[Book] Digital Forensics Elsevier

Thank you for reading this document. Digital Forensics Elsevier is a comprehensive guide on digital forensics, providing insights into the methodologies, tools, and techniques used in the field. The book is designed for both practitioners and students, offering a detailed overview of the current state of digital forensics. It covers the selection of qualified experts, the process of retrieving evidence, and the legal aspects involved. The text is written in clear language, making it accessible to non-technical individuals. It also includes numerous illustrations and examples to aid in understanding complex concepts. Whether you are a beginner or an experienced professional, Digital Forensics Elsevier is an invaluable resource for anyone working in the field of digital forensics.
Digital Forensics Processing and Procedures—David Lilburn Watson 2013-08-30 This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody—from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications

Implementing Digital Forensic Readiness—Jason Sachowski 2019-06-07 Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and reducing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stances, a company’s preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

Strategic Leadership in Digital Evidence—Paul Reedy 2020-10-08 Strategic Leadership in Digital Evidence: What Executives Need to Know provides leaders with broad knowledge and understanding of practical concepts in digital evidence, along with its impact on investigations. The book’s chapters cover the differentiation of related fields, new market technologies, operating systems, social networking, and much more. This guide is written at the layperson level, although the audience is expected to have reached a level of achievement and seniority in their profession, principially law enforcement, social networking and intelligence. Additionally, this book will appeal to legal professionals and others in the broader justice system. Covers a broad range of challenges confronting investigators in the digital environment Addresses gaps in currently available resources and the future focus of a fast-moving field Written by a manager who has been a leader in the field of digital forensics for decades

Google Earth Forensics—Michael Harrington 2014-12-09 Google Earth Forensics is the first book to explain how to use Google Earth in digital forensic investigations. This book teaches you how to leverage Google’s free tool to craft compelling location-based evidence for use in investigations and in the courtroom. It shows how to extract location-based data that can be used to display evidence in compelling audiovisual manners that explain and inform the data in contextual, meaningful, and easy-to-understand ways. As mobile computing devices become more and more prevalent and powerful, they are becoming more and more useful in the field of law enforcement investigations. With the wide use of mobile devices comes more potential for helping solve crimes than those with geo-location tools. Written for investigators and forensic practitioners, Google Earth Forensics is written by an investigator and trainer with more than 13 years of experience in law enforcement who will show you how to use this valuable tool anywhere at the crime scene, in the lab, or in the courtroom. Learn how to extract location-based evidence using the Google Earth program or app on computers and mobile devices Covers the basics of GPS systems, the usage of Google Earth, and helps sort through data imported from external evidence sources Includes tips on presenting evidence in compelling, easy-to-understand formats

Cloud Storage Forensics—Darren Quick 2013-11-16 To reduce the risk of digital forensic evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting digital forensic investigations and examinations. Digital forensic investigation in the cloud computing environment, however, is in infancy due to the comparatively recent prevalence of cloud computing. Cloud Storage Forensics presents the first evidence-based cloud forensic framework. Using three popular cloud storage services and one private cloud storage service as case studies, the authors show you how their framework can be used to undertake research into the data remnants on both cloud storage servers and client devices when a user undertakes a variety of methods to store, upload, and access data in the cloud. By determining the data remnants on client devices, you gain a better understanding of the types of terrestrial artifacts that are likely to remain at the Identification stage of an investigation. Once it is determined that a cloud storage service account has potential evidence of relevance to an investigation, you can communicate this to legal liaison points within service providers to enable them to respond and secure evidence in a timely manner. Learn to use the methodology and tools from the first evidenced-based cloud forensic framework Case studies provide detailed tools for analysis of cloud storage devices using popular cloud storage services Includes coverage of the legal implications of cloud storage forensic investigations Discussion of the future evolution of cloud storage and its impact on digital forensics

Android Forensics—Andrew Hoog 2011 The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics covers an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply standards to use Android devices. The book details how digital forensic procedures can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and reducing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stances, a company’s preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

Contemporary Digital Forensic Investigations of Cloud and Mobile Applications—Kim-Kwang Raymond Choo 2016-10-12 Contemporary Digital Forensic Investigations of Cloud and Mobile Applications comprehensively discusses the implications of cloud (storage) services and mobile applications on digital forensic investigations. The book provides both digital forensic practitioners and researchers with an up-to-date and advanced knowledge of collecting and preserving electronic evidence from different types of cloud services, such as digital remnants of cloud applications accessed through mobile devices. This is the first book that covers the investigation of a wide range of cloud services. Dr. Kim-Kwang Raymond Choo and Dr. Ali Dehghantanha are leading researchers in cloud and mobile security and forensics, having organized research, led research, and been published widely in the field. Users will gain a deep overview of seminal research in the field while also identifying prospective future research topics and open challenges. Presents the most current, leading edge research on cloud and mobile applications in the field Introduces the first book to provide an in-depth overview of the issues surrounding digital forensic investigations in cloud and associated mobile apps Covers key technical topics and provides readers with a complete understanding of the most current research findings Includes discussions on future research directions and challenges

Malware Detection—Mihai Christodorescu 2007-03-06 This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Digital Triage Forensics—Stephen Pearson 2010-07-13 Digital Triage Forensics: Processing the Digital Crime Scene provides the tools, training, and techniques in Digital Triage Forensics (DTF), a procedural model for the
investigation of digital crime scenes including both traditional crime scenes and the more complex battlefield crime scenes. The DTF is used by the U.S. Army and other traditional police agencies for current digital forensic applications. The tools, training, and techniques from this practice are being brought to the public in this book for the first time. Now corporations, law enforcement, and consultants can benefit from the unique perspectives of the experts who coined Digital Triage Forensics. The text covers the collection of digital media and data from cellular devices and SIM cards. It also presents outlines of pre- and post-blast investigations. This book is divided into six chapters that present the overview of the age of warfare, key concepts of digital triage and battlefield forensics, and methods of conducting pre/post-blast investigations. The book considers how improvised explosive devices (IEDs) have changed from basic booby traps to the primary attack method of the insurgents in Iraq and Afghanistan. It also covers the emergence of a sustainable vehicle for prosecuting enemy combatants under the Rule of Law in Iraq as U.S. airmen, marines, sailors, and soldiers perform roles outside their normal military duties and responsibilities. The remaining chapters detail the benefits of DTF model, the roles and responsibilities of the weapons intelligence team (WIT), and the challenges and issues of collecting digital media in battlefield situations. Moreover, data collection and processing as well as debates on the changing role of digital forensics investigators are explored. This book will be helpful to forensic scientists, investigators, and military personnel, as well as to students and beginners in forensics. Includes coverage on collecting digital media.

Outlines pre- and post-blast investigations Features content on collecting data from cellular devices and SIM cards

Cybercrime Case Presentation-Brett Shavers 2013-01-15 Cybercrime Case Presentation is a “first look” excerpt from Brett Shavers’ new Syngress book, Placing the Suspect Behind the Keyboard. The book considers how the role of digital forensics investigators is an evolution of typical digital forensics, in which evidence is gathered from network traffic in near real time for real-time crime scenes. The DTF is used by the U.S. Army and other traditional police agencies for current digital forensic applications. The tools, training, and techniques from this practice are being brought to the public in this book for the first time. Now corporations, law enforcement, and consultants can benefit from the unique perspectives of the experts who coined Digital Triage Forensics. The text covers the collection of digital media and data from cellular devices and SIM cards. It also presents outlines of pre- and post-blast investigations. This book is divided into six chapters that present the overview of the age of warfare, key concepts of digital triage and battlefield forensics, and methods of conducting pre/post-blast investigations. The book considers how improvised explosive devices (IEDs) have changed from basic booby traps to the primary attack method of the insurgents in Iraq and Afghanistan. It also covers the emergence of a sustainable vehicle for prosecuting enemy combatants under the Rule of Law in Iraq as U.S. airmen, marines, sailors, and soldiers perform roles outside their normal military duties and responsibilities. The remaining chapters detail the benefits of DTF model, the roles and responsibilities of the weapons intelligence team (WIT), and the challenges and issues of collecting digital media in battlefield situations. Moreover, data collection and processing as well as debates on the changing role of digital forensics investigators are explored. This book will be helpful to forensic scientists, investigators, and military personnel, as well as to students and beginners in forensics. Includes coverage on collecting digital media.

