**Applied Cryptography (UE20CS314)**

**Lab 6**

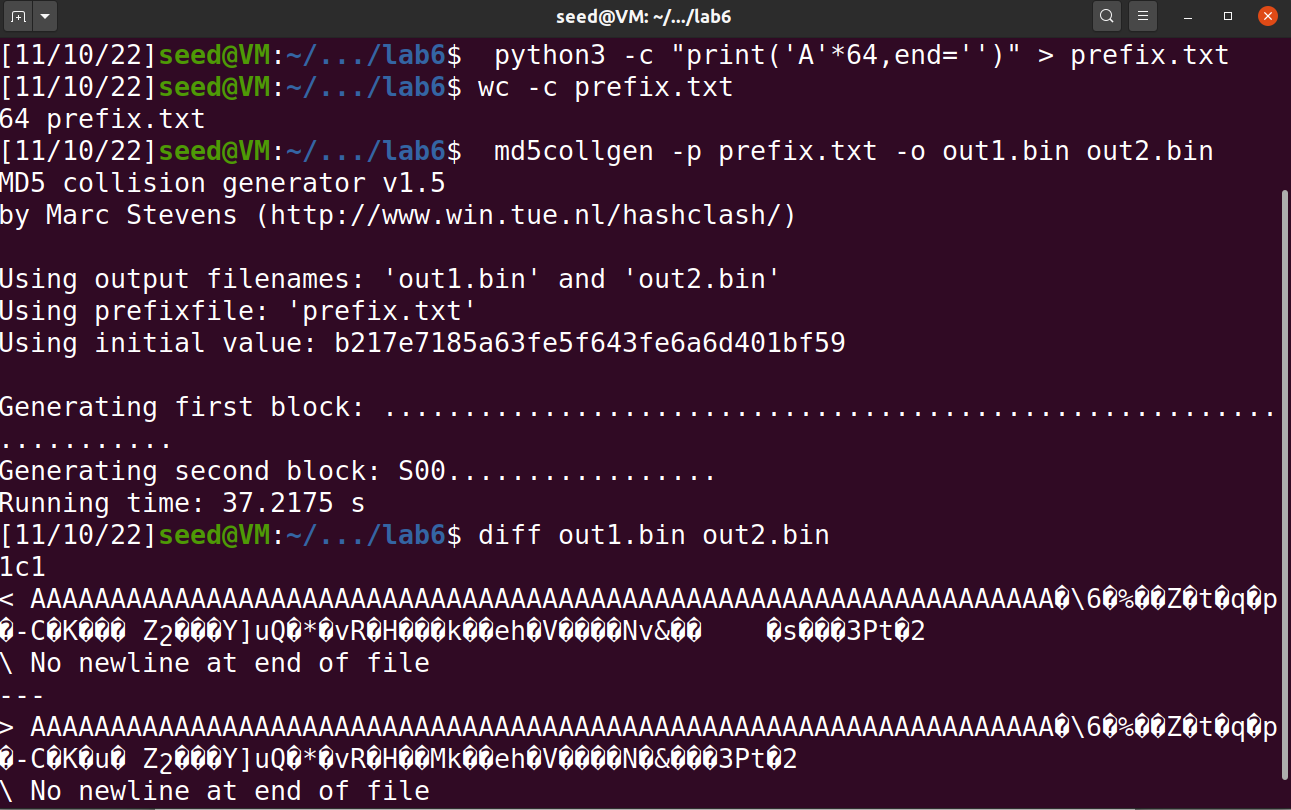
**Name: Vishwa Mehul Mehta**

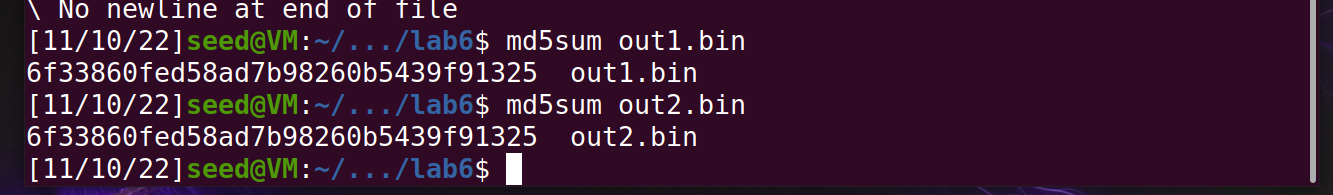
