TORTURE Volume 20, Number 1, 2010

Photographic documentation, a practical guide for non professional forensic photography

Önder Özkalipci, MD* & Muriel Volpellier, MD

Abstract

Forensic photography is essential for documentation of evidence of torture. Consent of the alleged victim should be sought in all cases. The article gives information about when and how to take pictures of what as well as image authentication, audit trail, storage, faulty pictures and the kind of camera to use.

Key words: Istanbul Protocol, forensic photography, torture, camera technology, photo identification

Paragraph 106 of the Istanbul protocol¹ stipulates that during the procedures of a torture investigation "colour photographs should be taken of the injuries of persons alleging that they have been tortured, of the premises where torture has allegedly occurred (interior and exterior) and of any physical evidence found there".

The photographic documentation of evidence for presentation of an argument in a court of law is forensic photography. Forensic photography is essential for documentation of physical evidence and it is essential that the pictures are taken and handled in a correct way.

Consent

Specific consent of the alleged victim should be obtained before taking any photographs. The consent must be valid. A valid consent is a consent that is given freely, without fear, duress, or fraud and that is appropriately informed.

The alleged victim needs to know and understand what sort of pictures will be taken and for what purposes. Even if the photographs are not taken on the occasion of a medico-legal examination, for instance if the pictures are taken in a rehabilitation centre for torture survivors, the patient needs to know that the pictures may be revealed in subsequent court proceedings. Equally, in all cases, the patient needs to know that the pictures may be used for teaching purposes or for publication in medical journals.

The issue of anonymity should be discussed and if possible to guarantee it or not.

The patient needs to be competent to receive information about photographic documentation and able to weigh that information and come to a rational decision.

Photographic documentation: when?

The timing of photographic documentation depends on how soon after the alleged torture you see the victim.

If the alleged torture happened recently, photographs should be taken as soon as

^{*)} International Rehabilitation Council for Torture Victims Denmark irct@irct.org

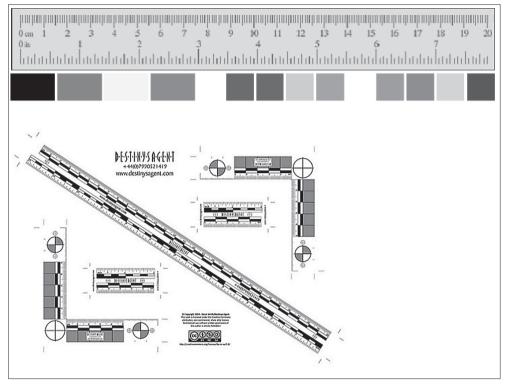


Figure 1. Example of forensic rulers.

possible. It is also advised to take pictures during the follow up examinations of recent torture allegations in order to show the changes of the physical findings. Keep in mind that bruises can take hours to appear after trauma.²

If the alleged torture didn't happen recently, there is no time constraint.

Photographic documentation: what?

It is advised to take close-up photographs
of all lesions with serial pictures from
different angles of important lesions.
 A picture of the lesion at a 90 degree angle should always be taken (inexpensive
professional marking rulers (Figure 1.)
have one or more circles printed which

- help to ensure that a picture is taken at a 90 degree angle).
- In addition to close up photos, photographs of the injury from normal distance permiting the viewer to see clearly which part of the body has been injured should be taken. This is to avoid distorting the size or shape of the injury, and to prevent misinterpretation.³
- Broader pictures of the person should be taken, including full length shots as well as head and shoulders shots.
- Photograph all clothing involved if applicable.
- Photograph the premises where torture allegedly happened (inside and outside views) if applicable.

- Photograph the instruments used in the alleged torture if applicable.
- It is important to stress that besides documenting torture-related areas, areas of skin diseases should also be photographed since the occurrence of new skin disease or the aggravation of existing skin condition can be related to physical or psychological trauma following torture.⁴

It is advised to take pictures of the body parts of the alleged victim even when there is no visible sign of trauma in recent torture allegations.

Photographic documentation: how?

