10-27-2022

# An Evaluation Framework For Digital Image Forensics Tools

Zainab Khalid
*National University of Science and Technology - Pakistan*, zainabkhalid2315@gmail.com

Sana Qadir
*National University of Sciences and Technology - Pakistan*, sana.qadir@seecs.nust.edu.pk

## Recommended Citation

# AN EVALUATION FRAMEWORK FOR DIGITAL IMAGE FORENSICS TOOLS

Zainab Khalid and Sana Qadir

National University of Science and Technology (NUST)

School of Electrical Engineering and Computer Science (SEECS)

Islamabad, 44000, Pakistan

{zkhalid.msis18seecs, sana.qadir}@seecs.edu.pk

## ABSTRACT

The boom of digital cameras, photography, and social media has drastically changed how humans live their day-to-day, but this normalization is accompanied by malicious agents finding new ways to forge and tamper with images for unlawful monetary (or other) gains. Disinformation in the photographic media realm is an urgent threat. The availability of a myriad of image editing tools renders it almost impossible to differentiate between photo-realistic and original images. The tools available for image forensics require a standard framework against which they can be evaluated. Such a standard framework can aid in evaluating the suitability of an image forensics tool for use in a criminal investigation, commercial operation, or academic research. This paper proposes an evaluation framework designed for image forensics tools based on the conformance methodology of testing that employs test assertions and test cases. It is then used to evaluate four image forensics tools namely FotoForensics, Ghiro, Imago Forensics, and Exif Reader. The comparative insight of test results produced by the framework provides a ground for ranking the tools from best to least comprehensive. The results also provide information necessary for users to make intelligent choices about tools and help vendors shortlist areas of improvement in their tools.

**Keywords**: conformance testing, evaluation framework, image forensics, test assertions, test cases, tool testing

## 1. INTRODUCTION

The New York Times predicted the yearly count of pictures taken by the late 2010s to amount to trillions (Heyman, 2015); accurate today. Consequently, images have trickled into every profession. In some industries, however, like the news industry, medical imaging, social media, and e-commerce, they play a defining role (Heyman, 2015; Qazi et al., 2013). Most importantly, they are crucial (and at times the deciding factor) in trials and criminal investigations.

Image forensics aims at validating the *authenticity* of images by recovering information about their history. This includes *source camera identification*, *forgery detection* and *determination of photo-realistic images* (Redi, Taktak, & Dugelay, 2011).

The most common scenario in an ongoing investigation is *passive blind forgery detection.* In such a case, the investigator does not
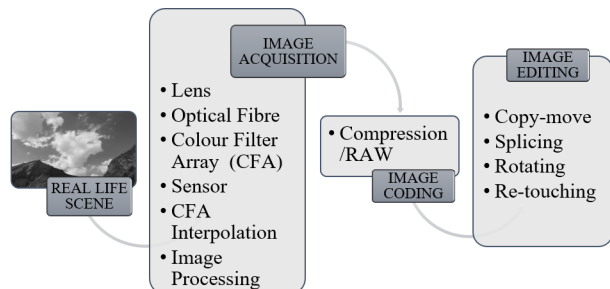
Figure 1. Digital Image Life Cycle

have any information about the image, like camera make/model or the post-processing operations performed prior to its acquisition as potential digital evidence. In other words, the investigator has to carry out a blind detection of image forgeries (Piva, 2013).

The field of image forensics makes use of the Digital Image Life Cycle (DILC) (Fig. 1) to extract artifacts called *fingerprints* or *signatures* introduced in every step of the DILC which can facilitate in detecting forgeries (Piva, 2013).

There are different types of forgery detection techniques: pixel-based techniques, format-based techniques, camera-based techniques, physics-based techniques, and geometric-based techniques (Qureshi, & Deriche, 2014). These techniques depend on variables like forgery methods used to tamper with an image or the different fingerprints used to detect forgeries.

Nowadays, there are many Digital Image Forensics Tools (DIFTs) that can be useful for forensic analysis of images. To ensure reliability, these DIFTs require evaluation using a standard. The Computer Forensics Tool Testing (CFTT) project by the National Institute of Standards and Technology (NIST)[1] is working on tool testing by designing frameworks for each computer forensics discipline, based on *conformance* and *quality* testing

methodologies (Allen, 2017). These methodologies are based on *design science* which is a scientific problem-solving method used especially in Information Systems (IS) (Piirainen, Gonzalez, & Kolfschoten, 2010).

However, no evaluation framework has been designed for image forensics by CFTT or any other organization as of yet. This research work adopts the standard CFTT methodology to develop the very first evaluation framework for DIFTs. The framework is capable of evaluating these tools with respect to their features and functionalities. Consequently, it produces detailed findings about the expected and unexpected results of a tool's performance. The conformance methodology of testing employed in the framework evaluates DIFTs using various *test requirements*, *test assertions* and *test cases*. This helps consumers make informed choices about image forensics tools. It also helps vendors and developers make needed improvements in their tools in addition to setting a benchmark for tool validation, admissibility, and standardization. Finally, the evaluation framework is used to test four DIFTs.

## 2. RELATED WORK

Methodologies used for framework design and tool evaluation in other digital forensics disciplines in reference to the CFTT project are reviewed as follows.

Anobah, Saleem, and Popov, (2014) proposed an extension to the evaluation framework developed by CFTT for mobile device forensics tools. The framework was based on the conformance testing methodology, providing additional test assertions and test cases that covered more profiles in the domain of mobile device forensics. The authors contributed 16 assertions in 5 profiles to the evaluation framework. This included one interesting profile of anti-forensic techniques

for smartphones. They also tested tools such as XRY, Cellebrite's UFED, and Paraben's Device Seizure. The tests performed to evaluate these tools included the ones designed by CFTT and others added by the authors. Results of the evaluation showed XRY to be the most comprehensive tool.

Rehman, Ahmad, and Saleem, (2017) designed an evaluation framework for Windows memory forensics tools, based on CFTT. First, a survey of several memory forensics tools was conducted. They were generally discussed in light of different profiles such as registry data, drivers, running processes, Dynamic Link Libraries (DLL), event logs, Web activity, and malware analysis. The authors designed a framework using the conformance methodology for testing to develop the test specifications/requirements and consequently develop the test assertions and test cases. Additionally, they provided traceability matrices that related test requirements to test assertions.

Saleem, Popov, Kubi and Kwame, (2013) and Kubi, Saleem, and Popov, (2011) presented an evaluation of mobile device forensics tools. A *quantitative* analysis methodology was used to provide a mathematical basis for evaluation. The authors used tool specifications and test cases developed by CFTT for mobile forensics tools to evaluate XRY 5.0 and UFED Physical Pro tools, obtaining results from CFTT's framework. These results were then quantified using a rating metric that used Confidence Interval (CI). The mathematical evaluation included determining the error rates of the tools called the Margin of Error (MoE). The MoE results were subjected to hypothesis testing and the tools were rated.

# 3.  DIFT EVALUATION FRAMEWORK

Given the fact that no prior framework(s) for DIFTs exist, the proposed image forensics evaluation framework is designed using test specifications/requirements of the image forensics discipline. These requirements are established following exhaustive research in the domain, vendor insights, and knowledge/feedback from consumers of the tools. Test requirements are then used to formulate test assertions. A *test assertion* is a verifiable statement about a single condition after an action is performed by the tool under test (Holder, & Robinson, 2008). A *test case* checks an assertion after the action of a single execution of the tool under test. The *conformance indicator* is declared if the tool under evaluation complies with the assertion being tested.

Every forensics discipline is categorized into different *profiles*. The framework for image forensics is categorized into 18 profiles regarding the current landscape of image forensics:

- Multipurpose Internet Mail Extensions (MIME) information
- Image file type support
- Upload images to tool
- Metadata
- GPS localization
- Tamper detection
- Hash digest
- Thumbnail
- Highlight critical data
- JPEG%
- Hidden pixels
- Reporting
- Multiple image analysis
- Annotations
- Color adjustments
- Similar images
- By-case distinction

- Multiple users and multi-level access system

While the stated profiles are elaborated in the framework itself, a broader discussion particularly on *image metadata* would be beneficial for understanding. A focus on *file system metadata* fields such as creation, modification, and last accessed timestamps is pertinent and carried out in the framework. This is in addition to the *EXIF metadata* fields that reflect the latest advancements in image specifications and formats that the tools support. These include file type, file size, camera make/model, camera ID, dimensions, ISO, aperture, shutter speed, orientation, color space, bit-depth, focal length, flash setting, subject distance, and GPS information. Images are formatted in a varying range of formats such as JPEG, BMP, TIFF, PNG, PSD, GIF, RAW, WebP, PXR, etc. The evaluation framework can be used to test an image forensics tool for any image format that the tool is capable of analyzing.

The DIFT framework consists of *core* and *optional* parts. A tool must comply with core assertions to qualify as an image forensics tool. Optional assertions are not mandatory, but compliance with them enhances the standard of the tool. Standard CFTT nomenclature is followed in the framework. The following terminology is used:

- DIFT–Digital Image Forensics Tool
- CR–Core Requirement
- OR–Optional Requirement
- CA–Core Assertion
- AO–Optional Assertion

The proposed *core evaluation framework* consists of 18 core assertions under 7 profiles. The *optional evaluation framework* consists of 30 optional assertions under 16 profiles. All assertions are tested using 69 test cases.

It is pertinent to note that the profiles and test assertions listed in the framework are exhaustive, with respect to the current landscape of the image forensics tools that exist. With advancements in research and development, tools are introduced with novel features under possibly newer profiles. For that matter, the framework can be updated with the addition of new test assertions and profiles. The core and optional parts of the framework are elaborated as follows.

## 3.1 Core Assertions and Test Cases

Table 1 gives an overview of core assertions with brief explanations. A detailed explanation of the assertions under their profiles is given as follows. With every test assertion, corresponding test case(s) and conformance indicator(s) are also given.

### 3.1.1 MIME Information

**Assertion DIFT-CA-01**: If the tool is capable of reading the media type as an image from the MIME information, it shall read/load the image.

Test Action DIFT-01: Attempt to read/load the image using the tool.

Conformance Indicator: The tool successfully read/loaded the image.

### 3.1.2 Image File Type Support

**Assertion DIFT-CA-02**: If the tool provides support for forensic analysis of the read image file type, it shall report that the file type is supported.

Test Action DIFT-02: Attempt to read/load the particular file type in the tool.

Conformance Indicator: The tool supports the file type of the image.

**Assertion DIFT-CA-03**: If the tool does not provide support for forensic analysis of the read image file type, it shall report that the file type is not supported.

Table 1. Core assertions

| DIFT-CA-01 | Determine media type from MIME information |
|---|---|
| DIFT-CA-02 | Determine if image file type is supported by tool |
| DIFT-CA-03 | Determine if image file type is not supported |
| DIFT-CA-04 | Determine if tool uploads single image directly from computer |
| DIFT-CA-05 | Determine file name of image |
| DIFT-CA-06 | Determine size of image |
| DIFT-CA-07 | Determine dimensions of image |
| DIFT-CA-08 | Determine time of image capture |
| DIFT-CA-09 | Determine the last time image was modified |
| DIFT-CA-10 | Determine the last time image was accessed |
| DIFT-CA-11 | Determine the camera make |
| DIFT-CA-12 | Determine the camera model |
| DIFT-CA-13 | Determine if image has been stripped off metadata |
| DIFT-CA-14 | Determine if camera model supports GPS localization |
| DIFT-CA-15 | Determine the GPS coordinates |
| DIFT-CA-16 | Determine if the tool performs Error Level Analysis (ELA) |
| DIFT-CA-17 | Determine if tool calculates hashes of the images |
| DIFT-CA-18 | Determine if tool performs search via hash matching |

Test Action DIFT-03: Attempt to read-/load the particular file type in the tool.

Conformance Indicator: The tool does not support the file type of the image.

### 3.1.3 Upload Images to Tool

**Assertion DIFT-CA-04**: If the tool is capable of reading a digital image, it shall upload the image from the computer onto the tool directly.

Test Action DIFT-04: Attempt to load image from the computer.

Conformance Indicator: The tool uploaded image from the computer.

### 3.1.4 Metadata

**Assertion DIFT-CA-05**: If the tool provides support for the image file type and reads it without error, it shall determine the filename of the image and report it in a user-friendly manner.

Test Action DIFT-05: Attempt to read the filename of the image loaded into tool.

Test Action DIFT-06: Compare the actual name of the image on the computer with the one read by the tool.

Conformance Indicator: The tool read the filename of the image.

**Assertion DIFT-CA-06**: If the tool provides support for the image file type and reads it without error, it shall determine the size of the image and report it in a user-friendly manner.

Test Action DIFT-07: Attempt to determine size of the image loaded into tool.

Test Action DIFT-08: Compare the actual size of image on the computer with the one read by the tool.

Conformance Indicator: The tool determined the size of the image.

**Assertion DIFT-CA-07**: If the tool provides support for the image file type and reads it without error, it shall determine the dimensions of the image and report them in a user-friendly manner.

Test Action DIFT-09: Attempt to determine dimensions of the image loaded into tool.

Test Action DIFT-10: Compare actual dimensions of image on the computer with the ones read by the tool.

Conformance Indicator: The tool determined the dimensions of the image.

**Assertion DIFT-CA-08**: If the tool provides support for the image file type and reads it without error, it shall determine timestamp of the image, i.e., creation date and time, and report it in a user-friendly manner.

Test Action DIFT-11: Attempt to determine the creation date and time of image using the tool.

Test Action DIFT-12: Compare the date and time determined using the tool with the actual timestamp of the image.

Conformance Indicator: The tool determined the creation date and time of the image.

**Assertion DIFT-CA-09**: If the tool provides support for the image file type and reads it without error, it shall determine the date and time of modification and report it in a user-friendly manner.

Test Action DIFT-13: Attempt to modify an image and note the date and time.

Test Action DIFT-14: Attempt to determine the modified date and time using the tool.

Test Action DIFT-15: Compare determined modified timestamp with actual modified time and date.

Conformance Indicator: The tool determined the modified timestamp of the image.

**Assertion DIFT-CA-10**: If the tool provides support for the image file type and reads it without error, it shall determine the date and time of last access and report it in a user-friendly manner.

Test Action DIFT-16: Attempt to determine the last accessed date and time using the tool.

Test Action DIFT-17: Compare determined last accessed timestamp with actual last accessed timestamp.

Conformance Indicator: The tool determined the last accessed timestamp of the image.

**Assertion DIFT-CA-11**: If the tool provides support for the image file type and reads it without error, it shall determine the make (manufacturing company) of the source camera of the image and report it in a user-friendly manner.

Test Action DIFT-18: Attempt to determine the make of the source camera of the image using the tool.

Test Action DIFT-19: Compare the determined make using tool with the actual make of the source camera of the image.

Conformance Indicator: The tool determined the make of the source camera of the image.

**Assertion DIFT-CA-12**: If the tool provides support for the image file type and reads it without error, it shall determine the model of the source camera of the image and report it in a user-friendly manner.

Test Action DIFT-20: Attempt to determine the model of the source camera of the image using the tool.

Test Action DIFT-21: Compare the model determined using the tool with the actual camera model of the source camera of the image.

Conformance Indicator: The tool determined the model of the source camera of the image.

**Assertion DIFT-CA-13**: If the tool provides support for the image file type and reads it without error, it shall determine if the image has no metadata (i.e., has been stripped

off metadata intentionally) and report it in a user-friendly manner.

Test Action DIFT-22: Attempt to strip off metadata of an image using a tool (e.g., Exiftool).

Test Action DIFT-23: Attempt to determine metadata of the image using the tool.

Conformance Indicator: The tool determined that the image has no metadata.

### 3.1.5    GPS Localization

**Assertion DIFT-CA-14**: If the tool provides support for the image file type and reads it without error, it shall determine the support for GPS localization in the model of the source camera.

Test Action DIFT-24: Attempt to determine the support for GPS localization using the tool.

Conformance Indicator: The tool determined that the model of the source camera supports GPS localization.

**Assertion DIFT-CA-15**: If the tool determines whether model of the source camera supports GPS localization, it shall determine the GPS coordinates of the location where the image was captured.

Test Action DIFT-25: Attempt to determine the GPS coordinates of the location where the image was captured.

Conformance Indicator: The tool determined GPS coordinates of the location where the image was captured.

### 3.1.6    Tamper Detection

**Assertion DIFT-CA-16**: If the tool provides support for the image file type and reads it without error, it shall perform the Error Level Analysis (ELA) of the image and display the result in a user-friendly manner.

Test Action DIFT-26: Attempt to tamper with the subject image.

Test Action DIFT-27: Attempt to perform ELA of the image using the tool.

Conformance Indicator: The tool performed accurate ELA of the tampered image.

### 3.1.7    Hashes

**Assertion DIFT-CA-17**: If the tool provides support for the image file type and reads it without error, it shall calculate the hash digest of the image and report it in a user-friendly manner.

Test Action DIFT-28: Attempt to generate hash digest of the image using tool.

Conformance Indicator: The tool computed different types of hash digests of the image.

**Assertion DIFT-CA-18**: If the tool provides support for the image file type and reads it without error, it shall search for an image using the hash digest and report it in a user-friendly manner.

Test Action DIFT-29: Attempt to search for image using hash digest as search criterion using the tool.

Conformance Indicator: The tool searched for the image using the hash digest.

## 3.2    Optional Assertions and Test Cases

Table 2 gives an overview of optional assertions with brief explanations. A detailed explanation of optional assertions is given as follows. With every test assertion, corresponding test case(s) and conformance indicator(s) are also given.

