Abstract

This review paper assesses the existing body of knowledge associated with digital forensic investigation process models. To this end, eleven of the existing models are critically reviewed and evaluated against an assessment criteria, namely the Daubert Test, to determine which models have taken the most scientific approach. This review and assessment reveal that the authors of these models have developed their models based on their own personal experience and on an ad-hoc basis. The critical review and assessment also reveal that there does not exist a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonizes and extends the previous models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response.
References


Index Terms

Computer Science
Security

Keywords