- Light: If possible pictures should be taken in daylight or with background lighting.
 - The presence of bright lights or reflective surfaces can produce a wash out of the detail (overexposure) and the injury will become less visible on the photograph. Remember: lighting can be critical to the appearance of some injuries.⁵
- Background: taking pictures in a crowded and colourful background must be avoided in order to prevent different colour reflection.
- Close up pictures: close up pictures of lesions are taken 10 to 12 inches away or 25 to 30 cm away.
- Scale of reference (also known as measuring tape or evidence ruler, see Fig. 1.): first take one picture of the injury in its original condition, then take a second picture with an evidence ruler. When a scale of reference is used, the camera's back should be parallel to the scale and the scale should be parallel to the lesion in order to get a more accurate representation of the lesion. This is *especially significant* for photography of lesions like bite marks or lesions which present specific features of

- the object used during torture. "L" shaped rulers are crucial in bite mark analysis. While using measuring tapes, make sure not to obscure any information present.
- Date: It is essential to date the picture.
 All current cameras have a date feature.
 It is advised to use a date scale during photography. In some cases, a physician should consider taking a picture of the patient with a recent newspaper as a proof of date.
- Identification of the person photographed.

The identification of the person photographed should appear on every picture either as a full name or a case number. Non identifiable pictures are worthless in court and can only be used for teaching purposes.

Image authentication

The digital processing of images, the potential for image modification and the problem of defining what is an original, make it difficult to establish with ease that an image is authentic. This is a critical step if an image is to be used as evidence. There are two elements to establish authenticity: to have an "audit trail" which records everything that happens to the image from capture to its presentation in court; and/or in the case of digital images, to have a technological solution which brands or "watermarks" the image at the time of capture and can subsequently show it is authentic.⁶

Audit trail: chain of custody or chain of evidence

It is generally believed that digital images are easily manipulated and film images are much less susceptible to manipulation. The facts of the matter are that the first statement is true and the second, is, to a large degree, false⁷. This is why proper procedures are to be followed in all cases.

The Chain of evidence (COE) procedure is a means by which the handling and "journey" of any evidence is clearly documented, and by which its integrity, that is, its origin, history, handling, storage and processing, is assured. There must be an unbroken chain in the continuity of its progress. There must be a "paper trail" which must be able to account for this and which may be subject to and be capable of withstanding scrutiny.

When the sample is stored, it must be possible to demonstrate that it is securely stored, with limited access and with a means by which any one that has access to that sample, may be identified.

- For conventional photography: information on production serial number of the roll of the film and original item number of each pose in the roll should be written in relation with each picture captured, as well as the date of the picture, the name of the person who took the picture and the persons who were present during photography. This information should be secured together with the negatives and prints of the photograph.
- For digital photography: information on the digital camera, authentic number of each picture file in relation with each pose, name of authentic pictures file on authentic writeable CD or on computer, as well as the date of the picture, size of the picture in bytes (Figure 2.) and the name of the person who took the picture, the name of the persons who were present during photography and the name of the person who downloaded the authentic pictures from the camera on authentic writeable CD or on computer should be written. The images should be transferred as soon as possible after capture to a WORM (Write Once Read Many) medium such as a CD-R.

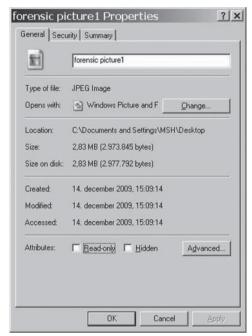


Figure 2. The size of this picture should be recorded as 2.973.845 bytes.

Watermarks provide an extra level of security to an image in addition to an audit trail if they are added at source as the image is being captured by the camera. With a conventional image the watermark (eg. an identifying code or logo) would need to be visible in the scene and may thus obscure other vital information. In a digital image it is possible to hide the watermark within the image data with a form of encryption: although the watermark can be present in all parts of the image (down to pixel scale), the image looks normal and the watermark can be viewed only with the appropriate decryption key. It would also be possible to encrypt the whole image so that it is meaningless to anyone viewing it without the appropriate equipment and decryption key.

Digital signature: Digital signatures can be used for authenticating messages and documents sent electronically and, equally, could be adapted for authenticating images. The American Bar Association⁸ describes digital signatures as using public key cryptography and a "hash function" derived from the message itself. The hash function is an algorithm created from enough of the message data to ensure that it could only be created from those data. The message and the hash function are then encrypted with the sender's private encryption key to make a digital signature which is unique. The receiver decodes the message with a related version of the encryption key previously given to the intended recipient by the sender (or held by a trusted third party). The message is verified by computing the hash function again and comparing it with the original.9

Storage

- Conventional photography: Negatives of the films should never be exposed to heat or light which may decay the films. It should always be remembered that because of long lasting trials sometimes these pictures may be needed after several years. Negatives and photographs should be kept in a locked cupboard with limited access. Each time someone has access to the photographs, the name of the person, date, time and purpose of the access should be recorded.
- Digital photography: The images should be transferred as soon as possible after capture to a WORM medium such as a CD-R. Do at least two copies of the CD-R. Keep the CD's in a locked cupboard with limited access. Each time someone has access to the photographs, the name of the person, date, time and purpose of the access should

be recorded. If the digital images are kept in a computer, the computer must be secure, with limited user access and advanced password protection. It is also possible to use a special hard disk for the only purpose of storing pictures. Nothing must be extracted from the original image and nothing must be inserted onto the original image.

If the photos are not processed immediately, place the flashcard in an envelope with the identification details of the case and signature of the photograph. Seal the envelope. The envelope should then be logged in a book and placed in a locked cupboard with limited access.

If the photos are processed immediately, transfer the content of the flash card on a computer, burn a WORM CD or store the images on a password protected memory key. It is best practice to create two case folders, one on the hard drive of the computer, one on a zip cartridge. Then two folders should be created and inserted into each case folder - one labeled "raw images" and the other labeled "processed images". At this point, the right click copy tool should be used to duplicate the contents of the flash card into both of the "raw images folders." These folders should never be opened until after the images have been permanently duplicated later on. The content of the flash card should be duplicated a second time and placed in the "processed image folder" in the computer hard drive and the zip card. Check if the images in the "processed image folder" are visible and if yes, remove the Zip cartridge from the computer and secure it.

Erase the flash card so that you can reuse it.

When two password protected zip drives are filled, the content should be transferred

to a WORM CD. The cases that have been recorded on a particular CD should be listed along with the CD serial number.¹⁰

Enter in the logbook which CD holds the content of the flashcard.

Open a few images on the CD to make sure that the file is readable. Once it is ascertained that the images on the CD are readable, the zip drive should be reformatted and made available for reuse.

Faulty pictures

It is proper to discard images that are clearly of no value because of photographic technique or errors.¹¹ However, it is important to document that some images have been discarded and the reasons why.

Photography in rehabilitation centres and prison

Establishing a medical photography unit with professionals and developing standard operating procedures for photography is essential for the medical units of prisons and for the rehabilitation centres dealing with the survivors of torture. Support from forensic experts may be needed while establishing these standard operating procedures for the photography unit.

The professionals using this unit should have training on forensic photography. Whether having adequate staff/unit for photography or not, medical doctors in contact with prisoners or torture victims should have knowledge on the basics of photography.

If there is no existing photography unit, the prison doctor or the medical doctor of the rehabilitation centre should make an effort to create a space favourable to photography in the examination room or in a facility close to examination room.

What kind of camera should be chosen for photography documentation?

Any digital camera with four mega pixel capacity should be quite enough for documentation purposes. Metadata for a digital photograph typically includes the date and time at which it was created and details of the camera settings (such as focal length, aperture, exposure). Many digital cameras record metadata in their digital images, in formats like exchangeable image file format (EXIF) or IPEG. Some cameras can automatically include extended metadata such as the location the picture was taken (e.g., from a GPS). Most image editing software includes at least some metadata in the digital image, and can include content about the image's provenance and licensing.1

There are several different technologies and factors, for example with wide angle or normal lenses: image sensor size, focal length etc. You may get good pictures with different combinations of these factors.

