Image Forensics Evaluation Framework and Tool Testing

by

Zainab Khalid
00000276295

Supervisor

Dr. Sana Qadir

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Science in Information Security (MS-IS)

Department of Computing (DoC)

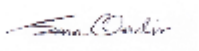
School of Electrical Engineering and Computer Science (SEECS)

National University of Sciences and Technology (NUST)

Dec, 2020

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Image Forensics Evaluation Framework and Tool Testing" written by ZAINAB KHALID, (Registration No 00000276295), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: 

Name of Advisor: Dr. Sana Qadir

Date: 06-Dec-2020

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "Image Forensics Evaluation Framework and Tool Testing" submitted by ZAINAB KHALID have been found satisfactory for the requirement of the degree

Advisor : Dr. Sana Qadir

Signature: _____

Date: 06-Dec-2020

Committee Member 1:Dr. Shahzad Saleem

Signature: _____

Date: 08-Dec-2020

Committee Member 2:Dr. Mehdi Hussain

Signature: _____

Date: 04-Dec-2020

Committee Member 3:Dr. Yousra Javed

Signature: _____

Date: 05-Dec-2020

Dedicated to my Daji, with love and gratitude.

CERTIFICATE OF ORIGINALITY

I hereby declare that the research paper titled "***Image Forensics Evaluation Framework and Tool Testing***" is my own work to the best of my knowledge. It contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NIIT or any other education institute, except where due acknowledgment is made in the thesis. Any contribution made to the research by others, with whom I have worked at NIIT or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic is acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: Zainab Khalid

Signature: 

ACKNOWLEDGEMENTS

I would like to extend my gratitude to my supervisor, Dr. Sana Qadir, for keeping me motivated and guiding me comprehensively throughout this journey. This research work would not have been possible without her kind supervision. Thanks to all the GEC committee members: Dr. Shahzad Saleem, Dr. Mehdi Hussain, and Dr. Yousra Javed for their valuable insights and suggestions.

Thanks to my family and friends for their encouragement and support.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIA – Automatic Image Annotation
AO – Optional Assertion
BMP – BitMaP
CA – Core Assertion
CCD – Charge Coupled Device
CFTT – Computer Forensics Tool Testing
CMOS – Complementary Metal Oxide Semiconductor
CR – Core Requirement
CRF – Camera Response Function
DCT – Discrete Cosine Transform
DIFT – Digital Image Forensics Tool
DILC – Digital Image Life Cycle
DIS – Draft International Standard
ELA – Error Level Analysis
EXIF – EXchangeable Image File Format
GIF – Graphic Interchange Format
GPS – Global Positioning System
IEC – International Electrotechnical Commission
IPTC – International Press Telecommunications Council
IS – Information Systems
ISO – International Organization for Standardization
JPEG – Joint Photographic Experts Group
MIME – Multipurpose Internet Mail Extensions
NIST – National Institute of Standards and Technology
OBIA – Object Based Image Retrieval
OR – Optional Requirement
OVA – Open Virtualisation Format
PXR – PiXaR file
PNG – Portable Network Graphics
PRNU – Photo Response Non Uniformity
PSD – PhotoShop Document
SVM – Support Vector Machine
TIFF – Tagged Image File Format
UCS-2 – Universal Code Character Set
WebP – Web Picture format
XMP – eXtensible Metadata Platform

ABSTRACT

The phrase ‘seeing is believing’ has been validated to the point where any proposition to the contrary sounds bizarre. The boom of the digital camera, photography, and social media has drastically changed how humans live their day-to-day, but this normalisation has been accompanied by malicious agents finding new ways to forge and tamper with images. Primarily, the motivation is unfair or unlawful monetary gain.

Disinformation in the photographic media realm is an urgent threat. There are so many image editing tools available today that it is almost impossible to differentiate between a photo-realistic and an original image. 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 for academic research. This research work proposes an evaluation framework for image forensics tools.

The proposed framework is based on the conformance methodology of testing which employs test assertions and test cases. It is then tested by evaluating four image forensics tools namely FotoForensics, Ghiro, Imago Forensics, and Exif Reader.

The framework provides a comparative insight into the tools based on test results. The evaluation of the image forensics tools revealed that FotoForensics provides a lot of optional features efficiently in addition to core features. The test results of Ghiro conformed to its usability features while Imago Forensics and Exif Reader lacked in providing a majority of optional features. This comparison can provide the information necessary for users to make intelligent choices about tools and it can help vendors shortlist areas of improvement in their tools.

Keywords:

Image Forensics, Tool Testing, Evaluation Framework

1. INTRODUCTION

This chapter contains the following:

- Section 1.1 provides background of image forensics.
- Section 1.2 highlights the motivation of this research.
- Section 1.3 presents the problem statement.
- Section 1.4 states the research objectives.
- Section 1.5 defines the scope of this research.

1.1 Background

Image forensics is a relatively new sub-discipline of digital forensics. It has received little attention compared to the more popular sub-disciplines (like network forensics, mobile forensics, database forensics, and firewall forensics) that have been the focus of most research in this field.

Research in image forensics started in the early 2000s, coherent with the normalisation of digital cameras and mobile phone cameras [1]. The explosive use of the camera was accurately predicted by a New York Times report which estimated that by late 2010s, 1.3 trillion pictures would be taken annually [2]. This Butterfly Effect has had a life changing impact on how people go on about their lives today, both positively and negatively.

One of the most significant negative impacts has been due to the easy availability of free and open-source editing software and tools for images like Photoshop CC, Lightroom, GIMP, Snapseed, and Corel Paintshop Pro. There have been incidents where people have leveraged forged images for their malicious intentions. For example, a Malaysian politician Jeffrey Wong Su En claimed he was knighted by Queen Elizabeth to support his campaign and used a forged image to back his claim [1].

Owing to the massive number of pictures taken and shared online each year, images have trickled into almost every industry. In some industries, however, like news industry, medical imaging, social media, and e-commerce, they play a defining role [3]. But most importantly, they are crucial in trials and criminal investigations.

1.1.1 Digital Forensics

According to the National Institute of Standards and Technology (NIST), digital forensics is "the field of forensic science that is concerned with retrieving, storing and analysing electronic data that can be used in criminal investigations" [4]. This includes data from various sources such as computers, storage devices (hard drives and soft drives), mobile phones, and cloud storage [4]. The data/information that can potentially serve as a piece of evidence in a criminal case is called *digital evidence*.

There are many cases that involve image media or video that serve as digital evidence; they can make or break a case. That being said, the issue of admissibility of these media in court is also

questionable owing to the free editing tools available that allow people to tamper with images easily. This means that 'seeing is no longer believing' and there is a need for image forensics practices and tools to not only differentiate tampered images from real ones but also to validate the images for admissibility in court [5].

1.1.2 Image Forensics

Image forensics is a research field that aims at validating the authenticity of images by recovering information about their history [1]. This includes source camera identification and forgery detection [1].

The image forensics techniques are categorized into:

- **Active techniques** which include watermarks and digital signatures computed by the camera [3]. These techniques are fundamentally preventive and require prior information about the image and the camera itself. In this approach, the watermarks or digital signatures are checked for modifications [3]. The camera is used to grant authenticity of the images and any change indicates a doctored image. This scenario is however impractical, because in common forensics scenarios involving images, the camera is not available for the investigators to analyze.
- **Passive techniques** do not require any prior information about the camera for forensic analysis [3]. These techniques are responsive in their nature and determine the history of the image using the image data only.

Among the active and passive techniques, the most common scenario in an on-going investigation is called the *passive blind forgery detection*. In this case, the investigator does not have any information about the image such as camera make/model or the post-processing operations performed. The investigator just has the image to work with. In other words, the investigator has to carry out a blind detection of image forgeries. Hence, the passive blind forgery detection is a major highlight in the research done in image forensics. Holistically, image forensics answers the following questions [5]:

- What was the source camera of the image?
- Was the image, by any means, forged or tampered with?
- Is the image entirely photo-realistic?

A photo-realistic image is graphic content that is created digitally. It is visually as real as an actual photograph of a real scene [5]. This makes it hard for analysts to distinguish between real and photo-realistic images.

1.2 Motivation

During the film-photography era, images subject to admissibility checks in court were required to be presented with negatives of the images [6]. Tampering with a film-based image is harder and any modifications done during the development process of the photo from its negative was

detected relatively easily. A simple comparison with the negative would reveal forgeries. Digital images, on the other hand, are very easily doctored with no original reference for comparison, and thus questionable as digital evidence.

Several cases have highlighted the importance of having suitable criteria for deciding on the admissibility of an image in a courtroom. The State vs. Swinton case from 2004 is one such example [7]. Swinton was charged for murdering a 28 year old woman. The photographs of abuse marks on the victim's body were enhanced by the prosecution in order to make a match of the marks to the suspect's mould of teeth. The defendant, however, launched an appeal on the ground that the image was enhanced using Photoshop which puts a question mark on its admissibility in court. As a result, the court had to rule in favour of the defendant and disallow the photos [7].

In the OJ Simpson murder trial, the Time magazine published a darkened image of him on the cover. The magazine immediately faced backlash for having a racist agenda, and had to change the cover to the original image. The editor of the photo defended himself by claiming that he did not have any racist intentions but merely wanted to express the dramatic nature of the case [1].

Nowadays, there are many tools that can be useful for the forensic analysis of images. To ensure reliability, these tools need to be evaluated using a standard. This research work is centred upon developing the criteria of this standard. Once an image has been evaluated using a tool that conforms to this standard, its result can be considered valid. It can be admissible in the court of law or used for other purposes. In this regard a few questions are important:

- What core functionalities must a tool have to qualify as an image forensics tool?
- What criteria (e.g. performance and functionalities) should be used for tool comparison?
- How are tools tested?
- What models are followed to design frameworks for tool testing?

These questions originate from the requirement that results produced by tools need to be reliable, consistent, and are admissible as digital evidence.

1.3 Problem Statement

The Computer Forensics Tool Testing (CFTT) Project by NIST is working on tool testing by designing frameworks for each computer forensics discipline. These frameworks are based on conformance and quality testing methods that are internationally accepted [8]. CFTT has designed frameworks for a range of tools like Hard Drive Imaging Tools, Software Hard Drive Write Protect, Hardware Hard Drive Write Protect, Deleted File Recovery, Forensic Media Preparation, Forensic String Searching, and Mobile Forensics Data Extraction [8]. However, no such framework has been designed for image forensics by CFTT or any other project or organisation.

So the need of the hour is to achieve validation of tools for standardisation. A framework following standard methodology of design needs to be developed and evaluated for image forensics.

This research work adopts the standard CFTT methodology for developing a framework for image forensics tools. The framework is capable of evaluating these tools with respect to features and functionalities. Consequently it produces findings about the expected and unexpected results for tools in a meaningful way [8]. The conformance methodology of testing adopted by CFTT evaluates tools using *test requirements*, *test assertions*, and *test cases*. The same methodology will be used in this research. The second part of this research tests four tools using the designed framework and presents the results obtained through tool testing. This helps consumers make better choices in tools. It also helps developers make needed improvements in their tools in addition to setting a benchmark for tool validation, admissibility, and standardisation.

1.4 Research Objectives

- **Develop** an **evaluation framework** for image forensics tools based on the CFTT project methodology of conformance testing. This step involves the development of test requirements, test assertions, and test cases for image forensics tools. The main objective of designing this framework is *standardisation.* This is done by creating a benchmark against which tools are evaluated in order to qualify as valid image forensics tools.
- **Test** the **evaluation framework** using four image forensics tools. Distinguish between image forensics tools and other tools that do not qualify because they do not have the core functionalities required for an image forensics tool.

1.5 Scope

The criterion for choosing the tools for testing was easy availability. The shortlisted tools are FotoForensics [9], Ghiro [10], Imago Forensics [11], and Exif Reader [12]. Ghiro is an open-source tool while the other three are free tools. The scope of this research includes:

- Photographic image media of all formats (e.g. JPEG, PNG, and TIFF) and source cameras such as Nikon, Canon, Android, and iPhone.
- This framework is limited to image forensics tools only. For the purpose of this research, the four mentioned tools i.e. FotoForensics, Ghiro, Imago Forensics, and Exif Reader will be evaluated.
- The testing environments are Windows and Linux. Any other environment a tool might operate in can also be used with this framework.
- The images used for the test cases were taken from the following databases:
  - The *Dresden Image Database* is a database that was created for image forensics and consists of approximately 14,000 images from 73 different digital cameras belonging to 25 different companies [13].

- The *Columbia Uncompressed Image Splicing Detection Database* is a database of 363 authentic and spliced images, made to detect splicing in images [14].
- The GitHub repository of images with Exchangeable Image File Format (EXIF) data [15].
- Images selected by the researcher from Google images.
- A small collection of pictures taken by the researcher using Nikon D5300, Samsung S4, and Samsung A20s cameras.

2. LITERATURE REVIEW

This chapter contains the following:

- Section 2.1 explains image metadata types.
- Section 2.2 explains the process of capturing images.
- Section 2.3 discusses forgery detection techniques.
- Section 2.4 discusses related works.

2.1 Image Metadata

Metadata is data about data. Image metadata includes technical and administrative information about the image file. This metadata can be used in image forensics to aid in reconstructing the history of an image to detect forgeries. It can be categorized into the following types:

- Exif Metadata
- International Press Telecommunications Council (IPTC)/eXtensible Metadata Platform (XMP) Metadata

2.1.1 Exif Metadata

Exif metadata includes technical information about an image. This type of metadata is generated by the source camera. It consists of camera settings. Exif metadata fields are listed below:

- *File type* is file format of an image.
- *File size* is size of an image in bytes/megabytes.
- *Make* is the manufacturing company of a camera.
- *Model* depicts the type of camera.
- *Camera ID* is a unique serial ID of the camera. This serial ID can be used to distinguish between cameras of the same make and model.
- *Resolution* is the number of pixels in an image.
- *Timestamp* refers to the creation, modification, and last accessed date and time of an image.
- *ISO* refers to sensitivity of a camera to light. It can be adjusted depending on the light setting in a scene. If the scene is dark, ISO can be adjusted to cater for the lack of light.
- *Aperture* of a camera is used to control the amount of light entering the camera through its lens. The aperture is expressed in f-numbers. For example, f/1.4 indicates more light is entering through the lens as compared to aperture value of f/16.
- *Shutter speed* indicates the time window during which the shutter of a camera is open while capturing the image.
- *Orientation* of an image indicates its horizontal or vertical orientation.
- *Colour-space* indicates whether the image is coded in RGB, YCbCr or any other available colour spaces.

- *Bit-depth* indicates how many bits were used to store information in each colour channel of the colour space. An image can be stored in 8, 12, 14 or 16 bit depth.
- *Focal Length* indicates the level of magnification of a camera lens while capturing an image.
- *Subject distance* is the approximate distance of a subject from the camera.
- *Flash setting* contains information about the flash of a camera while capturing an image.
- *GPS information* indicates the location where an image was captured.

2.1.2 IPTC/XMP Metadata

The IPTC/XMP metadata includes administrative information about an image. The ownership and copyright information can be added by the photographer. This type of metadata is useful in stock photography. XMP metadata is the latest version of IPTC metadata. Most often they are used interchangeably in applications. They contain the following fields:

- *Tag/Description/Keyword/Comment* fields can be added to indicate ownership or convey a message.
- *Copyright protection* field can be added to indicate that the image can be used under a particular licence obtained from the owner.

2.2 Digital Image Life Cycle

Source-camera identification and forgery detection are the fundamental questions of this domain. Answers to these questions lie at the heart of the **Digital Image Life Cycle (DILC)**. The DILC is an amalgam of all the processes that an image goes through from the moment a camera lens captures a scene to its storage on the memory. It consists of the following three phases:

- Image Acquisition
- Image Coding
- Image Editing

These three phases are what make an image [16] [5]. Figure 2.1 shows the process flow of the DILC.

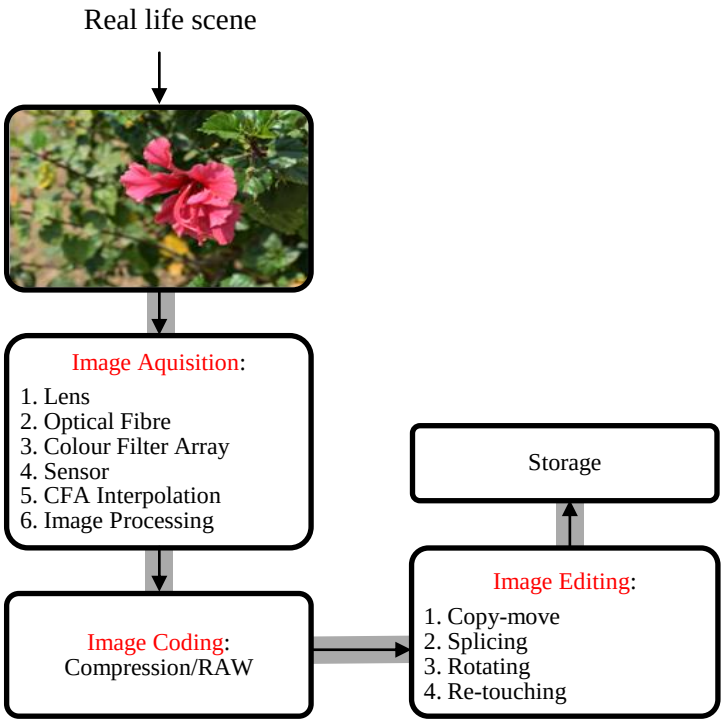


Fig 2.1 – Digital Image Life Cycle

Each step from acquisition of the image to its storage in memory introduces *artefacts*, unique to every camera, lens, the type of each process adopted for that instance, coding format, and editing techniques. These artefacts are called *fingerprints* or *signatures* [16]. In other words the acquisition, coding and editing phases create fingerprints that can later be used for forensic analysis of the images [5]. These fingerprints if unchanged can reveal significant metadata about an image. On the other hand, if they are changed they reveal traces that an image has been tampered with. The following sections discuss these three phases in detail along with the possible fingerprints each phase can introduce into an image.

2.2.1 Image Acquisition

The image acquisition phase encompasses the processes that range from the capture of light from the real life scene to the in-camera functions performed on that captured scene [16] [5].

- **Lens:**
  The camera lens is used to capture the scene in the form of light. This light is focused onto the sensor. A lens introduces aberration fingerprints in the final image, such as chromatic aberration. Every camera make and model has different types of lenses which make the resulting aberrations different in each case. This can serve as a fingerprint in the forensic analysis process.
- **Optical Fibre**
  The light captured by the lens passes through an optical fibre.

- **Colour Filter Array**
  The light then passes through a Colour Filter Array (CFA) which captures the colour information of the scene. There are different CFAs present and distinguishing them in different cameras can be potential key information.
- **Sensor**
  The colour information from the CFA falls on the Charge Coupled Device (CCD) or Complementary Metal Oxide Semiconductor (CMOS) sensors which translate information into pixel data. Sensors are susceptible to damage, either during the manufacturing process or during use. Even minor flaws in the sensor are translated into an image in the form of noise called Photo Response Non-Uniformity (PRNU). Since every sensor has unique PRNU, this fingerprint is useful in the forensics process.
- **CFA Interpolation**
  The process of demosaicing the image data obtained from the sensor in order to turn it into a digital image is called CFA interpolation [16] [5]. The demosaicing artefacts can be used to detect forged regions.
- **Image Processing**
  The last stage in the acquisition phase comprises all the operations that a camera may perform on the obtained image before it is stored on the memory. This can include enhancements and sharpening processes.

2.2.2 Image Coding

The image coding stage, by means of compression, stores the image digitally [16] [5]. Compression can be lossy or lossless. Lossless compression retains all the image data and stores it as it is. On the other hand, if memory on the storage device is limited, lossy compression is employed which discards redundant image data to save storage space. This type of compression is essentially a trade-off between image quality and image size.

An image can be binary, gray-scale, coloured or multispectral and depending on how the image coding is performed it is categorized into a range of image formats that we have today, some of which are listed below [17] [18]:

- Joint Photographic Experts Group (JPEG)
- BitMaP (BMP)
- Tagged Image File Format (TIFF)
- Portable Network Graphics (PNG)
- PhotoShop Document (PSD)
- Graphics Interchange Format (GIF)
- RAW
- Web Picture format (WebP)
- PiXar file (PXR)

These image formats introduce different fingerprints because their coding methods vary from one format to the next. A JPEG image, for example, is formed using quantization tables and Discrete Cosine Transform (DCT). The fingerprints added by these processes can later be used to identify the JPEG image and any traces of tampering.

2.2.3 Image Editing

Image editing techniques are categorized into:

- **Copy-move forgery** where a part of an image is copied and pasted to another part of the same image [19]. This introduces duplication in the forged image. Figure 2.2 shows an example of this type of forgery.

Fig 2.2 – Copy-move Forgery

- **Image Splicing** where a part of an image is cut and pasted onto another image. These images are called *composite images* because they are a product of more than one image. Image splicing has been widely exploited for creating misleading images for unlawful purposes. Figure 2.3 shows an example of this type of forgery.

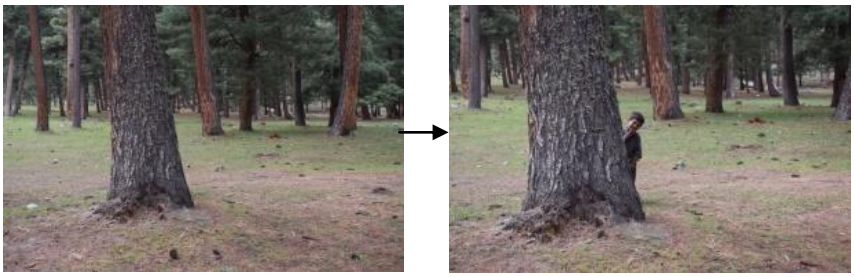


Fig 2.3 – Image Splicing

- **Re-touching** is all the post-processing done on the image [20]. This may include a wide array of modifications such as listed below [20]:
  - Contrast adjustment
  - Colour enhancement
  - Colour modification
  - Rotation
  - Zoom
  - Scaling
  - Cropping
  - Filtering

  Figure 2.4 shows an example of image re-touching.

Fig 2.4 – Re-touching

2.3 Forgery Detection Techniques

The Digital Image Forensics Tools (DIFT) use fingerprints (to reveal the manipulation history), examine metadata (if available), and other functionalities. Different fingerprints are used by different forgery detection techniques. These techniques vary depending on variables like forgery methods used to tamper with an image. They can be classified into the following categories [19]:

- Pixel-based techniques
- Format-based techniques
- Camera-based techniques
- Physics-based techniques
- Geometric-based techniques

2.3.1 Pixel-based Techniques

Common forgeries performed in image forensics are pixel-level forgeries such as copy-move, splicing and re-touching. Pixel-based techniques are used to detect these forgeries [19]. These techniques use statistical fingerprints or other correlation artefacts introduced in an image due to forgery [19]. Both spatial and transform domains are used by these techniques for detection [19]. Given the fact that copy-move forgery, splicing and retouching are the most common methods of forgery, pixel-based techniques of detection are one of the most common detection techniques.

In theory there are several tools that explore the possibility of employing fingerprints for forensic analysis using pixel-based techniques. These tools however perform singular tasks like detecting duplicate images [21], and copy-move forgery detection [22].

[21] proposes and tests a tool Magec, an image searching tool that searches for duplicates of an image specified by the user. A duplicate of an image is a copy-pasted version of it. Magec returns the duplicates of an image even if the names and other attributes have been modified. It detects identical images using the original image modification attribute as a signature [21]. It also detects hidden images. According to the authors, it is more efficient at detecting image duplicity than other tools. A drawback in this research work is that it performs only one task.

In copy-move forgery detection, correlation artefacts in the image are used. An image tampered using copy-move forgery contains portions of the same image at different locations. To detect such forgery, **block-based** or **keypoint-based** approaches are used [19]. In block-based approaches, an image is divided into blocks. These blocks are matched using a matching algorithm to detect similar blocks [19]. This technique is fairly computational. In keypoint-based approaches, the key points in an image are used to create feature vectors [19]. Different feature vectors are matched to detect similar ones.

