Forensics CTF 4

Platform: picoCTF 2024

Challenge Name: Verify

Category: Forensics

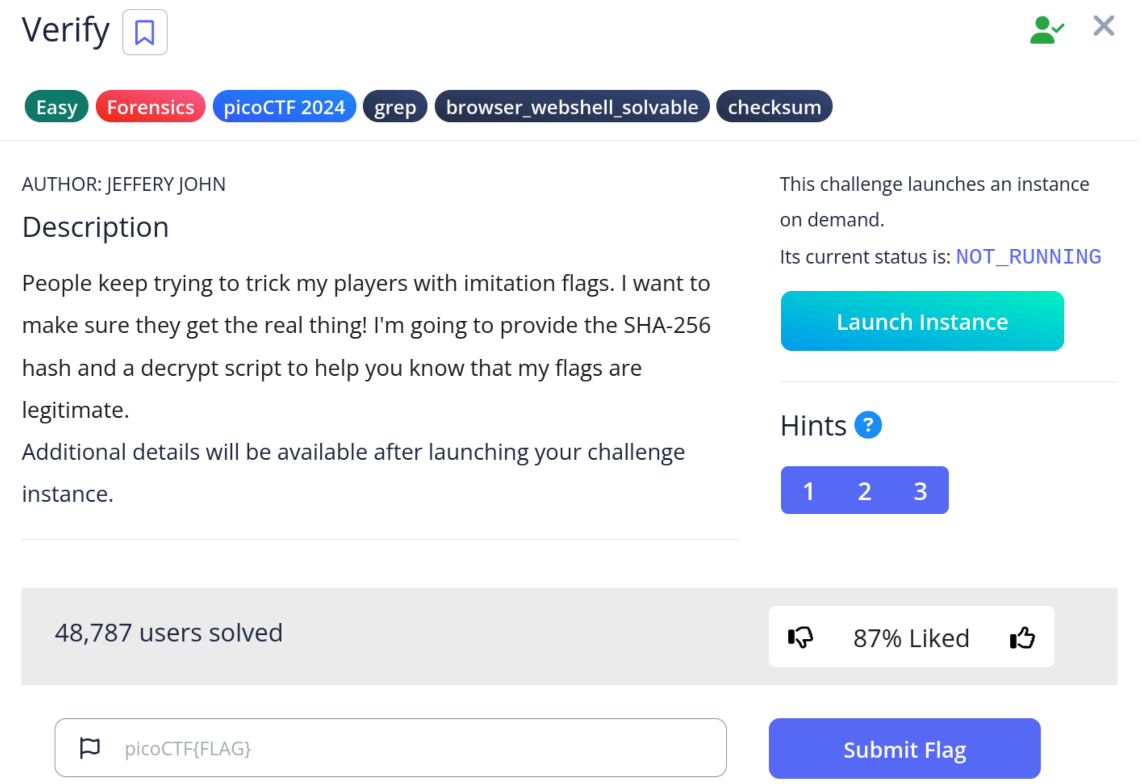
Difficulty: Easy

Submitted By: Gurleen Kaur Brar

Objective

The goal of this challenge was to validate the authenticity of a flag using a SHA-256 checksum and a provided decryption script.

Challenge Description



Verify

AUTHOR: JEFFERY JOHN

Description

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate.

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

48,787 users solved

87% Liked

Files and Tools Used

- **Files Provided via Instance:**
  - `checksum.txt` – contains the correct SHA-256 hash
  - `decrypt.sh` – decryption script
  - `files/` – directory of potential flag files
- **Tools Used:**
  - SSH (to connect to the provided server)
  - `sha256sum` (to hash local files)

Step-by-Step Process

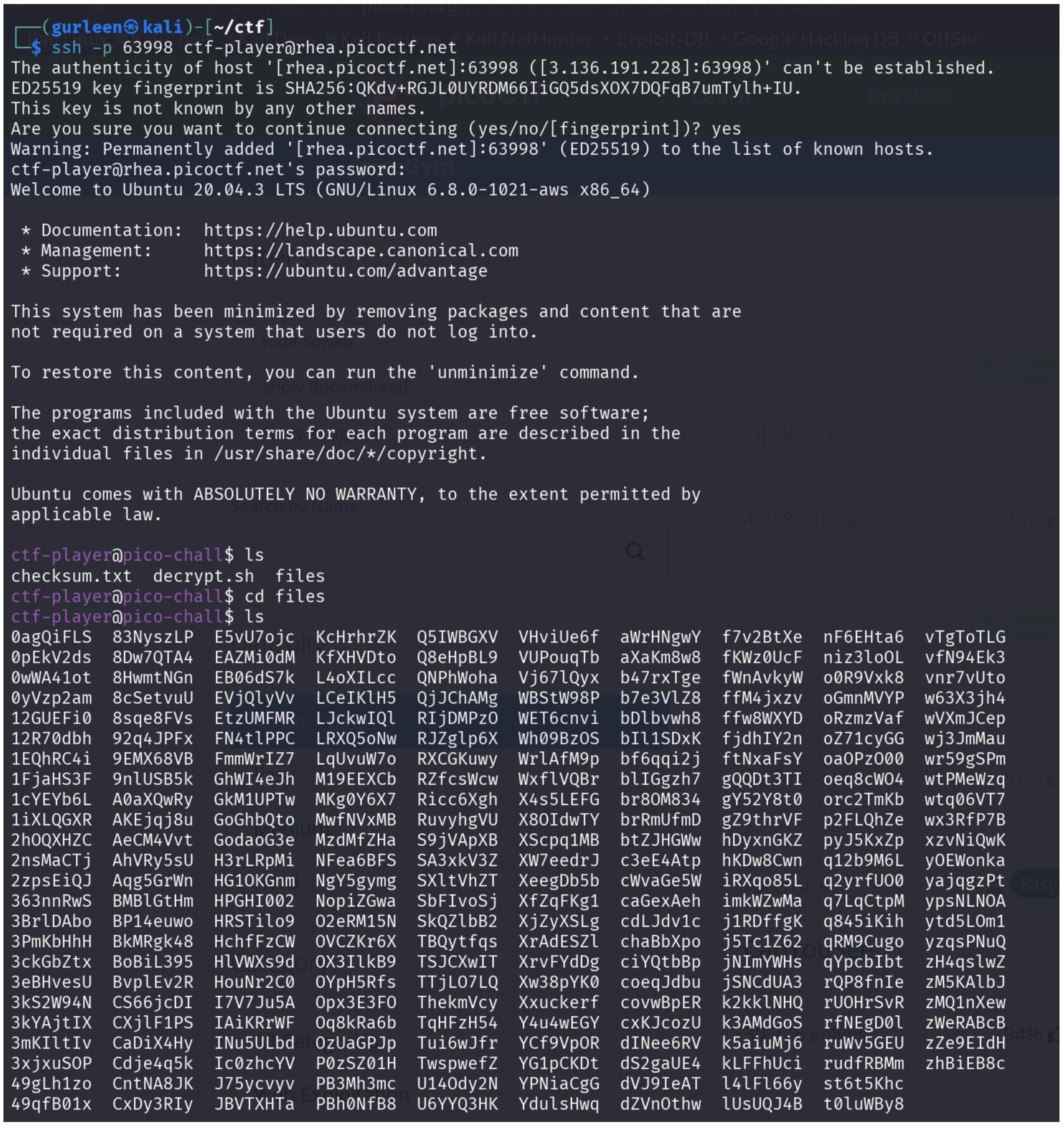
Step 1: Launch the Challenge Instance

Used SSH to connect to the provided server:

```
ssh -p 63998 ctf-player@rhea.picoctf.net
```

Once logged in, verified available files:

```
ls
cd files
```



```
┌──(gurleen㉿kali)-[~/ctf]
└─$ ssh -p 63998 ctf-player@rhea.picoctf.net
The authenticity of host '[rhea.picoctf.net]:63998 ([3.136.191.228]:63998)' can't be established.
ED25519 key fingerprint is SHA256:QKdv+RGJL0UYRDM66IiGQ5dsXOX7DQFqB7umTylh+IU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[rhea.picoctf.net]:63998' (ED25519) to the list of known hosts.
ctf-player@rhea.picoctf.net's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 6.8.0-1021-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
ctf-player@pico-chall$ cd files
ctf-player@pico-chall$ ls
0agQiFLS  83NyszLP  E5vU7ojc  KcHrhrZK  Q5IWBGXV  VHviUe6f  aWrHNgwY  f7v2BtXe  nF6EHta6  vTgToTLG
0pEkV2ds  8Dw7QTA4  EAZMi0dM  KfXHVDto  Q8eHpBL9  VUPouqTb  aXaKm8w8  fKWz0UcF  niz3loOL  vfN94Ek3
0wWA41ot  8HwmtNGn  EB06dS7k  L4oXILcc  QNPhWoha  Vj67lQyx  b47rxTge  fWnAvkyW  o0R9Vxk8  vnr7vUto
0yVzp2am  8cSetvuU  EVjQlyVv  LCeIKlH5  QjJChAMg  WBStW98P  b7e3VlZ8  ffM4jxzv  oGmnMVYP  w63X3jh4
12GUEFi0  8sqe8FVs  EtzUMFMR  LJckwIQl  RIjDMPzO  WET6cnvi  bDlbvwh8  ffw8WXYD  oRzmzVaf  wVXmJCep
12R70dbh  92q4JPFx  FN4tlPPC  LRXQ5oNw  RJZglp6X  Wh09BzOS  bIl1SDxK  fjdhIY2n  oZ71cyGG  wj3JmMau
1EQhRC4i  9EMX68VB  FmmWrIZ7  LqUvuW7o  RXCGKuwy  WrlAfM9p  bf6qqi2j  ftNxaFsY  oaOPzO00  wr59gSPm
1FjaHS3F  9nlUSB5k  GhWI4eJh  M19EEXCb  RZfcsWcw  WxflVQBr  blIGgzh7  gQQDt3TI  oeq8cWO4  wtPMeWzq
1cYEYb6L  A0aXQwRy  GkM1UPTw  MKg0Y6X7  Ricc6Xgh  X4s5LEFG  br8OM834  gY52Y8t0  orc2TmKb  wtq06VT7
1iXLQGXR  AKEjqj8u  GoGhbQto  MwfNVxMB  RuvyhgVU  X8OIdwTY  brRmUfmD  gZ9thrVF  p2FLQhZe  wx3RfP7B
2hOQXHZC  AeCM4Vvt  GodaoG3e  MzdMfZHa  S9jVApXB  XScpq1MB  btZJHGWw  hDyxnGKZ  pyJ5KxZp  xzvNiQwK
2nsMaCTj  AhVRy5sU  H3rLRpMi  NFea6BFS  SA3xkV3Z  XW7eedrJ  c3eE4Atp  hKDw8Cwn  q12b9M6L  yOEWonka
2zpsEiQJ  Aqg5GrWn  HG1OKGnm  NgY5gymg  SXltVhZT  XeegDb5b  cWvaGe5W  iRXqo85L  q2yrfUO0  yajqgzPt
363nnRwS  BMBlGtHm  HPGHI002  NopiZGwa  SbFIvoSj  XfZqFKg1  caGexAeh  imkWZwMa  q7LqCtpM  ypsNLNOA
3BrlDAbo  BP14euwo  HRSTilo9  O2eRM15N  SkQZlbB2  XjZyXSLg  cdLJdv1c  j1RDffgK  q845iKih  ytd5LOm1
3PmKbHhH  BkMRgk48  HchfFzCW  OVCZKr6X  TBQytfqs  XrAdESZl  chaBbXpo  j5Tc1Z62  qRM9Cugo  yzqsPNuQ
3ckGbZtx  BoBiL395  HlVWXs9d  OX3IlkB9  TSJCXwIT  XrvFYdDg  ciYQtbBp  jNImYWHs  qYpcbIbt  zH4qslwZ
3eBHvesU  BvplEv2R  HouNr2C0  OYpH5Rfs  TTjLO7LQ  Xw38pYK0  coeqJdbu  jSNCdUA3  rQP8fnIe  zM5KAlbJ
3kS2W94N  CS66jcDI  I7V7Ju5A  Opx3E3FO  ThekmVcy  Xxuckerf  covwBpER  k2kklNHQ  rUOHrSvR  zMQ1nXew
3kYAjtIX  CXjlF1PS  IAiKRrWF  Oq8kRa6b  TqHFzH54  Y4u4wEGY  cxKJcozU  k3AMdGoS  rfNEgD0l  zWeRABcB
3mKIltIv  CaDiX4Hy  INu5ULbd  OzUaGPJp  Tui6wJfr  YCf9VpOR  dINee6RV  k5aiuMj6  ruWv5GEU  zZe9EIdH
3xjxuSOP  Cdje4q5k  Ic0zhcYV  P0zSZ01H  TwspwefZ  YG1pCKDt  dS2gaUE4  kLFFhUci  rudfRBMm  zhBiEB8c
49gLh1zo  CntNA8JK  J75ycvyv  PB3Mh3mc  U14Ody2N  YPNiaCgG  dVJ9IeAT  l4lFl66y  st6t5Khc
49qfB01x  CxDy3RIy  JBVTXHTa  PBh0NfB8  U6YYQ3HK  YdulsHwq  dZVnOthw  lUsUQJ4B  t0luWBy8
```

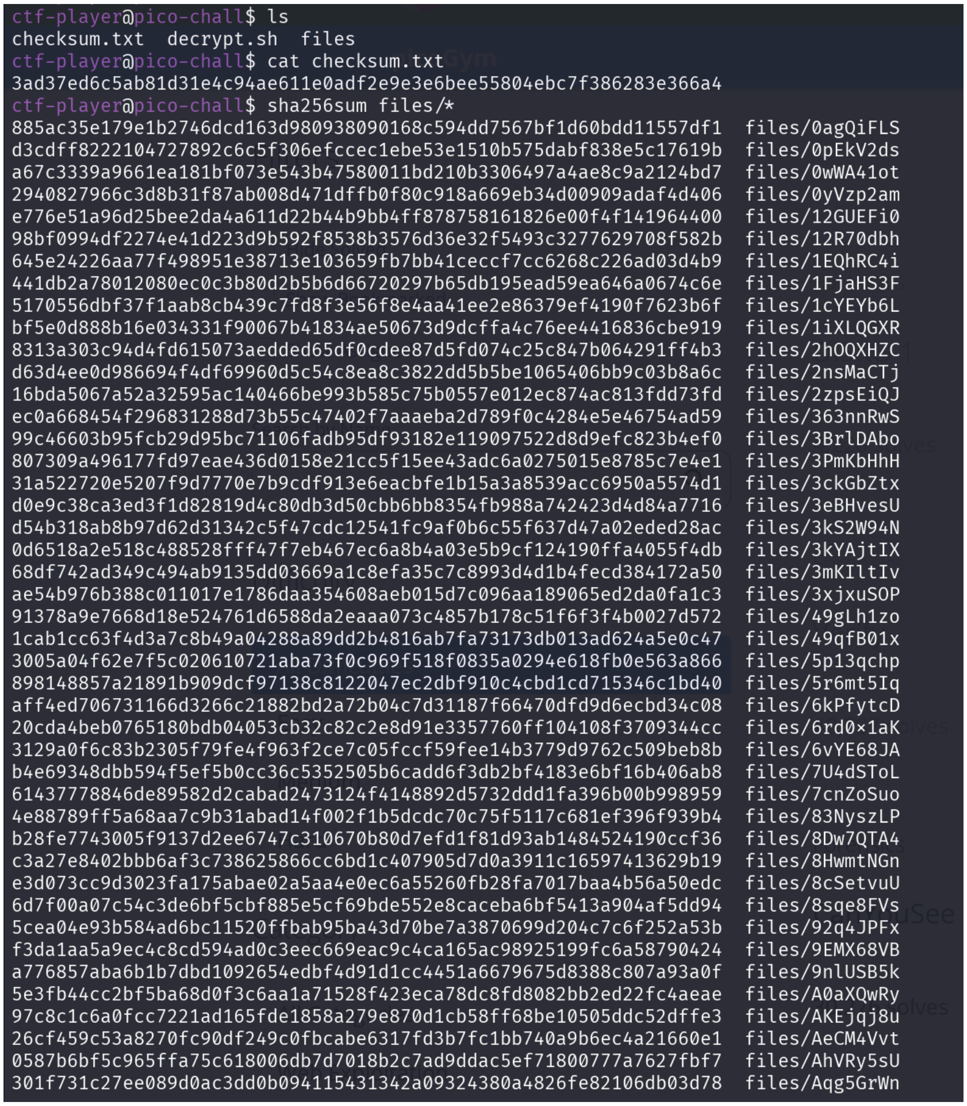
Step 2: Read the Provided Checksum

Returned to the root directory and opened `checksum.txt` to get the SHA-256 hash:

```
cat checksum.txt
```

