Foreword

Computer forensics is a relatively new field, and over the years it has been called many things: "computer forensics," "digital forensics," and "media analysis" to name a few. It has only been in the past few years that we have begun to recognize that all of our digital devices leave digital breadcrumbs and that these breadcrumbs are valuable evidence in a wide range of inquiries. While criminal justice professionals were some of the first to take an interest in this digital evidence, the intelligence, information security, and civil law fields have enthusiastically adopted this new source of information.

Digital forensics has joined the mainstream. In 2003, the American Society of Crime Laboratory Directors–Laboratory Accreditation Board (ASCLD–LAB) recognized digital evidence as a full-fledged forensic discipline. Along with this acceptance came increased interest in training and education in this field. The Computer Forensic Educator's Working Group (now known as the Digital Forensic Working Group) was formed to assist educators in developing programs in this field. There are now over three-dozen colleges and universities that have, or are, developing programs in this field. More join their ranks each month.

I have had the pleasure of working with many law enforcement agencies, training organizations, colleges, and universities to develop digital forensic programs. One of the first questions that I am asked is if I can recommend a good textbook for their course or courses. There have been many books written about this field. Most take a targeted approach to a particular investigative approach, such as incident response or criminal investigation. Some tend to be how-to manuals for specific tools. It has been hard to find a book that provides a solid technical and process foundation for the field…That is, until now.

This book is the foundational book for file system analysis. It is thorough, complete, and well organized. *Brian Carrier has done what needed to be done for this field*. This book provides a solid understanding of both the structures that make up different file systems and how these structures work. Carrier has written this book in such a way that the readers can use what they know about one file system to learn another. This book will be invaluable as a textbook and as a reference and needs to be on the shelf of every digital forensic practitioner and educator. It will also provide accessible reading for those who want to understand subjects such as data recovery.

When I was first approached about writing this Foreword, I was excited! I have known Brian Carrier for a number of years and I have always been impressed with his wonderful balance of incredible technical expertise and his ability to clearly explain not just what he knows but, more importantly, what you need to know. Brian's work on Autopsy and The Sleuth Kit (TSK) has demonstrated his command of this field—his name is a household name in the digital forensic community. I have been privileged to work with Brian in his current role at Purdue University, and he is helping to do for the academic community what he did for the commercial sector: He set a high standard.

So, it is without reservation that I recommend this book to you. It will provide you with a solid foundation in digital media.

Mark M. Pollitt
President, Digital Evidence Professional Services, Inc.
Retired Director of the FBI's Regional Computer Forensic Laboratory Program