Example of computer crime-scene investigation term paper

Law, Evidence

Electronic evidence is information and data stored or transmitted through electronic devices. A computer crime scene is therefore an area where a computer or an electronic device was used as a means of committing a crime or a media through which the crime was committed. It is clear that electronic evidence is fragile and can be easily altered hence there must be proper manner of handling a computer crime scene (Fisher, et al., 1981). The first step in a crime scene is to ensure that it is secured and clearly marked. Documentation of the scene is clearly done to ensure that everything that is in the scene can be used as evidence to solve the case (Comey & Budowle, 1991). To ensure that evidence is not destroyed or compromised it should be quickly documented collected and preserved. Collection of evidence at the crime scene always begins with evidence that is fragile and easily lost. To avoid contamination of computer devices they should be collected from the scene then packaged and safely kept (Comey & Budowle, 1991).

Another initial step that should be taken is to document all the facilities and clearly label them. Digital evidence can be lost through alteration, damage or destruction as a result of improper handling of the computer devices. Suspects can also deny some of the evidences presented in court if they are not properly labelled. Evidence can be found in the printers, telephones, monitor, computer system unit, fixed storage devices and external storage devices such as flask discs (Schiro, 1995). All of the possible evidence devices must be well documented from the scene. Documentation is different from analysing or examining the evidence. This is just the process of ensure that evidence is verifiable and traceable by all the parties (Schiro, 1995).

Computer crime scene should be secured once it has been identified. Only authorized people should access the scene using a single path to and from the scene. Such a measure ensures that evidence is not destroyed. There may be other physical evidence that can be recovered from the scene if not interfered with.

If a crime scene is not well secured possible evidence or devices with evidence can be concealed by the suspect or the sympathisers. Other evidence can also be introduced in a computer crime scene with an aim of misleading the investigations. If a crime scene of not secured, crucial evidence can also be destroyed just at the crime scene. Documentation and proper package of evidence at a computer crime scene ensures that there is traceability of evidence. Investigators will face a lot of challenges if they are not able to account for missing evidence or proving that presented evidence was actually from that particular crime scene.

References

Comey, CT, and Budowle, B 1991, Validation Studies on the Analysis of the HLA DQà Locus Using the Polymerase Chain Reaction, Journal of Forensic Sciences, Vol. 36, No. 6, Nov. pp. 1633-1648

Fisher, Barry AJ, Arne Svensson, and Otto Wendel (1981), Techniques of Crime Scene Investigation. New York: Elseveir.

Schiro, G 1995, Collection and Preservation of Evidence. What We Do - Law Enforcement Series. Compiled by Captain Merril L. Boling, Jefferson Parish Sheriff's Office.