“All▪in▪One Is All You Need.”

ALL▪IN▪ONE

CCFP℠

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℠ Certified Cyber Forensics Professional Certification

Exam Guide

Chuck Easttom

McGraw Hill Education

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)²® and is not affiliated with (ISC)² in any manner. This publication and CD-ROM are not sponsored by, endorsed by, or affiliated with (ISC)² 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)² 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)² 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.

CCFP^{SM} Certified Cyber Forensics Professional Certification All-in-One Exam Guide

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.

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 $(ISC)^2$, 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)^2, 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)^2 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)^2. 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)^2 Code of Ethics (discussed in Chapter 2 of this book). Your application must then be endorsed by a current (ISC)^2 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/. This website will be updated from time to time and expanded as needed. You can also visit my personal website: 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
1.0 Legal and Ethical Principles			
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
2.0 Investigations			
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
3.0 Forensic Science			
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
4.0 Digital Forensics			
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

Official Exam Objective	All-in-One Coverage	Chapter Numbers	Page Numbers
5.0 Application Forensics			
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
6.0 Hybrid and Emerging Technologies			
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