An example of use of these copy-move forgery detection techniques is proposed in [22]. This paper proposes NO-SHAM, a tool that detects any images that have been tampered with using copy-move forgery. Usually detection of copy-move forgery is done using either **block-based approaches** or **keypoint-based approaches**. The proposed tool uses a hybrid approach where it uses both the techniques based on relativity [22]. This saves computation time and achieves better accuracy. This tool performs one function; it cannot detect other types of forgeries e.g. splicing and retouching modifications in an image. Other functions may include metadata analysis or calculating hash digests of the image.

[25] is another research paper that proposes a technique to detect copy-move forgery. They adopt a **DCT based feature extraction technique** to achieve detection with block sizes of up to 64×64 [25]. The blocks are first DCT transformed, followed by feature extraction. The features are then subjected to a detection algorithm.

[26] proposes a tamper detection technique. It uses a **noise histogram** to act as a feature to detect any tampering done with the image without any prior knowledge of the image [26]. The difference of noise in the original and tampered parts of the image is leveraged to detect manipulated areas. This technique gives a performance accuracy of 91.31% on average [26].

[28] proposes a classifier for detection of image splicing. This classifier works on the concept that each image has different colour information. This colour information is a combined result of the hardware of the camera and the software settings. When a part of one image is pasted onto a second image it will introduce a difference in the colour information which the authors attempt to detect by training a classifier.

Another example of pixel-based forgery detection is via **histogram analysis**. [25] proposes a forgery detection algorithm which detects contrast enhancement in images using histogram analysis. A visual example of this is shown in Figure 2.5. This figure shows an image with contrast enhancement re-touching. The image contrast is enhanced to 100%. The difference between the two images is still very minimal. The visual difference may not be obvious to the naked eye if the enhancement is done at a lower percentage.

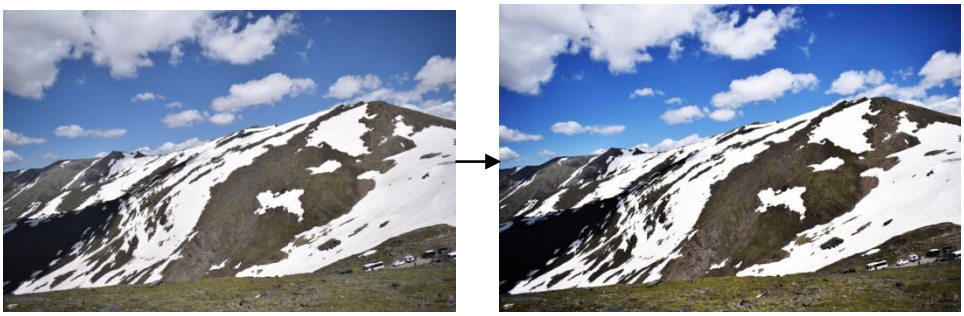


Fig 2.5 – Original Image vs. Contrast-enhanced Image

However, if the histograms of both the images are analysed and compared against each other as shown in Figure 2.6, it gives a clear indication that the image was modified.

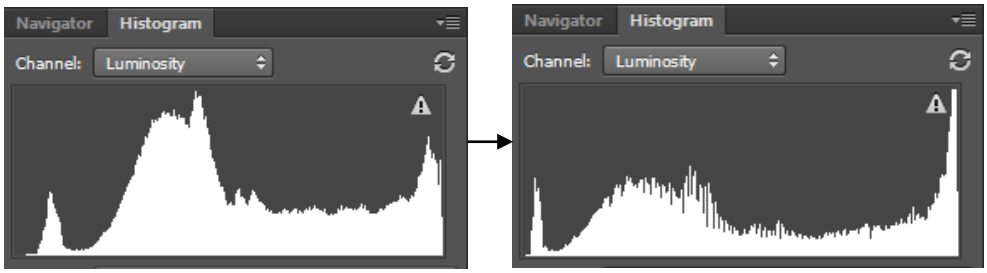


Fig 2.6 – Histogram of Original Image vs. Modified Image

2.3.2 Format-based Techniques

Usually if an image is compressed after forgery using any format of image coding, it becomes more difficult to detect the forgery. This is due to the loss of information during image compression. However, some format-based forgery detection techniques employ these formats to aid the detection.

There are several image formats that are used for image coding. However, format-based techniques use JPEG to perform forgery detection. This is mainly because this format is the most common.

An example of forgery detection using image coding fingerprints is **Error Level Analysis (ELA).** ELA is a tamper detection technique that has evolved to be the most used technique for tamper detection in tools today owing to its simplicity and efficient execution. This technique

uses the differences in compression levels in a compressed image format to determine the presence of any abnormal inconsistencies. Usually the forged regions in the image have different compression levels as compared to the rest of the image.

Figure 2.7 shows an example of ELA performed using a DIFT, on a picture that was slightly modified using image splicing (left side of the image). Here, ELA gives a visual representation of the forged area in this image. Usually, the manipulations are obvious around the edges of spliced objects in the image under analysis. ELA gives an image forensics analyst a means of observing the variations in an image and to detect exactly where tampering was done. This means that ELA mostly relies on the observation skills of the analyst.

One limitation of ELA occurs when a JPEG has been resaved more than several times (which means that the JPEG% of the image is relatively low). It loses a large amount of image data because of compression, and that leaves little room for ELA to work.

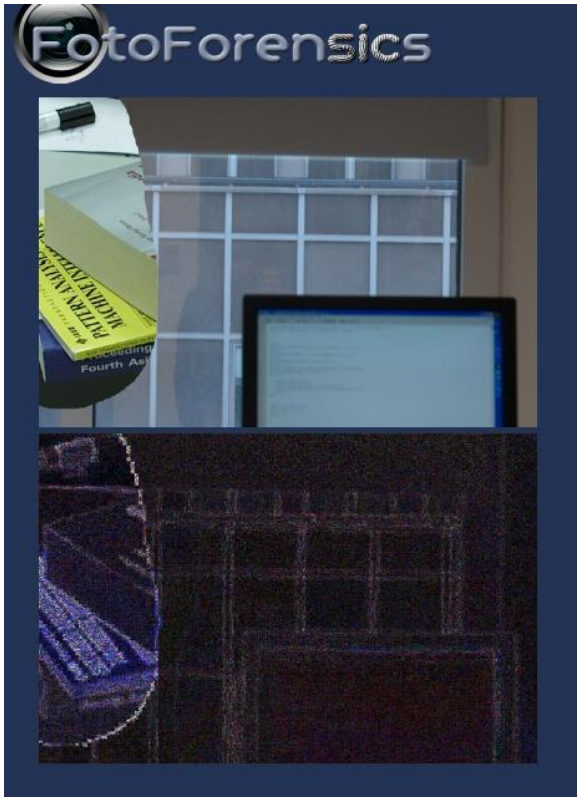


Fig 2.7 – Error Level Analysis using FotoForensics

[27] proposes a JPEG file carving tool that automates the process of recovery of fragmented JPEG images. The results show better performance in recovery and speed as compared to other tools such as APF [27].

2.3.3 Camera-based Techniques

The DILC describes the process of capturing an image and storing it in the memory using a camera. This involves the lens, sensor, and CFA along with other elements. The techniques that use source camera fingerprints to detect forgeries are called camera-based techniques. These techniques involve using fingerprints such as lens aberrations, sensor noise, and CFA interpolation [19].

[18] discusses a forgery detection technique which uses lateral chromatic aberration as a fingerprint. An image with forged regions has inconsistencies in lateral chromatic aberration across those regions. This can be used to indicate the regions that were tampered.

[24] performs experiments to evaluate a source camera identification technique. This technique uses noise introduced in images by the sensor. The results indicate that in some cases the technique withstands image-processing, while in other cases it does not [24].

2.3.4 Physics-based Techniques

Physics-based techniques in forgery detection involve light settings of images. If an image has been forged using multiple images, the parts from different images will have different light settings because the environment of each constituent image is different. The cameras may have different light settings while capturing these constituent images. However, physics-based techniques are not common as compared to pixel-based and format-based techniques.

[30] proposes a physics-based technique that analyzes the light components of objects in an image and determines inconsistencies throughout the image. The technique is tested for different sample images. It is concluded that the algorithm works efficiently in scenes where there is one light source (like outdoor scenes) as compared to indoor scenes where there are multiple sources of light.

2.3.5 Geometric-based Techniques

When a camera captures an image it projects a *principal point* at the centre of the image [19]. When images are forged, these principal points are dislocated. This means that the actual *perspective* of the image is off. Geometric-based techniques in forgery detection use principles in projective geometry to analyse the perspectives of an image and detect forgery [19].

[31] proposes a geometric-based technique and for image splicing detection. Firstly, the spliced boundary is manually guessed which is used to determine the geometry invariants. These geometry invariants are used to compute Camera Response Function (CRF) [31]. Cross-fitting techniques are then used to determine errors which are fed to a Support Vector Machine (SVM) classifier to determine if the image was spliced or authentic [31].

Table 2.1 presents a comparative analysis of the tools and algorithms discussed.

Tool/Algorithm	Technique	DILC Stage	Advantage	Limitation
Magec [21]	Pixel-based technique	Image editing	• Detects duplicate images using image modification signature as an attribute. • Takes less time as compared to others tools.	The tool detects copy-move forgery only.
NO-SHAM [22]	Pixel-based technique	Image editing	• Uses hybrid approach to detect copy-move forgery. • Applicable to smooth and non-smooth images.	The tool detects copy-move forgery only.
[25]	Pixel-based technique	Image editing	• Uses DCT and feature extraction to detect copy-move forgery. • Robust against JPEG compression.	• The tool performs single task. • Limited block size.
[26]	Pixel-based technique	Image editing	• Uses noise histogram to detect tampered regions. • Performance accuracy of 91.31%.	The tool performs single task.
[28]	Pixel-based technique	Image editing	• Classifier based on colour representation to detect image splicing. • Robust to JPEG compression.	• Classifier trained with Macbeth colour chart only. • The tool performs single task.
JPEG file carving tool [27]	Format-based technique	Image coding	• Automates recovery of fragmented JPEG files. • More efficient than APF tool.	Limited to JPEG files.
ELA	Format-based technique	Image coding	• Detects tampered regions in an image. • Easy to implement. • Less computation.	• Results depend on observation of analyst. • Less effective for images compressed multiple times.
[18]	Camera-based technique	Image acquisition	• Detects forgery using lateral chromatic aberration.	• This technique is ineffective for smooth regions in an image.
M-FAT [24]	Camera-based technique	Image acquisition	• Uses sensor noise for source camera identification.	• Not robust to post-processing.
[30]	Physics-based technique	Image editing	• Detects inconsistencies in light components of an image.	• Works efficiently only for images with few light sources.
[31]	Geometric-based technique	Image editing	• Detects image-splicing forgery using geometry invariants and CRF. • 87% accuracy on a dataset of 363 images.	• This technique is semi-automatic. • Detects image splicing only.

Table 2.1 – Comparative Study of DIFT and Algorithms in Literature

2.4 Metadata Analysis in Image Forensics

In addition to forgery detection techniques which are a significant part of DIFT, metadata analysis is also important. Metadata can be used to connect the dots in forensic analysis process because it reveals details about the source camera and the settings when an image is captured.

An example of how metadata can be used to aid the image forensics process is explained. Usually the software and tools used to perform image editing leave traces of their use in the metadata of the image. For example, the image retouched in Figure 2.8 was edited using Photoshop CC. The use of Photoshop introduced metadata fields in the image that can easily be detected and analysed using image forensics tools. This metadata reveals the modification and creation timestamps of the image along with other details.

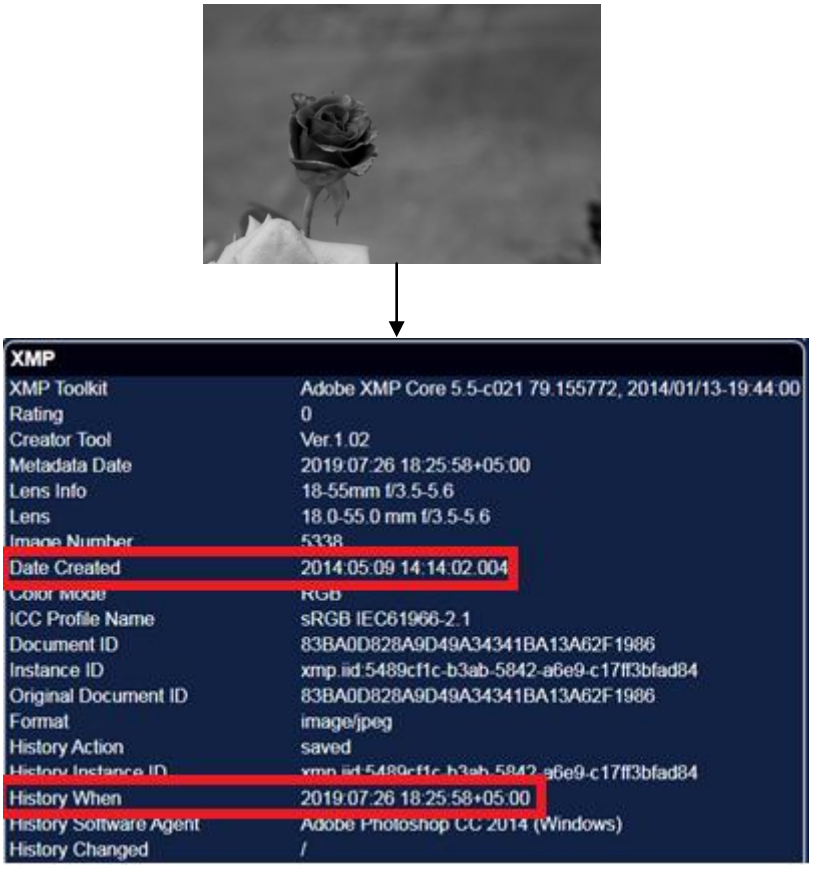


Fig 2.8 – Forgery Detection via FotoForensics

[23] proposes a tool which provides:

- Automated metadata analysis
- Forensic analysis of the Windows 7 Recycle bin

For metadata analysis, it uses **Exiftool** which is a Windows command line tool that performs metadata analysis and manipulation. The key functionality provided is to take the metadata obtained from the Exiftool and automatically compile all the results in one report. It also performs GPS localisation using Google Earth. In other words, if an image was captured with a camera that had GPS enabled, it will locate the place where the image was taken using Google Earth. The second part of this tool performs forensic analysis of deleted files using the Windows 7 Recycle bin. It recovers artefacts left by these files that are not permanently deleted by the user but only sent to the Recycle Bin [23].

This tool relies on Exiftool and Google Earth so any drawbacks or inaccuracies in these tools will reflect in the results produced for forensic analysis. Also, Exiftool is not, in the strict sense, an image forensics tool. It extracts and manipulates image metadata but there are other core requirements for an image forensics tool e.g. forgery detection that it does not have. Nonetheless, Exiftool is a valuable tool that has been used frequently for image metadata analysis, manipulation, and deletion. Many existing tools use it in the backend for EXIF metadata analysis.

[29] aims at automating the extraction of thumbnails of deleted images. These thumbnails are produced by different image viewers as opposed to the OS and thumbnail recovery from the Recycle bin.

2.5 Related Works

This section reviews the methodologies used for tool evaluation and framework design in other digital forensics disciplines with reference to the CFTT project. Test specifications, test assertions and test cases are main components of these frameworks. This kind of benchmark provides stakeholders such as consumers with relevant information to make intelligent choices regarding their tools. It also provides developers with criteria to assess their tools and figure out possible improvements for maximum optimality.

2.5.1 CFTT-based Evaluation Frameworks that use Conformance Methodology

2.5.1.1 Testing Framework for Mobile Device Forensics Tools

[32] is an extension to the evaluation framework developed by the CFTT for mobile device forensics tools. The authors have proposed, based on the conformance testing methodology, additional test assertions, and test cases that cover more profiles in the domain of mobile device forensics. They contribute 16 assertions in 5 profiles to the evaluation framework. This includes one interesting profile of anti-forensics techniques for smart-phones. They also test out tools

such as XRY, Cellebrite's UFED and Paraben's Device Seizure [32] [33]. The tests performed to evaluate these tools include the ones designed by CFTT and the ones added by the authors. The results showed XRY to be the most comprehensive tool.

This research makes one significant contribution about the term *support* and how it can be evaluated and quantified. The first part is to define what it means when a vendor claims that a tool supports certain functionalities, features or mobiles [32]. This includes defining a criteria or standard to validate the support claimed by vendors. The authors introduce a grading equation that can be employed to quantify the results obtained from the evaluation framework. The grading equation weighs the optional assertions to be half of the core assertions. This grade-based system for evaluation of tools is a first in the test assertion/test case methodology of evaluation. No such grading-based system has been employed by the CFTT project for conformance testing frameworks.

2.5.1.2 A Brief Survey of Memory Analysis Tools

This research work is also based on the CFTT project. It designs an evaluation framework for Windows memory forensics tools.

There are two parts; the first part is a survey of several memory forensics tools. They are 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 [34].

The second part develops a framework that uses the conformance methodology for testing to develop the test specifications/requirements, and consequently develop the test assertions and test cases [34] [35]. The main contribution is the framework design. Additionally, they provide traceability matrices that relate the test requirements to the test assertions.

2.5.2 CFTT-based Evaluation Frameworks that use Quantitative Methodology

2.5.2.1 Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis

This research work [36] [37] presents the evaluation of mobile device forensics tools. However, they use a quantitative analysis methodology to provide a mathematical basis for evaluation.

This work uses the CFTT, NIST tool specifications and test cases for mobile forensics tools to evaluate the XRY 5.0 and UFED Physical Pro tools. They obtain results from the CFTT framework [36] [37] [38]. These results are quantified using a rating metric that uses **Confidence Interval (CI)** [36]. The mathematical evaluation includes determining error rates of the tools called the **Margin of Error (MoE).** The MoE results are subjected to hypothesis testing and the tools are rated.

Table 2.2 presents a comparative analysis of the related works.

	Testing Framework for Mobile Device Forensics Tools [32] [33]	**A Brief Survey of Memory Analysis Tools [34] [35]**	**Evaluating and Comparing Tools for Mobile Device Forensics Using Quantitative Analysis [36] [37] [38]**
Forensics Discipline	Mobile Forensics	Windows Memory Forensics	Mobile Forensics
Methodology	Conformance Methodology	Conformance Methodology	Quantitative Methodology
Tools Tested	• UFED v1.1.0.5 • XRY v6.3.1 • PARABEN v4.0	• Volatility Framework • Redline • Rekall Framework • FTK Imager • Memdump Extractor • Internet Evidence Finder	• UFED v1.1.3.8 • XRY v5.0
Contributions	• Development of 16 new assertions in 5 profiles on top of existing framework of CFTT for smart phones. • Evaluation of the given tools. • Defining the term "support" with respect to tools using a grading equation to quantify results.	• Development of specifications for memory forensics tools. • Development of test assertions and test cases. • Use of traceability matrices • Testing each test case using the given tools. • Test results in the form of screenshots.	• Evaluate tools using CFTT framework for smart phones. • Development of rating metric that uses CI. • Determination of error rates using MoE. • Hypothesis testing to rate tools.

Table 2.2 – Comparative Study of Related Works

With the rapid pace of research in other sub-disciplines there is a growing interest in image forensics techniques and tools. There are new techniques being explored like ELA and some other pixel-based, format-based, source camera-based, and geometric-based techniques [19]. However, the need for an image forensics evaluation framework is urgent.

3. METHODOLOGY

The design of evaluation framework uses the conformance methodology of software testing. This methodology is based on design science [39]. Design science is a scientific problem solving method used specially in Information Systems (IS) [37]. Artefacts related to information systems are designed and scrutinised to solve practical problems [37]. In this research, the problem of tool evaluation is solved using conformance testing.

The conformance testing method is adopted by the NIST project for tool testing called CFTT. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Draft International Standard (DIS) 10641 defines conformance testing as "test to evaluate the adherence or non-adherence of a candidate implementation to a standard" [40]. The understanding here is that if an implementation (e.g. software tools) fulfils certain *requirements* or *specifications* then it conforms to certain *assertions* that grants the tool a *conformance indicator* to validate its compliance with the acceptable standard. The tool undergoes a number of *test cases* in order to prove its compliance with these requirements and test assertions.

The methodology used to design the framework is based on conformance testing adopted by CFTT. Therefore, it will follow their steps and nomenclature of test requirements, test assertions, and test cases. The step-wise method used for conformance testing is:

- Highlight all the requirements of the tools of a certain domain.
- Frame out the assertions based on the requirements.
- Develop all the test cases necessary for the conformance of each test assertion.

Conformance testing consists of the following steps.

- **Test Requirement/Specification:**
  Test specifications are a set of requirements that a tool should have in order to qualify as a standard tool in the said domain. These requirements are developed by:
  (a) Research in the domain.
  (b) Vendor insights and knowledge.
  (c) Feedback from the consumers of the tools.
- **Test Assertion:**
  A test assertion is a verifiable statement about a single condition after an action is performed by the tool under test [41].
- **Test Case:**
  A test case usually checks an assertion after the action of a single execution of the tool under test [41]. The test cases are divided into *core* and *optional* test cases. Core test cases are carried out for every tool that is tested for that domain. Optional test cases are selected for every tool based on their offered features.

- **Conformance Indicator:**
  The conformance statement is declared given the tool under evaluation complies with the test assertion that is being tested.

The process of the research methodology is given in Figure 3.1.

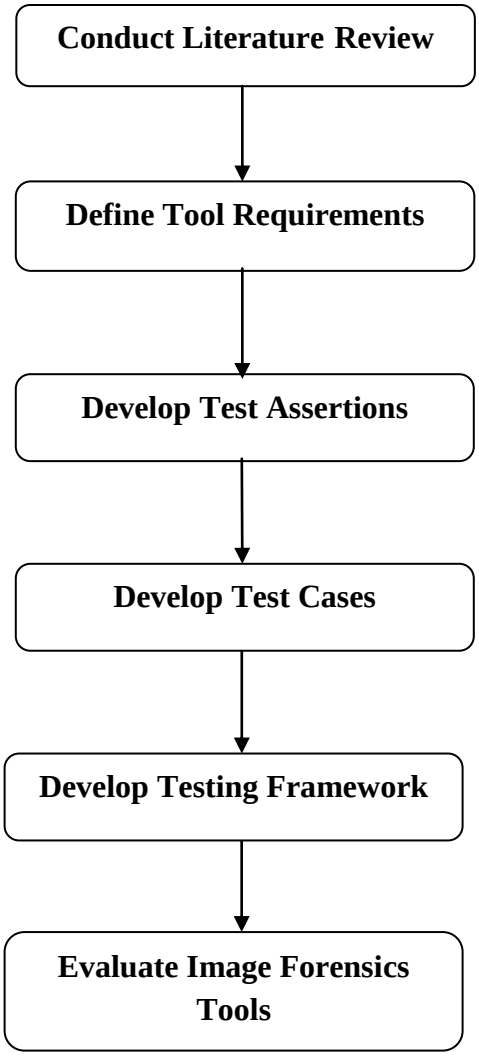


Fig 3.1 – Process of Research Methodology

Table 3.1 explains the research methodology.

Steps in detail	
Literature Review:	• Research state-of-the-art in image forensics. • Research evaluation frameworks already developed for other disciplines in digital forensics.
Tool Requirements/Specifications:	Develop a list of requirements (which are the features/functionalities that must be provided by the subject software/tool). The development of these requirements is based on: • current standards used by vendors • state-of-the-art research • feedback from the users
Test Assertions:	• The general statements or conditions that are marked 'check' after a test validates its presence and correct functionality in a software/tool. • The test assertions are derived from the requirements developed in the previous step.
Test Cases:	• The descriptive procedure of executing a test to confirm/validate a particular functionality (assertion) is known as a test case. • A test assertion can have one or more test cases in order for it to be 'checked' on the testing framework.
Testing Framework:	• A table that lists down test cases against assertions. • It is utilized to log the functionalities of every tool so that overall picture of its results can be inferred from the framework for the purpose of evaluating the tool. • The framework is also able to compare different tools against each other for every assertion.
Tools Evaluation:	Test the following tools using the developed framework: • FotoForensics • Ghiro • Imago Forensics • Exif Reader

Table 3.1 – Details of Methodology for Proposed Framework

4. DEVELOPMENT OF PROPOSED FRAMEWORK

This chapter contains the following:

- Section 4.1 provides the profiles of image forensics tools.
- Section 4.2 defines the test requirements/specifications of the proposed framework.
- Section 4.3 defines the test assertions and test cases of the proposed framework.

