ELITE TECH INTERN INTERNSHIP DOCUMENTATION

TASK1: FILE INTEGRITY CHACKER.

- INTEGRITY: It is the part of CIA TRAID which is designed to guide the policies for information security within the organization. Ensuring data is not modified either in transit or at storage. This can be achieved my using Hashing
- Hashing is the transformation of string of characters into fixed length of value or key that represents the original string

Examples: ABCDEFG 2ECDDE398067540867136D is the hash value of the string

- Hashing is one way it is not possibly get data back from the Hash value.
- Hashing is used to ensure the integrity of the data.
- There are many ways to calculate the Hash value
- MD5 HASH: 32 BIT HEXADECIMMAL CHARACTERS STRING
- SHA1 HASH: 40 BIT HEXADECIMAL CHARACTERS STRING
- SHA 256 HASH: 64BIT HEXADECIMAL CHARACTERS STRING
- SHA 512 HASH: 128 HEXADECIMAL CHARACTERS STRING

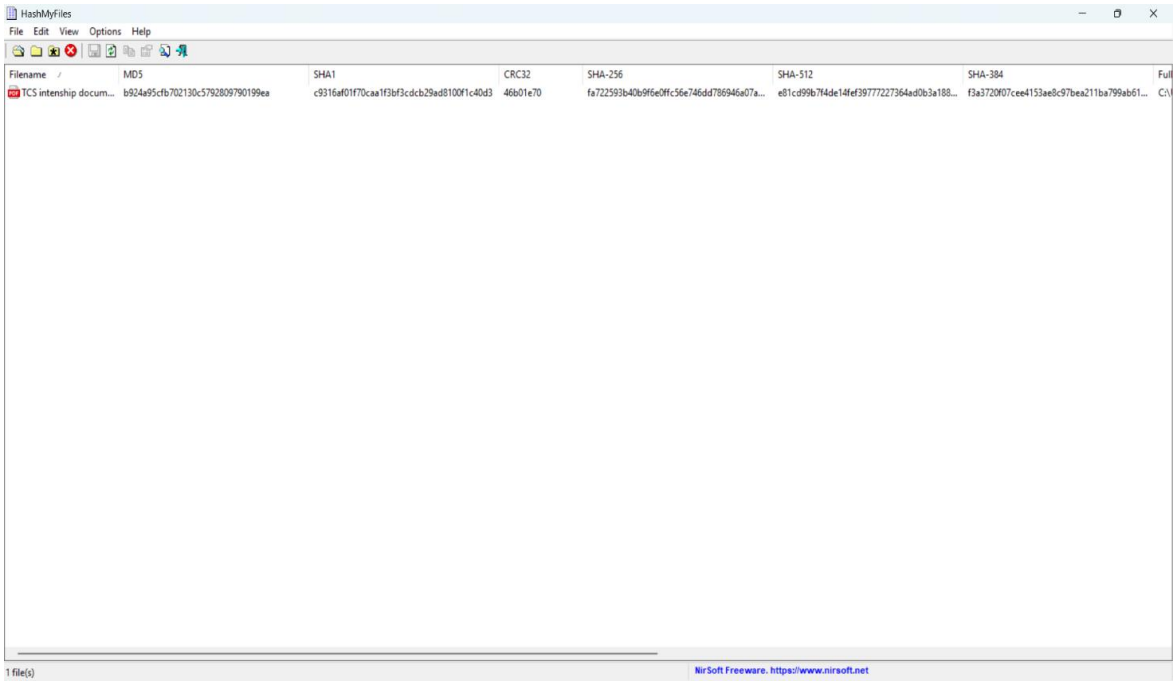
TOOLS USED TO CHECK THE INTEGRITY OF THE FILE

1. HASH MY FILES
2. HASH CAL
3. VIRUS TOTAL
4. HASH TOOL
5. HASH PAD USED BY MICROSOFT
6. FTKIMAGER/AUTOSPY These two are the forensic tools used for examining Digital evidence and they can also generate and compare hashes of file system images.

