VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

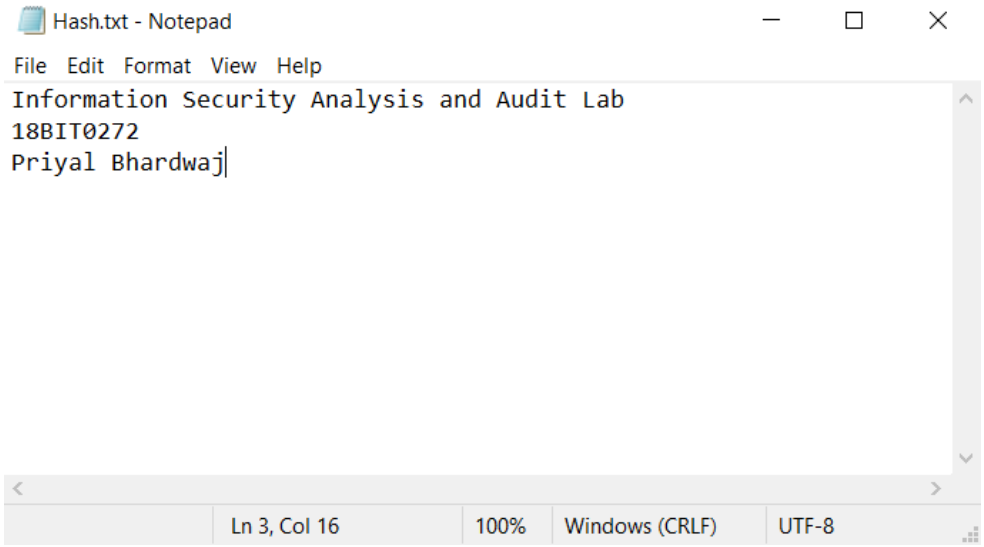
Lab Assessment-IV, AUGUST 2020

B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

Calculate Hash, Checksum, or HMAC to ensure the data Integrity of a file, before and after modification, using the HashCalc Tool.

