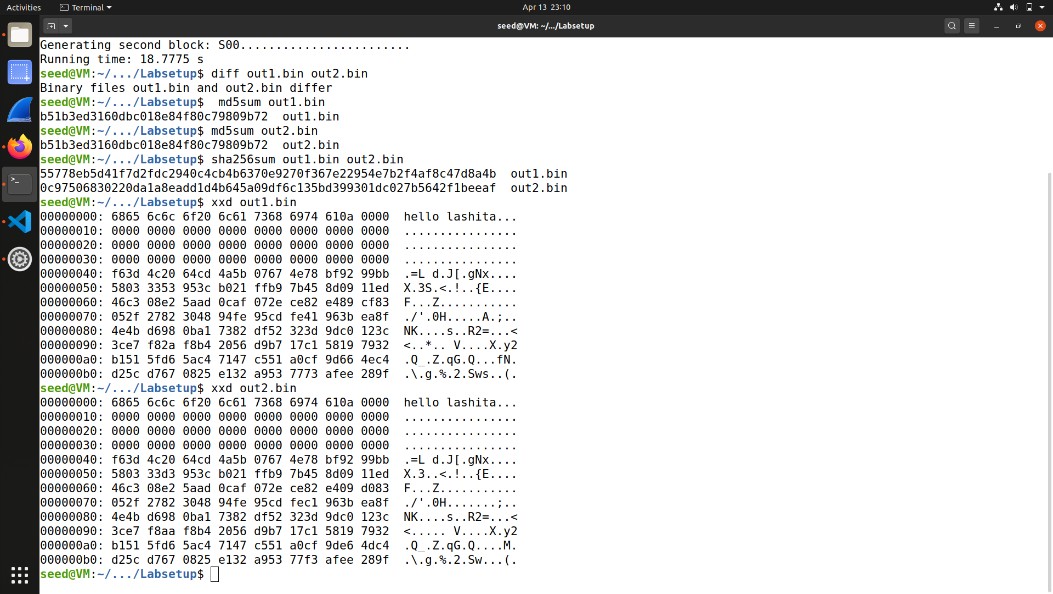
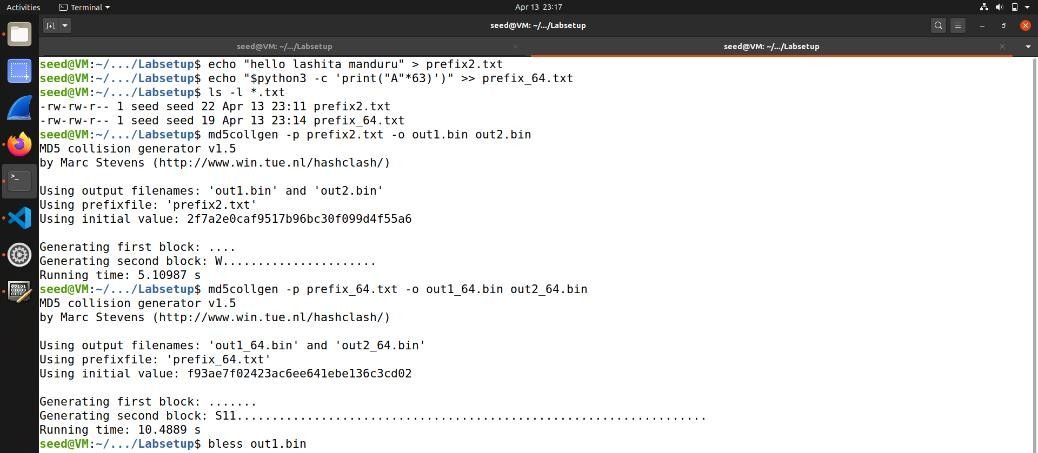
ACS 54500 Cryptography and Network Security Lab 8: MD5 Collision Attack Lab