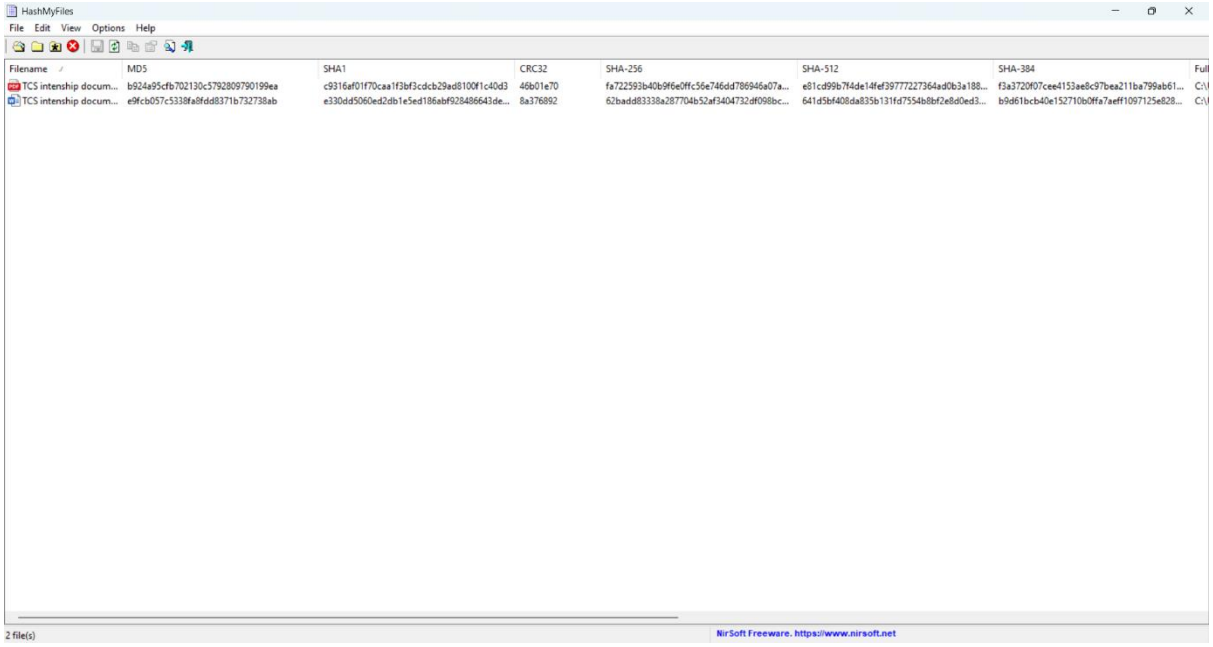
   Hash value of two files will not be the same.
   Hash value of the file changes even if we add a small space or comma, or string or a line
   Hash value will be different for same file with different file extension i.e., DOC, PDF.

   If two different files having the same hash value then the file is corrupted
   Or these can also occur because of the collision which means two files used SHA1 hashing algorithm.
   It is always recommended to use updated hash algorithms always it is recommended to use SHA 512 Hashing.

   I am attaching some of the practical observations of file hashes in different algorithms using hash my files and virus total

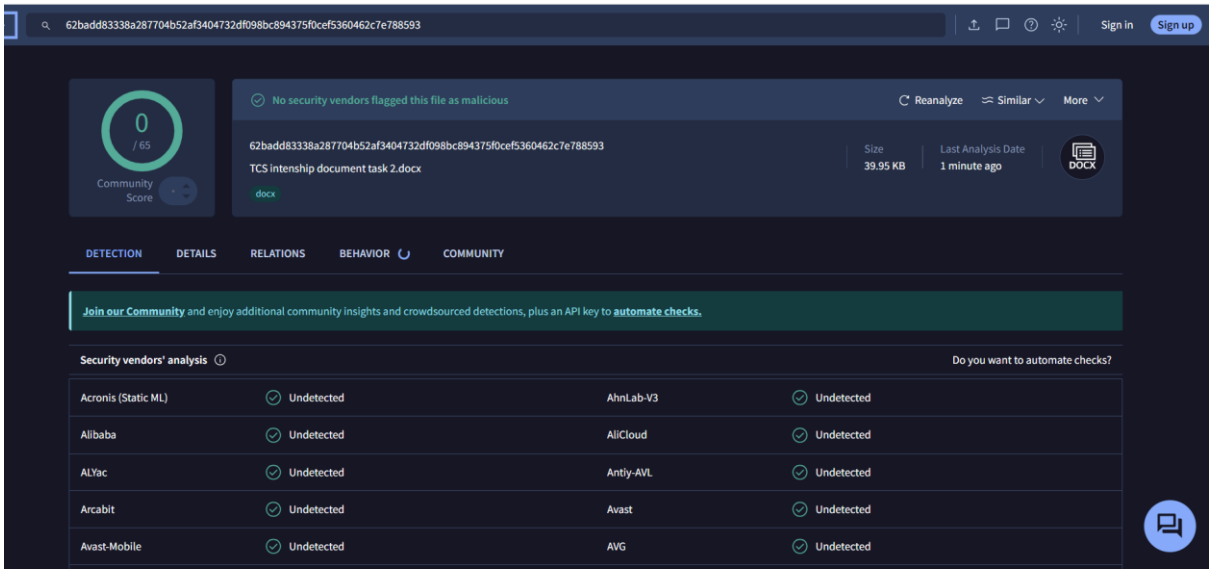


MD5, SHA1, CRC32, SHA256, SHA512, SHA384 OF A FILE WITH THE EXTENSION OF .PDF

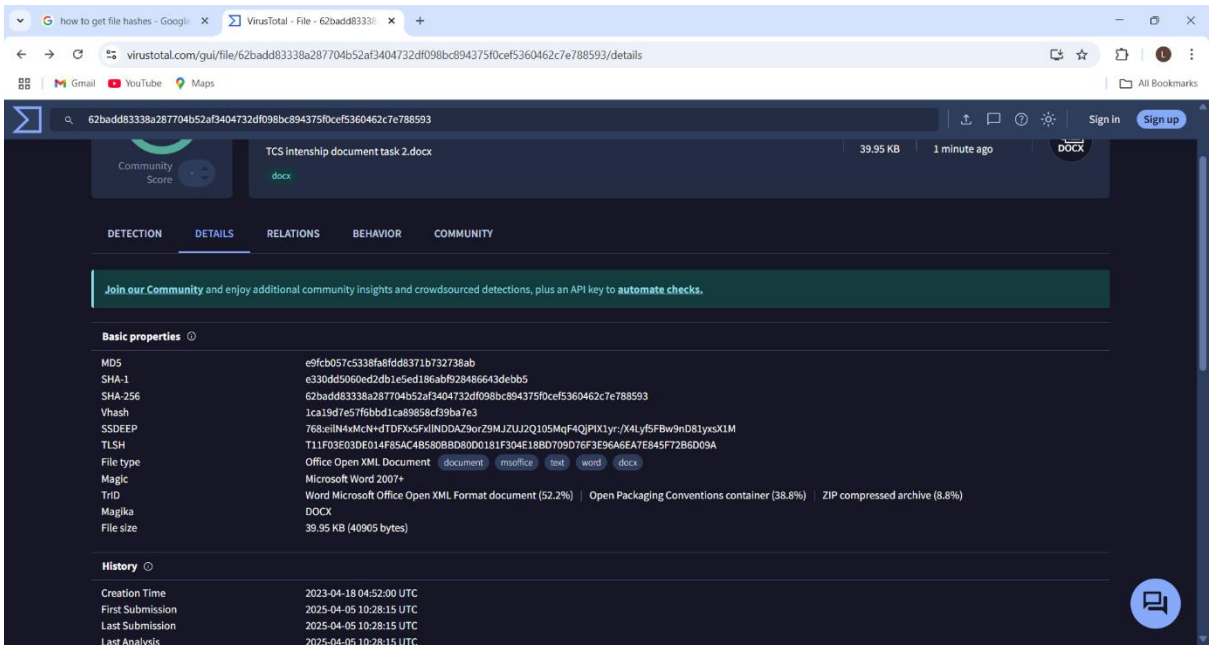


MD5, SHA1, CRC32, SHA256, SHA512, SHA384 OF A FILE WITH THE EXTENSION OF .PDF AND .DOC

Hash values of the files using virus total tool with different extensions.



