The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice

This thesis is presented for the degree of
Doctor of Philosophy of Murdoch University

By
Richard Brian Adams

2012
Declaration

I declare that this thesis is my own account of my research and contains as its main content work which has not previously been submitted for a degree at any tertiary education institution.

Signature:

Date: 5 March 2013
Acknowledgments

I would like to express my sincere gratitude to my supervisors, Dr Val Hobbs and Dr Graham Mann, for their unfailing support and encouragement – I could not have completed this thesis without them.

Special thanks are due to Phill Russo, Tim Thomas and Dr Colin Armstrong for their help and willingness to provide constructive feedback on my ideas and to all those who took part in the evaluation process.

Finally, I would like to acknowledge the love and support of my wife, Jane, and our children James, Matthew and Charlotte to whom I dedicate this work.
Abstract

Given the pervasive nature of information technology, the nature of evidence presented in court is now less likely to be paper-based and in most instances will be in electronic form. However, evidence relating to computer crime is significantly different from that associated with the more ‘traditional’ crimes for which, in contrast to digital forensics, there are well-established standards, procedures and models to which law courts can refer.

The key problem is that, unlike some other areas of forensic practice, digital forensic practitioners work in a number of different environments and existing process models have tended to focus on one particular area, such as law enforcement, and fail to take into account the different needs of those working in other areas such as incident response or ‘commerce’.

This thesis makes an original contribution to knowledge in the field of digital forensics by developing a new process model for digital data acquisition that addresses both the practical needs of practitioners working in different areas of the field and the expectation of law courts for a formal description of the process undertaken to acquire digital evidence.

The methodology adopted for this research is design science on the basis that it is particularly suited to the task of creating a new process model and an ‘ideal approach’ in the problem domain of digital forensic evidence. The process model employed is the Design Science Research Process (DSRP) (Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen and Bragge, 2006) that has been widely utilised within information systems research.

A review of current process models involving the acquisition of digital data is followed by an assessment of each of the models from a theoretical
perspective, by drawing on the work of Carrier and Spafford (2003)\(^1\), and from a legal perspective by reference to the Daubert test\(^2\). The result of the model assessment is that none provide a description of a generic process for the acquisition of digital data, although a few models contain elements that could be considered for adaptation as part of a new model.

Following the identification of key elements for a new model (based on the literature review and model assessment) the outcome of the design stage is a three-stage process model called the Advance Data Acquisition Model (ADAM) that comprises of three UML\(^3\) Activity diagrams, overriding Principles and an Operation Guide for each stage. Initial testing of the ADAM (the Demonstration stage from the DSRP) involves a ‘desk check’ using both in-house documentation relating to three digital forensic investigations and four narrative scenarios. The results of this exercise are fed back into the model design stage and alterations made as appropriate.

The main testing of the model (the DSRP Evaluation stage) involves independent verification and validation of the ADAM utilising two groups of ‘knowledgeable people’. The first group, the Expert Panel, consists of international ‘subject matter experts’ from the domain of digital forensics. The second group, the Practitioner Panel, consists of peers from around Australia that are digital forensic practitioners and includes a representative from each of the areas of relevance for this research, namely: law enforcement, commerce and

\(^1\) Who provide a list of the essential requirements for a digital forensic process model
\(^2\) This is a test originating from the United States that has been used by courts to assess ‘scientific’ evidence in various jurisdictions (for instance it is mimicked in a discussion paper by the Law Commission for England and Wales (Edmond, 2010)).
\(^3\) Unified Modeling Language
incident response. Feedback from the two panels is considered and modifications applied to the ADAM as appropriate.

This thesis builds on the work of previous researchers and demonstrates how the UML can be practically applied to produce a generic model of one of the fundamental digital forensic processes, paving the way for future work in this area that could include the creation of models for other activities undertaken by digital forensic practitioners. It also includes the most comprehensive review and critique of process models incorporating the acquisition of digital forensics yet undertaken.
Table of contents

CHAPTER 1: INTRODUCTION TO THE RESEARCH ................................................. 1
  1.1 BACKGROUND ................................................................................. 1
  1.2 RESEARCH PROBLEM ....................................................................... 7
  1.3 RESEARCH OBJECTIVE AND QUESTIONS ......................................... 7
  1.4 RESEARCH SCOPE ............................................................................ 8
  1.5 RESEARCH CONTRIBUTION ................................................................. 12
  1.6 METHODOLOGY ................................................................................. 12
  1.7 OUTLINE OF THE THESIS ................................................................. 22
  1.8 SUMMARY .......................................................................................... 23

CHAPTER 2: LITERATURE REVIEW ............................................................... 25
  2.1 INTRODUCTION .................................................................................. 25
  2.2 DIGITAL EVIDENCE ........................................................................... 26
  2.3 STANDARDS AND GUIDELINES IN DATA ACQUISITION ....................... 29
  2.4 THE FIRST DIGITAL FORENSIC RESEARCH WORKSHOP ................. 36
  2.5 REVIEW OF DIGITAL FORENSIC PROCESS MODELS ....................... 37
  2.6 SUMMARY ......................................................................................... 81

CHAPTER 3: MODEL REQUIREMENTS ......................................................... 82
  3.1 INTRODUCTION .................................................................................. 82
  3.2 ASSESSMENT CRITERIA FOR PREVIOUS MODELS .............................. 82
  3.3 ASSESSMENT OF PREVIOUS MODELS ............................................... 85
  3.4 SUMMARY OF MODEL ANALYSIS ....................................................... 118
  3.5 SUMMARISING THE REQUIREMENTS FOR A NEW MODEL .............. 121
  3.6 SUMMARY ......................................................................................... 124

CHAPTER 4: DESIGN AND DEVELOPMENT .............................................. 125
  4.1 INTRODUCTION .................................................................................. 125
  4.2 MODEL DESIGN ELEMENTS ............................................................... 125
  4.3 STAGE 1: INITIAL PLANNING ............................................................. 130
  4.4 STAGE 2: THE ONSITE PLAN .............................................................. 141
  4.5 STAGE 3: ACQUISITION OF DIGITAL DATA ..................................... 144
  4.6 MODEL CREATION ............................................................................. 145
  4.7 SUMMARY ......................................................................................... 157

CHAPTER 5: DEMONSTRATION ................................................................. 158
  5.1 INTRODUCTION .................................................................................. 158
  5.2 CASE DOCUMENTATION COMPARISON ........................................ 159
  5.3 SCENARIO ‘WALKTHROUGHS’ ............................................................ 167
  5.4 SUMMARY ......................................................................................... 184

CHAPTER 6: EVALUATION ........................................................................... 185
  6.1 INTRODUCTION .................................................................................. 185
  6.2 USE OF EXPERT AND PEER REVIEWERS ........................................ 186
  6.3 THE EXPERT PANEL ........................................................................ 186
  6.4 THE PRACTITIONER PANEL ............................................................... 188
  6.5 FEEDBACK FROM PANELS ................................................................. 191
  6.6 COMPLETED ADAM ............................................................................ 208
  6.7 SUMMARY ......................................................................................... 208

CHAPTER 7: CONCLUSION .......................................................................... 209
  7.1 INTRODUCTION .................................................................................. 209
  7.2 COMMUNICATION ............................................................................. 209
  7.3 RESEARCH SUMMARY ....................................................................... 210
  7.4 RESEARCH QUESTIONS REVISITED ................................................ 213
Figures

Figure 1    Design Science Research Process (DSRP) model after Peffers et al (2006) ........... 15
Figure 2    Digital Crime Scene Investigation Phases after Carrier and Spafford (2004) .......... 39
Figure 3    The IDIP after Carrier and Spafford (2004) ............................................. 40
Figure 4    The EDIPM after Baryamureeba and Tushabe (2004) ..................................... 46
Figure 5    The Three Stage Process after Kohn et al (2006) .......................................... 53
Figure 6    The Four Step Forensic Process (FSFP) after Kent et al (2006) ......................... 48
Figure 7    TDERAPM Phases after Khatir et al (2008) ................................................. 53
Figure 8    Digital Forensic Principles after Ieong (2006) .............................................. 61
Figure 9    Process Flow Between Roles in a Forensic Investigation after Ieong (2006) ........ 62
Figure 10   EEDI stages after Stephenson (2003) ......................................................... 70
Figure 11   Kruse & Heiser Activity diagram after Kohn et al (2008) ............................... 75
Figure 12   Kruse & Heiser Use Case diagram after Kohn et al (2008) ............................. 75
Figure 13   US DoJ Activity diagram after Kohn et al (2008) ......................................... 76
Figure 14   US DoJ Use Case diagram after Kohn et al (2008) ......................................... 76
Figure 15   Forensic Process Use Case after Ruan and Huebner (2009) ......................... 77
Figure 16   Forensic Process Activity Diagram after Ruan and Huebner (2009) ............... 77
Figure 17   The Perambulation Procedure after Wang and Yu (2007) ............................ 80
Figure 18   The ADAM Stage 1 – Initial Planning (version 1) ......................................... 148
Figure 19   The ADAM Stage 2 – The Onsite Plan (version 1) ......................................... 149
Figure 20   The ADAM Stage 3 – Acquisition of Digital Data (version 1) ......................... 150
Figure 21   The ADAM Stage 3 – Acquisition of Digital Data (version 2) ......................... 166
Figure 22   The ADAM Stage 2 amended (within shaded area) for MOD #3 ..................... 204
Figure 23   The ADAM Stage 3 amended (within shaded area) for MODs #3 and #4 ......... 205
Figure 24   The ADAM Stage 3 amended (within shaded area) for MOD #6 ..................... 206
Figure 25   The ADAM Stage 3 amendments catering for network/cloud/live acquisition .... 207
Figure 26   The ADAM Stage 1 (Initial Planning) ...................................................... 225
Figure 27   The ADAM STAGE 2 (Creating the Onsite Plan) ....................................... 226
Figure 28   The ADAM STAGE 3 (Acquiring Digital Data) ........................................... 227