Dissertation For Computer Forensics

Eventually, you will extremely discover a extra experience and realization by spending more cash. yet when? realize you admit that you require to get those all needs later having significantly cash? Why dont you try to get something basic in the beginning? Thats something that will lead you to comprehend even more nearly the globe, experience, some places, next history, amusement, and a lot more?

It is your unquestionably own times to take action reviewing habit. in the middle of guides you could enjoy now is **Dissertation For Computer Forensics** below.

LACI GLOVER

Computational Intelligence in Digital Forensics: Forensic Investigation and Applications Springer
Scores of talented and dedicated people serve the forensic science community, performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.
Gathering Evidence John Wiley & Sons
Peterson's Graduate Programs in the Physical Sciences, Mathematics, Agricultural Sciences, the Environment & Natural Resources contains a wealth of information on colleges and universities that offer graduate work in these exciting fields. The institutions listed include those in the United States and Canada, as well international institutions that are accredited by U.S. accrediting bodies. Up-to-date information, collected through Peterson's Annual Survey of Graduate and Professional Institutions, provides valuable information on degree offerings, professional accreditation, jointly offered degrees, part-time and evening/weekend programs, postbaccalaureate distance degrees, faculty, students, degree requirements, entrance requirements, expenses, financial support, faculty research, and unit head and application contact information. Readers will find helpful links to in-depth descriptions that offer additional detailed information about a specific program or department, faculty members and their research, and much more. In addition, there are valuable articles on financial assistance, the graduate admissions process, advice for international and minority students, and facts about accreditation, with a current list of accrediting agencies.
Developing a Proactive Digital Forensics System Springer
This dissertation, "New Cryptographic Schemes With Application in Network Security and Computer Forensics" by Lin, Jiang, □□, was obtained from The University of Hong Kong (Pokfulam, Hong Kong) and is being sold pursuant to Creative Commons: Attribution 3.0 Hong Kong License. The content of this dissertation has not been altered in any way. We have altered the formatting in order to facilitate the ease of printing and reading of the dissertation. All rights not granted by the above license are retained by the author. DOI: 10.5353/th_b4475322 Subjects: Data encryption (Computer science) Computer networks - Security measures Computer crimes - Investigation Computer security Forensic sciences
A Study of Computer Forensics from a Cross-cultural Perspective Peterson's
Computer Forensics and Digital Evidence explains the relevance of computer forensics within investigations related to crimes which involve technological support. The paramount importance that technological innovations have gained in people's life is a signal of the necessity to acquire knowledges about them. This statement must be considered in regards to crime investigations, where an unlawful act could irremediably damage lives and rights. Experts in this area are constantly asked to improve their competence in regards to technological data collection, analysis, and conservation due to the difficulty to preserve them as a reliable proof in the Court. Although many difficulties still cause flaws within computer forensic investigations, the development of this branch of knowledge is increasing every day. This publication gives a detailed account of computer forensics from a scientific and legal point of view.
Social Networking and Computational Intelligence Peterson's
Photographic imagery has come a long way from the pinhole cameras of the nineteenth century. Digital imagery, and its applications, develops in tandem with contemporary society’s sophisticated literacy of this subtle medium. This book examines the ways in which digital images have become ever more ubiquitous as legal and medical evidence, just as they have become our primary source of news and have replaced paper-based financial documentation. Crucially, the contributions also analyze the very profound problems which have arisen alongside the digital image, issues of veracity and progeny that demand systematic and detailed response: It looks real, but is it? What camera captured it? Has it been doctored or subtly altered? Attempting to provide answers to these slippery issues, the book covers how digital images are created, processed and stored before moving on to set out the latest techniques for forensically examining images, and finally addressing practical issues such as courtroom admissibility. In an environment where even novice users can alter digital media, this authoritative publication will do much so stabilize public trust in these real, yet vastly flexible, images of the world around us.
Advances in Digital Forensics X Jones & Bartlett Learning

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.
Modern Cryptography Springer Nature
Computer forensics is the process of gathering and analyzing evidentiary data concerning a suspected digital crime. Traditionally, the tools and approaches for gathering and analyzing such data have all been reactive. Thus, they were only useful after an invasion, attack, or some other malicious act had been perpetrated. This dissertation examines the concept of proactive digital forensics, and specifically explores the possibility of creating a proactive digital forensics system.
Investigation Models for Emerging Computer Forensic Challenges Springer
Advancing technologies, especially computer technologies, have necessitated the creation of a comprehensive investigation and collection methodology for digital and online evidence. The goal of cyber forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device or on a network and who was responsible for it. Critical Concepts, Standards, and Techniques in Cyber Forensics is a critical research book that focuses on providing in-depth knowledge about online forensic practices and methods. Highlighting a range of topics such as data mining, digital evidence, and fraud investigation, this book is ideal for security analysts, IT specialists, software engineers, researchers, security professionals, criminal science professionals, policymakers, academicians, and students.
Strengthening Forensic Science in the United States Pearson It Certification
This dissertation, "Investigation Models for Emerging Computer Forensic Challenges" by Yuet-wing, Law, □□□, was obtained from The University of Hong Kong (Pokfulam, Hong Kong) and is being sold pursuant to Creative Commons: Attribution 3.0 Hong Kong License. The content of this dissertation has not been altered in any way. We have altered the formatting in order to facilitate the ease of printing and reading of the dissertation. All rights not granted by the above license are retained by the author. DOI: 10.5353/th_b4697132 Subjects: Computer crimes - Investigation Forensic sciences
Computer Forensics Methodology and Praxis Academic Conferences Limited
Over the decades, computer forensics has expanded from primarily examining computer evidence found on hard drives into the examination of digital devices with increasing storage capacity, to the identification of crimes and illegal activities involving the use of computers, to addressing standards and practices deficiencies, and to addressing the need to educate and train law enforcement, computer forensic technicians, and investigators. This dissertation presents the concept mapping case domain modeling approach to aid examiners/investigators in searching and identifying digital evidence and analyzing the case domain during the examination and analysis phase of the computer forensic investigation. The examination and analysis phases of a computer forensic process are two of the most important phases of the investigative process because the search for and identification of evidence data is crucial to a case; any data uncovered will help determine the guilt or innocence of a suspect. In addition, these phases can become very time consuming and cumbersome. Therefore, finding a method to reduce the amount of time spent searching and identifying potential evidence and analyzing the case domain would greatly enhance the efficiency of the computer forensic process. The hypothesis of this dissertation is that the concept mapping case domain modeling approach can serve as a method for organizing, examining, and analyzing digital forensic evidence and can enhance the quality of forensic examinations without increasing the time required to examine and analyze forensic evidence by more than 5%. Four experiments were conducted to evaluate the effectiveness of the concept mapping case domain modeling approach. Analysis of the experiments supports the hypothesis that the concept mapping case domain modeling approach can be used to organize, search, identify, and analyze digital evidence in an examination.
Digital Forensics, Investigation, and Response Springer
This edited book presents scientific results of the 20th IEEE/ACIS International Summer Semi-Virtual Conference on Computer and Information Science (ICIS 2021) held on June 23–25, 2021 in Shanghai, China. The aim of this conference was to bring together researchers and scientists, businessmen and entrepreneurs, teachers, engineers, computer users, and students to discuss the numerous fields of computer science and to share their experiences and exchange new ideas and information in a meaningful way. Research results about all aspects (theory, applications and tools) of computer and information science, and to discuss the practical challenges encountered along the way and the solutions adopted to solve them. The conference organizers selected the best papers from those papers accepted for presentation at the conference. The papers were chosen based on review scores submitted by members of the program committee and underwent further rigorous rounds of review. From this second round of review, 13 of the conference’s most promising papers are then published in this Springer (SCI) book and not the conference proceedings. We impatiently await the important contributions that we know these authors will bring to the field of computer and information science.
ICCWS2014- 9th International Conference on Cyber Warfare & Security Peterson's
Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information. With the proliferation of E-commerce initiatives and the increasing criminal activities on the web, this area of study is catching on in the IT industry and among the law enforcement agencies. The objective of the study is to explore the techniques of computer forensics from the computer security perspective. Specifically, the thesis looks into the application of forensic principles and techniques, security designs of computer hardware and software, and network protocols, in an effort to discover the trails of the computer hackers. The theses subsequently packages this knowledge into a curriculum for a twelve weeks resident course at the Naval Postgraduate School. Complementing the research and course materials are surveys conducted on agencies and vendors currently providing computer forensic courses and training, reading materials, and software tools applicable to computer forensic investigation. The purpose of these surveys is to provide a depository of useful information related to the specialized discipline of computer security.
Research in Computer Forensics Peterson's
Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence.

Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues Internet Crime Investigations Forensic Techniques Mobile Device Forensics Cloud Forensics Forensic Tools This book is the eleventh volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and prac tice in digital forensics. The book contains a selection of twenty edited papers from the Eleventh Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida in the winter of 2015. Advances in Digital Forensics XI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Computer Security Fundamentals Springer Nature

Over the past decade, wireless mobile communication technology based on the IEEE 802.11 Wireless Local Area Networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cybercrime. WLAN digital forensics is seen as not only a response to cybercrime in wireless networks, but also a means to stem the increase of cybercrime in WLANs. The main challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation on them. In an attempt to address this issue, the study presents firstly how a WLAN functions by simply studying the association mechanism between mobile stations and the Access Point (AP), and secondly how traffic is transmitted from a source to a destination address and the security attacks associated with such transmission. Furthermore, the dissertation analyses different digital forensic process models because every digital forensic investigation should follow a digital forensic investigation process. The study also looks at various tools for extracting the everincreasing amount of evidential data that passes through the WLAN. These tools are scrutinised to observe if they possess any digital forensic capabilities and a model is proposed to implement digital forensic readiness in WLANs. The proposed model is designed to monitor, log, preserve, analyse and report wireless network traffic for digital forensic investigations. Thus, the information needed by the digital forensic experts is rendered readily available, should it become necessary to conduct a digital forensic investigation. The availability of this digital information maximises the chances of its being used as digital evidence and reduces the cost of conducting the entire digital forensic investigation process. The proposed model is then translated into a prototype to show its viability. The results of the prototype are then analysed through experiments. The experiments were found to increase the usefulness of the forensically captured network traffic. The experiments showed that organisations that use WLANs can greatly benefit by deploying the forensic readiness model and if an incident were to be reported later on and a digital forensic investigation is warranted, the organisation would simple extract the forensically captured and stored data and conduct an analysis rather than conducting the investigation from the beginning. The dissertation also provides a critical analysis of the proposed solution and lastly, the dissertation provides the legal issues with regard to traffic interception in the South African context.

Proceedings of the 12th European Conference on Information Warfare and Security Springer

This thesis lays the groundwork for creation of a graduate-level computer forensics course. It begins with an introduction explaining how computing has invaded modern life and explains what computer forensics is and its necessity. The thesis then argues why universities need to be at the forefront of educating students in the science of computer forensics as opposed to proprietary education courses and the benefits to law enforcement agencies of having a computer scientist perform forensic analyses. It continues to detail what computer forensics is and is not. The thesis then addresses legal issues and the motivation for the topic. Following this section is a review of current literature pertaining to the topic. The last half of the thesis lays a groundwork for design of a computer forensics course at the graduate level by detailing a methodology to implement which contains associated laboratory praxis for the students to follow.

Digital Image Forensics Springer Science & Business Media

The suggestions for cross-cultural, cross-border and collaborative digital forensic investigations can be provided based on the discoveries of this research. This thesis essentially helps the mutual understanding between Australian and Taiwanese computer forensic investigators. The understanding is able to improve the chances of success of future cooperation between Australia and Taiwan.

A Concept Mapping Case Domain Modeling Approach for Digital Forensic Investigations Open Dissertation Press

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XVIII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: This book is the eighteenth volume in the annual series

produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of eleven edited papers from the Eighteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, a fully-virtual event held in the winter of 2022.

Cyber Investigations Pearson IT Certification

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics X describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: - Internet Crime Investigations; - Forensic Techniques; - Mobile Device Forensics; - Forensic Tools and Training. This book is the 10th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-two edited papers from the 10th Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Vienna, Austria in the winter of 2014. Advances in Digital Forensics X is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

Computer and Information Science 2021—Summer Wolf Legal Publishers

Peterson's Graduate Programs in Engineering & Applied Sciences contains a wealth of information on colleges and universities that offer graduate degrees in the fields of Aerospace/Aeronautical Engineering; Agricultural Engineering & Bioengineering; Architectural Engineering, Biomedical Engineering & Biotechnology; Chemical Engineering; Civil & Environmental Engineering; Computer Science & Information Technology; Electrical & Computer Engineering; Energy & Power engineering; Engineering Design; Engineering Physics; Geological, Mineral/Mining, and Petroleum Engineering; Industrial Engineering; Management of Engineering & Technology; Materials Sciences & Engineering; Mechanical Engineering & Mechanics; Ocean Engineering; Paper & Textile Engineering; and Telecommunications. Up-to-date data, collected through Peterson's Annual Survey of Graduate and Professional Institutions, provides valuable information on degree offerings, professional accreditation, jointly offered degrees, part-time and evening/weekend programs, postbaccalaureate distance degrees, faculty, students, degree requirements, entrance requirements, expenses, financial support, faculty research, and unit head and application contact information. As an added bonus, readers will find a helpful "See Close-Up" link to in-depth program descriptions written by some of these institutions. These Close-Ups offer detailed information about the specific program or department, faculty members and their research, and links to the program Web site. In addition, there are valuable articles on financial assistance and support at the graduate level and the graduate admissions process, with special advice for international and minority students. Another article discusses important facts about accreditation and provides a current list of accrediting agencies.

Advances in Digital Forensics V Springer Nature

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images Features real-word examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.