoYgq  ZQjoMAN3  hsZLoSXk  pnhMXO3p  un6ZHz0e
2FIADT9u  8sUHOjM7  FtGO80xL  LSMiaalf  Ub08FosM  ZhGjuu2v  iFnFKpVL  pxKORB4V  uo9aUJdP
2LTy7YRY  8yTBxI4v  FxmX4w7K  MMGIrZ55  UjetrHPP  Znx4Xpfi  ieJLcMYO  q30YVhab  uzg6XOFM
2UMAS2p2  9FtSmvK5  GBDcO5Pa  MO79elKL  UlRpvG8u  Zq2mCXwh  j07bNrl3  r6FsLTvB  vBUBdOuy
2rKgMv8c  9KG1pS7T  GQXRJmJu  Ml44INPY  Ux5G59vK  aMljWfFE  jB1c5scq  r92m1UDg  vJehPgVf
3KUshLDa  9UZV3xac  GSByhhKZ  My9Kp8ZA  UxPuU73P  atHaAoUC  jFbRb7wj  rBM6NRwG  vXYnwV3P
3UW4pd1W  9tbrqt4Y  GgtJe3SU  N3SNvAmC  VLGyhdAs  bGh0uZeD  jNNQQzb1  rEZeIuRn  vbxNxmUk
3ilcq3gx  AIoQddOi  Gq2ZRgLe  N8R1ys84  VOEJzNP2  bdUnh7m6  jTcfKktD  rRttgMHP  voEWTNSE
3prn067q  AirkohNr  GsgAtvrb  NS7Qnwir  VOjYeNtB  bheCko97  kB6sCehC  rSWW6ipO  wuXahgtz
3qWq1TN3  AqMzf0n2  H50vrxOK  NZTSTH5A  VWTwNKu3  bsKASoce  kapgdCsi  rdA3ruK2  x0smR87K
46AqjzCq  BPvvZjS9  HN6EEPc6  NrlytMB2  WEDxO3X6  cGRwaMk0  lV8Ixto4  rfAqPrsA  x3Gv21XB
46WNzKYd  BVY8OQ0e  HQFxiOEu  Ns3xXxB5  Wi5SEOjH  cVFYrGoy  lYqT3IRy  rkCAdhvs  xF6kBrl5
4QGcXMTp  BWdbr5cq  HVBNhFQc  NscGxWxZ  Wx4RUTW9  ceBDSnSU  loxycTNs  rsApvRKS  xFDlSCmJ
4QVModrw  CEspEjyg  HgS1N97B  OMqqj7Xk  X6JD0WpV  dF9EQHIP  lsXXPRi9  rsEKIPjs  xcfp3yIm
4sJHXNNF  CT7LNb1T  HzafQHON  OiKl3wW4  XAdjt2s8  dca0Qs7E  lzTkstGC  s7VlhxlU  y89nYsgz
4xecXhZ4  CUDvSkny  I1455zff  OnPMhqJ5  XSRu1xaq  dj997w8b  m1U53qWB  sWpLgx0J  yTT0lx6G
5TUD0SZF  CzbvRGDo  I6LbUYfM  OpmMaJBF  XZuonMvs  e35XNxx0  m8GvPwVf  sbihxrWK  yXiVuruK
5Vj9ClxH  Datqg1v2  IFy9a5p5  P26pCl75  XiZaGi61  e7AcpKRs  mHLTMNSO  sj0iqSJG  yisohBrh
5poCHpW5  DcsLfXjS  IG04o3sP  PcqBeajv  XpWKp9fz  eYBYpOHG  mOIEj8VU  tR0Y5yfI  yyGB4b75
69PdHGt5  DcyUooAk  IHGEu9Zb  Pg5nkeLx  XpaaSf35  etQnybdM  mOUnwqiD  tRkHgp0K  zBZlq5zB
6KbViYDH  Ddb2Td4s  IYT9PkO0  Q3OZ8GkE  Y5Tn1wLV  fJ6pvukO  mpNouhjz  tS6DeoZw  zPynJW9E
6SMm8dlr  Dns88jCD  IdIvJbNq  RLZkIXH2  Y9H1DmrO  fTqruZ68  nBZMpkJM  tbovFK8G  ztuBoBBF
6dNjhwX0  Dp46Djws  IdXxcFb9  RXJ0t0my  YBq98P0M  fXqCnhTW  nEq3tDyr  tiXMolZ2
6rbLdRBE  E8SGu5PF  JGXKRz8A  RodAuF8c  YCzWDWAo  fnv5I86x  nHzcMsWi  tikqdZ3g
7BqS9rvi  EC92VSv1  JPCV0NEQ  RxzpvEH8  YHlglizc  gPLfq6Wg  ndS20AY1  tuGNi15d
7HasXrdt  EFIHChZt  JfwqmDD1  Rzf7hI8S  YZ24V6Jg  gXXhG1vR  nkMZhFIu  u2mrJxJP
7YwKDwt5  EfBLA0Qb  JjgW49uM  T65EuxFS  YaSTJVDY  gi2BZ2Sh  nq6y1LoG  uDAtsQX0
```

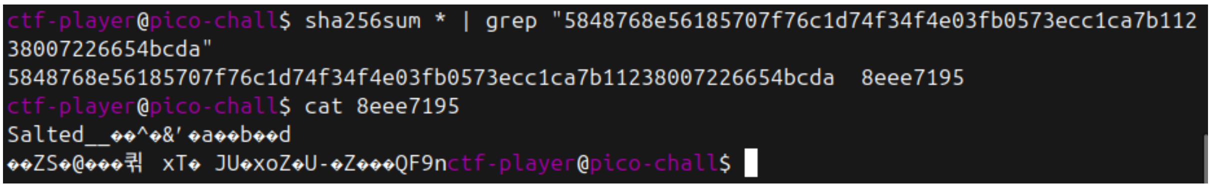
setelah melakukan identifikasi, saya kira semua file isinya akan digabung ternyata tidak, saya mencoba untuk melakukan verifikasi terhadap semua file yang ada di folder files, dengan menggunakan sha256sum, untuk melihat file mana yang otentik dengan checksum.txt



