

## Index

This portion of the book will be replaced by an index in the final version

### Detailed outline

Forward.....	6
Forward to the peer review edition.....	6
Appreciation.....	7
My background.....	7
Who and what this book is designed for.....	8
1 Introduction and overview.....	9
Introduction.....	9
Assumptions and a perspective.....	10
Overview of the book.....	11
Questions.....	13
2 An overview of digital forensics.....	14
Introduction.....	14
The legal context.....	16
The processes involved with digital forensic evidence.....	18
Identification.....	19
Collection.....	19
Transportation.....	21
Storage.....	21
Examination and traces.....	22
Analysis.....	22
Interpretation.....	23
Attribution.....	24
Reconstruction.....	25
Presentation.....	27
Destruction.....	27
Expert witnesses.....	27
Tools and tool use in digital forensics.....	29
Challenges and legal requirements.....	32
Make or miss faults.....	35
Accidental or intentional faults.....	35
False positives and negatives.....	36
The Legal Process.....	37
Pre-legal records retention and disposition.....	38
First filing.....	40
Notice.....	41
Preservation orders.....	41
Disclosures and productions.....	42
Depositions.....	43

# Digital Forensic Evidence Examination

Motions, Sanctions, and Admissibility.....	44
Pre-trial.....	45
Testimony.....	47
Case closed.....	48
Duties.....	48
Honesty, Integrity, and Due Care.....	48
Competence.....	50
Retention and disposition.....	50
The science of digital forensic evidence examination.....	51
Other resources.....	52
Questions.....	52
3 The physics of digital information.....	54
The nature of digital forensic evidence.....	54
The physics of DFE is different from that of matter.....	54
Finite granularity.....	54
Exact copies without altering the originals.....	55
You can "take" bits without removing the original.....	56
Bits move very - but finitely - quickly from place to place.....	56
DFE is created by artificial means.....	56
Finite state machines are the most common artifice.....	57
Homing sequences and FSMs.....	57
How time transforms the artifice.....	58
The results are always bits.....	59
Results are always "exact".....	59
FSM produce partially ordered output sequences.....	59
Limits on accuracy and precision based on representation.....	60
Some legal perspectives.....	60
Forgery is indiscernible at the level of individual bits.....	60
DFE is latent by nature.....	61
DFE is trace evidence but not transfer evidence.....	61
DFE is generally circumstantial and hearsay.....	61
Information content in context and related issues.....	63
Languages have different content per density.....	63
Compression and other codings that alter content densities.....	64
Lossy and lossless transforms.....	64
Hash functions and digital signatures as lossy examples.....	65
Content only has meaning in context.....	66
Semantic information content.....	66
Eats shoots and leaves.....	66
Cognitive limits of computers and people constructing them.....	67
Faults and fault models.....	67
Computational complexity.....	68
Limits of what can be done.....	68
Limits on the examiner.....	71
Limits on the evidence and statements about it.....	72
Designs that take advantage of complexity.....	73

# Digital Forensic Evidence Examination

Outside the artifice.....	73
Fault tolerant computing and testing.....	73
Accidental violations of digital space assumptions.....	74
Intentional violations of digital space assumptions.....	75
Where worlds collide - the interface.....	76
What sensors sense and actuators actuate.....	77
Summary of properties.....	78
How computers work.....	81
General purpose computers and special purpose computers.....	81
Special and general purpose operating environments.....	82
Processes, files, and other structures in computers.....	83
Higher level structures.....	84
Extensions of information physics.....	85
Questions.....	85
4 A theoretical examination framework.....	87
Previous models.....	87
Gladyshev's model.....	87
Carrier's model.....	89
Kwan et. al.'s model.....	90
The present model.....	92
The legal context.....	92
The hypothesized claims.....	93
The hypothesized events.....	93
The traces.....	94
The internal consistency relationship between traces.....	94
The demonstration consistency of traces.....	95
The forensic procedures.....	96
Available resources.....	96
The schedule.....	97
Some discussion of the model.....	98
The proposed model is complex.....	98
The sizes of the model components.....	99
Limits on what we know about this model and digital forensics.....	103
The model and information physics.....	105
Translating words in events into testable statements.....	106
Questions.....	108
5 Analysis.....	110
Starting with a bag-of-bits.....	110
Redundancy in the bag-of-bits.....	110
Moving from the bag-of-bits to a meaningful context.....	111
Testing and fault models as an approach.....	111
Feature and characteristic detection and analysis.....	113
What is the symbol set?.....	114
Trace typing.....	116
Exact copies, regular expressions, and similar analyses.....	117
Equivalent content in different formats.....	120

