Network Security

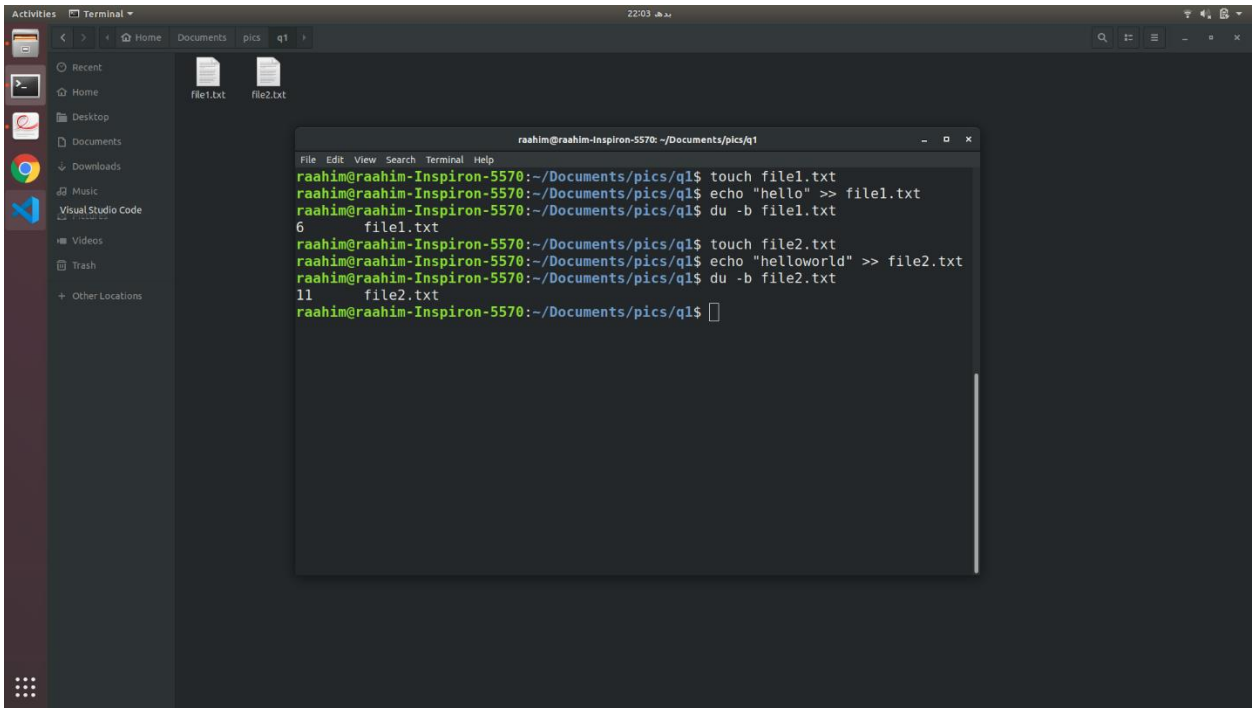
Cryptography Lab (One-Way Hash Functions and MAC)

