Practice activity - Hashing

In this practice activity, you will apply your knowledge of hashing to verify the integrity of some files that you have received.

Your company has received some confidential files through email from their business partner. As a Cyber Security professional, your boss has requested you to verify if the files have been tampered. It is your job to verify the integrity of the received files.

Resources:

- **Files**: Picnic.jpg, Confidential.pdf (both files also available in this resource section)
- For calculating md5, you can use a web client or shell utility:

  Online: *https://md5file.com/calculator*

  Windows: *certutil -hashfile <filename> MD5*

  Mac: *md5 <filename>*

You have received the following files from a sender, and you have downloaded the hashes for these files from an authentic source:

Item	Value
Filename	Picnic.jpg
md5 Hash from Authentic Source	b120214077c052b6a6024b9512a64aad

Item	Value
Filename	Confidential.pdf
md5 Hash from Authentic Source	e78fdb2eca221b2f92c1bf03d111eb42

Task:

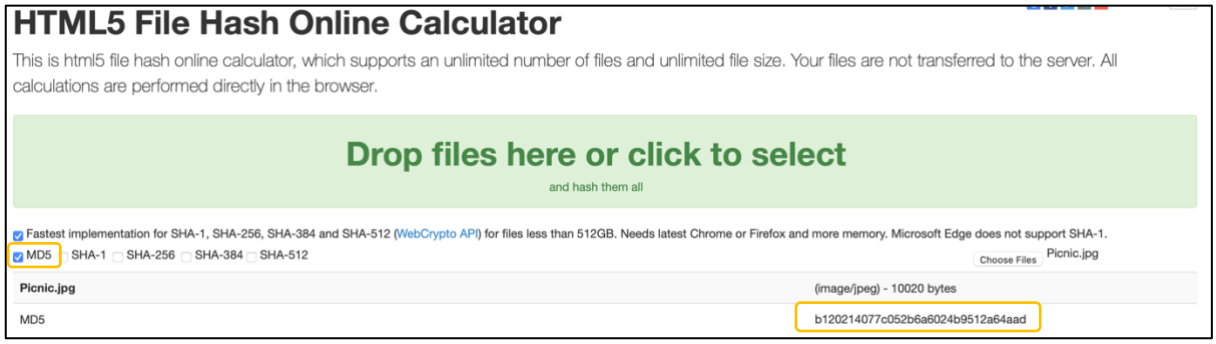
Can you verify if the integrity of any of the files has been compromised during communication? (Solution on next page)

Solution

We need to independently calculate the hash of the two files and then compare with the hash received from an authentic source.

Picnic.jpg

Online: *https://md5file.com/calculator*



Terminal (Mac)

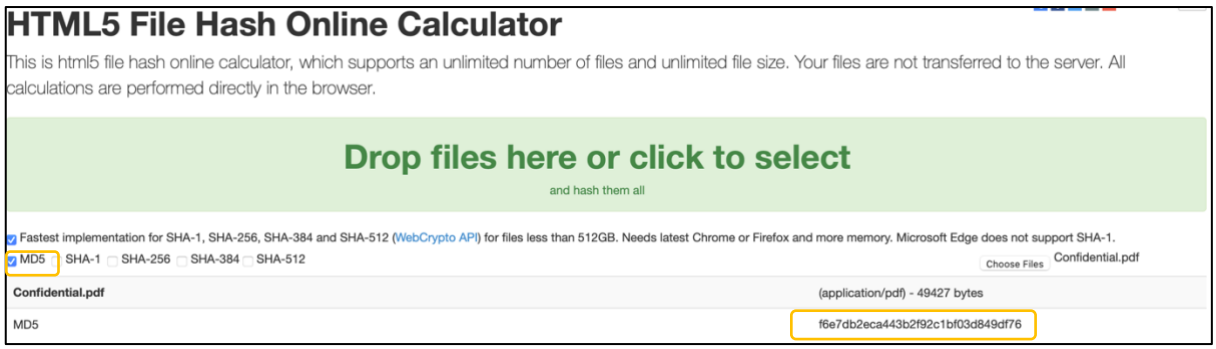
Decision: Since the obtained hash is the same as the hash from the authentic source, therefore the file's integrity is **intact**.

Hash from authentic source: b120214077c052b6a6024b9512a64aad

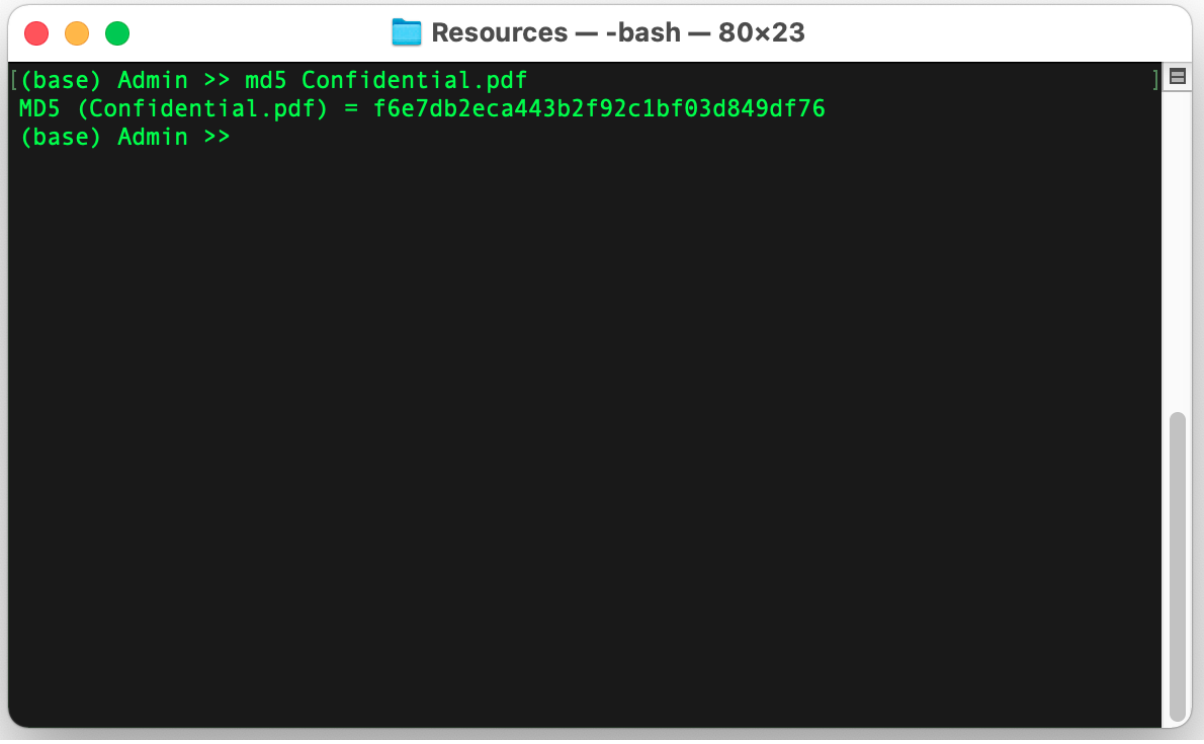
Calculated hash: b120214077c052b6a6024b9512a64aad

Confidential.pdf

Online: https://md5file.com/calculator



Terminal (Mac)



Decision: Since the obtained hash is different from the hash obtained from an authentic source, therefore the file's integrity is **not intact**.

Hash from authentic source: e78fdb2eca221b2f92c1bf03d111eb42

Calculated hash: f6e7db2eca443b2f92c1bf03d849df76