

*"All-in-One Is All You Need."*

ALL-IN-ONE

CCFP<sup>SM</sup>

Certified Cyber Forensics  
Professional Certification

EXAM GUIDE



Electronic content  
includes:

- 250 practice exam questions
- Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain
- PDF copy of the book

*Complete coverage of all  
six CCFP exam domains*



*Ideal as both a study tool  
and an on-the-job reference*



*Filled with practice exam  
questions and in-depth  
explanations*

**Mc  
Graw  
Hill**  
Education

CHUCK EASTTOM

ALL IN ONE

# CCFP<sup>SM</sup> Certified Cyber Forensics Professional Certification

Exam Guide

Chuck Easttom



New York Chicago San Francisco  
Athens London Madrid Mexico City  
Milan New Delhi Singapore Sydney Toronto

McGraw-Hill Education is an independent entity from the International Information Systems Security Certification Consortium, Inc., (ISC)<sup>2</sup> and is not affiliated with (ISC)<sup>2</sup> in any manner. This publication and CD-ROM are not sponsored by, endorsed by, or affiliated with (ISC)<sup>2</sup> in any manner. This publication and CD-ROM may be used in assisting students to prepare for the Certified Cyber Forensics Professional (CCFP) exam. Neither (ISC)<sup>2</sup> nor McGraw-Hill Education warrant that use of this publication and CD-ROM will ensure passing any exam. CCFP is a service mark of (ISC)<sup>2</sup> in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Cataloging-in-Publication Data is on file with the Library of Congress

McGraw-Hill Education books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative, please visit the Contact Us pages at [www.mhprofessional.com](http://www.mhprofessional.com).

**CCFP<sup>SM</sup> Certified Cyber Forensics Professional Certification All-in-One Exam Guide**

Copyright © 2015 by McGraw-Hill Education. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

All trademarks or copyrights mentioned herein are the possession of their respective owners and McGraw-Hill Education makes no claim of ownership by the mention of products that contain these marks.

1234567890 DOC DOC 10987654

ISBN: Book p/n 978-0-07-183611-1 and CD p/n 978-0-07-183974-7  
of set 978-0-07-183976-1

MHID: Book p/n 0-07-183611-X and CD p/n 0-07-183974-7  
of set 0-07-183976-3

**Sponsoring Editor**  
Meghan Riley Manfre

**Editorial Supervisor**  
Patty Mon

**Project Manager**  
Harleen Chopra,  
Cenveo® Publisher Services

**Acquisitions Coordinator**  
Mary Demery

**Technical Editor**  
George (Buzz) Murphy

**Copy Editor**  
Lisa McCoy

**Proofreader**  
Paul Tyler

**Indexer**  
Karin Arrigoni

**Production Supervisor**  
Jean Bodeaux

**Composition**  
Cenveo Publisher Services

**Illustration**  
Cenveo Publisher Services

**Art Director, Cover**  
Jeff Weeks

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

---

## ABOUT THE AUTHOR

**Chuck Easttom** has over 20 years of practical experience in all aspects of the IT industry. That experience includes teaching and practicing all aspects of computer security, including forensics. In addition to the practical experience, he has been teaching IT topics for over 14 years. Most notably, he has taught forensics to the U.S. Secret Service and to the Internal Revenue Service, as well as private companies. This is his eighteenth book and his second forensics book. He also has 29 different IT certifications, including CISSP, CISSP- ISSAP, CHFI, and CEH, and three computer-related patents. Mr. Easttom also frequently serves as an expert witness in computer-related cases. You can find out more about him at [www.ChuckEasttom.com](http://www.ChuckEasttom.com).

### About the Technical Editor

**George (Buzz) Murphy**, CISSP, CASP, is a sought-after public speaker, corporate trainer, author, and cybersecurity evangelist who has touched the lives of thousands of adult learners across the country over the past 20 years with courses, seminars, and consulting presentations on a variety of technology topics. A former Dell technology training executive, he has addressed audiences at Comdex, NetWorld, and the National Computer Conference. Buzz has earned more than 19 IT and cybersecurity certifications from (ISC)<sup>2</sup>, CompTIA, and many other industry organizations. Having held a top-secret security clearance in both U.S. and NATO intelligence, he has trained network cybersecurity ops for the U.S. Army, various government security agencies, and foreign military personnel across Conus and EMEA, and has been involved with facilitating such subjects as site EMP hardening, cryptographic methodology, and computer forensic sciences as well as cyber-warfare training.