4.1 Profiles

The requirements, test assertions, and test cases laid down in this chapter encompass the evaluation framework for image forensics tools. They are divided into different *profiles.*

4.1.1 Included Profiles

Listed below are profiles included in the framework for the sake of organised distinction.

- **Multipurpose Internet Mail Extensions (MIME) Information**
  Every data object, or to be more specific, every media type is identified by a *reader* of that data object using a *magic number* embedded inside the object. This defines the type of media in the file. It can be an image, a video, or a text file. The MIME information is necessary for a tool to be able to identify, read, and categorise image files.
- **Image File Type Support**
  Every tool does not support all image formats, so a tool needs to specify to the user if it does not support an image format.
- **Upload Images to Tool**
  This profile falls under the usability aspect of a tool. In some cases a forensic analyst needs to be able to upload multiple images simultaneously. In some cases the image is online and another useful feature is uploading the image onto the tool directly using its internet URL.
- **Metadata**
  The metadata of the image refers to meaningful information about an image such as the size, file type, image resolution, and camera settings.
- **GPS Localisation**
  Some advanced cameras have GPS localisation feature, where if the camera has GPS tagging enabled while taking the image, the location can be traced later using the tools. The longitudes and latitudes of the point where the image was taken can be obtained. Some advanced tools provide an option to show that location on a map for better visualisation.
- **Tamper Detection**
  As discussed earlier, there are three main categories of tampering namely copy-move forgeries, splicing and re-touching. Most tools use ELA to do tamper detection. There are techniques in research that detect copy-move forgery and image splicing. However, most

practical tools have only been able to implement ELA for tamper detection in general. The detection of type of tampering done is yet to be incorporated in practical tools.

- **Hash Digest:**
  The hash digests of images are useful for multiple purposes. If an analyst has the digest only, it can be used to search for the corresponding image. If the analyst has the original image and the forged copy, then the analyst can generate hash digests of each image and compare them to indicate which image has been tampered.
- **Thumbnail**
  The thumbnail of an image is a small preview of the image.
- **Highlight Critical Data**
  The information about an image (e.g. metadata, maker notes) can be a lot. It is useful for the analyst to have the critical information about the image highlighted.
- **JPEG %**
  JPEG % represents the saved quality of the image after JPEG compression. While this is particular to only JPEG and its variants, it is very useful because it determines how easy it is for a tool to forensically analyse an image. A low quality image (say a 10% JPEG) will be harder to analyse compared to a high quality image (say a 90% JPEG) because the latter has lost significant amount of image data.
- **Hidden Pixels**
  Images sometimes contain hidden pixels which are not displayed by applications and are dealt with differently by each tool. Thus they can be a potential source of artefacts for an analyst.
- **Reporting**
  Good usability of a tool also suggests the automatic generation of a report on the images.
- **Multiple Image Analysis**
  A tool that is able to analyse a set of images and display results simultaneously is convenient with respect to time, analysis and comparison of the results.
- **Annotations**
  Being able to add notes and annotations to an image is an optional feature that can come in handy in investigation.
- **Colour Adjustments**
  Some images require colour adjustments before their finer details can be made visible for analysis.
- **Similar Images**
  The search for images similar to the one under observation or variants of it is useful because the potential source of the image can reveal helpful information.
- **By-case Distinction**
  Another usability feature is the ability to incorporate the different ongoing cases into a tool. This helps to keep the images organised in their distinctive cases.

- **Multiple Users and Multi-level Access System**
  Usually in a case there are multiple people working under the head investigator. A usability feature is a multi-level access system that allows the head to relinquish limited access to different users. This also allows convenient collaboration.

4.1.2 Eradicated Profiles

The profiles mentioned below are discarded. The details and justifications are given below.

- **Usability**
  Since the overall usability/ease of use, is an important part of the efficiency and practicality of a tool, this is a potential profile. However, it is not something that can be easily measured or quantified.
- **Size Inconsistencies**
  One of the techniques of information hiding makes use of the End of Image (EOI) marker. It marks the end of an image and any data entered after EOI is ignored by the image applications. Adding data after EOI increases the size of the image file. A simple comparison would reveal the hidden information. Given the fact that this technique belongs to the information hiding discipline and has not been incorporated in any of the tools, it is eradicated for now.
- **Copyright Information**
  Embedded copyright information also belongs to information hiding. None of the current tools provide the functionality for detection of copyright information.

4.2 Requirements/Specifications for Digital Image Forensics Tools

The following requirements have been narrowed down for the evaluation framework after the literature review. They are divided into the core and optional requirements. The standard CFTT nomenclature is followed. The following terminology is used:

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

For example, DIFT-CR-01 refers to the first core requirement for the digital image forensics tool.

4.2.1 Core Requirements/Specifications

The core requirements are mandatory for a tool and are listed below under their respective profiles.

4.2.1.1 MIME Information

DIFT-CR-01: The tool shall have the ability to determine the media type from the MIME information.

4.2.1.2 Image File Type Support

DIFT-CR-02: The tool shall have the ability to determine if the image file type is supported by the tool.

DIFT-CR-03: The tool shall have the ability to determine and report if the image file type is not supported by the tool.

4.2.1.3 Upload Images to Tool

DIFT-CR-04: The tool shall have the ability to directly upload the image to the tool from the computer.

4.2.1.4 Metadata

DIFT-CR-05: The tool shall have the ability to determine the filename of the image.

DIFT-CR-06: The tool shall have the ability to determine the size of the image.

DIFT-CR-07: The tool shall have the ability to determine the dimensions of the image.

DIFT-CR-08: The tool shall have the ability to determine the time the image was taken/created i.e. creation date and time.

DIFT-CR-09: The tool shall have the ability to determine the last time the image was modified.

DIFT-CR-10: The tool shall have the ability to determine the last time the image was accessed.

DIFT-CR-11: The tool shall have the ability to determine the camera make (manufacturing company) of the source camera of the image.

DIFT-CR-12: The tool shall have the ability to determine the camera model of the source camera of the image.

DIFT-CR-13: The tool shall have the ability to determine and report if no metadata exists for an image i.e. it has been stripped off metadata intentionally.

4.2.1.5 GPS Localisation

DIFT-CR-14: The tool shall have the ability to determine if the camera model supports GPS localisation of the images.

DIFT-CR-15: The tool shall have the ability to determine the GPS coordinates of the image (i.e. longitude and latitude).

4.2.1.6 Tamper Detection

DIFT-CR-16: The tool shall have the ability to do Error Level Analysis (ELA) of the image.

4.2.1.7 Hashes

DIFT-CR-17: The tool shall have the ability to generate a hash digest of the image.

DIFT-CR-18: The tool shall have the ability to search images through hash digests.

4.2.2 Optional Requirements/Specifications

The optional requirements are non-mandatory for the tool. They are listed below under their respective profiles.

4.2.2.1 Upload Images to Tool

DIFT-OR-01: The tool shall have the ability to access the image through the URL of the image online.

DIFT-OR-02: The tool shall have the ability to upload multiple images onto the tool simultaneously.

4.2.2.2 Metadata

DIFT-OR-03: The tool shall have the ability to determine the unique ID (serial number) of the source camera of the image.

DIFT-OR-04: The tool shall have the ability to determine the orientation of the image (i.e. landscape or portrait).

DIFT-OR-05: The tool shall have the ability to determine any tags/description/comments associated with the image.

DIFT-OR-06: The tool shall have the ability to determine the bit-depth of the image.

DIFT-OR-07: The tool shall have the ability to determine the colour-space of the image.

DIFT-OR-08: The tool shall have the ability to extract different types of metadata from the image (in case it exists).

DIFT-OR-09: The tool shall have the ability to determine the ISO of the image

DIFT-OR-10: The tool shall have the ability to determine the focal length of the source camera of the image.

DIFT-OR-11: The tool shall have the ability to determine the shutter speed of the image.

DIFT-OR-12: The tool shall have the ability to determine the subject distance in the image.

DIFT-OR-13: The tool shall have the ability to determine the flash setting in the image.

DIFT-OR-14: The tool shall have the ability to determine the aperture value of the image.

4.2.2.3 Thumbnail

DIFT-OR-15: The tool shall have the ability to determine if the thumbnail of the image is available.

DIFT-OR-16: The tool shall have the ability to determine any difference between the thumbnail and the actual image.

4.2.2.4 Tamper Detection

DIFT-OR-17: The tool shall have the ability to determine the type of tampering done with the image.

4.2.2.5 Highlight Critical Data

DIFT-OR-18: The tool shall have the ability to highlight critical metadata of the image.

4.2.2.6 JPEG %

DIFT-OR-19: The tool shall have the ability to determine the JPEG quality (i.e. JPEG %) of the image.

4.2.2.7 Hidden Pixels

DIFT-OR-20: The tool shall have the ability to determine any hidden pixels in the image.

4.2.2.8 Reporting

DIFT-OR-21: The tool shall have the ability to generate an automated report.

DIFT-OR-22: The tool shall have the ability to share reports with other users online.

4.2.2.9 Multiple Image Analysis

DIFT-OR-23: The tool shall have the ability to deal with multiple images simultaneously.

4.2.2.10 Annotations

DIFT-OR-24: The tool shall have the ability to add annotations to the image.

4.2.2.11 Colour Adjustments

DIFT-OR-25: The tool shall have the ability to make colour adjustments to the image.

4.2.2.12 Similar Images

DIFT-OR-26: The tool shall have the ability to find any image related to the image under analysis. This includes any identical image, variant image, or related image.

4.2.2.13 By-case Distinction

DIFT-OR-27: The tool shall have the ability to create multiple/separate cases in the tool interface (associated with multiple/separate ongoing investigations).

4.2.2.14 Multiple Users

DIFT-OR-28: The tool shall have the ability to allow multiple user accounts.

4.2.2.15 Multi-level Access System

DIFT-OR-29: The tool shall have the ability to allow a user to relinquish controlled access of a case to other users i.e. it should have a multi-level access system with respect to other users.

4.2.2.16 GPS Localisation

DIFT-OR-30: The tool shall have the ability to localise the image on a map.

4.3 Digital Image Forensics Tool Assertions and Test plan Version 1.0

The test assertions and respective test cases are laid down below. They map to the core and optional specifications provided in section 4.2.1 and 4.2.2 respectively.

4.3.1 Core Assertions and Test Cases

4.3.1.1 MIME Information

DIFT-CA-01: If the digital image forensics tool is capable of reading the media type as image from the MIME information, then the tool shall read/load the image.

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

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

4.3.1.2 Image File Type Support

DIFT-CA-02: If the digital image forensics 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 digital image forensics tool supports the file type of the image.

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

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

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

4.3.1.3 Upload Images to Tool

DIFT-CA-04: If the digital image forensics 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 digital image forensics tool uploaded image from computer.

4.3.1.4 Metadata

DIFT-CA-05: If the digital image forensics 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 digital image forensics tool read the filename of the image.

DIFT-CA-06: If the digital image forensics 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 digital image forensics tool determined the size of the image.

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

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

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

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

DIFT-CA-08: If the digital image forensics tool provides support for the image file type and reads it without error, it shall determine the timestamp of the image i.e. the 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 digital image forensics tool determined the creation date and time of the image.

DIFT-CA-09: If the digital image forensics 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 the determined modified timestamp with the actual modified time and date.

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

DIFT-CA-10: If the digital image forensics 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 the determined last accessed timestamp with the actual last accessed timestamp.

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

DIFT-CA-11: If the digital image forensics 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 digital image forensics tool determined the make of the source camera of the image.

DIFT-CA-12: If the digital image forensics 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 digital image forensics tool determined the model of the source camera of the image.

DIFT- CA -13: If the digital image forensics 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 digital image forensics tool determined that the image has no metadata.

4.3.1.5 GPS Localisation

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

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

Conformance Indicator: The digital image forensics tool determined that the model of the source camera supports GPS localisation.

DIFT-CA-15: If the digital image forensics tool determines whether model of the source camera supports GPS localisation, 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 digital image forensics tool determined the GPS coordinates of the location where the image was captured.

4.3.1.6 Tamper Detection

DIFT-CA-16: If the digital image forensics tool provides support for the image file type and reads it without error, it shall perform the 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 do ELA of the image using the tool.

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

4.3.1.7 Hashes

DIFT- CA -17: If the digital image forensics 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 digital image forensics tool computed different types of hash digests of the image.

DIFT- CA -18: If the digital image forensics 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 digital image forensics tool searched for the image using the hash digest.

4.3.2 Optional Assertions and Test Cases

4.3.2.1 Upload Images to Tool

DIFT-AO-01: If the digital image forensics 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.

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

DIFT-AO-02: If the digital image forensics 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 digital image forensics tool uploaded multiple images from the computer.

4.3.2.2 Metadata

DIFT- AO -03: If the digital image forensics 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 digital image forensics tool determined the unique ID (serial number) of the source camera.

DIFT- AO -04: If the digital image forensics 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 digital image forensics tool determined the orientation of the image.

DIFT- AO -05: If the digital image forensics tool provides support for the image file type and reads it without error, it shall determine any tags/description/comments of the image (if present) 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 digital image forensics tool determined the tags/description/comments of the image.

DIFT- AO -06: If the digital image forensics 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 digital image forensics tool determined the bit-depth of the image.

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

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

Conformance Indicator: The digital image forensics tool determined the colour-space of the image.

DIFT- AO -08: If the digital image forensics 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 digital image forensics tool determined the additional metadata types of the image.

DIFT- AO -09: If the digital image forensics 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 digital image forensics tool determined the ISO of the image.

DIFT- AO -10: If the digital image forensics 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 digital image forensics tool determined the focal length of the image.

DIFT- AO -11: If the digital image forensics 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 digital image forensics tool determined the shutter speed of the image.

DIFT- AO -12: If the digital image forensics 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 digital image forensics tool determined the subject distance of the image.

DIFT- AO -13: If the digital image forensics 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 digital image forensics tool determined the flash setting of the image.

DIFT- AO -14: If the digital image forensics 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 the determined aperture value with the actual aperture value of the source camera.

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

4.3.2.3 Thumbnail

DIFT- AO -15: If the digital image forensics 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 digital image forensics tool determined thumbnail existence of the image.

DIFT- AO -16: If the digital image forensics 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 digital image forensics tool determined difference (if any) between thumbnail and image.

4.3.2.4 Tamper Detection

DIFT- AO -17: If the digital image forensics tool detects tampering in the image, it shall determine the type of tampering done with the image 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 digital image forensics tool determined type of tampering.

4.3.2.5 Highlight Critical Data

DIFT- AO -18: If the digital image forensics 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 digital image forensics tool highlighted critical data.

4.3.2.6 JPEG %

DIFT- AO -19: If the digital image forensics 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 digital image forensics tool determined the JPEG quality of the image.

4.3.2.7 Hidden Pixels

DIFT- AO -20: If the digital image forensics 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 digital image forensics tool determined the hidden pixels in the image.

4.3.2.8 Reporting

DIFT- AO -21: If the digital image forensics 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 digital image forensics tool generated an automated report of results for an image.

DIFT- AO -22: If the digital image forensics 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 digital image forensics tool shared reports with online users.

4.3.2.9 Multiple Image Analysis

DIFT- AO -23: If the digital image forensics 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 digital image forensics tool performed forensic analysis of multiple images simultaneously.

4.3.2.10 Annotations

DIFT- AO -24: If the digital image forensics 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 digital image forensics tool added annotations to the image.

4.3.2.11 Colour Adjustments

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

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

Conformance Indicator: The digital image forensics tool made colour adjustments to the image.

4.3.2.12 Similar Images

DIFT- AO -26: If the digital image forensics 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 digital image forensics tool found variants of the image online.

4.3.2.13 By-case Distinction

DIFT- AO -27: The digital image forensics 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 digital image forensics tool created multiple cases.

4.3.2.14 Multiple Users

DIFT- AO -28: The digital image forensics tool shall allow multiple users to use the tool.

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

Conformance Indicator: The digital image forensics tool allowed multiple users.

4.3.2.15 Multi-level Access System

DIFT- AO -29: The digital image forensics 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 digital image forensics tool assigned different levels of access authority (to case material) to different users.

4.3.2.16 GPS Localisation

DIFT-AO-30: If the digital image forensics tool determines support for GPS localisation 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 digital image forensics tool localised the image on a map.

A summary of the entire evaluation framework is provided in Table 4.1 and 4.2.

Profiles	Core Requirements	Core Assertions	Test Cases
MIME Information	DIFT-CR-01	DIFT-CA-01	DIFT- 01
Image File Type Support	DIFT-CR-02	DIFT-CA-02	DIFT- 02
	DIFT-CR-03	DIFT-CA-03	DIFT- 03
Upload Images to Tool	DIFT-CR-04	DIFT-CA-04	DIFT- 04
Metadata	DIFT-CR-05	DIFT-CA-05	DIFT- 05
			DIFT- 06
	DIFT-CR-06	DIFT-CA-06	DIFT- 07
			DIFT- 08
	DIFT-CR-07	DIFT-CA-07	DIFT- 09
			DIFT- 10
	DIFT-CR-08	DIFT-CA-08	DIFT- 11
			DIFT- 12
	DIFT-CR-09	DIFT-CA-09	DIFT- 13
			DIFT- 14
			DIFT- 15
	DIFT-CR-10	DIFT-CA-10	DIFT- 16
			DIFT- 17
	DIFT-CR-11	DIFT-CA-11	DIFT- 18
			DIFT- 19
	DIFT-CR-12	DIFT-CA-12	DIFT- 20
			DIFT- 21
	DIFT-CR-13	DIFT-CA-13	DIFT- 22
			DIFT- 23
GPS Localisation	DIFT-CR-14	DIFT-CA-14	DIFT- 24
	DIFT-CR-15	DIFT-CA-15	DIFT- 25
Tamper Detection	DIFT-CR-16	DIFT-CA-16	DIFT- 26
			DIFT- 27
Hashes	DIFT-CR-17	DIFT-CA-17	DIFT- 28
	DIFT-CR-18	DIFT-CA-18	DIFT- 29

Table 4.1 – The Digital Image Forensics Tools Evaluation Framework (Core)

Profiles	Optional Requirements	Optional Assertions	Test Cases
Upload Images to Tool	DIFT-OR-01	DIFT-AO-01	DIFT- 30
			DIFT- 31
	DIFT-OR-02	DIFT-AO-02	DIFT- 32
Metadata	DIFT-OR-03	DIFT-AO-03	DIFT- 33
	DIFT-OR-04	DIFT-AO-04	DIFT- 34
	DIFT-OR-05	DIFT-AO-05	DIFT- 35
			DIFT- 36
	DIFT-OR-06	DIFT-AO-06	DIFT- 37
			DIFT- 38
	DIFT-OR-07	DIFT-AO-07	DIFT- 39
	DIFT-OR-08	DIFT-AO-08	DIFT- 40
	DIFT-OR-09	DIFT-AO-09	DIFT- 41
			DIFT- 42
	DIFT-OR-10	DIFT-AO-10	DIFT- 43
			DIFT- 44
	DIFT-OR-11	DIFT-AO-11	DIFT- 45
			DIFT- 46
	DIFT-OR-12	DIFT-AO-12	DIFT- 47
	DIFT-OR-13	DIFT-AO-13	DIFT- 48
			DIFT- 49
	DIFT-OR-14	DIFT-AO-14	DIFT- 50
			DIFT- 51
Thumbnail	DIFT-OR-15	DIFT-AO-15	DIFT- 52
			DIFT- 53
	DIFT-OR-16	DIFT-AO-16	DIFT- 54
Tamper Detection	DIFT-OR-17	DIFT-AO-17	DIFT- 55
Highlight Critical Data	DIFT-OR-18	DIFT-AO-18	DIFT- 56
JPEG %	DIFT-OR-19	DIFT-AO-19	DIFT- 57
			DIFT- 58
Hidden Pixels	DIFT-OR-20	DIFT-AO-20	DIFT- 59
Reporting	DIFT-OR-21	DIFT-AO-21	DIFT- 60
	DIFT-OR-22	DIFT-AO-22	DIFT- 61
Multiple Image Analysis	DIFT-OR-23	DIFT-AO-23	DIFT- 62
Annotations	DIFT-OR-24	DIFT-AO-24	DIFT- 63
Colour Adjustments	DIFT-OR-25	DIFT-AO-25	DIFT- 64
Similar Images	DIFT-OR-26	DIFT-AO-26	DIFT- 65
By-case Distinction	DIFT-OR-27	DIFT-AO-27	DIFT- 66
Multiple Users	DIFT-OR-28	DIFT-AO-28	DIFT- 67
Multi-level Access System	DIFT-OR-29	DIFT-AO-29	DIFT- 68
GPS Localisation	DIFT-OR-30	DIFT-AO-30	DIFT- 69

Table 4.2 – The Digital Image Forensics Tools Evaluation Framework (Optional)

5. EVALUATION OF TOOLS USING PROPOSED FRAMEWORK

This chapter contains the following:

- Section 5.1 provides a feature list of the four tools.
- Section 5.2 lists working environments under which the test cases were performed for each tool. This is followed by the test case selection for each tool. The test case selections indicate the optional test cases that were tested and the ones that were not tested because the feature was unavailable in the tool.
- Section 5.3 tabulates the test results in a comparative manner.
- Section 5.4 provides more details of the test results.

5.1 Feature Lists

To test the proposed framework, four image forensics tools were tested namely FotoForensics, Ghiro, Imago Forensics, and Exif Reader.

Table 5.1 lists the features of each tool.

Features	FotoForensics	Ghiro	Imago	Exif Reader
Open-source Tool		✓		
Free Tool	✓		✓	✓
MIME Information	✓	✓	✓	✓
Metadata Extraction	✓	✓	✓	✓
GPS Localisation	✓	✓	✓	✓
Error Level Analysis	✓	✓	✓	
Thumbnail Review	✓	✓		✓
Hash Generation	✓	✓	✓	✓
Hash Matching		✓		
Highlight Critical Data		✓		
Similar Picture Search	✓			
Hidden Pixel Extraction	✓			
Colour Adjustments	✓			
Annotations	✓			
JPEG %	✓			
Detection of Nudity (in Beta)			✓	
Python based tool			✓	
Web browser backed by VM		✓		
Public Website	✓			
Recursive Directory Navigation			✓	
SQLite export			✓	
CSV export			✓	

Table 5.1 – Feature List of Tools

5.2 Working Environments and Test Case Selections

5.2.1 Execution Environment

Execution Environment: Windows 7 Professional Service Pack 1
Processor: Intel(R) Core(TM) i3-2310M CPU @ 2.10 GHz
Installed Memory (RAM): 4.00 GB
System Type: 64-bit Operating System

Test Computer: HP ProBook 4530s

5.2.2 FotoForensics

FotoForensics is a public Website that offers forensic analysis of images of different formats. It can be accessed using any OS e.g. Windows or Linux.

5.2.2.1 Working Environment

Tool Tested: FotoForensics (public Website)
Software Version: 1.1.3294

Supplier: Hacker Factor

Website: http://fotoforensics.com/

5.2.2.2 Test Case Selection

Supported Optional Feature	Test Case ID
Upload Images to Tool	30, 31
Metadata	33-51
Thumbnail	52, 53
JPEG%	57, 58
Hidden Pixels	59
Reporting	60, 61
Annotations	63
Colour Adjustments	64
Similar Images	65
GPS Localisation (map feature)	69

Table 5.2 – Selected Test Cases for FotoForensics

Unsupported Optional Feature	Test Case ID
Upload Images to Tool (Multiple images upload)	32
Thumbnail	54
Tamper Detection (type of tampering)	55
Highlight Critical Data	56
Multiple Image Analysis	62
By-case Distinction	66
Multiple Users	67
Multi-level Access System	68

Table 5.3 – Omitted Test Cases for FotoForensics

5.2.3 Ghiro

The Ghiro appliance is run on Linux. The interface that Ghiro uses is Internet based. It provides a user-friendly environment for forensic analysis of images.

