A STUDY ON THE DIGITAL FORENSICS INFRASTRUCTURE IN SRI LANKA

M.B.K. Mendis

Faculty of Graduates Studies, University of Colombo, Sri Lanka
Corresponding author: buddhikamendis83@gmail.com

This research paper discusses the current digital forensics infrastructure in Sri Lanka and its problems. Investigations were conducted in the Criminal Investigation Department, the Technology Computer Emergency Response Team of Sri Lanka, the Sri Lanka Computer Emergency Response Team and the Centre for Digital Forensics. The sample of thirty four (34) investigators and two hundred and sixty one cases (261) were selected for our study from the above organisations. In addition to that, a sample of sixty eight (68) lawyers was selected from the Attorney General Department. Close-ended questionnaires were used to collect the data. The collected quantitative data were analysed by using Service Provisioning System Software to make the conclusions. The results showed that the current digital forensics infrastructure uses the unorganized methods and waste limited resources. Furthermore, the results showed how the lack of literacy of Information and Communication Technology (ICT) and laws affect investigations. This research identified the need for improvement of the resources used on the investigation and knowledge on ICT and law of investigators and lawyers. It shows that the open source tools and assemble digital forensics workstation could be used to reduce the cost. It also identified that the phases such as preparation, collection, examination, analysis and presentation were necessary to conduct a successful investigation. Finally, the thesis proposes phases, methods and tools suitable for digital forensics in Sri Lanka.

Keywords: Criminal investigation, Information and communication technology, Lawyers