

If you think you may have grounds for a Computer Forensic Investigation, what should you do now?

Step 1 – Preserve Evidence

Retain all electronic data such as emails, documents, files, digital photographs etc. Do not delete items, empty recycle bins, reload software or any similar action that might lead to valuable data being compromised or made harder to recover. If in doubt, keep everything, preferably with backup copies to guard against unforeseen circumstances. Where important data resides on servers or computer equipment that other people use or have access to it may be wise to engage the services of Computer Science Labs to take a forensic duplicate or 'clone' of data from such devices as the best way to preserve key data. This can be done at a convenient time and in a manner that will avoid undue disruption and maintain discretion.

Step 2 – Record information

Make a note of everything that may be relevant to any potential investigation: names, dates, times, filenames, email addresses etc. as well as any and all communications with the parties involved.

Step 3 – Consider what the ultimate objective of any potential investigation would be, and what other courses of action may result from it.

Following these simple steps will allow Computer Science Labs to give you the best advice on any potential investigation and offer the greatest chances for a successful outcome.