5.2.3.1 Working Environment

Tool Tested: Ghiro
Software Version: 0.2.1-1, Open Virtualisation Appliance (OVA) version

Supplier: Open-source project – developer: Alessandro Tanasi

Website: https://www.getghiro.org/

5.2.3.2 Test Case Selection

Supported Optional Feature	Test Case ID
Upload Images to Tool	30-32
Metadata	33-51
Thumbnail	52-54
Highlight Critical Data	56
Reporting	60, 61
Multiple Image Analysis	62
By-case Distinction	66
Multiple Users	67
Multi-level Access System	68
GPS Localisation (map feature)	69

Table 5.4 – Selected Test Cases for Ghiro

Unsupported Optional Feature	Test Case ID
Tamper Detection (type of tampering)	55
JPEG%	57. 58
Hidden Pixels	59
Annotations	63
Colour Adjustments	64
Similar Images	65

Table 5.5 – Omitted Test Cases for Ghiro

5.2.4 Imago Forensics

Imago forensics is a command line tool that runs on Linux OS. It performs forensic analysis of the images present in the specified target directory and produces a CSV file or a SQLite database of the results obtained from the analysis.

5.2.4.1 Working Environment

Tool Tested: Imago Forensics
Software Version: V.1.0.5

Supplier: Matteo Redaelli

Website: https://github.com/redaelli/imago-forensics

5.2.4.2 Test Case Selection

Supported Optional Feature	Test Case ID
Upload Images to Tool	32
Metadata	33-51
Reporting	60, 61
Multiple Image Analysis	62

Table 5.6 – Selected Test Cases for Imago Forensics

Unsupported Optional Feature	Test Case ID
Upload Images to Tool	30,31
Thumbnail	52-54
Tamper Detection (type of tampering)	55
Highlight Critical Data	56
JPEG%	57, 58
Hidden Pixels	59
Annotations	63
Colour Adjustments	64
Similar Images	65
By-case Distinction	66
Multiple Users	67
Multi-level Access System	68
GPS Localisation (map feature)	69

Table 5.7 – Omitted Test Cases for Imago Forensics

5.2.5 Exif Reader

Exif Reader is a simple tool that runs on the Windows OS. It reads the EXIF metadata of the images under analysis.

5.2.5.1 Working Environment

Tool Tested: Exif Reader
Software Version: 3.00

Supplier: Ryuuji Yoshimoto

Website: http://www.takenet.or.jp/~ryuuji/minisoft/exifread/english/download.html

5.2.5.2 Test Case Selection

Supported Optional Feature	Test Case ID
Upload Images to Tool	32
Metadata	33-51
Thumbnail	52,53
Reporting	60
Multiple Image Analysis	62

Table 5.8 – Selected Test Cases for Exif Reader

Unsupported Optional Feature	Test Case ID
Upload Images to tool	30,31
Reporting	61
Thumbnail	54
Tamper Detection (type of tampering)	55
Highlight Critical Data	56
JPEG%	57,58
Hidden Pixels	59
Annotations	63
Colour Adjustments	64
Similar Images	65
By-case Distinction	66
Multiple Users	67
Multi-level Access System	68
GPS Localisation (map feature)	69

Table 5.9 – Omitted Test Cases for Exif Reader

5.3 Test Results

Table 5.10 and 5.11 provide the core and optional test results of the four tools respectively. The test result is stated as either 0 or 1 where 0 represents the inability of the tool to perform the given test case successfully and 1 represents compliance with the test case. This table provides a comparative view of the results obtained from the framework and directly maps the tools onto the framework.

Profile	Test Case ID	FotoForensics	Ghiro	Imago	Exif Reader
MIME Information	DIFT-01	1	1	1	1
Image File Type Support	DIFT-02	1	1	1	1
	DIFT-03	1	1	1	1
Upload Images to Tool	DIFT-04	1	1	1	1
Metadata	DIFT-05	1	1	1	1
	DIFT-06	1	1	1	1
	DIFT-07	1	1	1	0
	DIFT-08	1	1	1	0
	DIFT-09	1	1	1	1
	DIFT-10	1	1	1	1
	DIFT-11	1	1	0	1
	DIFT-12	1	1	0	1
	DIFT-13	0	0	0	0
	DIFT-14	0	0	0	0
	DIFT-15	0	0	0	0
	DIFT-16	0	0	1	0
	DIFT-17	0	0	1	0
	DIFT-18	1	1	1	1
	DIFT-19	1	1	1	1
	DIFT-20	1	1	1	1
	DIFT-21	1	1	1	1
	DIFT-22	1	1	1	1
	DIFT-23	1	1	1	1
GPS Localisation	DIFT-24	1	1	1	1
	DIFT-25	1	1	1	1
Tamper Detection	DIFT-26	1	1	1	0
	DIFT-27	1	1	1	0
Hashes	DIFT-28	1	1	1	0
	DIFT-29	0	1	0	0

Table 5.10 – Comparative Test Results of Evaluation of Tools (Core)

Profile	Test Case ID	FotoForensics	Ghiro	Imago	Exif Reader
Upload Images to Tool	DIFT-30	1	0	N/A	N/A
	DIFT-31	1	0	N/A	N/A
	DIFT-32	N/A	1	1	1
Metadata	DIFT-33	1	1	0	0
	DIFT-34	1	0	1	0
	DIFT-35	1	1	1	0
	DIFT-36	1	1	1	0
	DIFT-37	1	0	0	1
	DIFT-38	1	0	0	1
	DIFT-39	1	1	1	1
	DIFT-40	1	1	0	0
	DIFT-41	1	1	1	1
	DIFT-42	1	1	1	1
	DIFT-43	1	1	1	1
	DIFT-44	1	1	1	1
	DIFT-45	1	1	1	1
	DIFT-46	1	1	1	1
	DIFT-47	0	0	0	0
	DIFT-48	1	0	1	1
	DIFT-49	1	0	1	1
	DIFT-50	1	0	0	1
	DIFT-51	1	0	0	1
Thumbnail	DIFT-52	1	1	N/A	1
	DIFT-53	1	1	N/A	1
	DIFT-54	N/A	0	N/A	N/A
Tamper Detection	DIFT-55	N/A	N/A	N/A	N/A
Highlight Critical Data	DIFT-56	N/A	1	N/A	N/A
JPEG%	DIFT-57	1	N/A	N/A	N/A
	DIFT-58	1	N/A	N/A	N/A
Hidden Pixels	DIFT-59	1	N/A	N/A	N/A
Reporting	DIFT-60	1	1	1	1
	DIFT-61	1	0	0	N/A
Multiple Image Analysis	DIFT-62	N/A	1	1	1
Annotations	DIFT-63	1	N/A	N/A	N/A
Colour Adjustments	DIFT-64	1	N/A	N/A	N/A
Similar Images	DIFT-65	1	N/A	N/A	N/A
By-case Distinction	DIFT-66	N/A	1	N/A	N/A
Multiple Users	DIFT-67	N/A	1	N/A	N/A
Multi-level Access System	DIFT-68	N/A	1	N/A	N/A
GPS Localisation	DIFT-69	1	1	N/A	N/A

Table 5.11 – Comparative Test Results of Evaluation of Tools (Optional)

The test results of the tools indicate that majority of the tools conformed to all the core test cases except for the modification timestamp. Exif Reader was unable to conform to ELA which is an important core requirement for tamper detection. In the case of optional features, FotoForensics provided the most features except for features like multi-level access system, by-case distinction and multiple users. These usability features, on the other hand, were provided by Ghiro. But

Ghiro was unable to conform to some of the other optional features. Imago Forensics and Exif Reader did not provide majority of the optional features.

5.4 Detailed Test Results

This section provides details of the test results of each of the four tools. The results are presented with respect to test case IDs. Each test case is tested and the results are listed in the respective table. The possible result values in the table are explained below:

1. **As expected** means the tool successfully conformed to the test case (this maps to 1 in Table 5.10 and Table 5.11)
2. **Not checked** means the tool was unable to conform to the test case (this maps to 0 in Table 5.10 and Table 5.11)
3. **Option not available** means the tool does not provided the feature (this maps to N/A in Table 5.10 and Table 5.11)

5.4.1 FotoForensics Test Results Report

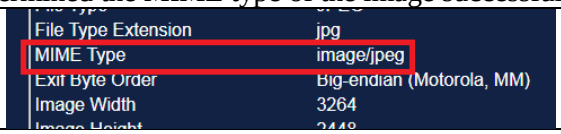
Test Case DIFT-01	
Results	As expected
Analysis and Comments	The tool determined the MIME type of the image successfully.
Screenshots	

Table 5.12 – FotoForensics Test Result DIFT-01

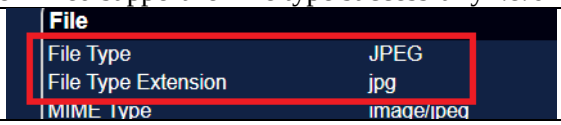
Test Case DIFT-02	
Results	As expected
Analysis and Comments	The tool determined support for file type successfully i.e. JPEG.
Screenshots	

Table 5.13 – FotoForensics Test Result DIFT-02

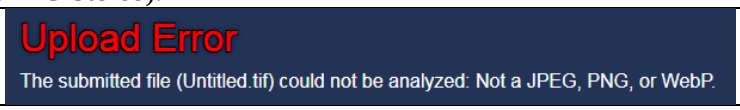
Test Case DIFT-03	
Results	As expected
Analysis and Comments	• The tool detected an unsupported image i.e. a TIF image. • Any file type other than JPEG, PNG, and WebP is an unsupported file type. • The tool also analysed variants of the JPEG format such as .jps (JPEG Stereo).
Screenshots	

Table 5.14 – FotoForensics Test Result DIFT-03

Test Case DIFT-04	
Results	As expected
Analysis and Comments	The tool uploaded the image directly from computer successfully.
Screenshots	

Table 5.15 – FotoForensics Test Result DIFT-04

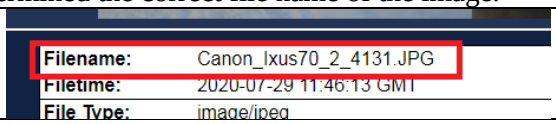
Test Case DIFT-05, 06	
Results	As expected
Analysis and Comments	The tool determined the correct file name of the image.
Screenshots	

Table 5.16 – FotoForensics Test Result DIFT-05, 06

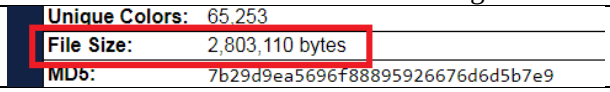
Test Case DIFT-07, 08	
Results	As expected
Analysis and Comments	The tool determined the correct file size of the image.
Screenshots	

Table 5.17 – FotoForensics Test Result DIFT-07, 08

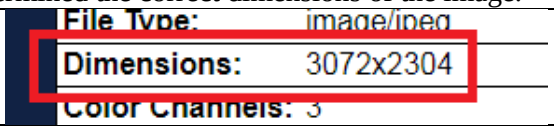
Test Case DIFT-09, 10	
Results	As expected
Analysis and Comments	The tool determined the correct dimensions of the image.
Screenshots	

Table 5.18 – FotoForensics Test Result DIFT-09, 10

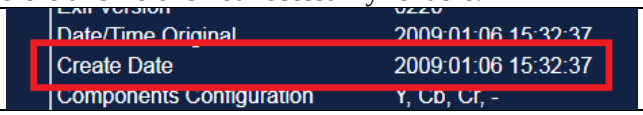
Test Case DIFT-11, 12	
Results	As expected
Analysis and Comments	• The tool determined the correct creation date and time of the image. • It is common for cameras to have the wrong time settings (e.g. incorrect time zone or date). This reflects in the metadata. Therefore this field is not necessarily reliable.
Screenshots	

Table 5.19 – FotoForensics Test Result DIFT-11, 12

Test Case DIFT-13-15	
Results	Not checked
Analysis and Comments	• The tool was unable to detect the correct last modified timestamp in this test, which was 9/2/2020 5:50 pm. • Modification using some software (like PhotoShop) was detected, while modification using other software (like Paint) was not detected. One reason is that PhotoShop adds many artefacts and metadata.
Screenshots	

Table 5.20 – FotoForensics Test Result DIFT-13-15

Test Case DIFT-16, 17	
Results	Option not available
Analysis and Comments	The tool does not provide the last accessed timestamp.
Screenshots	-

Table 5.21 – FotoForensics Test Result DIFT-16, 17

Test Case DIFT-18, 19	
Results	As expected
Analysis and Comments	The tool determined the make of source camera correctly.
Screenshots	

Table 5.22 – FotoForensics Test Result DIFT-18, 19

Test Case DIFT-20, 21	
Results	As expected
Analysis and Comments	The tool determined the model of source camera correctly.
Screenshots	

Table 5.23 – FotoForensics Test Result DIFT-20, 21

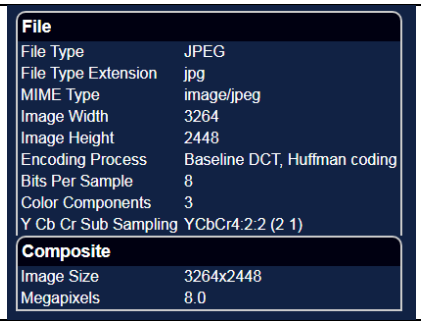
Test Case DIFT-22, 23	
Results	As expected
Analysis and Comments	• The tool was tested with an image that was stripped off metadata using the Exiftool. • The tool gave basic file attributes of the image file. The Exif metadata that was deleted beforehand was not detected.
Screenshots	

Table 5.24 – FotoForensics Test Result DIFT-22, 23

Test Case DIFT-24	
Results	As expected
Analysis and Comments	The tool detected GPS coordinates of the subject image that had GPS tagging enabled.
Screenshots	

Table 5.25 – FotoForensics Test Result DIFT-24

Test Case DIFT-25	
Results	As expected
Analysis and Comments	The tool determined the longitude and latitude of the location where the image was taken.
Screenshots	

Table 5.26 – FotoForensics Test Result DIFT-25

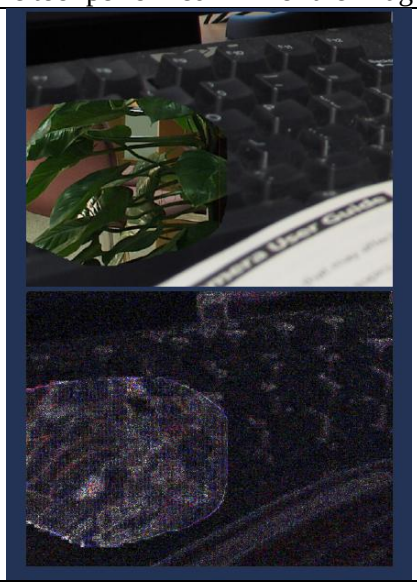
Test Case DIFT-26, 27	
Results	As expected
Analysis and Comments	The tool performed ELA of the image.
Screenshots	

Table 5.27 – FotoForensics Test Result DIFT-26, 27

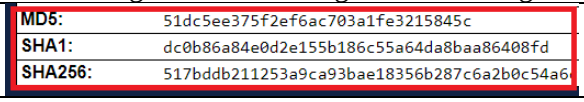
Test Case DIFT-28	
Results	As expected
Analysis and Comments	The tool generated hash digests of the image.
Screenshots	

Table 5.28 – FotoForensics Test Result DIFT-28

Test Case DIFT-29	
Results	Option not available
Analysis and Comments	The tool does not provide the option of searching based on hash digests.
Screenshots	-

Table 5.29 – FotoForensics Test Result DIFT-29

Test Case DIFT-30, 31	
Results	As expected
Analysis and Comments	• The tool uploaded the image using its URL. • In some cases, however, the tool performed forensic analysis of the thumbnail of the image rather than the actual image.
Screenshots	

Table 5.30 – FotoForensics Test Result DIFT-30, 31

Test Case DIFT-32	
Results	Option not available
Analysis and Comments	The tool does not upload multiple images simultaneously.
Screenshots	-

Table 5.31 – FotoForensics Test Result DIFT-32

Test Case DIFT-33	
Results	As expected
Analysis and Comments	• The tool determined the serial number of the source camera. • The serial number rarely exists in the metadata once an image has been edited. Any editing discards some metadata fields. So if an image has never been edited there is a possibility that the serial number exists in the metadata. In this case the tool is able to detect it. Otherwise, if it does not exist in the metadata, the tool cannot detect it.
Screenshots	

Table 5.32 – FotoForensics Test Result DIFT-33

Test Case DIFT-34	
Results	As expected
Analysis and Comments	The tool determined the orientation of the image.
Screenshots	

Table 5.33 – FotoForensics Test Result DIFT-34

Test Case DIFT-35, 36	
Results	As expected
Analysis and Comments	The tool determined the tags and comments associated with the image.
Screenshots	

Table 5.34 – FotoForensics Test Result DIFT-35, 36

Test Case DIFT-37, 38	
Results	As expected
Analysis and Comments	The tool determined the bit-depth of the image.
Screenshots	

Table 5.35 – FotoForensics Test Result DIFT-37, 38

Test Case DIFT-39	
Results	As expected
Analysis and Comments	The tool determined the colour-space of the image.
Screenshots	

Table 5.36 – FotoForensics Test Result DIFT-39

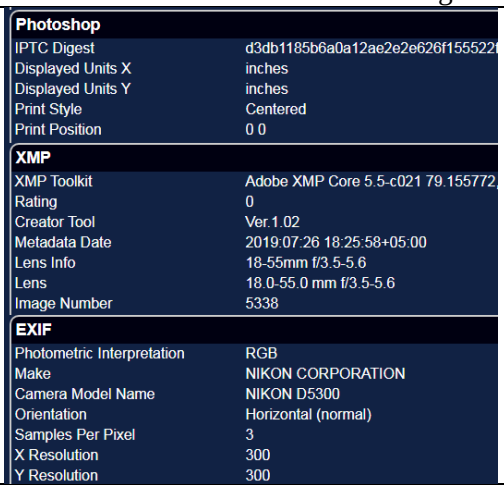
Test Case DIFT-40	
Results	As expected
Analysis and Comments	The tool determined the various metadata of the image.
Screenshots	

Table 5.37 – FotoForensics Test Result DIFT-40

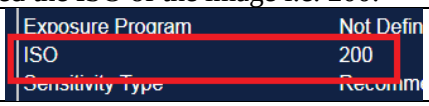
Test Case DIFT-41, 42	
Results	As expected
Analysis and Comments	The tool determined the ISO of the image i.e. 200.
Screenshots	

Table 5.38 – FotoForensics Test Result DIFT-41, 42

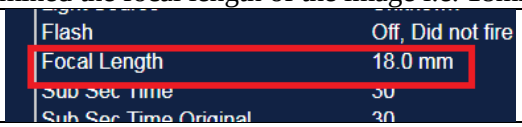
Test Case DIFT-43, 44	
Results	As expected
Analysis and Comments	The tool determined the focal length of the image i.e. 18mm.
Screenshots	

Table 5.39 – FotoForensics Test Result DIFT-43, 44

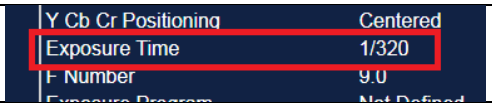
Test Case DIFT-45, 46	
Results	As expected
Analysis and Comments	The tool determined the shutter speed/exposure time of the image i.e. 1/320s.
Screenshots	

Table 5.40 – FotoForensics Test Result DIFT-45, 46

Test Case DIFT-47	
Results	Not checked
Analysis and Comments	The tool does not determine the subject of the image.
Screenshots	-

Table 5.41 – FotoForensics Test Result DIFT-47

Test Case DIFT-48, 49	
Results	As expected
Analysis and Comments	The tool determined the flash setting of the image.
Screenshots	

Table 5.42 – FotoForensics Test Result DIFT-48, 49

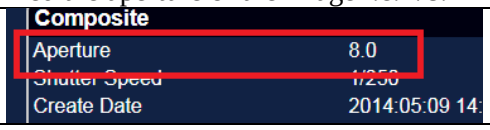
Test Case DIFT-50, 51	
Results	As expected
Analysis and Comments	The tool determined the aperture of the image i.e. f/8.
Screenshots	

Table 5.43 – FotoForensics Test Result DIFT-50, 51

Test Case DIFT-52,53	
Results	As expected
Analysis and Comments	The tool determined the thumbnail information of the image.
Screenshots	

Table 5.44 – FotoForensics Test Result DIFT-52, 53

Test Case DIFT-54	
Results	Option not available
Analysis and Comments	The tool does not do thumbnail and image differentiation.
Screenshots	-

Table 5.45 – FotoForensics Test Result DIFT-54

Test Case DIFT-55	
Results	Option not available
Analysis and Comments	The tool does not determine the type of tampering done.
Screenshots	-

Table 5.46 – FotoForensics Test Result DIFT-55

Test Case DIFT-56	
Results	Option not available
Analysis and Comments	The tool does not highlight critical data about the image.
Screenshots	-

Table 5.47 – FotoForensics Test Result DIFT-56

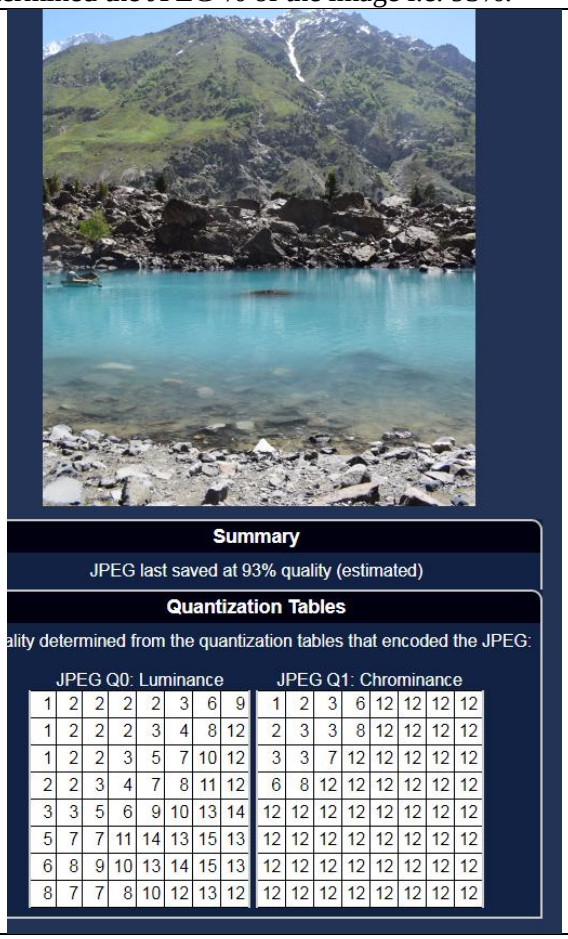
Test Case DIFT-57, 58	
Results	As expected
Analysis and Comments	The tool determined the JPEG % of the image i.e. 93%.
Screenshots	

Table 5.48 – FotoForensics Test Result DIFT-57, 58

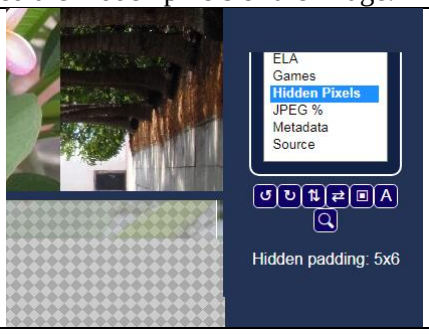
Test Case DIFT-59	
Results	As expected
Analysis and Comments	The tool determined the hidden pixels of the image.
Screenshots	

Table 5.49 – FotoForensics Test Result DIFT-59

Test Case DIFT-60	
Results	As expected
Analysis and Comments	The tool created an automated report of the forensic analysis.
Screenshots	Refer to Appendix A – FotoForensics Report for complete report.

Table 5.50 – FotoForensics Test Result DIFT-60

Test Case DIFT-61	
Results	As expected
Analysis and Comments	The tool shared the analysis report via Facebook, Twitter, Pinterest, and Reddit.
Screenshots	

Table 5.51 – FotoForensics Test Result DIFT-61

Test Case DIFT-62	
Results	Option not available
Analysis and Comments	The tool does not perform forensic analysis of multiple images simultaneously.
Screenshots	-

Table 5.52 – FotoForensics Test Result DIFT-62

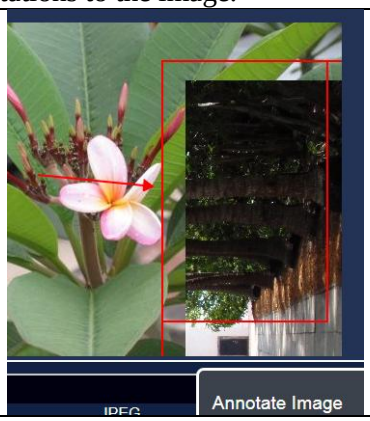
Test Case DIFT-63	
Results	As expected
Analysis and Comments	The tool added annotations to the image.
Screenshots	

Table 5.53 – FotoForensics Test Result DIFT-63

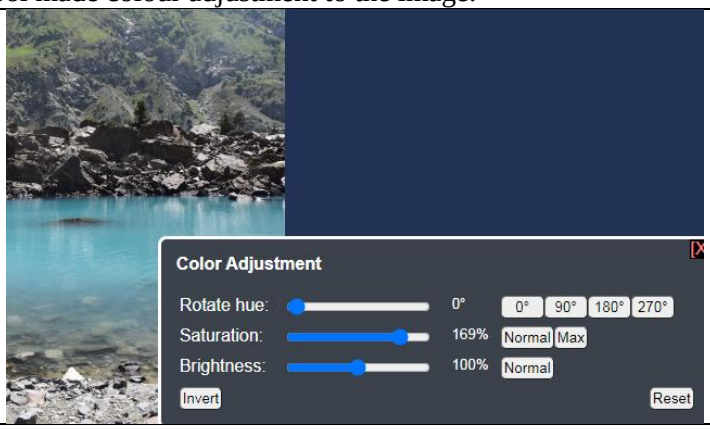
Test Case DIFT-64	
Results	As expected
Analysis and Comments	The tool made colour adjustment to the image.
Screenshots	

Table 5.54 – FotoForensics Test Result DIFT-64

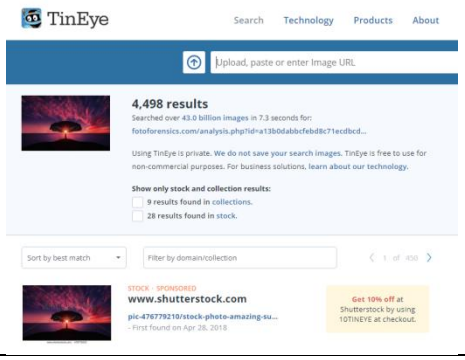
Test Case DIFT-65	
Results	As expected
Analysis and Comments	The tool used different search engines to perform a search for any similar images that might be present on the Internet. TinEye, Google, Bing, RootAbout are some of the source tools/search engines.
Screenshots	

Table 5.55 – FotoForensics Test Result DIFT-65

Test Case DIFT-66	
Results	Option not available
Analysis and Comments	The tool does not allow case-based distinction.
Screenshots	-

Table 5.56 – FotoForensics Test Result DIFT-66

Test Case DIFT-67	
Results	Option not available
Analysis and Comments	The tool does not allow multiple user accounts.
Screenshots	-

Table 5.57 – FotoForensics Test Result DIFT-67

Test Case DIFT-68	
Results	Option not available
Analysis and Comments	The tool does not implement multi-level access system.
Screenshots	-

Table 5.58 – FotoForensics Test Result DIFT-68

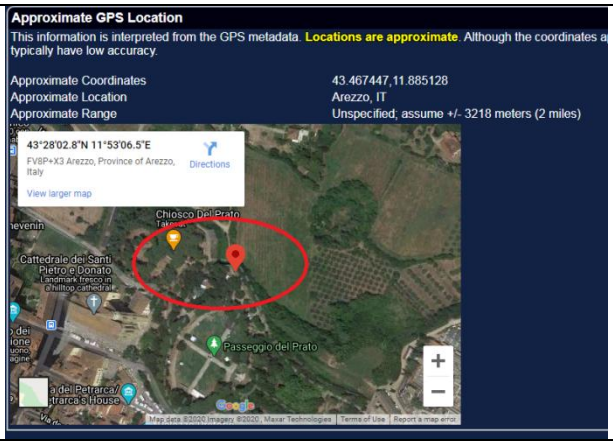
Test Case DIFT-69	
Results	As expected
Analysis and Comments	The tool was able to map out the determined longitude and latitude on a map.
Screenshots	

Table 5.59 – FotoForensics Test Result DIFT-69

5.4.2 Ghiro Test Results Report

Test Case DIFT-01	
Results	As expected
Analysis and Comments	The tool determined the MIME type of the image successfully.
Screenshots	

Table 5.60 – Ghiro Test Result DIFT-01

Test Case DIFT-02	
Results	As expected
Analysis and Comments	The tool determined support for file type successfully i.e. JPEG.
Screenshots	

Table 5.61 – Ghiro Test Result DIFT-02

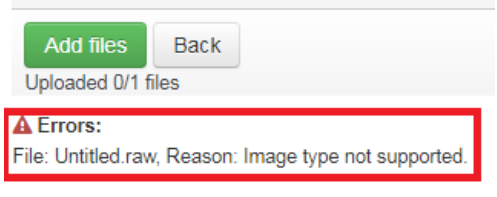
Test Case DIFT-03	
Results	As expected
Analysis and Comments	The tool determined the unsupported file type successfully.
Screenshots	

Table 5.62 – Ghiro Test Result DIFT-03

Test Case DIFT-04	
Results	As expected
Analysis and Comments	The tool uploaded the image directly from the computer successfully.
Screenshots	

Table 5.63 – Ghiro Test Result DIFT-4

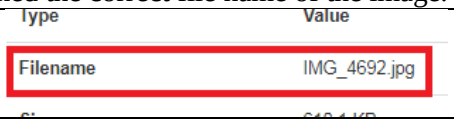
Test Case DIFT-05, 06	
Results	As expected
Analysis and Comments	The tool determined the correct file name of the image.
Screenshots	

Table 5.64 – Ghiro Test Result DIFT-05, 06

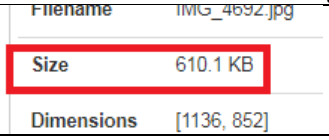
Test Case DIFT-07, 08	
Results	As expected
Analysis and Comments	The tool determined the correct file size of the image.
Screenshots	

Table 5.65 – Ghiro Test Result DIFT-07, 08

Test Case DIFT-09, 10	
Results	As expected
Analysis and Comments	The tool determined the correct dimensions of the image.
Screenshots	

Table 5.66 – Ghiro Test Result DIFT-09, 10

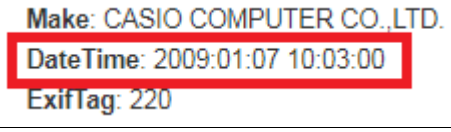
Test Case DIFT-11, 12	
Results	As expected
Analysis and Comments	The tool determined the correct creation timestamp of the image i.e. 2009:01:07 10:03:00.
Screenshots	

Table 5.67 – Ghiro Test Result DIFT-11, 12

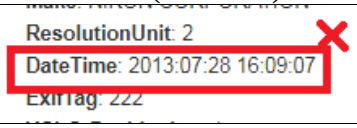
Test Case DIFT-13-15	
Results	Not checked
Analysis and Comments	Modification using some software (like PhotoShop) was detected, while modification using other software (like Paint) was not detected.
Screenshots	

Table 5.68 – Ghiro Test Result DIFT-13-15

Test Case DIFT-16, 17	
Results	Option not available
Analysis and Comments	The tool does not provide the last accessed timestamp.
Screenshots	-

Table 5.69 – Ghiro Test Result DIFT-16, 17

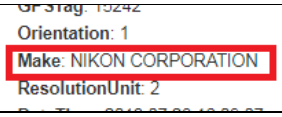
Test Case DIFT-18, 19	
Results	As expected
Analysis and Comments	The tool determined the make of the source camera correctly.
Screenshots	

Table 5.70 – Ghiro Test Result DIFT-18, 19

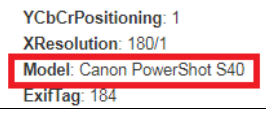
Test Case DIFT-20, 21	
Results	As expected
Analysis and Comments	The tool determined the model of the source camera correctly.
Screenshots	

Table 5.71 – Ghiro Test Result DIFT-20, 21

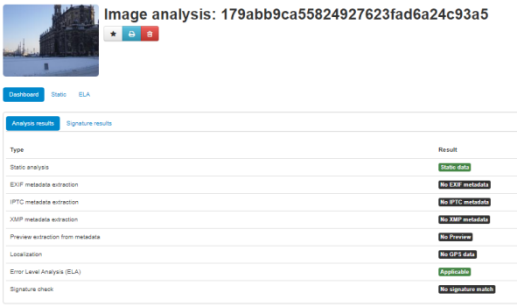
Test Case DIFT-22, 23	
Results	As expected
Analysis and Comments	• The tool was tested with an image that was stripped off metadata using the Exiftool. • The tool gave basic file attributes of the image file. The Exif metadata that was deleted beforehand was not detected.
Screenshots	

Table 5.72 – Ghiro Test Result DIFT-22, 23

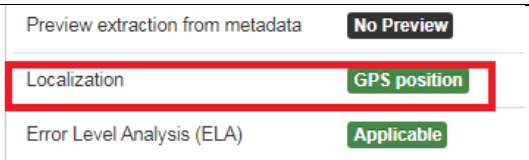
Test Case DIFT-24	
Results	As expected
Analysis and Comments	The tool detected GPS coordinates of the subject image that had GPS tagging enabled.
Screenshots	

Table 5.73 – Ghiro Test Result DIFT-24

Test Case DIFT-25	
Results	As expected
Analysis and Comments	The tool determined the longitude and latitude of the location where the image was taken.
Screenshots	GPSLONGITUDE 116/1 18/1 23882/4096 GPSLATITUDEREF N GPSALTITUDE 304/1 GPSLATITUDE 33/1 52/1 129675/4096 GPSMAPDATUM WGS-84 GPSVERSIONID 2 0 0 0 GPSLONGITUDEREF W GPSALTITUDEREF 0

Table 5.74 – Ghiro Test Result DIFT-25

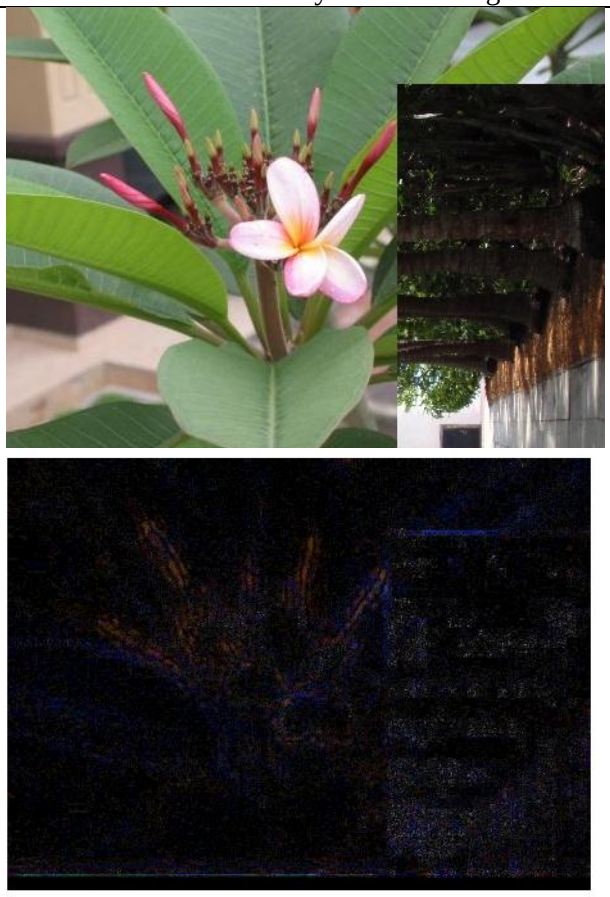
Test Case DIFT-26, 27	
Results	As expected
Analysis and Comments	The tool performed Error Level Analysis of the image.
Screenshots	

Table 5.75 – Ghiro Test Result DIFT-26, 27

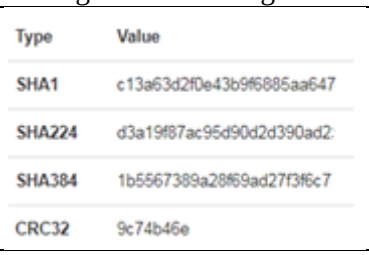
Test Case DIFT-28	
Results	As expected
Analysis and Comments	The tool calculated hash digests of the image.
Screenshots	

Table 5.76 – Ghiro Test Result DIFT-28

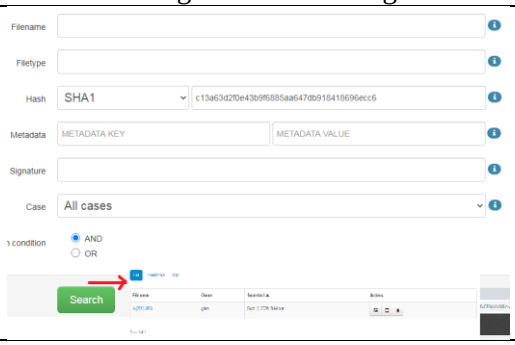
Test Case DIFT-29	
Results	As expected
Analysis and Comments	The tool searched for the image via the hash digest.
Screenshots	

Table 5.77 – Ghiro Test Result DIFT-29

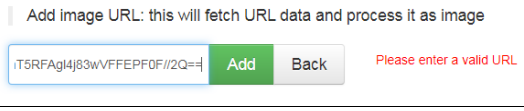
Test Case DIFT-30, 31	
Results	Not checked
Analysis and Comments	The tool was unable to load valid URLs of images.
Screenshots	

Table 5.78 – Ghiro Test Result DIFT-30, 31

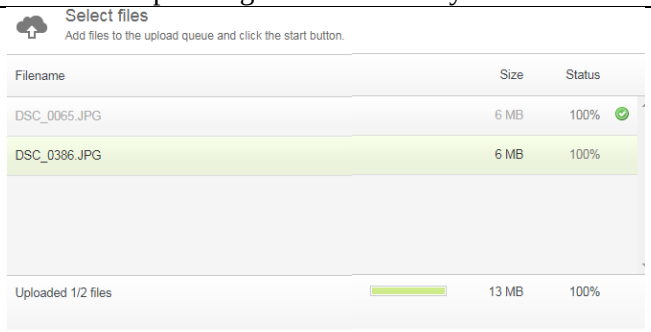
Test Case DIFT-32	
Results	As expected
Analysis and Comments	The tool loaded multiple images simultaneously.
Screenshots	

Table 5.79 – Ghiro Test Result DIFT-32

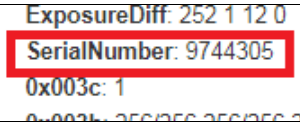
Test Case DIFT-33	
Results	As expected
Analysis and Comments	• The tool determined the serial number of the source camera. • The serial number rarely exists in the metadata once an image has been edited. Any editing discards some metadata fields. So if an image has never been edited there is a possibility that the serial number exists in the metadata. In this case the tool is able to detect it. Otherwise, if it does not exist in the metadata, the tool cannot detect it.
Screenshots	

Table 5.80 – Ghiro Test Result DIFT-33

Test Case DIFT-34	
Results	Not checked
Analysis and Comments	The tool did not determine the orientation of the image.
Screenshots	-

Table 5.81 – Ghiro Test Result DIFT-34

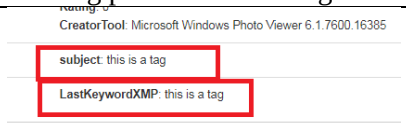
Test Case DIFT-35, 36	
Results	As expected
Analysis and Comments	The tool determined the tag present in the image.
Screenshots	

Table 5.82 – Ghiro Test Result DIFT-35, 36

Test Case DIFT-37, 38	
Results	Not checked
Analysis and Comments	The tool did not determine the bit-depth of the image.
Screenshots	-

Table 5.83 – Ghiro Test Result DIFT-37, 38

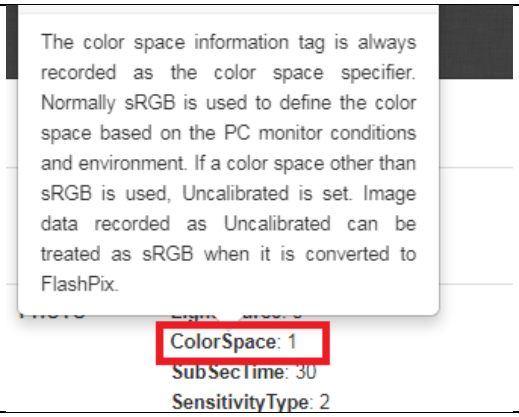
Test Case DIFT-39	
Results	As expected
Analysis and Comments	The tool determined the colour-space of the image. The calibrated and uncalibrated form is used to indicate sRGB and other colour spaces respectively.
Screenshots	

Table 5.84 – Ghiro Test Result DIFT-39

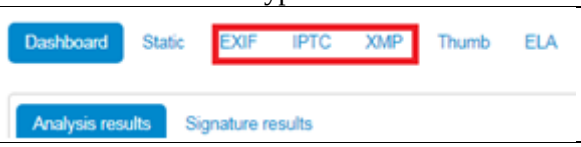
Test Case DIFT-40	
Results	As expected
Analysis and Comments	The tool determined the different types of metadata of the image.
Screenshots	

Table 5.85 – Ghiro Test Result DIFT-40

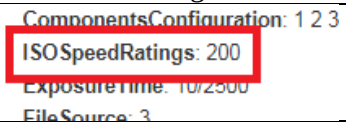
Test Case DIFT-41, 42	
Results	As expected
Analysis and Comments	The tool determined the ISO of the image i.e. 200.
Screenshots	

Table 5.86 – Ghiro Test Result DIFT-41, 42

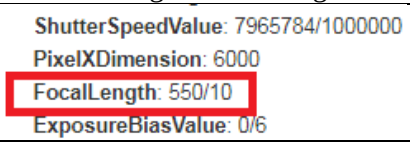
Test Case DIFT-43, 44	
Results	As expected
Analysis and Comments	The tool determined the focal length of the image. i.e. 55mm.
Screenshots	

Table 5.87 – Ghiro Test Result DIFT-43, 44

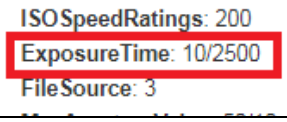
Test Case DIFT-45, 46	
Results	As expected
Analysis and Comments	The tool determined the exposure time/shutter speed of the image i.e. 1/250s.
Screenshots	

Table 5.88 – Ghiro Test Result DIFT-45, 46

Test Case DIFT-47	
Results	Not checked
Analysis and Comments	The tool did not determine the subject distance of the image.
Screenshots	-

Table 5.89 – Ghiro Test Result DIFT-47

Test Case DIFT-48, 49	
Results	Not checked
Analysis and Comments	The tool did not determine the correct flash setting of the image.
Screenshots	Flash: 16 FlashpixVersion: 48 49 48 48 SceneCaptureType: 0

Table 5.90 – Ghiro Test Result DIFT-48, 49

Test Case DIFT-50, 51	
Results	Not checked
Analysis and Comments	The tool did not determine the correct aperture value of the image.
Screenshots	CustomRendered: 0 ApertureValue: 6/1 PixelYDimension: 4000

Table 5.91 – Ghiro Test Result DIFT-50, 51

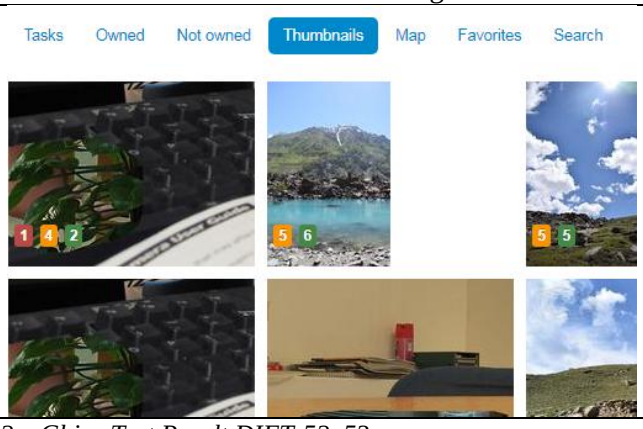
Test Case DIFT-52, 53	
Results	As expected
Analysis and Comments	The tool determined the thumbnail of the image.
Screenshots	

Table 5.92 – Ghiro Test Result DIFT-52, 53

Test Case DIFT-54	
Results	Not checked
Analysis and Comments	The tool did not have a feature to check for thumbnail consistency.
Screenshots	-

Table 5.93 – Ghiro Test Result DIFT-54

Test Case DIFT-55	
Results	Option not available
Analysis and Comments	The tool does not determine the type of tampering.
Screenshots	-

Table 5.94 – Ghiro Test Result DIFT-55

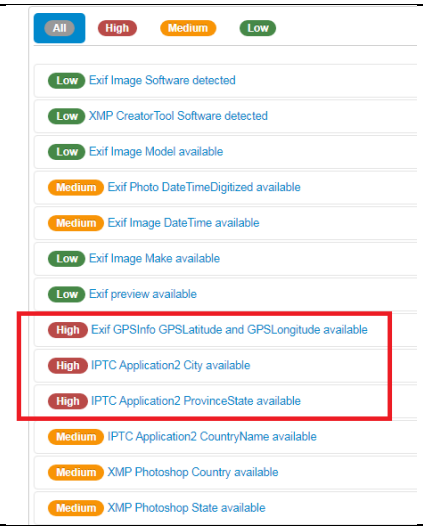
Test Case DIFT-56	
Results	As expected
Analysis and Comments	The tool highlighted the critical metadata of the image. Here the detected GPS information has been highlighted by the tool as high priority.
Screenshots	

Table 5.95 – Ghiro Test Result DIFT-56

Test Case DIFT-57, 58	
Results	Option not available
Analysis and Comments	The tool does not determine the JPEG % of the image.
Screenshots	-

Table 5.96 – Ghiro Test Result DIFT-57, 58

Test Case DIFT-59	
Results	Option not available
Analysis and Comments	The tool does not determine the hidden pixels of the image.
Screenshots	-

Table 5.97 – Ghiro Test Result DIFT-59

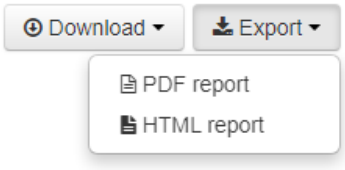
Test Case DIFT-60	
Results	As expected
Analysis and Comments	The tool generated an automated forensic analysis report of the image.
Screenshots	 Refer to Appendix B – Ghiro Report for complete report.