Muhammad Raahim Khan

21100157

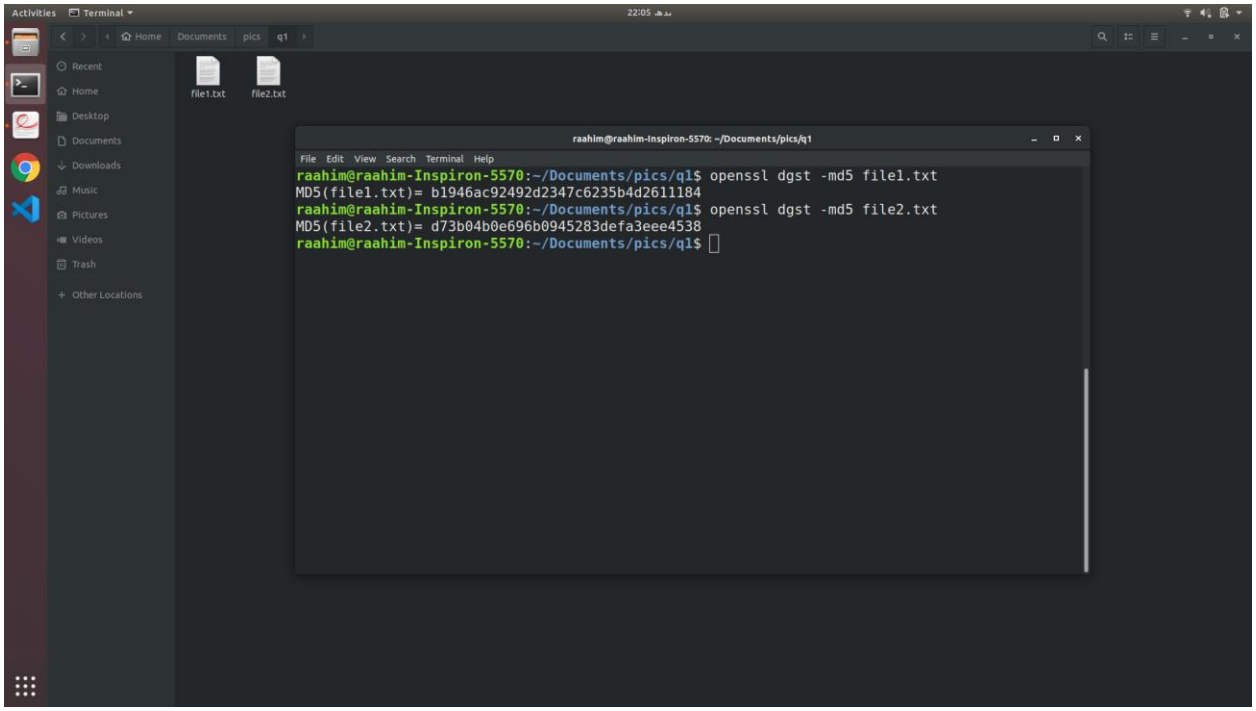
- **<u>Task1:</u>**

1) First I created two text files as shown in the screenshot below of sizes 6 and 11 bytes.

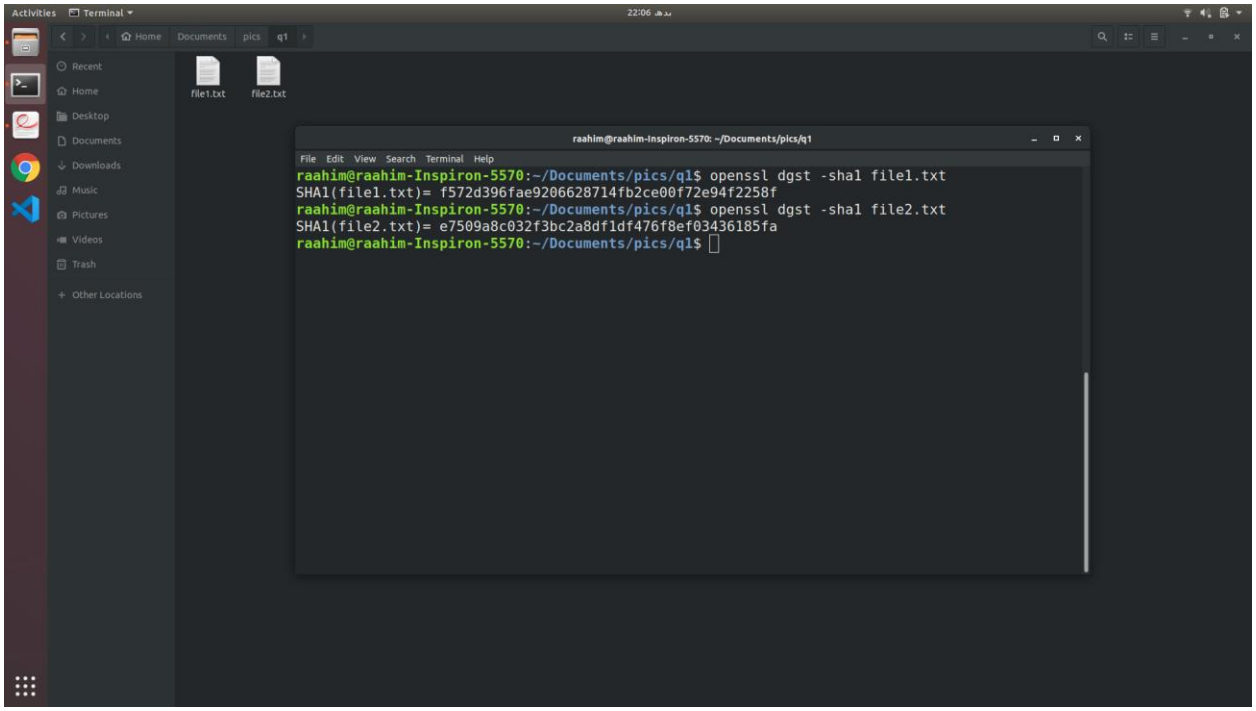


Afterwards, I computed the hash for both of these files using md5, sha1, and sha256 dgsttype.