### 3.2.1    Upload Images to Tool

**Assertion DIFT-AO-01**: If the tool is capable of reading a digital image, it shall download the image from the internet onto the tool using a URL.

Test Action DIFT-30: Attempt to obtain the URL of the online image.

Test Action DIFT-31: Attempt to upload image onto the tool using URL.

Table 2. Optional assertions

| | |
|---|---|
| **DIFT-AO-01** | Determine if tool can access online image through URL |
| **DIFT-AO-02** | Determine if tool can upload multiple images onto it simultaneously |
| **DIFT-AO-03** | Determine the unique ID of the source camera |
| **DIFT-AO-04** | Determine the orientation of the image |
| **DIFT-AO-05** | Determine the tags/description of image (if any) |
| **DIFT-AO-06** | Determine the bit-depth of the image |
| **DIFT-AO-07** | Determine the color space of the image |
| **DIFT-AO-08** | Determine if tool extracts different types of metadata |
| **DIFT-AO-09** | Determine ISO of the image |
| **DIFT-AO-10** | Determine the focal length of the image |
| **DIFT-AO-11** | Determine the shutter speed of the image |
| **DIFT-AO-12** | Determine subject distance in the image |
| **DIFT-AO-13** | Determine flash setting in the image |
| **DIFT-AO-14** | Determine aperture value of the image |
| **DIFT-AO-15** | Determine if thumbnail of the image is available |
| **DIFT-AO-16** | Determine difference between thumbnail and actual image |
| **DIFT-AO-17** | Determine type of tampering done with image |
| **DIFT-AO-18** | Determine ability to highlight most critical metadata of the image |
| **DIFT-AO-19** | Determine JPEG quality of the image |
| **DIFT-AO-20** | Determine any hidden pixels in the image |
| **DIFT-AO-21** | Determine ability to generate an automated report |
| **DIFT-AO-22** | Determine ability to share reports with other users online |
| **DIFT-AO-23** | Determine ability to perform analysis of multiple images simultaneously |
| **DIFT-AO-24** | Determine ability to add annotations to the image |
| **DIFT-AO-25** | Determine ability to make color adjustments to image |
| **DIFT-AO-26** | Determine ability to find other related images online |
| **DIFT-AO-27** | Determine ability to create multiple cases in tool interface for distinction of cases |
| **DIFT-AO-28** | Determine ability to create multiple user account |
| **DIFT-AO-29** | Determine ability to allow user to relinquish access of case to other users i.e., multi-level access system |
| **DIFT-AO-30** | Determine ability to localize the image on a map |

Conformance Indicator: The tool uploaded the image onto the tool using URL.

**Assertion DIFT-AO-02**: If the tool is capable of reading an image, it shall upload multiple images onto the tool directly.

Test Action DIFT-32: Attempt to upload multiple images from the computer.

Conformance Indicator: The tool uploaded multiple images from the computer.

### 3.2.2 Metadata

**Assertion DIFT-AO-03**: If the tool provides support for the image file type and reads it without error, it shall determine the unique ID (serial number) of the source camera and report it in a user-friendly manner.

Test Action DIFT-33: Attempt to determine the unique ID (serial number) of the source camera.

Conformance Indicator: The tool determined the unique ID (serial number) of the source camera.

**Assertion DIFT-AO-04**: If the tool provides support for the image file type and reads it without error, it shall determine the orientation of the image (landscape or portrait) and report it in a user-friendly manner.

Test Action DIFT-34: Attempt to determine the orientation of the image.

Conformance Indicator: The tool determined the orientation of the image.

**Assertion DIFT-AO-05**: If the tool provides support for the image file type and reads it without error, it shall determine any tags/description/comments of the image (if any) and report it in a user-friendly manner.

Test Action DIFT-35: Attempt to determine tags/description/comments of the image.

Test Action DIFT-36: Compare the determined tags/description/comments with the actual tags/description of the image.

Conformance Indicator: The tool determined the tags/description/comments of the image.

**Assertion DIFT-AO-06**: If the tool provides support for the image file type and reads it without error, it shall determine the bit-depth of the image and report it in a user-friendly manner.

Test Action DIFT-37: Attempt to determine the bit-depth of the image.

Test Action DIFT-38: Compare the determined bit-depth with the actual bit-depth of the image.

Conformance Indicator: The tool determined the bit-depth of the image.

**Assertion DIFT-AO-07**: If the tool provides support for the image file type and reads it without error, it shall determine the color space of the image and report it in a user-friendly manner.

Test Action DIFT-39: Attempt to determine the color space of the image.

Conformance Indicator: The tool determined the color space of the image.

**Assertion DIFT-AO-08**: If the tool provides support for the image file type and reads it without error, it shall determine the other types of metadata that exist e.g., XMP metadata, IPTC metadata, and report it in a user-friendly manner.

Test Action DIFT-40: Attempt to determine the various types of metadata of the image.

Conformance Indicator: The tool determined the additional metadata types of the image.

**Assertion DIFT-AO-09**: If the tool provides support for the image file type and reads it without error, it shall determine the ISO of the image and report it in a user-friendly manner.

Test Action DIFT-41: Attempt to determine the ISO of the image.

Test Action DIFT-42: Compare the determined ISO with the actual ISO of the image.

Conformance Indicator: The tool determined the ISO of the image.

**Assertion DIFT-AO-10**: If the tool provides support for the image file type and reads it without error, it shall determine the focal length of the source camera of the image and report it in a user-friendly manner.

Test Action DIFT-43: Attempt to determine the focal length of the image.

Test Action DIFT-44: Compare the determined focal length with the actual focal length of the image.

Conformance Indicator: The tool determined the focal length of the image.

**Assertion DIFT-AO-11**: If the tool provides support for the image file type and reads it without error, it shall determine the shutter speed of the source camera of the image and report it in a user-friendly manner.

Test Action DIFT-45: Attempt to determine the shutter speed of the image.

Test Action DIFT-46: Compare the determined shutter speed with the actual shutter speed of the image.

Conformance Indicator: The tool determined the shutter speed of the image.

