1. Record Nr. UNINA9910158881603321

Autore	Roussev Vassil
Titolo	Digital forensic science : issues, methods, and challenges / / Vassil Roussev, University of New Orleans
Pubbl/distr/stampa	[San Rafael, California] : , : Morgan & Claypool Publishers, , 2017 ©2017
ISBN	1-62705-465-0
Descrizione fisica	1 online resource (157 pages) : illustrations
Collana	Synthesis Lectures on Information Security, Privacy, and Trust, , 1945-9750 ; ; Number 19
Disciplina	363.25968
Soggetti	Computer crimes - Investigation Data recovery (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Part of: Synthesis digital library of engineering and computer science.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	1. Introduction -- 1.1 Scope of this book -- 1.2 Organization -- 2. Brief history -- 2.1 Early years (1984-1996) -- 2.2 Golden age (1997-2007) -- 2.3 Present (2007-) -- 2.4 Summary -- 3. Definitions and models -- 3.1 The Daubert standard -- 3.2 Digital forensic science definitions -- 3.2.1 Law-centric definitions -- 3.2.2 Working technical definition -- 3.3 Models of forensic analysis -- 3.3.1 Differential analysis -- 3.3.2 Computer history model -- 3.3.3 Cognitive task model -- 4. System analysis -- 4.1 Storage forensics -- 4.1.1 Data abstraction layers -- 4.1.2 Data acquisition -- 4.1.3 Forensic image formats -- 4.1.4 Filesystem analysis -- 4.1.5 Case study: FAT32 -- 4.1.6 Case study: NTFS -- 4.1.7 Data recovery and file content carving -- 4.1.8 File fragment classification -- 4.2 Main memory forensics -- 4.2.1 Memory acquisition -- 4.2.2 Memory image analysis -- 4.3 Network forensics -- 4.4 Real-time processing and triage -- 4.4.1 Real-time computing -- 4.4.2 Forensic computing with deadlines -- 4.4.3 Triage -- 4.5 Application forensics -- 4.5.1 Web browser -- 4.5.2 Cloud drives -- 4.6 Cloud forensics -- 4.6.1 Cloud basics -- 4.6.2 The cloud forensics landscape -- 4.6.3 IaaS forensics -- 4.6.4 SaaS forensics -- 5. Artifact analysis -- 5.1 Finding known objects: cryptographic hashing -- 5.2 Block-level analysis -- 5.3 Efficient hash representation:

Bloom filters -- 5.4 Approximate matching -- 5.4.1 Content-defined data chunks -- 5.4.2 Ssdeep -- 5.4.3 Sdhash -- 5.4.4 Evaluation -- 5.5 Cloud-native artifacts --
6. Open issues and challenges -- 6.1 Scalability -- 6.2 Visualization and collaboration -- 6.3 Automation and intelligence -- 6.4 Pervasive encryption -- 6.5 Cloud computing -- 6.5.1 From SaaP to SaaS -- 6.5.2 Separating cloud services from their implementation -- 6.5.3 Research challenges -- 6.6 Internet of things (IoT) -- Bibliography -- Author's biography.

Sommario/riassunto

Digital forensic science, or digital forensics, is the application of scientific tools and methods to identify, collect, and analyze digital (data) artifacts in support of legal proceedings. From a more technical perspective, it is the process of reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system or (digital) artifacts. Over the last three decades, the importance of digital evidence has grown in lockstep with the fast societal adoption of information technology, which has resulted in the continuous accumulation of data at an exponential rate. Simultaneously, there has been a rapid growth in network connectivity and the complexity of IT systems, leading to more complex behavior that needs to be investigated. The goal of this book is to provide a systematic technical overview of digital forensic techniques, primarily from the point of view of computer science. This allows us to put the field in the broader perspective of a host of related areas and gain better insight into the computational challenges facing forensics, as well as draw inspiration for addressing them. This is needed as some of the challenges faced by digital forensics, such as cloud computing, require qualitatively different approaches; the sheer volume of data to be examined also requires new means of processing it.