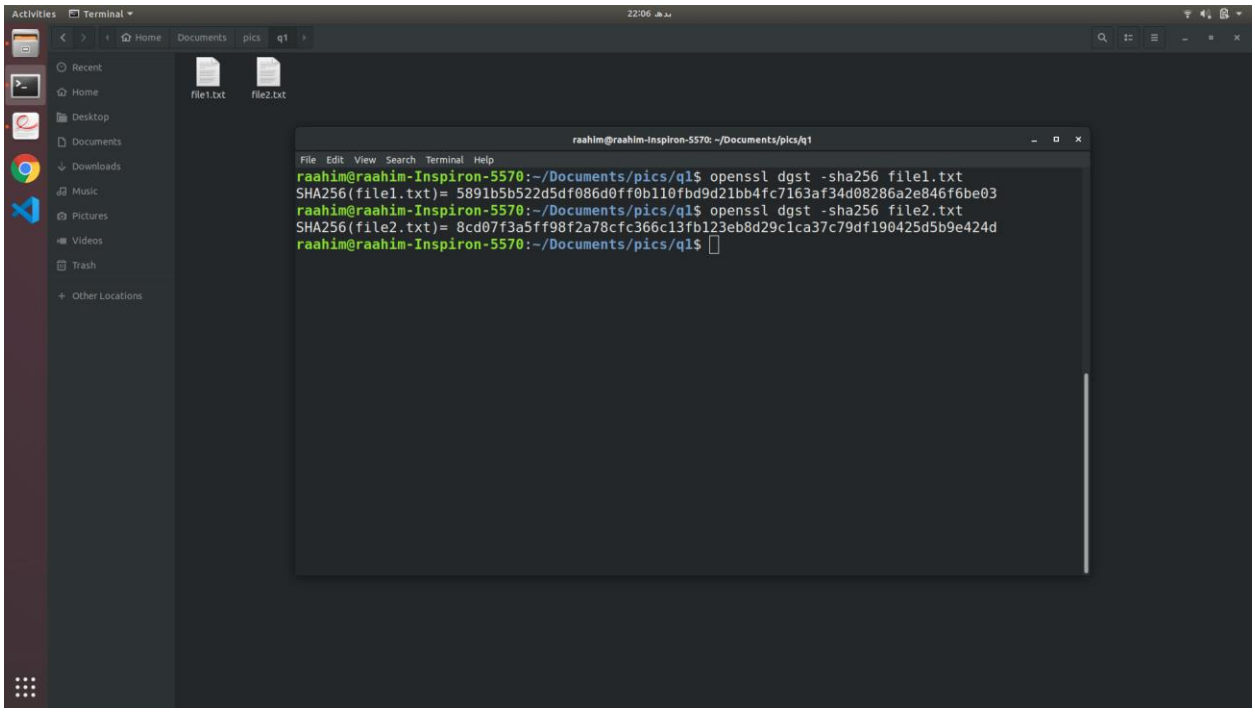
For md5:



For sha1:



For sha256:



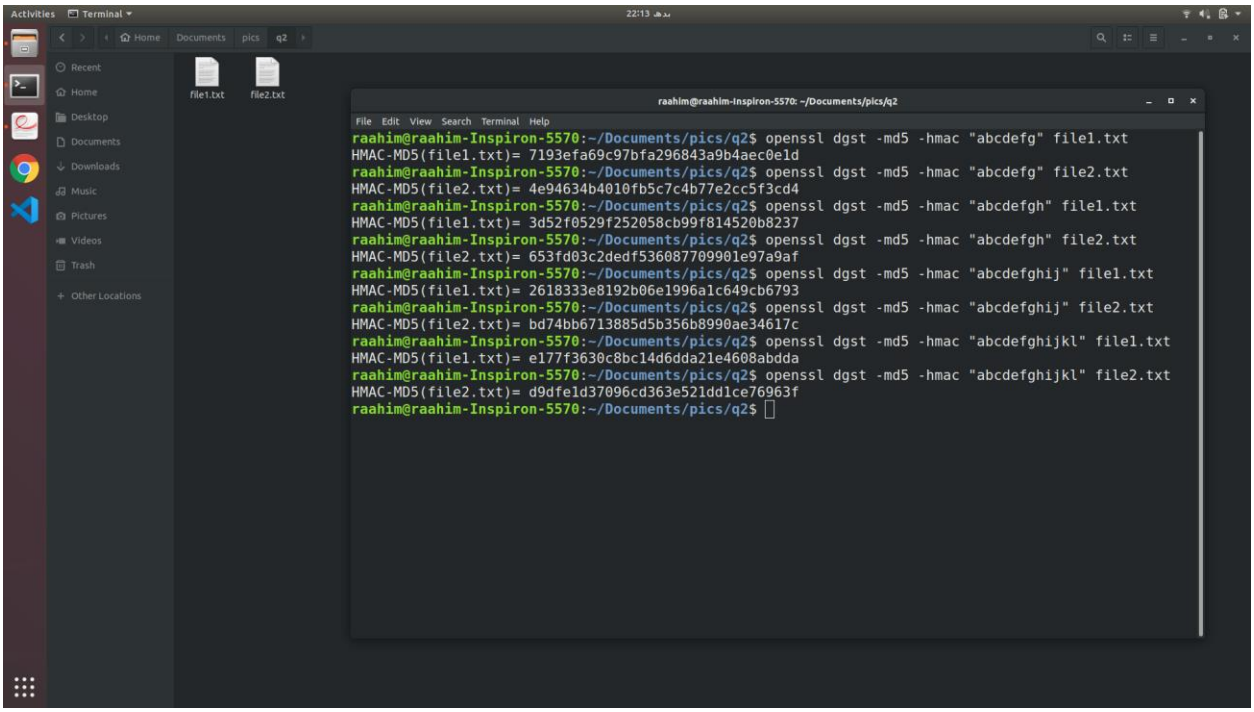
From the above screenshots it can be seen that:

- For md5, hash computed is of 128 bits.
- For sha1, hash computed is of 160 bits.
- For sha256, hash computed is of 256 bits.

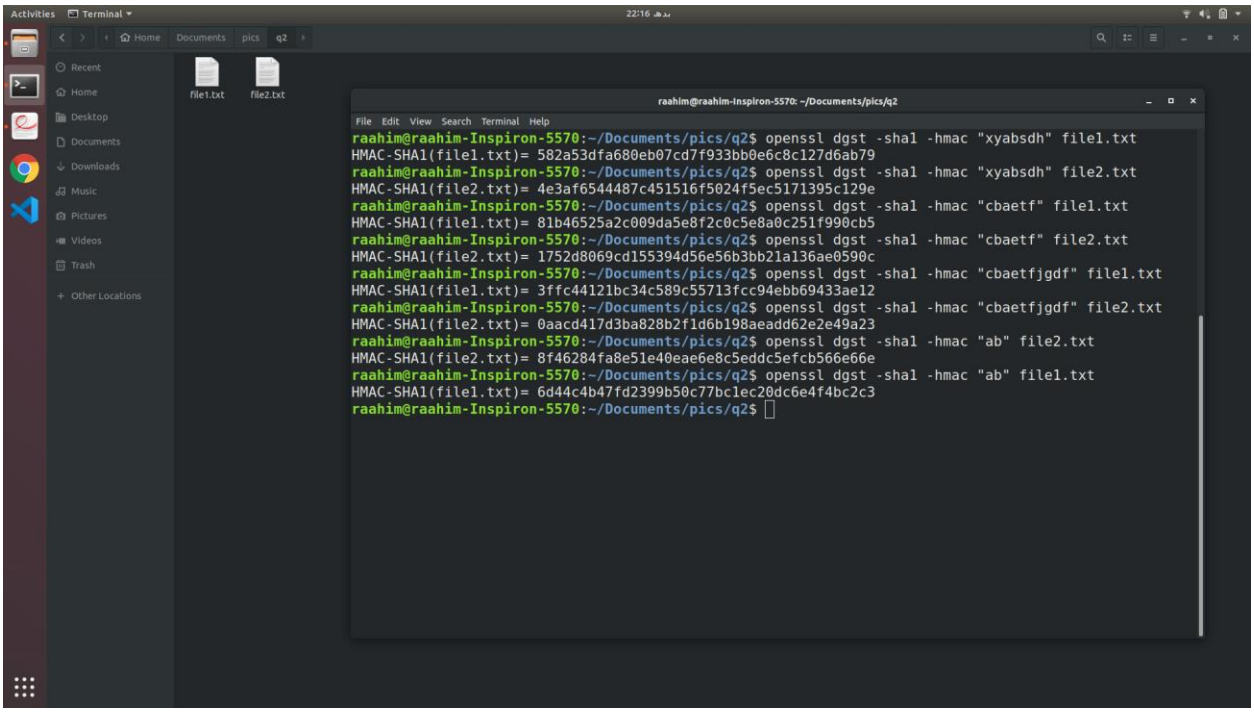
2) It can be seen from the screenshots above that digest size is not different for files of different lengths. Hashes were generated using files of different lengths. The resulting hashes were all of similar length (if same category of hash is used on files of different lengths).

➢ Task2:

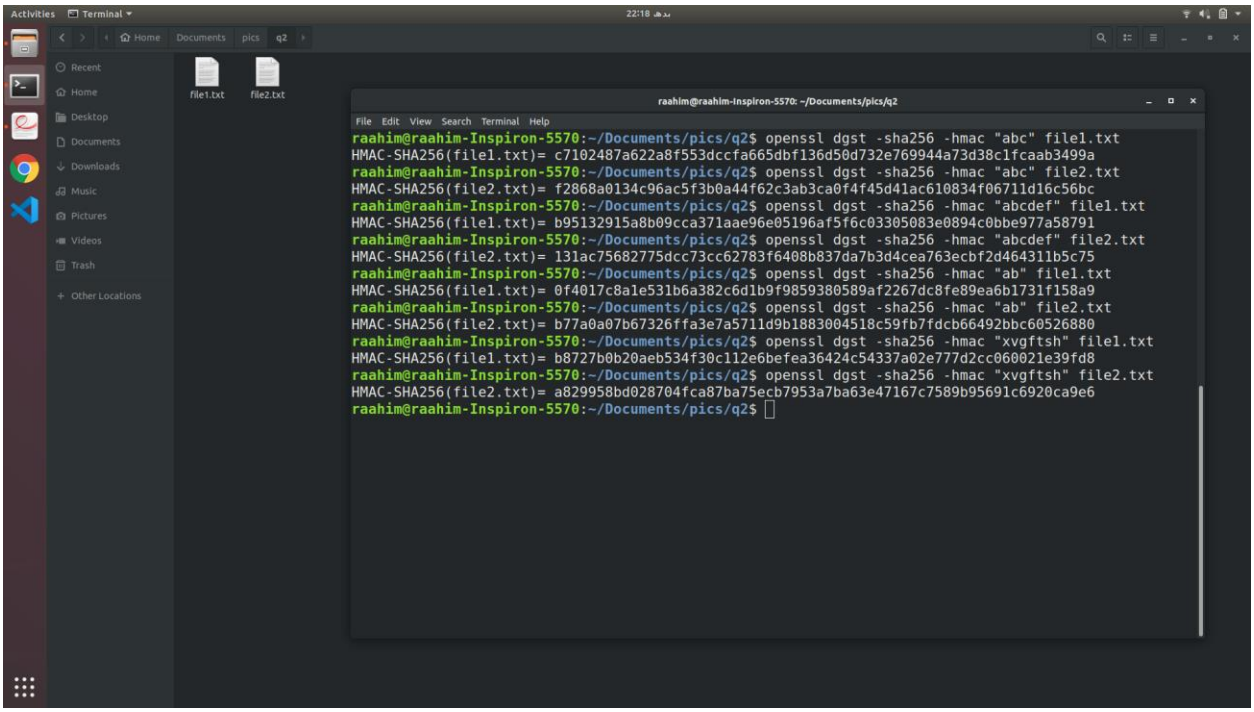
Keyed hash generated using HMAC-MD5:



Keyed hash generated using HMAC-SHA1:



Keyed hash generated using HMAC-SHA256:



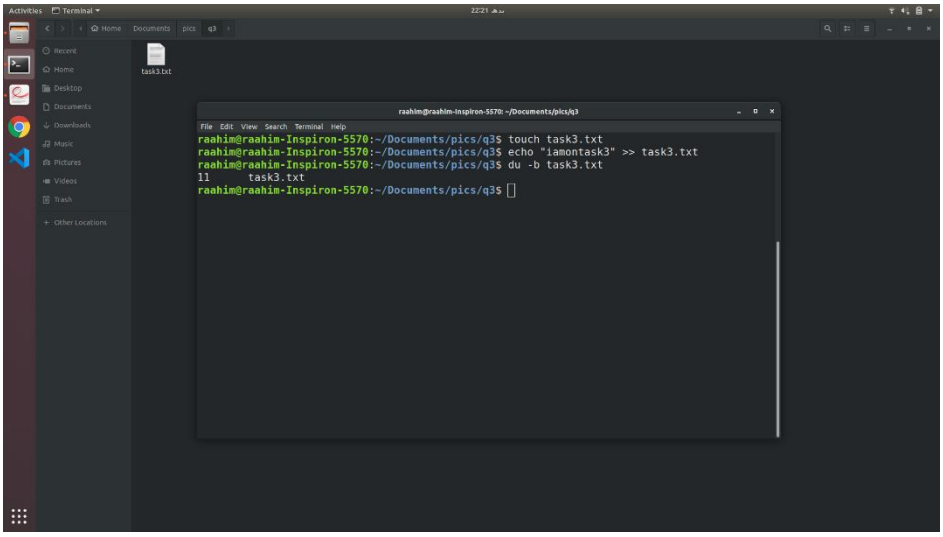
1) No, we do not have to use a key with a fixed size in HMAC.

2) We do not have to use a key with a fixed size in HMAC, hence, there is no fixed key size.

3) Reason is "no" because HMAC is a cryptographic hash function which map data of arbitrary size to a bit string of a fixed size (a hash). This is opposite to block ciphers which typically need a fixed length key. According to https://tools.ietf.org/html/rfc2104 "The key for HMAC can be of any length…".

