STANDARD OPERATING PROCEDURE (SOP)

FOR

PRESERVATION OF DIGITAL PHOTOGRAPHS AND VIDEO CLIPS

Ref:

i. Judgments dated 31.01.2022 of the High Court of Orissa in W.P. (C) No. 31622 of 2021 and W.P. (C) No. 32580 of 2021

ii. Order dated 25.04.2022 of the High Court of Orissa in W.P. (C) No. 32580 of 2021

1. A digital photograph shall ordinarily mean the following:-

    a. An image produced using a digital/mobile camera and stored as an electronic file.

    b. An image originally produced using a digital/mobile camera and rendered for viewing as a virtual image or on film or paper; also called digital print.

2. Photography and Videography referred to in this SOP can be done through digital camera / mobile phone camera in such a manner that the output (Photograph/Video) is properly visible.

3. Whenever digital photographs are taken or video recording is made with regard to vehicles or NDPS items, they should be done in such manner so as to show all relevant portions of the item or process in question so as to enable the Court in forming necessary opinion in the matter.

    In case of vehicles, digital photographs should clearly show the registration number, engine number and chassis number.

4. No video recording shall be of duration of more than one minute.
5. The file type of the images should be in JPG/JPEG/PNG format and the video should be of MP4/MOV/AVI etc. format
6. Every digital photograph and video clip should carry date and time stamp with regard to their origin.
7. **It shall be necessary to furnish a certificate as to under which official's supervision the photographs or videos were taken. This certificate should be ordinarily furnished to the Presiding Officer and be made part of the order sheet. Such certificate can be furnished by any Court official upon whom the duty is delegated by the Court to monitor the taking of digital photographs or recording of video, as the case may be.**
8. The certificate at clause (7) shall be made part of the case record and this fact shall be reflected in the order sheet.
9. In case of any seized vehicle or any other conveyance which cannot be conveniently produced before the Court, any skilled photographer and/or one cameraman (for video recording) may be deputed to the place of detention for the purpose of taking photography or video clips as per order of the concerned Court and appropriate certificate as prescribed by Court must be furnished by such person to that effect.
10. The order of the Court should mention the details as stated under **Appendix -I.**
11. It will be necessary to keep an encrypted copy of the digital photograph and the video clip and calculate the hash value of both. The hash value along with date and time stamp of the photograph and video shall be noted in the order sheet.
12. Please see **Appendix II** for guidance on encrypting a digital photograph or video file.

13. Please see **Appendix III** for guidance on how to generate hash value of a digital photograph or video file.

14. The encrypted digital photograph and/or video clip is to be ordinarily stored on a pen drive or an external hard drive or any other appropriate storage device which in turn is to be kept in a secure cover in the file. The encryption key should be kept separately but securely preserved to be accessible by the Court in future.

15. The aforementioned digital file may be simultaneously stored on a server kept either in the concerned Court premises or in the server of the jurisdictional District Court and the encryption key/password should be kept securely and confidentially. It should be transmitted by the Presiding Officer to his/her successor at the time of demitting office. It may be transmitted to any other official or staff who may be required to access the encrypted file and show it to any authority after decryption. A note of this should be kept in the case file every time anyone accesses an encrypted file.

    Till such time a central storage server is provided, the digital photographs, video clips can be stored in an external hard disc drive (HDD). District Judges shall procure and supply one HDD each to the Judges hearing the matters including those in the outlying stations. The HDD should be of at least 1TB storage capacity. In case of any difficulty in complying with the above, the data of all the Courts in a single Court complex can be stored on a common HDD till provision of one HDD to each Court in such complex. The District Court will utilize the funds available in the District Court budget under the appropriate head of accounts for the above purpose.

16. While accessing in future the digital photographs and video clips, stored on such storage device/server, the integrity of the said digital photograph and video clip may be verified by

matching the current hash value of the file with the hash value noted in the order sheet. If the above mentioned hash values do not match, then modification in the digital files can be inferred and reasons thereof may be ascertained and necessary action as deemed fit and proper may be taken.

17. Access to stored digital files should always be under the written permission of the Court. Pending development of prescribed facility of recording logs electronically, Court should keep record in order sheet of the details of the person accessing the stored digital photographs/video files along with the purpose of accessing the same every time such access is permitted by Court.