```
ctf-player@pico-chall$ sha256sum *
8c939ff784b9bc798a4821bd5b34cf3b4baeec547b2cdd3ecd6d87f79fb5e094  0Djw1Yn9
c67ea887485e7901c8f46d448290f32f37eae06a6543224c6930296050867845  0hCC1ddM
a76047c1a4ec98a108e7c4226da5b63d438f6d8010830dd668a1a3424046c468  0kEeuzpD
5f98b64074c42a83fb06c0496f4aa1051e0f9b322927f011302b95eed0782fff  11fCd9FK
51e6d8171dde54b14ef02176c1e88a12f9267613aaed19023a3553937022aba1  127Gabqy
f3c96520e40bfaf193ea2aa39d815002f66cedf2c914625d4b3f482b5bfd76c2  1KCxp56l
2dd8e013d485252c374e1caac0135f490709ca4c3f42a7b0917f9cbe55d83ddb  1lJlucQi
ba49bcfce18b9de03b8a9394b63f6f9135bf3d433a20b50b53605d91d995ef9f  29LfqZCV
994a867b2daf90fdbbcd5a5efe5daa52b17ebe8bc6bcd8343db924333584af07  2FIADT9u
74927f430c4754fba477550a036a06834aaf4e1aefcbeacb8e29ca5ee2fbb36a  2LTy7YRY
ce97846f370e23efcbe320d8b03e40dcc7e5076b6198dede9846fbd7b6d21a49  2UMAS2p2
3c2efe3725d282482bb74d05f1dd7c72b2f5e8991f0a22f99e0f90156b4326b4  2rKgMv8c
f602472c740f627951c9287a2197da0998ce388d123d547264149782333e1b88  3KUshLDa
7fc0b54d75e318869d90dee50e03a2c9fd23839d83af9400410c344ccc914743  3UW4pd1W
1e0fa14350bddfb84cd7b02e4a4c37b9453c96c997f0fc3f7a10dcbeba9d2588  3ilcq3gx
d7362b2994e75646178483220e5db708cb1b712b41e3c9bdce4e490339151443  3prn067q
805f46ba4373a15d6805765969ede85a44942564f5df1bfebe7b04034d58943c  3qWq1TN3
0c9c5ad215f078db8f3dc0b03ad01572b2800c090eef4c2040b7d05b39ba11fe  46AqjzCq
5a131e1ec0859ed2732df65ed09b2688701a95358a66b5e0efb97292888dd000  46WNzKYd
e9007b1284cdccffa71c9ab9f389d7e1aa71f04144cdd0ba2965416a6b919157  4QGcXMTp
40d555b2d7be62d6e7acfa645ec2b8e9742a8157f6a6777dd501464db8d9e03b  4QVModrw
add18c33dea49fd3212356c3e5eefbd64cc02d5d9432512c9786bc6cad461b47  4sJHXNNF
5ffc4898992f983563ba1ca2e394df9635fe1013f4e3ecfa19b8d249262f863b  4xecXhZ4
6928c58d09b12cd1e204f82476268ec6cae6cf941981886c729b4f7b9abd4cd2  5TUD0SZF
dbef8f9021ca1ad38c96711b0b77f6fff20a52227a9c5b884a705b54b61d6673  5Vj9ClxH
61bc8ee9e4d8a500e68bdbbd2c700d5cab66bbb6302bc0022cf73c97a8e091cc  5poCHpW5
340274745a2fc3e51128f781be1e31e8d77c472fd554ea66697e144bb603635e  69PdHGt5
ae55187d4837f23d5f727b12ede5021800da5328b44ea2444b6327945733ea1a  6KbViYDH
53c03f89814448d6f6d2958c9b839f76a1dc0aba75841a7aed005e39246d54fa  6SMm8dlr
c22850850bda01a5c2fd402733338b35dda91d0956d720badcf9b4236f644a03  6dNjhwX0
5e8652b3e46bd17d7317ef058fce7e1356285c2b2cb4ef367c380bf550315452  6rbLdRBE
c3c406acfb3a21e7839eb3d5979cfda112cf899fcd488658c78cd6c1d633b188  7BqS9rvi
b6cadb603d9bb191bd7c2eddbbb52256db31ef343ec4b0201f2785412da1c94e  7HasXrdt
1a00253d723a431f5061c20647a171563abceba9006bdd8f33077e6c3e3e52c4  7YwKDwt5
1b9b67f14c7d8236a3be05123cbc9408111d2986daa362829a28163f4a1180fe  7gssXCp6
```

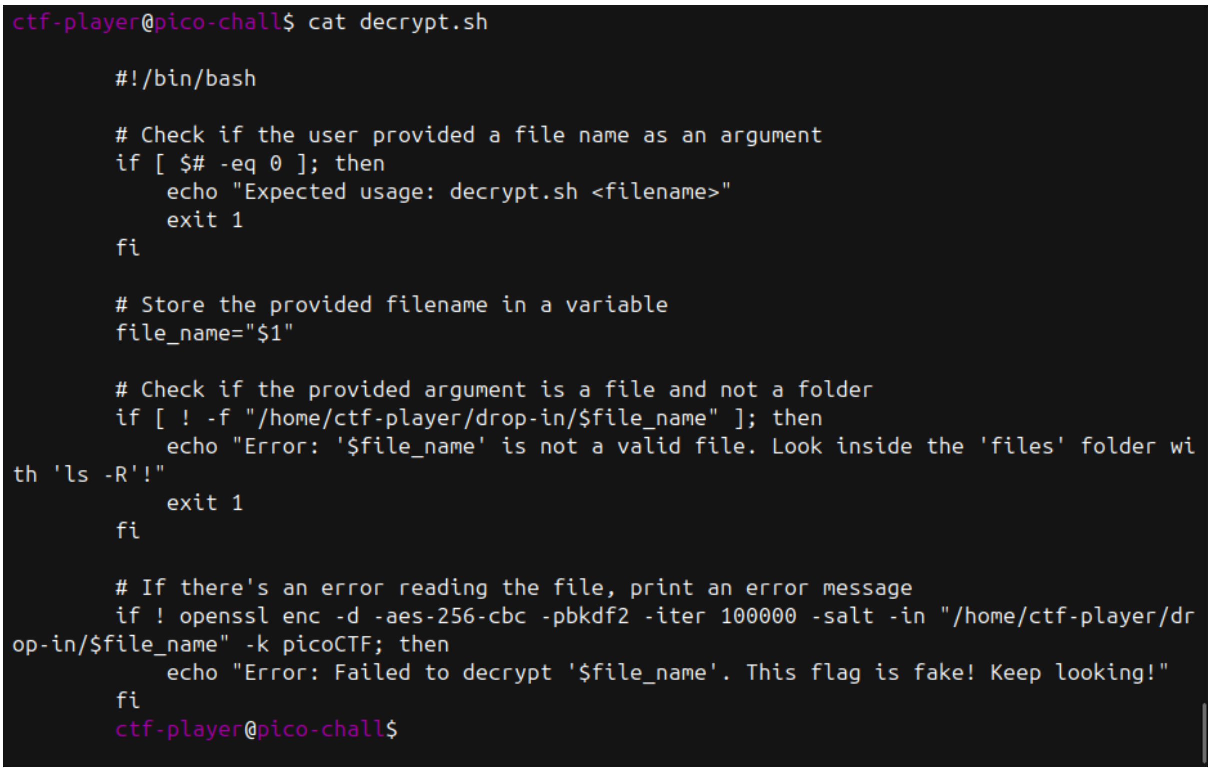
terlalu banyak jika kita mencari dengan mata telanjang oleh sebab itu kita akan melakukan nya menggunakan grep agar lebih mudah dan efisien,dengan command

sha256sum * | grep “(sum yang tadi ada pada checksum.txt) 5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda”