# Digital Forensic Evidence Examination

Generating characteristics and features of traces.....	122
Consistency analysis of characteristics and features.....	130
Ordering assumptions and detection of out of order entries.....	130
Sourcing and travel patterns.....	132
Consistency checks across related records.....	134
Anchor events and external correlation.....	136
Differentials and jitter.....	138
Building sieves and counting things.....	140
Extracting traces from other traces.....	140
Building and using derived traces.....	141
Counting things.....	143
Combining mechanisms and dealing with resulting errors.....	143
Finding things that are intentionally hidden.....	146
Deletion and placement in hard-to-find places.....	146
Steganographic content and other transformations.....	147
Recursive embedded languages.....	151
Indicators.....	152
Visualization and other sensory methods in analysis.....	153
Examples.....	156
Farmer and Venema.....	156
Willassen.....	158
Other comments on the use of time for trace consistency.....	160
ForensiX.....	162
The Coroner's ToolKit.....	163
The NIJ view of analysis.....	163
Summary.....	165
Questions.....	165
6 Interpretation.....	168
Interpretation of traces and analysis results.....	169
Keeping alternative explanations in mind.....	169
Examples of trace interpretation.....	170
Interpretation and the presentation of statistics.....	171
Unstructured trace interpretation.....	173
Over-interpretation of traces and going "a bridge too far".....	174
Limitations of tools and false depictions in trace interpretation.....	175
Interpretation of missing traces.....	178
The use of redundancy to mitigate interpretation errors.....	180
Evaluating trace interpretation with information physics.....	181
Interpretation of events.....	186
The interpretation of words and implications in events.....	187
Event interpretation in light of information physics.....	189
Resource limits and interpretation - the schedule.....	195
Interpretation in statements and reports.....	197
Notions of "similarity" and quantification.....	199
So close and yet so far?.....	199
Substitutions and similar comparison mechanisms.....	200

# Digital Forensic Evidence Examination

Measurements of similarity and caution in their use.....	201
Other similar dubious interpretations.....	203
Making assumptions in interpretation.....	210
Assumptions provided to the examiner.....	210
Making assumptions "favorable" to the other side.....	210
Making assumptions based on trace analysis.....	211
Making assumptions based on consistent events and traces.....	212
Making inconsistent assumptions.....	213
Legal strategy in interpretation.....	214
Complex interpretations with assumptions.....	215
Interpretation relating to hidden content.....	216
Visualization in interpretation and analytical product.....	218
Interpretation errors and challenges.....	220
Questions.....	225
7 Attribution.....	228
The nature of statistics.....	229
If not statistics, how causality with complexity?.....	231
FSM predictability.....	231
Simulation approaches.....	231
Complexity arguments and cryptographic mechanisms.....	231
Sensors used for other purposes and related approaches.....	232
Correlating redundant sources of data.....	235
Attributing actions to human actors.....	236
Types of authentication methods.....	237
Keystroke analysis and similar authentication methods.....	237
Failure rates for biometric authentication methods.....	238
Something the user has.....	239
Something the user knows or can do.....	239
Other behavioral characteristics.....	240
N-Gram Analysis and Other Statistical Methods.....	240
Differentiation by how people type.....	241
Differentiation by how people attack.....	241
Limitations of these approaches.....	242
Using redundancy to build a consistent pattern.....	245
Summary of human attribution from DFE.....	245
Attribution of actions to automated mechanisms.....	246
Level 1 network attribution.....	246
Level 2 network attribution.....	248
Device identification and attribution.....	250
Operating environment identification and attribution.....	252
Complexity-related authenticators.....	253
Predicted behavior of programs.....	256
Limits of attribution to automated mechanisms.....	258
Information physics attribution limits and approaches.....	258
Making assumptions to make progress.....	264
Attribution of damages to parties.....	264

