



A Workflow to Support Forensic Database Analysis

Research Masters with Training Thesis

Rojesh Susaimanickam

27th November 2012

Dr. Kevin Lee

Supervisor, Murdoch University, Perth WA

Mr. Richard Boddington

Supervisor, Murdoch University, Perth WA

Acknowledgements

I would like to thank my supervisors Kevin Lee and Richard Boddington for their guidance and support throughout the project. Their guidance and inspiration have been instrumental in directing the course of this research. Thank you both for giving me the opportunity to spend this time researching and for sharing of your insight, time, energy and experience.

I would like to thank Mario Pinelli, Quentin Kuhl and Adam Baker for all the support and guidance they provided at work during this time.

I would also like to thank my Parents, my uncle Fr. Terry for their support, guidance and encouragement. Their support was essential in making this degree a reality. In addition, I would like to thank my sisters Christina & Bibiana for all the support, encouragement and reading my drafts.

Finally, I would like to thank Ms. Rose for all her support throughout this degree, Ms. Bishop for reading all my drafts, the Somascan youth and all my friends who supported me throughout this process.

Copyright Acknowledgement

I understand that, under the provisions of sub-section 51.2 of the Copyright Act 1968, all or part of this thesis may be copied without infringement of copyright where such a reproduction is for the purposes of study and research.

This statement does not signal any transfer of copyright away from the author.

Signed:

Full Name of Degree: Research Masters with Training - Information Technology

Thesis Title: A Workflow to Support Forensic Database Analysis

Author: Rojesh Susaimanickam

Year: 2012

Statement of Authorship

The work contained in this thesis has not been previously submitted for a degree or diploma at any other higher education institution. To the best of my knowledge and belief, this thesis contains no material previously published or written by another person except where due reference is made.

_____ Signature of Author

Abstract

Governments and private organisations are increasingly aware that vital information stored in their databases is no longer safe behind perimeter firewalls, intrusion prevention systems and other edge protections. Databases store a broad range of private and important information, making them a prime target for exploitation by wrongdoers wishing to breach confidentiality, damage the integrity of the data or make it unavailable to its users.

The intricate nature and the non-stoppable critical services running in databases makes forensic examination of database difficult and challenges the forensics recovery and examination processes.

The research presented in this thesis discusses the feasibility of developing an enhanced workflow that provides insight into the challenging complexities of examining and using database evidence. It lays the foundation for the development and establishment of standards in database forensic analysis and forensic case management.

The major contribution of this research is a literature review that summarises the state-of-the-art in database forensics. It argues for the need for more in-depth research in this field and highlights limited availability of forensic data. To improve this, the research presents the design of a generic workflow of database forensic examination. This is evaluated using a qualitative and case study based evaluation and highlights the various limitations and drawback of the workflow.

In summary, the research in this thesis proposes a system that allows a forensic examiner to focus on what is relevant to a case in a systematic way that can be proved in court. The workflow also acts as a case management tool by aiding the forensic

examiner to apply established standards and procedures to identify best-case result by systematically, thoroughly and efficiently collecting and validating digital evidence.

1	INTRODUCTION.....	10
1.1	OVERVIEW.....	10
1.2	AIMS.....	12
1.3	STRUCTURE OF THIS THESIS.....	13
2	BACKGROUND.....	15
2.1	OVERVIEW.....	15
2.2	DATABASE, DATABASE APPLICATIONS AND DATABASE USERS.....	15
2.3	DATABASE SYSTEMS ARCHITECTURE.....	18
2.4	CYBER FORENSICS.....	31
2.5	DATABASE RELATED INCIDENTS.....	32
2.6	DATABASE SECURITY FLAWS.....	37
2.7	CHALLENGES IN DATABASE FORENSICS.....	47
2.8	FORENSIC ARTIFACTS CONTAINED IN A DATABASE.....	51
2.9	SUMMARY.....	53
3	FORENSIC EXAMINATION FRAMEWORKS.....	55
3.1	OVERVIEW.....	55
3.2	COMPUTER FORENSIC INVESTIGATIVE PROCESS (CFIP).....	55
3.3	AN EVENT BASED DIGITAL INVESTIGATION FRAMEWORK (EBDFIF).....	56
3.4	THE ENHANCED DIGITAL INVESTIGATION PROCESS MODEL (EDIPM).....	57
3.5	FORENSIC PROCESS MODEL (FPM).....	59
3.6	THE ABSTRACT DIGITAL FORENSIC MODEL (ADFM).....	60
3.7	THE INTEGRATED DIGITAL INVESTIGATION MODEL (IDIM).....	61
3.8	NEW DIGITAL FORENSIC INVESTIGATION PROCEDURE MODEL (NDFIPM).....	63
3.9	SYSTEMATIC DIGITAL FORENSIC INVESTIGATION MODEL (SDFIM).....	65
3.10	CYBER FORENSIC FRAMEWORKS & MODEL COMPARISON.....	67
4	A GENERIC WORKFLOW FOR DATABASE FORENSICS EXAMINATION.....	70
4.1	OVERVIEW.....	70
4.2	REQUIREMENT ANALYSIS.....	71
4.3	PRE-EXAMINATION PHASE.....	78
4.4	A GENERIC HIGH LEVEL WORKFLOW FOR DATABASE FORENSIC EXAMINATION.....	80
4.5	PHASE 1: INCIDENT REPORTING PHASE – DATABASE.....	82
4.6	PHASE 2: EXAMINATION PREPARATION PHASE.....	83
4.7	PHASE 3: PHYSICAL & DIGITAL EXAMINATION PHASE.....	84
4.8	PHASE 4: DOCUMENTATION AND PRESENTATION PHASE.....	88
4.9	PHASE 5: POST EXAMINATION PHASE.....	89
4.10	PHASE 6: POST EXAMINATION ANALYSIS PHASE.....	89
4.11	SUMMARY.....	90
5	EVALUATION.....	91
5.1	OVERVIEW.....	91
5.2	IMPLEMENTATION.....	91
5.3	DEPLOYMENT OVERVIEW.....	91
5.4	SYSTEM LIFE CYCLE.....	92
5.5	SYSTEM DATA FLOW DIAGRAM.....	94

5.6	HARDWARE AND SOFTWARE REQUIREMENTS	94
5.7	SYSTEM DESIGN INTERFACE.....	95
5.8	QUALITATIVE EVALUATION.....	111
5.9	CASE STUDY BASED EVALUATION.....	117
5.10	NAME ASSIGNING FOR COMPARISON	130
5.11	LIMITATION OF THE PROPOSED WORKFLOW	132
5.12	SUMMARY	133
6	CONCLUSIONS.....	135
6.1	OVERVIEW.....	135
6.2	OVERVIEW OF THESIS.....	135
6.3	MAJOR CONTRIBUTIONS.....	137
6.4	SUGGESTIONS FOR FUTURE WORK	138
6.5	CONCLUDING REMARKS	138
APPENDIX A	VULNERABILITY DETAIL.....	139
APPENDIX B	ONLINE TOOLS AND RESOURCES.....	144
APPENDIX C	DATABASE CREATION CODE.....	148
7	REFERENCE.....	157
8	GLOSSARY	170

List of Figures:

FIGURE 1: MONOLITHIC OR CENTRALISED SYSTEMS (WEDDELL, 2006)	21
FIGURE 2: PARALLEL DATABASE SYSTEMS (WEDDELL, 2006)	22
FIGURE 3: CLIENT SERVER SYSTEM (WEDDELL, 2006).....	23
FIGURE 4: MULTI-DATABASE SYSTEMS WITHOUT A GATEWAY (WEDDELL, 2006).....	24
FIGURE 5: MULTI-DATABASE WITH GATEWAY (WEDDELL, 2006)	24
FIGURE 6: COMPONENTS OF A DBMS (HELLERSTEIN, STONEBRAKER, & HAMILTON, 2007)	25
FIGURE 7: DATABASE VULNERABILITIES (LITCHFIELD, ANLEY, HEASMAN, & GRINDLAY, 2005, P. 5).....	39
FIGURE 8: COMPUTER FORENSIC INVESTIGATIVE PROCESS (POLLITT M. M., 1995)	55
FIGURE 9: FIVE DISTINCTIVE CATEGORIES IN THE EBDIF (CARRIER & SPAFFORD, 2004).....	56
FIGURE 10: ENHANCED DIGITAL INVESTIGATION PROCESS MODEL (BARYAMUREEBA & TUSHABE, 2006).....	58
FIGURE 11: ABSTRACT DIGITAL FORENSIC MODEL (YUSOFF, ROSLAN, & ZAINUDDIN, 2011)	61
FIGURE 12: INTEGRATED DIGITAL INVESTIGATION MODEL (YUSOFF, ROSLAN, & ZAINUDDIN, 2011)	62
FIGURE 13: NEW DIGITAL FORENSIC INVESTIGATION PROCEDURE MODEL (SHIN, 2008)	63
FIGURE 14: SYSTEMATIC DIGITAL FORENSIC INVESTIGATION MODEL (AGARWAL, GUPTA, GUPTA, & GUPTA, 2011)	65
FIGURE 15: PRE-EXAMINATION PHASE.....	78
FIGURE 16: A GENERIC HIGH LEVEL WORKFLOW FOR DATABASE FORENSIC EXAMINATION	80
FIGURE 17: INCIDENT-REPORTING PHASE	82
FIGURE 18: EXAMINATION PREPARATION PHASE.....	84
FIGURE 19: PHYSICAL EXAMINATION PHASE	85
FIGURE 20: DIGITAL EXAMINATION PHASE.....	86
FIGURE 21: DOCUMENTATION AND PRESENTATION PHASE.....	88
FIGURE 22: POST EXAMINATION PHASE.....	89
FIGURE 23: POST EXAMINATION ANALYSIS PHASE.....	90
FIGURE 24: DEPLOYMENT OVERVIEW	92
FIGURE 25: SYSTEM LIFE CYCLE	93
FIGURE 26: SYSTEM DATA FLOW DIAGRAM	94
FIGURE 27: SYSTEM LOGIN PAGE	96
FIGURE 28: NEW EXAMINER REGISTRATION PAGE.....	96
FIGURE 29: EXAMINER HOME PAGE	97
FIGURE 30: ADMIN HOME PAGE.....	98
FIGURE 31: INCIDENT REPORTING PHASE 1 - CONTACT DETAILS.....	99
FIGURE 32: INCIDENT-REPORTING PHASE 1 - INCIDENT TYPE.....	100
FIGURE 33: INCIDENT REPORTING PHASE 1 - SYSTEM AUDIT.....	101
FIGURE 34: INCIDENT REPORTING PHASE 1 - SYSTEM DETAILS	102
FIGURE 35: INCIDENT REPORTING PHASE 1 - NETWORK DETAILS	103
FIGURE 36: INCIDENT REPORTING PHASE 1 - PHYSICAL SECURITY	104
FIGURE 37: INCIDENT PREPARATION - NETWORK ISOLATION.....	105
FIGURE 38: PHYSICAL EXAMINATION PHASE.....	106
FIGURE 39: DIGITAL EXAMINATION PHASE.....	107
FIGURE 40: DOCUMENTATION & PRESENTATION PHASE.....	108
FIGURE 41: POST EXAMINATION PHASE	109
FIGURE 42: POST EXAMINATION ANALYSIS.....	110
FIGURE 43: COMPARISON OF BARRACUDA NETWORK DATABASE INCIDENT WITH THAT OF A NORMAL PROCESS.....	120
FIGURE 44: BARRACUDA NETWORK PAGE WITH VULNERABLE PHP SCRIPT (PULLICINO, 2012).....	121
FIGURE 45: MD5 HASHED PASSWORD (PULLICINO, 2012).....	121

FIGURE 46: HASHED USER DETAILS (PULLICINO, 2012).122
FIGURE 47: INTRUSION ROUTE TO THE SONY SYSTEM (ROTHACKER, 2011)127

List of Tables:

TABLE 1: ASSIGNING SHORT NAME.....66
TABLE 2: COMPARING EXISTING CYBER FORENSIC FRAMEWORKS67
TABLE 3: ASSIGNING SHORT NAME.....130
TABLE 4: COMPARISON OF THE PROPOSED WORKFLOW WITH OTHER CYBER FORENSIC FRAMEWORKS.....131