---

## ACKNOWLEDGMENTS

Writing a book is an arduous task. It is always my goal to make each book better than the last. While a single author's name may go on the cover, many people helped make this book a success. I have to thank several people for aiding me in this endeavor. First, the very helpful editorial staff at McGraw-Hill Education. They were simply wonderful to work with! And their commitment to quality is unsurpassed in the publishing world. The team included copy editors, layout editors, graphics design people, etc., all working to make sure no mistakes crept into the book. Also, thanks to Buzz Murphy for doing a tech edit of the chapters. Finally, I must thank my wife Teresa, who was so patient when I spent long hours working on this book.

---

# INTRODUCTION

Cyber forensics is a growing field. Reaffirming this, (ISC)<sup>2</sup>, creators of the CISSP credential, have created a comprehensive cyber forensics certification, the Certified Cyber Forensics Professional (CCFP). This certification is not a vendor tool certification, but rather a broad-based general cyber forensics certification. The certification requires a four-year degree with three years of experience in cyber forensics or IT security in at least three out of the six (ISC)<sup>2</sup> CCFP domains. If you don't have a degree, then six years of experience are required. If you have no experience, you can take the test and become an Associate of (ISC)<sup>2</sup>. The test consists of 125 multiple-choice questions. You have four hours and must pass with a 70 percent (700 points) or greater. After you've passed the exam successfully, you must also agree to adhere to the (ISC)<sup>2</sup> Code of Ethics (discussed in Chapter 2 of this book). Your application must then be endorsed by a current (ISC)<sup>2</sup> member (someone with the CCFP, CISSP, or similar certification) in order to achieve the credential.

This book is intended to thoroughly prepare you to take the CCFP exam. In this book, you will learn about forensics concepts, how to create forensics reports, various forensics techniques, computer forensics, mobile device forensics, and emerging trends. While we assume general IT security knowledge, we don't assume prior cyber forensics knowledge, although the CCFP exam assumes three years' experience. We will teach you everything you need to know to function effectively as a cyber forensics professional.

This book starts with general concepts in Chapter 1. Chapter 2 makes certain you have the appropriate technical background for cyber forensics. For most readers, Chapter 2 should be a review. As you progress through the chapters, you will see a mixture of theory along with practical techniques and advice. Look for extra test tips and notes in the chapters—these are meant to provide some extra information for you.



**EXAM TIP** Chapter 10 gives you a good introduction to mobile forensics. This is an increasingly important topic in forensics, and for the CCFP exam. You should pay particular attention to this chapter, and I recommend memorizing all the various terms found therein.

In addition to the book, I have created a website designed to be an aid to readers and forensics practitioners: [www.digitalforensicscert.com/](http://www.digitalforensicscert.com/). This website will be updated from time to time and expanded as needed. You can also visit my personal website: [www.ChuckEasttom.com](http://www.ChuckEasttom.com).

## How to Use This Book

As you read the book, you will encounter all the material you need to know to successfully take and pass the CCFP exam. I recommend you give each chapter a casual read and then return and spend time studying topics that were new to you or were difficult. If there are hands-on exercises or labs in a chapter (and there are several), whenever

possible actually execute the exercise or the lab. Anytime you encounter a new term or acronym, it is important that you memorize it. Don't just read it—make sure you commit it to memory.

Each chapter ends with review questions, and there are additional questions that accompany the book in electronic format. These questions will test your knowledge related to the CCFP domains, but these are not actual questions from the CCFP exam. The point is not to memorize the questions and answers, but use them to probe your knowledge and see how much has been retained. While the test assumes you have experience in cyber forensics, this book does not. My experience has been that a lot of working professionals, in any field, have very deep knowledge of some areas, and gaps in others. This book should review what you already know and fill in gaps in other areas.

As I mentioned, pay special attention to the Exam Tips in the chapters. These are specific guidelines discussing what you will need to know for the test, and in some cases, things you don't need to know for the test. When you finish a chapter, take a moment to reflect on it. Make sure you fully understood the chapter and memorized any new terms or acronyms before you move on to the next chapter.