Table 5.98 – Ghiro Test Result DIFT-60

Test Case DIFT-61	
Results	Not checked
Analysis and Comments	The tool did not allow sharing of the report via the tool specifically. Once a report has been downloaded from the tools, it can be shared using other mediums.
Screenshots	-

Table 5.99 – Ghiro Test Result DIFT-61

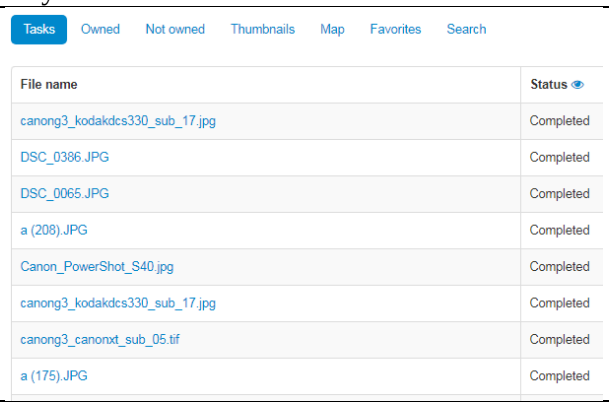
Test Case DIFT-62	
Results	As expected
Analysis and Comments	The tool performed forensic analysis of multiple images simultaneously.
Screenshots	

Table 5.100 – Ghiro Test Result DIFT-62

Test Case DIFT-63	
Results	Option not available
Analysis and Comments	The tool does not add annotations to the image.
Screenshots	-

Table 5.101 – Ghiro Test Result DIFT-63

Test Case DIFT-64	
Results	Option not available
Analysis and Comments	The tool does not make colour adjustments to the image.
Screenshots	-

Table 5.102 – Ghiro Test Result DIFT-64

Test Case DIFT-65	
Results	Option not available
Analysis and Comments	The tool does not have the ability to search for similar pictures online.
Screenshots	-

Table 5.103 – Ghiro Test Result DIFT-65

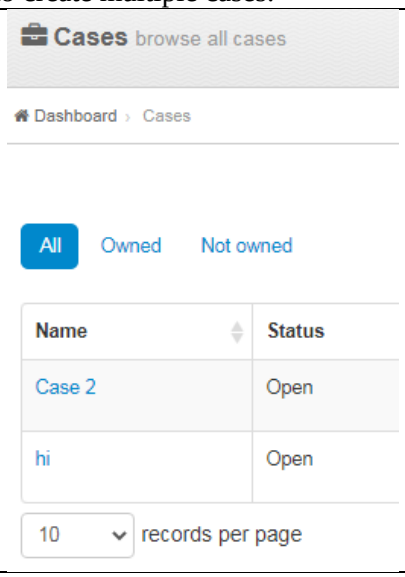
Test Case DIFT-66	
Results	As expected
Analysis and Comments	The tool was able to create multiple cases.
Screenshots	

Table 5.104 – Ghiro Test Result DIFT-66

Test Case DIFT-67	
Results	As expected
Analysis and Comments	The tool was able to create multiple user accounts.
Screenshots	

Table 5.105 – Ghiro Test Result DIFT-67

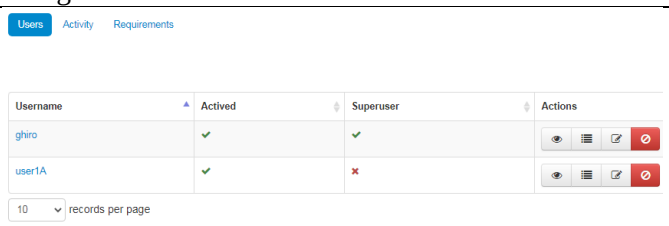
Test Case DIFT-68	
Results	As expected
Analysis and Comments	The tool assigned different access levels to different users.
Screenshots	

Table 5.106 – Ghiro Test Result DIFT-68

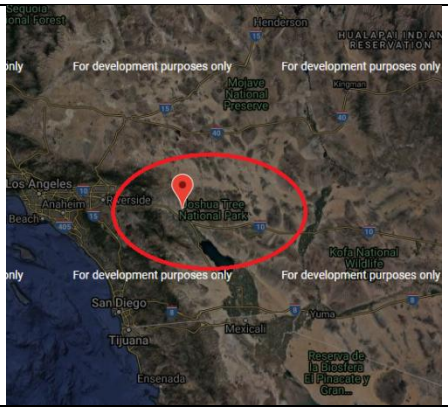
Test Case DIFT-69	
Results	As expected
Analysis and Comments	The tool was able to indicate the determined longitude and latitude on a map.
Screenshots	

Table 5.107 – Ghiro Test Result DIFT-69

5.4.3 Imago Forensics Test Results Report

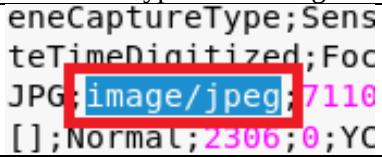
Test Case DIFT-01	
Results	As expected
Analysis and Comments	The tool determined the MIME type of the image correctly.
Screenshots	

Table 5.108 – Imago Forensics Test Result DIFT-01

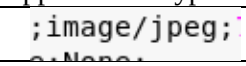
Test Case DIFT-02	
Results	As expected
Analysis and Comments	The tool determined the supported file type successfully i.e. JPEG.
Screenshots	

Table 5.109 – Imago Forensics Test Result DIFT-02

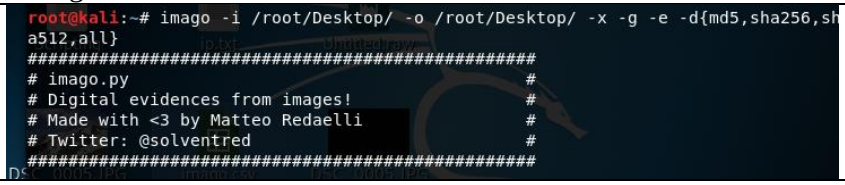
Test Case DIFT-03	
Results	As expected
Analysis and Comments	The tool ignored the unsupported file type and displayed the default message.
Screenshots	

Table 5.110 – Imago Forensics Test Result DIFT-03

Test Case DIFT-04	
Results	As expected
Analysis and Comments	• Since Imago Forensics is a command line tool, it operates by accessing the image directly from its location on the computer (which is specified while typing in the command for forensic analysis). Therefore, for this tool, accessing the image from its location is assumed to be equivalent of uploading the image file into the tool. • The tool accessed image from the desktop successfully.
Screenshots	

Table 5.111 – Imago Forensics Test Result DIFT-04

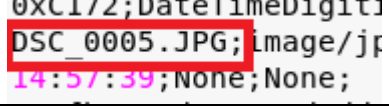
Test Case DIFT-05, 06	
Results	As expected
Analysis and Comments	The tool determined the file name of the image correctly.
Screenshots	

Table 5.112 – Imago Forensics Test Result DIFT-05, 06

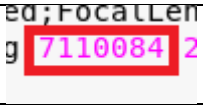
Test Case DIFT-07, 08	
Results	As expected
Analysis and Comments	The tool determined the size of the file correctly.
Screenshots	

Table 5.113 – Imago Forensics Test Result DIFT-07, 08

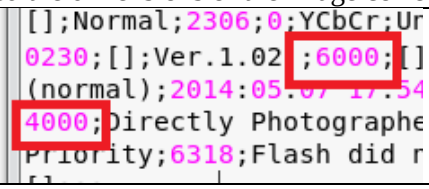
Test Case DIFT-09, 10	
Results	As expected
Analysis and Comments	The tool determined the dimensions of the image correctly.
Screenshots	

Table 5.114 – Imago Forensics Test Result DIFT-09, 10

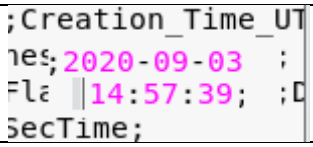
Test Case DIFT-11, 12	
Results	Not checked
Analysis and Comments	The tool was unable to determine the correct creation date and time of the image.
Screenshots	

Table 5.115 – Imago Forensics Test Result DIFT-11, 12

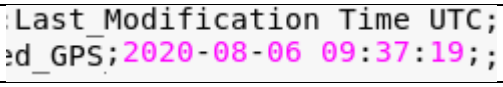
Test Case DIFT-13-15	
Results	Not checked
Analysis and Comments	The tool was unable to determine the correct modification date and time of the image.
Screenshots	

Table 5.116 – Imago Forensics Test Result DIFT-13-15

Test Case DIFT-16, 17	
Results	As expected
Analysis and Comments	The tool determined the last accessed date and time correctly.
Screenshots	;Last_Access_Time_UTC; ; 2020-09-03 14:58:00;

Table 5.117 – Imago Forensics Test Result DIFT-16, 17

Test Case DIFT-18, 19	
Results	As expected
Analysis and Comments	The tool determined the make of source camera correctly.
Screenshots	;Standard;Recommended Exp)0;NIKON CORPORATION;Auto; 0 105 0 115 0 32

Table 5.118 – Imago Forensics Test Result DIFT-18, 19

Test Case DIFT-20, 21	
Results	As expected
Analysis and Comments	The tool determined the model of source camera correctly.
Screenshots	17:54:57;4100;sRGB; ;27;NIKON D5300;Hori nal;[];[];5;Digital

Table 5.119 – Imago Forensics Test Result DIFT-20, 21

Test Case DIFT-22, 23	
Results	As expected
Analysis and Comments	The tool was tested with an image that was stripped off metadata using the Exiftool. All metadata fields had the value 0.
Screenshots	Canon_lxi auto mod 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Table 5.120 – Imago Forensics Test Result DIFT-22, 23

Test Case DIFT-24	
Results	As expected
Analysis and Comments	The tool detected GPS coordinates of the subject image that had GPS tagging enabled.
Screenshots	IMG_4692.jpg;image/jpeg;624744;2020-08-05 17:02:36;2020-09-03 15:36:57;2020-09-03 15:36:28;33.8754608154;-116.301619602;Indio;77719;United States of America;Riverside County;California;92241;us;Dillon Road;871666ee99b90e51c69af02f77f021aa;

Table 5.121 – Imago Forensics Test Result DIFT-24

Test Case DIFT-25	
Results	As expected
Analysis and Comments	The tool determined the longitude and latitude of the location where the image was taken.
Screenshots	96];2006:03:02 11:07:04;287/ 180;[116, 18, 11941/2048];Ho Camera;852;Pixels/Inch;[2,

Table 5.122 – Imago Forensics Test Result DIFT-25

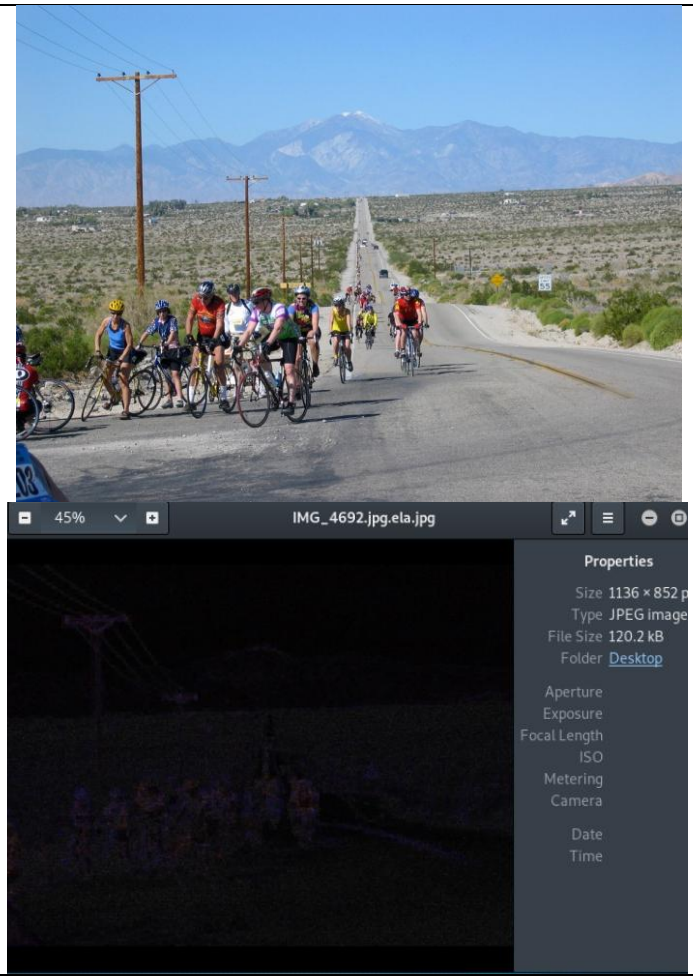
Test Case DIFT-26, 27	
Results	As expected
Analysis and Comments	The tool performed Error Level Analysis of the image.
Screenshots	

Table 5.123 – Imago Forensics Test Result DIFT-26, 27

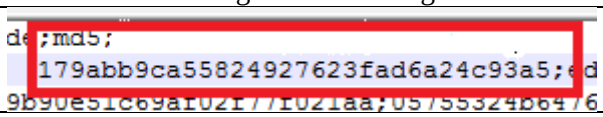
Test Case DIFT-28	
Results	As expected
Analysis and Comments	The tool calculated the hash digests of the image.
Screenshots	

Table 5.124 – Imago Forensics Test Result DIFT-28

Test Case DIFT-29	
Results	Option not available
Analysis and Comments	The tool does not provide the option of search based on hash digests.
Screenshots	-

Table 5.125 – Imago Forensics Test Result DIFT-29

Test Case DIFT-30, 31	
Results	Option not available
Analysis and Comments	The tool does not perform forensic analysis of images obtained via URL.
Screenshots	-

Table 5.126 – Imago Forensics Test Result DIFT-30, 31

Test Case DIFT-32	
Results	As expected
Analysis and Comments	• Since Imago Forensics is a command line tool, it operates by accessing the image directly from its location on the computer (which is specified while typing in the command for forensic analysis). Therefore, for this tool, accessing the image from its location is assumed to be equivalent of uploading the image file into the tool. • The tool accessed multiple images on the desktop simultaneously.
Screenshots	Casio_EX-Z150_0_5002.JPG;IMG_4692.jpg;Canon_Ixus70_1_3725.JPG;

Table 5.127 – Imago Forensics Test Result DIFT-32

Test Case DIFT-33	
Results	Not checked
Analysis and Comments	The tool did not determine the serial number of the source camera.
Screenshots	-

Table 5.128 – Imago Forensics Test Result DIFT-33

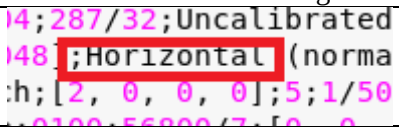
Test Case DIFT-34	
Results	As expected
Analysis and Comments	The tool determined the orientation of the image correctly.
Screenshots	

Table 5.129 – Imago Forensics Test Result DIFT-34

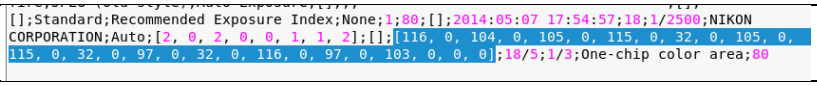
Test Case DIFT-35, 36	
Results	As expected
Analysis and Comments	The tool determined the tag of the image but displayed it in the UCS2 format.
Screenshots	

Table 5.130 – Imago Forensics Test Result DIFT-35, 36

Test Case DIFT-37, 38	
Results	Not checked
Analysis and Comments	The tool did not determine the bit-depth of the image.
Screenshots	-

Table 5.131 – Imago Forensics Test Result DIFT-37, 38

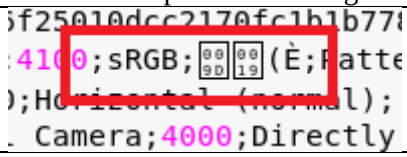
Test Case DIFT-39	
Results	As expected
Analysis and Comments	The tool determined the colour-space of the image correctly.
Screenshots	

Table 5.132 – Imago Forensics Test Result DIFT-39

Test Case DIFT-40	
Results	Not checked
Analysis and Comments	The tool does not determine the different types of metadata.
Screenshots	-

Table 5.133 – Imago Forensics Test Result DIFT-40

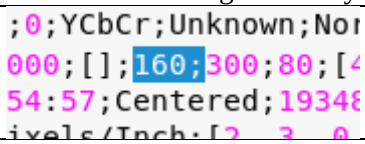
Test Case DIFT-41, 42	
Results	As expected
Analysis and Comments	The tool determined the ISO of the image correctly i.e. 160.
Screenshots	

Table 5.134 – Imago Forensics Test Result DIFT-41, 42

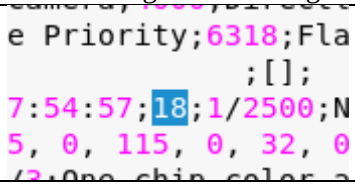
Test Case DIFT-43, 44	
Results	As expected
Analysis and Comments	The tool determined the focal length of the image correctly i.e. 18mm.
Screenshots	

Table 5.135 – Imago Forensics Test Result DIFT-43, 44

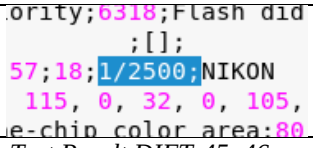
Test Case DIFT-45, 46	
Results	As expected
Analysis and Comments	The tool determined the shutter speed of the image correctly i.e. 1/2500s.
Screenshots	

Table 5.136 – Imago Forensics Test Result DIFT-45, 46

Test Case DIFT-47	
Results	Not checked
Analysis and Comments	The tool did not determine the subject distance of the image.
Screenshots	-

Table 5.137 – Imago Forensics Test Result DIFT-47

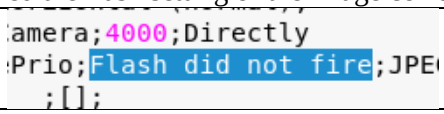
Test Case DIFT-48, 49	
Results	As expected
Analysis and Comments	The tool determined the flash setting of the image correctly.
Screenshots	

Table 5.138 – Imago Forensics Test Result DIFT-48, 49

Test Case DIFT-50, 51	
Results	Not checked
Analysis and Comments	The tool did not determine the aperture value of the image.
Screenshots	-

Table 5.139 – Imago Forensics Test Result DIFT-50, 51

Test Case DIFT-52, 53	
Results	Option not available
Analysis and Comments	The tool does not determine the thumbnail of the image.
Screenshots	-

Table 5.140 – Imago Forensics Test Result DIFT-52, 53

Test Case DIFT-54	
Results	Option not available
Analysis and Comments	The tool does not determine thumbnail inconsistency.
Screenshots	-

Table 5.141 – Imago Forensics Test Result DIFT-54

Test Case DIFT-55	
Results	Option not available
Analysis and Comments	The tool does not determine the type of tampering done with the image.
Screenshots	-

Table 5.142 – Imago Forensics Test Result DIFT-55

Test Case DIFT-56	
Results	Option not available
Analysis and Comments	The tool does not highlight any critical data that might be present.
Screenshots	-

Table 5.143 – Imago Forensics Test Result DIFT-56

Test Case DIFT-57, 58	
Results	Option not available
Analysis and Comments	The tool does not determine the JPEG % of the image.
Screenshots	-

Table 5.144 – Imago Forensics Test Result DIFT-57, 58

Test Case DIFT-59	
Results	Option not available
Analysis and Comments	The tool does not determine any hidden pixels in the image.
Screenshots	-

Table 5.145 – Imago Forensics Test Result DIFT-59

Test Case DIFT-60	
Results	As expected
Analysis and Comments	The tool generated the forensic analysis report in the form of a CSV file.
Screenshots	Refer to Appendix C – Imago Forensics Report for complete report.

Table 5.146 – Imago Forensics Test Result DIFT-60

Test Case DIFT-61	
Results	Not checked
Analysis and Comments	The tool did not provide an option for sharing report via the tool. However the CSV file can be shared via other means.
Screenshots	-

Table 5.147 – Imago Forensics Test Result DIFT-61

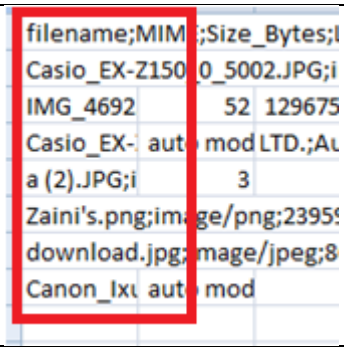
Test Case DIFT-62	
Results	As expected
Analysis and Comments	The tool performed forensic analysis of all the images in the specified location on the computer.
Screenshots	

Table 5.148 – Imago Forensics Test Result DIFT-62

Test Case DIFT-63	
Results	Option not available
Analysis and Comments	The tool does not add annotations to the image.
Screenshots	-

Table 5.149 – Imago Forensics Test Result DIFT-63

Test Case DIFT-64	
Results	Option not available
Analysis and Comments	The tool does not make colour adjustments to the image.
Screenshots	-

Table 5.150 – Imago Forensics Test Result DIFT-64

Test Case DIFT-65	
Results	Option not available
Analysis and Comments	The tool does not do the similar image search.
Screenshots	-

Table 5.151 – Imago Forensics Test Result DIFT-65

Test Case DIFT-66	
Results	Option not available
Analysis and Comments	The tool does not have the ability to make separate cases to distinguish images belonging to different cases.
Screenshots	-

Table 5.152 – Imago Forensics Test Result DIFT-66

Test Case DIFT-67	
Results	Option not available
Analysis and Comments	The tool does not have the ability to create multiple user accounts.
Screenshots	-

Table 5.153 – Imago Forensics Test Result DIFT-67

Test Case DIFT-68	
Results	Option not available
Analysis and Comments	The tool does not have a multi-level access system.
Screenshots	-

Table 5.154 – Imago Forensics Test Result DIFT-68

Test Case DIFT-69	
Results	Option not available
Analysis and Comments	The tool does not map the location of the image on a map.
Screenshots	-

Table 5.155 – Imago Forensics Test Result DIFT-69

5.4.4 Exif Reader Test Results Report

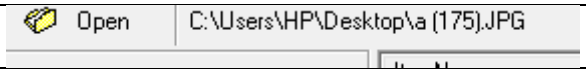
Test Case DIFT-01	
Results	As expected
Analysis and Comments	The tool determined the MIME type of the image correctly and loaded the image on the tool.
Screenshots	

Table 5.156 – Exif Reader Test Result DIFT-01

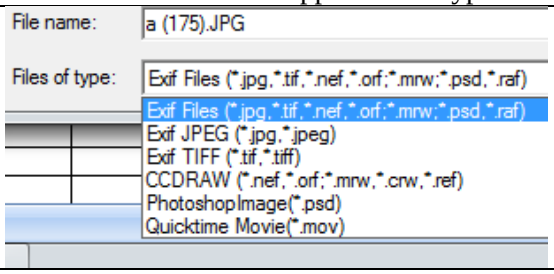
Test Case DIFT-02	
Results	As expected
Analysis and Comments	The tool determined and loaded the supported file type on the tool.
Screenshots	

Table 5.157 – Exif Reader Test Result DIFT-02

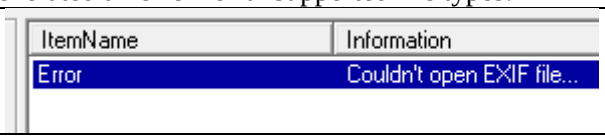
Test Case DIFT-03	
Results	As expected
Analysis and Comments	The tool generated an error for unsupported file types.
Screenshots	

Table 5.158 – Exif Reader Test Result DIFT-03

Test Case DIFT-04	
Results	As expected
Analysis and Comments	The tool loaded the image from the computer successfully.
Screenshots	

Table 5.159 – Exif Reader Test Result DIFT-04

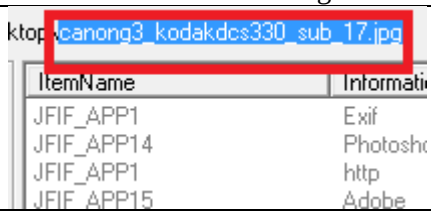
Test Case DIFT-05, 06	
Results	As expected
Analysis and Comments	The tool determined the file name of the image correctly.
Screenshots	

Table 5.160 – Exif Reader Test Result DIFT-05, 06

Test Case DIFT-07, 08	
Results	Not checked
Analysis and Comments	The tool did not determine the file size of the image.
Screenshots	-

Table 5.161 – Exif Reader Test Result DIFT-07, 08

Test Case DIFT-09, 10	
Results	As expected
Analysis and Comments	The tool determined the dimensions of the image correctly.
Screenshots	

Table 5.162 – Exif Reader Test Result DIFT-09, 10

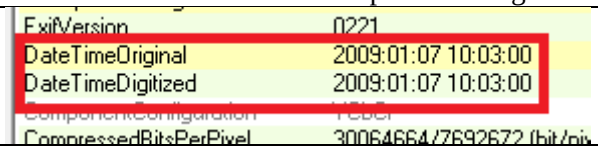
Test Case DIFT-11, 12	
Results	As expected
Analysis and Comments	The tool determined the creation timestamp of the image correctly.
Screenshots	

Table 5.163 – Exif Reader Test Result DIFT-11, 12

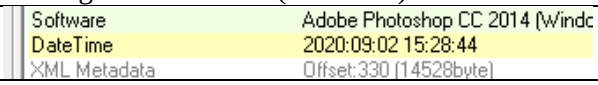
Test Case DIFT-13-15	
Results	Not checked
Analysis and Comments	Modification using some software (like PhotoShop) was detected, while modification using other software (like Paint) was not detected.
Screenshots	

Table 5.164 – Exif Reader Test Result DIFT-13-15

Test Case DIFT-16, 17	
Results	Option not available
Analysis and Comments	The tool does not determine the last accessed timestamp.
Screenshots	-

Table 5.165 – Exif Reader Test Result DIFT-16, 17

Test Case DIFT-18, 19	
Results	As expected
Analysis and Comments	The tool determined the make of source camera correctly.
Screenshots	

Table 5.166 – Exif Reader Test Result DIFT-18, 19

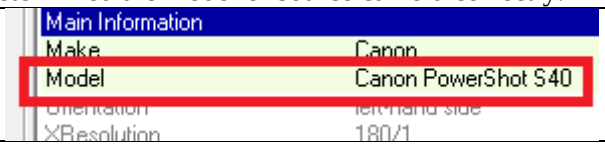
Test Case DIFT-20, 21	
Results	As expected
Analysis and Comments	The tool determined the model of source camera correctly.
Screenshots	

Table 5.167 – Exif Reader Test Result DIFT-20, 21

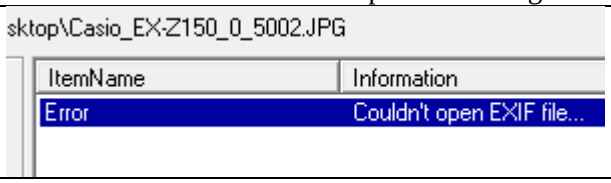
Test Case DIFT-22, 23	
Results	As expected
Analysis and Comments	An image that was stripped off metadata using the Exiftool was uploaded onto the tool. The tool did not upload the image for analysis.
Screenshots	

Table 5.168 – Exif Reader Test Result DIFT-22, 23

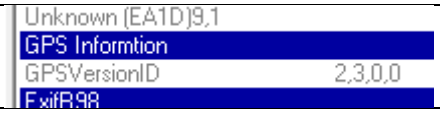
Test Case DIFT-24	
Results	As expected
Analysis and Comments	The tool detected GPS coordinates of the subject image that had GPS tagging enabled.
Screenshots	

Table 5.169 – Exif Reader Test Result DIFT-24

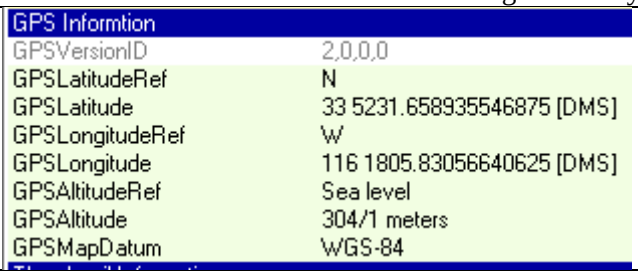
Test Case DIFT-25	
Results	As expected
Analysis and Comments	The tool determined the GPS coordinates of the image correctly.
Screenshots	

Table 5.170 – Exif Reader Test Result DIFT-25

Test Case DIFT-26, 27	
Results	Option not available
Analysis and Comments	The tool does not perform Error Level Analysis of the images.
Screenshots	-

Table 5.171 – Exif Reader Test Result DIFT-26, 27

Test Case DIFT-28	
Results	Option not available
Analysis and Comments	The tool does not calculate hash digests of the images.
Screenshots	-

Table 5.172 – Exif Reader Test Result DIFT-28

Test Case DIFT-29	
Results	Option not available
Analysis and Comments	The tool does not have the ability to search images by hash digests.
Screenshots	-

Table 5.173 – Exif Reader Test Result DIFT-29

Test Case DIFT-30, 31	
Results	Option not available
Analysis and Comments	The tool does not provide the option to upload by URL
Screenshots	-

Table 5.174 – Exif Reader Test Result DIFT-30, 31

Test Case DIFT-32	
Results	As expected
Analysis and Comments	If an image is uploaded from a specific directory on the computer, the tool also uploads other images in that directory. It then provides the option to view them using the left and right arrow keys.
Screenshots	

Table 5.175 – Exif Reader Test Result DIFT-32

Test Case DIFT-33	
Results	Not checked
Analysis and Comments	The tool did not determine the serial number of the source camera.
Screenshots	-

Table 5.176 – Exif Reader Test Result DIFT-33

Test Case DIFT-34	
Results	Not checked
Analysis and Comments	The tool did not determine the orientation of the image.
Screenshots	-

Table 5.177 – Exif Reader Test Result DIFT-34

Test Case DIFT-35, 36	
Results	Not checked
Analysis and Comments	The tool did not determine the tags/comments of the image.
Screenshots	-

Table 5.178 – Exif Reader Test Result DIFT-35, 36

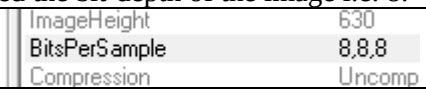
Test Case DIFT-37, 38	
Results	As expected
Analysis and Comments	The tool determined the bit-depth of the image i.e. 8.
Screenshots	

Table 5.179 – Exif Reader Test Result DIFT-37, 38

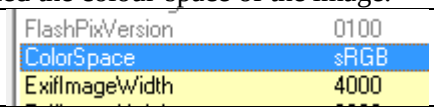
Test Case DIFT-39	
Results	As expected
Analysis and Comments	The tool determined the colour-space of the image.
Screenshots	

Table 5.180 – Exif Reader Test Result DIFT-39

Test Case DIFT-40	
Results	Option not available
Analysis and Comments	The tool is essentially an Exif metadata reader, so it does not read other types of metadata (such as XMP, and IPTC).
Screenshots	-

Table 5.181 – Exif Reader Test Result DIFT-40

Test Case DIFT-41, 42	
Results	As expected
Analysis and Comments	The tool determined the ISO of the image correctly i.e. 200.
Screenshots	

Table 5.182 – Exif Reader Test Result DIFT-41, 42

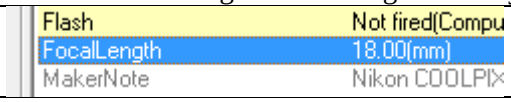
Test Case DIFT-43, 44	
Results	As expected
Analysis and Comments	The tool determined the focal length of the image correctly i.e. 18mm.
Screenshots	

Table 5.183 – Exif Reader Test Result DIFT-43, 44

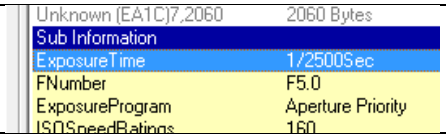
Test Case DIFT-45, 46	
Results	As expected
Analysis and Comments	The tool determined the shutter speed of the image correctly i.e. 1/2500s.
Screenshots	

Table 5.184 – Exif Reader Test Result DIFT-45, 46

Test Case DIFT-47	
Results	Not checked
Analysis and Comments	The tool did not determine the subject distance of the image.
Screenshots	-

Table 5.185 – Test Result DIFT-47

Test Case DIFT-48, 49	
Results	As expected
Analysis and Comments	The tool determined the flash setting of the image.
Screenshots	

Table 5.186 – Exif Reader Test Result DIFT-48, 49

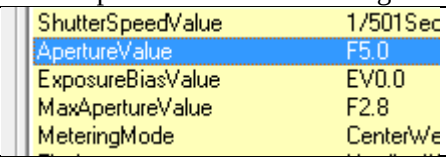
Test Case DIFT-50, 51	
Results	As expected
Analysis and Comments	The tool determined the aperture value of the image i.e. f/5.
Screenshots	

Table 5.187 – Exif Reader Test Result DIFT-50, 51

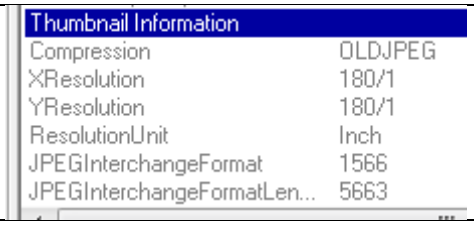
Test Case DIFT-52, 53	
Results	As expected
Analysis and Comments	The tool determined the thumbnail information of the image.
Screenshots	

Table 5.188 – Exif Reader Test Result DIFT-52, 53

Test Case DIFT-54	
Results	Option not available
Analysis and Comments	The tool does not determine the thumbnail consistency of the image.
Screenshots	-

Table 5.189 – Exif Reader Test Result DIFT-54

Test Case DIFT-55	
Results	Option not available
Analysis and Comments	The tool does not determine the type of tampering.
Screenshots	-

Table 5.190 – Test Result DIFT-55

Test Case DIFT-56	
Results	Option not available
Analysis and Comments	The tool does not highlight critical metadata of the image.
Screenshots	-

Table 5.191 – Exif Reader Test Result DIFT-56

Test Case DIFT-57, 58	
Results	Option not available
Analysis and Comments	The tool does not determine the JPEG % of the image.
Screenshots	-

Table 5.192 – Exif Reader Test Result DIFT-57, 58

Test Case DIFT-59	
Results	Option not available
Analysis and Comments	The tool does not determine the hidden pixels of the image.
Screenshots	-

Table 5.193 – Exif Reader Test Result DIFT-59

Test Case DIFT-60	
Results	As expected
Analysis and Comments	The tool created a forensic analysis report of the image.
Screenshots	Refer to Appendix D – Imago Forensics Report for complete report.

Table 5.194 – Exif Reader Test Result DIFT-60

Test Case DIFT-61	
Results	Option not available
Analysis and Comments	The tool does not have the ability to share reports.
Screenshots	-

Table 5.195 – Exif Reader Test Result DIFT-61

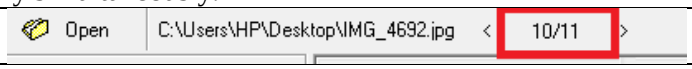
Test Case DIFT-62	
Results	As expected
Analysis and Comments	The tool performed forensic analysis of multiple images in the same directory simultaneously.
Screenshots	

Table 5.196 – Exif Reader Test Result DIFT-62

Test Case DIFT-63	
Results	Option not available
Analysis and Comments	The tool does not add annotations to the image.
Screenshots	-

Table 5.197 – Exif Reader Test Result DIFT-63

Test Case DIFT-64	
Results	Option not available
Analysis and Comments	The tool does not make colour adjustments to the image.
Screenshots	-

Table 5.198 – Exif Reader Test Result DIFT-64

Test Case DIFT-65	
Results	Option not available
Analysis and Comments	The tool does not perform similar image search.
Screenshots	-

Table 5.199 – Exif Reader Test Result DIFT-65

Test Case DIFT-66	
Results	Option not available
Analysis and Comments	The tool does not have the ability to make separate cases to distinguish images belonging to different cases.
Screenshots	-

Table 5.200 – Exif Reader Test Result DIFT-66

Test Case DIFT-67	
Results	Option not available
Analysis and Comments	The tool does not have the ability to create multiple use accounts.
Screenshots	-

Table 5.201 – Exif Reader Test Result DIFT-67

Test Case DIFT-68	
Results	Option not available
Analysis and Comments	The tool does not have a multi-level access system.
Screenshots	-

Table 5.202 – Exif Reader Test Result DIFT-68

Test Case DIFT-69	
Results	Option not available
Analysis and Comments	The tool does not map the location of the image on a map.
Screenshots	-

Table 5.203 – Exif Reader Test Result DIFT-69

5.5 Summary of Results

FotoForensics was successful in conforming to all the core assertions efficiently apart from assertions related to timestamps. It also provided a lot of optional features and conformed to them efficiently. However, it did not provide the optional features of multiple user accounts, by-case distinction and multi-level access system. It also does not provide the functionality of analysing multiple images simultaneously. Overall, FotoForensics was user-friendly and efficient in the functionalities that it provided.

Ghiro was also successful in conforming to all the core assertions apart from assertions related to timestamps. It also provided the optional features of multiple user accounts, by-case distinction and multi-level access system and conformed to them efficiently. However, it was unable to conform to some of the other optional features. The user interface of Ghiro was practical and convenient. It was also able to perform forensic analysis of multiple images simultaneously which is an important functionality in cases involving multiple images.

Imago Forensics was also successful in conforming to all the core assertions apart from some assertions related to timestamps. It provided a limited number of optional features. This tool extracted results in the form of a CSV file. Reading results and finding particular result fields proved to be inefficient. Hence, this tool was not user-friendly.

Exif Reader was successful in most core assertions except some assertions related to timestamps. It does not provide tamper detection (ELA) which is an important requirement for image forensics tools. Also, this tool provided a limited number of optional features. Overall, the interface of Exif Reader was user-friendly but it was unable to provide important functionalities.

6. CONCLUSION AND FUTURE WORK

This chapter contains the following:

- Section 6.1 concludes this research.
- Section 6.2 provides future work.

6.1 Conclusion

Image forensics is a new research discipline and the scope for discovery, design and improvements in the techniques and tools involved are vast. The important and progressive aspect of evaluation frameworks is the acceleration in advancement and practicality of the forensic practices. Vaguely, this can be termed as technical hit and trial; the 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 each and 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. A convenient aspect of the evaluation frameworks is that they can be revisited and improved indefinitely, as the tools evolve and advance. More test assertions can be added with additional test cases. The continuous technical hit and trial is an attempt to set standards for the tools to achieve. These standards complement all areas of life in which the tool may be employed e.g. criminal investigation, commercial use, or academic research and study.

This research work is the development of the first evaluation framework for image forensics tools. It is based on the conformance methodology adopted by the CFTT project (where they have fashioned similar testing frameworks for other digital forensics disciplines).

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 comparative analysis of the results obtained showed that FotoForensics was able to perform efficiently in most test cases. It is consequently the most efficient tool out of all the four tools tested. It also offers a lot of optional features. The version of FotoForensics that was tested in this research work was the free online version. It also has a paid version i.e. the FotoForensics Lab which is more secure (because online tools are more vulnerable to attacks compared to the ones that can be downloaded and installed on a local machine).

Ghiro, an open-source tool, is the second most useful tool according to the results. This is because Ghiro is easy to use and has some additional optional features (such as multiple user accounts, case-by-case distinction, multi-level access system, and highlighting critical forensic data). But Ghiro is also a web interface tool, which means that the security of the results may be more at risk when compared to results generated using a desktop tool.

Imago Forensics is a command line tool and requires effort from the user in order to obtain results. Also, navigating through the dump of metadata information in the CSV file to find a specific data field can be time-consuming and inefficient.

Exif Reader is a simple Windows tool that reads the Exif metadata of an image. It does not provide support for many other features.

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, the efficiency of FotoForensics and the usability of Ghiro combined would make a very practical image forensics tool.

6.2 Future Work

- 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 tools (apart from the four included in this thesis) 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 to their products.

REFERENCES

[1] Redi, J. A., Taktak, W., & Dugelay, J. L. "Digital image forensics: A booklet for beginners". Article, *Multimedia Tools and Applications*, 2011, 133–162. https://doi.org/10.1007/s11042-010-0620-1.

[2] "Photos, Photos Everywhere." *The New York Times article*, 29 July 2015, www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html.

[3] T. Qazi et al., "Survey on blind image forgery detection," *Journal IET Image Processing*, vol. 7, no. 7, pp. 660–670, 2013.

[4] robin.materese@nist.gov. 'Digital Evidence.' NIST article, 30 June 2016, www.nist.gov/topics/digital-evidence.

[5] A. Piva, "An Overview on Image Forensics," ISRN Signal Processing., review article, vol. 2013, pp. 1–22, 2013.

[6] David P. Nagosky. "Admissibility of Digital Photographs in Criminal Cases*". Journal FBI Law Enforcement Bulletin* Volume: 74 Issue:12 December 2005 Pages:1-8, Dec. 2005.

[7] Zachariah B. Parry. "Digital manipulation and photographic evidence: defrauding the courts one thousand words at a time" *Journal of Law, Technology and Policy,* Vol. 2009.

[8] thelma.allen@nist.gov. "Computer Forensics Tool Testing Program (CFTT)." NIST, 8 May 2017, www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

[9] Factor, Hacker. "FotoForensics" Fotoforensics.Com, 2012, fotoforensics.com/.

[10] "Ghiro - Automated Digital Image Forensics Tool.", www.getghiro.org/.

[11] Redaelli, Matteo. "Redaelli/Imago-Forensics." GitHub, 26 Sept. 2019, github.com/redaelli/imago-forensics.

[12] Yoshimoto, Ryuuji. "Exif Reader - English Version." Www.Takenet.or.Jp, www.takenet.or.jp/~ryuuji/minisoft/exifread/english/.

[13] T. Gloe and R. Böhme, "The dresden image database for benchmarking digital image forensics," Journal of Digital Forensic Practice., vol. 3, no. 2–4, pp. 150–159, 2010.

[14] Y.-F. H. and S. Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency" Department of Electrical Engineering Columbia University," IEEE International Conference on Multimedia and Expo, pp. 549–552, 2006.

[15] Github. "EXIF Sample Images." Https://Github.Com/Ianare/Exif-Samples.

[16] A. Singh, N. Jindal, K. Singh "A Review on Digital Image Forensics," International Conference on Signal Processing., 2017.

[17] R. S. Khalaf and A. Varol, "Digital forensics: Focusing on image forensics," 7th International Symposium on Digital Forensics and Security. ISDFS 2019, pp. 1–5, 2019.

[18] T. Van Lanh, K. Sen Chong, S. Emmanuel, and M. S. Kankanhalli, "A survey on digital camera image forensic methods," Proc. 2007 IEEE International Conference on Multimedia and Expo, ICME 2007, pp. 16–19, 2007.

[19] M. Ali Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," 2014 IEEE 11th Int. Multi-Conference Syst. Signals Devices, SSD 2014, pp. 1–5, 2014.

[20] M. Arun Anoop, "Image forgery and its detection: A survey," ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Comm. Systems., 2015.

[21] S. Al Sharif, M. Al Ali, N. Al Reqabi, F. Iqbal, T. Baker, and A. Marrington, "Magec: An image searching tool for detecting forged images in forensic investigation," 2016 8th IFIP International Conference on New Technologies, Mobility and Security. NTMS, 2016.

[22] L. U. P. Singh and A. Agrawal, "NO-SHAM: An effective tool based on a novel hybrid approach to detect copy-move forgery in images," 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics. UPCON 2017.

[23] T. Mehrotra and B. M. Mehtre, "An automated forensic tool for image metadata and Windows 7 Recycle Bin," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies. ICCICCT 2014, pp. 419–425, 2014.

[24] S. Mashhadani, H. Al-Kawaz, N. Clarke, S. Furnell, and F. Li, "A novel multimedia-forensic analysis tool (M-FAT)," 2017 12th International Conference for Internet Technology and Secured Transactions. ICITST 2017, pp. 388–395, 2018.

[25] J. Charpe and A. Bhattacharya, "Revealing image forgery through image manipulation detection," Global Conference on Communication Technologies. GCCT 2015, no. Gcct, pp. 723–727, 2015.

[26] J. Fan, T. Chen, and J. Cao, "Image tampering detection using noise histogram features," International Conference on Digital Signal Processing. DSP, vol. 2015-Septe, pp. 1044–1048, 2015.

[27] J. De Bock and P. De Smet, "JPGcarve: An Advanced Tool for Automated Recovery of Fragmented JPEG Files," Journal IEEE Transactions on Information Forensics and Security 11(1):19—34, 2016.

[28] "Towards learned color representations for image splicing detection" Benjamin Hadwiger, Daniele Baracchi, Alessandro Piva, Christian Riess, ICASSP 2019 - IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) pp. 8281–8285, 2019.

[29] W. Van Der Meer, K. K. R. Choo, M. T. Kechadi, and N. A. Le-Khac, "Investigation and automating extraction of thumbnails produced by image viewers," 2017 IEEE Trustcom/BigDataSE/ICESS.

[30] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", In *ACM Multimedia and Security Workshop*, New York, NY, 2005.

[31] Y.-F. Hsu and S. F. Chang, "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency", In *ICME*, Toronto, Canada, July 2006.

[32] M. Anobah, S. Saleem, and O. Popov, "Testing Framework for Mobile Device Forensics Tools," Journal of Digital Forensics, Security and Law, pp. 221–234, 2014.

[33] M. Anobah, "Testing Framework for Mobile Forensic Investigation Tools," Thesis, 2013.

[34] Zia Rehman, A. Ahmad, and S. Saleem, "A Brief Survey of Memory Analysis Tools," NUST Journal of Engineering Sciences, vol. 10, no. 2, 2017.

[35] Zia Rehman and S. Saleem, "Windows Memory Forensics Tools Specification, Test Assertions and Test Plan," Thesis, 2017.

[36] S. Saleem, O. Popov, O. K. Appiah-Kubi "Evaluating and comparing tools for mobile device forensics using qualitative analysis," 4th International Conference on Digital Forensics & Cyber Crime, pp. 156–174, 2013.

[37] O. K. Appiah-Kubi, "Evaluation of UFED Physical Pro 1.1.3.8 and XRY 5.0 : Tools for Extracting e-Evidence from Mobile Devices," Thesis, 2011.

[38] A. K. Kubi, S. Saleem, and O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," 2011 5th International Conference on Application of Information and Communication Technologies (AICT), no. 10, 2011.

[39] K. Piirainen, R. Gonzalez, and G. Kolfschoten, “Quo Vadis, Design Science? A Survey of Literature’, in Global Perspectives on Design Science Research, International Conference on design science research in information systems, pp. 93–108,” 2010.

[40] jbass, “Overview of Conformance Testing”, NIST, 8 Sept. 2010, https://www.nist.gov/itl/ssd/information-systems-group/overview-conformance-testing.

[41] E. H. Holder and L. O. Robinson, “Special Report Test Results for Digital Data Acquisition Tool”, CFTT, NIST, Nij, 2008.

[42] A. Castiglione, G. Cattaneo, M. Cembalo, and U. F. Petrillo, “Source camera identification in real practice: A preliminary experimentation,” Proc. - 2010 International Conference on Broadband, Wireless Computing Communication and Applications. BWCCA 2010, pp. 417–422, 2010.

[43] M. C. Stamm and K. J. R. Liu, “Anti-forensics of digital image compression,” Journal IEEE Transactions on Information Forensics and Security., vol. 6, no. 3 PART 2, pp. 1050–1065, 2011.

[44] I. A. Yari and S. Zargari, “An Overview and Computer Forensic Challenges in Image Steganography,” 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 360–364, 2018.

[45] Y. Kim, J. Bang, S. Lee, and J. Lim, “Detection of hidden information in forensic tools,” 2008 International Conference on Information Security and Assurance (isa 2008), pp. 248–252, 2008.

[46] L. Lin et al., “The impact of exposure settings in digital image forensics,” 2018 25th IEEE International Conference on Image Processing (ICIP), pp. 540–544, 2018.

[47] V. S. Vijayalakshmi, B. Shwetha, and S. V. Sathyanarayana, “Image classifier based digital image forensic detection - A review and simulations,” 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), pp. 23–28, 2016.

[48] A. Elliethy and G. Sharma, “Image anonymization for PRNU forensics: A set theoretic framework addressing compression resilience,” 2016 IEEE International Conference on Image Processing (ICIP), no. 3, pp. 3907–3911, 2016.

[49] Z. Chen, Y. Zhao, and R. Ni, “Forensics of blurred images based on no-reference image quality assessment,” IEEE China Summit and International Conference on Signal and Information Processing, pp. 437–441, 2013.

[50] N. Kanagavalli, L. Latha, “A survey of copy-move image forgery detection techniques,” 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1–6, 2017.

[51] D. Hu, L. Wang, Y. Zhou, Y. Zhou, X. Jiang, and L. Ma, “D-S evidence theory based digital image trustworthiness evaluation model,” 2009 International Conference on Multimedia Information Networking and Security, vol. 1, pp. 85–89, 2009.

[52] H. Zeng, J. Chen, X. Kang, and W. Zeng, “Removing camera fingerprint to disguise photograph source,” 2015 IEEE International Conference on Image Processing (ICIP), vol, no. 2011, pp. 1687–1691, 2015.