Hash value of the file with the extension .docx



Details of the file along with hash values with the extension.docx

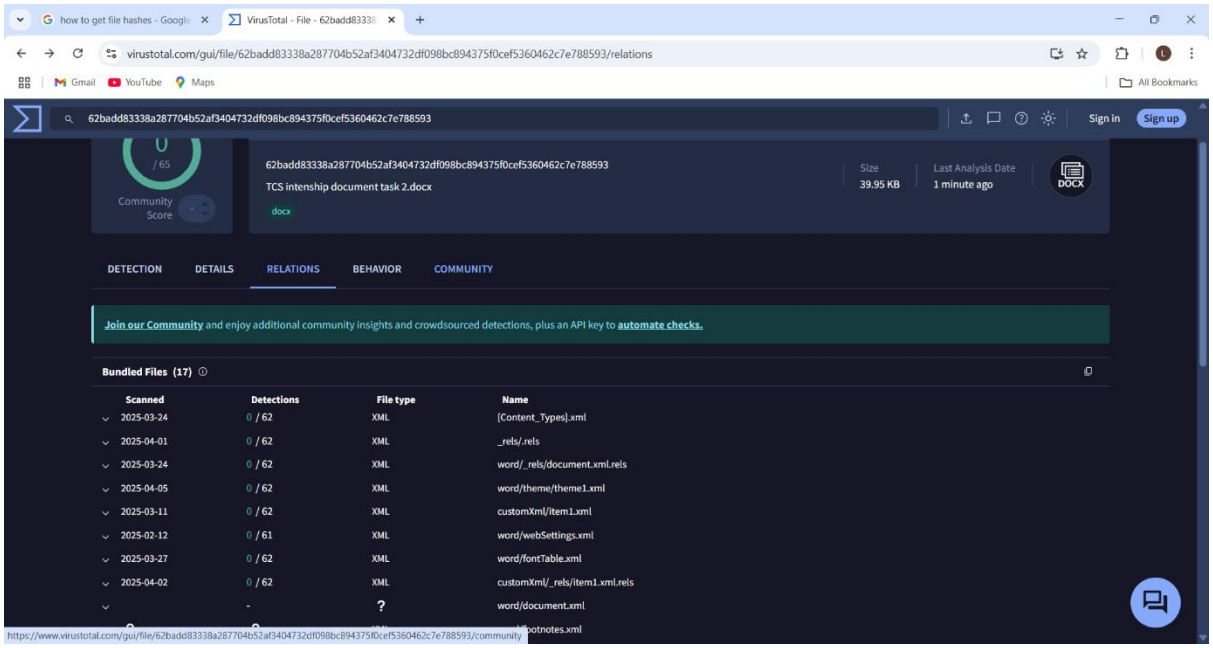


Image showing relations of the file

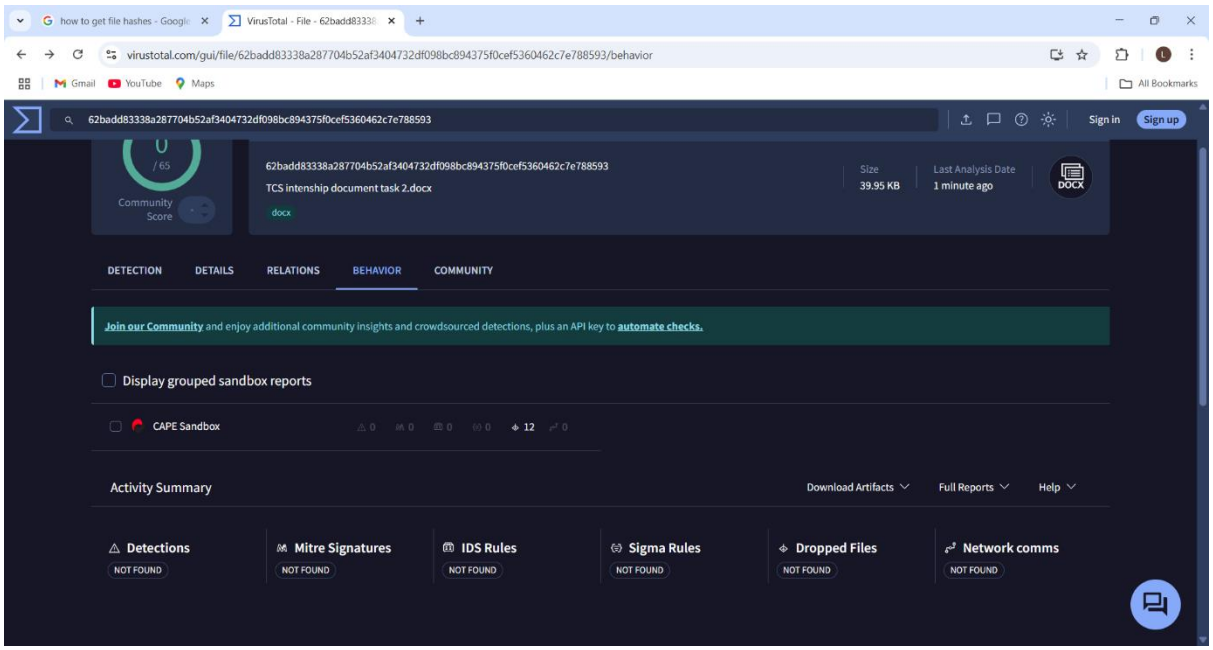


Image showing behaviour of the file