18. A backup shall be created simultaneously of each electronic record stored in accordance with (14) and (15). The backup shall be stored at a separate location. If the integrity of the digital photographs/video clips in the main storage is found to have been compromised, then backup photographs/video clips may be relied upon provided that their current hash values match with their respective hash values as noted in the case record.

19. A separate register shall be maintained in every Court or Court complex as the case may be, of the digital files received, verified and transferred to the storage. The entries in this register should show details of the case and description of the digital files in terms of their contents.

20. To avoid difficulties which may arise out of unexpected loss of data from the storage media, Court shall also cause photographs (in physical form) to be retained in the case record after taking them in the same manner as prescribed under (2) and (3). Each such photograph shall on its back side carry the signature and seal of the Presiding Officer.

21. There should not be any connection of the stored digital photographs and video files to the internet.

22. No portion of the photographs or video recordings in relation to any case should be reproduced or transmitted in any form or manner except without express consent of the Court.

23. **The presence of the Informant/ Complainant and accused persons shall not be mandatory while complying with the SOP.**

24. **If the Court considers it fit and proper having regard to the facts and circumstances of the case, it may direct that the Applicant shall at his or her cost prepare digital photographs and videos of the seized items in the manner prescribed in the SOP and produce the same before the Court in an electronic storage media. In every such case, Clauses-7 (as modified) and 8 of the SOP shall be strictly followed.**

    Whenever the Applicant submits the digital files, it shall be transferred immediately to the Court's storage device at his own cost by following the SOP. In such cases, the final encryption and hash value shall be generated at the time of storage of digital files in the Court's storage device provided that the Court is satisfied that the SOP has been followed in preparing the digital photographs and videos of the items, and the transmission and storage of the same in the Court storage device.

25. **It will be open to the Judge who is in charge of accounts of the concerned Court establishment/ complex to hire the services of the local photographers/ videographers by following the relevant rules for the purpose of complying with the SOP.**

Directions and guidelines issued from time to time in the matter shall automatically form part of this SOP.

APPENDIX – I

DETAILS TO BE MENTIONED IN COURT'S ORDER

Name of the Court —

Case No. —

Cause Title of the Case —

Name and Details of Person tendering the Digital Photograph/Video -

Description (Brand name, Serial number, etc.) , if any, of storage media (whether CD/DVD/Pen Drive etc) -

Operating System and Software/Application required to view the digital photograph/video -

Number of files and size of each as contained in the storage media. -

Duration of video file -

Date on which data was stored or copied on said storage media (DD:MM:YY). -

Hash Function used (SHA-256/ MD5 and/or any other algorithm notified from time to time) and software used to generate the hash value. -

Hash Value -

Hash Function used (SHA-256/ MD5 and/or any other algorithm notified from time to time) and software used to generate the hash value. -

Hash Value -

Any other particulars –

APPENDIX – II

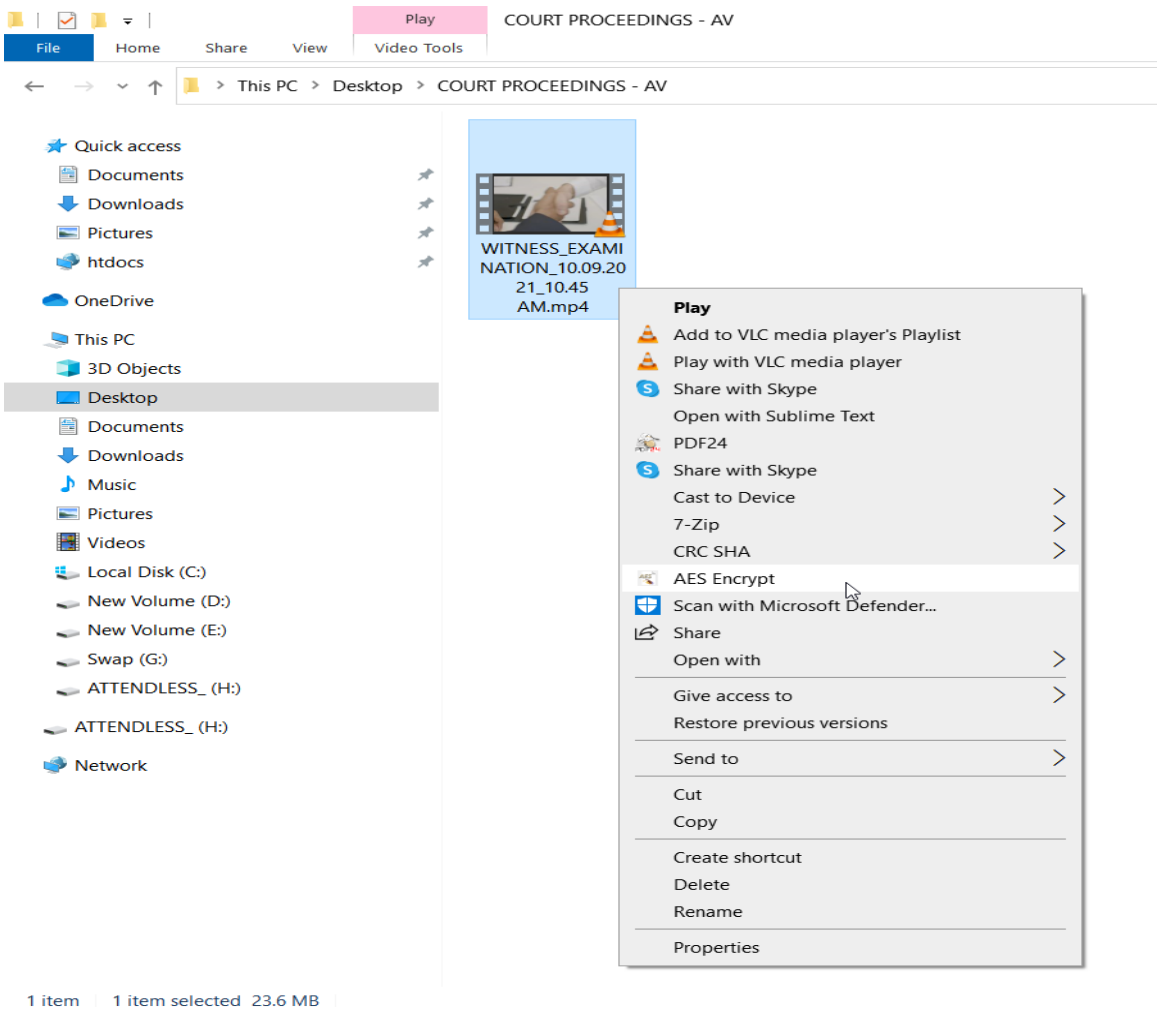
How to encrypt & decrypt digital files

There are various tools/softwares available for encrypting digital files. Steps below may be followed to encrypt digital files using free & open source tools.

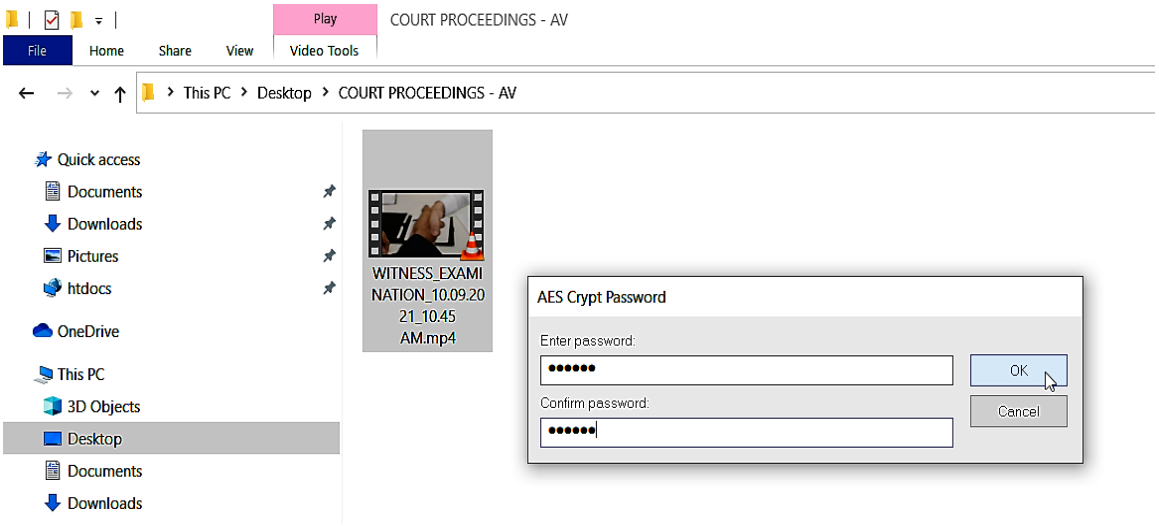
AES Crypt: AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES), 256-bit encryption algorithm, to easily and securely encrypt files. https://www.aescrypt.com/download/

Download and install the above application first.