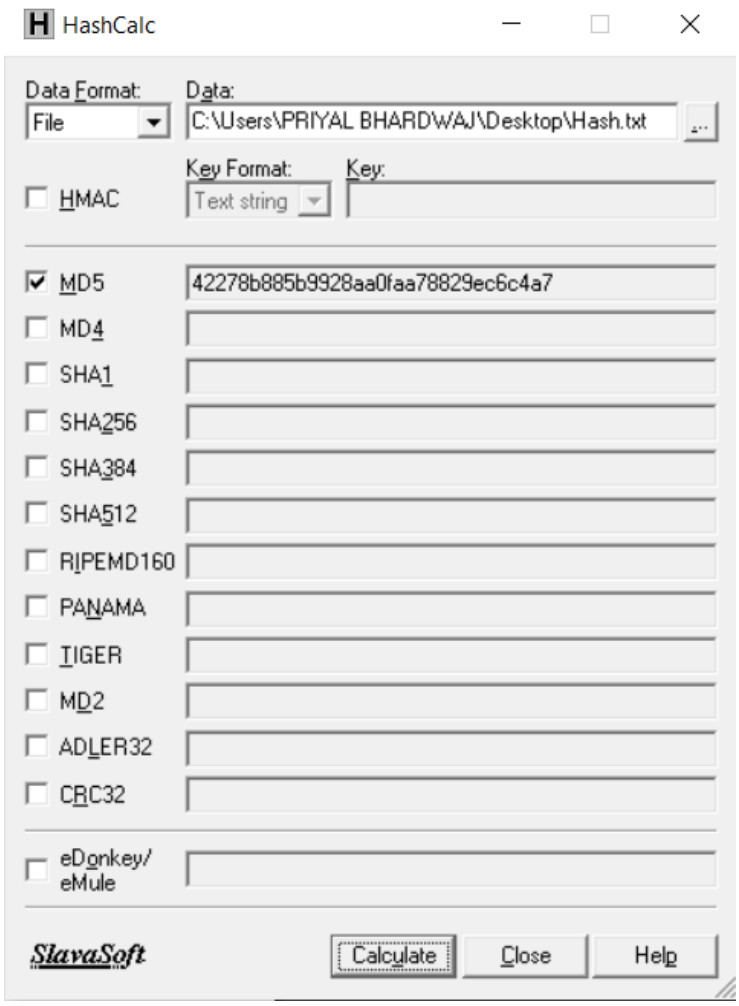
Step 1: Create a Text file



Step 2: Install HashCalc

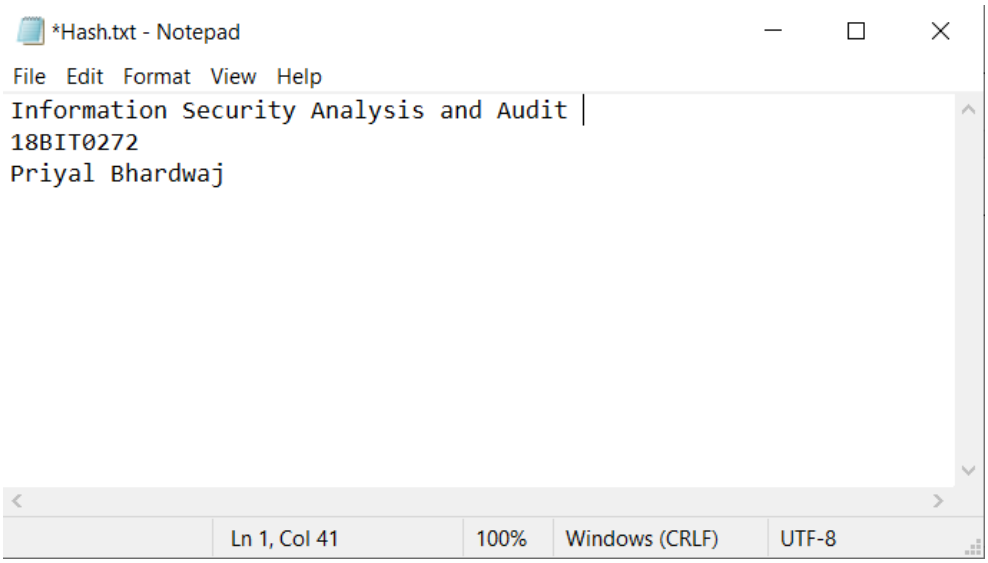
Step 3: Calculate a hash of the Hash.txt file