```
ctf-player@pico-chall$ sha256sum * | grep "5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b112
38007226654bcda"
5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda  8eee7195
ctf-player@pico-chall$ cat 8eee7195
Salted__��^�&'�a��b��d
��ZS�@���퀵 xT� JU�xoZ�U-�Z���QF9nctf-player@pico-chall$ █
```

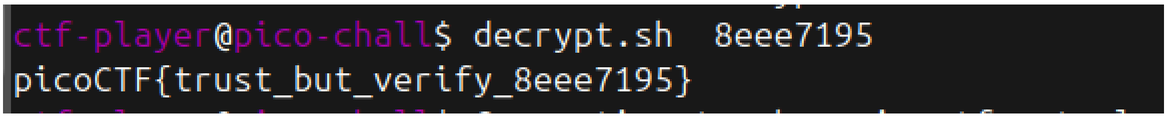
berdasarkan program decrypt.sh



```
ctf-player@pico-chall$ cat decrypt.sh

        #!/bin/bash

        # Check if the user provided a file name as an argument
        if [ $# -eq 0 ]; then
            echo "Expected usage: decrypt.sh <filename>"
            exit 1
        fi

        # Store the provided filename in a variable
        file_name="$1"

        # Check if the provided argument is a file and not a folder
        if [ ! -f "/home/ctf-player/drop-in/$file_name" ]; then
            echo "Error: '$file_name' is not a valid file. Look inside the 'files' folder wi
th 'ls -R'!"
            exit 1
        fi

        # If there's an error reading the file, print an error message
        if ! openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt -in "/home/ctf-player/dr
op-in/$file_name" -k picoCTF; then
            echo "Error: Failed to decrypt '$file_name'. This flag is fake! Keep looking!"
        fi
        ctf-player@pico-chall$
```

dia akan melakukan cek dengan nama file yang dimasukan, lalu setlah itu akan menyimpan nama file kedalam file_name, dan melakukan verifikasi bahwa file adalah file yang tepat dan program akan membacanya dan melakukan proses decrypting dengan biner yang ada di dalam file yang tepat

dengan merunning decrypt.sh <8eee7195> adalah file yang tepat dengan checksum maka kita akan menghasilkan sebuah flag



```
ctf-player@pico-chall$ decrypt.sh  8eee7195
picoCTF{trust_but_verify_8eee7195}
```

picoCTF{trust_but_verify_8eee7195}