Cryptography: Hash Functions and HashCalc Tool

Overview:

Hash functions generate a unique fixed-size bit string, known as a message digest, from any block of information. These functions condense data in a file, regardless of its size, into a fixed-length number, usually between 128 and 256 bits. If any bit in the input changes, approximately half of the output bits will change as well. Due to the computational difficulty, it is nearly impossible to find two different files with the same message digest.

HashCalc Tool:

HashCalc is a versatile tool that computes various hashes, checksums, and HMACs for files, text, and hex strings. It supports a wide range of hash algorithms, including:

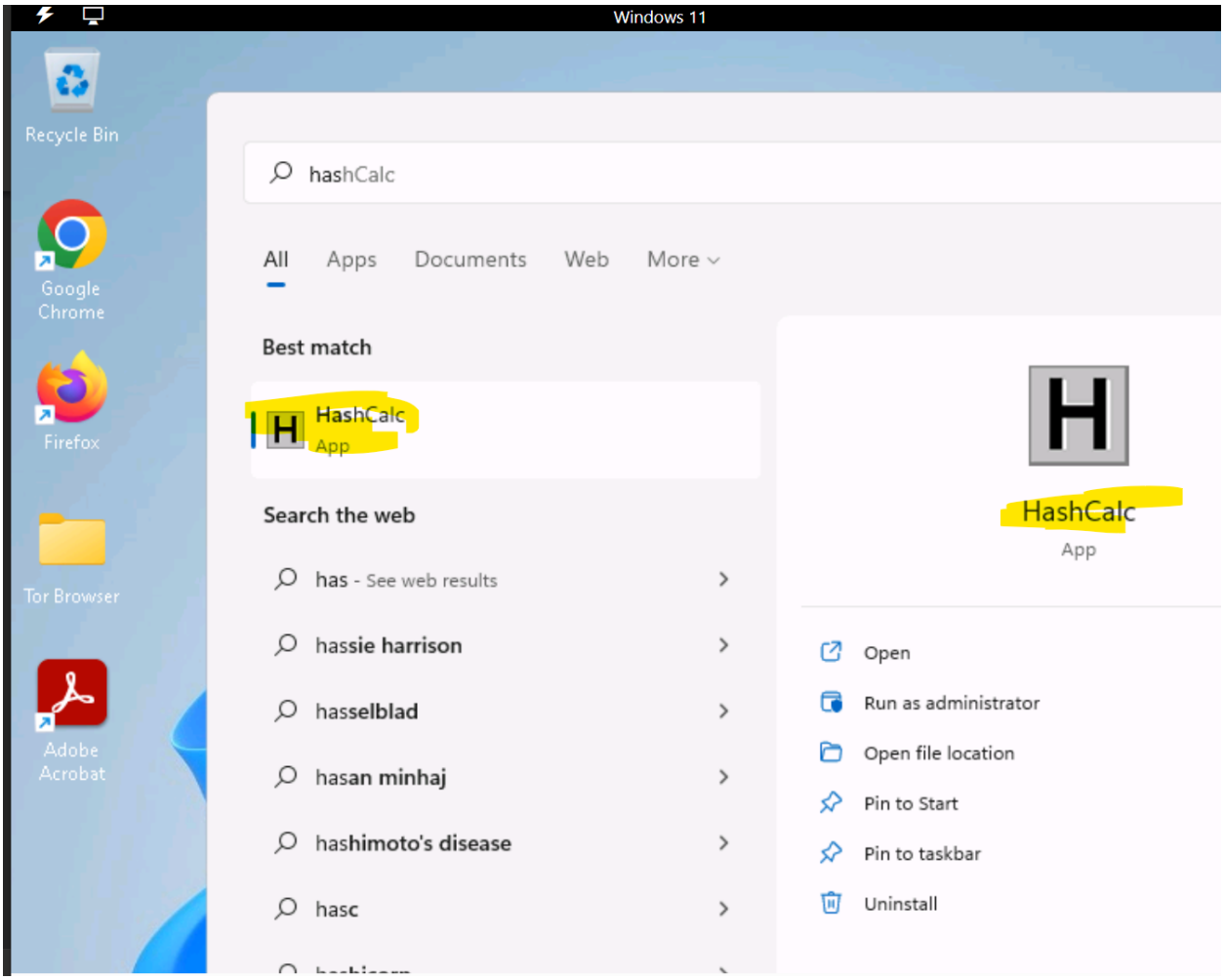
- MD2, MD4, MD5
- SHA1, SHA2 (SHA256, SHA384, SHA512)
- RIPEMD160, PANAMA, TIGER
- CRC32, ADLER32
- Hashes used in peer-to-peer applications like eDonkey and eMule

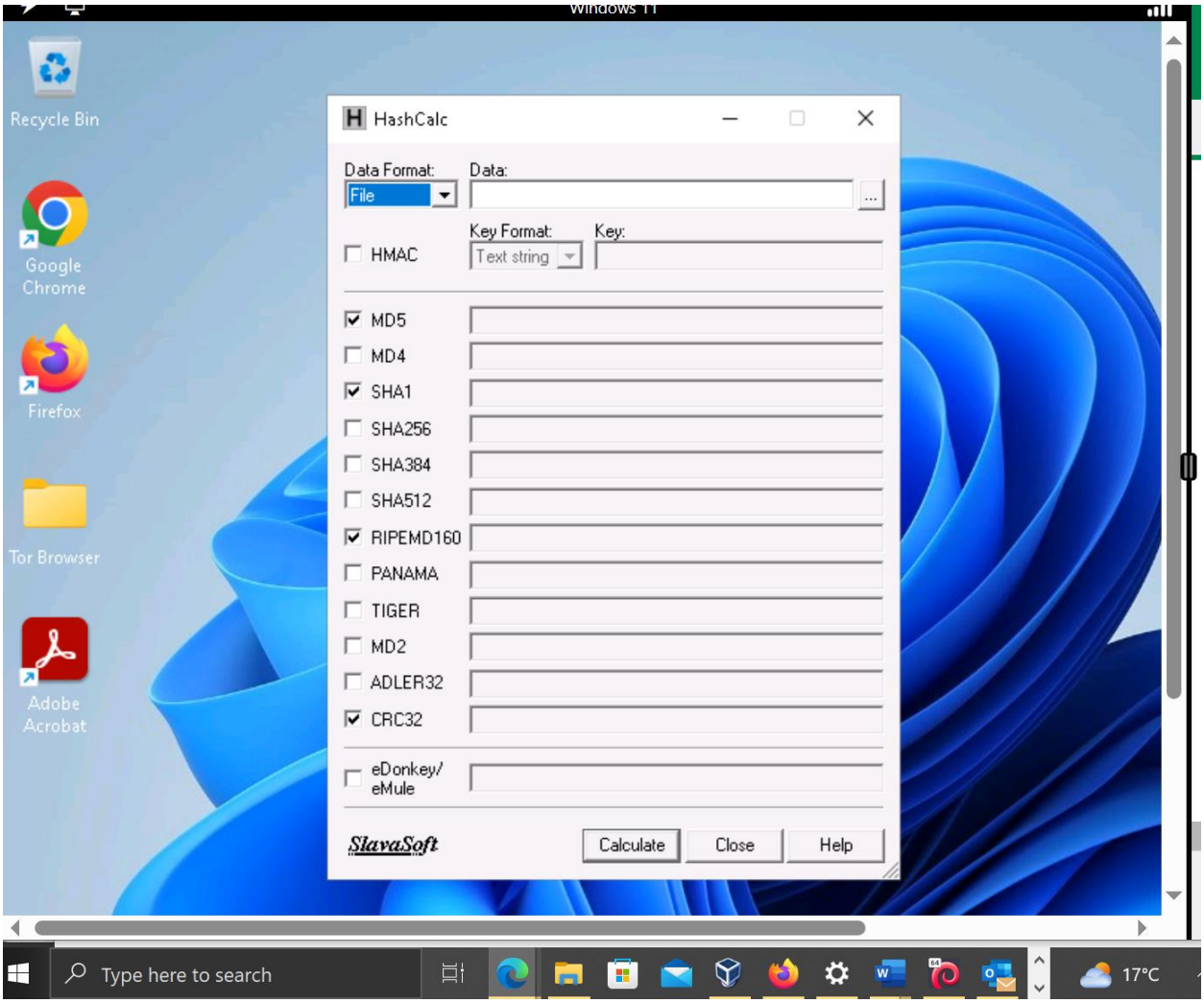
Project Objective:

Using a virtual machine (VM) provided by EC-Council with preinstalled tools, the objective of this project is to create a folder, use HashCalc to calculate one-way hashes, and verify the integrity of a file.