**SRN: PES2UG20CS389**

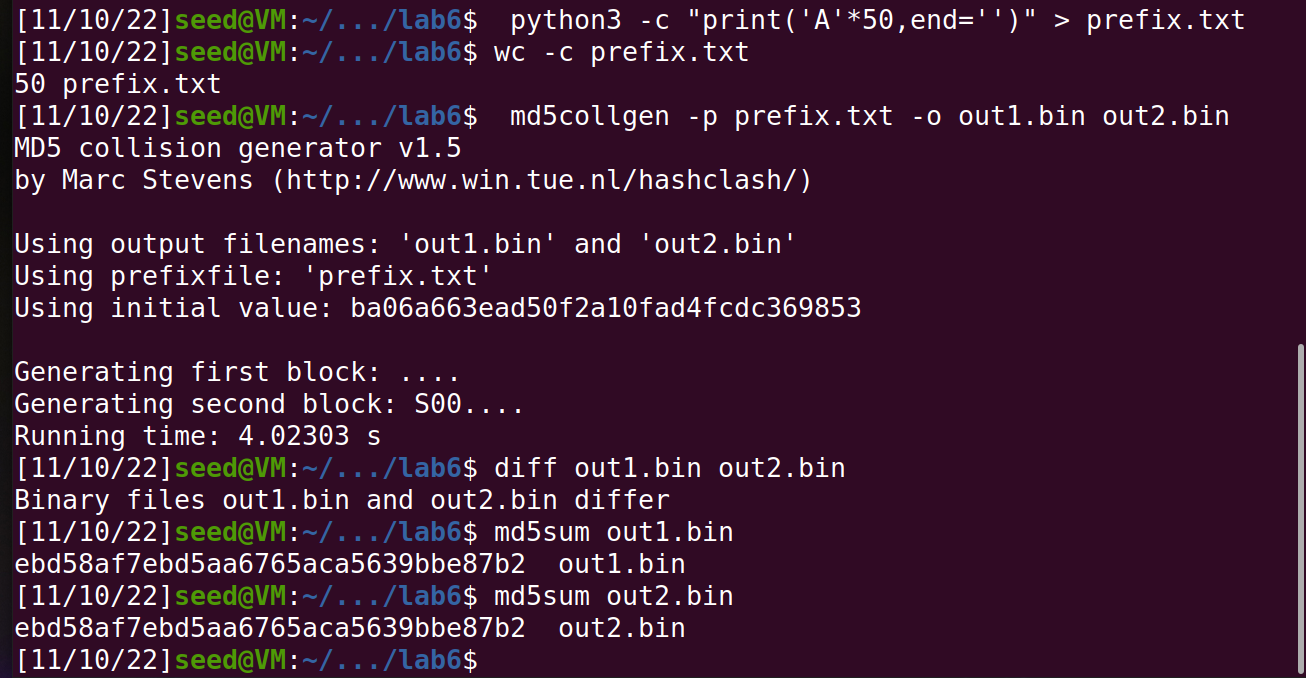
**Section: F**

**Task 1:**

**Screenshot:**





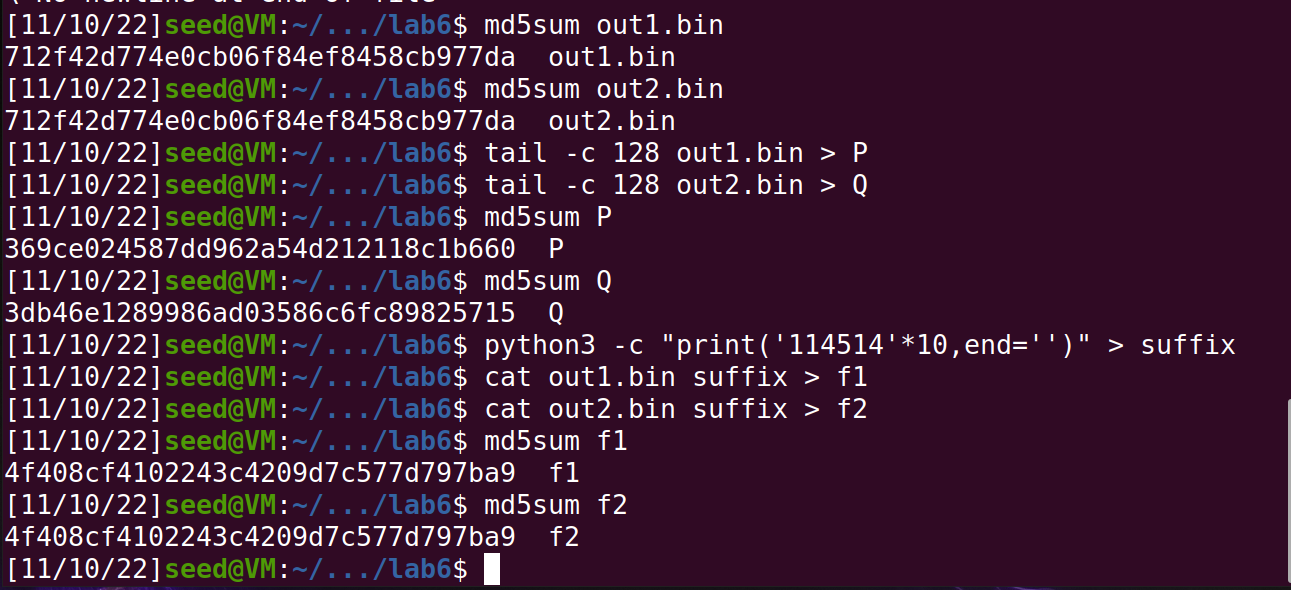


**Observation:**

When the length is not a multiple of 64 the outputs out1.bin and out2.bin differ but they have the same md5sum.

**Task 2:**

**Screenshot:**

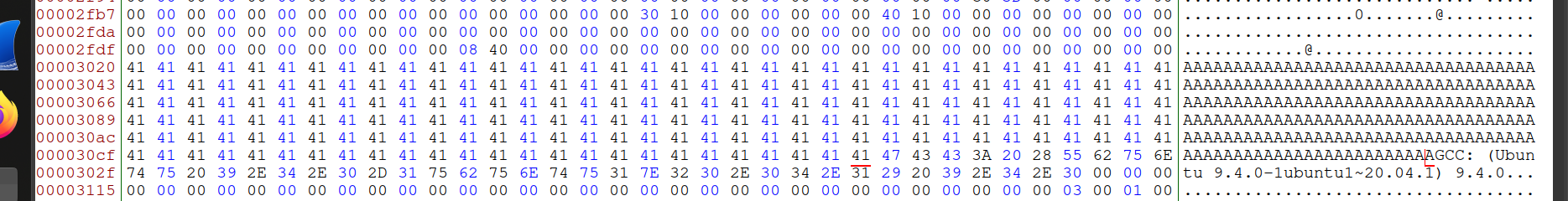


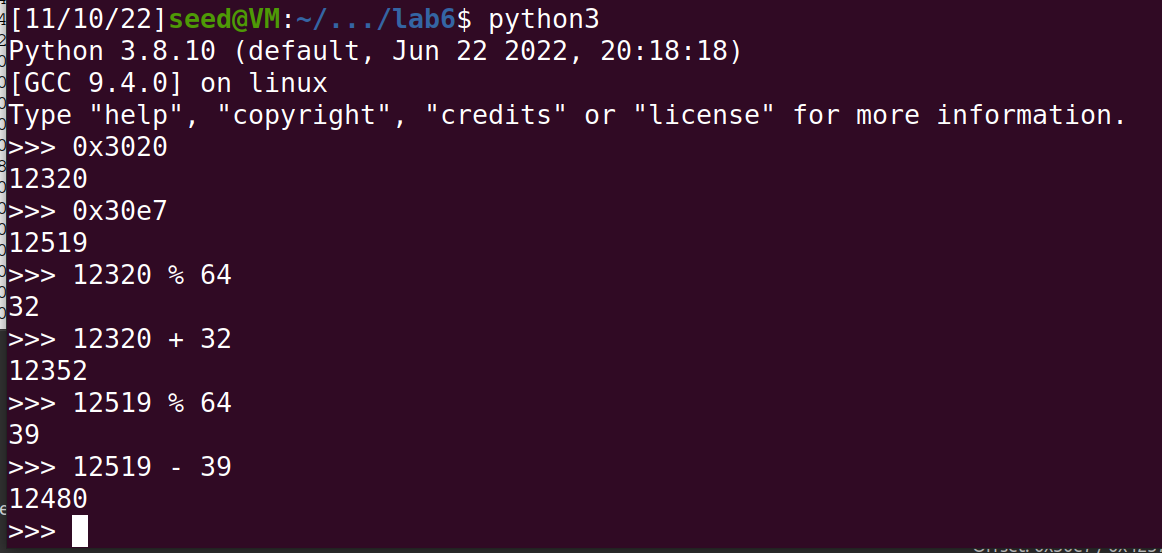
**Observation:**

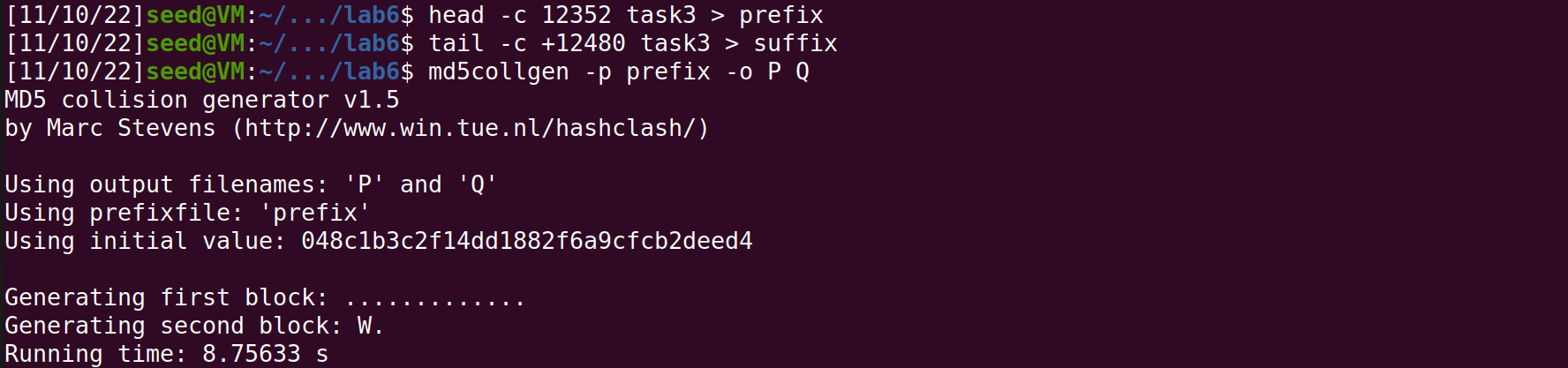
Here, we have shown that adding the same suffix to different prefixes will result in the same hash even though the hashes of the initial prefixes were different.

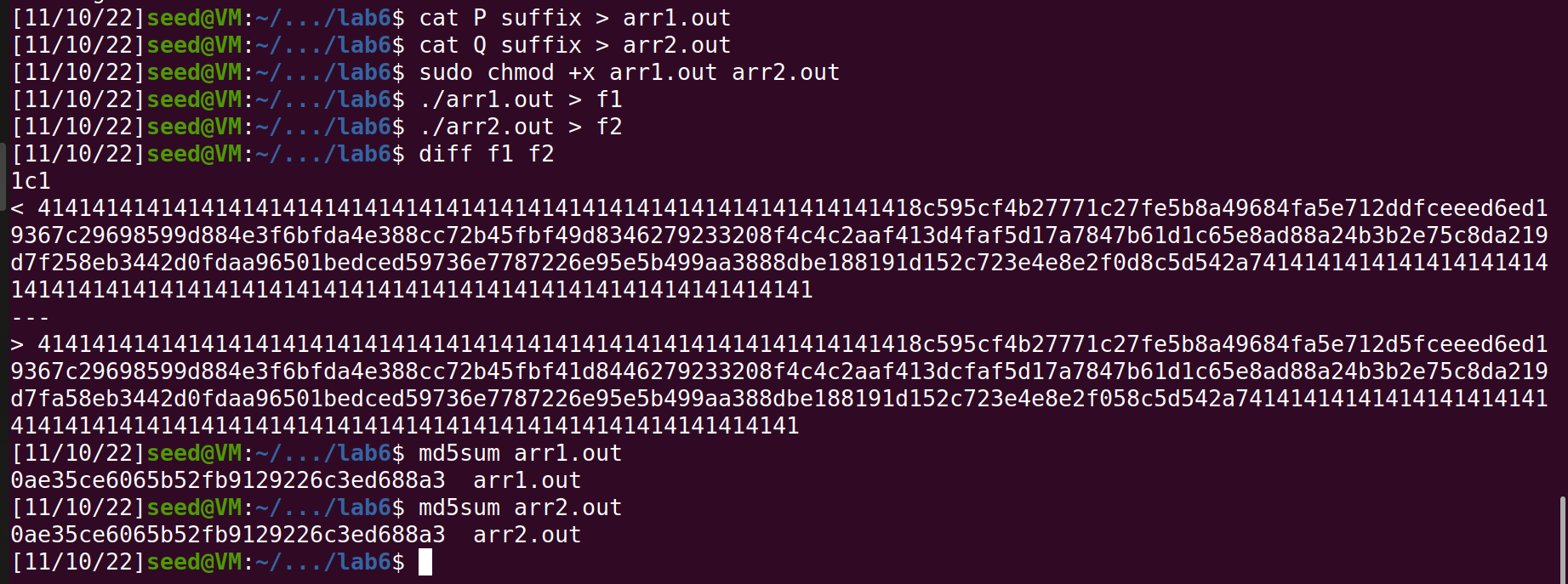
**Task 3:**

**Screenshot:**







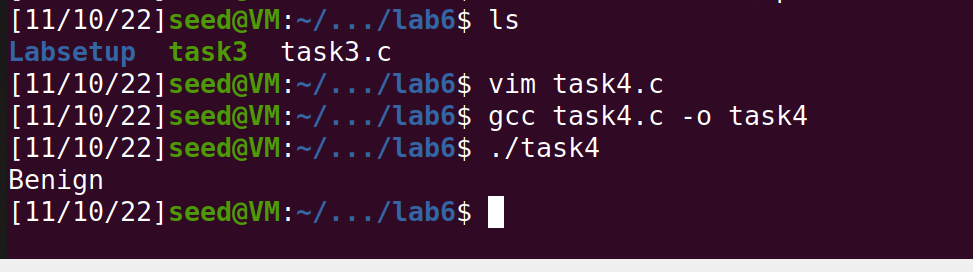