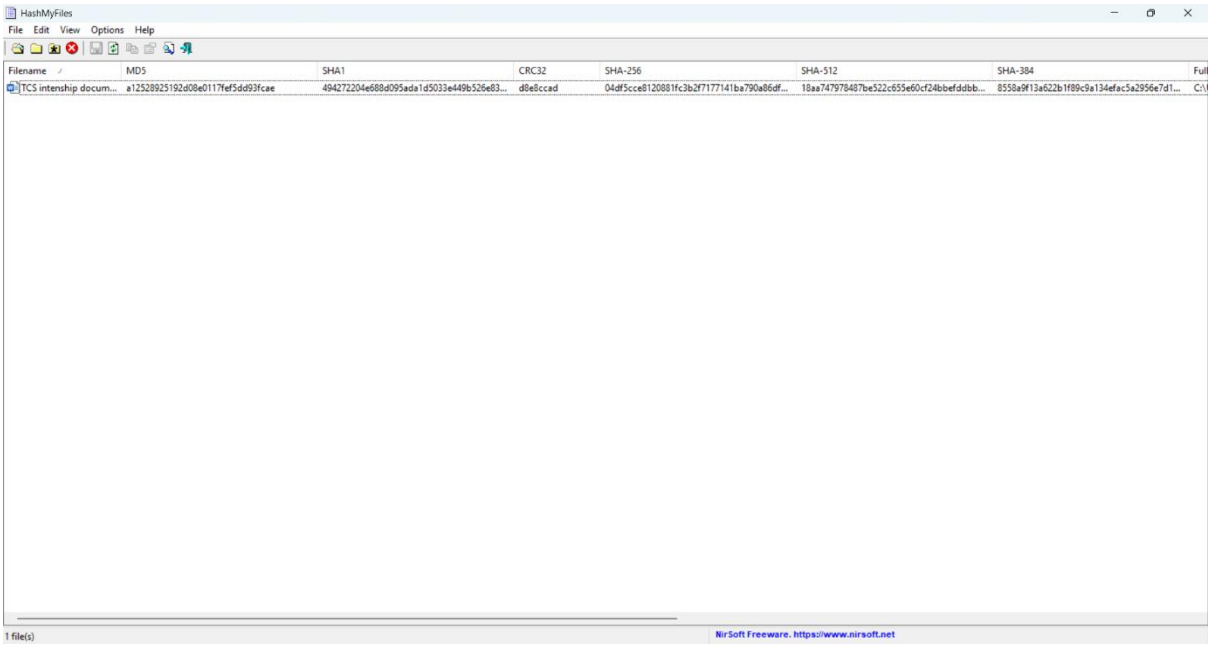


Image showing change in the Hash value of the file by changing the text of the file

OBSRVE CHANGES IN THE HASH VALUE OF THE FILES

Now I will represent some practical observations of changes in the hash values of the file by comparing them with original hash value of the file