Outlines pre- and post-blast investigations Features content on collecting data from cellular devices and SIM cards

Computer Incident Response and Forensics Team Management-Leighton Johnson 2013-11-08 Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management Outlines the steps to completing a successful computer incident response investigation Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams

Alternate Data Storage Forensics-Amber Schroeder 2011-04-18 Learn to pull “digital fingerprints from alternate data storage (ADS) devices including: iPod, Xbox, digital cameras and more from the cyber sleuths who train the Secret Service, FBI, and Department of Defense in bleeding edge digital forensics techniques. This book sets a new forensic methodology standard for investigators to use. This book begins by describing how alternate data storage devices are used to both move and hide data. From here a series of case studies using bleeding edge forensic analysis tools demonstrate readers how to perform forensic investigations on a variety of ADS devices including: Apple iPods, Digital Video Recorders, Cameras, Gaming Consoles (Xbox, PS2, and PSP), Bluetooth devices, and more using state of the art tools. Finally, the book takes a look into the future at “not yet everyday devices which will soon be common repositories for hiding and moving data for both legitimate and illegitimate purposes. Authors are undisputed leaders who train the Secret Service, FBI, and Department of Defense Book presents “one of a kind” bleeding edge information that absolutely can not be found anywhere else. Today the industry has exploded and cyber investigators can be found in almost every field

Cybercrime Case Presentation-Brett Shavers 2013-01-15 Cybercrime Case Presentation is a “first look” excerpt from Brett Shavers’ new Syngress book, Placing the Suspect Behind the Keyboard. Case presentation requires the skills of a good forensic examiner and great public speaker in order to convey enough information to an audience from Brett Shavers’ new Syngress book, Placing the Suspect Behind the Keyboard. Case presentation requires the skills of a good forensic examiner and great public speaker in order to convey enough information to an audience.

Cybercrime Case Presentation-Brett Shavers 2013-01-15 Cybercrime Case Presentation is a “first look” excerpt from Brett Shavers’ new Syngress book, Placing the Suspect Behind the Keyboard. Case presentation requires the skills of a good forensic examiner and great public speaker in order to convey enough information to an audience from Brett Shavers’ new Syngress book, Placing the Suspect Behind the Keyboard. Case presentation requires the skills of a good forensic examiner and great public speaker in order to convey enough information to an audience.

Ethics in Forensic Science-J. C. Upshaw Downs 2012 The word “ethical” can be defined as proper conduct. A failure of forensic scientists to act ethically can result in serious adverse outcomes. However, while seemingly simple to define, the application of being “ethical” somewhat more obscure. That is, when is ethical, ethical, and when is it not? Because we have an adversarial legal system, differences of opinion exist in forensic science. However, there are instances when differences are so divergent that an individual’s ethics are called into question. In light of not only the O.J. Simpson trial - the first national trial to question the ethical behavior of forensic scientists - and the National Academy of Science critique of forensic science, ethical issues have come to the forefront of concern within the forensic community.

Encyclopedia of Forensic Sciences 2012-12-28 Forensic science includes all aspects of investigating a crime, including: chemistry, biology and physics, and also incorporates countless other specialties. Today, the service offered under the guise of ‘forensic science’ includes specialties from virtually all aspects of modern science, medicine, engineering, mathematics and technology. The Encyclopedia of Forensic Sciences, Second Edition is a reference source that will inform both the crime scene worker and the laboratory worker of each other’s protocols, procedures and limitations. Written by leading scientists in each area, every article is peer reviewed to establish clarity, accuracy, and comprehensiveness. As reflected in the specialties of its Editorial Board, the contents covers the core theories, methods and techniques employed by forensic scientists - and applications of these that are used in forensic analysis. This 4-volume set represents a 30% growth in articles from the first edition, with a particular increase in coverage of DNA and digital forensics. Includes an international collection of contributors. The second edition features a new 21-member editorial board, half of which are internationally based.

Includes over 300 articles, approximately 10pp on average Each article features a) suggested readings which point readers to additional sources for more information, b) a list of related Web sites, c) a 5-10 word glossary and definition paragraph, and d) cross-references to related articles in the encyclopedia Available online via SciVerse ScienceDirect. Please visit www.info.sciencedirect.com for more information This new edition continues the reputation of the first edition, which was awarded an Honorable Mention in the prestigious Dartmouth Medal competition for 2001. This award honors the creation of reference works of outstanding quality and significance, and is sponsored by the RUSA Committee of the American Library Association

