Scientific Working Group on Digital Evidence

SWGDE Data Integrity Within Computer Forensics

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Data Integrity Within Computer Forensics

1.0 Digital Evidence

Digital Evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved. The commonly accepted method to achieve this is to use a hashing function. The hashing function will generate a mathematical value for either an individual file or an entire drive. This value will be changed dramatically if any data is altered or the file is accessed.

2.0 Security

Security, both logical and physical, is used to prevent the contamination between cases or unauthorized access to the original evidence or forensic image. This can be accomplished by different means depending on the agency's protocols and the type of evidence. It is incumbent upon the examiner to document all procedures used.

3.0 Hashing

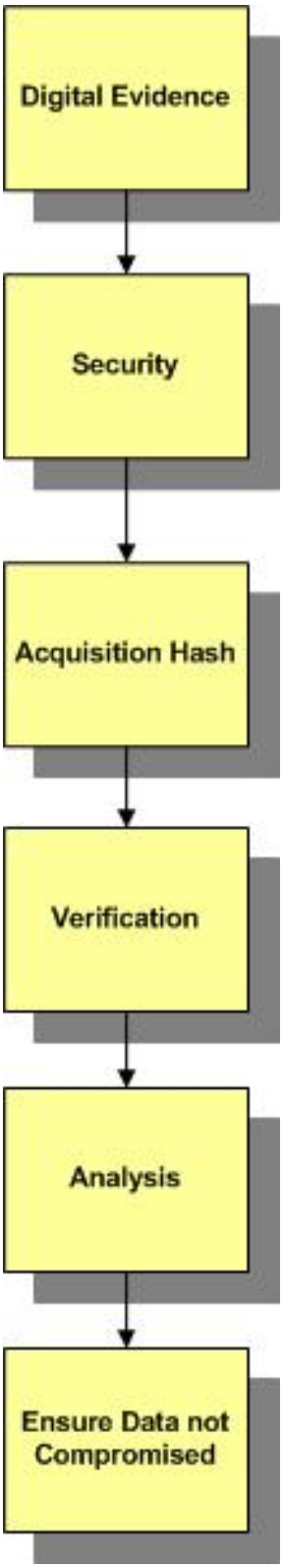
Hashing of the original data, commonly referred to as an acquisition hash, should be done when an image of the data is being created.

4.0 Verification/Analyzation

A verification hash of the image is done after the completion of acquisition but before the image is analyzed to ensure that the integrity of the data has not been compromised.

5.0 Rehash of Image

At the conclusion of the examination, the image can be hashed to prove that no alterations have occurred to the data. If a re-examination is requested, hashing can be performed to authenticate the image as a true and accurate representation of the original evidence.


Digital Evidence
Security
Acquisition Hash
Verification
Analysis
Ensure Data not Compromised