Task 1: Generating Two Different Files with the Same MD5 Hash

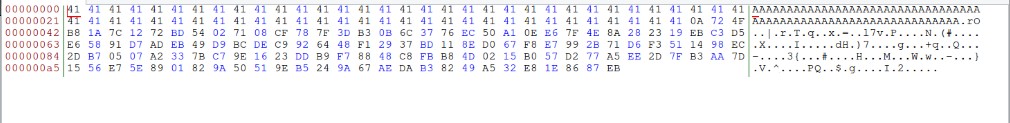
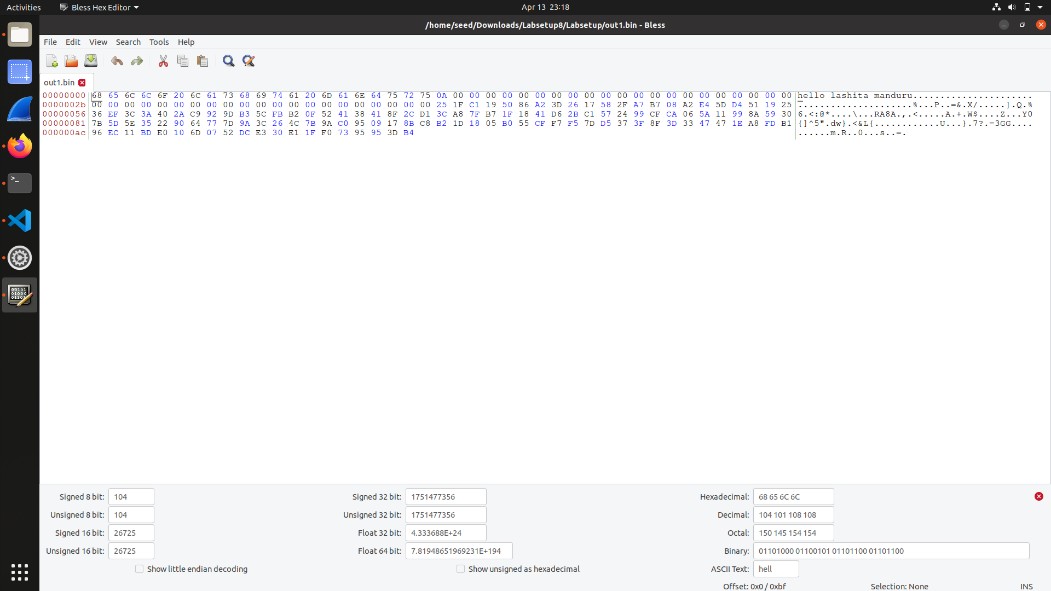
Generating the binary files.

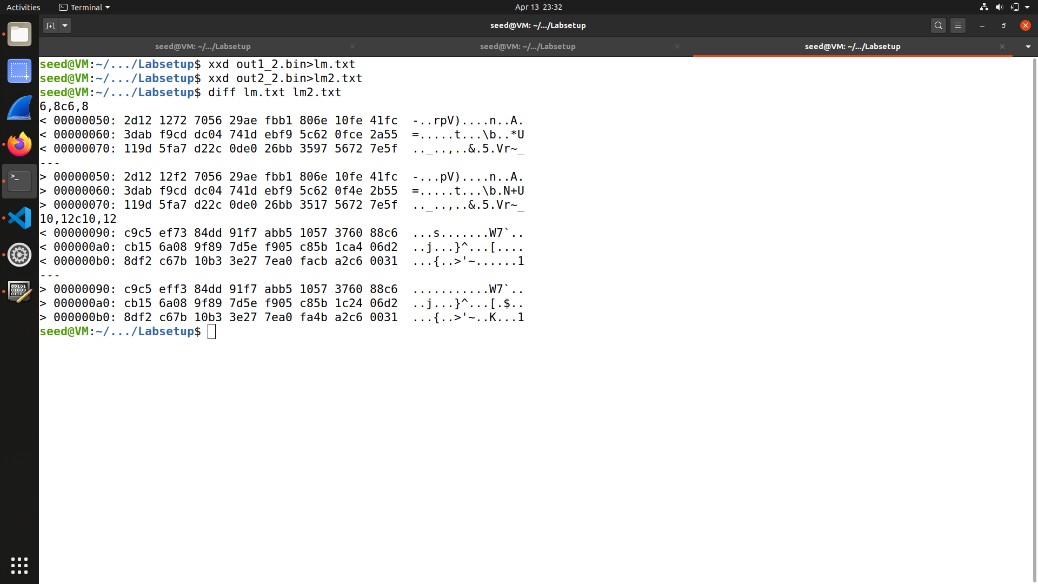
Observing that binary files are different:

Analyzing the binary file, the length of prefix will be padded only if it is a multiple of 64.

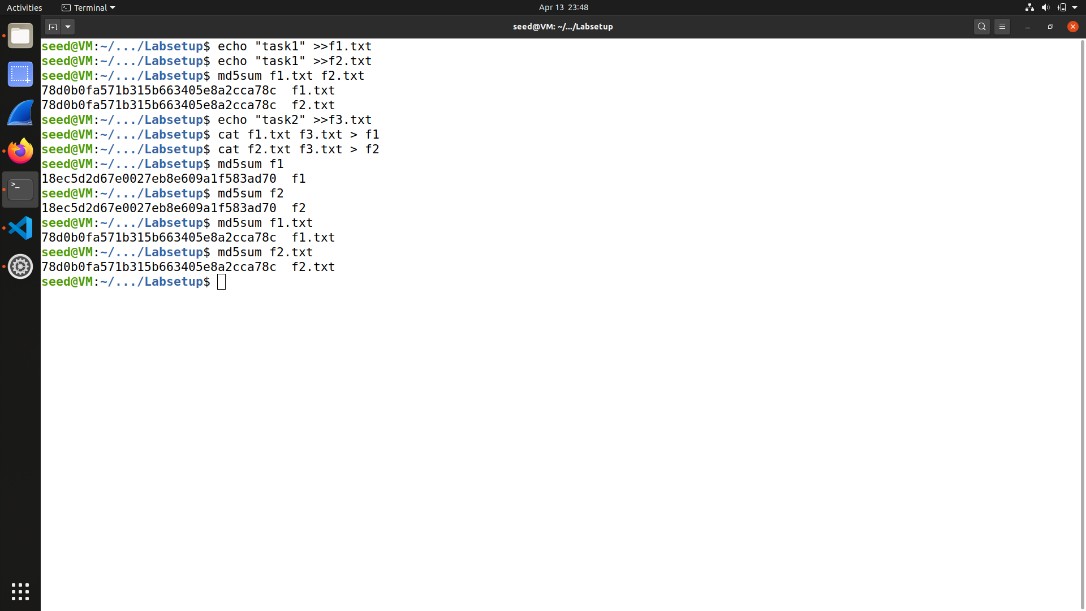
Question 2:

Now prefix file is a multiple of 64:

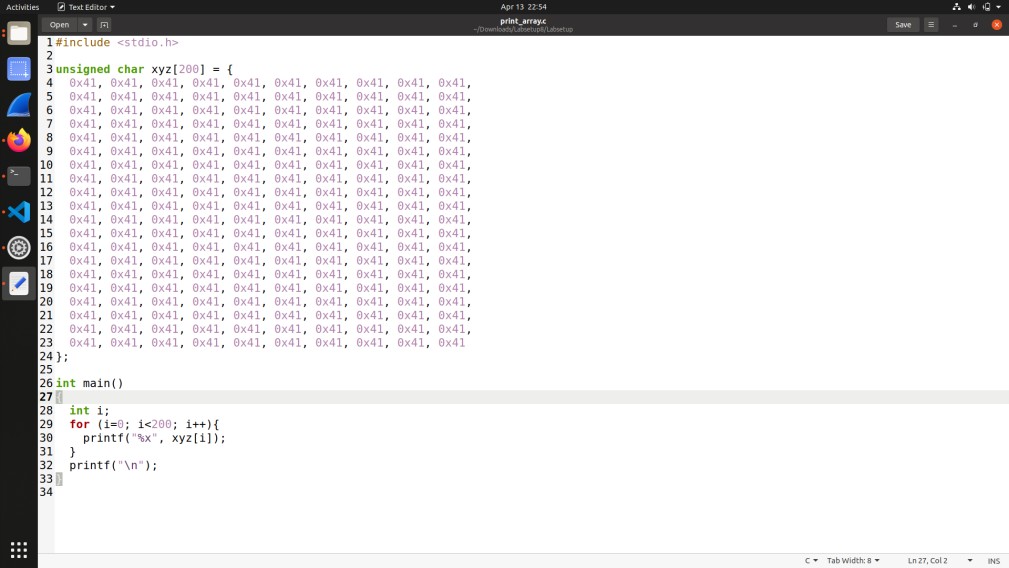


Question 3:

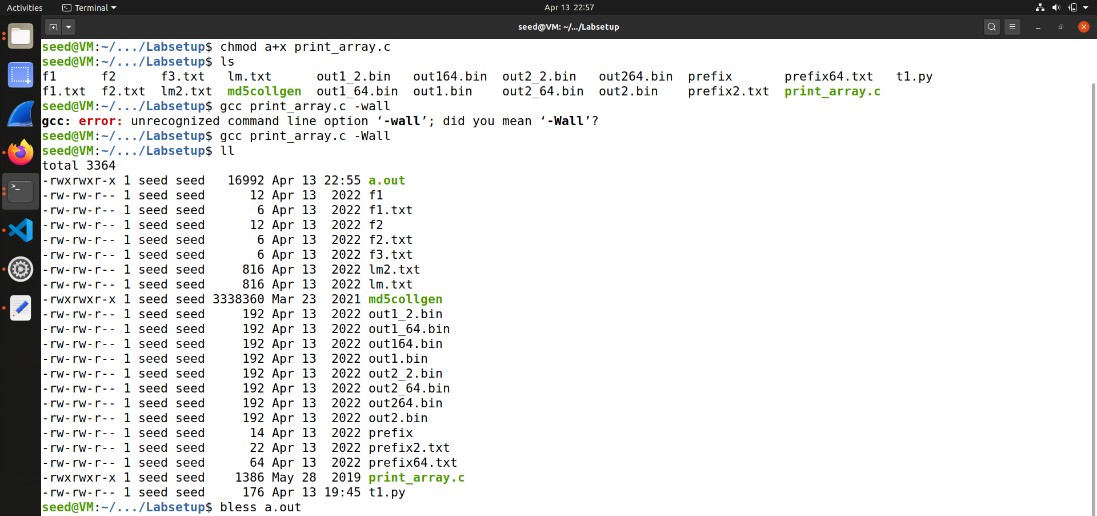
Bytes are different.

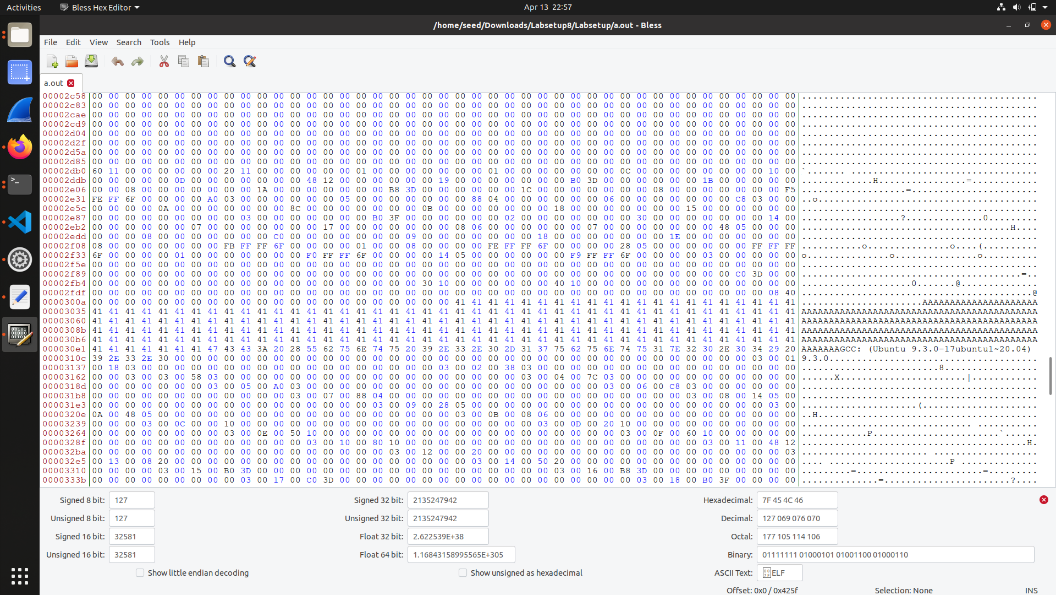
 Task 2: Understanding MD5’s

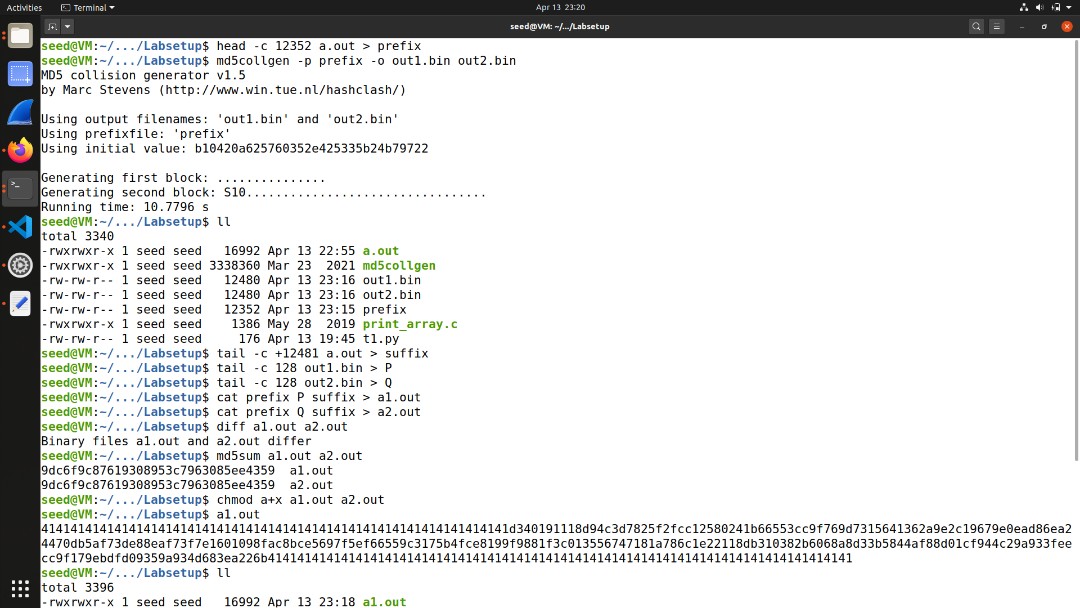
Property

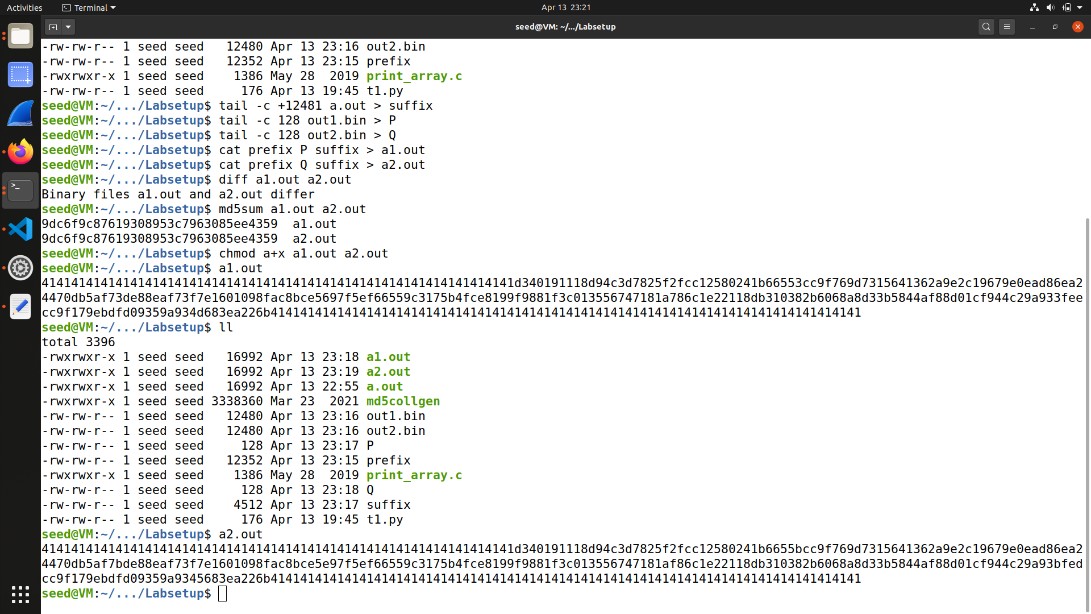
Task 3: Generating Two Executable Files with the Same MD5 Hash