Virtualization and Forensics-Diane Barrett 2010-08-06 Virtualization and Forensics: A Digital Forensic Investigators Guide to Virtual Environments offers an in-depth view into the world of virtualized environments and the implications they have on forensic investigations. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this guide gives you the end-to-end knowledge needed to identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun. It covers technological advances in virtualization tools, methods, and issues in digital forensic investigations, and explores trends and emerging technologies surrounding virtualization technology. This book consists of three parts. Part I explains the process of virtualization and the different types of virtualized environments. Part II details how virtualization interacts with the basic forensic process, describing the methods used to find virtualization artifacts in dead and live environments as well as identifying the virtual activities that affect the examination process. Part III addresses advanced virtualization issues, such as the challenges of virtualized environments and the implications they have on forensic investigations. This book will be a valuable resource for forensic investigators (corporate and law enforcement) and incident response professionals. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this guide gives you the end-to-end knowledge needed to identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun. It covers technological advances in virtualization tools, methods, and issues in digital forensic investigations. Exploring emerging technologies surrounding virtualization technology.

Digital Forensics for Network, Internet, and Cloud Computing-Clint P Garrison 2010-07-02 Network forensics is an evolution of typical digital forensics, in which evidence is gathered from network traffic in near real time. This book will help security and forensics professionals as well as network administrators build a solid foundation with the fundamentals of digital forensic evidence collection from large and small networks alike. The forensic scientists and investigators are some of the fastest growing jobs in the United States with over 70,000 individuals employed in 2008. Specifically in the area of cybercrime and digital forensics, the federal government is conducting a talent search for 10,000 qualified specialists. Almost every technology company has developed or is
developing a cloud computing strategy. To cut costs, many companies are moving toward network-based applications like Salesforce.com, PeopleSoft, and HR Direct. Every day, we are moving companies' proprietary data images. It can be stored anywhere in the world. The cloud can be hosted anywhere.

Steve Bolt wrote the first whitepaper on XBOX investigations for forensic and incident response professionals, including those in federal government, commercial/private sector examination, but there is currently no map for you to follow as there may be with other digital media. XBOX 360 with social networking sites and chatrooms, transfer files, and more — it just may contain evidence to assist in

XBOX 360 Forensics

The Best Damn Cybercrime and Digital Forensics Book Period

Jack Wiley 2011-04-18 Electronic discovery refers to a process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case. Computer forensics is the application of computer investigation and analysis techniques to perform an investigation to find out exactly what happened on a computer and who was responsible. IDC estimates that the U.S. market for computer forensics will be grow from $252 million in 2004 to $630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market will be $1.8 billion dollars. The Techno Forensics Conference has increased in size by almost 50% in its second year; another example of the rapid growth in the market. This book is the first to combine cybercrime and digital forensic topics to provide law enforcement and IT security professionals with the information needed to manage a digital investigation. Everything needed for analyzing forensic data and recovering digital evidence can be found in one place, including instructions for building a digital forensics lab. * Digital investigation and forensics is a growing industry * Corporate I.T. departments investigating corporate espionage and criminal activities are learning as they go and need a comprehensive guide to e-discovery * Appeals to law enforcement agencies with limited budgets

Python Forensics

Chet Hosmer 2014-05-19 Python Forensics provides many never-before-published proven modules, libraries, and solutions that can be used right out of the box. In addition, detailed instruction and documentation provided with the code samples will allow even novice Python programmers to add their own unique twists or use the models presented to build new solutions. Rapid development of new cybercrime investigation tools is an essential ingredient in virtually every case and environment. Whether you are performing post-mortem investigation, executing live triage, extracting evidence from mobile devices or cloud services, or you are collecting and processing evidence from a network, Python forensic implementations can fill in the gaps. Drawing upon years of practical experience and using numerous examples and illustrative code samples, author Chet Hosmer discusses how to:

- Develop new forensic solutions independent of large vendor software release schedules Participate in an open-source workbench that facilitates direct involvement in the design and implementation of new methods that augment or replace existing tools
- Advance your career by creating new solutions along with the construction of cutting-edge automation solutions to solve old problems Provides hands-on tools, code samples, and detailed instruction and documentation that can be put to use immediately Discusses how to use Python in the mobile device operating systems: iOS, Android, and Windows 8

