

Windows Data Recovery Techniques Computer Repair Professionals

When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybercrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandated by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. Scene of the Cybercrime, Second Edition is a completely revised and updated book which covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience; IT security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. Scene of the Cybercrime, Second Edition provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital, forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.

Maximum PC is the magazine that every computer fanatic, PC gamer or content creator must read. Each and every issue is packed with punishing product reviews, insightful and innovative how-to stories and the illuminating technical articles that enthusiasts crave.

The first book completely devoted to this important part of security in a Windows environment.

This three volume book contains the Proceedings of 5th International Conference on Advanced Computing, Networking and Informatics (ICACNI 2017). The book focuses on the recent advancement of the broad areas of advanced computing, networking and informatics. It also includes novel approaches devised by researchers from across the globe. This book brings together academic scientists, professors, research scholars and students to share and disseminate information on knowledge and scientific research works related to computing, networking, and informatics to discuss the practical challenges encountered and the solutions adopted. The book also promotes translation of basic research into applied investigation and convert applied investigation into practice.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills. 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 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

A series of Book of Computers . The ebook version does not contain CD.

The research that was examined during the course of this project was to demonstrate the impact solid state drives will and is having on computer forensic examinations and the ability to conduct them successfully. This is accomplished by covering the questions of how will data recovery become more difficult with the implementation of the SSD? How will SSDs impede computer forensic examiners and how will Windows based data recovery tools be able to examine SSDs? Discussing these topical areas demonstrates that there are formidable issues that are currently making forensic exams difficult and sometimes impossible to successfully complete. The current Windows based tools are having varying success rates in assisting forensic examiners in completing their tasks and improvements are on-going. The continuous review of these devices as they are developed and placed in more wide spread usage is going to be critical in overcoming the issue of recovering data from these devices. The success in

overcoming current obstacles is only going to be achievable through testing, which should begin with the current available SSD models that are on the market. Each of the various types should be tested and documented methodically to develop an understanding of how these drives work and how to develop the tools to work with these drives in the future. New testing should also coincide with the most recent work with these drives that is currently taking place. Personal interviews with examiners will help testers further in continuing with this work. Diligence and persistence in working with SSDs will aid in forwarding the computer forensic profession.

This is the official CHFI (Computer Hacking Forensics Investigator) study guide for professionals studying for the forensics exams and for professionals needing the skills to identify an intruder's footprints and properly gather the necessary evidence to prosecute. The EC-Council offers certification for ethical hacking and computer forensics. Their ethical hacker exam has become very popular as an industry gauge and we expect the forensics exam to follow suit. Material is presented in a logical learning sequence: a section builds upon previous sections and a chapter on previous chapters. All concepts, simple and complex, are defined and explained when they appear for the first time. This book includes: Exam objectives covered in a chapter are clearly explained in the beginning of the chapter, Notes and Alerts highlight crucial points, Exam's Eye View emphasizes the important points from the exam's perspective, Key Terms present definitions of key terms used in the chapter, Review Questions contains the questions modeled after real exam questions based on the material covered in the chapter. Answers to the questions are presented with explanations. Also included is a full practice exam modeled after the real exam. The only study guide for CHFI, provides 100% coverage of all exam objectives. CHFI Training runs hundreds of dollars for self tests to thousands of dollars for classroom training.

Blockchain technology allows value exchange without the need for a central authority and ensures trust powered by its decentralized architecture. As such, the growing use of the internet of things (IoT) and the rise of artificial intelligence (AI) are to be benefited immensely by this technology that can offer devices and applications data security, decentralization, accountability, and reliable authentication. Bringing together blockchain technology, AI, and IoT can allow these tools to complement the strengths and weaknesses of the others and make systems more efficient.