MD5 Value: 42278b885b9928aa0faa78829ec6c4a7



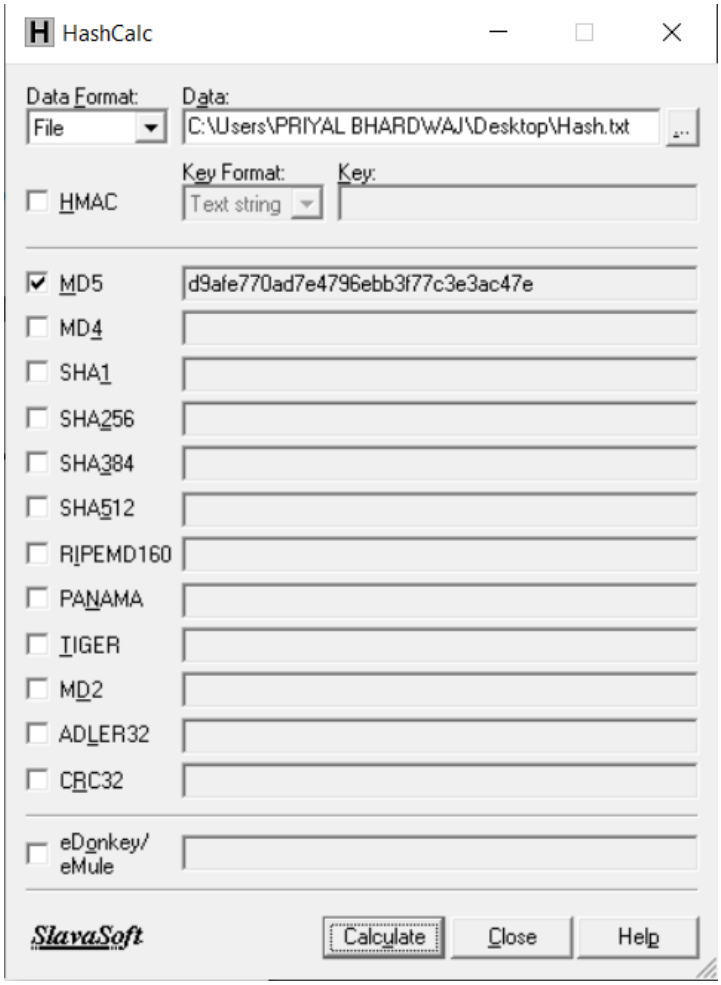
Step 4: Make a change to the Hash.txt file

Deleted “Lab” from the text.



Step 5: Calculate a new hash of the Hash.txt file

a. New MD5 Value: d9afe770ad7e4796ebb3f77c3e3ac47e
Yes, MD5 value in Step 3 and Step 5 is different because file content has changed because content of Hash.txt has changed now.

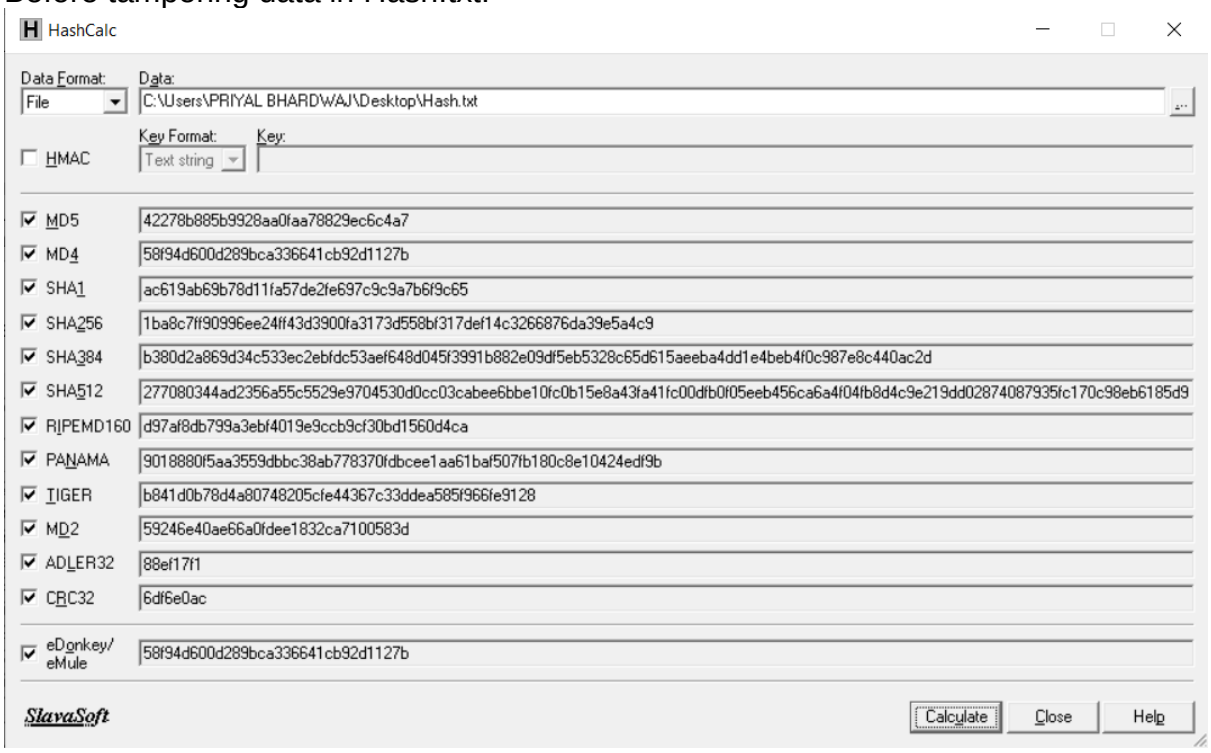


Calculating all hash types

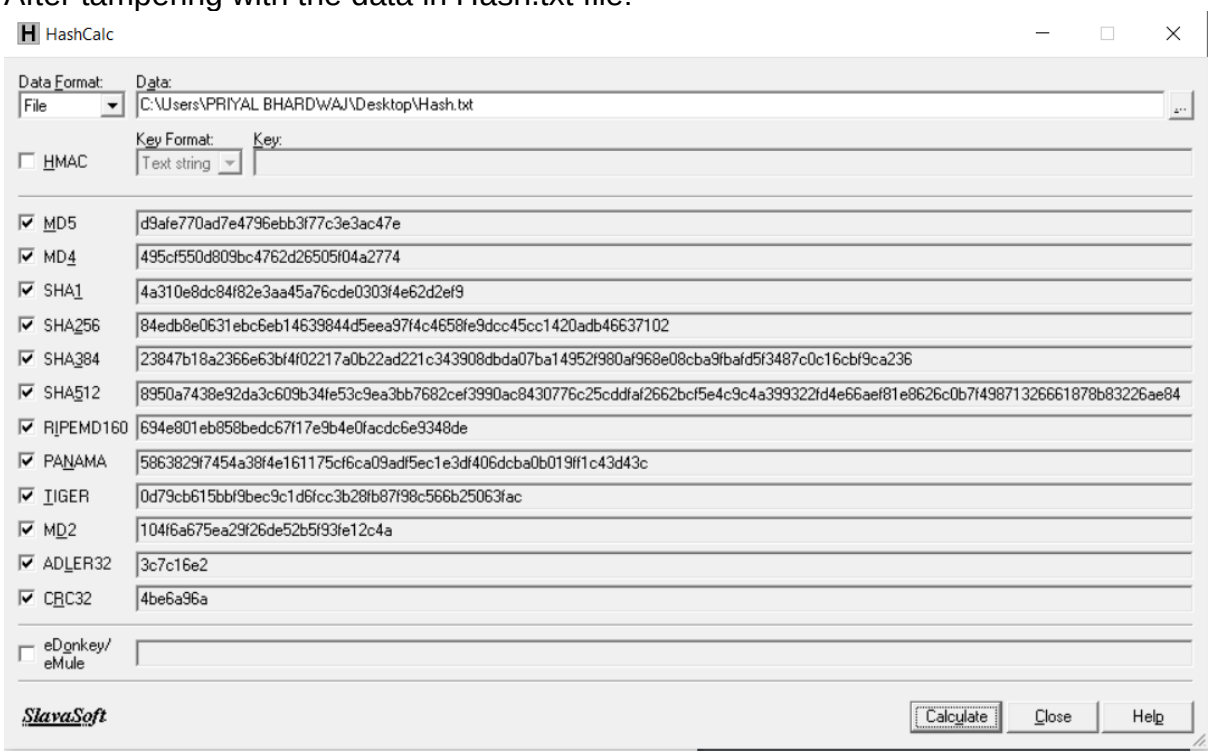
d. Many of the hash types create a hash of a different length because they have different algorithms for calculating the hash function. For example, MD5 generates 128 bit and SHA256 generates 256 bits.

It depends on key size as well but here we have unchecked HMAC so we do not need to provide key.

Before tampering data in Hash.txt:

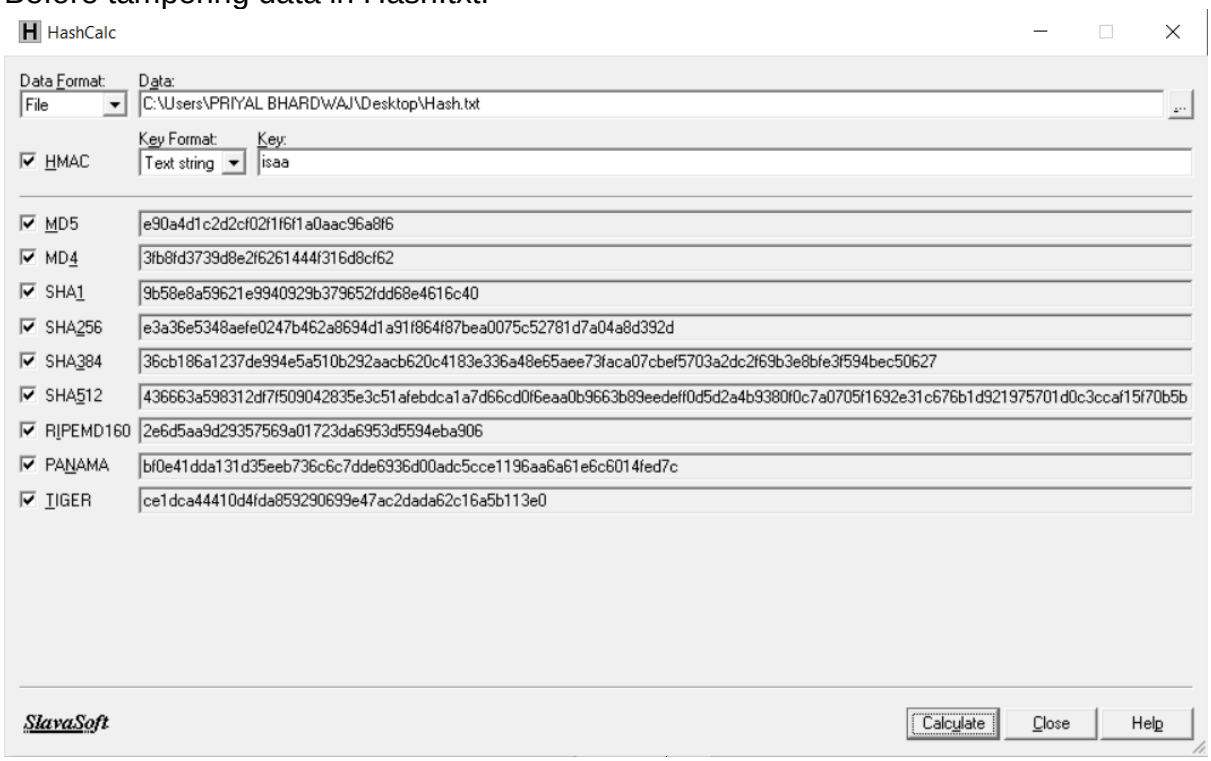


After tampering with the data in Hash.txt file:

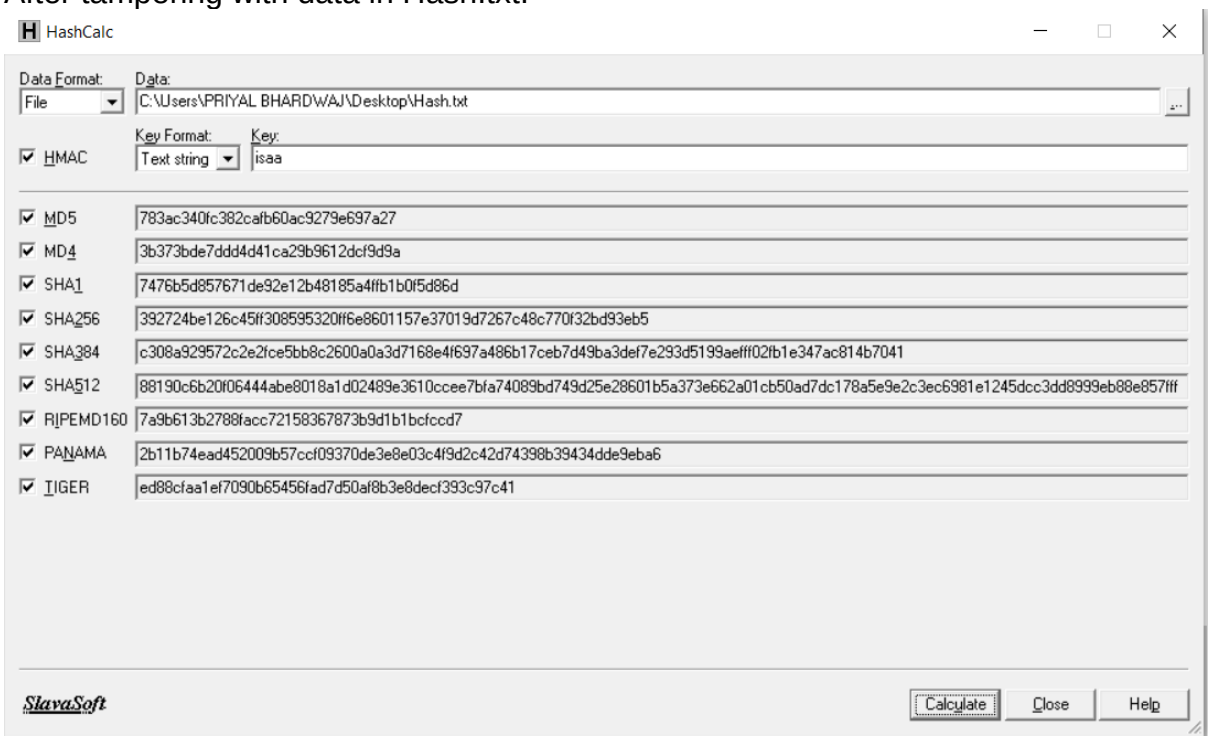


Now we have enabled ***HMAC*** and provided random text “isaa” as key and calculated hash values again. We can see the hash values are different from the ones obtained in above step without key.

Before tampering data in Hash.txt:



After tampering with data in Hash.txt:



****