XBOX 360 Forensics

Steven Bolt 2011-02-07 XBOX 360 Forensics is a complete investigation guide for the XBOX game console. Because the XBOX 360 is no longer just a video game console — it streams movies, connects with social networking sites and chatrooms, transfer files, and more — it just may contain evidence to assist in your next criminal investigation. The forensics community has already begun to receive game consoles for examination, but there is currently no map for you to follow as there may be with other digital media. XBOX 360 Forensics provides that map and presents the information in an easy-to-read, easy-to-reference format. This book is organized into 11 chapters that cover topics such as XBOX 360 hardware; XBOX LIVE; configuration of the console; initial forensic acquisition and examination; specific file types for XBOX 360, XBOX 360 hard drive, post-system update drive artifacts; and XBOX Live redemption code and Facebook. This book will appeal to computer forensic and incident response professionals, including those in federal government, commercial/private sector contractors, and consultants. Game consoles are routinely seized and contain evidence of criminal activity Author Steve Bolt wrote the first whitepaper on XBOX investigations

Understanding Forensic Digital Imaging

Herbert L. Blitzer 2010-07-26 Understanding Forensic Digital Imaging offers the principles of forensic digital imaging and photography in a manner that is straightforward and easy to digest for the professional and student. It provides information on how to photograph any setting that may have forensic value, details how to follow practices that are acceptable in court, and recommends what variety of hardware and software are most valuable to a practitioner. In addition to chapters on basic topics such as light and lenses, resolution, and file formats, the book contains specific information on SWGIT and the use of photography in investigations and in court. Of particular note is Chapter 17, Establishing Quality Requirements, which offers information on how to create a good digital image, and is more comprehensive than any other source currently available. Covers topics that are of vital importance to the practicing professional Serves as an up-to-date reference in the rapidly evolving world of digital imaging Uses clear and concise language so that any reader can understand the technology and science behind digital imaging

Windows Registry Forensics

Harlan Carvey 2011-01-03 Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Packed with real-world examples using freely available open source tools Deep explanation and understanding of the Windows Registry – the most difficult part of Windows to analyze forensically Includes a CD containing code and author-created tools discussed in the book

TechnoSecurity’s Guide to E-Discovey and Digital Forensics

Jack Wiley 2011-10-13 TechnoSecurity’s Guide to E-Discovey and Digital Forensics provides IT security professionals with the information (hardware, software, and procedural requirements) needed to create, manage and sustain a digital forensics lab and investigative team that can accurately and effectively analyze forensic data and recover digital evidence, while preserving the integrity of the electronic evidence for discovery and trial. Internationally known experts in computer forensics share their years of experience at the forefront of digital forensics Bonus chapters on how to build your own Forensics Lab 50% discount to the upcoming Techno Security conference for everyone who purchases a book

Big Data Analytics and Computing for Digital Forensic Investigations

Suneeta Satpathy 2020-03-17 Big Data Analytics and Computing for Digital Forensic Investigations has recently gained a notable development and become the most demanding area in today's information security requirement. This book investigates the areas of digital forensics, digital investigation and data analysis procedures as they apply to computer fraud and cybercrime, with the main objective of describing a variety of digital crimes and retrieving potential digital evidence. Big Data Analytics and Computing for Digital Forensic Investigations gives a contemporary view on the problems of information security. It presents the idea that protective mechanisms and software must be integrated along with forensic capabilities into existing forensic software using big data computing tools and techniques. Features Describes trends of digital forensics served for big data and the challenges of evidence acquisition Enables digital forensic investigators and law enforcement agencies to enhance their digital investigation capabilities with the application of data science analytics, algorithms and fusion technique This book is focused on helping professionals as well as researchers to get ready with next-generation security systems to mount the rising challenges of computer fraud and cybercrimes as well as with digital forensic investigations. Dr Suneeta Satpathy has more than ten years of teaching experience in different subjects of the Computer Science and Engineering discipline. She is currently working as an associate professor in the Department of Computer Science and Engineering, College of Bhubaneswar, affiliated with Biju Patnaik University and Technology, Odisha. Her research interests include computer forensics, cybersecurity, data fusion, data mining, big data analysis and decision mining. Dr Sachin Nandan Mohanty is an associate professor in the Department of Computer Science and Engineering at ICFAI Tech, ICFAI Foundation for Higher
Education, Hyderabad, India. His research interests include data mining, big data analysis, cognitive science, fuzzy decision-making, brain-computer interface, cognition and computational intelligence.

Darkweb Cyber Threat Intelligence Mining—John Robertson 2017-04-04 The important and rapidly emerging new field known as ‘cyber threat intelligence’ explores the paradigm that defenders of computer networks gain a better understanding of their adversaries by understanding what assets they have available for an attack. In this book, a team of experts examines a new type of cyber threat intelligence from the heart of the malicious hacking underworld - the dark web. These highly secure sites have allowed anonymous communities of malicious hackers to exchange ideas and techniques, and to buy/sell malware and exploits. Aimed at both cybersecurity practitioners and researchers, this book represents a first step toward a better understanding of malicious hacking communities on the dark web and what to do about them. The authors examine real-world darkweb data through a combination of human and automated techniques to gain insight into these communities, describing both methodology and results.

Placing the Suspect Behind the Keyboard—Brett Shavers 2013-02-01 Placing the Suspect Behind the Keyboard is the definitive book on conducting a complete investigation of a cybercrime using digital forensics techniques as well as physical investigative procedures. This book merges a digital analysis examiner’s work with the work of a case investigator in order to build a solid case to identify and prosecute cybercriminals. Brett Shavers links traditional investigative techniques with high tech crime analysis in a manner that not only determines elements of crimes, but also places the suspect at the keyboard. This book is a first in combining investigative strategies of digital forensics analysis processes alongside physical investigative techniques in which the reader will gain a holistic approach to their current and future cybercrime investigations. Learn the tools and investigative principles of both physical and digital cybercrime investigations—and how they fit together to build a solid and complete case. Master the techniques of conducting a holistic investigation that combines both digital and physical evidence to track down the ‘suspect behind the keyboard’. The only book to combine physical and digital investigative techniques.

The Five Technological Forces Disrupting Security—Steve Van Till 2017-08-18 The Five Technological Forces Disrupting Security: How Cloud, Social, Mobile, Big Data and IoT are Transforming Physical Security in the Digital Age explores the major technological forces currently driving digital disruption in the security industry, and what they foretell for the future. The book provides a high-level perspective on how the industry is changing as a whole, as well as practical guidance on how to incorporate these new technologies to create better security solutions. It also examines key questions on how these new technologies have lowered barriers for new entrants in the field and how they are likely to change market dynamics and affect customer choices. Set in the context of one of the early dot.com companies to enter physical security, the narrative is written for professionals from Chief Security Officers and systems integrators to product managers and investors. Explores the five major technological forces driving digital change in commercial security. Shows practitioners how to align security strategy with changes. Examines how the consumerization of security will change the vendor playing field. Illustrates how security professionals can leverage these changes in their own careers. Provides an adoption scorecard that ranks trends and timeline for impact.

Practical Forensic Imaging—Bruce Nikkel 2016-12-16

X-Ways Forensics Practitioner’s Guide—Brett Shavers 2013-08-10 The X-Ways Forensics Practitioner’s Guide is more than a manual—it’s a complete reference guide to the full use of one of the most powerful forensic applications available, software that is used by a wide array of law enforcement agencies and private forensic examiners on a daily basis. In the X-Ways Forensics Practitioner’s Guide, the authors provide you with complete coverage of this powerful tool, walking you through configuration and X-Ways fundamentals, and then moving through case flow, creating and importing hash databases, digging into OS artifacts, and conducting searches. Through X-Ways Forensics Practitioner’s Guide, you will be able to use X-Ways Forensics to its fullest potential without any additional training. The book takes you from installation to the most advanced features of the software. Once you are familiar with the basic components of X-Ways, the authors demonstrate never-before-documented features using real life examples and information on how to present investigation results. The book culminates with chapters on reporting, triage and preview methods, as well as electronic discovery and tool X-Ways apps. Provides detailed explanations of the complete forensic investigation processes using X-Ways Forensics. Goes beyond the basics: hands-on case demonstrations of never-before-documented features of X-Ways. Provides the best resource of hands-on information to use X-Ways Forensics.

Handbook of Computer Crime Investigation—Eoghan Casey 2001-10-22 Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey brings together a few top experts to write this first detailed guide for professionals who are already familiar with digital evidence. The Handbook of Computer Crime Investigation helps readers master the forensic analysis of computer systems with a three-part approach covering tools, technology, and case studies. The Tools section provides the details on leading software programs, with each chapter written by that product’s creator. The section ends with an objective comparison of the strengths and limitations of each tool. The main Technology section provides the technical “how to” information for collecting and analyzing digital evidence in common situations, starting with computers, moving on to networks, and culminating with embedded systems. The Case Examples section gives readers a sense of the technical, legal, and practical challenges that arise in real computer investigations. The Tools section provides details of leading hardware and software. The main Technology section provides the technical “how to” information for collecting and analysing digital evidence in common situations. Case Examples give readers a sense of the technical, legal, and practical challenges that arise in real computer investigations.