Cameras with wide angle lenses are cheaper then normal lenses. With normal lenses camera can cover a larger area and a wider distance range with clear image, you can get closer to the object or you can take good quality picture from a long distance. With wide angles you can cover a smaller area with clear image.

There are also other factors like flash light, speed, auto focus, image capacity, white balance, image processor, exposure control etc. Each factor increases the quality of working conditions.

In short, the camera should have a minimum of four mega pixel or more of picture size.

You can take a trial picture of a printed text with eight point font size from 20 cm distance. If the text can be readable on the picture of the text then it is a good camera for documentation purposes.

If there are enough funds for photographic equipment, cameras with normal lenses are always recommended.

Can we take pictures with cell phones?

It should not be forgotten that the image quality of the cell phones pictures is not really sufficient for judicial purposes. The image resolutions or sizes are not good enough to print big pictures. A good digital picture should be more than four mega pixels. Also, as the mobile phone lens has a wide angle, the images can be distorted on the sides.

What to do if the applicant refuses to give a picture?

If the examination is performed through the request of a prosecutor as part of a crime investigation because of "torture allegation" then it is part of a proper documentation to take photographs. The physician should explain this and the importance of photography to the complainant. If the complainant refuses to allow the physician to take pictures, then the physician should get a written and signed refusal from the complainant.

If the examination is performed independently from a judicial process then the physician should clearly explain the importance of photography and should take note of the person's refusal.

References

- Istanbul Protocol Manual on the effective investigation and documentation of torture and other cruel, inhuman, or degrading treatment or punishment professional training series number 8/Rev.1. New York and Geneva: United Nations, 2004:135.
- Dalton M. Forensic gynaecology. RCOG Press, 2004.
- Rediscker DR. The practical methodology of forensic photography. 2nd ed. CRC Press, 2001:189.
- Danielsen L, Rasmussen V. Dermatological findings after alleged torture. Torture 2006;16:108-27.
- Rediscker DR. The practical methodology of forensic photography. 2nd ed. CRC Press, 2001:183.
- www.publications.parliament.uk/pa/ld199798/ld-select/ldsctech/064v/st0504.htm
- Blitzer HL, Jacobia J. Forensic digital imaging and photography. Academic Press, 2007:201.
- 8. Digital Signature Guidelines. www.abanet.org/ scitech/ec/isc
- www.publications.parliament.uk/pa/ld199798/ld-select/ldsctech/064v/st0504.htm.
- Blitzer HL, Jacobia J. Forensic digital imaging and photography. Academic Press, 2007:210-9.
- 11. Blitzer HL, Jacobia J. Forensic digital imaging and photography. Academic Press, 2007:206.

TORTURE Volume 20, Number 1, 2010

CONSENT FORM FOR PHOTOGRAPHS

I consent to the taking of the photographs indicated below.

I understand that these will be used:

- 1.*As part of the medical record of my examination, and that they may form part of a report based on that examination and may be revealed in subsequent court proceedings.
- 2.*For lectures and teaching purposes.
- 3.*For publication in medical journals, textbooks or similar publications. In which case I understand that:
- (a) The material will be published without my name attached and every attempt will be made to ensure my anonymity. I understand however, that complete anonymity cannot be guaranteed. It is possible that somebody somewhere-perhaps for example somebody who looked after me if I was in hospital or a relative may identify me;
- (b) the material may be published in medical journals worldwide, which are distributed mainly to doctors but are seen by many non-doctors, including journalists;
- (c) the material may also be placed on a worldwide web site;
- (d) medical book publishers may also use the material;
- (e) the material will not be used for advertising or packaging.

*)	Ľ	elete)	as	appro	priate
----	---	--------	----	-------	--------

Subject of article of photograph	
Signed	Date

It is good practice to advise the patient that consent to use photographic material for research, peer review or teaching is for life and not limited by time, as seeking renewed consent when necessary is almost impossible for an FME (Forensic Medical Examiner). Photographic images taken during the course of an investigation should never be used for any purpose other than evidential while the case remains *sub judice*.

Example of consent form for photographs (from Good Practice Guidelines for Forensic Medical Examiners. Metropolitan Police April 2007).