Multidisciplinary Functions of Blockchain Technology in AI and IoT Applications deliberates upon prospects of blockchain technology using AI and IoT devices in various application domains. This book contains a comprehensive collection of chapters on machine learning, IoT, and AI in areas that include security issues of IoT, farming, supply chain management, predictive analytics, and natural languages processing. While highlighting these areas, the book is ideally intended for IT industry professionals, students of computer science and software engineering, computer scientists, practitioners, stakeholders, researchers, and academicians interested in updated and advanced research surrounding the functions of blockchain technology in AI and IoT applications across diverse fields of research.

Data loss can be happened either human made cause or system failure. If we know the reasons of data loss, we can reduce our data loss. In this section of this book, I'll introduce you with most common reason of data loss. After reading this book, you will be able to take necessary steps to protect your data from loss & recover it. What You'll Get Inside: Data Loss Reason of Data Loss 1) System Failure Prevention 2) Human Errors 3) Software Corruption 4) Computer viruses and Malware 5) Natural Disasters What is Data Recovery? How Data Recovery Process Work File Data Recovery for Hard Drive How you can determine a Physical Hard Drive Failure When you will have to Recover Hard Drive Recovering Hard Drive Deleted File Recovery [Windows] Formatted Drive Recovery RAW Recovery Recovering Files on Partition is lost File/Data Recovery for unreachable partition File Recovery in case all the Partitions are lost File Data Recovery for Mac Introduction to MAC Undelete files on MAC Recovering deleted file from Trash Why deleted data is recoverable File recovery in MAC Hard Drive Data Recovery for MAC Lost Partition Recovery in MAC Recovering Data from Lost Partition File Data Recovery for USB What is USB Flash Drive Reason of losing files from USB Flash Drive Recovering File from Formatted USB Drive Recovering Lost Data from Pen Drive Reasons of File/Data Loss on Pen Drive Recovering Pen Drive Data (Using EaseUs Data Recovery Software) File Data Recovery for Memory Card & SD Card Reasons and Solutions of Data Loss File Data Recovery for Android Reason of Data Loss on Android Recovering Lost Data File Data Recovery For iPhone Reason of Data Losing on I-Phone Recovering iPhone Data Process 1 [Restoring data directly from iPhone] Process 2 [Restoring data from iTunes Backup] Process 3 [Restoring data from iCloud Backup] Data Recovery Software's Data Recovery Software for PC 1. Recuva 2. Pandora Recovery 3. Puran File Recovery 4. Glary Undelete 5. SoftPerfect File Recovery 6. EaseUS Data Recovery Wizard 7. Wise Data Recovery 8. Restoration 9. Free Undelete 10. ADRC Data Recovery Tools Data Recovery Software for Android 1. Android Data Recovery 2 Data Recovery for Android 3. iCare Recovery 4. Data Recovery from Google Store 5. MyJad Android Data Recovery Take a Sneak Peak Inside (page 12): "Mac is the one of the most favorite operating system to users. It is introduced by Apple Inc. From the very beginning of the release Mac has won users mind. The developer of Mac has worked to give maximum protection to their user's data. However, like windows Mac users also face problem of data losing. Reason of data losing is same as data losing on Windows. Now I am going to describe how you can recover files on MAC using a small software called "EaseUs Data Recovery." It allows users to quickly get deleted, damaged or formatted data." Since 1993, the Information Security Management Handbook has served not only as an everyday reference for information security practitioners but also as an important document for conducting the intense review necessary to prepare for the Certified Information System Security Professional (CISSP) examination. Now completely revised and updated and in its fifth edition, the handbook maps the ten domains of the Information Security Common Body of Knowledge and provides a complete understanding of all the items in it. This is a ...must have... book, both for preparing for the CISSP exam and as a comprehensive, up-to-date reference.

Considered the gold-standard reference on information security, the Information Security Management Handbook provides an authoritative compilation of the fundamental knowledge, skills, techniques, and tools required of today's IT security professional. Now in its sixth edition, this 3200 page, 4 volume stand-alone reference is organized under the C

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts,

providing the benchmark resource for information security, network security, information privacy, and information warfare.

This comprehensive manual covers three areas in which system administrators must be proficient to successfully recover data: the structure and operating principles of the most popular file systems, automatic data recovery techniques, and manual recovery techniques used in cases of total data destruction. Data recovery from hard drives and optical storage in Windows, BSD, and Linux file systems is described, as are automatic recovery utilities, manual and automatic recovery of deleted files on ext2/ext3 partitions and NTFS partitions, formatted NTFS partitions and deleted UFS/FFS files, RAID data recovery, media restoration with physical damage, and data loss prevention.

Annotation "With the acceptance of computers in our everyday life, a new line of crime has emerged revolving around the computer. Just as computers make daily transactions more efficient, they have also made many crimes more efficient. This trend is likely to continue, and for that reason alone police investigators should make themselves better prepared for computer related crime investigations. Divided into four sections, this book proposes theoretical and practical information, interventions, directives, and ideas. This text will be a useful resource for law enforcement professionals, criminal justice students, security professionals, and private business."--BOOK JACKET.Title Summary field provided by Blackwell North America, Inc. All Rights Reserved.

"Digital Crime Investigation" written by Benild Joseph gives an insight to investigators helping them with the background and tools that they need to investigate crime occurring in the digital world. This extremely useful guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to assist investigations. Law enforcement departments and security officers all over the world having the responsibility for enforcing, investigating and prosecuting cybercrime are overpowered, not only with the increasing number of crimes being committed but also by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover.

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

HANDS-ON MICROSOFT WINDOWS SERVER 2016 is the perfect resource for learning Windows Server 2016 from the ground up. Designed to build a foundation in basic server administration, this book requires no previous server experience. It covers all of the critical Windows Server 2016 features, including the advantages unique to this new server operating system. Readers learn how to choose the right server edition for their needs. They also learn to install, configure, customize, manage, and troubleshoot today's servers most effectively. If the reader is new to server administration, this book provides the background and knowledge needed to manage servers on small to large networks. If the reader is an experienced server administrator, this book provides a fast way to get up to speed on new Windows Server 2016 administration. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This step-by-step, highly visual text provides a comprehensive introduction to managing and maintaining computer hardware and software. Written by best-selling author and educator Jean Andrews, A+ Guide to IT Technical Support, 9th Edition closely integrates the CompTIA+ Exam objectives to prepare you for the 220-901 and 220-902 certification exams. The new Ninth Edition also features extensive updates to reflect current technology, techniques, and industry standards in the dynamic, fast-paced field of PC repair and information technology. Each chapter covers both core concepts and advanced topics, organizing material to facilitate practical application and encourage you to learn by doing. The new edition features more coverage of updated hardware, security, virtualization, new coverage of cloud computing, Linux and Mac OS, and increased emphasis on mobile devices. Supported by a wide range of supplemental resources to enhance learning with Lab Manuals, CourseNotes online labs and the optional MindTap that includes online labs, certification test prep and interactive exercises and activities, this proven text offers students an ideal way to prepare for success as a professional IT support technician and administrator.

Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. Use this hands-on guide to understand the ever growing and complex world of digital security. Learn how to protect yourself from digital crime, secure your communications, and become anonymous online using sophisticated yet practical tools and techniques. This book teaches you how to secure your online identity and personal devices, encrypt your digital data and online communications, protect cloud data and Internet of Things (IoT), mitigate social engineering attacks, keep your purchases secret, and conceal your digital footprint. You will understand best practices to harden your operating system and delete digital traces using the most widely used operating system, Windows. Digital Privacy and Security Using Windows offers a comprehensive list of practical digital privacy tutorials in addition to being a complete repository of free online resources and tools assembled in one place. The book helps you build a robust defense from electronic crime and corporate surveillance. It covers general principles of digital privacy and how to configure and use various security applications to maintain your privacy, such as TOR, VPN, and BitLocker. You will learn to encrypt email communications using Gpg4win and Thunderbird. What You'll Learn Know the various parties interested in having your private data Differentiate between government and corporate surveillance, and the motivations behind each one Understand how online tracking works technically Protect digital data, secure online communications, and become anonymous online Cover and destroy your digital traces using Windows OS Secure your data in transit and at rest Be aware of cyber security risks and countermeasures Who This Book Is For End users, information security professionals, management, infosec students

How To Recover Deleted Files Your Step-By-Step Guide To Recovering Deleted Files HowExpert PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

?? HDD/USB ?????????? Windows 10 Chrome ????? Cookies???? ???? iPad????? Android ??????????????

This book presents a general introduction to the computational aspects of forensic science, covering the different tools needed for forensic investigations, the importance of forensics and biometrics, and the use of Benford's law for biometrics and network traffic analysis. It specifically focuses on the application of these techniques in Africa, and how they can be of benefit in the investigation of crime in Nigeria in particular.

Forensic Accounting provides comprehensive coverage of fraud detection and deterrence and includes the broader educational material of the forensic accounting field with all the necessary accompaniments. The text follows the model curriculum for education in fraud and forensic funded by the U.S. national Institute of Justice and developed by a Technical Working Group of experts in the field. The text serves as a comprehensive and authoritative resource for teaching forensic accounting concepts and procedures that is also and appropriate and pedagogically ready for class room use. This easy to read, comprehensive textbook includes case study examples to clearly explain technical concepts and bring the material to life.

If you want to discover how to solve your problems regarding loss data in your computer then, check this "How To Recover Deleted Files" guide. In this step-by-step guide, you will reap the following benefits: - Resolve data loss problems. - Learn how to prevent data loss. - Learn how to recover data due to system boot issue. - Learn how to recover data due to hard disk issue. - Discover how to recover Office data files. - Impress your friends to recover their computer from viruses, corrupted registry and files. -

Discover how to make use of the computer data recovery tools. - Recover operating system from an unstable program. - Learn how to back-up your files and folders. - And much more. HowExpert publishes quick 'how to' guides on all topics from A to Z by everyday experts.

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Written by computer guru Tittel, this is the perfect study guide to help candidates pass this core exam for both the MCSE Windows Server 2003 and MCSA programs. The accompanying CD features PrepLogic* Practice Tests, Preview Edition.

The 70-688 Supporting Windows 8.1 textbook helps prepare students for the second of two exams required for Microsoft Certified Solutions Associate (MCSA): Windows 8 certification. Students master configuration or support for Windows 8 computers, devices, users and associated network and security resources. Those in this IT Professional career field work with networks configured as a domain-based or peer-to-peer environment with access to the Internet and cloud services. These IT Professionals could be a consultant, full-time desktop support technician, or IT generalist who administers Windows 8-based computers and devices as a portion of their broader technical responsibilities. Additional skills addressed, including the recent 8.1 objectives, in this textbook: Design an Installation and Application Strategy Maintain Resource Access Maintain Windows Clients and Devices Manage Windows 8 Using Cloud Services and Microsoft Desktop Optimization Pack The MOAC IT Professional series is the Official from Microsoft, turn-key Workforce training program that leads to professional certification and was authored for college instructors and college students. MOAC gets instructors ready to teach and students ready for work by delivering essential resources in 5 key areas: Instructor readiness, student software, student assessment, instruction resources, and learning validation. With the Microsoft Official Academic course program, you are getting instructional support from Microsoft; materials that are accurate and make course delivery easy.

Discover the tools and techniques of mobile forensic investigations and make sure your mobile autopsy doesn't miss a thing, all through powerful practical recipes About This Book Acquire in-depth knowledge of mobile device acquisition using modern forensic tools Understand the importance of clouds for mobile forensics and learn how to extract data from them Discover advanced data extraction techniques that will help you to solve forensic tasks and challenges Who This Book Is For This book is aimed at practicing digital forensics analysts and information security professionals familiar with performing basic forensic investigations on mobile device operating systems namely Android, iOS, Windows, and Blackberry. It's also for those who need to broaden their skillset by adding more data extraction and recovery techniques. What You Will Learn Retrieve mobile data using modern forensic tools Work with Oxygen Forensics for Android devices acquisition Perform a deep dive analysis of iOS, Android, Windows, and BlackBerry Phone file systems Understand the importance of cloud in mobile forensics and extract data from the cloud using different tools Learn the application of SQLite and Plists Forensics and parse data with digital forensics tools Perform forensic investigation on iOS, Android, Windows, and BlackBerry mobile devices Extract data both from working and damaged mobile devices using JTAG and Chip-off Techniques In Detail Considering the emerging use of mobile phones, there is a growing need for mobile forensics. Mobile forensics focuses specifically on performing forensic examinations of mobile devices, which involves extracting, recovering and analyzing data for the purposes of information security, criminal and civil investigations, and internal investigations. *Mobile Forensics Cookbook* starts by explaining SIM cards acquisition and analysis using modern forensics tools. You will discover the different software solutions that enable digital forensic examiners to quickly and easily acquire forensic images. You will also learn about forensics analysis and acquisition on Android, iOS, Windows Mobile, and BlackBerry devices. Next, you will understand the importance of cloud computing in the world of mobile forensics and understand different techniques available to extract data from the cloud. Going through the fundamentals of SQLite and Plists Forensics, you will learn how to extract forensic artifacts from these sources with appropriate tools. By the end of this book, you will be well versed with the advanced mobile forensics techniques that will help you perform the complete forensic acquisition and analysis of user data stored in different devices. Style and approach This book delivers a series of extra techniques and methods for extracting and analyzing data from your Android, iOS, Windows, and Blackberry devices. Using practical recipes, you will be introduced to a lot of modern forensics tools for performing effective mobile forensics.

Learners will master the skills necessary to launch and complete a successful computer investigation with the updated fourth edition of this popular book, *GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS*. This resource guides readers through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. Updated coverage includes new software and technologies as well as up-to-date reference sections. Learn how to set up a forensics lab, how to acquire the proper and necessary tools, and how to conduct the investigation and subsequent digital analysis. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Perfect Reference for the Multitasked SysAdmin This is the perfect guide if network security tools is not your specialty. It is the perfect introduction to managing an infrastructure with freely available, and powerful, Open Source tools. Learn how to test and audit your systems using products like Snort and Wireshark and some of the add-ons available for both. In addition, learn handy techniques for network troubleshooting and protecting the perimeter. * Take Inventory See how taking an inventory of the devices on your network must be repeated regularly to ensure that the inventory remains accurate. * Use Nmap Learn how Nmap has more features and options than any other free scanner. * Implement Firewalls Use netfilter to perform firewall logic and see how SmoothWall can turn a PC into a dedicated firewall appliance that is completely configurable. * Perform Basic Hardening Put an IT security policy in place so that you have a concrete set of standards against which to measure. * Install and Configure Snort and Wireshark Explore the feature set of these powerful tools, as well as their pitfalls and other security considerations. * Explore Snort

Add-Ons Use tools like Oinkmaster to automatically keep Snort signature files current. * Troubleshoot Network Problems See how to reporting on bandwidth usage and other metrics and to use data collection methods like sniffing, NetFlow, and SNMP. * Learn Defensive Monitoring Considerations See how to define your wireless network boundaries, and monitor to know if they're being exceeded and watch for unauthorized traffic on your network. Covers the top 10 most popular open source security tools including Snort, Nessus, Wireshark, Nmap, and Kismet Follows Syngress' proven "How to Cheat" pedagogy providing readers with everything they need and nothing they don't

[Copyright: 5521ca6e17595812c8a0a54c6d7d82d5](#)