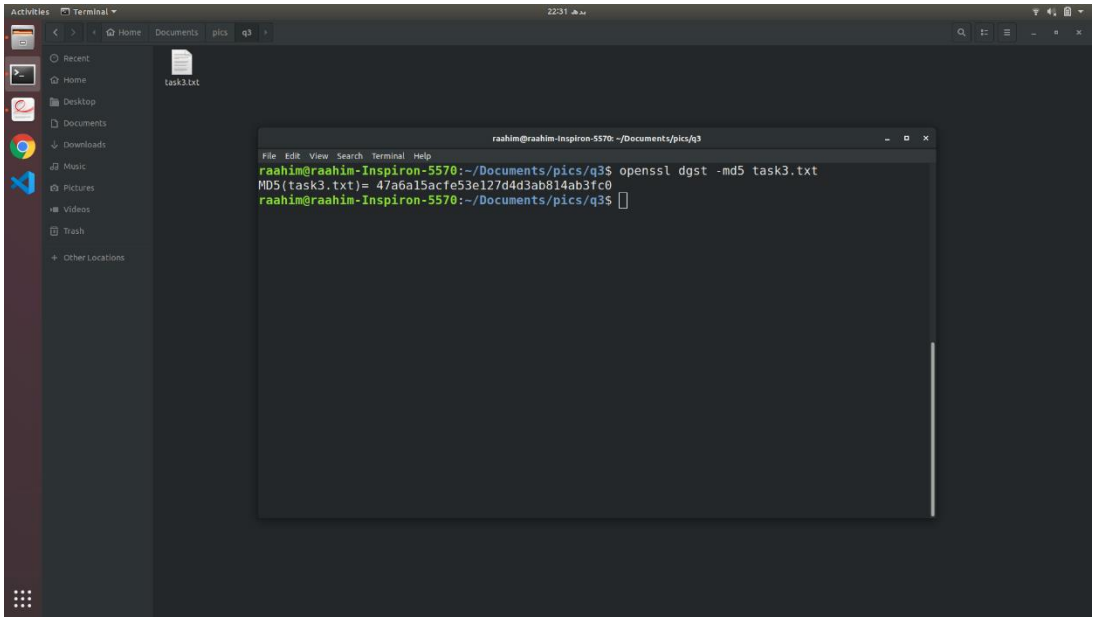
➢ Task3:

First, a text file of size 11 bytes was created (two times: first for MD5 and then for SHA256)

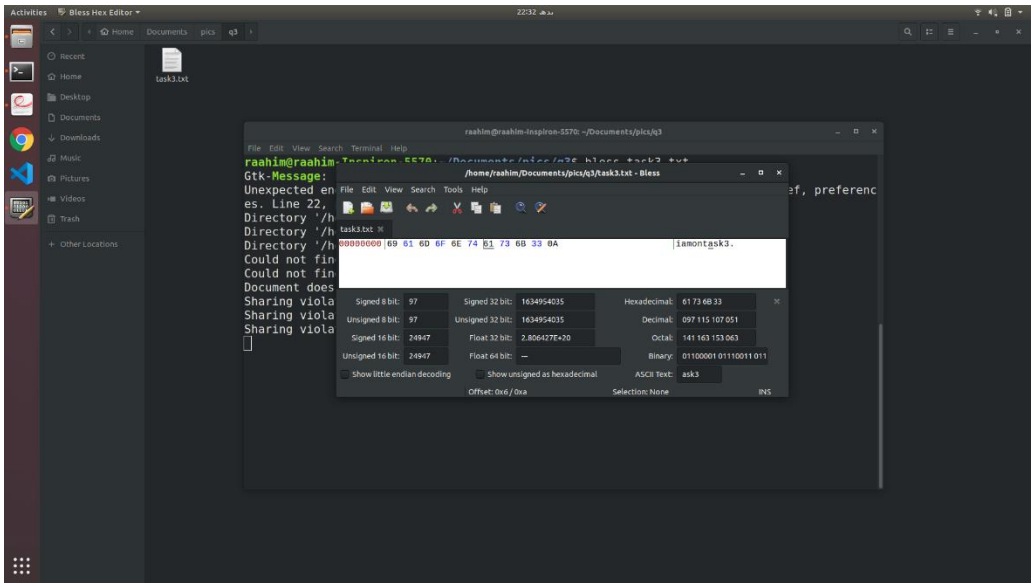


- For MD5:

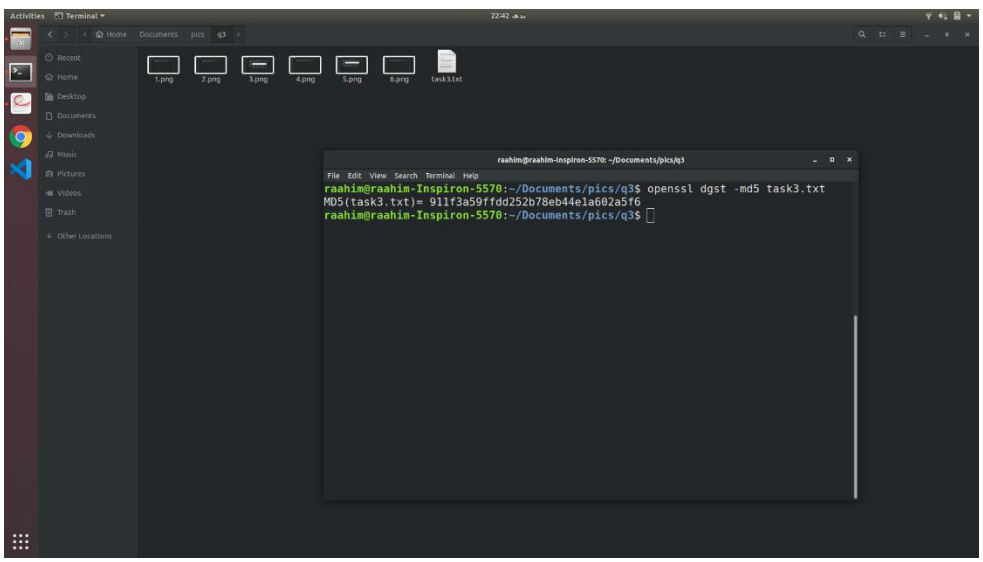
  H1 was as follows:



Using Bless, the underlined byte was changed from 61 to 67 i.e. 1 was changed to 7:

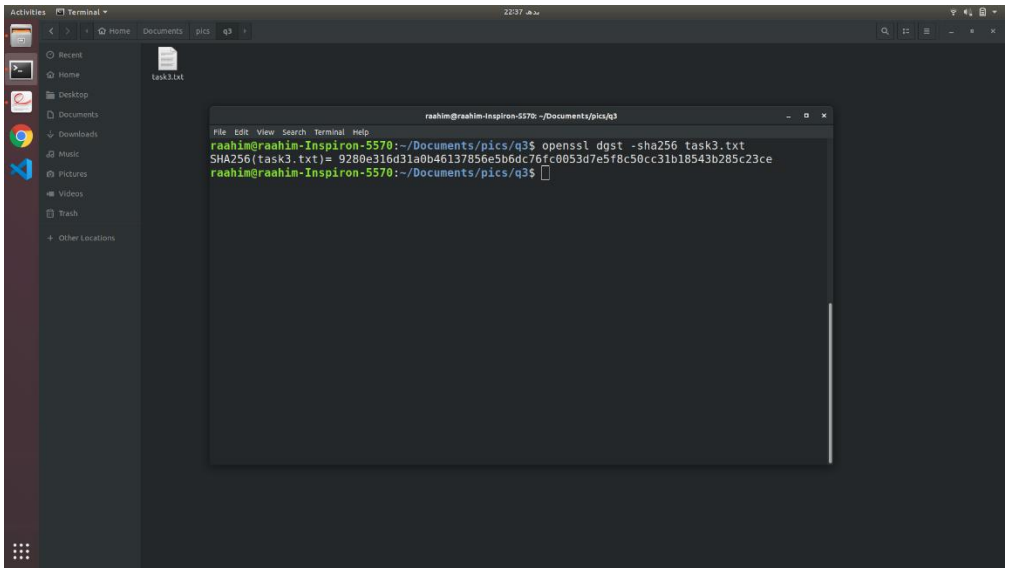


H2 was as follows:

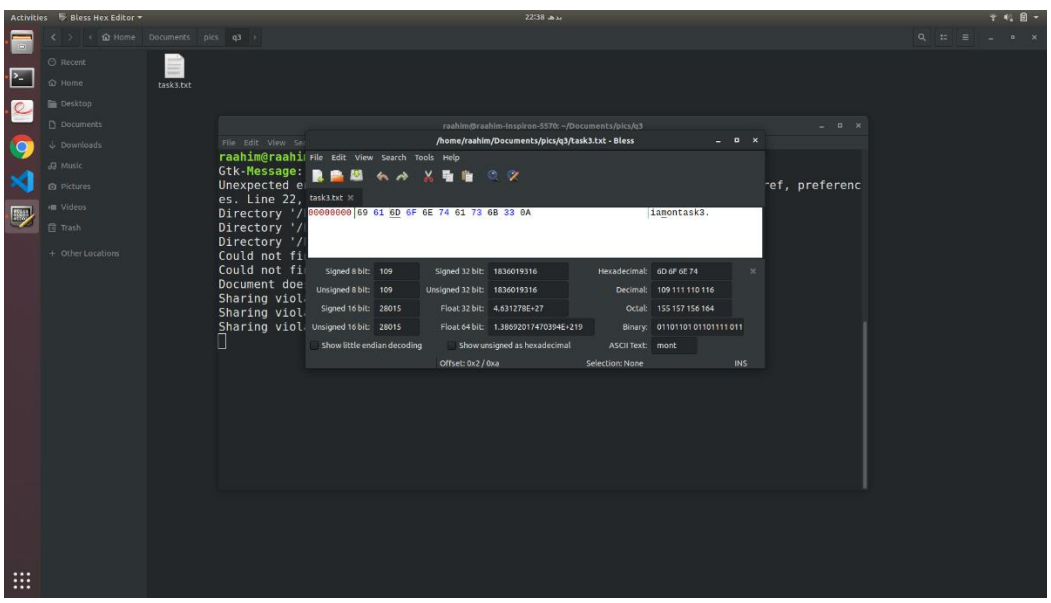


- For SHA256:

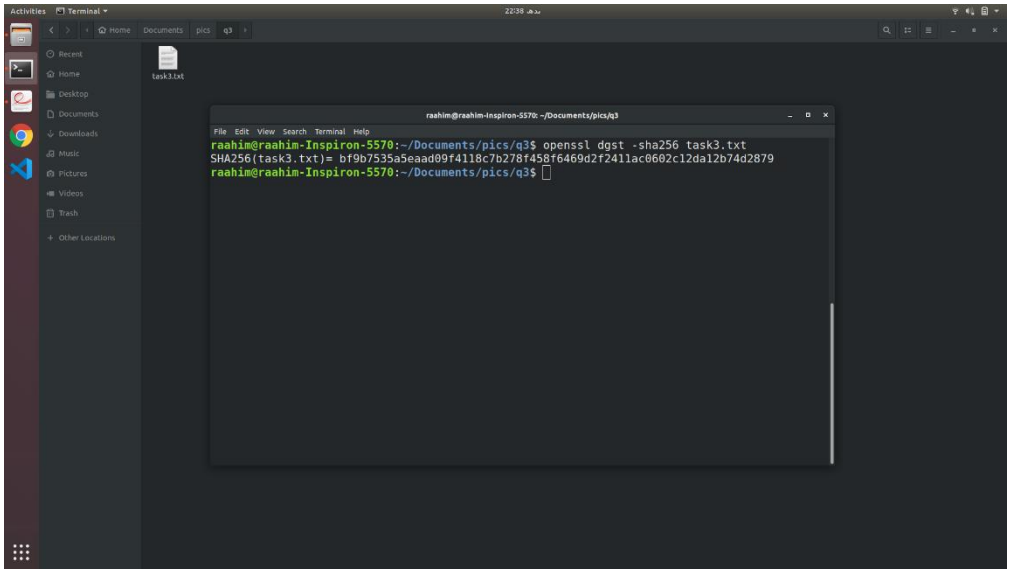
  H1 was as follows:



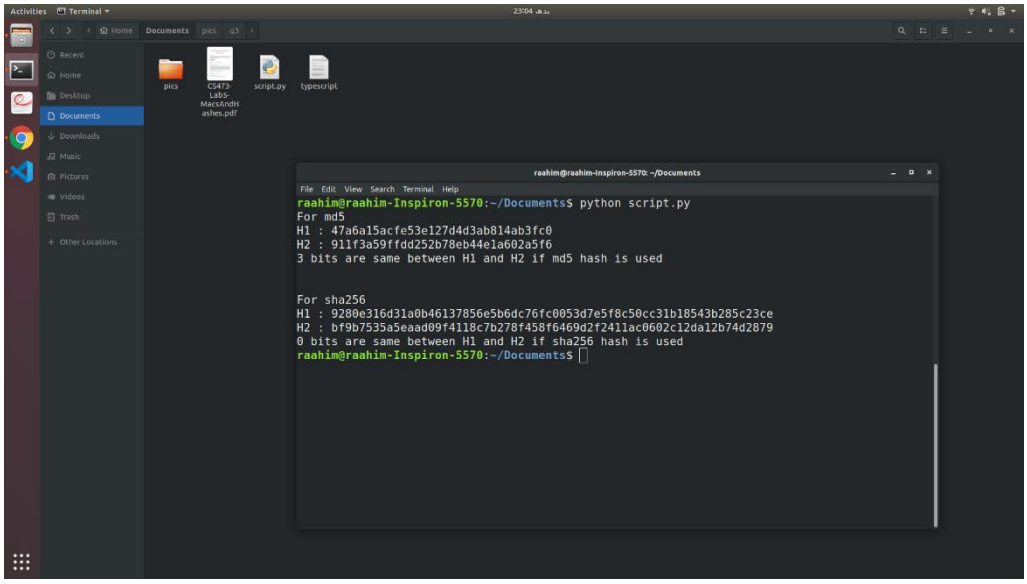
  Using Bless, the underlined byte was changed from 6D to 6A i.e. D was changed to A:



H2 was as follows:



I wrote a short script to count how many bits are the same between H1 and H2 and the results were as follows:



It can be seen that 3 bits are same between H1 and H2 using MD5 algorithm whereas using SHA256 algorithm, there is no same bit between H1 and H2.