Computer evidence processing guidlines essay

The best way to preserve digital forensic evidence is to follow the four guidelines created. The four guidelines pertain to evidence collection, storage, processing, retrieval and documentation.

Four General Evidence Processing Guidelines Digital forensic evidence is extremely fragile and should be handled with care in order to avoid alteration which is why guidelines and procedures are created. There are four guidelines that should be followed in order to keep evidence in its most original state. Guideline One. Digital evidence is not readable; however a printout is can be submitted as evidence under the “ best evidence rule”. The best evidence rule applies when a person wants to submit a copy of a document because the original document is unavailable (Nolo Dictionary, 2011).

CollectionAny and all investigating officers should keep this in mind as well as have a warrant baring the proper wording and language that adheres to search and seizure of a personal computer in order to avoid violating any privacy rights. First the officer should check to see if the computer is on or off. If an officer finds that the computer is not on, he or she should not turn it on the evidence must not be altered; however if the officer finds the computer on then the officer should photograph the screen even if the screen is in sleep mode.

Once the computer is photographed the power should be disconnected. In other words the modem should be drained of power by unplugging it. Next the officer should be sure to insert a police disc into the CD or DVD drive; bear in mind the disc should be blank and after inserting it the drive should be sealed. All other hardware connected to the system should be photographed in order to have a record of how the system was connected. All wires should be labeled separately and then the computer is transported from the scene in a secure vehicle and then stored in a secure area or room. A chain of custody must always be in order to know who handled the evidence and when (Ashcroft, Daniels & Hart, 2004).

Guideline Two **Storing**Once the computer is removed from the crime scene photographs of the scene must be taken also a thorough search must be conducted because the area may valuable information that may be needed during the investigation like; user ids and passwords. All other software discs, devices, manuals, notes and books should also be seized and stored in containers, sealed and marked. Any people at the site must be interviewed in order to obtain potential passwords and how to operate the software. After all the software evidence is collected it should also be transported in a secure vehicle and then brought to a secure location. Once the computer and all other software arrive at the secure location the original will be stored on backup discs that will be made. The backups that are made include all hard disks, CDs and DVDs. All evidence that is being processed should be carried out on the backups only this will reduce compromising the evidence already on the computer.

The computer must remain in its original state. Most importantly the data security and the chain of custody must be maintained at all times. If the proper steps are not taken within the chain of custody and security measures are not taken questions relating to security issues will be raised in court (Ashcroft, Daniels & Hart, 2004). Guideline Three **Processing** The data on all the computer evidence must be authenticated mathematically. There are different software that can assist in this process; however it is best to use the software that is the most current and acceptable in court. There is also a great probability the defense will make the claim that law enforcement officials have altered the evidence which is the sole purpose for authenticating the data. During the data authentication process the chain of custody must be maintained and in addition to the chain of custody the system date and time must be documented in doing this the evidence will bear the exact date and time each of the different files were created or modified.

All officers should be sure to take care of the document, so it remains unchanged because then the court cannot label the evidence as hearsay. The by-product of a machine operation which uses for its input ‘ statements’ entered into the machine” and was “ was generated solely by the electrical and mechanical operations of the computer and telephone equipment” (Civil action Group, 2006). There are legal guidelines that must be met in court like; computer hardware reliability, software reliability the manner in which the information was entered, accuracy of data, how data was stored and all precautions that were taken to ensure no evidence was lost. The software program should be presented to show how to works in processing the data and how accuracy is ensured this will result in the data being entered in court as any other record (Ashcroft, Daniels & Hart, 2004).

Guideline Four **Retrieval** The evidence that is being evaluated a list of key words should be typed into the software. The list of key words can be obtained from the case, circumstances and the suspect’s motives as well as the purpose for which the suspect was using the computer. After the list is made the software can search the discs and hard drive automatically. The Windows Swap File should also be searched because the file will normally get erased when the computer is shut down.

The Windows Swap File is located on the hard drive that temporarily stores information, this file normally gets erased when the computer closes down, but it can be recreated (Indiana University, 2010). The swap file can have critical information like the location of files. A forensic officer should investigate and assess the file slack. Basically, files slacks are memory dumps that occur when files are closed; however forensic software can reconstruct the files. The file slack is very important to investigators because it allows them to obtain key words to get important information.

“ Data storage space that exists from the end of the file to the end of the last cluster assigned to the file is known as the file slack” (file slack, 2008). The investigating officer should also be sure to examine and assess erased files and can be restored using forensic software. The erased files should be examined because this is the primary place where incriminating evidence could be lurking. All the files that have been recovered from Window Swap File, file slack and erased files he dates, time of creation or modification can be recovered and must be documented. **Document**Documenting all processing of the evidence and what was performed or done is very important in the incident the evidence becomes altered at any point. There are current forensic software tools that can be used to create a database to document details and can be presented in court; however any abnormalities within the storage, file or program they must be documented and then the software should be evaluated by running a functionality report that generates through the software then a copy of the final software used should be made.

Whenever there is computer evidence involved in a case, it is necessary to establish or document that it has been kept in its original state. If any alteration is made there will be differences in the dates of file modification leading to challenges in the court room (King, Bertram & Whiten, n. d.). If an officer or investigator fails to follow the guidelines for the procedure of collecting digital evidence the evidence is altered. If a computer is just turned on it changes the evidence within the computer files and other data stored in the hard drive can be altered which is why it is ultimately important to leave the computer in its original state.

Any evidence that becomes changed will be considered altered in court and may not be admissible which is why documenting a chain of custody is very important. “ The simple act of turning a computer on can destroy or change critical evidence and render that evidence useless” (Daniels, n. d.). In conclusion all guidelines must be followed when the seizure of the computer occurs which means the computer should not be turned on or altered in any other way.

The secure storage, secure chain of custody, search of the computer, data authentication, documentation and the process of collecting evidence should also follow guidelines which means all processing of the evidence is performed on backups of the original data taken from the computer.

Performing all evidence processing procedures on backups will not damage the original evidence and will allow it to be admissible in court.