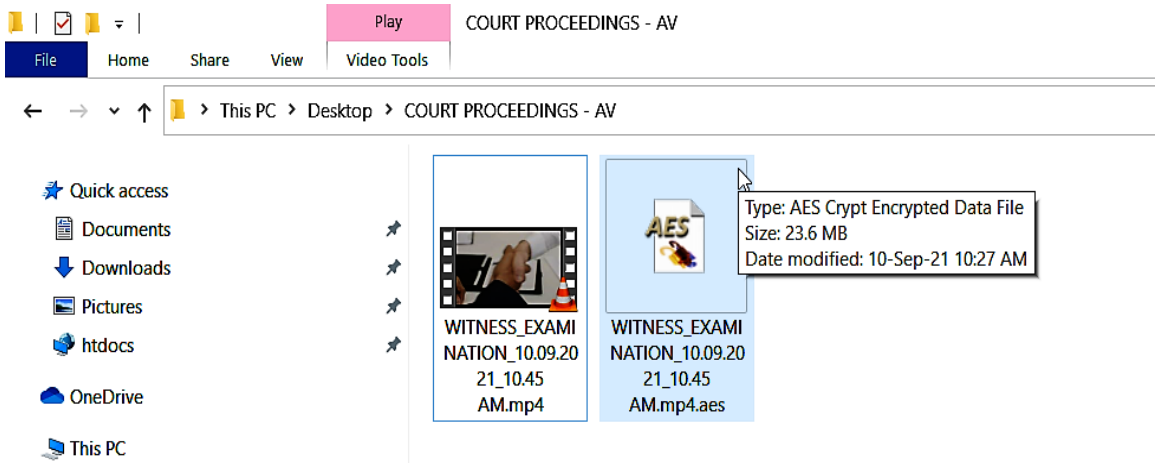
1. Right click on the image/video file and select 'AES Encrypt'.



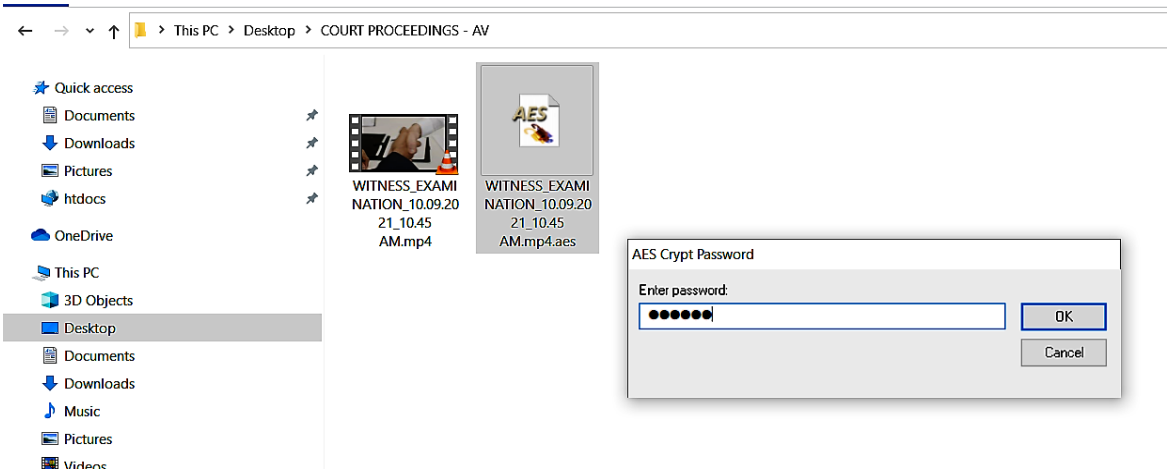
2. Enter the password/key for encryption.