**Assertion DIFT-AO-12**: If the tool provides support for the image file type and reads it without error, it shall determine the subject distance in the image and report it in a user-friendly manner.

Test Action DIFT-47: Attempt to determine the subject distance of the image.

Conformance Indicator: The tool determined the subject distance of the image.

**Assertion DIFT-AO-13**: If the tool provides support for the image file type and reads it without error, it shall determine the flash setting of the source camera and report it in a user-friendly manner.

Test Action DIFT-48: Attempt to determine the flash setting of the image.

Test Action DIFT-49: Compare the determined flash setting with the actual flash setting of the image.

Conformance Indicator: The tool determined the flash setting of the image.

**Assertion DIFT-AO-14**: If the tool provides support for the image file type and reads it without error, it shall determine the aperture value of the source camera and report it in a user-friendly manner.

Test Action DIFT-50: Attempt to determine the aperture value of the source camera.

Test Action DIFT-51: Compare determined aperture value with actual aperture value of the source camera.

Conformance Indicator: The tool determined the aperture value of the source camera.

### 3.2.3 Thumbnail

**Assertion DIFT-AO-15**: If the tool provides support for the image file type and reads it without error, it shall determine if the thumbnail of the image exists.

Test Action DIFT-52: Attempt to upload an image with a thumbnail onto the tool.

Test Action DIFT-53: Attempt to determine, using the tool, if a thumbnail exists.

Conformance Indicator: The tool determined thumbnail existence of the image.

**Assertion DIFT-AO-16**: If the tool finds the thumbnail of the image, it shall determine if there is any difference between the thumbnail and the actual image and report it in a user-friendly manner.

Test Action DIFT-54: Attempt to determine any difference between uploaded image and its thumbnail.

Conformance Indicator: The tool determined difference (if any) between thumbnail and image.

### 3.2.4 Tamper Detection

**Assertion DIFT-AO-17**: If the tool detects tampering in the image, it shall determine the type of tampering done and report it in a user-friendly manner.

Test Action DIFT-55: Attempt to determine the type of tampering in the image.

Conformance Indicator: The tool determined type of tampering.

### 3.2.5 Highlight Critical Data

**Assertion DIFT-AO-18**: If the tool provides support for the image file type and reads it without error, it shall highlight the most critical metadata about the image.

Test Action DIFT-56: Attempt to read/find any highlighted critical data.

Conformance Indicator: The tool highlighted critical data.

### 3.2.6 JPEG%

**Assertion DIFT-AO-19**: If the tool provides support for the image file type and reads it without error, it shall determine the JPEG quality (JPEG%) of the image and report it in a user-friendly manner.

Test Action DIFT-57: Attempt to determine the JPEG quality of the image.

Test Action DIFT-58: Compare the determined JPEG quality with the actual JPEG quality of the image.

Conformance Indicator: The tool determined the JPEG quality of the image.

### 3.2.7 Hidden Pixels

**Assertion DIFT-AO-20**: If the tool provides support for the image file type and reads it without error, it shall determine any hidden pixels in the image and report it in a user-friendly manner.

Test Action DIFT-59: Attempt to determine hidden pixels in an image.

Conformance Indicator: The tool determined the hidden pixels in the image.

### 3.2.8 Reporting

**Assertion DIFT-AO-21**: If the tool provides support for the image file type and reads it without error, it shall compile all results in a user-friendly manner and generate an automated report.

Test Action DIFT-60: Attempt to generate a forensic analysis report for an image.

Conformance Indicator: The tool generated an automated report of results for an image.

**Assertion DIFT-AO-22**: If the tool provides support for the image file type and reads it without error, it shall share reports with other online users.

Test Action DIFT-61: Attempt to share report with other online users.

Conformance Indicator: The tool shared reports with online users.

### 3.2.9 Multiple Image Analysis

**Assertion DIFT-AO-23**: If the tool provides support for several image file types and reads them without error, it shall perform forensic analysis of multiple images simultaneously and report results in a user-friendly manner.

Test Action DIFT-62: Attempt to do forensic analysis of multiple images simultaneously.

Conformance Indicator: The tool performed forensic analysis of multiple images simultaneously.

### 3.2.10 Annotations

**Assertion DIFT-AO-24**: If the tool provides support for the image file type and reads it without error, it shall be able to add annotations to the image.

Test Action DIFT-63: Attempt to add annotations to the image.

Conformance Indicator: The tool added annotations to the image.

### 3.2.11 Colour Adjustments

**Assertion DIFT-AO-25**: If the tool provides support for the image file type and reads it without error, it shall make color adjustments to the image.

Test Action DIFT-64: Attempt to make color adjustments to the image.

Conformance Indicator: The tool made color adjustments to the image.

### 3.2.12 Similar Images

**Assertion DIFT-AO-26**: If the tool provides support for the image file type and reads it without error, it shall find other online images that are variations of the image under analysis or related to it in any way, and report it in a user-friendly manner.

Test Action DIFT-65: Attempt to find other online images that are variations of the image under analysis or related to it in any.

Conformance Indicator: The tool found variants of the image online.

### 3.2.13 By-case Distinction

**Assertion DIFT-AO-27**: The tool shall create multiple/separate cases in the tool interface (associated with multiple/separate ongoing investigations).

Test Action DIFT-66: Attempt to create multiple cases in the tool.

Conformance Indicator: The tool created multiple cases.

### 3.2.14 Multiple Users

**Assertion DIFT-AO-28**: The tool shall allow multiple users to use the tool.

Test Action DIFT-67: Attempt to create multiple user accounts.

Conformance Indicator: The tool allowed multiple users.

### 3.2.15 Multi-level Access System

**Assertion DIFT-AO-29**: The tool shall allow a user to relinquish controlled access of a case to other users i.e., it should provide multi-level access with respect to other users.

Test Action DIFT-68: Attempt to assign different levels of access authority (to case material) to different users.

Conformance Indicator: The tool assigned different levels of access authority (to case material) to different users.

