*Proper evidence preservation, follow these procedures in order (Do not use the computer or search for evidence)*

1. Photograph the computer and scene
2. If the computer is off do not turn it on
3. If the computer is on photograph the screen
4. Collect live data - start with RAM image (Live Response locally or remotely via F-Response) and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.
5. If hard disk encryption detected (using a tool like Zero-View) such as full disk encryption i.e. PGP Disk — collect "logical image" of hard disk using dd.exe, Helix - locally or remotely via F-Response
6. Unplug the power cord from the back of the tower - If the computer is a laptop and does not shut down when the cord is removed then remove the battery
7. Diagram and label all cords
8. Document all device model numbers and serial numbers
9. Disconnect all cords and devices
10. Check for HPA then image hard drives using a write blocker, Helix or a hardware imager, dd.exe dd image
11. Package all components (using anti-static evidence bags- faraday gage bag, case cage)
12. Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)
13. Keep all media away from magnets, radio transmitters and other potentially damaging elements  
    Collect instruction manuals, documentation and notes
14. Document all steps used in the seizure

**Order of volatility of digital evidence**

1. CPU, cache and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system / swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media