3. Encrypted file will be generated.



4. Double click on the encrypted file to decrypt it. Provide the secret key/password when asked.



APPENDIX - III

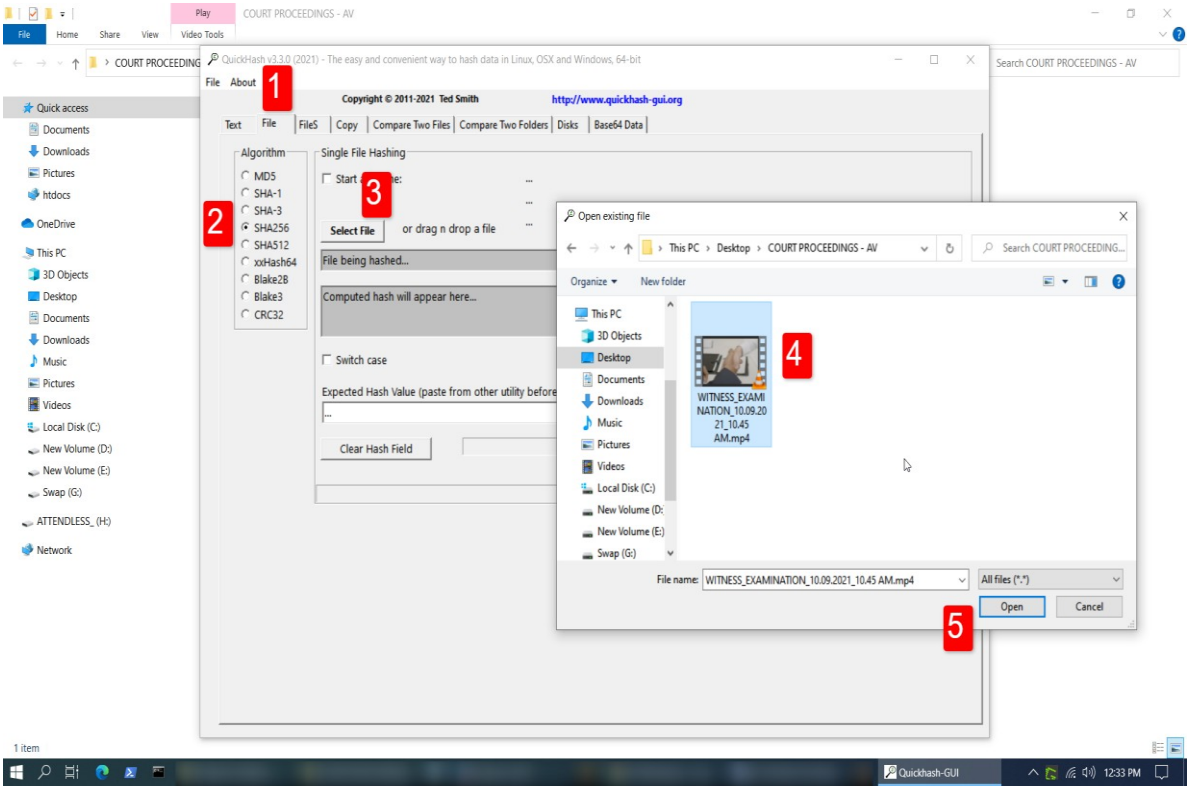
HOW TO GENERATE HASH VALUE

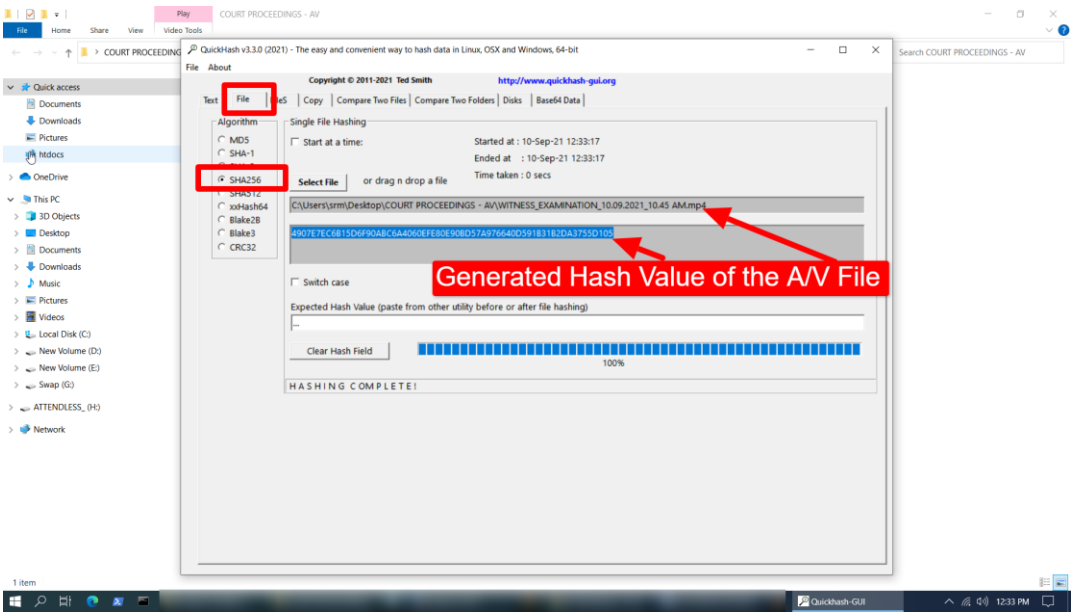
There are various tools/softwares available for generating Hash Value of the digital files. Steps below may be followed to generate Hash Values of digital files using free & open source tools.

