Preface

It is a capital mistake to theorize before one has data. Insensibly, one begins to twist facts to suit theories, instead of theories to suit facts.

Sherlock Holmes
Sir Arthur Conan Doyle's "A Scandal in Bohemia", 1891

Cain committed the first crime in the world and the history of crime is as old as the world itself. Forensics—the process, means, and methods for collecting crime evidence—can be said to date back to the 18th century stemming from forensic medicine and studies of anatomy and fingerprints. Crime manifests itself in various ways and forms and digital crime is the newest one. As the essence of the various forms of crime has remained unaltered throughout the passage of time, it is safe to assume that digital crime will exhibit this property too and it is this "permanence" factor that makes imperative for organizations and individuals to understand the issues and complexities that arise.

In 2003, 82% of American companies surveyed by the Computer Security Institute, faced security problems and dealt with damages that were estimated at $27.3 million. And even though organizations already spend considerable amounts of money on safeguarding their information assets, according to surveys published by monitoring organizations such as the Computer Crime Research Centre in the U.S. (March 2004) there will be an increase in the information security market because of cyber criminality growth.

The *Organization for Economic Co-operation and Development* (OECD) defines "computer crime" as "any illegal, unethical, or unauthorized behavior relating to the automatic processing and the transmission of data". A common categorization of computer crime is by dividing it to computer crimes and computer related crimes (Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, 2002). Computer crimes encompass all offences against the confidentiality, integrity and availability of computer data and systems such as illegal access to computer systems or mali-

cious code writing. Computer-related crimes are "traditional crimes that can be, or have been, committed utilizing other means of perpetration which are now being, or are capable of being, executed via the Internet, computer-related venue (e-mail, newsgroups, internal networks) or other technological computing advancement. Examples are intellectual property rights infringement (e.g., software piracy) and payment system frauds (e.g., credit card fraud via the Internet).

The multiplicity of computer fraud incidents translates to the urgency for developing and maintaining a digital forensics capability as part of a holistic risk management framework. This urgency is projected through the directives and various announcements by a plethora of standards bodies and financial corporations. For example, the Basel Committee on Banking Supervision recommends in the 14th principle for risk management: "... banks should develop… a process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents as well as to assist in the prosecution of attackers… ."

At the *Digital Forensic Research Workshop* (DFRWS) in 2001, digital forensic science was defined as "…the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." This volume is a collection of contributions that present the state of the art of many facets of digital forensics delving deep into the technical realm but also covering issues that reach beyond it as this process involves many stakeholders such as criminal prosecutors, law enforcement officials, IT managers, security administrators, internal and external auditors, government and private organizations, and others.

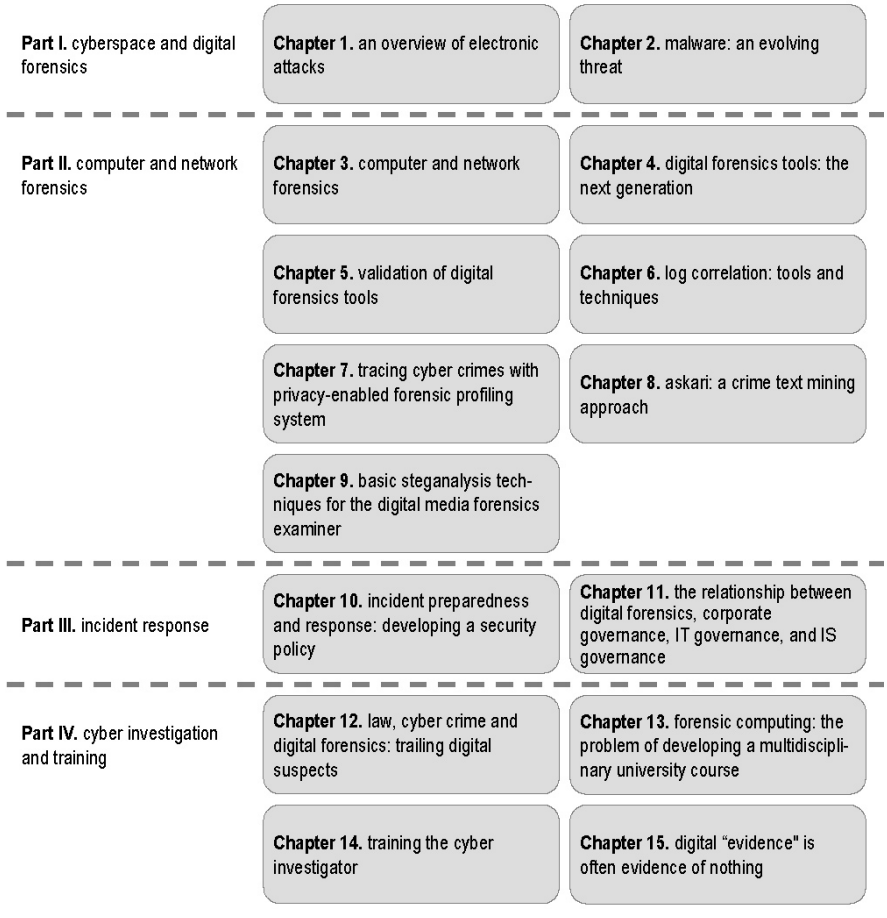
To this end, the book is subdivided into four sections (also depicted in Figure 1) covering to a large extent most aspects of digital forensics science.

Section I

In the first chapter of this section, Chen and Davis draw attention to a fundamental truth that underlines the phenomenon of digital crime; it is the ease of carrying out electronic attacks that adds to the temptation for attackers. Thus, an understanding of attackers and the methods they employ is a prerequisite to digital forensics. Although the authors acknowledge the fact that the range of possible attacks is almost unlimited, they provide an interesting taxonomy of attacks and proceed in providing an extensive overview of the major types encountered today and likely to continue into the foreseeable future. This chapter succeeds in providing the necessary background for a number of other chapters in this book that cover technical aspects of digital forensics in depth and in serving as a reminder that the increasing sophistication of attacks implies that digital forensics will have proportionately greater importance in investigating, diagnosing, and analyzing cyber crimes.

In turn, Furnell and Ward take the subject of electronic attacks a step further and focus on malware which, in the two decades since its first significant appearance, has become

Figure 1. Organization of the book



the most prominent and costly threat to modern IT systems. The essence of the chapter and consequently their contribution to this volume lies in the comprehensive coverage of the evolution of this particular type. The authors highlight that, as well as the more obvious development of propagation techniques; the nature of payload activities (and the related motivations of the malware creators) is also significantly changing, as is the ability of the malware to defeat defenses. This is certainly a moving target, but by tracing its history, a deeper understanding of its various manifestations can be gained and the inquisitive reader can draw similarities as well as differences with other types of electronic attacks. Engaged in this process, one has made the necessary first steps in order to untangle this complex ecosystem. On a hopeful note, and for malware in particular, the authors conclude that the risk and resultant impacts can be substantially mitigated by appropriate use of carefully planned and implemented safeguards.

Section II

As the phenomenon of crimes being committed using digital means is relatively new, and is expected to grow in the foreseeable future, Sitaraman and Venkatesan introduce aspects falling under the umbrella of computer and network forensics in the first chapter of this part. Roughly speaking, computer forensics deals with preserving and collecting digital evidence on a single machine whilst network forensics deals with such operations in a connected digital world. A number of sophisticated tools have been developed for forensic analysis of computers and networks and this chapter presents an overview of the most prominent ones. Following a critical analysis, it becomes apparent that most of the tools presented are suffering from limitations and only few have been validated for providing evidence that can be used in court.

