Metadata (EXIF)

Metadata is additional information about the picture contained in a file attached to every picture in the form of an Exchangeable Image File (EXIF). This can be read using a photo editing program or be using dedicated exif viewing software (freely available).

The EXIF file contains specific information about the picture such as the camera model, time of taking, camera settings and sometimes also the location (geo-tagging).

This information is important allows an investigator to discover a great deal about the picture such as if flash was used or if the camera selected a slower than expected shutter speed.

It can also be used to confirm the account of someone submitting a picture for examination and can indicate if the image has been edited after it has been taken.

Unfortunately, it is possible to use software to rewrite or erase all or part of the metadata. It is also possible to edit or remove some parts of the metadata such as a geo-tag which may be desirable.

Keep the original picture

After making your working copy keep the original file in a safe place. This may be on an external device or in the cloud. No changes should be made to this original picture but you may wish to use it in order to make further copies

Publicity ?

If you believe that a picture you have taken may show something significant you should seek a further opinion from a trusted organisation such as the SPR before you approach the news or social media.

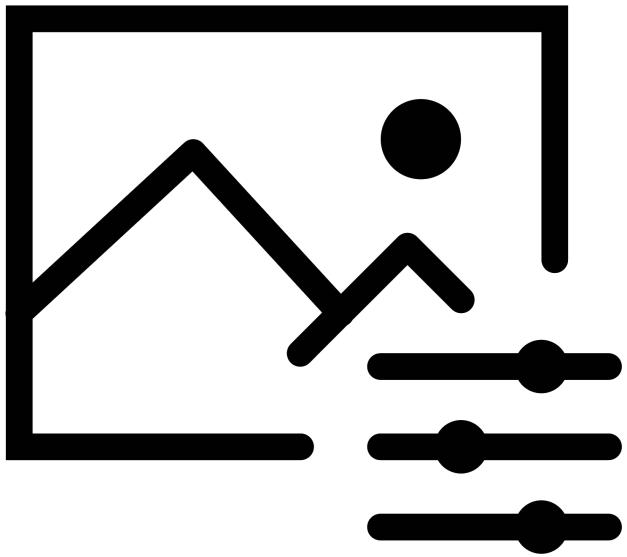
Viewing Tests

It is often helpful to ask several people to look at the picture and report what, if anything they can see. Take care to to avoid using leading statements when doing this e.g. “can you see a face on the left?”.

Try to avoid group viewing tests or using social media as these carry a greater risk of participants being influenced by the opinions of others.

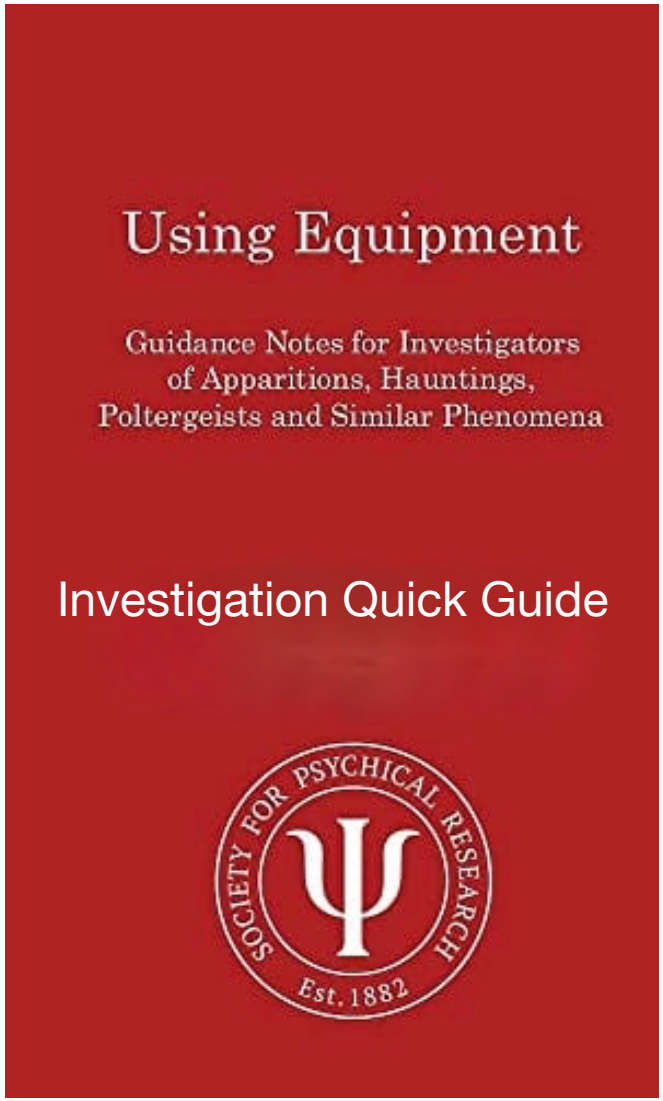
Participants should be asked to describe what they see, they should not be prompted or guided about where to look and what to look for. If a participant fails to see anything, this failure should be recorded.

Participants who are not associated with the location or who have little knowledge of the case are preferred.



Analysing Pictures

Examining a picture can provide a lot of additional information. Pictures may be taken during a site visit or supplied by witnesses and other third parties.



The first steps

Always begin by making a copy of the picture. This copy will be used for all future actions. The original should be retained and carefully filed.

Avoid just loading the picture into your photo editing software and making random changes to the exposure, contrast, brightness or some other parameter, hoping for something to reveal itself.

Using a technique similar to that employed by forensic image analysis; create a folder for each picture to be analysed and save an unaltered copy here as your reference. Then create a new text file and give it the same title as the picture and save this in the same folder.

Systematically work through any changes or alterations you wish to make to the picture changing just one parameter at a time. Following every change, save a copy of the changed picture into the folder, giving it a unique and meaningful file name e.g. *"locationpicture1.jpg".* Use the text file to record information about every change e.g. *"location picture1 - exposure increased by 50%"*. Repeat this step for every new change you make.

This technique will allow you to demonstrate every step you have used to draw any conclusion about the nature of the picture. It also lets you step back through your analysis allowing you and others to check your conclusions.

Third party photographs

Investigators are often sent pictures that have been taken by witnesses or other third parties. The first step is to ask the sender why they took the picture and what they believe it purports to show. This can then be compared with the metadata in order to confirm some of the account information.

Then check the file name, this should comply with one of the standard file indexing systems used by the camera manufacturers. If it does not, you should immediately suspect that the picture has been edited in some way. Also look out for pictures with descriptive file names e.g. *"ghostpic.jpg"* as this is also an indication that the picture has been edited in some way.

Next, check the metadata file and confirm that the information it contains agrees with the information supplied by the person supplying the picture. The metadata file can usually be quickly accessed from within your chosen photo editing or viewing software by selecting the 'file info' option.

Sometimes you may find that only the date or time is wrong, often caused by the person failing to set these correctly beforehand. If any other parts of the metadata appear to be incorrect or possibly changed, you may reasonably suspect that the picture has been edited or altered in some way.

If you suspect that an image has been tampered with, proceed with caution. It is worthwhile checking with the sender that the information they have supplied is correct.

Making random changes rarely provides helpful data.

Making a series of changes to a picture, changing the exposure, contrast and colour using photo editing software will rarely prove to be helpful.

Keep an open mind when examining a picture

Don't let your beliefs or your expectations cloud your judgement. Consider every possibility, genuinely anomalous pictures are incredibly rare.

Further Information

For those seeking more comprehensive information about analysing pictures; the Society for Psychical Research has published a useful book.

Using Equipment Guidance Notes for Investigators of Apparitions, Hauntings, Poltergeists and Similar Phenomena.

The book is available in soft back format directly from the SPR website: www.spr.ac.uk (books for sale) and also from Amazon in either printed or kindle formats.

Email: secretary@spr.ac.uk

1 Vernon Mews, London, W14 0RL