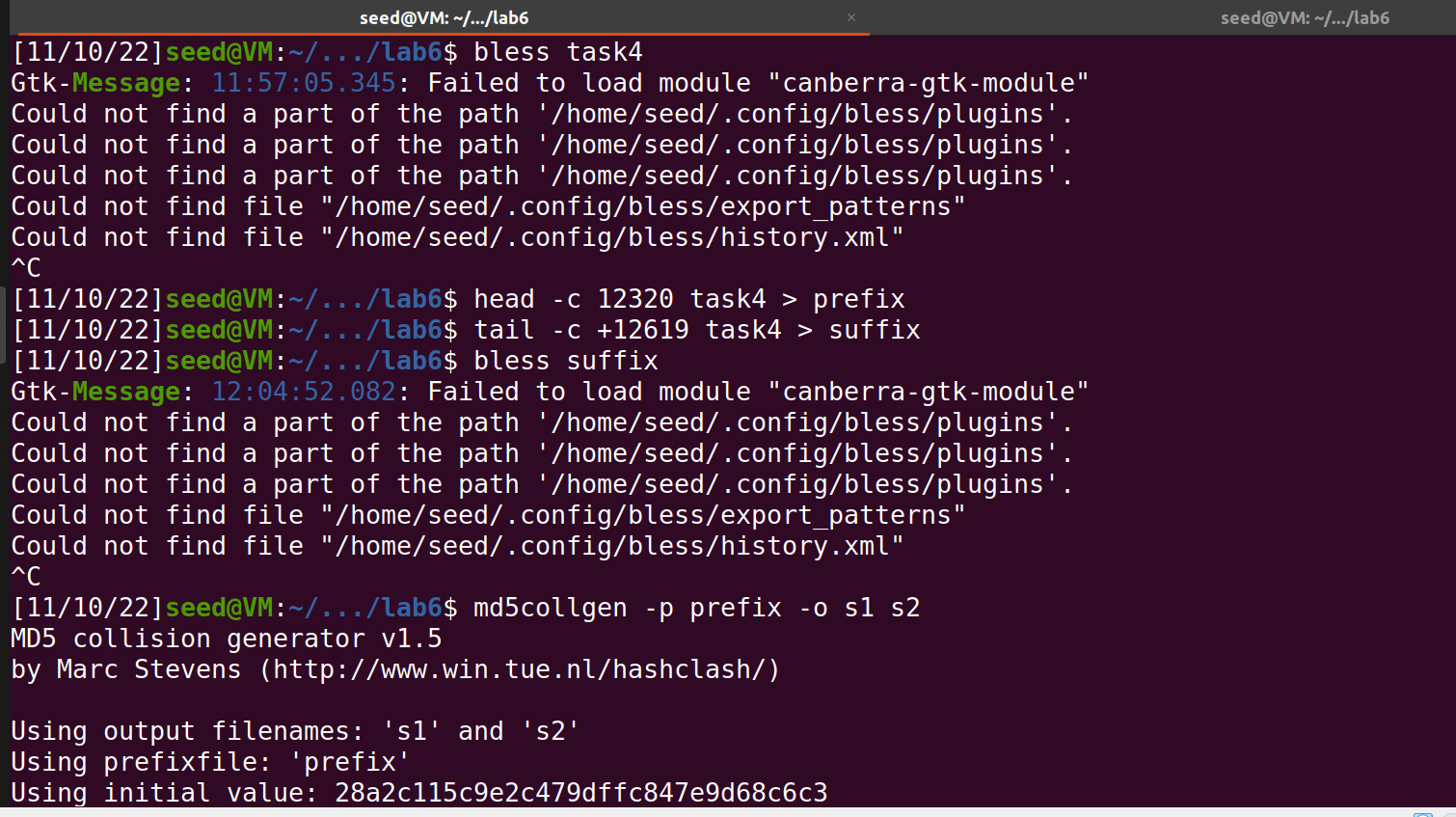
**Observation:**

We have generated different values for the output but the same md5sum.

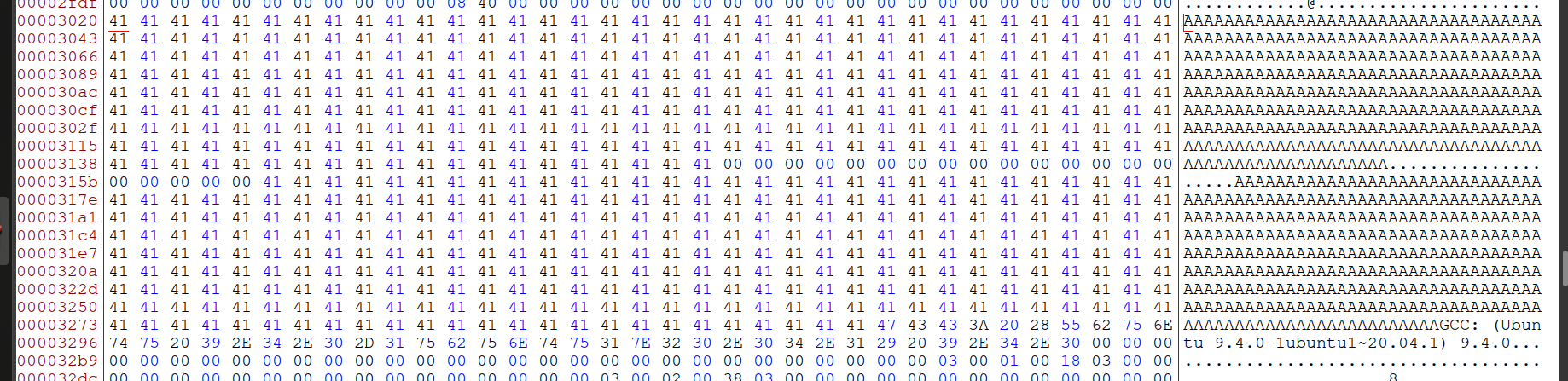
**Task 4:**

**Screenshot:**

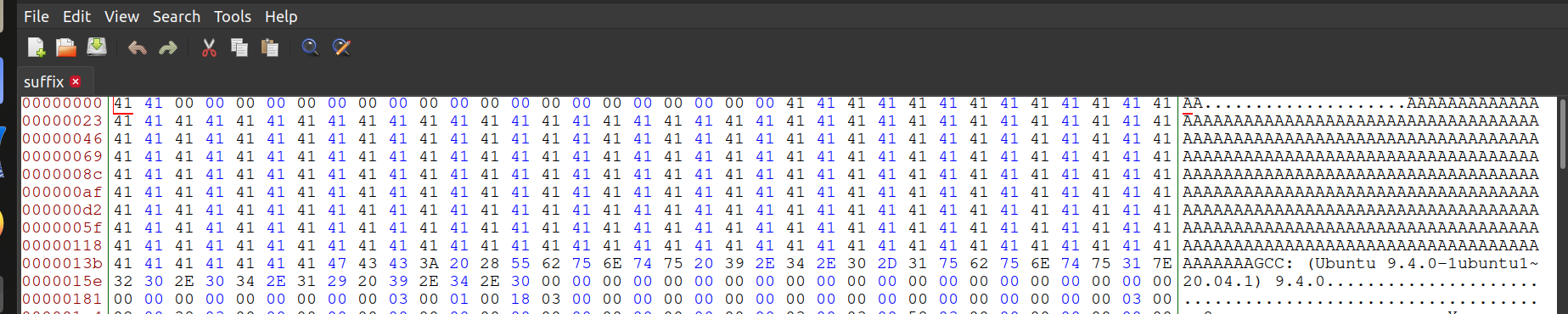


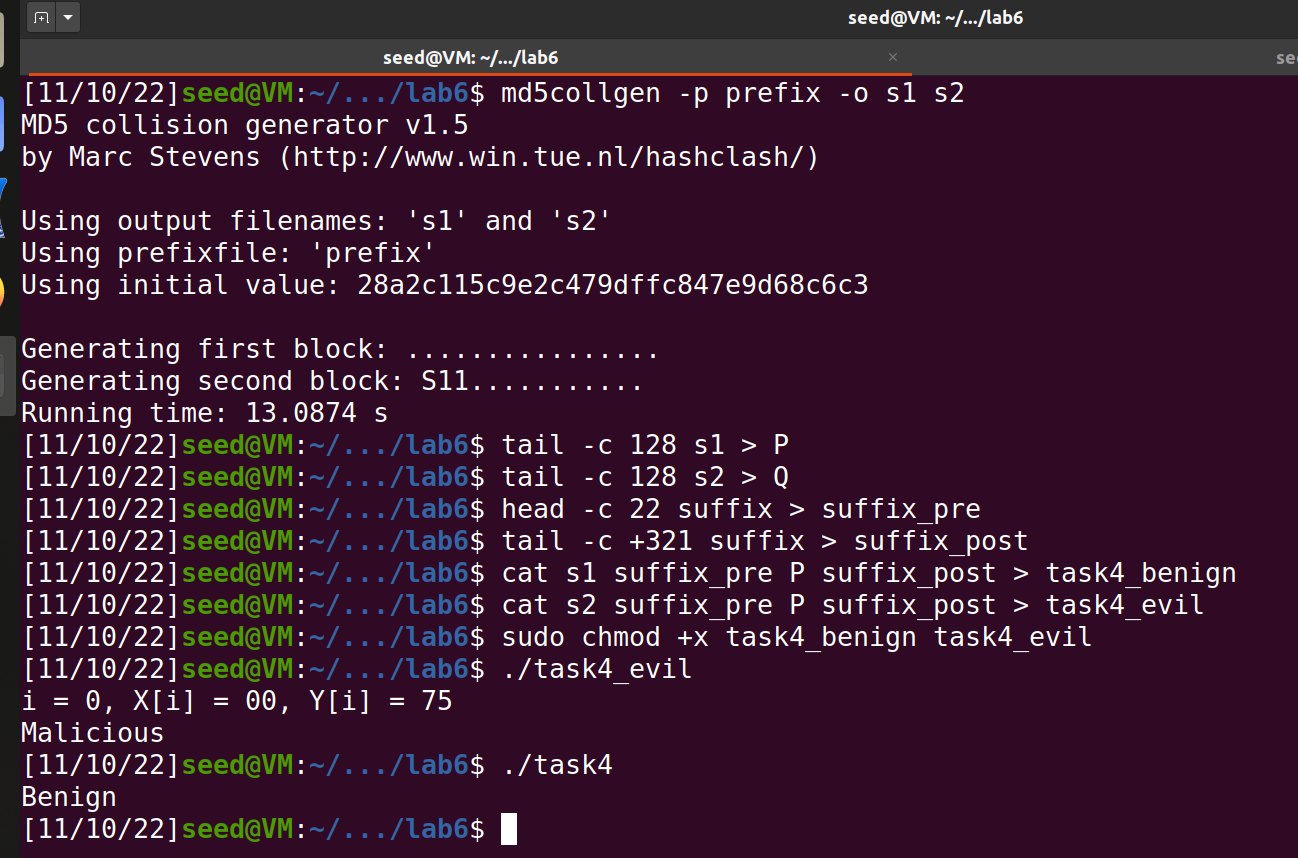


Bless task4:



Bless suffix:





**Observation:**

Since we find a way to generate the same md5 hash value we can get the malicious software authorized.