As the technology pace is increasing sharply, current limitations of tools used by forensics investigators will eventually become obstacles in performing investigations in an efficient and reliable way. This has motivated Richard and Roussev to deal with the problem of identifying requirements that next generation of digital forensics tools should meet. The authors introduce the notions of *machine* and *human scalability* as two perspectives of the same problem, and present various approaches to address it. By taking into account the needs of digital forensics community, it is recommended the next generation of the digital forensics tools to employ high performance computing, more sophisticated evidence discovery and analysis techniques, as well as better collaborative functions.

The chapter written by Craiger, Swauger, Marberry, and Hendricks, takes the subject one step further, focusing on the validation of digital forensics tools. As noted by the authors, this should be an indispensable part of the software design and development process for tools being used in digital forensics; otherwise the results of cyber investigations cannot be introduced in courts. Contrary to typical software tool validation frameworks, special requirements are imposed if these are to be applied in the digital forensics context, most notably the lack of capability to conduct extensive validation due to time constraints. Important concepts and well-known methodologies currently used in forensic tool validation, along with the alternative *just-in-time tool validation* method, are described in detail.

In the sequel, the subject of this part is specialized by Forte in the study of tools and techniques widely used in log file correlation, presented from the perspective of digital forensics. The increasing number of information systems being connected over the network makes the difficulty of the cyber investigative process extremely high and necessitates the development of new more complex digital forensics investigative procedures. Log file correlation is comprised of two components, namely intrusion detection and network forensics. The author deals with the general requirements log files and associated tools should meet, and additional requirements imposed by the digital forensics community. Experimentations and results obtained from a research project are also presented leading to conclusions about the applicability of current practices in distributed architectures.

The chapter written by Kahai, Namuduri, and Pendse also treats the subject of network forensics focusing on intrusion detection and issues of tracing cyber crimes. Most

organizations employ intrusion detection systems and other security measures to protect their network without enabling mechanisms in order to collect evidence and identify the attackers. This is attributed to the lack of tools and techniques for identification and IP trace back, as well as, to the inherent complexity of doing so in a universal cyber space. Motivated by this fact, the authors propose a forensic profiling system monitoring any anomalous activity in the network and accommodating real-time evidence collection. The proposed system is designed such that communication behavior of only suspicious sources is investigated, thus protecting the privacy of lawful users. It is argued that such a system may drastically reduce the time spent to filter system log files during forensic investigations.

The advancement of communication technologies has facilitated forms of organized crime, leading to a significant increase of concern about national security. Hence, the amounts of data that need to be analyzed by criminal investigators are in many cases prohibitively large. The identification of patterns revealing criminal behavior in large data sets is also considered by Chibelushi, Sharp, and Shah. Because such data sets contain large amount of information stored in textual and unstructured form, data mining, and in particular text mining, are two key technologies well suited to the discovery of underlying patterns. The authors review the use of these techniques in crime detection projects and describe in detail the text mining approach followed in ASKARI project. They propose an approach combining agent technology with text mining techniques to dynamically extract criminal activity patterns and discover associations between criminal activities across multiple sources. Limitations of proposed methodology are identified and directions for future research are also given.

The chapter by Agaian and Rodriguez focuses on the development of digital forensic steganalysis tools and methods by analyzing and evaluating the techniques most widely used. These techniques are mainly applied by digital forensics examiners to analyze, identify, and interpret concealed digital evidence (information appropriately embedded within multimedia objects with practically no visible effect). Many advanced open source steganography utilities are authored and distributed over the Internet and there are indications that cyber criminals may be using these freely available tools to hide communications in order to avoid drawing the attention of law enforcement agencies. As concluded in the DFRWS 2001, there are indications that cyber criminals may be using these freely available tools to hide communications in order to avoid drawing the attention of law enforcement agencies. To this end, it is of great importance to find means to effectively detect, estimate the length, extract, and trace the hidden information in all its forms; all such issues are presented by the authors in a simple and comprehensible manner. The results yielded have considerably improved currently achieved rates of detecting hidden information by existing algorithms, even in the presence of added noise, and this is validated by the extensive simulations performed.

Section III

No one can argue that the consequences following the aftermath of an attack that compromises the security of the information and telecommunications infrastructure are anything less than devastating. Of course impact and severity levels vary but the more organizations depend on information technologies even minor attacks will cause major disturbances. Some of the costs can be counted in dollars and severe financial loss emanating from loss of business. Others, such as poor public relations and lost customer confidence, cannot be directly measured but are of equal or greater importance. Incident preparedness and response that is part of a corporate security strategy is becoming increasingly important for organizations that must develop and demonstrate the required set of related competencies. Wylupski, Champion, and Grant examine the preparedness level and responses of three U.S. southwestern companies to their own specific threats to corporate cyber-security. They do so in sufficient detail and they paint a picture, which as reality itself, is a rather complex one. It becomes obvious by putting all the pieces together that effective intrusion preparedness and response relies on a combination of policies and processes, organizational commitment, and employee accountability. The authors place a heavy emphasis on the practical side of things by laying out the basic blocks one needs to define an effective security policy for corporate networks as well as provide a glimpse on emerging technologies that can be used as the means for implementing it. They do so without undermining and loosing sight of the role and importance of the human element that more often than not proves to be the weak link of even the most concrete security policies.

According to OECD, *"*Corporate Governance*"* is the framework by which business corporations are directed and controlled. Technology and systems are central to this framework pumping the information that without it no "directing" or "controlling" would be possible. In the 2½ years since the passage of the Sarbanes-Oxley Act in July 2003 both private and public organizations worldwide found themselves looking at the mirror with respect to the security and integrity of their information assets. So in the midst of it all there is also IT governance and information security governance. But where does Digital Forensics fit in the picture? von Solms and Louwrens argue that for any company that wants to create an effective Digital Forensics environment, it seems prudent to know precisely what the relationships between Digital Forensics, Information Security, IT Governance and Corporate Governance are. The reason being that if a Digital Forensics environment is created, and any of the relationships mentioned above are ignored, it may result in an environment that will not operate optimally. This has obvious implications for incident preparedness and response and how we are thinking and approaching it. The authors proceed in determining and defining these interrelationships. They investigate the overlaps and they provide detailed analyses of their content. Their conclusions help us to clarify the place and importance of digital forensics in relation to governance; a relation that organizations need to understand, nurture and manage.

Section IV

Many could argue that crime and punishment in the real world (as opposed to the digital and virtual one) is not that complicated an affair. At least if one makes the assumption that the mediators, in other words, the courts of justice abide by the rules as set in the books of law. Evidence is evidence and for each known crime there is the law that defines it as such. In the digital worlds we are not sure what constitutes evidence and each new day brings a new crime. To enhance the conditions under which cyber crime can be investigated, certain technical and organizational measures are necessary in an effort to detail further and support the legal framework. Mitrakas and Zaitch start their chapter with an overview of digital forensics from a criminology viewpoint prior to reviewing some pertinent legal aspects. Pursuant to the criminological typology of cyber crime, some definitions and specific features of cyber crime, this chapter reviews certain legal aspects of forensic investigation, the overall legal framework in the EU and US and additional self-regulatory measures that can be leveraged upon to investigate cyber crime in forensic investigations. The authors claim that while full-scale harmonization of forensic investigation processes across the EU and beyond is unlikely to happen in the foreseeable future, cross-border investigations can be greatly facilitated by initiatives aiming at mutual assistance arrangements based on a common understanding of threats and shared processes. They add that the involvement of users through self-regulation and accountability frameworks might also contribute to reducing risks in electronic communications that emanate from cyber criminal threats. In summary, the authors demonstrate how forensic readiness that complements the security set-up of an organization can improve security posture and provide coverage from cyber crime.

To be called a "science" or even a "discipline" one must have a distinct subject matter and some means of describing and classifying its subject matter. If we take practice aside for a moment, how well-defined as a field of study is digital Forensics? Is this a fully-fledged one or is it just emerging? These are interesting questions and one needs to dig deep into the nature and the core of the discipline, trace its roots, examine epistemological and ontological questions and perhaps draw parallels with other disciplines in order to reach a conclusion. Some answers to the above are given (directly or indirectly) from Stahl, Carroll-Mayer, and Norris by setting out to design a full undergraduate BS degree in forensic computing at a British University. Their experience is valuable as they bring out the issues and challenges for deciding what the knowledge base of a digital forensics professional should be. The authors emphasize the problem of interdisciplinary agreement on necessary content and the importance of the different aspects. Their contribution is important because its is bound to stir and simulate debate; something which as they point out will help us come to an agreement what the skills requirement for digital forensics professionals should be.

If the training issue was set in an academic context in the preceding chapter, Malinowski looks at it from a practitioner's perspective drawing on from his experience after being with the New York Police Department for over 20 years. Training possibilities for digital forensic investigators are presented, differentiating between civil service and industry needs for training, whereas any differences in considerations for providing such train-

ing are cited as well. While each organization has its own requirements, different paradigms and forums for training are offered. The chapter's added value is that it allows the reader to develop training plans that may be unique to his/her organization. This is achieved by providing solid foundations; those common subject matter areas that are felt critical to all organizations and needs, as well as, a "core" knowledge and skill base around that one needs in order to plan a training strategy.

The last chapter could have fitted well into any section of the book. Indeed, it could have been an integral part of this introduction. We decided to place it at the end of the volume, and in its own way this short chapter by Caloyannides provides a fitting epilogue. If we take for granted that it is impossible for more than one person to have the same fingerprints, then evidence is evidence. The author makes an argument that "Digital evidence is often evidence of nothing". The points that the author raises demand to be considered. In our opinion and regarding digital forensics in general, we would all be a little bit wiser after doing so.

Intended Audience

Generally, the book is intended for those who are interested in a critical overview of what forensic science is, care about privacy issues, and wish to know what constitutes evidence for computer crime. However, special attention has been given so that the book is would be of great value to the following target groups:

- *Academics* in the fields of computer science, software engineering, and information systems that need a source of reference covering the state of research in digital forensics.

The book has been designed so as to provide the basic reading material that could potentially serve as the backbone of an advanced course on cyber crime and digital forensics, covering current trends in cyber crime, tools used in computer and network forensics, technologies and interdisciplinary issues encountered, as well as, legal aspects of digital forensics. Hence, it is envisaged the book will be of assistance in identifying and further establishing research priorities in this area.

- *Security professionals*, as well as, internal and external auditors that must be aware of all aspects governing computer and network forensics.

Towards this direction, an overview of network attacks (including malware) launched to modern IT systems today is given, indicating most commonly used approaches followed by attackers. Further, the book also provides a detailed analysis of a wide variety of tools, both commercial and open source, commonly used to protect organizations from such attacks and also employed in all phases of digital forensics process.

Pros and cons of these tools are derived in a systematic manner and current trends are brought to the attention of the professional in order to assist him develop an effective security policy and informatively choose the proper action plan.

- *Information technology managers* that must have the necessary know-how in order to handle an investigation and deal with cyber-investigators.

All aspects (organizational, technical, legal) of the investigation and the evidence collection processes are carefully examined. The book reviews the current legal framework in the EU and U.S. that can be leveraged upon to investigate cyber crime in forensic investigations, and deals with the important issue of what constitutes digital evidence what does not. Furthermore, different paradigms for training cyber-investigators are considered and the core knowledge and skills that need to be developed are clearly identified.

Panagiotis Kanellis
Evangelos Kiountouzis
Nicholas Kolokotronis
Drakoulis Martakos