ITMS 538 Assignment 02b_s

Alan Palayil

Due Date: 09/18/2022

In this lab, we are presented on how we handle evidence. We learn about the position of submission folder along with the command prompt to create the text file which contains the MD5 and SHA1 hashes. We are introduced with WinHex that is an application used to make a forensic copy of the evidence. It is utilized for data examination, editing, recovery, and so on and through the option of "Compute Hash" in the tool's menu, we can check if the hash values of the original and copy are same. The other application we are presented is AccessData FTK Imager which is utilized to make an accurate duplicate of original evidence without making any changes to it. We can verify the Image Verification and check the validity of the hash values using the menu options. This was an introductory lab to get us acquainted with the applications we will utilize.

We use SHA1 and MD5 hash values for forensic images. The SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes the input and produces a 160-bit hash value which is known as a message digest. The MD5 (Message-Direct 5 algorithm) is cryptographic hash function that results in a 128-bit hash value that verifies a file and is used for authentication. An algorithm utilized in hashing is known as a hash function, and the value returned by this function is called a "Message Digest" or Hash value. We utilize these hash values to check and verify if the original file isn't tampered or altered during the investigation as a result of the utilization of various tools for data analysis and evidence collection. Any changes in the file, changes the hash values and can be utilized to demonstrate the security quotient of file integrity via hash functions.

SHA1 and MD5 are both hashing algorithm.MD5 is based on an older protocol and the principal difference is that SHA-1 returns a 160-byte hash while MD5 returns a 32-byte hash. The SHA-1 is less inclined to brute-force attacks but MD5 is more efficient in terms of speed. MD5 is five times faster than SHA1 but only returns 1/fifth 5th the bytes. MD5 has a collision rate of 2^32. Even though it is faster, you will need 3-5 iterations of MD5 to get a similar degree of security in SHA1. Hashing is utilized to ensure the evidence integrity. Hash functions are one-way functions which implies you can't reverse a hashing process to extract original data from hash value. The size of hash value is constantly fixed and it's independent of the size of input data. The hash value can't be duplicated for two different input files. The utilization of MD5 and SHA1 hash algorithms is a common practice in digital forensics. These algorithms permit investigators to preserve digital evidence from the moment they acquire it to the point it is delivered in court.

I believe the reason we don't use a single hash function for verification is improve the preservation of the original data file. The MD5 is a fast-hashing function however with a considerable amount of computational power, it can be cracked. This can lead to hash collision where two different files having different contents yet the same MD5 hash value. To ensure that hash collisions don't take place we use SHA-1 hash function as well to add an extra layer of security.