APPENDIX A – FOTOFORENSICS REPORT

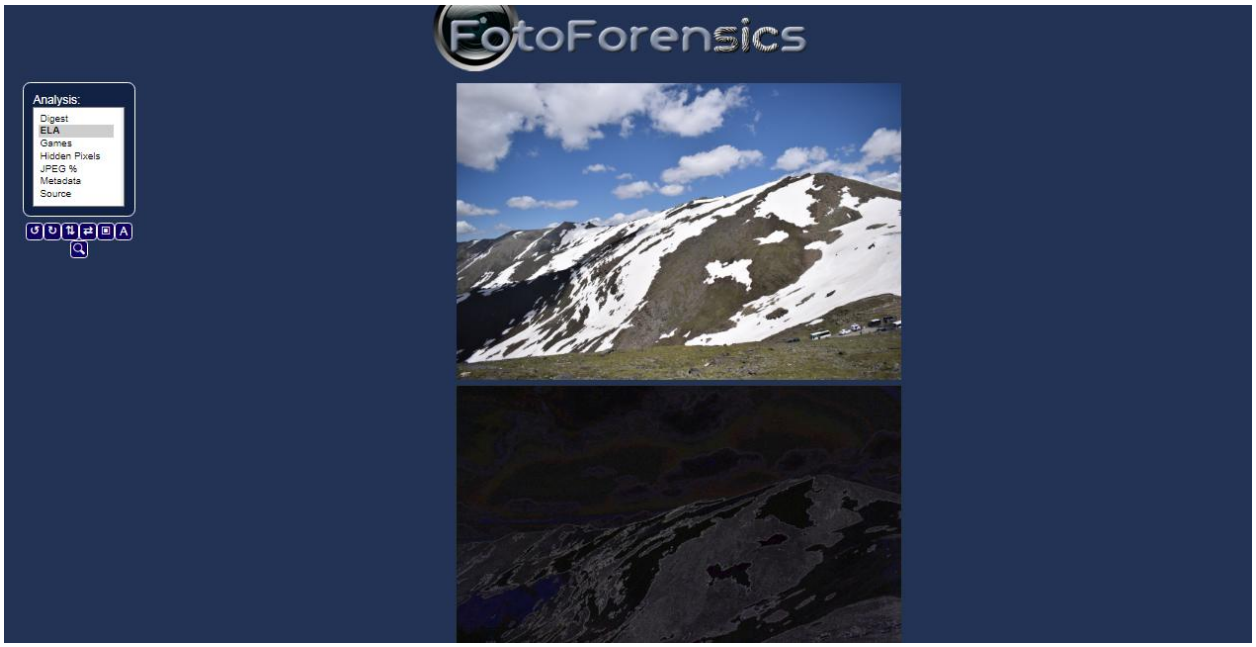


Fig A.1 – FotoForensics Error Level Analysis (ELA)

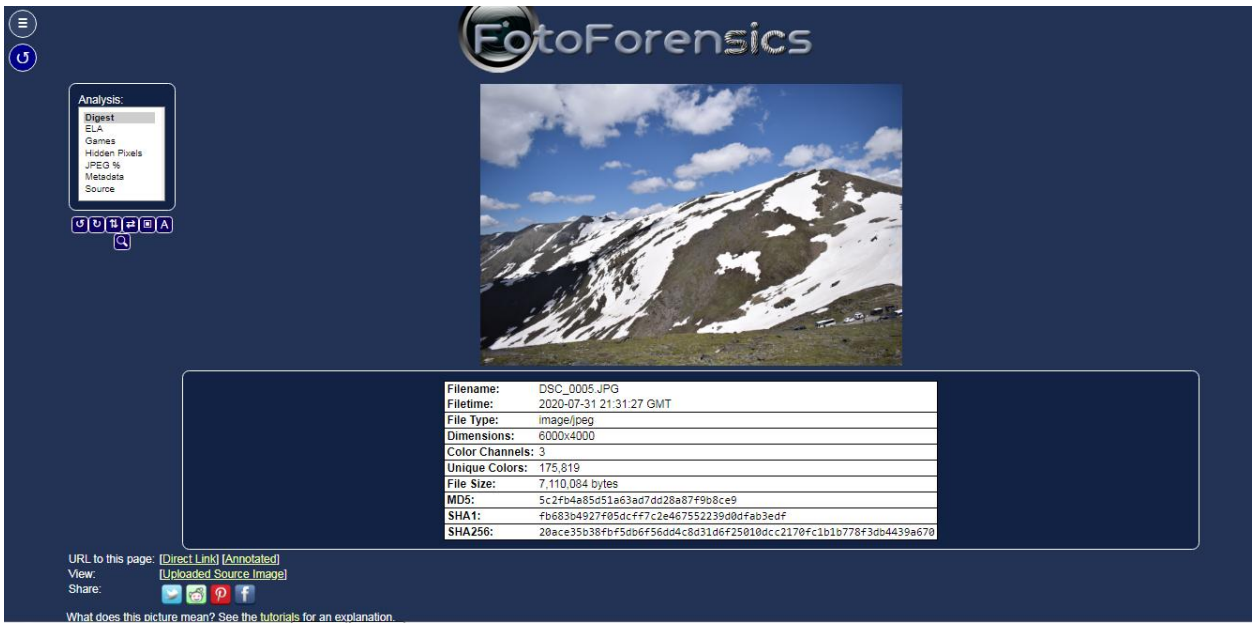


Fig A.2 – FotoForensics Hash Digests

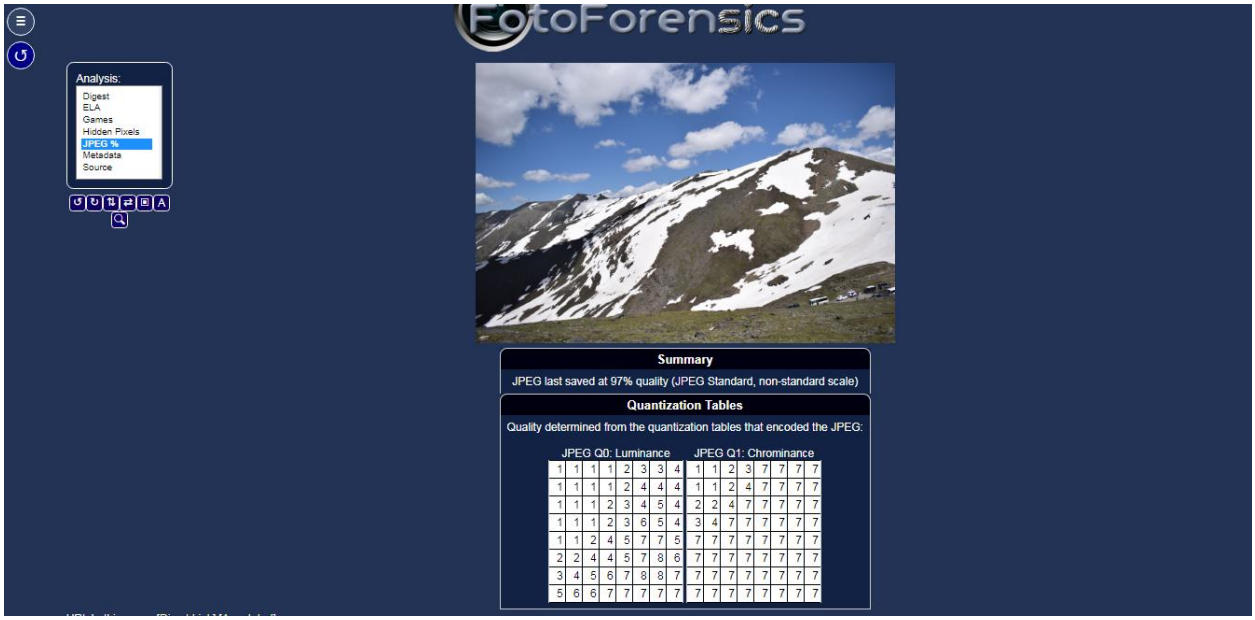


Fig A.3 – FotoForensics JPEG%

Fig A.4 – FotoForensics Metadata

APPENDIX B – GHIRO REPORT

Image analysis: 871666ee99b90e51c69af02f77f021aa

Fig B.1 – Ghiro Image under Analysis

Dashboard

Type	Result
Static analysis	Static data
EXIF metadata extraction	EXIF Metadata
IPTC metadata extraction	IPTC Metadata
XMP metadata extraction	XMP Metadata
Preview extraction from metadata	No Preview
Localization	GPS position
Error Level Analysis (ELA)	Applicable
Signature check	Signature matches

Fig B.2 – Ghiro Dashboard

Static Data

Type	Value
Filename	IMG_4692.jpg
Size	610.1 KB
Dimensions	[1136, 852]
Analyzed at	July 31, 2020, 2:19 p.m.

Static Data - FileType

Type
JPEG image data, JFIF standard 1.02

Fig B.3 – Ghiro Static Data and Static Data – FileType

Static Data - Hashes

Type	Value
SHA1	2b125736f64ff94ce423358edc5771d055cdfd7b
SHA224	ea432f7abf4f1e977e82d14d7c802c0cad5fee884094c45384a3d9b46
SHA384	d81eec56014ddaf00bdd4c0625612f3486f9d8f1edfe656527b6a272635bfc4b581f7552fc3f4616772533e89c244e65
CRC32	ce2b5598
SHA256	05755324b6476d2b31f2d88f1210782c3fdce880e4b6bfa9a5edb23d8be5bedb
SHA512	d3be8dc4ece5b6d0f9b0d58d9ee49cc7a5eee2a8d7e0ee5f570d6d98ee0f1f534506649ba124dcc16cc29a79acfad9efe8739994f9b3bec85f1330b586ac7283
MD5	871666ee99b90e51c69af02f77f021aa

Fig B.4 – Ghiro Static Data – Hashes

Static Data - Strings

Relevant strings

http://www.apple.com/DTDs/PropertyList-1.0.dtd
http://ns.adobe.com/xap/1.0/
http://www.w3.org/1999/02/22-rdf-syntax-ns
http://ns.adobe.com/iX/1.0/'>
http://ns.adobe.com/pdf/1.3/'>
http://ns.adobe.com/photoshop/1.0/'>
http://ns.adobe.com/xap/1.0/'>
http://ns.adobe.com/xap/1.0/mm/'>

Fig B.5 – Ghiro Static Data – Strings

EXIF metadata extraction

Segment	Key: Value
PHOTO	**ColorSpace**: 65535 **ExposureMode**: 0 **Flash**: 24 **FlashpixVersion**: 48 49 48 48 **SceneCaptureType**: 0 **MeteringMode**: 5 **ExifVersion**: 48 50 50 48 **ExposureBiasValue**: 0/3 **ShutterSpeedValue**: 287/32 **PixelXDimension**: 1136 **FocalLength**: 749/32 **DateTimeDigitized**: 2006:02:11 11:06:37 **ApertureValue**: 170/32 **FocalPlaneYResolution**: 1704000/210 **WhiteBalance**: 0 **CompressedBitsPerPixel**: 5/1 **SensingMethod**: 2 **FNumber**: 63/10 **CustomRendered**: 0 **DateTimeOriginal**: 2006:02:11 11:06:37 **PixelYDimension**: 852 **ComponentsConfiguration**: 1 2 3 0 **FocalPlaneXResolution**: 2272000/280 **FileSource**: 3 **ExposureTime**: 1/500 **FocalPlaneResolutionUnit**: 2 **MaxApertureValue**: 147/32 **DigitalZoomRatio**: 2272/2272
IMAGE	**YResolution**: 180/1 **GPSTag**: 988 **Orientation**: 1 **Make**: Canon **ResolutionUnit**: 2 **DateTime**: 2006:03:02 11:07:04 **ExifTag**: 240 **YCbCrPositioning**: 1 **XResolution**: 180/1 **Model**: Canon PowerShot A80 **Software**: Adobe Photoshop Elements 2.0
IMAGE	**YResolution**: 180/1 **GPSTag**: 988 **Orientation**: 1 **Make**: Canon **ResolutionUnit**: 2 **DateTime**: 2006:03:02 11:07:04 **ExifTag**: 240 **YCbCrPositioning**: 1 **XResolution**: 180/1 **Model**: Canon PowerShot A80 **Software**: Adobe Photoshop Elements 2.0
THUMBNAIL	**YResolution**: 72/1 **ResolutionUnit**: 2 **Compression**: 6 **XResolution**: 72/1 **JPEGInterchangeFormatLength**: 0 **JPEGInterchangeFormat**: 1250
GPSINFO	**GPSLongitude**: 116/1 18/1 23882/4096 **GPSLatitudeRef**: N **GPSAltitude**: 304/1 **GPSLatitude**: 33/1 52/1 129675/4096 **GPSMapDatum**: WGS-84 **GPSVersionID**: 2 0 0 0 **GPSLongitudeRef**: W **GPSAltitudeRef**: 0

Fig B.6 – Ghiro Exif Metadata Extraction

IPTC metadata extraction

Segment	Key: Value
APPLICATION2	**CountryName**: United States **City**: 18 km NE of Cathedral City **ProvinceState**: California **RecordVersion**: 2

Fig B.7 – Ghiro IPTC Metadata Extraction

XMP metadata extraction

Segment	Key: Value
XMPMM	**InstanceID**: uuid:4dd5c600-ab6e-11da-9542-bfb44dc3b46e **DocumentID**: adobe:docid:photoshop:4dd5c5ff-ab6e-11da-9542-bfb44dc3b46e
PHOTOSHOP	**City**: 18 km NE of Cathedral City **State**: California **Country**: United States
XMP	**CreatorTool**: Adobe Photoshop Elements for Macintosh, version 2.0

Fig B.8 – Ghiro XMP Metadata Extraction

Localization

GPSLONGITUDE	116/1 18/1 23882/4096
GPSLATITUDEREF	N
GPSALTITUDE	304/1
GPSLATITUDE	33/1 52/1 129675/4096
GPSMAPDATUM	WGS-84
GPSVERSIONID	2 0 0 0
GPSLONGITUDEREF	W
GPSALTITUDEREF	0

Latitude	33.8754608154
Longitude	-116.301619602
Altitude	304.0

Fig B.9 – Ghiro Localisation

Fig B.10 – Ghiro Error Level Analysis (ELA)

Signature check

Exif Image Software detected	
Category:	Editing information
Description:	This tag records the name and version of the software or firmware of the camera or image input device used to generate the image. The detailed format is not specified, but it is recommended that the example shown below be followed. When the field is left blank, it is treated as unknown.
Additional data:	EXIF Image Software: *Adobe Photoshop Elements 2.0*

XMP CreatorTool Software detected	
Category:	Editing information
Description:	Photo editing software name is available in metadata
Additional data:	XMP CreatorTool: *Adobe Photoshop Elements for Macintosh, version 2.0*

Exif Image Model available	
Category:	Hardware information
Description:	The model name or model number of the equipment. This is the model name or number of the DSC, scanner, video digitizer or other equipment that generated the image. When the field is left blank, it is treated as unknown.
Additional data:	EXIF Image Model: *Canon PowerShot A80*

Exif Photo DateTimeDigitized available	
Category:	Time information
Description:	The date and time when the image was stored as digital data.
Additional data:	EXIF Photo DateTimeDigitized: *2006:02:11 11:06:37*

Exif Image DateTime available	
Category:	Time information
Description:	Photo date and time is available in metadata
Additional data:	EXIF Image DateTime: *2006:03:02 11:07:04*

Exif Image Make available	
Category:	Hardware information
Description:	The manufacturer of the recording equipment. This is the manufacturer of the DSC, scanner, video digitizer or other equipment that generated the image. When the field is left blank, it is treated as unknown.
Additional data:	EXIF Image Make: *Canon*

Exif preview available	
Category:	Editing information
Description:	A thumbnail in exif metadata is available

Fig B.11 – Ghiro Signatures – Part I

Exif GPSInfo GPSLatitude and GPSLongitude available	
Category:	Position information
Description:	EXIF GPS localization data are available

IPTC Application2 City available	
Category:	Position information
Description:	Identifies city of object data origin according to guidelines established by the provider.
Additional data:	IPTC Application2 City: *18 km NE of Cathedral City*

IPTC Application2 ProvinceState available	
Category:	Position information
Description:	Identifies Province/State of origin according to guidelines established by the provider.
Additional data:	IPTC Application2 ProvinceState: *California*

IPTC Application2 CountryName available	
Category:	Position information
Description:	Country name localization data is available
Additional data:	IPTC Application2 CountryName: *United States*

XMP Photoshop Country available	
Category:	Position information
Description:	Country name localization data is available
Additional data:	XMP Photoshop Country: *United States*

XMP Photoshop State available	
Category:	Position information
Description:	State name localization data is available
Additional data:	XMP Photoshop State: *California*

XMP Photoshop City available	
Category:	Position information
Description:	City name localization data is available
Additional data:	XMP Photoshop City: *18 km NE of Cathedral City*

Exif GPSInfo available	
Category:	Position information
Description:	EXIF GPSInfo data are available.

Fig B.12 – Ghiro Signatures – Part II

APPENDIX C – IMAGO FORENSICS REPORT

Figure C.1 presents the CSV file created by Imago Forensics opened using Wordpad.


```
filename;MIME;Size_Bytes;Last_Modification_Time_UTC;Last_Access_T
ime_UTC;Creation_Time_UTC;Parsed_GPS_Latitude;Parsed_GPS_Langitud
e;ContinuousDriveMode;FocalPlaneYResolution;ExifOffset;Components
Configuration;CustomRendered;ExposureMode;Tag 0x0027;Tag
0x0024;Tag 0x0025;Tag 0x0022;Tag
0x0023;MeteringMode;EasyShootingMode;InteroperabilityVersion;Foca
lUnitsPerMM;DateTimeOriginal;SequenceNumber;AFAreaMode;ThumbnailI
mageValidArea;ExposureBiasValue;FocusMode;DateStampMode;FirmwareV
ersion;ExifImageWidth;Unknown;FocalLength;XResolution;Sharpness;Y
Resolution;FirmwareRevision;FocalPlaneResolutionUnit;Interoperabi
lityIndex;ShutterSpeedValue;LensType;Quality;ResolutionUnit;White
Balance;ExposureTime;ImageType;YCbCrPositioning;ISO;NumAFPoints;S
aturation;JPEGInterchangeFormatLength;ModelID;RecordMode;DigitalZ
oomRatio;ColorSpace;ManualFlashOutput;RelatedImageLength;FlashMod
e;FlashInfo;FlashPixVersion;Flash;AESetting;ImageUniqueID;JPEGInt
erchangeFormat;Contrast;FileSource;ExifImageLength;FocalType;Macr
omode;CompressedBitsPerPixel;OwnerName;FocusType;SubjectDistance;
SpotMeteringMode;Compression;SelfTimer;FlashDetails;SceneCaptureT
ype;CanonImageWidth;Make;ISOSpeedRatings;MaxApertureValue;Sensing
Method;FocalPlaneXResolution;Tag
0x0000;AFPointUsed;DateTime;ImageStabilization;ExifVersion;ValidA
FPoints;Model;DigitalZoom;ApertureValue;InteroperabilityOffset;Re
latedImageWidth;FNumber;Tag 0x001F;Tag 0x001D;Tag 0x0019;Tag
0x0018;ImageNumber;ImageSize;FlashBias;AFPointSelected;UserCommen
t;SlowShutter;DateTimeDigitized;LongFocalLengthOfLensInFocalUnits
;Orientation;FlashActivity;ShortFocalLengthOfLensInFocalUnits
Canon_Ixus70_1_3725.JPG;image/jpeg;2251039;2020-08-05
11:03:21;2020-08-05 11:05:41;2020-08-05 11:04:05;None;None;Single
Or Timer;2304000/169;196;YCbCr;Normal;Auto Exposure;[6, 0, 0,
730, 23824, 56345];[156, 35, 0, 0, 0, 1, 1, 16, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, ... ];[14, 35, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0];[416, 0, 0, 16, 8, 1, 1, 640, 480, 0, 0, 0, 0, 0, 8, 384, 0,
0, 0, 0, ... ];[8, 0];Evaluative;Full Auto;[48, 49, 48,
48];1000;2009:01:07 11:07:01;0;Spot AF;[0, 0, 0,
0];0;Single;Off;Firmware Version
1.01;3072;4;29/5;180;Normal;180;16843264;2;R98;189/32;65535;Super
fine;Pixels/Inch;Auto;1/60;IMG:DIGITAL IXUS 70
JPEG;Centered;Auto;9;Normal;3570;PowerShot SD1000 / Digital IXUS
70 / IXY Digital 10;JPEG;1;sRGB;n/a;2304;Auto + Red-Eye
Reduction;[0, 0, 0, 0];0100;Flash did not fire, auto mode;Normal
AE;[218, 2, 16, 93, 25, 220, 135, 74, 164, 65, 212, 154, 144, 91,
7, 171];5108;Normal;Digital
Camera;2304;4;Normal;5;;Auto;6553;Center;JPEG (old-
style);0;Manual;Standard;2304;Canon;80;95/32;One-chip color
area;40960/3;[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0];0;2009:01:07 11:07:01;4;0220;3072;Canon DIGITAL IXUS
70;None;95/32;3334;3072;14/5;[138, 1, 0, 4, 8, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, ... ];[32, 1, 0, 2, 2, 2, 2, 0, 0, 0,
0, 0, 0, 0, 0, 0];1;[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, ... ];1000031;Large;0 EV;4;[0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0];Off;2009:01:07 11:07:01;17400;Horizontal
(normal);4;5800
```


Fig C.1 – Imago Forensics Report

APPENDIX D – EXIF READER REPORT

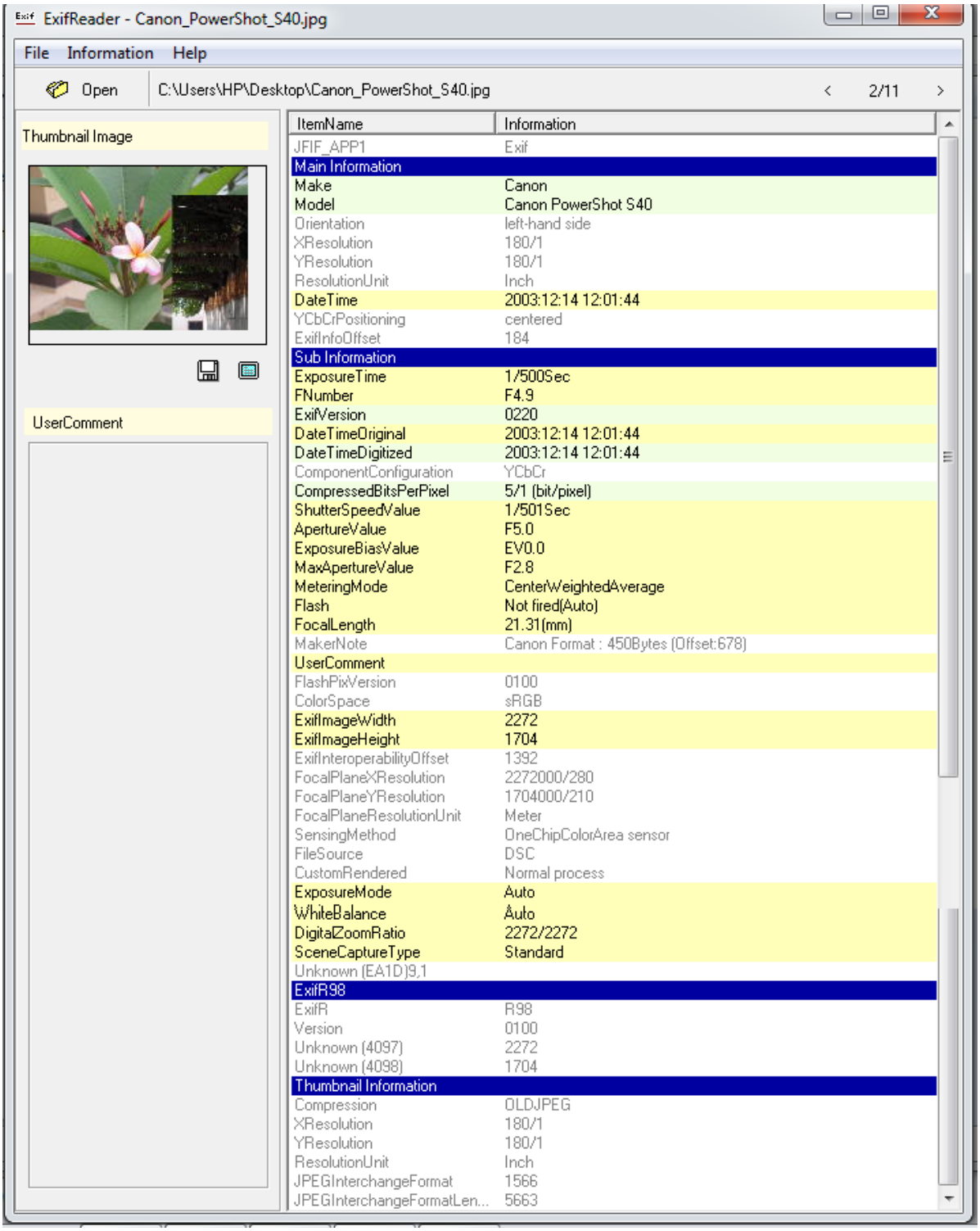


Fig D.1 – Exif Reader Forensics Report