Table of Contents

Acknowledgements ix

About the Author xi

About the editors xiii

- Dr. Richard Hipp xiii
- Heather Mahalik xiii
- Brett Shavers xiv
- Eric Zimmerman xiv

Chapter 1 Introduction 1

- SQLite SQL basics 4
  - Creating a table 4
  - Inserting data into a table 9
  - Simple queries 10
  - *References* 12

Chapter 2 SQLite database file format 13

- Pages 14
- Database header 15
- B-trees 17
- B-tree pages 20
- Page Header 20

Table leaf pages 22

Cell Pointer Array 24

Cells & Records 25

Varints 25

- Negative varints 27

Record structure 28

- Interior table B-tree page record format 28
- Leaf table B-tree record format 28
- Interior index B-tree record format 29
- Leaf index B-tree record format 29

Table leaf pages 29

- Records/Serial types 32

Table interior pages 38

Index B-tree leaf tables 43

Index B-tree interior tables 46

WITHOUT ROWID tables 49

Overflow pages 50

Freeblock records 56

Pointer map pages 59

Lock-byte page 62

Freelist pages 63

Summary 65

References 65

Chapter 3 SQLite record recovery 67

Secure delete 68

Structure intact 70

Case 1 – A record with a valid entry in the cell pointer array 70

Orphaned records 73

Case 2 – Invalid serial types array 74

Case 3 – Length of serial types does not match payload length 74

Case 4 – Valid record 75

Case 5 – ALTER TABLE utilized since the record was stored 78

Case 6 - SQLite's loose affinity rules 80

Partial records 83

Example – A decoded record, before it is deleted 83

Partial record recovery 90

Case 7 – Decoding from byte zero 93

Case 8 – Decoding from byte one 93

Case 9 – Decoding a cell with an overwritten record length 95

Enable Null Trim 97

Changes to working copy databases 98

Summary 101

References 101

Chapter 4 SQLite rollback journals 103

Rollback Journal file format 106

The Journal Header 107

The journal page record 108

Page checksum 108

Journals in practice 109

Journal modes 110

Transaction walkthrough 111

Transactions 115

Master Journals 116

Rollback journal Forensics 117

Examining the content of a DB in the presence of a HOT journal 118

Examining the content of a DB in the presence of a COLD journal 121

Secure Delete 129

Summary 129

References 129

Chapter 5 Write-Ahead Logs 131

Write-Ahead Log file format 133

The Write-Ahead Log header 134

Checksum algorithm 134

SQLite WAL Frame header 135

The Shared Memory file (-shm) 135

The Write-Ahead Log in practice 136

Checkpoints 140

Write-Ahead Log Forensics 141

Why you should not use non-forensic tools........ 141

Peeling back WAL history 144

Determining when a record was added/deleted 150

Secure delete........ 160

Summary 160

References........ 160

Chapter 6 The Schema 161

The database schema........ 162

Table constraints 169

Foreign keys........ 171

Indexes 174

Triggers........ 176

Views 182

Summary 185

References:........ 185

Chapter 7 SQL........ 187

SQLite SELECT statement 187

Column aliases........ 190

WHERE clause........ 191

JOINs........ 194

LEFT JOIN/LEFT OUTER JOIN 196

INNER JOIN 202

CROSS JOIN 204

NATURAL JOIN 206

Aggregate functions 207

Count() 207

Sum() 207

Min(), Max(), Avg() 207

Group By 208

Group_Concat() 209

Dates and times in SQLite 211

Displaying using inbuilt SQLite functions 211

Forensic Browser for SQLite datetime SQL extensions 216

Forensic Browser for SQLite display functions 217

SQLite core functions 218

String handling 218

SubStr() 219

InStr() 221

Hex() 224

Length() 224

Lower(), Upper() 224

Typeof() 224

Case statements 225

Attaching a second database 226

Union/Intersect/Except 227

Common Table Expressions 229

Recursive Common Table Expressions 230

Built-in queries in The Forensic Browser for SQLite 234

Summary 235

References 236

Chapter 8 Odds and Ends 237

Introduction 237

FTS 237

R*TREE 241

Encryption 244

Passwords vs. keys 248

Dealing with BLOBs and structured data 249

ROWIDs 250

Summary 252

References 253

Chapter 9 Case study iOS sms.db 255

The structure of the iOS sms.db 255

Sample questions 259

Q. Can you create a report on all recovered messages? 259

Q. Is there any evidence of deleted messages? 267

Q. Can you recover any deleted messages?.......... 269

Q. Are there any other ways of determining who the third party is?.......... 272

Q. Can you determine when the specified messages were deleted? 283

Q. Why is it so difficult to link a user to a deleted message?.......... 286

Summary 295