

Datasheet: Forensics Guidelines and Best Practice



Listed below are some key guidelines of what to do when seizing a computer for forensic examination, these are as per the ACPO (Association of Chief Police Officers) UK Good Practice Guide for Computer Based Electronic Evidence.

These guidelines are principally aimed at the individual within your organisation who would be responsible for the isolation and subsequent investigation of a PC, server, laptop or removable media device. The lead investigator is often from HR, Audit, IT, the Legal department or Finance.

Electronic data should be treated in a similar manner to that of traditional forensic evidence retrieval and these guidelines are aimed to meet the same high standards. This will ensure case integrity and compliance with current UK legislation.

If you suspect that your organisations computer systems may contain information pertinent to an enquiry then you should introduce the procedures detailed in Appendix 1 and Appendix 2.

If you are on site, follow the steps detailed overleaf (Appendix 1), alternatively ask a trusted individual to carry out points 1 and 2 on your behalf.

Sapphire has also provided an evidence seizure chart, which you may find easier to follow (Appendix 2).

**DO NOT TURN ON OR ATTEMPT TO INVESTIGATE A SUSPECT COMPUTER
WITHOUT PROFESSIONAL AND EXPERT ADVICE**

Appendix 1:

1. Identify all computers and storage media that may contain evidence including:
 - The suspect's desktop or laptop computer.
 - The suspect's secretary's computer.
 - The suspect's PDA.
 - The suspect's mobile telephone.
 - The server.
 - Backup tapes.
 - CDs, Floppy disks, DVDs, USB drives, Flash memory.
 - Home computers.
 - Connected third-party computer systems.

1. Quarantine of computer media:

Upon discovery of computer equipment which appears to be switched off:

- Secure and take control of the area containing the equipment.
- Move people away from any computers and power supplies.
- Photograph or video the scene and all the components including the leads 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.
- Allow any printers to finish printing.
- Do not, in any circumstances, switch the computer on.
- Make sure that the computer is switched off – 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.
- Be aware that some laptop computers may power on by opening the lid.
- Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss.
- Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket). A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of files.
- Label the ports and cables so that the computer may be reconstructed at a later date.
- Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.
- Search the area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.
- Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.
- Make detailed notes of all actions taken in relation to the computer equipment.

Upon discovery of computer equipment which is switched on:

- Secure the area containing the equipment.
- Move people away from computer and power supply.
- Photograph or video the scene and all the components including the leads 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.

- Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.
- Record what is on the screen by photographing and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is suspected to be present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video the screen and note its content. If password protection is shown, continue as below without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances.
- Where possible, collect data that would otherwise be lost by removing the power supply e.g. running processes and information about the state of network ports at that time. Ensure that for actions performed, changes made to the system are understood and recorded. See section on Network forensics and volatile data.
- Consider advice from the owner/user of the computer but make sure this information is treated with caution.
- Allow any printers to finish printing.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices. Ensure that all items have signed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.
- Allow the equipment to cool down before removal.
- Search area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.
- Ensure that detailed notes of all actions are taken in relation to the computer equipment.

If the power is removed from a running system, any evidence stored in encrypted volumes will be lost, unless the relevant key is obtained. Also, note that potentially valuable live data could be lost, leading to damage claims, e.g. corporate data.

2. Call Sapphire. Sapphire will create evidentially sound images of the relevant computers and storage media.

Appendix 2:

