

ebp-1c is the char index

File1:

ebp-0x20 must be 5

ebp-0x28 must be 5

ebp-0x2C must be 0x0A

1st char must be F

3rd char must be L

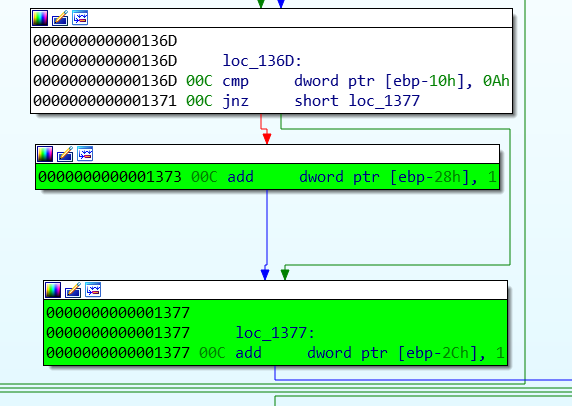
5th char must be A

9th char must be G

10th char must be 1

\* IMPORTANT \*

For file1: Having hex 0x0A will trigger addition of ebp-0x28.



Final file1:



File2:

2nd char must be F

4th char must be L

6th char must be A

12th char must be G

13th char must be 2

ebp-2C must be 0x1E

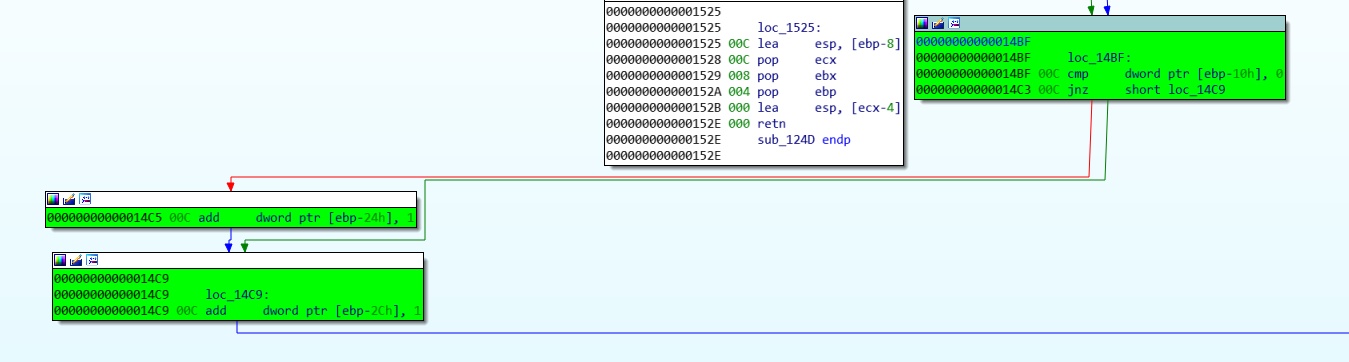
ebp-24 must be 0x19

ebp-20 must be 5        -> hit

\* IMPORTANT \*

For file2:

Having hex 0x00 will trigger addition of 0x24 and 0x2C



Final file2:

