

Taking possession of equipment for computer investigation

Before taking possession (or "seizing") computers, storage tapes, floppy Disks, CDs DVDs, mobile phones, cameras, or any such equipment that is to be submitted for forensic examination, it is important that you consult with a member of the Computer Science Labs forensic department. He or she will advise you as to how this work **must** be carried out. **Failing to comply with proper procedures means valuable evidence cannot be used and time, effort and money will be wasted and an unsatisfactory outcome may result.**

The following general guidelines are however useful to note:

- Ensure that you gain control of the premises and the occupants.
- Do not allow anyone to touch the computers or equipment.
- Do not in any circumstances power the computer or equipment on.
- Make sure that the computer or equipment is switched off.
- Laptops may power on by opening the lid.
- Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Note that a computer may be in stand-by mode and may be accessed remotely, allowing the alteration or deletion of files.
- Photograph the scene and all of the components in situ, ensure that the picture depicts the layout of the equipment, floppy disks and other storage media and is date and time stamped.
- Ensure all items are secured that will allow the reconstruction at a later date.
- Search the area for diaries, notebooks or pieces of paper for passwords.
- Ask the user if there are any passwords and if these are given record them accurately
- If a computer is connected to or is part of a network consult with a member of the Computer Science Labs forensic department.
- Do not take advice from the owner/user of the computer.
- Photograph the information displayed on the screen.
- For all desktop computers remove the power supply by pulling out the end attached to the computer and not that attached to the socket.

In Criminal matters the Computer Science Labs Forensic department will not accept any items if they are not correctly bagged & tagged and supplied with all supporting documentation.

Typical List of Items for seizure:

- Main unit : usually the box to which the monitor and keyboard are attached
- Monitor, keyboard and mouse
- Connectivity Leads
- Power supply units and leads
- Hard disks not fitted inside or connected to the computer
- Dongles: i.e. small connectors plugged into the back of the machine
- Modem or signalling equipment
- External hard drives and other external devices
- Wireless network cards
- Digital cameras and web cams
- Floppy disks
- Back up tapes
- Jaz/zip drives

- CD
- DVD
- PCMCIA cards
- Memory sticks and memory cards
- Manuals of computer software

Transportation

When transported, equipment should be handled with care, securely packed and placed in an upright position to prevent physical shocks. Equipment must be kept away from magnetic sources (heated car seats and windows, loudspeakers and hand held radios). Loose hard disks or floppy disks should be placed in anti-static bags.

Comment

The essential concern when acquiring equipment is not to change the evidence on the hard disk and to produce an image that represents its exact state when it was seized. Only a competent person who understands the implications of his or her actions and is able to fully explain them in a court of law should be involved. If in any doubt contact the Computer Science Labs forensic department.