### 3.2.16 GPS Localization

**Assertion DIFT-AO-30**: If the tool determines support for GPS localization by the model of the source camera, it shall show the location of the image on a map.

Test Action DIFT-69: Attempt to view the image on a map.

Conformance Indicator: The tool localized the image on a map.

# 4. EVALUATION OF TOOLS USING DIFT FRAMEWORK

The proposed evaluation framework was used to test four DIFTs: (1) FotoForensics[2] v1.1.3294, (2) Ghiro[3] v0.2.1-1, (3) Imago Forensics[4] v1.0.5 and (4) Exif Reader[5] v3.00. The execution environment for the test cases is given below:

- Execution Environment: Windows 7 Professional Service Pack 1
- Test computer: HP ProBook 4530s, Intel(R) Core(TM) i3-2310M CPU @ 2.10 GHz
- RAM: 4.00 GB
- System Type: 64-bit Operating System

Each tool provides different features given in Table 3.

The images used for testing were taken from various databases and other sources, as follows:

- Dresden Image Database (Gloe, & Böhme, 2010): Database created for image forensics consisting of approximately 14,000 images from 73 different digital cameras belonging to 25 different companies.
- Wikimedia Commons (*Wikimedia Commons*, 2021): Online database regularly updated, with roughly 73 million images at the time of this research.
- Splicing Database (Hsu, & Chang, 2006): A database of 363 authentic and spliced images.

---

[2]https://fotoforensics.com/

[3]https://www.getghiro.org/

[4]https://github.com/redaelli/imago-forensics

[5]http://www.takenet.or.jp/ ryuuji/minisoft/exif-read/english/

Table 3. Feature lists of DIFTs

| Features | FotoForensics | Ghiro | Imago Forensics | Exif Reader |
|---|---|---|---|---|
| Open-source tool | ✗ | ✓ | ✗ | ✗ |
| Free tool | ✓ | ✗ | ✓ | ✓ |
| MIME information | ✓ | ✓ | ✓ | ✓ |
| Metadata extraction | ✓ | ✓ | ✓ | ✓ |
| GPS localization | ✓ | ✓ | ✓ | ✓ |
| Error Level Analysis | ✓ | ✓ | ✓ | |
| Thumbnail review | ✓ | ✓ | ✗ | ✓ |
| Hash generation | ✓ | ✓ | ✓ | ✓ |
| Hash matching | ✗ | ✓ | ✗ | ✗ |
| Highlight critical data | ✗ | ✓ | ✗ | ✗ |
| Similar picture search | ✓ | ✗ | ✗ | ✗ |
| Hidden pixel extraction | ✓ | ✗ | ✗ | ✗ |
| Colour adjustments | ✓ | ✗ | ✗ | ✗ |
| Annotations | ✓ | ✗ | ✗ | ✗ |
| JPEG% | ✓ | ✗ | ✗ | ✗ |
| Python-based tool | ✗ | ✗ | ✓ | ✗ |
| Web browser backed by VM | ✗ | ✓ | ✗ | ✗ |
| Public website | ✓ | ✗ | ✗ | ✗ |
| Recursive directory navigation | ✗ | ✗ | ✓ | ✗ |
| SQLite export | ✗ | ✗ | ✓ | ✗ |
| CSV export | ✗ | ✗ | ✓ | ✗ |

- GitHub repository (Sevi, 2013): A GitHub repository of images with Exchangeable Image File Format (EXIF) data.
- Google: Various images from Google.

The purpose of these databases is to take images that have *established metadata*. When an image is used to test certain assertions for a tool, the metadata that is determined using the tool can be compared with the actual metadata of the image. This actual metadata is already established to be true for the image before proceeding to test an assertion for a tool. For example, the Dresden Image Database has images with their metadata stated and established. The image metadata determined using DIFTs is compared with the established metadata to check the accu-

racy of the results of the tools. Another point to note is that the file-system metadata of an image is also pre-determined from the established metadata. That is, the creation, modification, and last accessed timestamps are recorded and the results obtained from tools are then compared with the recorded timestamps.

This framework is inherently used to produce *detailed test results* with critical analysis of the tool's behavior under every test. While testing each DIFT, all the core test cases of the framework are carried out and the detailed results are tabulated for compliance or non-compliance. However, the optional test cases to be carried out for each tool are selected based on the features it provides. If the given DIFT does not provide a certain

feature, the test cases for that profile are omitted. The results provide a comparative insight into the functionality and features of each tool. Tables 4, 5, 6 and 7 show example evaluations of various assertions for FotoForensics, Ghiro, Imago Forensics and Exif Reader, respectively.

Table 4. Detailed results sample for FotoForensics-Test Case DIFT-[13-15]

| Assertion | DIFT-CA-09: If the tool provides support for the image file type and reads it without error, it shall determine the date and time of modification and report it in a user-friendly manner |
|---|---|
| Result | Not checked |
| Analysis and Comments | The tool was unable to detect the correct last modified timestamp in this test, which was 9/2/2020 at 5:50 pm. Modification using some software (like PhotoShop) was detected, while modification using other software (like Paint) was not detected. One possible reason is that PhotoShop adds many artifacts and metadata. |
| Screenshot |  |

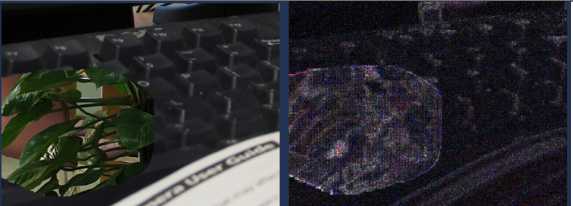Table 5. Detailed results sample for Imago Forensics-Test Case DIFT-26, 27

| Assertion | DIFT-CA-16: If the tool provides support for the image file type and reads it without error, it shall perform the Error Level Analysis (ELA) of the image and display the result in a user-friendly manner. |
|---|---|
| Result | As expected |
| Analysis and Comments | The tool performed Error Level Analysis of the image. |
| Screenshot |  |