QuickHash: QuickHash GUI is an open-source data hashing tool for Linux, Windows, and Apple Mac OSX with graphical user interface (GUI). Hash algorithms currently available are: MD5, SHA1, SHA-3 (256 bit), SHA256, SHA512, Blake2B (256 bit) and Blake3, CRC32 etc.

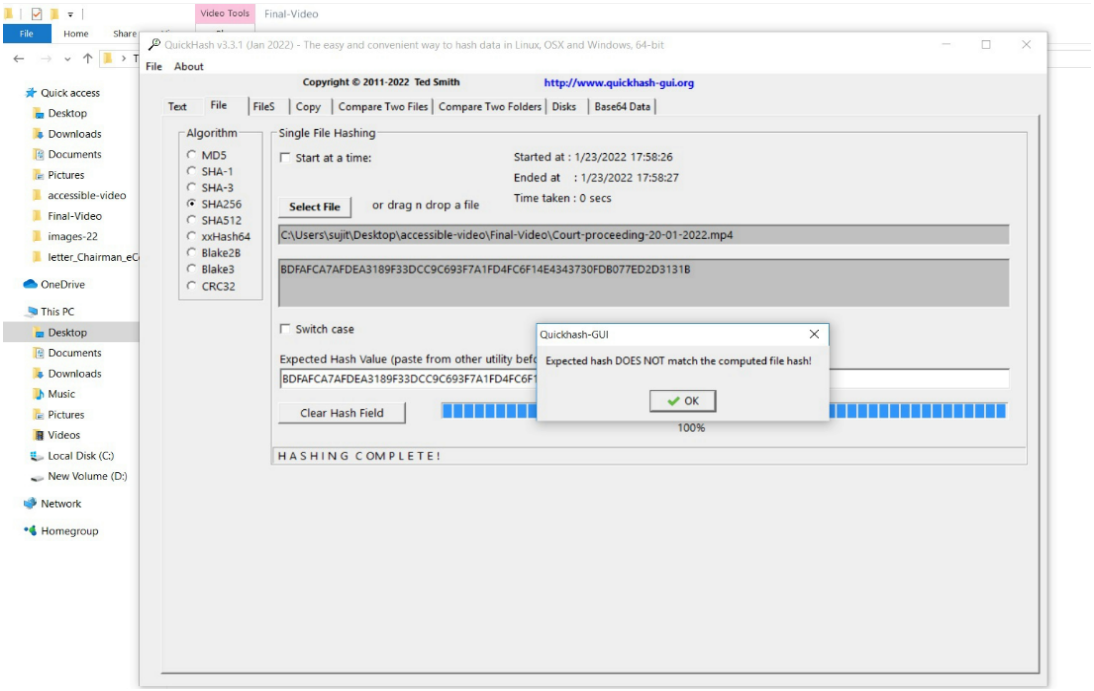
Visit https://www.quickhash-gui.org/ . Download and install the application.

1. Click on the File tab.
2. Select the algorithm in the left hand side.
3. Select and browse the digital file for which hash is to be calculated.
4. Copy and keep the hash value generated.





5. To check if the file has been altered, provide the stored hash in the "Expected Hash Value" field and it will match/not match with the hash value. Mismatch ordinarily denotes that the file has been altered unless there are materials before the Court to indicate otherwise.



Hash Values using two different hash functions should be calculated and noted in the rows above to avoid chances of hash collision. If in the first hash value calculation algorithm SHA256 has been used, then for calculating the hash value again, any other algorithm (e.g. MD5) may be used and the same process as first time be followed. Both the hash values are to be mentioned in Appendix – I.