File System Forensic Analysis—Brian Carrier 2005-03-17 The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer’s file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today’s most valuable open source file system analysis tools—including tools he personally developed. Coverage includes preserving the digital crime scene and duplicating hard disks for “dead analysis” identifying hidden data on a disk’s Host Protected Area (HPA) reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more analyzing DOS, Apple, and GP partitions; BFD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques. Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques. Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more. Using The Sleuth Kit (TSK). Autopsy Forensic Browser, and related open source tools with each chapter dealing with a particular tool or approach and including a hands-on section. Are you a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use.

Forensic Dental Evidence—C. Michael Bowers 2004-01-29 This handbook is written for police investigators and forensic personnel who are tasked with developing investigations that require expertise in dentistry. The focus is providing the information necessary to recognize and professionally manage dental evidence. Investigators will understand the scientific nomenclature, scientific issues, and the specialized forensic nature of this type of forensic investigation. The emphasis is on human identification from dental structures, the identification of people from bite marks, and the signs and significance of dental injuries present in violent crime. Law enforcement personnel, coroners, and other death investigators often encounter crime scenes and victims that require dental expertise. Attorneys are asked to present dental evidence in court. This book delivers the backbone information for these individuals to better assess their needs in both casework and litigation. Forensic Dentistry contains numerous photographs of crime scene evidence and bite marks on victims and details for the reader the types of
dental evidence and what is expected regarding collection, documentation, and the capabilities of analytical methods. This book is the first of its kind to present essential information to the field investigator in a format that allows easy reference and comprehensive detail. * Contains previously unavailable information on digital photography and dental evidence * Includes dozens of photos that illustrate the proper collection and preservation of evidence * Provides desperately needed and essential information necessary to recognize, and professionally manage dental evidence

Malware Forensics Field Guide for Windows Systems - Cameron H. Malin 2012 Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treacherous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, Malware Forensics Field Guide for Windows Systems is a “tool” with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code

Artificial Intelligence Tools for Cyber Attribution - Eric Nunes 2018-02-16 This SpringerBrief discusses how to develop intelligent systems for cyber attribution regarding cyber-attacks. Specifically, the authors review the multiple facets of the cyber attribution problem that make it difficult for “out-of-the-box” artificial intelligence and machine learning techniques to handle. Attributing a cyber-operation through the use of multiple pieces of technical evidence (i.e., malware reverse-engineering and source tracking) and conventional intelligence sources (i.e., human or signals intelligence) is a difficult problem not only due to the effort required to obtain evidence, but the ease with which an adversary can plant false evidence. This SpringerBrief not only lays out the theoretical foundations for how to handle the unique aspects of cyber attribution – and how to update models used for this purpose – but it also describes a series of empirical results, as well as compares results of specially-designed frameworks for cyber attribution to standard machine learning approaches. Cyber attribution is not only a challenging problem, but there are also problems in performing such research, particularly in obtaining relevant data. This SpringerBrief describes how to use capture-the-flag for such research, and describes issues from organizing such data to running your own capture-the-flag specifically designed for cyber attribution. Datasets and software are also available on the companion website.

Crime Scene Photography - Edward M. Robinson 2010-02-03 Crime Scene Photography is a book wrought from years of experience, with material carefully selected for ease of use and effectiveness in training, and field tested by the author in his role as a Forensic Services Supervisor for the Baltimore County Police Department. While there are many books on non-forensic photography, none of them adequately adapt standard image-taking to crime scene photography. The forensic photographer, or more specifically the crime scene photographer, must know how to create an acceptable image that is capable of withstanding challenges in court. This book blends the practical functions of crime scene processing with theories of photography to guide the reader in acquiring the skills, knowledge and ability to render reliable evidence. Required reading by the IAI Crime Scene Certification Board for all levels of certification Contains over 500 photographs Covers the concepts and principles of photography as well as the “how to” of creating a final product Includes end-of-chapter exercises