HASH VALUE: AUTHENTICATION AND ADMISSIBILITY IN INDIAN PERSPECTIVE

Hash value plays a significant role in establishing the authenticity and integrity of data/evidence in the digital world particularly in Cryptography, Data Analyses and Forensic Imaging etc. Hash Value popularly known as Fingerprint of data is the crucial single factors which not only authenticate the integrity of data but also play crucial role in the validation of the forensic processes & equipments used for the forensic examination. The admissibility of the hash value have increased over the years as the hash values have unique identification capabilities that have a high degree of accuracy to confirm whether two records or files are a match or are dissimilar.

Hashing is the process of mapping large amount of data item to a smaller table with the help of a hashing function/algorithm. A hashing algorithm transforms an arbitrarily long block of data into a large number. The most widely used hash functions are Hash Functions are: MD5 and SHA-1. SHA-1 produces a message digest that is 160 bits long; A hash value is used to ensure that the examined copy/mirror image is the replica of the original. The basic principle adopted in the forensic examination of the electronic evidence is that examination is never conducted on the original evidence except under some exceptional circumstances. The image is used during the forensic examination to preserve the integrity of the original evidence. A hash value is taken of the imaged copy before any examination and matched with the hash value of the original evidence, if the hash values are same, then the copy is treated the same as original.

Hash value can be used to authenticate evidence in the court of law as well as during discovery process. One method of authenticating electronic evidence under Rule 901(b)(4) is the use of “hash values” or “hash marks” when making documents. A hash value" is an alphanumeric string that serves to identify an individual digital file as a kind of "digital fingerprint." Although it may be possible for two digital files to have hash values that "collide," or overlap, it is unlikely that the values of two dissimilar images will do so. United States v. Cartier, 543 F.3d 442, 446 (8th Cir. 2008). In the present case, the district court found that files with the same hash value have a 99.99percent probability of being identical.

Information Technology Act, 2000 also support the international accepted hash function as the unique and reliable method to authenticate the integrity of data as emerging from the explanation of Sec 3 which provides:-

> **Explanation.--** For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally

smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible--

a. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
b. that two electronic records can produce the same hash result using the algorithm.

Section 3, further provides that the authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function.

The rule 3, 4 and 5 of Information Technology (Certifying Authorities)Rules 2000 provides the use of the hash function in authentication of information by digital signature and in creation and verification of digital signatures and further provides that the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process. The rule 6 of the Information Technology (Certifying Authorities)Rules 2000 recognize the MD5 & SHA-2 as the accepted standard digital hash function.

The provision of Information Technology Act, 2000 also recognize the hash value as unique and MD5 & SHA-2 as the standard hash function attuned to International Standards but how far these are used in investigation or digital forensic and its admissibility in the India Courts is yet to be seen and still a long journey but burst in cyber offences in the last few years hardly leaves any choice for the investigation agencies and forensic institution.

http://www.neerajaarora.com/hash-value-authentication-and-admissibility-in-indian-perspective/