Table 6. Detailed results sample for Ghiro-Test Case DIFT-69

| Assertion | DIFT-AO-30: If the tool determines support for GPS localization by the model of the source camera, it shall show the location of the image on a map. |
|---|---|
| Result | As expected |
| Analysis and Comments | The tool was able to indicate the determined longitude and latitude on a map (Joshua Tree, National Park) |
| Screenshot |  |

Table 7. Detailed results sample for Exif Reader-Test Case DIFT-22, 23

| Assertion | DIFT-CA-13: If the tool provides support for the image file type and reads it without error, it shall determine if the image has no metadata (i.e., has been stripped off metadata intentionally) and report it in a user-friendly manner. |
|---|---|
| Result | As expected |
| Analysis and Comments | An image that was stripped off metadata using the Exiftool was uploaded onto the tool. The tool did not upload the image for analysis, indicating there was no EXIF metadata. |
| Screenshot |  |

Table 8. Comparative test results of (core) evaluation of tools

| Profiles | Test Case ID | FotoForensics | Ghiro | Imago Forensics | Exif Reader |
|---|---|---|---|---|---|
| MIME info | 01 | 1 | 1 | 1 | 1 |
| Image file type support | 02 | 1 | 1 | 1 | 1 |
| | 03 | 1 | 1 | 1 | 1 |
| Metadata | 04 | 1 | 1 | 1 | 1 |
| | 05 | 1 | 1 | 1 | 1 |
| | 06 | 1 | 1 | 1 | 1 |
| | 07 | 1 | 1 | 1 | 0 |
| | 08 | 1 | 1 | 1 | 0 |
| | 09 | 1 | 1 | 1 | 1 |
| | 10 | 1 | 1 | 1 | 1 |
| | 11 | 1 | 1 | 0 | 1 |
| | 12 | 1 | 1 | 0 | 1 |
| | 13 | 0 | 0 | 0 | 0 |
| | 14 | 0 | 0 | 0 | 0 |
| | 15 | 0 | 0 | 0 | 0 |
| | 16 | 0 | 0 | 1 | 0 |
| | 17 | 0 | 0 | 1 | 0 |
| | 18 | 1 | 1 | 1 | 1 |
| | 19 | 1 | 1 | 1 | 1 |
| | 20 | 1 | 1 | 1 | 1 |
| | 21 | 1 | 1 | 1 | 1 |
| | 22 | 1 | 1 | 1 | 1 |
| | 23 | 1 | 1 | 1 | 1 |
| GPS localization | 24 | 1 | 1 | 1 | 1 |
| | 25 | 1 | 1 | 1 | 1 |
| Tamper detection | 26 | 1 | 1 | 1 | 0 |
| | 27 | 1 | 1 | 1 | 0 |
| Hash digests | 28 | 1 | 1 | 1 | 0 |
| | 29 | 0 | 1 | 0 | 0 |

Table 9. Comparative test results of (optional) evaluation of tools

| Profiles | Test Case ID | FotoForensics | Ghiro | Imago Forensics | Exif Reader |
|---|---|---|---|---|---|
| Upload | 30 | 1 | 0 | N/A | N/A |
| images | 31 | 1 | 0 | N/A | N/A |
| to tool | 32 | N/A | 1 | 1 | 1 |
| | 33 | 1 | 1 | 0 | 0 |
| | 34 | 1 | 0 | 1 | 0 |
| | 35 | 1 | 1 | 1 | 0 |
| | 36 | 1 | 1 | 1 | 0 |
| | 37 | 1 | 0 | 0 | 1 |
| | 38 | 1 | 0 | 0 | 1 |
| | 39 | 1 | 1 | 1 | 1 |
| | 40 | 1 | 1 | 0 | 0 |
| | 41 | 1 | 1 | 1 | 1 |
| Metadata | 42 | 1 | 1 | 1 | 1 |
| | 43 | 1 | 1 | 1 | 1 |
| | 44 | 1 | 1 | 1 | 1 |
| | 45 | 1 | 1 | 1 | 1 |
| | 46 | 1 | 1 | 1 | 1 |
| | 47 | 0 | 0 | 0 | 0 |
| | 48 | 1 | 0 | 1 | 1 |
| | 49 | 1 | 0 | 1 | 1 |
| | 50 | 1 | 0 | 0 | 1 |
| | 51 | 1 | 0 | 0 | 1 |
| | 52 | 1 | 1 | N/A | 1 |
| Thumbnail | 53 | 1 | 1 | N/A | 1 |
| | 54 | N/A | 0 | N/A | N/A |
| Tamper detection | 55 | N/A | N/A | N/A | N/A |
| Highlight | 56 | N/A | 1 | N/A | N/A |
| JPEG | 57 | 1 | N/A | N/A | N/A |
| quality | 58 | 1 | N/A | N/A | N/A |
| Hidden pixels | 59 | 1 | N/A | N/A | N/A |
| Report | 60 | 1 | 1 | 1 | 1 |
| generation | 61 | 1 | 0 | 0 | N/A |
| Multiple image analysis | 62 | N/A | 1 | 1 | 1 |
| Annotations | 63 | 1 | N/A | N/A | N/A |
| Color adjustments | 64 | 1 | N/A | N/A | N/A |
| Similar images | 65 | 1 | N/A | N/A | N/A |
| By-case distinction | 66 | N/A | 1 | N/A | N/A |
| Multiple users | 67 | N/A | 1 | N/A | N/A |
| Multi-level access system | 68 | N/A | 1 | N/A | N/A |
| GPS localization | 69 | 1 | 1 | N/A | N/A |

*Complete and detailed evaluation reports of all four tools are available on request.

Based on test results of a particular test assertion, compliance and non-compliance are indicated in the result field of the table as *'as expected'* or *'not checked'* respectively, in line with the CFTT standard. The optional features that are unavailable in a tool and therefore omitted are marked 'N/A'.

