Authenticate the Evidence

DO NOT damage your evidence!!!

- Digital evidence must be preserved in its original state.
- Law requires that evidence be authentic and unaltered.

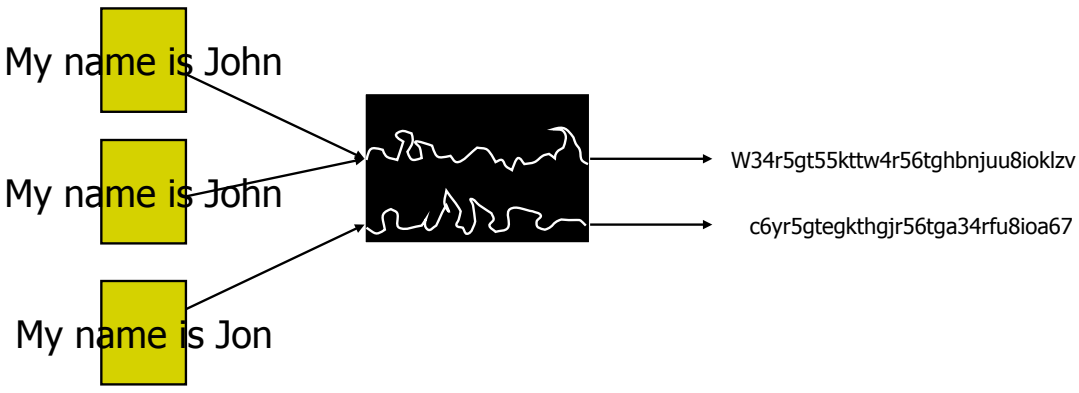
Authenticate the Evidence

- MD5
- SHA

Message Digests & digital signatures

- Message Digest: The result of applying a hash function to a data object
- A cryptographic hash algorithm
  - One-way form of encryption
  - Always produces the same number for a given input
  - Collision free algorithm: Functionally impossible to create a document that has the same hash value as another document

Message Digests & digital signatures



Message Digests & digital signatures (Con't)

- Hash functions are used by forensic examiners in two ways
  - Positively verify that a file has been altered by comparing its message digest with the original message digest
  - Verify that files (or their copies) are intact and have not changed

Generate MD5 checksums

- For the drive and every partition
  - Generate MD5 hash for the original drive
  - Bit-to-bit copy the drive
  - Generate MD5 hash for the copy
  - Compare the values to verify data integrity
  - *man md5sum*