

# CONTENTS - COMPUTER FORENSICS

<b>1. COMPUTER FORENSICS.....</b>	<b>5</b>
INTRODUCTION .....	5
STRUCTURE OF THIS PAPER .....	5
HISTORY OF COMPUTER FORENSICS .....	7
COMPUTER FORENSICS VS ELECTRONIC DISCOVERY VS DATA RECOVERY .....	7
<i>Computer forensics</i> .....	7
<i>Electronic discovery</i> .....	8
<i>Data recovery</i> .....	8
<b>2. OVERVIEW OF INFORMATION TECHNOLOGY .....</b>	<b>9</b>
WHAT IS A COMPUTER?.....	9
<i>External view</i> .....	9
<i>Theory of operation</i> .....	12
<i>Looking inside the computer</i> .....	14
DATA STORAGE CAPACITY .....	16
<i>Basic units and multiples</i> .....	16
<i>Average storage capacity of modern computer</i> .....	17
<i>Comparison with printed documents</i> .....	17
NETWORKS AND THE INTERNET .....	17
<i>Implications for locating evidence</i> .....	17
<i>Network traffic as evidence</i> .....	18
<i>Cloud Computing</i> .....	18
ELECTRONIC STORAGE MEDIA.....	19
<b>3. ELECTRONIC EVIDENCE .....</b>	<b>21</b>
ELECTRONIC DOCUMENTS.....	21
<i>Storage of electronic documents</i> .....	21
<i>Metadata</i> .....	22
COMPUTER GENERATED DOCUMENTS .....	25
<i>The “trace” evidence of computer forensics</i> .....	25
<i>Examples of computer generated documents</i> .....	26
<b>4. COMPUTER FORENSIC SOFTWARE .....</b>	<b>29</b>
MODERN COMPUTER FORENSIC SOFTWARE .....	29
ENCASE .....	29
FTK.....	30
RELIABILITY OF COMPUTER FORENSIC ANALYSIS PROGRAMS.....	31
<i>Discussion in EnCase Legal Journal</i> .....	32
DISCLOSURE OF KNOWN FLAWS IN COMPUTER FORENSIC SOFTWARE .....	33
SECTION 137 OF THE EVIDENCE ACT 2006 .....	33
WHO IS REALLY GIVING EVIDENCE?.....	34
<b>5. COMPUTER FORENSICS – SCIENCE OR NOT? .....</b>	<b>37</b>
DEFINING “SCIENCE” .....	37
SCIENTIFIC ACTIVITY IN THE FIELD OF COMPUTER FORENSICS.....	37
COMPUTER FORENSIC EXPERTS – SCIENTISTS OR NOT?.....	38
CATEGORIES OF COMPUTER FORENSIC EXPERTS.....	39
<i>Technicians</i> .....	40
<i>Developers</i> .....	41
<i>Scientists</i> .....	41
<b>6. COMPUTER FORENSIC ANALYSIS PROCESS .....</b>	<b>43</b>
SELECTION OF EXPERT .....	43
INSTRUCTION .....	44
<i>Financial arrangements</i> .....	46
ACQUISITION OF EVIDENCE .....	46

<i>Volatility of electronic data</i> .....	47
<i>Forensically sound acquisition process</i> .....	47
<i>Storage of forensic clones</i> .....	48
<i>Establishing the integrity of a forensic clone</i> .....	49
<i>Format of forensic clone</i> .....	49
<i>Chain of custody</i> .....	50
EVIDENCE PREPARATION.....	50
INITIAL EXAMINATION.....	51
EXAMINATION.....	51
<i>Keyword search</i> .....	52
<i>Event reconstruction</i> .....	55
<i>Picture review</i> .....	56
<i>Video review (key-frames)</i> .....	56
SCIENTIFIC TESTING.....	56
DOCUMENTATION OF RESULTS.....	57
REPORTING.....	57
MANAGING COSTS.....	58
<b>7.    COMPUTER FORENSICS – EVIDENTIAL AND LEGAL ISSUES.....</b>	<b>59</b>
INTRODUCTION.....	59
<b>8.    PART ONE – BASIC PRINCIPLES.....</b>	<b>61</b>
ADMISSIBILITY OF EXPERT OPINION EVIDENCE.....	61
EXPERT.....	61
EXPERT EVIDENCE.....	62
ADMISSIBILITY.....	62
THE <i>DAUBERT</i> APPROACH.....	63
<i>The background to Daubert</i> .....	63
<i>The facts and procedural history in Daubert</i> .....	64
<i>The effect of Daubert</i> .....	64
<i>Daubert in the UK</i> .....	65
<i>Daubert in New Zealand?</i> .....	66
THE FACTUAL FOUNDATION.....	68
EXPERT EVIDENCE IN CIVIL PROCEEDINGS.....	68
EXPERT EVIDENCE IN CRIMINAL PROCEEDINGS.....	72
MACHINE EVIDENCE.....	73
SECTION 137 – GENERAL COMMENTS.....	74
<b>9.    PART TWO – THE ISSUES SURROUNDING THE INVESTIGATION AND</b>	
<b>EXAMINATION OF DIGITAL EVIDENCE.....</b>	<b>79</b>
INVESTIGATION AND EXPERTISE.....	79
HANDLING DIGITAL EVIDENCE.....	80
GATHERING THE EVIDENCE.....	81
AN ILLUSTRATION.....	81
THE EVIDENCE GATHERING PROCESS.....	83
DIGITAL EVIDENCE ANALYSIS.....	84
FORENSIC TOOLS.....	86
THE EXPERT’S REPORT.....	87
VALIDATING AND VERIFYING COMPUTER FORENSIC SOFTWARE.....	87
THE EVIDENTIAL FOUNDATION.....	90
PRESERVATION OF DATA.....	92
AUTHENTICATION BY OTHER THAN FORENSIC EXAMINATION.....	93
CONCLUSION.....	97