Hash:

```
3ad37ed6c5ab81d31e4c94ae611e04df2e9e3e6bee55804ebcf7386283e366a4
```

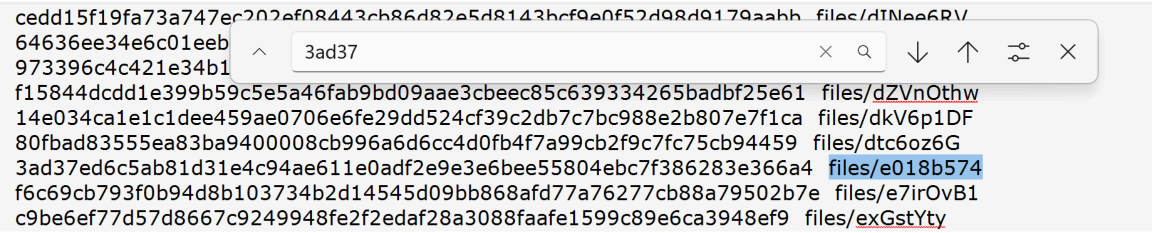


```
ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
ctf-player@pico-chall$ cat checksum.txt
3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4
ctf-player@pico-chall$ sha256sum files/*
885ac35e179e1b2746dcd163d980938090168c594dd7567bf1d60bdd11557df1  files/0agQiFLS
d3cdff8222104727892c6c5f306efccec1ebe53e1510b575dabf838e5c17619b  files/0pEkV2ds
a67c3339a9661ea181bf073e543b47580011bd210b3306497a4ae8c9a2124bd7  files/0wWA41ot
2940827966c3d8b31f87ab008d471dffb0f80c918a669eb34d00909adaf4d406  files/0yVzp2am
e776e51a96d25bee2da4a611d22b44b9bb4ff878758161826e00f4f141964400  files/12GUEFi0
98bf0994df2274e41d223d9b592f8538b3576d36e32f5493c3277629708f582b  files/12R70dbh
645e24226aa77f498951e38713e103659fb7bb41ceccf7cc6268c226ad03d4b9  files/1EQhRC4i
441db2a78012080ec0c3b80d2b5b6d66720297b65db195ead59ea646a0674c6e  files/1FjaHS3F
5170556dbf37f1aab8cb439c7fd8f3e56f8e4aa41ee2e86379ef4190f7623b6f  files/1cYEYb6L
bf5e0d888b16e034331f90067b41834ae50673d9dcffa4c76ee4416836cbe919  files/1iXLQGXR
8313a303c94d4fd615073aedded65df0cdee87d5fd074c25c847b064291ff4b3  files/2hOQXHZC
d63d4ee0d986694f4df69960d5c54c8ea8c3822dd5b5be1065406bb9c03b8a6c  files/2nsMaCTj
16bda5067a52a32595ac140466be993b585c75b0557e012ec874ac813fdd73fd  files/2zpsEiQJ
ec0a668454f296831288d73b55c47402f7aaaeba2d789f0c4284e5e46754ad59  files/363nnRwS
99c46603b95fcb29d95bc71106fadb95df93182e119097522d8d9efc823b4ef0  files/3BrlDAbo
807309a496177fd97eae436d0158e21cc5f15ee43adc6a0275015e8785c7e4e1  files/3PmKbHhH
31a522720e5207f9d7770e7b9cdf913e6eacbfe1b15a3a8539acc6950a5574d1  files/3ckGbZtx
d0e9c38ca3ed3f1d82819d4c80db3d50cbb6bb8354fb988a742423d4d84a7716  files/3eBHvesU
d54b318ab8b97d62d31342c5f47cdc12541fc9af0b6c55f637d47a02eded28ac  files/3kS2W94N
0d6518a2e518c488528fff47f7eb467ec6a8b4a03e5b9cf124190ffa4055f4db  files/3kYAjtIX
68df742ad349c494ab9135dd03669a1c8efa35c7c8993d4d1b4fecd384172a50  files/3mKIltIv
ae54b976b388c011017e1786daa354608aeb015d7c096aa189065ed2da0fa1c3  files/3xjxuSOP
91378a9e7668d18e524761d6588da2eaaa073c4857b178c51f6f3f4b0027d572  files/49gLh1zo
1cab1cc63f4d3a7c8b49a04288a89dd2b4816ab7fa73173db013ad624a5e0c47  files/49qfB01x
3005a04f62e7f5c020610721aba73f0c969f518f0835a0294e618fb0e563a866  files/5p13qchp
898148857a21891b909dcf97138c8122047ec2dbf910c4cbd1cd715346c1bd40  files/5r6mt5Iq
aff4ed706731166d3266c21882bd2a72b04c7d31187f66470dfd9d6ecbd34c08  files/6kPfytcD
20cda4beb0765180bdb04053cb32c82c2e8d91e3357760ff104108f3709344cc  files/6rd0×1aK
3129a0f6c83b2305f79fe4f963f2ce7c05fccf59fee14b3779d9762c509beb8b  files/6vYE68JA
b4e69348dbb594f5ef5b0cc36c5352505b6cadd6f3db2bf4183e6bf16b406ab8  files/7U4dSToL
61437778846de89582d2cabad2473124f4148892d5732ddd1fa396b00b998959  files/7cnZoSuo
4e88789ff5a68aa7c9b31abad14f002f1b5dcdc70c75f5117c681ef396f939b4  files/83NyszLP
b28fe7743005f9137d2ee6747c310670b80d7efd1f81d93ab1484524190ccf36  files/8Dw7QTA4
c3a27e8402bbb6af3c738625866cc6bd1c407905d7d0a3911c16597413629b19  files/8HwmtNGn
e3d073cc9d3023fa175abae02a5aa4e0ec6a55260fb28fa7017baa4b56a50edc  files/8cSetvuU
6d7f00a07c54c3de6bf5cbf885e5cf69bde552e8caceba6bf5413a904af5dd94  files/8sqe8FVs
5cea04e93b584ad6bc11520ffbab95ba43d70be7a3870699d204c7c6f252a53b  files/92q4JPFx
f3da1aa5a9ec4c8cd594ad0c3eec669eac9c4ca165ac98925199fc6a58790424  files/9EMX68VB
a776857aba6b1b7dbd1092654edbf4d91d1cc4451a6679675d8388c807a93a0f  files/9nlUSB5k
5e3fb44cc2bf5ba68d0f3c6aa1a71528f423eca78dc8fd8082bb2ed22fc4aeae  files/A0aXQwRy
97c8c1c6a0fcc7221ad165fde1858a279e870d1cb58ff68be10505ddc52dffe3  files/AKEjqj8u
26cf459c53a8270fc90df249c0fbcabe6317fd3b7fc1bb740a9b6ec4a21660e1  files/AeCM4Vvt
0587b6bf5c965ffa75c618006db7d7018b2c7ad9ddac5ef71800777a7627fbf7  files/AhVRy5sU
301f731c27ee089d0ac3dd0b094115431342a09324380a4826fe82106db03d78  files/Aqg5GrWn
```

Step 3: Find the Matching File

Used `sha256sum *` to compute hashes of all files inside the `files/` directory and matched it against the provided hash. The matching file was:

```
files/e018b574
```

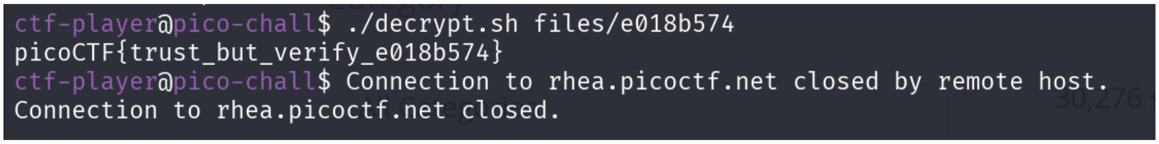


```
cedd15f19fa73a747ec202ef08443cb86d82e5d8143bcf9e0f52d98d9179aabb  files/dINee6RV
64636ee34e6c01eeb
973396c4c421e34b1
f15844dcdd1e399b59c5e5a46fab9bd09aae3cbeec85c639334265badbf25e61  files/dZVnOthw
14e034ca1e1c1dee459ae0706e6fe29dd524cf39c2db7c7bc988e2b807e7f1ca  files/dkV6p1DF
80fbad83555ea83ba9400008cb996a6d6cc4d0fb4f7a99cb2f9c7fc75cb94459  files/dtc6oz6G
3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4  files/e018b574
f6c69cb793f0b94d8b103734b2d14545d09bb868afd77a76277cb88a79502b7e  files/e7irOvB1
c9be6ef77d57d8667c9249948fe2f2edaf28a3088faafe1599c89e6ca3948ef9  files/exGstYty
```

Step 4: Decrypt the File

Used the provided decryption script to extract the flag:

```
./decrypt.sh files/e018b574
```



```
ctf-player@pico-chall$ ./decrypt.sh files/e018b574
picoCTF{trust_but_verify_e018b574}
ctf-player@pico-chall$ Connection to rhea.picoctf.net closed by remote host.
Connection to rhea.picoctf.net closed.
```

Output

```
picoCTF{trust_but_verify_e018b574}
```

The flag was successfully decrypted and verified as correct.