Introduction

As an auditor as well as researcher and author, I realize and value the importance of timely, well–focused, accurate information. It is with this philosophy in mind that the development of this project was undertaken.

To the reader, a note of explanation…. This is not a text, but rather a field manual. It has been written — better yet, compiled — and edited in a manner that will allow you to rapidly access a specific area of interest or concern and not be forced to sequentially wade through an entire text, chapter by chapter, to get to what is important to you.

In the true sense of a field manual, each "chapter" (and we use that term loosely) stands on its own and presents focused, timely information on a specific topic related to cyber forensics. The author of each "chapter" was selected for his or her expertise in a specific area within the very broad field of cyber forensics.

Often a limiting aspect of most projects, especially those written on emerging technical topics, is the inability to cover every aspect of the topic in a single all–inclusive text. This truth befalls this field manual that you are about to use.

Initial research into this growing discipline proved that it would be next to impossible to include all the areas of both interest and importance in the field of cyber forensics that would be needed and required by all potential readers and users in a single text. Thus, this field manual presents specific and selected topics in the discipline of cyber forensics, and addresses critical issues facing the reader who is engaged in or who soon will be (and you will!) engaged in the preservation, identification, extraction, and documentation of computer evidence.

As a user of this field manual, you will see that this manual's strength lies with the inclusion of an exhaustive set of chapters covering a broad variety of forensic subjects. Each chapter was thoroughly investigated; examined for accuracy, completeness, and appropriateness to the study of cyber forensics; reviewed by peers; and then compiled in a comprehensive, concise format to present critical topics of interest to professionals working in the growing field of cyber forensics.

We finally had to select several key areas and put pen to paper, entice several colleagues to share their ideas, and resign ourselves to the fact that we cannot say all that needs to be said in one text, book, or manual. We trust the material we have included will serve as a starting point for the many professionals who are beginning their journey into this exciting discipline.

We begin our journey into the realm of this relatively new discipline by opening with a brief discussion as to the current state of the environment relating to the need for this new field of forensics and then a brief examination of the origins of cyber forensics. Along the way, we will establish several basic definitions designed to assist the reader in moving easily through what could be difficult and confusing terrain.

> Although e–mail is becoming more mission–critical for enterprises, it also has the ability to haunt a company in times of trouble, because records of e–mail messages remain in the company systems after deletion — a feature highlighted during the Microsoft anti–trust trial. The case has featured critical testimony derived from old Microsoft e–mail messages.
>
> —*InfoWorld*, 10/25/99