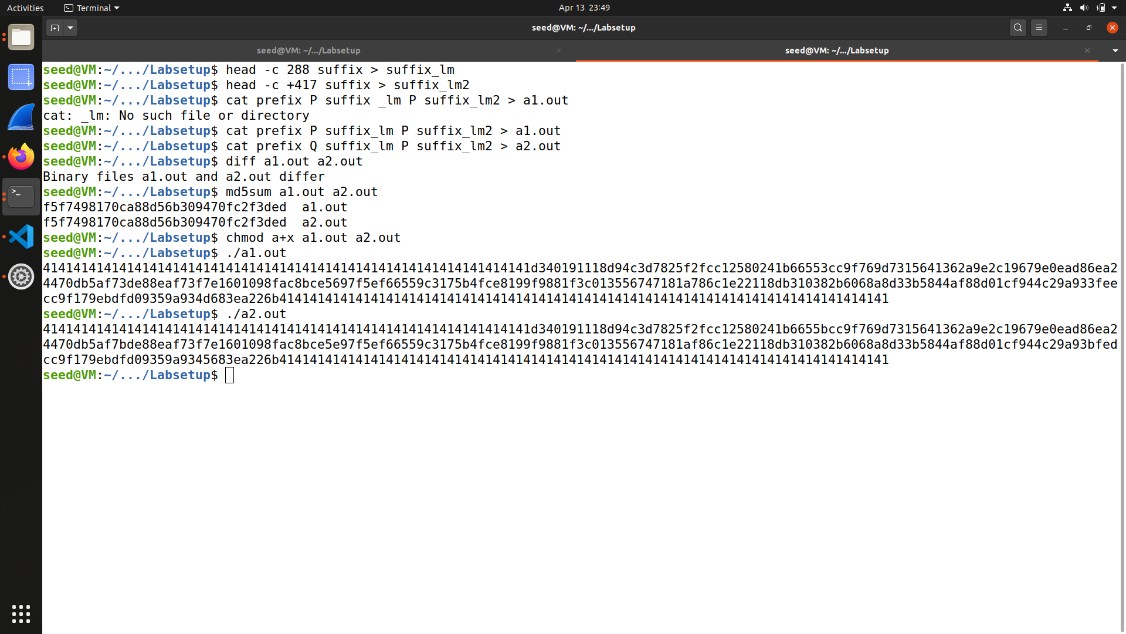
Using the print\_array.c file:



Length of the prefix needs to be multiple of 64 bytes:



both will have same hash value:

Task 4: Making the Two Programs Behave Differently

