**EXPERIMENT NO. 3**

|  |
| --- |
| **Student Name and Roll Number: Harshit Parashar 18csu081** |
| **Semester /Section:5th semester CS-V-CSA** |
| **Link to Code:** |
| **Date:10 SEPTEMBER 2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Automation of hashing tool |
| **Outcome:** The students will learn how to generates hashes of multiple files of a folder |
| **Problem Statement:** Automate hash generation for malware samples |
| **Background Study:** It is efficient to organize and store malware samples by hashes than by file names. Filenames can be easily changed and a single malware can have multiple filenames. Cryptographic hashes on the other hand never changes for a single sample. Additionally, many sites and forum stores malware by hashes   * Condenses a file of any size down to a fixed- length fingerprint * Common method to uniquely identify malware |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  **Download the hashcalc and extract it, it will look like as follows:**    **Drag and drop the malicious file(malware) here and generate the hash**    **Another tool is winMD5 to check sum the authenticity of file**    **Drag and drop the file here and verify it with the original hash** |
| **Question Bank:**  1.Antivirus signatures are constructed using which of the following?  a) Encryption algorithms  b) Random number generator  c) **Hashes**  d) Cyclic redundancy check  2. Antivirus program hash files on a computer in order to detect which of the following activities?  a) File size changes  b) File permission changes  c) **File content changes**  d) All of these  3. When a Hash function is used to provide message authentication, the hash function value is referred to as  a) **Message digest**  b) Message authentication code  c) Hashed based MAC  d) None of these  4. What is a Hash? (And How Does It Work?)  Answer: Hashes are the **output of a hashing algorithm** like MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms essentially aim to produce a unique, fixed-length string – the hash value, or “message digest” – for any given piece of data or “message”.  5. How Hashes Establish Identity?  Answer: **Hashes** cannot be reversed, so simply knowing the result of a file's **hash** from a **hashing** algorithm does not allow you to reconstruct the file's contents. What it does allow you to do, however, is **determine** whether two files are identical or not without knowing anything about their contents |