# Digital Forensic Evidence Examination

Summary of the legal environment.....	265
Summary of the technical environment.....	268
Overview of the attribution process.....	269
A general approach to listing damages.....	272
Demonstrating the forensically demonstrable properties.....	274
Quantification of damages.....	275
The continuous damages case.....	275
Putting time frames on damages.....	278
Tangibility of damages.....	279
Showing mitigation of harm.....	279
Demonstrating that the actions are uninvited.....	281
Demonstrating causality.....	282
A diligent effort to secure evidence.....	284
Most trespass damages are low valued.....	286
Attributing damages at a step.....	289
Overall attribution.....	290
Redundant records as indicators.....	290
Mens Rae and attribution.....	291
Verifying the integrity of attribution mechanisms.....	292
Verifying that the attribution goes in the right direction.....	293
Logical fallacies in attribution.....	295
Questions.....	302
8 Reconstruction.....	305
Reconstruction as driving time backwards.....	305
Reconstruction as an experimental approach.....	309
Some word usage.....	309
Forward reconstruction defined.....	311
What can be easily tested by reconstruction and how fast.....	313
Precision issues and prediction prior to experimentation.....	313
Repeatability of results.....	314
When is reconstruction not needed or revealing?.....	315
When is reconstruction needed or revealing?.....	315
The class approach and assumptions.....	316
Assumptions about properties typically made.....	317
Key properties in reconstruction.....	321
Identify a test that will confirm or refute a testable hypothesis.....	321
Bound the test.....	321
Construct a test environment.....	322
Perform the tests.....	324
Analyze the C-traces against the hypothesized C-traces.....	325
Optionally loop.....	325
Uncertainty in reconstruction.....	326
One approach to limited meaningful reconstruction.....	327
A slightly more complex reconstruction.....	328
A reconstruction to determine how to reconstruct.....	330
Legal restrictions and reconstruction.....	331

# Digital Forensic Evidence Examination

What does a DFE reconstruction laboratory look like?.....	333
What we can and cannot reasonably say.....	333
Who did what and how.....	334
The results of the experiments.....	335
The implication of these results as interpretation.....	335
Identifying assumptions and limitations.....	335
Questions.....	336
9 Tools and process.....	339
Clarifying the limitations of examination.....	340
Validation of examinations and examination systems.....	342
Validity of consistency results relating to traces.....	343
Validity of mechanism used to do the examination.....	345
Process controls.....	346
Defined and documented process.....	347
Tested components and tools.....	349
Keeping independent things separated.....	353
Assuring the purity of original and duplicated evidence.....	356
Validating purity of duplicated and derived evidence.....	356
Known test samples with known results.....	357
Contemporaneous notes.....	358
Calibration with known samples prior to use.....	359
Use of tools consistent with procedures.....	360
Checking results with redundant process after use.....	362
Presentation tools and visualization.....	362
Things tools don't show well or at all.....	363
Going faster using the visual cortex.....	364
Cognitive errors and visualization.....	365
The need to understand the tools and processes.....	366
Creating and using a "golden unit" environment.....	367
Creating the operating environment.....	367
Tools within WG.....	369
The next generation golden unit.....	369
Questions.....	370
10 Today and tomorrow.....	373
Today.....	373
Tomorrow.....	374
Questions.....	374
Index.....	375
Endnotes.....	383
Forward.....	383
Chapter 1.....	383
Chapter 2.....	383
Chapter 3.....	384
Chapter 4.....	385
Chapter 5.....	386
Chapter 6.....	388

# Digital Forensic Evidence Examination

Chapter 7.....	391
Chapter 8.....	395
Chapter 9.....	396
Chapter 10.....	396
Other end notes.....	396

ab13

**This portion of the book will be replaced by an index in the final version**