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

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.

List of Figures:

List of Tables: