Digital Forensics Tutorials Viewing Image Contents In Windows

X-Ways Forensics Practitioner’s Guide
Digital Forensics Explained
Digital Image Forensics
Digital Image Forensics
Computer Forensics: Investigating Data and Image Files (CHFI)
Digital Forensics for Legal Professionals
Fundamentals of Digital Forensics
Unleashing the Art of Digital Forensics
Introductory Computer Forensics
A Practical Guide to Digital Forensics Investigations
Practical Forensic Imaging
Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security
Big Digital Forensic Data
Fundamentals of Digital Forensics
Forensic Digital Image Processing
Digital Forensics for Handheld Devices
Digital Forensics with Kali Linux
Handbook of Digital Forensics of Multimedia Data and Devices
Computer Forensics For Dummies
Photo Forensics
Digital Triage Forensics
CD and DVD Forensics
Practical Forensic Imaging
File System Forensic Analysis
Practical Linux Forensics
Corporate Computer Forensics Training System Laboratory Manual Volume I
Digital Forensics with Open Source Tools
Practical Digital Forensics
Learn Computer Forensics
Digital Forensics Trial Graphics
Advances in Digital Forensics II
Cyber Forensics
Photoshop CS3 for Forensics Professionals
Practical Forensic Digital Imaging
Contemporary Digital Forensic Investigations of Cloud and Mobile Applications
Kali - Computer Forensics Data Recovery 101 - Training
Step by Step Tutorial IMAGE CLASSIFICATION Using Scikit-Learn, Keras, And TensorFlow with PYTHON GUI
Forensic Digital Imaging and Photography

TRUJILLO VALERIE

X-Ways Forensics Practitioner's Guide Springer
Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems
Digital Forensics Explained Academic Press
This practical and accessible textbook/reference describes the theory and methodology of digital forensic examinations, presenting examples developed in collaboration with police authorities to ensure relevance to real-world practice. The coverage includes discussions on forensic artifacts and constraints, as well as forensic tools used for law enforcement and in the corporate sector. Emphasis is placed on reinforcing sound forensic thinking, and gaining experience in common tasks through hands-on exercises. This enhanced second edition has been expanded with new material on incident response tasks and computer memory analysis. Topics and features: Outlines what computer forensics is, and what it can do, as well as what its limitations are Discusses both the theoretical foundations and the fundamentals of forensic methodology Reviews broad principles that are applicable worldwide Explains how to find and interpret several important artifacts Describes free and open source software tools, along with the AccessData Forensic Toolkit Features exercises and review questions throughout, with solutions provided in the appendices Includes numerous practical examples, and provides supporting video lectures online This easy-to-follow primer is an essential resource for students of computer forensics, and will also serve as a valuable reference for practitioners seeking instruction on performing forensic examinations. Joakim Kävrestad is a lecturer and researcher at the University of Skövde, Sweden, and an AccessData Certified Examiner. He also serves as a forensic consultant, with several years of experience as a forensic expert with the Swedish police.
Digital Image Forensics Packt Publishing Ltd
Digital imaging technology has been used in forensics since at least 1992, yet until now there?has been?no practical instruction available to address the unique issues of image processing in an everyday forensic environment. Photoshop CS3 for Forensics Professionals serves the everyday, real-world needs of law enforcement and legal personnel dealing with digital images (including both photos and video stills). This book is an excellent tool for: Law enforcement personnel, from crime scene and arson investigators, detectives, and patrol officers to forensic photographers, fingerprint examiners, video analysts, tool mark and footwear examiners, and criminalists. Security pros in such fields as private investigation, insurance, fraud detection, and loss prevention. Scientific and technical users of Photoshop with workflows similar to law enforcement, such as medical photographers, research imaging experts, engineering and architecture staff, and industrial photographers. Staff responsible for maintaining a photo archive or printing images for court. Photoshop CS3 for Forensics Professionals is the only book to provide forensics professionals with specific answers to their imaging questions. This is the perfect resource for those who want to move from simple theory to the essential skills needed to be more effective. This resource is divided into three parts: Part I: The Essentials is about setting up your workflow, archiving your images, and familiarizing yourself with Adobe Photoshop and Adobe Bridge, including the setting up of preferences. Also covered are the best practices in writing reports and providing courtroom testimony. Part II: The Digital Darkroom teaches how to use Photoshop to accomplish what traditionally was done in the darkroom, from correcting color casts to making prints and exhibits for courtroom use. Part III: Image Analysis & Enhancement covers techniques for clarifying images so that details can be better viewed and used for analysis or comparison, from contrast enhancement and pattern removal to even forensic video analysis. The companion CD-ROM provides sample images—including various accident and crime scenes—you can use to practice the techniques from the book while?following along with the tutorials. It also includes several scripts, plug-ins, and actions so you can work more effectively. In addition, instructor's materials are available so you can use book in workshops and training seminars. Order this one-of-a-kind resource today! Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.
Digital Image Forensics No Starch Press
The first comprehensive and detailed presentation of techniques for authenticating digital images. Photographs have been doctored since photography was invented. Dictators have erased people from photographs and from history. Politicians have manipulated photos for short-term political gain. Altering photographs in the predigital era required time-consuming darkroom work. Today, powerful and low-cost digital technology makes it relatively easy to alter digital images, and the resulting fakes are difficult to detect. The field of photo forensics—pioneered in Hany Farid's lab at Dartmouth College—restores some trust to photography. In this book, Farid describes techniques that can be used to authenticate photos. He provides the intuition and background as well as the

mathematical and algorithmic details needed to understand, implement, and utilize a variety of photo forensic techniques. Farid traces the entire imaging pipeline. He begins with the physics and geometry of the interaction of light with the physical world, proceeds through the way light passes through a camera lens, the conversion of light to pixel values in the electronic sensor, the packaging of the pixel values into a digital image file, and the pixel-level artifacts introduced by photo-editing software. Modeling the path of light during image creation reveals physical, geometric, and statistical regularities that are disrupted during the creation of a fake. Various forensic techniques exploit these irregularities to detect traces of tampering. A chapter of case studies examines the authenticity of viral video and famously questionable photographs including “Golden Eagle Snatches Kid” and the Lee Harvey Oswald backyard photo.

Computer Forensics: Investigating Data and Image Files (CHFI) John Wiley & Sons

The Computer Forensic Series by EC-Council provides the knowledge and skills to identify, track, and prosecute the cyber-criminal. The series is comprised of four books covering a broad base of topics in Computer Hacking Forensic Investigation, designed to expose the reader to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Learners are introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. In full, this and the other three books provide preparation to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker’s footprint through a client system. The series and accompanying labs help prepare the security student or professional to profile an intruder’s footprint and gather all necessary information and evidence to support prosecution in a court of law. Investigating Data and Image Files provides a basic understanding of steganography, data acquisition and duplication, encase, how to recover deleted files and partitions and image file forensics. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Digital Forensics for Legal Professionals Springer Nature

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 GPT partitions; BSD 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 When it comes to file system analysis, no other book offers this much detail or expertise. Whether you're 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.

Fundamentals of Digital Forensics BPB Publications

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide About This Book Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Who This Book Is For This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage. What You Will Learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites In Detail Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital forensics—acquisition, extraction, analysis, and presentation using Kali Linux tools. Style and approach While covering the best practices of digital forensics investigations, evidence acquisition, preservation, and analysis, this book delivers easy-to-follow practical examples and detailed labs for an easy approach to learning forensics. Following the guidelines within each lab, you can easily practice all readily available

forensic tools in Kali Linux, within either a dedicated physical or virtual machine.

Unleashing the Art of Digital Forensics Jeremy Martin

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Practically every crime now involves some digital evidence; digital forensics provides the techniques and tools to articulate this evidence. This book describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

Introductory Computer Forensics CRC Press

Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies

A Practical Guide to Digital Forensics Investigations CRC Press

Approximately 80 percent of the world’s population now owns a cell phone, which can hold evidence or contain logs about communications concerning a crime. Cameras, PDAs, and GPS devices can also contain information related to corporate policy infractions and crimes. Aimed to prepare investigators in the public and private sectors, Digital Forensics for Handheld Devices examines both the theoretical and practical aspects of investigating handheld digital devices. This book touches on all areas of mobile device forensics, including topics from the legal, technical, academic, and social aspects of the discipline. It provides guidance on how to seize data, examine it, and prepare it as evidence for court. This includes the use of chain of custody forms for seized evidence and Faraday Bags for digital devices to prevent further connectivity and tampering of evidence. Emphasizing the policies required in the work environment, the author provides readers with a clear understanding of the differences between a corporate investigation and a criminal investigation. The book also: Offers best practices for establishing an incident response policy and seizing data from company or privately owned digital devices Provides guidance in establishing dedicated examinations free of viruses, spyware, and connections to other devices that could taint evidence Supplies guidance on determining protocols for complicated crime scenes with external media and devices that may have connected with the handheld device Considering important privacy issues and the Fourth Amendment, this book facilitates an understanding of how to use digital forensic tools to investigate the complete range of available digital devices, including flash drives, cell phones, PDAs, digital cameras, and netbooks. It includes examples of commercially available digital forensic tools and ends with a discussion of the education and certifications required for various careers in mobile device forensics.

Practical Forensic Imaging IGI Global

Get up and running with collecting evidence using forensics best practices to present your findings in judicial or administrative proceedings Key Features Learn the core techniques of computer forensics to acquire and secure digital evidence skillfully Conduct a digital forensic examination and document the digital evidence collected Perform a variety of Windows forensic investigations to analyze and overcome complex challenges Book DescriptionA computer forensics investigator must possess a variety of skills, including the ability to answer legal questions, gather and document evidence, and prepare for an investigation. This book will help you get up and running with using digital forensic tools and techniques to investigate cybercrimes successfully. Starting with an overview of forensics and all the open source and commercial tools needed to get the job done, you'll learn core forensic practices for searching databases and analyzing data over networks, personal devices, and web applications. You'll then learn how to acquire valuable information from different places, such as filesystems, e-mails, browser histories, and search queries, and capture data remotely. As you advance, this book will guide you through implementing forensic techniques on multiple platforms, such as Windows, Linux, and macOS, to demonstrate how to recover valuable information as evidence. Finally, you'll get to grips with presenting your findings efficiently in judicial or administrative proceedings. By the end of this book, you'll have developed a clear understanding of how to acquire, analyze, and present digital evidence like a proficient computer forensics investigator.What you will learn Understand investigative processes, the rules of evidence, and ethical guidelines Recognize and document different types of computer hardware Understand the boot process covering BIOS, UEFI, and the boot sequence Validate forensic hardware and software Discover the locations of common Windows artifacts Document your findings using technically correct terminology Who this book is for If you're an IT beginner, student, or an investigator in the public or private sector this book is for you. This book will also help professionals and investigators who are new to incident response and digital forensics and interested in making a career in the cybersecurity domain. Individuals planning to pass the Certified Forensic Computer Examiner (CFCE) certification will also find this book useful.

Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security John Wiley & Sons

Section 1: What is Digital Forensics? Chapter 1. Digital Evidence is Everywhere Chapter 2. Overview of Digital Forensics Chapter 3. Digital Forensics -- The Sub-Disciplines Chapter 4. The Foundations of Digital Forensics -- Best Practices Chapter 5.

Overview of Digital Forensics Tools Chapter 6. Digital Forensics at Work in the Legal System Section 2: Experts Chapter 7. Why Do I Need an Expert? Chapter 8. The Difference between Computer Experts and Digital Forensic Experts Chapter 9. Selecting a Digital Forensics Expert Chapter 10. What to Expect from an Expert Chapter 11. Approaches by Different Types of Examiners Chapter 12. Spotting a Problem Expert Chapter 13. Qualifying an Expert in Court Sections 3: Motions and Discovery Chapter 14. Overview of Digital Evidence Discovery Chapter 15. Discovery of Digital Evidence in Criminal Cases Chapter 16. Discovery of Digital Evidence in Civil Cases Chapter 17. Discovery of Computers and Storage Media Chapter 18. Discovery of Video Evidence Ch ...

Big Digital Forensic Data Elsevier

An explanation of the basic principles of data This book explains the basic principles of data as building blocks of electronic evidential matter, which are used in a cyber forensics investigations. The entire text is written with no reference to a particular operation system or environment, thus it is applicable to all work environments, cyber investigation scenarios, and technologies. The text is written in a step-by-step manner, beginning with the elementary building blocks of data progressing upwards to the representation and storage of information. It inlcudes practical examples and illustrations throughout to guide the reader.

Fundamentals of Digital Forensics Syngress

In this book, implement deep learning-based image classification on classifying monkey species, recognizing rock, paper, and scissor, and classify airplane, car, and ship using TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy and other libraries. In chapter 1, you will learn how to use TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy and other libraries to perform how to classify monkey species using 10 Monkey Species dataset provided by Kaggle (https://www.kaggle.com/slothkong/10-monkey-species/download). Here's an overview of the steps involved in classifying monkey species using the 10 Monkey Species dataset: Dataset Preparation: Download the 10 Monkey Species dataset from Kaggle and extract the files. The dataset should consist of separate folders for each monkey species, with corresponding images.; Load and Preprocess Images: Use libraries such as OpenCV to load the images from the dataset. Resize the images to a consistent size (e.g., 224x224 pixels) to ensure uniformity.; Split the Dataset: Divide the dataset into training and testing sets. Typically, an 80:20 or 70:30 split is used, where the larger portion is used for training and the smaller portion for testing the model's performance.; Label Encoding: Encode the categorical labels (monkey species) into numeric form. This step is necessary to train a machine learning model, as most algorithms expect numerical inputs.; Feature Extraction: Extract meaningful features from the images using techniques like deep learning or image processing algorithms. This step helps in representing the images in a format that the machine learning model can understand.; Model Training: Use libraries like TensorFlow and Keras to train a machine learning model on the preprocessed data. Choose an appropriate model architecture, in this case, MobileNetV2.; Model Evaluation: Evaluate the trained model on the testing set to assess its performance. Metrics like accuracy, precision, recall, and F1-score can be used to evaluate the model's classification performance.; Predictions: Use the trained model to make predictions on new, unseen images. Pass the images through the trained model and obtain the predicted labels for the monkey species. In chapter 2, you will learn how to use TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy and other libraries to perform how to recognize rock, paper, and scissor using dataset provided by Kaggle (https://www.kaggle.com/sanikamal/rock-paper-scissors-dataset/download). Here's the outline of the steps: Step 1: Dataset Preparation: Download the rock-paper-scissors dataset from Kaggle by visiting the provided link and clicking on the "Download" button. Save the dataset to a local directory on your machine. Extract the downloaded dataset to a suitable location. This will create a folder containing the images for rock, paper, and scissors.; Step 2: Data Preprocessing: Import the required libraries: TensorFlow, Keras, NumPy, OpenCV, and Pandas. Load the dataset using OpenCV: Iterate through the image files in the dataset directory and use OpenCV's cv2.imread() function to load each image. You can specify the image's file extension (e.g., PNG) and directory path. Preprocess the images: Resize the loaded images to a consistent size using OpenCV's cv2.resize() function. You may choose a specific width and height suitable for your model. Prepare the labels: Create a list or array to store the corresponding labels for each image (rock, paper, or scissors). This can be done based on the file naming convention or by mapping images to their respective labels using a dictionary.; Step 3: Model Training: Create a convolutional neural network (CNN) model using Keras: Define a CNN architecture using Keras' Sequential model or functional API. This typically consists of convolutional layers, pooling layers, and dense layers. Compile the model: Specify the loss function (e.g., categorical cross-entropy) and optimizer (e.g., Adam) using Keras' compile() function. You can also define additional metrics to evaluate the model's performance. Train the model: Use Keras' fit() function to train the model on the preprocessed dataset. Specify the training data, labels, batch size, number of epochs, and validation data if available. This will optimize the model's weights based on the provided dataset. Save the trained model: Once the model training is complete, you can save the trained model to disk using Keras' save() or save_weights() function. This allows you to load the model later for predictions or further training.; Step 4: Model Evaluation: Evaluate the trained model: Use Keras' evaluate() function to assess the model's performance on a separate testing dataset. Provide the testing data and labels to calculate metrics such as accuracy, precision, recall, and F1 score. This will help you understand how well the model generalizes to new, unseen data. Analyze the model's performance: Interpret the evaluation metrics and analyze any potential areas of improvement. You can also visualize the confusion matrix or classification report to gain more insights into the model's predictions.; Step 5: Prediction: Use the trained model for predictions: Load the saved model using Keras' load_model() function. Then, pass new, unseen images through the model to obtain predictions. Preprocess these images in the same way as the training images (resize, normalize, etc.). Visualize and interpret predictions: Display the predicted labels alongside the corresponding images to see how well the model performs. You can use libraries like Matplotlib or OpenCV to show the images and their predicted labels. Additionally, you can calculate the accuracy of the model's predictions on the new dataset. In chapter 3, you will learn how to use TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy and other libraries to perform how to classify airplane, car, and ship using Multiclass-image-dataset-airplane-car-ship dataset provided by Kaggle (https://www.kaggle.com/abtabm/multiclassimagedatasetairplanecar). Here are the outline steps: Import the required libraries:

TensorFlow, Keras, Scikit-Learn, OpenCV, Pandas, NumPy. Load and preprocess the dataset: Read the images from the dataset folder. Resize the images to a fixed size. Store the images and corresponding labels.; Split the dataset into training and testing sets: Split the data and labels into training and testing sets using a specified ratio.; Encode the labels: Convert the categorical labels into numerical format. Perform one-hot encoding on the labels.; Build MobileNetV2 model using Keras: Create a sequential model. Add convolutional layers with activation functions. Add pooling layers for downsampling. Flatten the output and add dense layers. Set the output layer with softmax activation.; Compile and train the model: Compile the model with an optimizer and loss function. Train the model using the training data and labels. Specify the number of epochs and batch size.; Evaluate the model: Evaluate the trained model using the testing data and labels. Calculate the accuracy of the model.; Make predictions on new images: Load and preprocess a new image. Use the trained model to predict the label of the new image. Convert the predicted label from numerical format to categorical.

Forensic Digital Image Processing Lulu.com

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book's 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.

Digital Forensics for Handheld Devices Newnes

This is a training lab covering forensic data recovery using Kali linux

Digital Forensics with Kali Linux Springer

Uncover a digital trail of e-evidence by using the helpful, easy-to-understand information in Computer Forensics For Dummies! Professional and armchair investigators alike can learn the basics of computer forensics, from digging out electronic evidence to solving the case. You won't need a computer science degree to master e-discovery. Find and filter data in mobile devices, e-mail, and other Web-based technologies. You'll learn all about e-mail and Web-based forensics, mobile forensics, passwords and encryption, and other e-evidence found through VoIP, voicemail, legacy mainframes, and databases. You'll discover how to use the latest forensic software, tools, and equipment to find the answers that you're looking for in record time. When you understand how data is stored, encrypted, and recovered, you'll be able to protect your personal privacy as well. By the time you finish reading this book, you'll know how to: Prepare for and conduct computer forensics investigations Find and filter data Protect personal privacy Transfer evidence without contaminating it Anticipate legal loopholes and opponents' methods Handle passwords and encrypted data Work with the courts and win the case Plus, Computer Forensics for Dummies includes lists of things that everyone interested in computer forensics should know, do, and build. Discover how to get qualified for a career in computer forensics, what to do to be a great investigator and expert witness, and how to build a forensics lab or toolkit. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Handbook of Digital Forensics of Multimedia Data and Devices CRC Press

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigationsGather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10–specific feature forensicsUtilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

Computer Forensics For Dummies MIT Press

This book discusses blind investigation and recovery of digital evidence left behind on digital devices, primarily for the purpose of tracing cybercrime sources and criminals. It presents an overview of the challenges of digital image forensics, with a specific focus on two of the most common forensic problems. The first part of the book addresses image source investigation, which involves mapping an image back to its camera source to facilitate investigating and tracing the source of a crime. The second part of the book focuses on image-forgery detection, primarily focusing on "copy-move forgery" in digital images, and presenting effective solutions to copy-move forgery detection with an emphasis on additional related challenges such as blur-invariance, similar genuine object identification, etc. The book

concludes with future research directions, including counter forensics. With the necessary mathematical information in every chapter, the book serves as a useful reference resource for researchers and professionals alike. In addition, it can also be used as a supplementary text for upper-undergraduate and graduate-level courses on “Digital Image Processing”, “Information Security”, “Machine Learning”, “Computer Vision” and “Multimedia Security and Forensics”.

Photo Forensics Packt Publishing Ltd

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies Protect attached evidence media from accidental modification Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted drives using BitLocker, FileVault, and TrueCrypt; and others Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

Related with Digital Forensics Tutorials Viewing Image Contents In Windows:
• Hunie Pop 2 Guide : click here