Documenting detailed results and analyses of the four DIFTs (as illustrated in Tables 4-7) for all 69 test cases in the paper is impractical. Therefore, for the subject of this paper, these results are presented in a concise tabular manner. Tables 8 and 9 provide the core and optional test results of the four DIFTs, respectively. The test result is stated as either 0 or 1 (mapping to *not checked* and *as expected*, respectively). 0 represents the inability of the tool to perform the given test case successfully and 1 represents compliance with the test case. Each test case was tested 5 to 10 times using different images taken from the given databases.

The test results of DIFT tools indicate that majority of the tools conformed to all core test cases except for the modification timestamp (DIFT-CA-09). Additionally, Exif Reader was unable to conform to Error Level Analysis (ELA) which is an important core requirement for tamper detection. In the case of optional features, FotoForensics provided most features except for certain usability features like a multi-level access system, by-case distinction, and multiple users. These usability features, on the other hand, were provided by Ghiro. However, Ghiro was unable to conform to some of the other optional features, as evident by the tabulated results. Imago Forensics and Exif Reader did not provide the majority of the optional features. Based on the test results of the evaluation framework, FotoForensics is the most comprehensive and user-friendly tool, followed by Ghiro, Imago Forensic, and Exif Reader respectively.

## 4.1 Anti-forensic techniques

Anti-forensic techniques are typically adopted by malicious actors to cover their tracks. Concerning images, a prominent and obvious technique adopted is image metadata manipulation. Tools such as Exiftool[6] are widely known and used for metadata manipulation.

In the light of image forensics tools, the single counter to this practice is *hash digests* and *hash-matching*. If hashes of original images are known, it is pretty straightforward to perform hash-matching and identify if the image metadata has been tampered with at all. This reflects in the evaluation framework as well.

# 5. CONCLUSION AND FUTURE WORK

The important aspect of evaluation frameworks is the advancement and practicality of forensic tools and practices. Vaguely, this can be termed as technical hit and trial; since a feature identified as faulty or absent in a forensic tool can be updated or incorporated. Some may argue that the challenge involved in trying and testing every feature of a tool several times is time-consuming and that it should be an automated task. But any product (specifically a software tool) needs to be quality tested before being introduced to mainstream users.

The proposed framework in this research covers all the core features offered by image forensics tools today. It covers optional features as well. The testing framework was tested using four image forensics tools: FotoForensics, Ghiro, Imago Forensics, and Exif Reader. The results indicate FotoForensics as the most efficient, comprehensive, and user-friendly tool followed by Ghiro, Imago Forensics, and Exif Reader, respectively.

---

[6]https://exiftool.org/

It is evident that every tool has some shortcomings but the results obtained from the evaluation framework highlight all the areas that can be improved. The best features can also be combined to develop more comprehensive tools. For example, combining the efficiency of FotoForensics and the usability of Ghiro would make a very comprehensive image forensics tool.

The results of the evaluation of DIFTs presented herein are valid at the time the research was conducted. They might become outdated with future software updates.

As more research is conducted in image forensics, the evaluation framework can be revisited and updated with more profiles (and associated requirements, test assertions, and test cases). More image forensics tools can be tested using the proposed framework. The results of the tool testing (especially the identified shortcomings and missing features in the four tools tested) can be used as feedback by vendors to plan improvements for their products.

# REFERENCES

Allen, T. (2017). *Computer Forensics Tool Testing Program (CFTT).* Retrieved from www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Anobah, M., Saleem, S., & Popov, O. (2014). Testing Framework for Mobile Device Forensics Tools. *Journal of Digital Forensics, Security and Law*, *9*(18). doi: 10.15394/jdfsl.2014.1183

Gloe, T., & Böhme, R. (2010). The Dresden Image Database for Benchmarking Digital Image Forensics. *Journal of Digital Forensic Practice*, *3*(2-4), 150-159. doi: 10.1080/15567281.2010.531500

Heyman, S. (2015). *Photos, Photos Everywhere* (Tech. Rep.). The New York Times. Retrieved from https://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html

Holder, H., & Robinson, L. (2008). *Special Report Test Results for Digital Data Acquisition Tool* (Tech. Rep.). CFTT, NIST.

Hsu, Y., & Chang, S. (2006). Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. In *2006 ieee international conference on multimedia and expo* (p. 549-552). doi: 10.1109/ICME.2006.262447

Kubi, A., Saleem, S., & Popov, O. (2011). Evaluation of some tools for extracting e-evidence from mobile devices. In *2011 5th international conference on application of information and communication technologies (aict)* (p. 1-6). doi: 10.1109/ICAICT.2011.6110999

Piirainen, K., Gonzalez, R., & Kolfschoten, G. (2010). Quo Vadis, Design Science? – A Survey of Literature. In *Global perspectives on design science research* (p. 93-108).

Piva, A. (2013). An Overview on Image Forensics. *ISRN Signal Processing*, 1-22. doi: 10.1155/2013/496701

Qazi, T., Hayat, K., Khan, S., Madani, S., Khan, I., Kolodziej, J., ... Xu, C. (2013). Survey on blind image forgery detection. *IET Image Processing*, *7*, 660-670. doi: 10.1049/IET-IPR.2012.0388

Qureshi, M., & Deriche, M. (2014). A review on copy move image forgery detection techniques. In *2014 ieee 11th international multi-conference on systems, signals and devices (ssd14)* (p. 1-5). doi:

10.1109/SSD.2014.6808907

Redi, J.A., Taktak, W. & Dugelay, J. (2011). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications*, *51*, 133-162. doi: 10.1007/s11042-010-0620-1

Rehman, Z., Ahmad, A., & Saleem, S. (2017). A Brief Survey of Memory Analysis Tools. *NUST Journal of Engineering Sciences*, *10*.

Saleem, S., Popov, O., Kubi, A., & Kwame, O. (2013). Evaluating and Comparing Tools for Mobile Device Forensics Using Quantitative Analysis. In *Digital forensics and cyber crime* (p. 264-282).

Sevi, I. (2013). *EXIF Sample Images.* Retrieved from `https://github.com/ianare/exif-samples`

*Wikimedia Commons.* (2021). Retrieved from `https://commons.wikimedia.org`