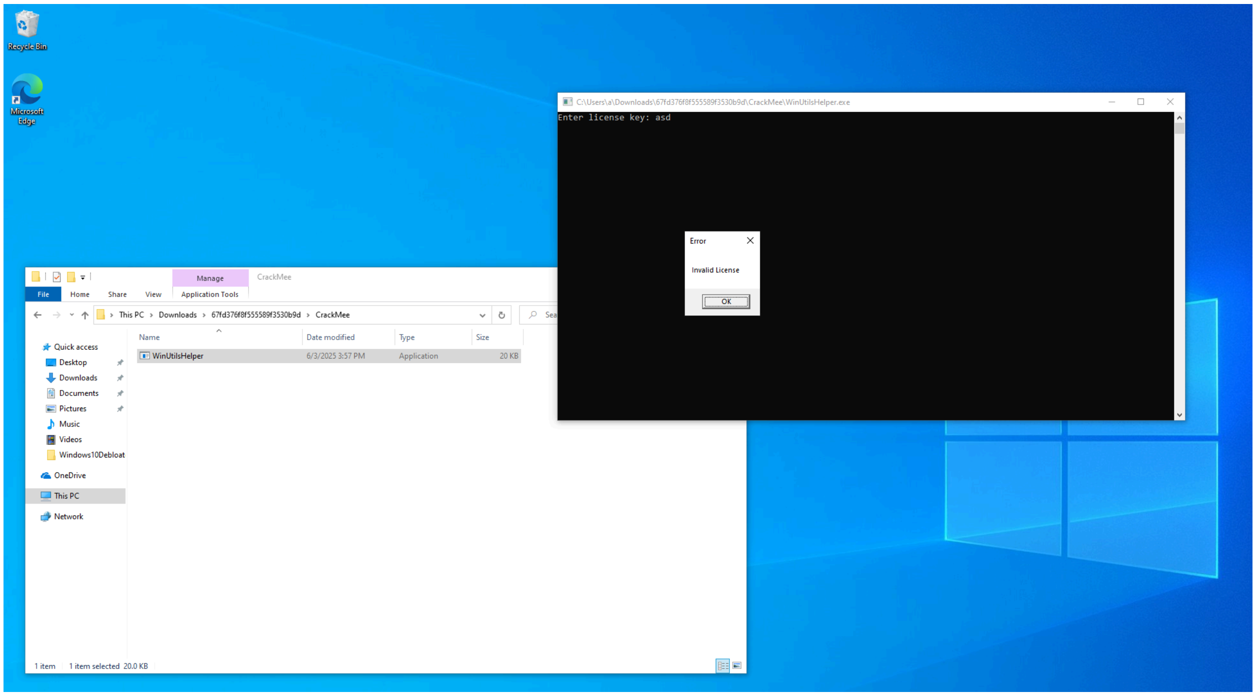
Simple crackme

https://crackmes.one/crackme/67fd376f8f555589f3530b9d

For the purpose of this reverse engineering, I was using a vmware windows 10 machine and ghidra

Upon downloading the file, I ran it to see how I am able to interact with the program. Upon launch, the program immediately asks for a key:



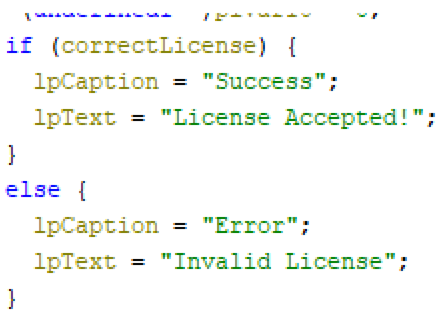
C:\Users\a\Downloads\67fd376f8f555589f3530b9d\CrackMee\WinUtilsHelper.exe

```
Enter license key: asd
```

Error

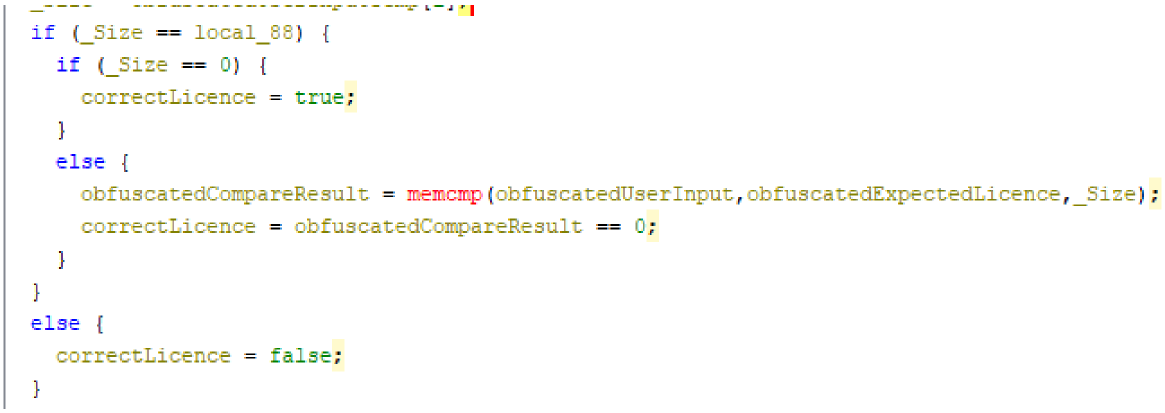
Invalid License

Knowing this, I load the program into ghidra and look through the code. As we were able to determine, we get an error popup message when an invalid key was entered. Therefore I was able to find the if-else statement that determines if I have entered the correct key.



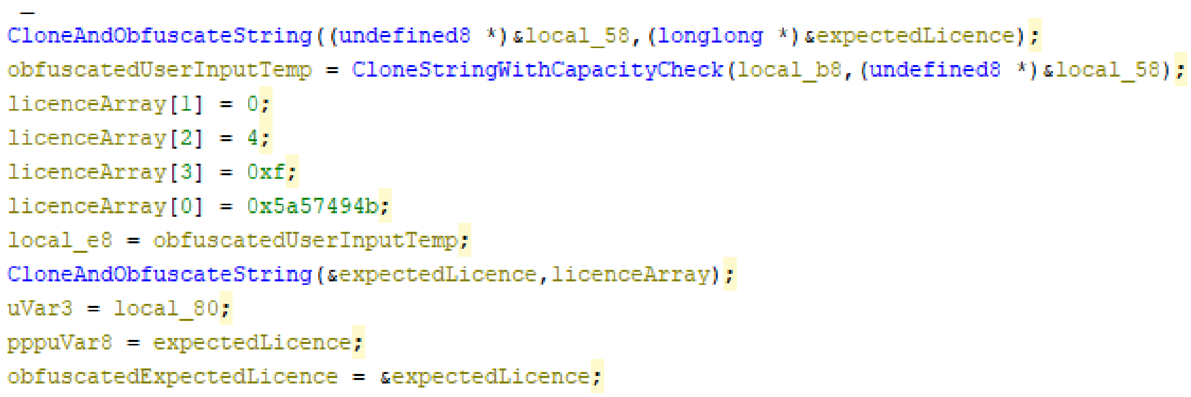
```
if (correctLicense) {
  lpCaption = "Success";
  lpText = "License Accepted!";
}
else {
  lpCaption = "Error";
  lpText = "Invalid License";
}
```

I then am able to work backwards from that piece of code, updating variable names as I go. Taking a glance at the whole function that the key check is in, it seems like there is a lot of obfuscation happening and redundancy. However, after the obfuscation, there is a comparison between the user input and the expected key which determines if the licence is correct.



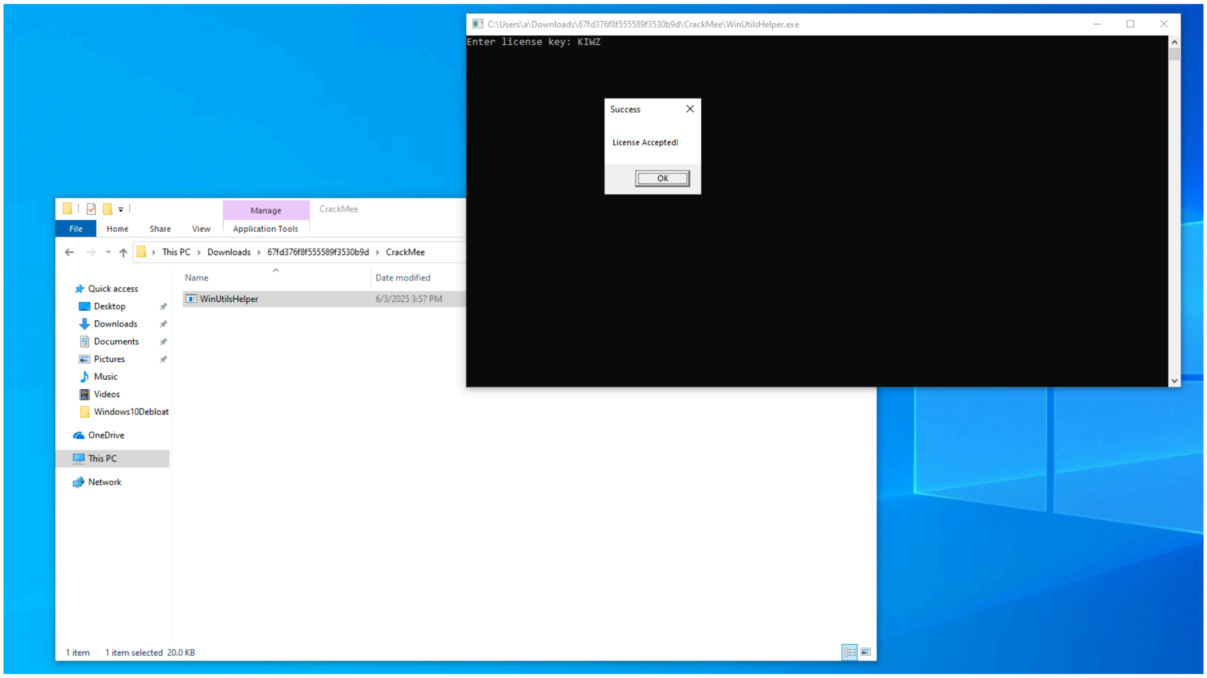
```
if (_Size == local_88) {
  if (_Size == 0) {
    correctLicence = true;
  }
  else {
    obfuscatedCompareResult = memcmp(obfuscatedUserInput,obfuscatedExpectedLicence,_Size);
    correctLicence = obfuscatedCompareResult == 0;
  }
}
else {
  correctLicence = false;
}
```

Sifting through the obfuscation, I was able to trace my way up to the root licence. In the licence array, the first entry is 0x5a57494b which is “ZWIK”, and due to it being in little endian then it would mean that “KIWZ” should be entered.



```
CloneAndObfuscateString((undefined8 *)&local_58,(longlong *)&expectedLicence);
obfuscatedUserInputTemp = CloneStringWithCapacityCheck(local_b8,(undefined8 *)&local_58);
licenceArray[1] = 0;
licenceArray[2] = 4;
licenceArray[3] = 0xf;
licenceArray[0] = 0x5a57494b;
local_e8 = obfuscatedUserInputTemp;
CloneAndObfuscateString(&expectedLicence,licenceArray);
uVar3 = local_80;
pppuVar8 = expectedLicence;
obfuscatedExpectedLicence = &expectedLicence;
```

Running the program again, I enter “KIWZ” and the popup shows that the input has been accepted.



```
C:\Users\a\Downloads\67fd376f8f555589f3530b9d\CrackMee\WinUtilsHelper.exe
Enter license key: KIWZ
```

Success

License Accepted!