The challenge involves exploiting a poorly memory bounds checked game to spawn in coins.

A screenshot of a video game

Description automatically generatedA screenshot of a video game

Description automatically generated

A pixelated cartoon characters

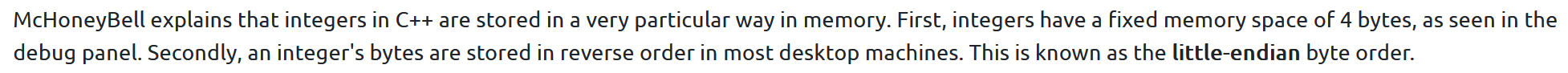
Description automatically generatedEach box counts as a byte of memory. There are 12 spaces before you begin to overwrite into the coins bound in memory. This is exploited when you approach Van Holly and change your name. He says he can change your name for 1 coin for every character.

All you need to do is farm for 16 coins then you can get 1094795585 coins.

**Question 1) If the coins variable had the in-memory value in the image below, how many coins would you have in the game?**

A close-up of a number

Description automatically generated



This is key information before I continue to solve this problem.

A screenshot of a number

Description automatically generatedA screenshot of a computer

Description automatically generated

**Answer**: 1397772111

A screenshot of a video game

Description automatically generated**Question 2) What is the value of the final flag?**

For this it requires you to realise that when buying items the game stores the id in memory (right side, in red).

A close-up of a card

Description automatically generatedNow this means that if I count the number of boxes before I reach the ID 1 in the ‘INV\_ITEMS’ memory location, it will take 45 characters.

A black and white text

Description automatically generated with medium confidenceGoing back to the name change you replace the 45th character with the ID of the star, which is ‘d’.

**NOTE**: I took this screenshot before I changed it back to lowercase.

This results in the bytes being overwritten and the star appearing in your inventory.

A picture of a star and a cross

Description automatically generated

A close-up of a black and white text

Description automatically generated