Steps:

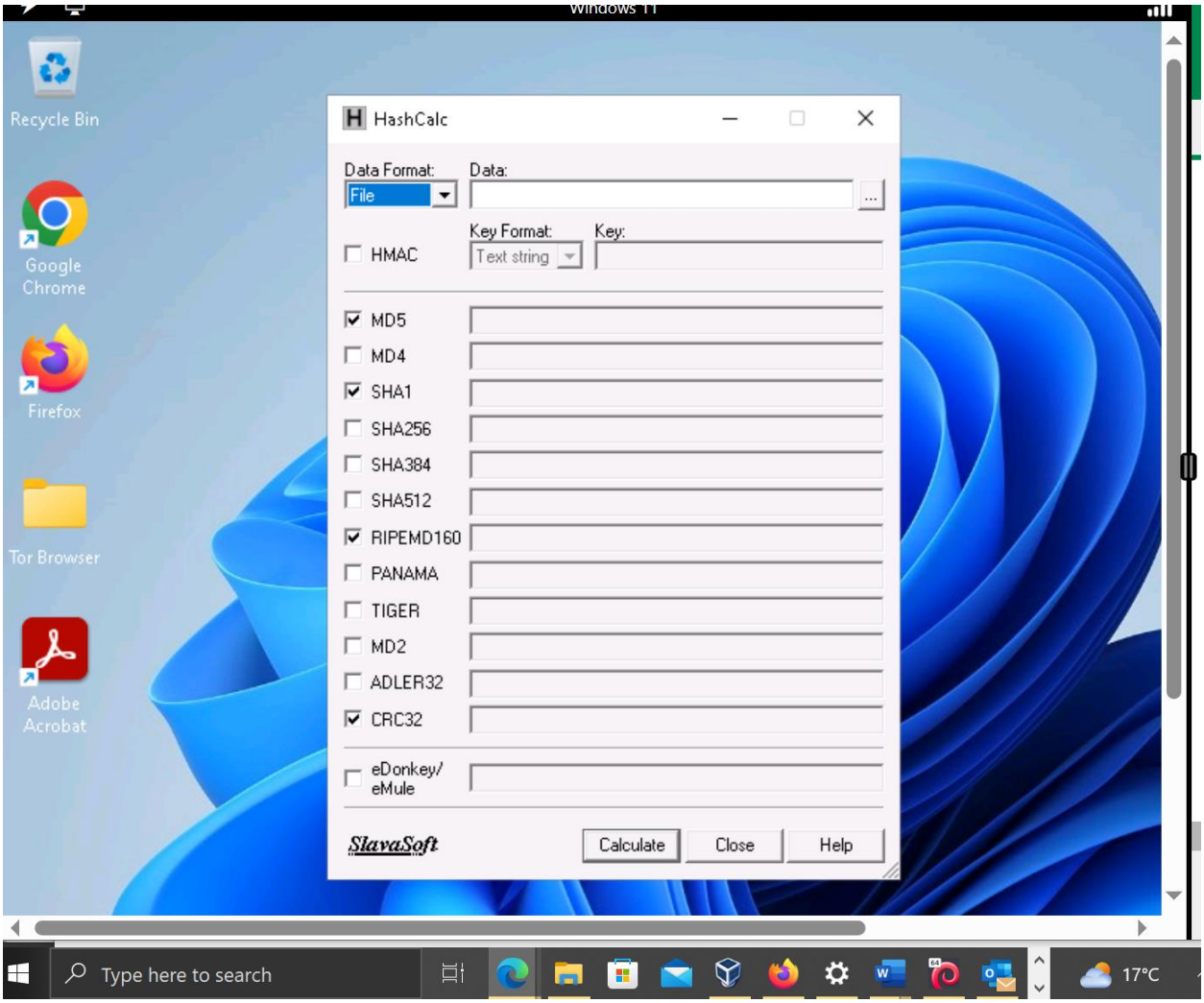
1. Launch HashCalc:
   - Open the ‘HashCalc’ application on the Windows 11 VM.


Windows 11
Recycle Bin
Google Chrome
Firefox
Tor Browser
Adobe Acrobat
hashCalc
All
Apps
Documents
Web
More
Best match
HashCalc
App
Search the web
has - See web results
hassie harrison
hasselblad
hasan minhaj
hashimoto's disease
hasc
HashCalc
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall



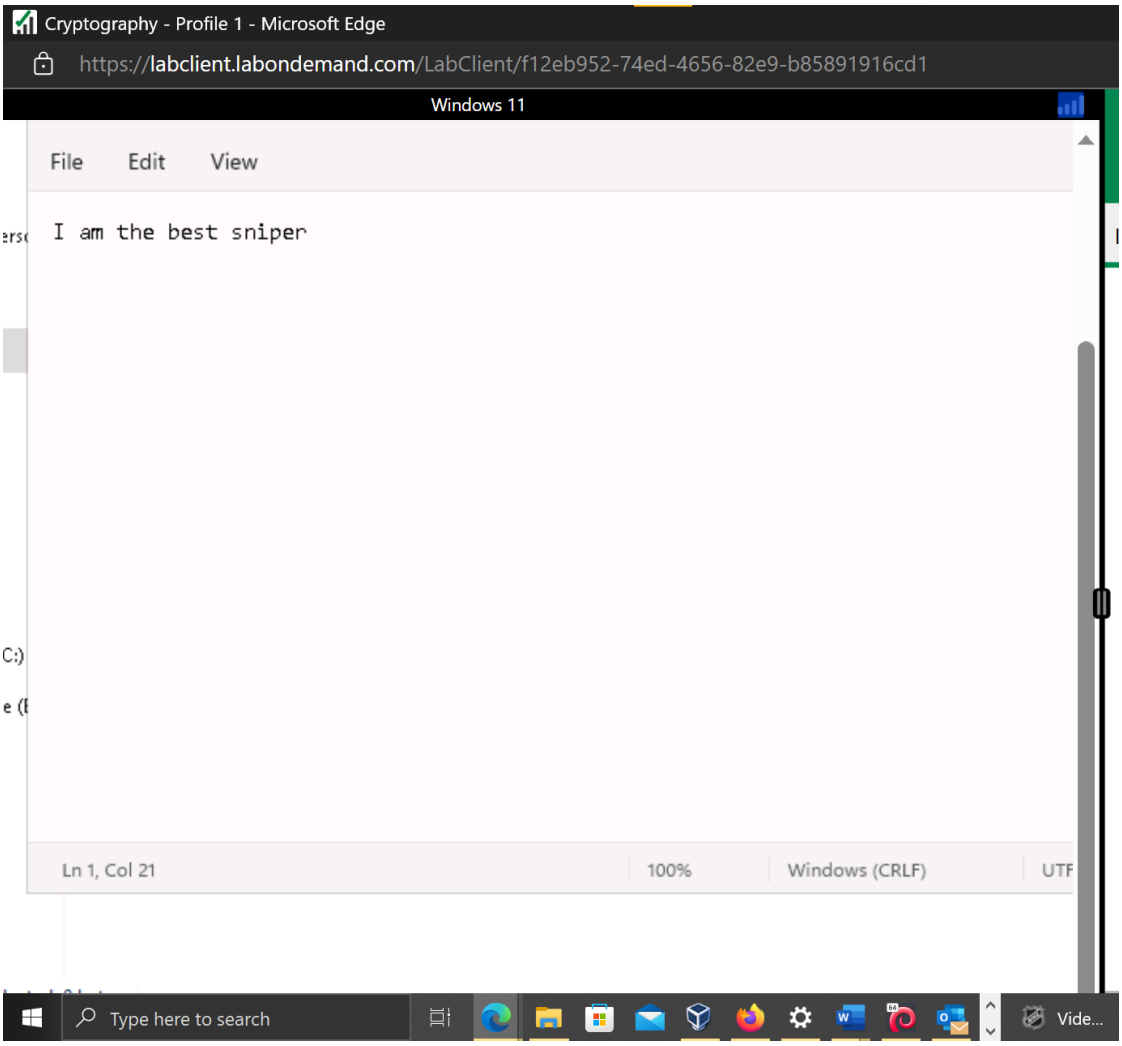
2. Created the File:

- Create a text document named ‘Izu_Encrypt.’


Windows 11
Recycle Bin
Google Chrome
Firefox
Tor Browser
Adobe Acrobat
HashCalc
Data Format:
File
Data:
HMAC
Key Format:
Text string
Key:
MD5
MD4
SHA1
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
Type here to search
17°C

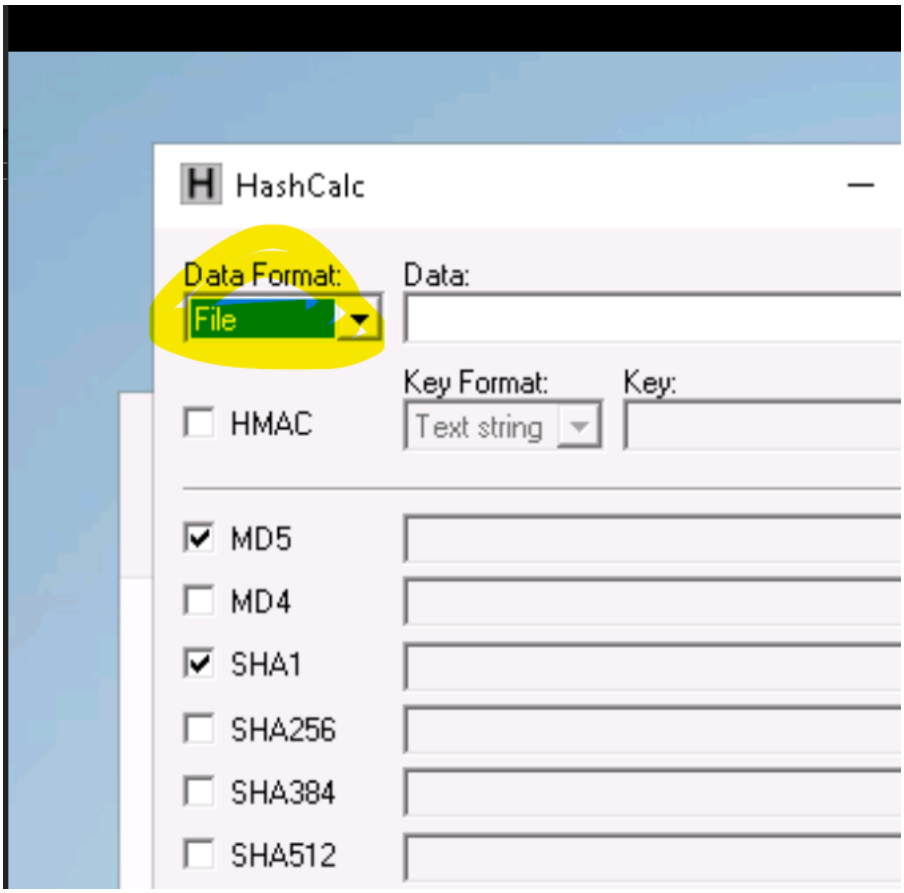
3. Write Random Text:

- Add random text to the document ‘Izu_Encrypt.’



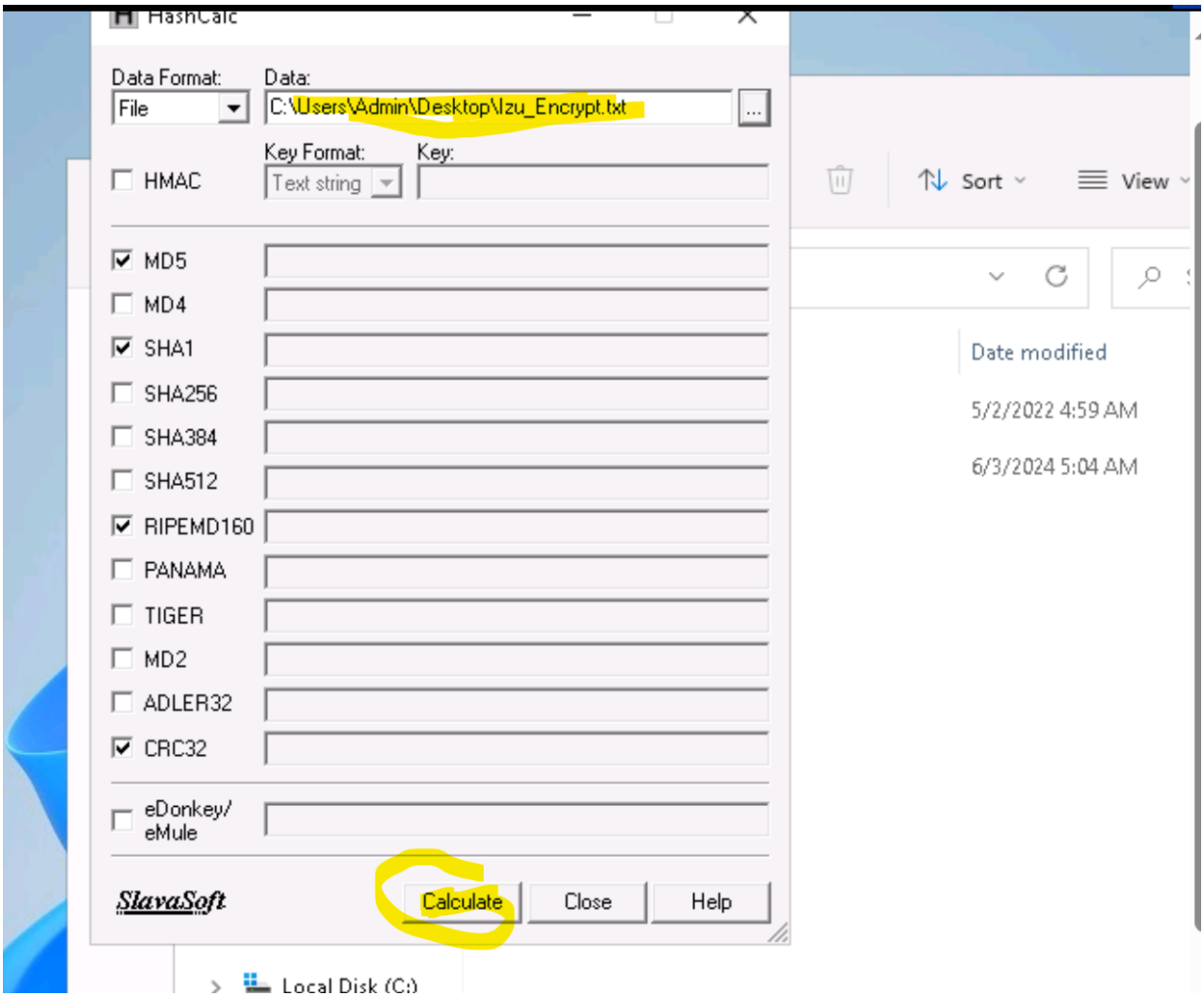
4. Select File Option:

- Since we are hashing a file, select the ‘File’ option in HashCalc.



5. Navigate to File Location:

Locate the ‘Izu_Encrypt’ file and open it. Select the hash functions MD5, SHA1, RIPEMD160, and CRC32.


HashCalc
Data Format:
File
Data:
C:\Users\Admin\Desktop\Izu_Encrypt.txt
...
HMAC
Key Format:
Text string
Key:
MD5
MD4
SHA1
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help
Sort
View
Date modified
5/2/2022 4:59 AM
6/3/2024 5:04 AM
Local Disk (C:)

6. Calculate Hash Values:

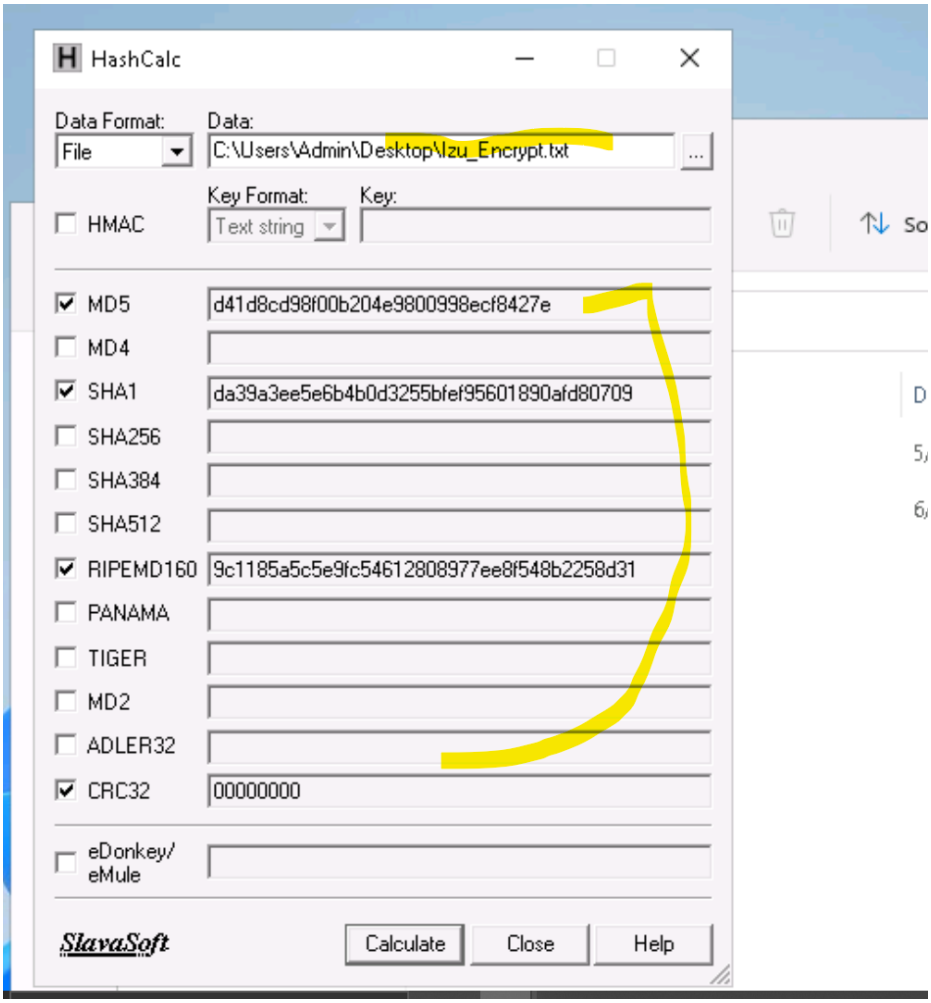
- The calculated hash values of the file will be displayed. Each hash algorithm differs in bit size:

- MD5: 128 bits

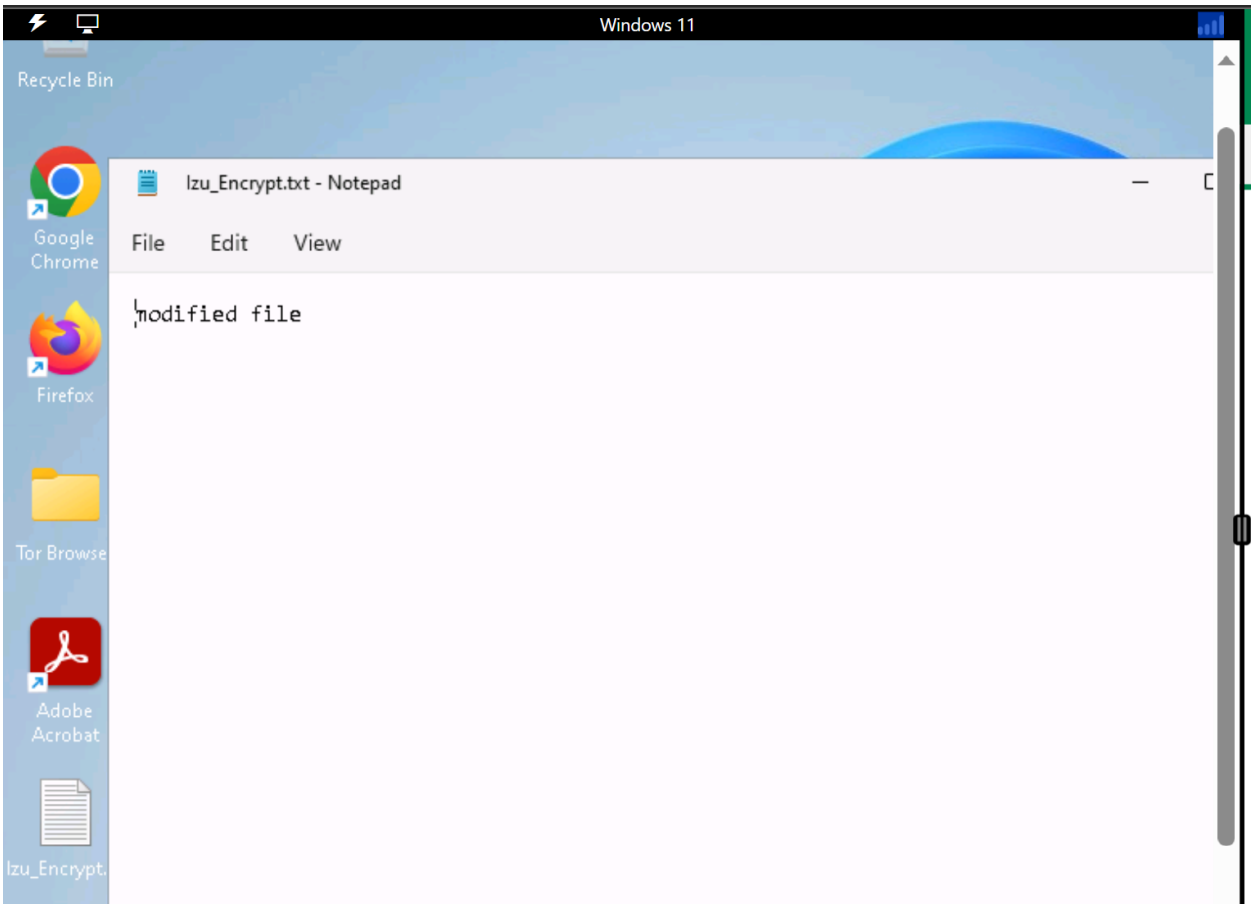
- SHA1: 160 bits

- RIPEMD160: 160 bits

- CRC32: 32 bits



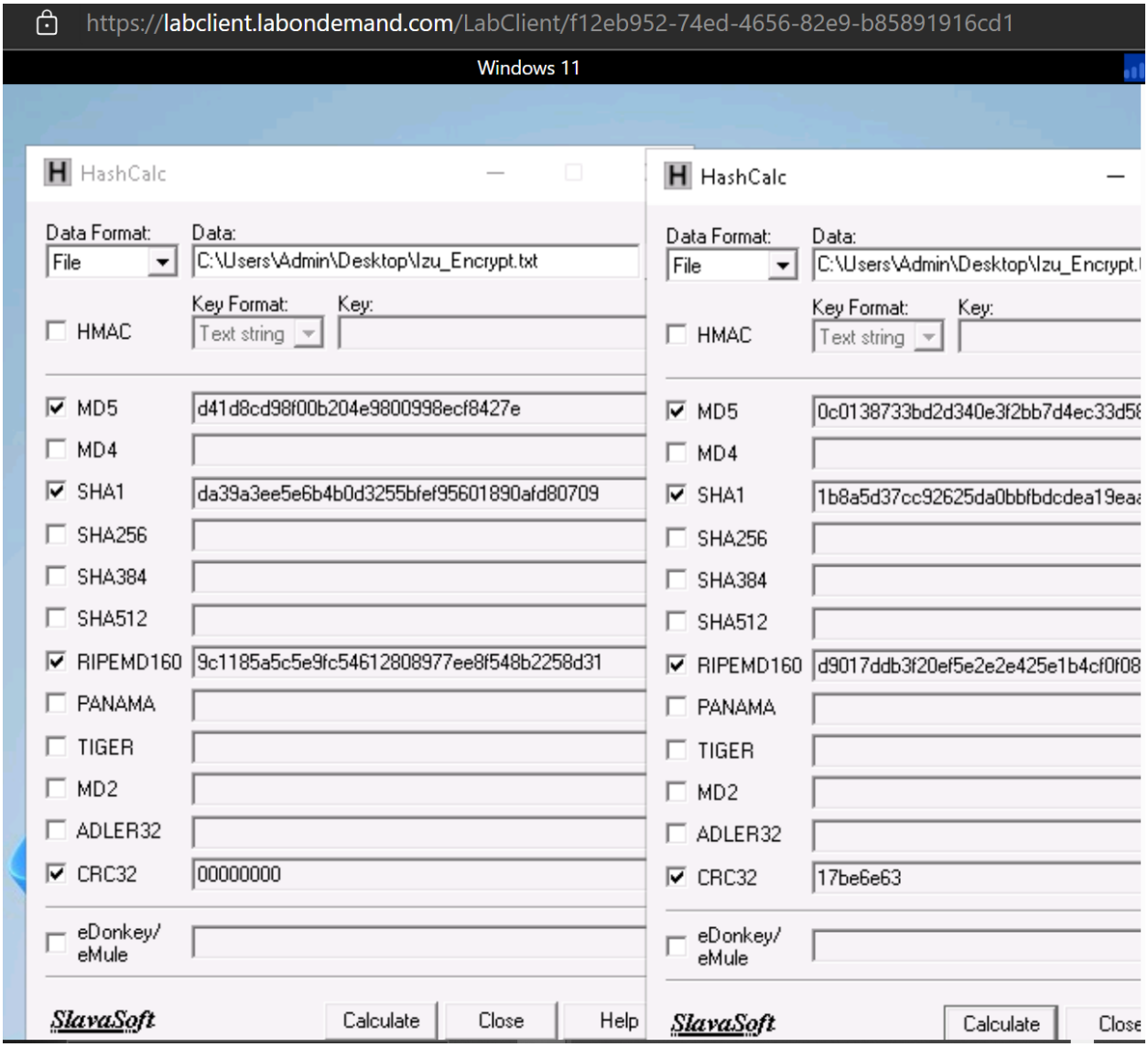
7. Modify the Original File:



- To verify the original calculated hash value, modify the content of the 'Izu_Encrypt' file and save it.

8. Calculate New Hash(Repeat step 5 & 6):

- Calculate a new hash for the modified file and compare it with the original calculated hash. The generated hashes will differ, demonstrating a simple way of verifying file integrity to ensure it has not been modified.



Conclusion:

This project illustrates how to use HashCalc to calculate and verify hash values, ensuring the integrity and authenticity of files by detecting any modifications.