## **The Examination**

I have taken many certification tests (29 as of this writing) and successfully taught many certification courses. Let me give you a few exam tips. First and foremost, make sure you are relaxed. Don't schedule the exam until you are really ready. And then schedule it at the best time for you. If you are a morning person, schedule it as early as you can. If you are not a morning person, then under no circumstances should you take a difficult test in the morning!

The day of the test, try to relax. On your way to the test, listen to your favorite music and relax. You will notice a few things when the test starts. The first is that occasionally you will see a question essentially repeated but worded a different way. That's okay and actually helps you. One way the question is worded might not be clear to you, but the other way is. This gives you a second chance to see what the question is asking and to answer it appropriately. Make sure you fully read each question. Four hours is plenty of time—don't rush.

You may have heard the old adage, never change your answer. That is only partially true. If a subsequent question is clearer to you and you know, absolutely know, that you need to change an answer, then do it. However, if your second answer is just a guess, stick with your first guess. Also, keep in mind that no matter how hard you study, you will probably encounter a question or two that you just don't know. Don't panic. You have a one in four chance of guessing right. Can you see at least one answer that you are certain is *not* correct? Well, you just raised your odds to one in three!

If you've read this book, you should feel confident that you've prepared, and prepared well. Last but not least, good luck!

# CCFP Exam Objective Map

Official Exam Objective	All-in-One Coverage	Chapter Numbers	Page Numbers
<b>1.0 Legal and Ethical Principles</b>			
1.1 Analyze the Nature of Evidence and Its Characteristics	1. What Is Computer Forensics? 1. Understanding the Field of Forensics 4. Identify and Classify Evidence	1, 4	3-5, 82
1.2 Analyze the Chain of Custody	1. Maintaining Chain of Custody 2. Chain of Custody	1, 2	23, 31-33
1.3 Analyze the Significance of Rules of Procedure	1. The Law and Cyber Forensics 1. General Legal Issues	1	23-26
1.4 Analyze the Role of Expert Witness	2. The Forensic Investigator as an Expert 13. Administrative Investigations	2, 13	46-51, 324
1.5 Apply Codes of Ethics	2. Code of Ethics 2. Ethical Conduct Outside the Investigation 2. Ethical Investigations	2	36-43
<b>2.0 Investigations</b>			
2.1 Analyze the Investigative Process	2. Examination	2	36
2.2 Analyze Evidence Management	2. The Evidence 3. Evidence Collection 3. Evidence Preservation 3. Evidence Transport 3. Evidence Tracking 3. Evidence Storage 5. Collecting the Evidence 5. Analyze the Evidence	2, 3, 5	43-46, 55-70, 105-106
2.3 Analyze Criminal Investigations	1. Elements of the Crime	1	5-6
2.4 Analyze Civil Investigations	2. Civil Investigations 13. Types of Investigations	2, 13	44, 323-325
2.5 Analyze Administrative Investigations	2. Administrative Investigations 13. Administrative Investigations	2, 13	
2.6 Analyze Forensic Response to Security Incidents	13. Disaster Recovery	13	328
2.7 Analyze Electronic Discovery	13. Electronic Discovery	13	322-325
2.8 Analyze Intellectual Property (IP) Investigation	2. Intellectual Property Investigations 13. Types of Investigations	2, 13	45-46, 323-325

Official Exam Objective	All-in-One Coverage	Chapter Numbers	Page Numbers
<b>3.0 Forensic Science</b>			
3.1 Analyze Fundamental Principles	2. Scientific Approach to Forensics 4. Scientific Approach to Forensics	2, 4	46-51, 77-81
3.2 Analyze Forensic Methods	4. Media File Forensic Steps 5. Planning	4, 5	99-102, 105-108
3.3 Evaluate Report Writing and Presentation	2. Documentation 5. Case Notes and Reports	2, 5	33-35, 108-114
3.4 Analyze Quality Assurance Control Management and Accreditation Procedures	5. Quality Control 5. Validation of Findings	5	106-107, 114-121
<b>4.0 Digital Forensics</b>			
4.1 Analyze Media and File System Forensics	1. Files and File Systems 6. Extracting Deleted Files	1, 6	11, 138-147
4.2 Analyze Computer and Operating System Forensics	6. Operating System Specifics	6	135-138
4.3 Analyze Network Forensics	8. Network Packet Analysis 8. Wireless 8. Router Forensics 8. Network Structure	8	183-204, 210-214
4.4 Apply Mobile Device Forensics	10. Cellular Device Concepts 10. What Evidence Can You Get From a Mobile Device? 10. Seizing Evidence From a Phone	10	233-260
4.5 Understand Embedded Device Forensics	10. Embedded Devices	10	260
4.6 Apply Virtual System Forensics	9. Types of Virtual Systems 9. The Cloud 9. Forensic Issues	9	217-229
4.7 Analyze Forensic Techniques and Tools	6. Windows Tools 9. Forensic Issues 10. Types of Acquisition	6, 9, 10	140-142, 225-229, 247-248
4.8 Understand Antiforensic Techniques and Tools	6. Encrypted Files 7. Cryptography 7. Steganography 7. Log Tampering 7. Other Methods	6, 7	148-150, 153-176, 179-181



<b>Official Exam Objective</b>	<b>All-in-One Coverage</b>	<b>Chapter Numbers</b>	<b>Page Numbers</b>
<b>5.0 Application Forensics</b>			
5.1 Apply Software Forensics	11. File Formats 11. Windows File Copying	11	265-277
5.2 Analyze Web, E-mail and Message Forensics	11. Web Forensics	11	277-281
5.3 Understand Database Forensics	11. Database Forensics	11	291-293
5.4 Understand Malware Forensics	12. Viruses 12. Trojan Horses 12. Spyware 12. Buffer Overflow 12. Rootkit 12. Logic Bomb 12. Ransomware 12. Advanced Persistent Threats 12. Malware Analysis	12	297-312
<b>6.0 Hybrid and Emerging Technologies</b>			
6.1 Understand Cloud Forensics	9. The Cloud	9	227
6.2 Understand Social Networks	8. Social Networks 13. Social Networks	8, 13	214-215, 315-321
6.3 Understand the Big Data Paradigm	13. Online Gaming	13	
6.4 Understand Control Systems	13. Control Systems and Infrastructure	13	321-322
6.5 Understand Critical Infrastructure	13. Control Systems and Infrastructure	13	321-322
6.6 Understand Online Gaming and Virtual/Augmented Reality	13. Online Gaming	13	312-322

---

# CONTENTS

	Acknowledgments .....	xi
	Introduction .....	xiii
<b>Part I</b>	<b>Legal and Ethical Principles .....</b>	<b>I</b>
<b>Chapter 1</b>	<b>Introduction to Forensics .....</b>	<b>3</b>
	What Is Cyber Forensics? .....	3
	Understanding the Science of Forensics .....	4
	Elements of the Crime .....	5
	Law .....	5
	Intent .....	5
	Burden of Proof .....	5
	Exculpatory Evidence .....	6
	Knowledge Base Needed for Cyber Forensics .....	6
	Hardware .....	6
	Operating Systems .....	9
	Networks .....	13
	The Fundamental Principles of Cyber Forensics .....	21
	Maintaining Chain of Custody .....	23
	The Law and Cyber Forensics .....	23
	General Legal Issues .....	24
	Discovery .....	24
	Warrants .....	25
	Federal Guidelines Forensics Investigators Need to Know .....	26
	FBI .....	26
	Secret Service .....	27
	The Need for Cyber Forensics Certification .....	27
	Chapter Review .....	29
	Questions .....	29
	Answers .....	30
	References .....	30
<b>Chapter 2</b>	<b>The Investigative Process .....</b>	<b>31</b>
	Chain of Custody .....	31
	Securing the Scene .....	33
	Documentation .....	33
	Authority and Objectives .....	35
	Examination .....	36

Code of Ethics	36
(ISC) <sup>2</sup> Ethics	37
American Academy of Forensic Science Ethics	37
ISO Code of Ethics	38
Ethical Conduct Outside the Investigation	40
Civil Matters	40
Criminal Matters	40
Other Issues	41
Ethical Investigations	41
The Chinese Wall	41
Relevant Regulations for Ethical Investigations	42
The Evidence	43
Criminal Investigations	43
Civil Investigations	44
Administrative Investigations	44
Intellectual Property Investigations	45
The Daubert Standard	46
The Forensic Investigator as an Expert	46
Qualities of an Expert	47
Chapter Review	51
Questions	51
Answers	53
References	53
<b>Chapter 3 Evidence Management</b>	<b>55</b>
Evidence Collection	55
Evidence Documentation	55
Evidence Preservation	57
Evidence Transport	64
Evidence Tracking	65
Evidence Storage	67
Environmental Hazards	67
Unauthorized Access	69
Electromagnetic Interference	69
U.S. Army Digital Evidence Storage	70
Evidence Access Control	71
Evidence Disposition	71
Chapter Review	71
Questions	72
Answers	73
References	73

<b>Part II</b>	<b>Forensic Science</b>	<b>75</b>
<b>Chapter 4</b>	<b>Principles and Methods</b>	<b>77</b>
	Scientific Approach to Forensics	77
	The Scientific Method	77
	The Philosophy of Science	78
	Peer Review	78
	Locard's Principle of Transference	79
	Inman-Rudin Paradigm	81
	Identify and Classify Evidence	82
	Locations Where Evidence May Reside	82
	Storage Media	83
	Hardware Interfaces	87
	File Systems	89
	File Format	90
	File Types	91
	Header Analysis	92
	Recovering Data	95
	Physical Damage	95
	Logical Damage	95
	File and Metadata Carving	96
	Known File Filtering	99
	Media File Forensic Steps	99
	Running Processes	100
	Netstat	101
	Chapter Review	102
	Questions	102
	Answers	103
	References	103
<b>Chapter 5</b>	<b>Forensic Analysis</b>	<b>105</b>
	Planning	105
	Collecting the Evidence	105
	Analyze the Evidence	106
	Case Notes and Reports	108
	Case Notes	108
	Reports	109
	Quality Control	114
	Lab Quality	114
	Investigator Quality Control	116
	Examination Quality Control	120
	Chapter Review	121
	Questions	121
	Answers	122
	References	123

<b>Part III</b>	<b>Digital Forensics</b>	<b>125</b>
<b>Chapter 6</b>	<b>Hardware Forensics</b>	<b>127</b>
	Hard Drive Specifications	127
	General Hard Drive Facts	127
	RAID	130
	Recovering from Damaged Media	132
	CMOS/BIOS	133
	The Swap File	134
	Operating System Specifics	135
	Operating System Essentials	135
	The Kernel	136
	The GUI	137
	Interrupts	137
	API	138
	Extracting Deleted Files	138
	Windows	138
	Windows Tools	140
	Scrubbing Files	144
	Linux	145
	Macintosh	147
	MacKeeper	147
	Encrypted Files	148
	EFS	148
	TrueCrypt	149
	How to Deal with Encrypted Drives and Files	150
	Chapter Review	151
	Questions	151
	Answers	152
	References	152
<b>Chapter 7</b>	<b>Hidden Files and Antiforensics</b>	<b>153</b>
	Cryptography	153
	The History of Encryption	154
	Modern Cryptography	157
	Symmetric Encryption	159
	Asymmetric Cryptography	163
	Cryptographic Hash	167
	Windows Passwords	169
	Steganography	170
	Historical Steganography	170
	Methods and Tools	171
	Steganalysis	175
	Cryptanalysis	176
	Frequency Analysis	177
	Kasiski	177
	Modern Methods	177

Log Tampering	179
Log Deletion	179
Auditpol	179
Winzapper	179
Other Techniques	179
Onion Routing	179
Spoofing	180
Wiping	181
Tunneling	181
Chapter Review	181
Questions	181
Answers	182
References	182
<b>Chapter 8 Network Forensics</b>	<b>183</b>
Network Packet Analysis	183
What Is a Packet?	183
Ports	186
Network Traffic Analysis	188
Log Files	190
Web Traffic	191
HTTP Sniffer	194
Web Traffic	194
Nmap	196
Snort	197
Wireless	198
Network-Related Cybercrimes	199
Router Forensics	200
Router Basics	200
Types of Router Attacks	202
Getting Evidence from the Router	202
Firewall Forensics	204
Firewall Basics	204
Logs to Examine	205
Windows Logs	205
Linux Logs	207
Operating System Utilities	207
Netstat	208
Net sessions	208
Openfiles	209
Network Structure	210
Types of Networks	210
Network Topology	210
Shares	213
Services	214
P2P Networks and Proxies	214
SANS	214

Social Networks	214
Chapter Review	215
Questions	215
Answers	216
References	216
<b>Chapter 9 Virtual Systems</b>	<b>217</b>
Types of Virtual Systems	217
Virtual Machines	217
Service-Based Systems	220
The Cloud	222
Forensic Issues	225
Technical Issues	225
VMware	226
VirtualBox	226
Virtual PC	227
Legal/Procedural Issues	227
Chapter Review	229
Questions	230
Answers	230
References	231
<b>Chapter 10 Mobile Forensics</b>	<b>233</b>
Cellular Device Concepts	233
The Basics	234
Networks	236
Operating Systems	237
Apps	243
What Evidence Can You Get from a Mobile Device?	243
Cell Phone Records	243
Photos and Videos	243
GPS Records	244
Evidence from Apps	244
What You Should Look For	245
Device Status	246
Seizing Evidence from a Phone	246
Imaging a Phone	247
Windows 8 Phone	257
The iPhone	257
Android Forensics	259
Embedded Devices	260
Summary	260
Questions	261
Answers	261
References	262

<b>Part IV Application Forensics and Emerging Technologies</b> .....	<b>263</b>
<b>Chapter 11 Application Forensics</b> .....	<b>265</b>
File Formats .....	265
The Registry .....	265
Windows Swap File .....	272
Index.dat .....	272
Other Files That Provide Evidence .....	273
Memory Analysis .....	274
Windows File Copying .....	276
Web Forensics .....	277
Basics of Web Applications .....	277
SQL Injection .....	277
Cross-Site Scripting .....	279
Cookie Manipulation .....	280
Forceful Browsing .....	281
XML Injection .....	281
E-mail Forensics .....	281
How E-mail Works .....	282
E-mail headers .....	283
E-mail Files .....	289
Tracing E-mail .....	290
E-mail Server Forensics .....	290
Database Forensics .....	291
Database Types .....	291
What to Look For .....	292
Record Carving and Database Reconstruction .....	293
Chapter Review .....	293
Questions .....	294
Answers .....	295
References .....	295
<b>Chapter 12 Malware Forensics</b> .....	<b>297</b>
Viruses .....	297
How a Virus Spreads .....	297
Real-World Cases .....	298
Types of Viruses .....	301
History of Viruses .....	302
Modern Virus Creation .....	304
Trojan Horses .....	305
Spyware .....	306
The Buffer Overflow .....	307
Rootkit .....	307
Logic Bombs .....	308
Ransomware .....	308



	Advanced Persistent Threats .....	309
	Malware Analysis .....	310
	Static Analysis .....	310
	Dynamic Analysis .....	310
	Chapter Review .....	312
	Questions .....	313
	Answers .....	313
	References .....	314
<b>Chapter 13</b>	<b>New and Emerging Forensics Technology .....</b>	<b>315</b>
	Social Networks .....	315
	Types and Applications of Social Networks .....	315
	Direct Evidence of Crimes .....	317
	Commission of Crimes .....	318
	New Devices .....	320
	Google Glass .....	320
	Cars .....	320
	Medical Devices .....	321
	Control Systems and Infrastructure .....	321
	Online Gaming .....	321
	Electronic Discovery .....	322
	Types of Investigation .....	323
	Liability and Proof .....	325
	Relevant Laws .....	325
	Big Data .....	327
	Steps in Electronic Data Discover .....	328
	Disaster Recovery .....	328
	Chapter Review .....	328
	Questions .....	329
	Answers .....	330
	References .....	330
<b>Appendix</b>	<b>About the CD-ROM .....</b>	<b>331</b>
	System Requirements .....	331
	Total Tester Premium Practice Exam Software .....	331
	Installing and Running Total Tester	
	Premium Practice Exam Software .....	331
	PDF Copy of the Book .....	332
	Technical Support .....	332
	Total Seminars Technical Support .....	332
	McGraw-Hill Education Content Support .....	332
	Glossary .....	333
	Index .....	337