Challenge: Shattered Tablet

Challenge Description :

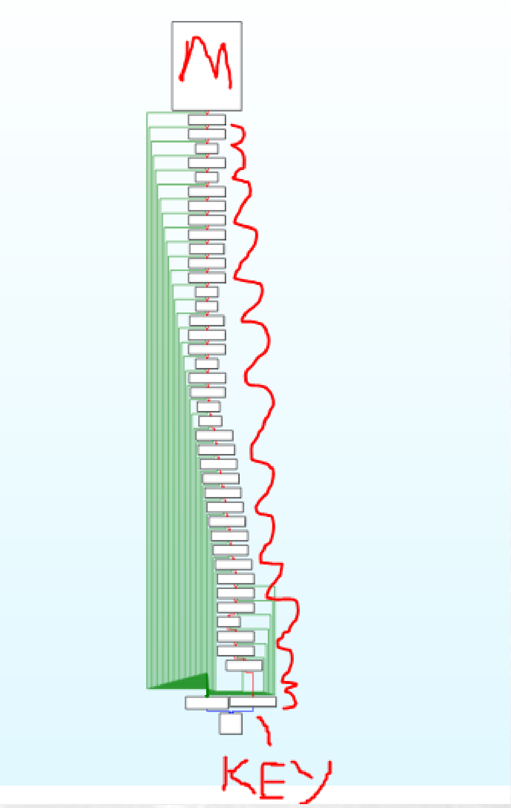
Deep in an ancient tomb, you've discovered a stone tablet with secret information on the locations of other relics. However, while dodging a poison dart, it slipped from your hands and shattered into hundreds of pieces. Can you reassemble it and read the clues?

Context :

- Analyze this Compiled file, for this one you must keep your eyes peeled as its looking at plain binary, for reconstruction on the HTB flag

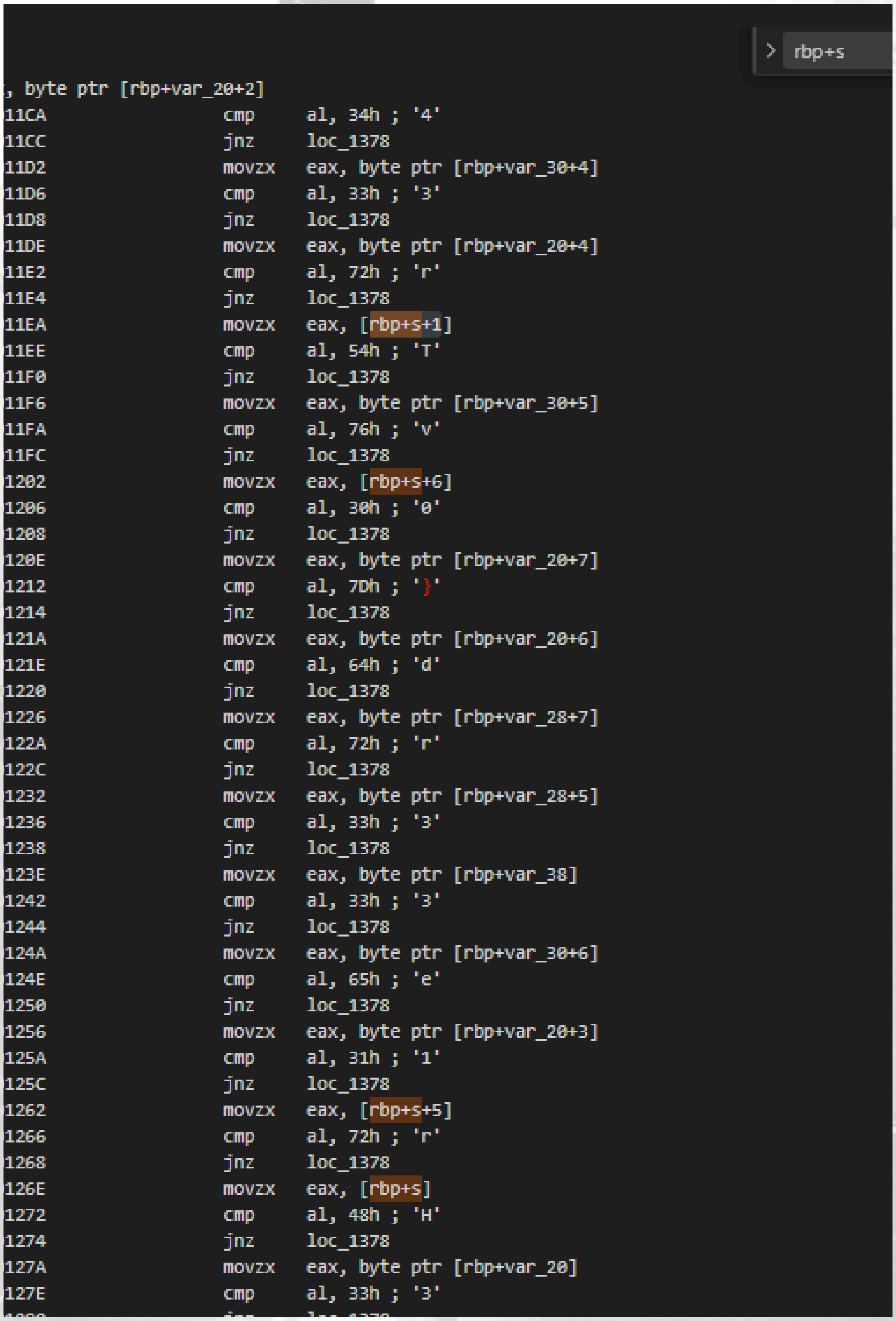
Flag :

- First Install the files and extract them, Load it up with a decompiler that supports ELF files at least.
- I opened it up with IDA Decompiler and went to start on the main function, to look for anything interesting.
- I only thing i found was some logic to enter a specific string, that had been messed about with and scattered in random binary locations



- The [M] at the top represents the main function and the boxes in-between leading downwards towards the [Key] each contain a single Characters i need to reconstruct the flag. The Last three boxes at the end is logic for if the flag is correct or not.
- Each of the Boxes in-between are also not in-order so i will need to find a pattern to match them.
- I was finally able to find a way to reconstruct the flag, reading the binary closely you can start to realize they are labeled to be put in order.
- For example a flag would be like : HTB{Ex4mpl3} . And the binary for H will be [rbp+s] and T will be [rbp+s+1]

- The Reconstruction of the flag wasn't as easy as i hoped, but going slowly one by one i was able to do it.



```
, byte ptr [rbp+var_20+2]
11CA                cmp     al, 34h ; '4'
11CC                jnz     loc_1378
11D2                movzx   eax, byte ptr [rbp+var_30+4]
11D6                cmp     al, 33h ; '3'
11D8                jnz     loc_1378
11DE                movzx   eax, byte ptr [rbp+var_20+4]
11E2                cmp     al, 72h ; 'r'
11E4                jnz     loc_1378
11EA                movzx   eax, [rbp+s+1]
11EE                cmp     al, 54h ; 'T'
11F0                jnz     loc_1378
11F6                movzx   eax, byte ptr [rbp+var_30+5]
11FA                cmp     al, 76h ; 'v'
11FC                jnz     loc_1378
1202                movzx   eax, [rbp+s+6]
1206                cmp     al, 30h ; '0'
1208                jnz     loc_1378
120E                movzx   eax, byte ptr [rbp+var_20+7]
1212                cmp     al, 7Dh ; '}'
1214                jnz     loc_1378
121A                movzx   eax, byte ptr [rbp+var_20+6]
121E                cmp     al, 64h ; 'd'
1220                jnz     loc_1378
1226                movzx   eax, byte ptr [rbp+var_28+7]
122A                cmp     al, 72h ; 'r'
122C                jnz     loc_1378
1232                movzx   eax, byte ptr [rbp+var_28+5]
1236                cmp     al, 33h ; '3'
1238                jnz     loc_1378
123E                movzx   eax, byte ptr [rbp+var_38]
1242                cmp     al, 33h ; '3'
1244                jnz     loc_1378
124A                movzx   eax, byte ptr [rbp+var_30+6]
124E                cmp     al, 65h ; 'e'
1250                jnz     loc_1378
1256                movzx   eax, byte ptr [rbp+var_20+3]
125A                cmp     al, 31h ; '1'
125C                jnz     loc_1378
1262                movzx   eax, [rbp+s+5]
1266                cmp     al, 72h ; 'r'
1268                jnz     loc_1378
126E                movzx   eax, [rbp+s]
1272                cmp     al, 48h ; 'H'
1274                jnz     loc_1378
127A                movzx   eax, byte ptr [rbp+var_20]
127E                cmp     al, 33h ; '3'
```

- The Flag when Constructed should be :

HTB{br0k3n_4p4rt...n3ver_t0_b3_r3p41r3d}