Abstract

Chain of custody is the procedure to do a chronological documentation of evidence, and it is an important procedure in the investigation process. Both physical and digital evidence is an important part in the process of investigation and courtroom. However, handling the chain of custody for digital evidence is more difficult than the handling of physical evidence. Nevertheless, the handling of digital evidence should still have the same procedure with the handling of physical evidence. Until now handling the chain of custody for digital evidence is still an open problem with a number of challenges, including the business model of the interaction of the parties that deal with digital evidence, recording of metadata information as well as issues of access control and security for all the handling digital chain of custody. The solution offered in this research is to build a model of Digital Evidence Cabinets as a new approach in implementing the digital evidence handling and chain of custody. The model is constructed through three approaches: Digital Evidence Management Frameworks, Digital Evidence Bags with Tag Cabinets as well as access control and secure communication. The proposed framework is expected to be a solution for the availability of an environment handling of digital evidence and to improve the integrity and credibility of digital evidence.
References

- P. G. Bradford and D. A. Ray, "Using Digital Chains of Custody on Constrained Devices to Verify Evidence," in Proc IEEE Intelligence and Security Informatics, pp. 8–15,
2007.

Index Terms

Computer Science  Security

Keywords

Digital Evidence  Digital Chain Of Custody  Digital Evidence Cabinets  Digital Evidence Bags.