Digital Forensic Evidence

The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime, and wildlife crimes are no exception. ***Wherever possible, specialist advice from a force's Digital Forensic Unit (DFU) should be sought in advance.***

Digital evidence can be found in a number of different locations:

1. **Locally on an end-user device** – typically a user's computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;
2. **On a remote resource that is public** – for example websites used for social networking, discussion forums, and newsgroups;
3. **On a remote resource that is private** – an internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's webmail account, and increasingly common, a user's remote file storage;
4. **In transit** – for example mobile phone text messages, or voice calls, emails, or internet chat.

Recovery of digital evidence from a crime scene / suspect

There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined.

Always consider:

1. Is ownership/attribution an issue? If so:
   - Ensure DNA precautions are taken before recovering
   - Recover in such a way that any friction ridge detail (fingerprints) are preserved and not damaged by contact with packaging materials (see below)
   - Request attendance of a CSI/SOCO
2. Is the device switched on and **unlocked?**
   - Put the device into Airplane mode and ***submit for urgent examination.***
3. Is the device switched on and **locked?**
   - If it has been unlocked at least once since it was last switched on (After First Unlock AFU state) more data can be extracted but this ***has to be examined within 3 days of seizure.***
   - If it has not been unlocked once since it was switched on (Before first unlock BFU state) the file system is encrypted and there is less urgency, you can switch the device off and place into a faraday bag to avoid remote wiping.

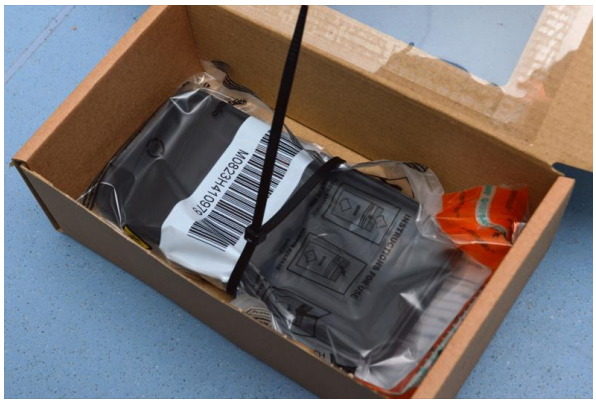
Recovery of small digital items (e.g. phones, cameras, data sticks)

The preferred method is to always have a CSI/SOCO present to advise or seize items in accordance with best practice in order to retrieve and/or preserve evidence. If this is not possible, always ensure that appropriate PPE is worn (clean nitrile gloves and a face mask) and clean packaging is used. Where an investigation is likely to involve the examination of user-created digital images consideration should be given to seizing all devices capable of taking digital photographs. Seizure of devices capable of taking digital photos could be useful not only for the data they store, but also to link these devices to previously identified photographs by the examination of digital metadata.

If given sufficient information about the investigation, DFUs will be able to advise on which items are most likely to provide the evidence sought.

For items where fingerprint examination may be required, ensure that they are secured in rigid packaging using cable ties or similar to prevent movement which may cause damage to any marks present. This may consist of a clean, unused box which can, in turn be placed into an evidence bag and sealed at the scene as below.

For items requiring DNA examination, ensure that boxes and bags are unused, preferably, sterile before placing the item within. Where boxes are utilised, in order to avoid contamination, it is advisable to place the item into a sterile tamper evident bag first, then secure into the box using cable ties or similar as below. The box should then be placed into a tamper evident bag, sealed and exhibited at scene.



If chargers are available, consideration should be given to their recovery as well, package separately to the phone and ensure that they are secured within a box so that packaging is not compromised by sharp edges. Bear in mind that it is unlikely that fingerprinting can be carried out after download as handling of the device is likely to damage marks and introduce contamination issues, therefore, any examination for FRD should be conducted prior to submission of the device to any DFU.

Desktop and laptop computers/games consoles

The scene should be fully documented by written notes and/or a photographic record.
If a device is powered on, it needs to be handled carefully to preserve any volatile data and to avoid unwanted changes to the stored data.

Consider removing the device from any network by engaging airplane mode if possible, as devices can be remotely accessed, causing alteration to the data - but balance this against the possibility of losing data of evidential value, such as the list of currently open connections. If unsure, seek expert advice.

Seizure steps:
1. Photograph or video the scene and all the components including the cables present in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date;

If switched off:
2. Do not, in any circumstance, switch the computer on;
3. Make sure that the computer is switched off, by moving the mouse – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on;
4. Be aware that some laptop computers may power on by opening the lid. Remove the battery from the laptop. Seize any power supply cables for future use.

If switched on:

5. Record what is on the screen by photographing it and by making a written note of the content of the screen

Packaging should take into account any DNA or fingerprint requirements as above and items secured and sealed at scene.

Care must be taken during transport that items are shielded from magnetic fields and physical shocks.

When attending scenes where recovery of data from routers may be required, any officer/staff held devices should be set to either airplane mode or switched off to ensure they do not overwrite data in trying to connect themselves to the wifi network at scene.