

SCHATZ, Bradley, B.Sc. (Comp. Sci.), University of Queensland

Thesis Title:

Digital evidence: representation and assurance

Supervisors:

Adjunct Prof. George Mohay (Principal)

Dr. Andrew Clark (Associate)

Citation:

This thesis addresses problems related to the complexity and volume of evidence drawn from computers and other digital devices (so-called digital evidence) in policing and legal matters. The research identifies methods for increasing the efficiency and reliability of investigations employing digital evidence, by proposing automated methods of processing and documenting such information. The research examined at a fundamental level the role of representation in interpreting and analysing digital evidence, identifying where a formal approach to representing digital investigations and digital evidence reduces the complexity and volume problems. A formal approach was shown to be of benefit in automating the identification of situations of interest from correlated event records sourced from computer security and other disparate event logs. Additionally a formal approach was shown to facilitate granular sharing of evidence and extensible documentation of investigations. Finally, the research identified flaws in the fundamental assumptions in the interpretation of time-stamped evidence, and proposed a novel method of inferring the temporal behaviour of arbitrary computers.