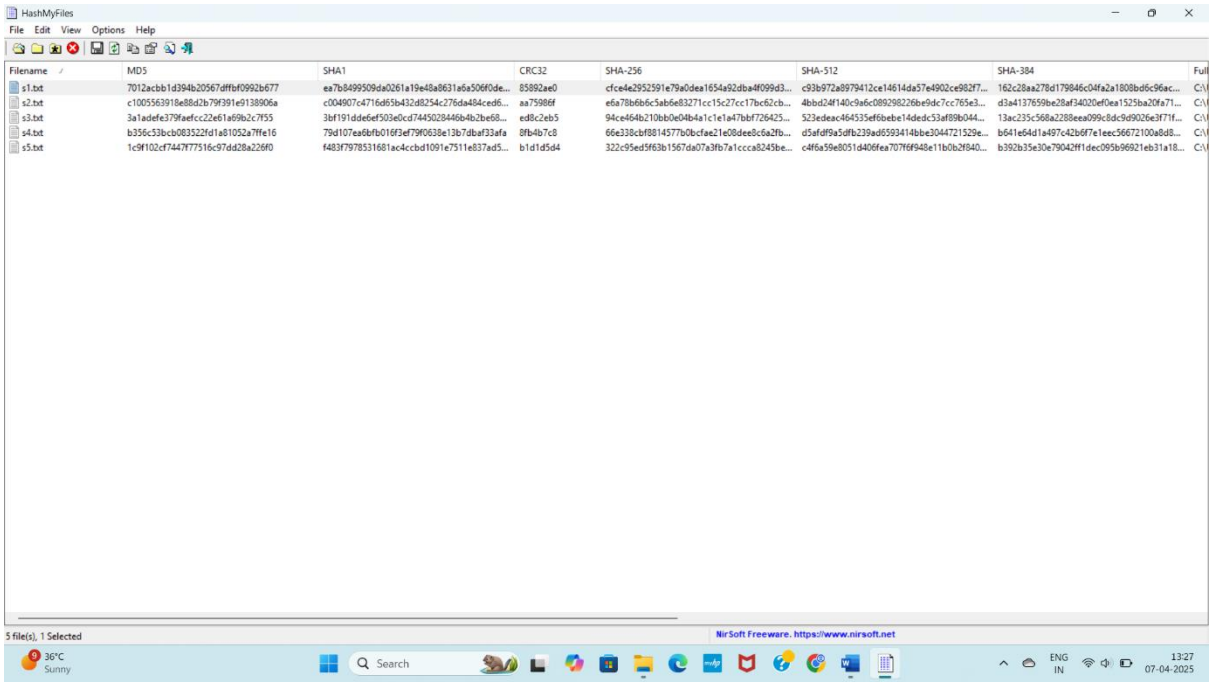


Image represents the hash values of the files and let us compare produced hash values with the original hash values of the respective files.

S1 - 7012acbb1d394b20567dffbf0992b67 file using MD5 hashing algorithm and it is unchanged obtained hash value of the file is: 7012acbb1d394b20567dffbf0992b677

S2 - 60e8b78478be471c0c0d77ca73dc5b78 file using MD5 hashing algorithm and it is changed c1005563918e88d2b79f391e9138906a

S3 - 3a1adefe379faefcc22e61a69b2c7f55 file using MD5 hashing algorithm and it is not changed 3a1adefe379faefcc22e61a69b2c7f55

S4 - 2c7994821e197168a87a96ecaf4bba5e file using MD5 hashing Algorithm and it is changed :b356c53bcb083522fd1a81052a7ffe16

S5 - d75caddc88f98fc6b01c5d6399838e3c file using MD5 hashing Algorithm and it is changed to 1c9f102cf7447f77516c97dd28a226f0

Comparing hash value of the files using virus total tool

Now I am representing my observations of changes in the hash values of the files by comparing them with the original hash values of the file. And the change in the hash values of the files is observed. And the changes has recorded same as hash my files tool. Detailed images of the observations are represented below. In this document . I am also representing the hash value of a URL analysed by using virus total tool by analysing the changes in the hash value of the malicious URL I obtained from phish Tank website

screenshots of virustotal hashvalues.pdf

Above pdf has all the hash observations using virus total tool

Standards measure to guarantee integrity include

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups