The digital crime phenomenon has achieved what I tend to call the “overwhelming” factor. A few years ago, incidents of this kind were few and almost entirely the works of computer and telecommunications aficionados that individually, or as members of groups, came to define what we now identify as the underground hacker (or cracker, depending on your point of view) culture. If such acts were carried out as is often claimed to prove and not to harm, today it is worrying to observe that increasingly the criminals of the digital age are driven by rather sinister motives and the numbers of incidents has increased with the publicity to match. Firstly, because even the “innocent” computer science student at a University lab starts to think differently if he knows that he can do what he pleases and go undetected especially if the rewards are high. Secondly, because digital crime acts are increasingly the collective and well-planned actions of organized crime syndicates and organizations.

Either as individuals or as organizations in the digital society we must understand what breaking the law electronically really means. Of course, what constitutes digital evidence in order to prosecute is controversial. The urgency of this is well-understood and it is becoming harder to simply ignore. Consider for example the findings of the Digital Risk survey which was carried out by the Economist Intelligence Unit (EIU) of 218 senior risk managers. Fifty five percent said that the biggest challenge their companies face in tackling IT risks is the growing sophistication of hackers and cyber criminals. Forty eight percent said IT and security problems pose a high risk to their business operations.

This book is important as it help us to understand the nature of cyber crime and as it familiarizes us with the various means by which crime can be detected and evidence collected. It provides a holistic coverage of the topic, i.e., offering technical as well as
managerial perspectives and it goes a step further pinpointing issues pertinent to the education and skills that the cyber investigator must possess and of the various challenges that we face in training the professionals of the future. In essence it educates and informs the interested readers about what it really means to be ready to confront. Solved digital crime cases will in the future read as good Sherlockian adventures. However, digital crime is not fiction, and this book is unique in exploring its multifaceted nature and defining the plateau where the battles between the good and bad guys are taking place. I hope you enjoy reading it as much as I did.

*Kyriakos Tsiflakos*
Partner, ERNST & YOUNG
Technology and Security Risk Services