



## Recommended Guidelines for Computer Forensic Analysis Evidence Submission



The following are suggestions for the proper submission of computer evidence for forensic examination. They are meant as only a guideline to help in the expeditious processing of evidence. They represent best practices and do not bestow any rights and/or privileges on any person.

- **Do not turn on the computer for any reason.**
- **Contact the agency that will do analysis for you as soon as is practical. Early involvement from them means a more efficient and timely seizure, submission and subsequent exam and investigation.**
- **Place evidence tape over the power supply and disk drives.**
- **Supply a search warrant or consent to search authorizing the analysis of the computer data.**
- **Supply a police report, affidavit or case summary for the examiner.**
- **Supply a list of words to be searched, if possible, on a diskette in a text (.txt) format with one word per line. When making a word search list try to use words unique to your investigation. Do not use words like money, drugs, sex, mail, etc.**
- **Know what you are interested in and communicate it to the lab. Computers contain vast amounts of data. It is unreasonable to expect timely results from a request in which the examiner doesn't know enough about the investigation to know what might impact it.**
- **Make sure what you are asking for is covered by your search warrant and/or consent. For instance, if your search warrant covers drug records, don't ask for an examination to find child porn.**
- **If there is more than one user of the computer please indicate who they are and, if possible, their computer identities and/or passwords.**
- **Indicate if the computer was part of a network. Supply as much of the following information as possible upon submission.**
  1. **Type and number of computers and operating systems.**
  2. **Type of network software and location of servers.**
  3. **Activities being processed on the network and type of connection to outside sources.**
- **Indicate whether encryption and/or password protection was being used.**
- **Indicate the computer skill level of the person from whom the computer was taken.**
- **For most submissions, monitors and printers do not need to be submitted. Generally, the computer and loose external media and drives are sufficient.**