Contents

Preface vii

Acknowledgments xi

List of Tables xii

List of Figures xiii

1 Introduction 1

1.1 Key developments 1
1.2 Digital devices in society 5
1.3 Technology and culture 6
1.4 Comment 7

2 Evidential Potential of Digital Devices 9

2.1 Closed vs. open systems 10
2.2 Evaluating digital evidence potential 17

3 Device Handling 19

3.1 Seizure issues 21
3.2 Device identification 31
3.3 Networked devices 36
3.4 Contamination 40

4 Examination Principles 43

4.1 Previewing 43
4.2 Imaging 47
4.3 Continuity and hashing 48
4.4 Evidence locations 49

5 Evidence Creation 55

5.1 A seven-element security model 56
5.2 A developmental model of digital systems 60

5.3 Knowing 61
5.4 Unknowing 63
5.5 Audit and logs 68

6 Evidence Interpretation 69

6.1 Data content 69
6.2 Data context 83

7 Internet Activity 85

7.1 A little bit of history 85
7.2 The ISO/OSI model 86
7.3 The internet protocol suite 90
7.4 DNS 94
7.5 Internet applications 96

8 Mobile Devices 109

8.1 Mobile phones and PDAs 109
8.2 GPS 116
8.3 Other personal technology 118

9 Intelligence 119

9.1 Device usage 119
9.2 Profiling and cyberprofiling 121
9.3 Evaluating online crime: automating the model 124
9.4 Application of the formula to case studies 126
9.5 From success estimates to profiling 129
9.6 Comments 129

10 Case Studies and Examples 131

10.1 Introduction 131
10.2 Copyright violation 131
10.3 Missing person and murder 133
10.4 The view of a defence witness 137

Appendix A The "Aircraft Carrier" PC 141

Appendix B Additional Resources 145

B.1 Hard disc and storage laboratory tools 145
B.2 Mobile phone/PDA tools 146
B.3 Live CDs 146
B.4 Recommended reading 146

Appendix C SIM Card Data Report 149

References 157

Index 161