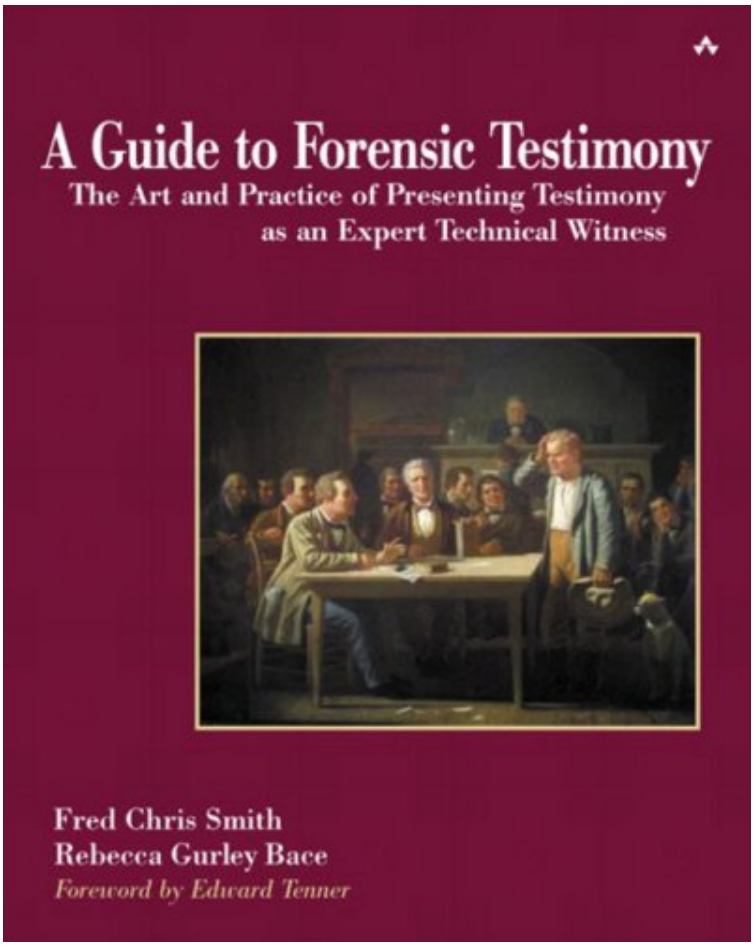
A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness

Fred Chris Smith, Rebecca Gurley Bace
*ePub | *DOC | audiobook | ebooks | Download PDF*



#1063313 in Books 2002-10-19Original language:EnglishPDF # 1 9.00 x 1.30 x 7.30l, 2.06 #File Name: 0201752794560 pages | File size: 28.Mb

Fred Chris Smith, Rebecca Gurley Bace : A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness before purchasing it in order to gage whether or not it would be worth my time, and all praised A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness:

0 of 0 people found the following review helpful. Too little known effort that explains the essence of forensics testimonyBy Jerry SapersteinThis is an under-appreciated book. I've met only one person in my area (computer forensics) who had heard of it. Of all the lawyers, judges and other forensics experts I've mentioned it to, none had ever heard of it - which is a pity. This book attempts to explain what an expert technical witness does and how they should be employed. The lay public, in general, has a distorted view of the value of forensic data and how it is used.

While the general press is loaded with stories of DNA, the more mundane aspects of forensics deal with things like why a metal support may have failed or, in my area, determining if certain data existed in a computer storage device. Billions of dollars can be at risk when a technical expert witness testifies - and all too often, the witness, the lawyers, the judge and (if there is one) the jury are clueless to some extent. This book tries to educate the technical expert witness as to their responsibilities to the court. Most expert witnesses I've encountered don't have a clue as to the judicial rules they operate under: this book, much to its credit, explains the basics. "A Guide To Forensic Testimony" does have it weaknesses. It tries to cover too much territory, I think, such as "non-verbal communication". While telling someone not to pick their nose while testifying is important, this kind of book may not be the appropriate place. (The example, by the way, doesn't appear in the book, but the suggestions offered are just as elementary.) On the whole, this is an interesting, helpful book which every technical expert who may be called upon to testify would benefit from reading. Be prepared, however, for a slow read. The authors' writing style is a bit pedantic.Jerry0 of 0 people found the following review helpful. Valuable insight.By anthony scarbroughMust have for forensic examiners. Regardless of your discipline, this books give valuable insight.0 of 0 people found the following review helpful. Five StarsBy AnonymousGreat buy. Great price.

Information technology is an increasingly large factor in legal proceedings. From large cases, such as the US Government's anti-trust suit against the Microsoft Corporation, to small civil lawsuits filed over the failure of a network, to criminal cases in which the authenticity of electronic evidence is questioned, the testimony of a technical expert is essential. But an understanding of the technology in question is not enough; an expert technical witness needs to understand much more in order to ensure the effectiveness of his or her testimony.

From the Back CoverInformation technology is an increasingly large factor in legal proceedings. In cases large and small, from the U.S. Government's antitrust suit against Microsoft Corporation, to civil lawsuits filed over the failure of a network, to criminal cases in which the authenticity of electronic evidence is questioned, the testimony of a technical expert is essential. But in order to be effective, an expert technical witness needs much more than an understanding of the technology in question. A Guide to Forensic Testimony is the first book to address the specific needs of the IT expert witness. It will arm you with the tools you need to testify effectively. Inside you'll find everything from an overview of basic witness responsibilities and challenges to a deeper exploration of what produces successful technical testimony. Written by a computer security authority who has served as a technical witness, and a trial attorney who focuses on how digital evidence and computer forensics are altering litigation, this book is your guide to the complicated forensic landscape that awaits the expert technical witness. This book contains a wealth of wisdom and experience from the front lines, including firsthand accounts of the challenges faced by expert technical witnesses, practical in-court examples, and helpful advice. Among the topics covered are: The evolution of the expert IT witness and the growing legal dependence on technical expertise Legal criteria established to determine the qualifications and abilities of a technical expert to stand as a witness The kinds of cases and problems that are apt to be encountered in digital forensic assignments Damage caused when the rules of professionalism and ethics are ignored or misapplied The construction and maintenance of a solid professional relationship between expert and attorney The creation and use of visual tools in courtroom testimony Ways to improve the demeanor and non-verbal communication skills of the technical witness Whether you are an information technologist asked to serve as an expert witness, a legal professional who works with information technology experts, a corporate risk manager, or a client whose interests are affected by the performance of IT experts, you will benefit greatly from A Guide to Forensic Testimony . 0201752794B09092002About the Author Fred Chris Smith is an experienced trial attorney who directed economic crime prosecutions for four consecutive New Mexico state attorneys general. For nearly twenty years he has also provided education and training programs throughout the country and abroad, in digital evidence and computer forensics. He has been involved as an attorney, business advisor, and teacher with information technology and legal professionals who are encountering the rapidly changing problems presented by electronic evidence in criminal cases, in the investigation of corporate network fraud and abuse, and in civil litigation. He currently serves as an Assistant United States Attorney. Rebecca Gurley Bace is a recognized network security authority and consultant. Her career includes work with the National Security Agency, where her contribution to building the national intrusion detection research community earned her an NSA Distinguished Leadership Award. After the NSA, she became the Deputy Security Officer for the Computing Information and Communications Division of the Los Alamos National Laboratory, where she was responsible for one of the world's most complex security-critical computing environments. She is currently President/CEO of Infidel, Inc., and a Venture Partner for Trident Capital. Bace is the author of Intrusion Detection (Macmillan Technical Publishing, 2000). 0201752794AB06252002Excerpt. Reprinted by permission. All rights reserved. Mark Twain is reported to have said, "An expert is just some guy from out of town." As usual, Twain is on the mark in suggesting that there should be something suspicious about a stranger who shows up and offers to help us with his expertise and then quickly hits the road. For our purposes this apothegm could be slightly altered to make an expert out to be someone from out of town who has an opinion. The revised adage may say as much

about communities of interest and the part they play today in deciding whom to trust as an expert as it says about experts and how they worked in Twain's era. This book is all about expert witnesses, with particular attention paid to those who specialize in information technologiesthe hardware, software, and data that make up computers and other digital systems used for data processing and communications. The level of technical knowledge needed to deal with these systems often makes the question of assessing the expertise of a particular person daunting to all but other experts in the technical domain in question. This is not by any means meant to be a legal textbook. Indeed, we explicitly disclaim any intention to offer or suggest legal advice to any reader. Such legal advice must come from legal counsel engaged to offer it, and the materials in this book should not be relied on as legal advice or passed onto others as such. Nor is this book meant to be treated as yet another technical manual, to be consulted only when the reader is in the midst of a crisis and in search of specific answers to specific technical problems. The book is perhaps best considered as analogous to a general travel guide to an exotic destination that the reader anticipates visiting in the near future. We appreciate the paucity of time available for technical experts to devote to reading a book such as this. Accordingly, although the book attempts to convey neither legal advice nor specific technical information, the chapters should still prove useful to the techie and his or her managers. The chapters can guide the consideration of "what if" scenarios that may well come to pass in the lives of many who read this book. Furthermore, like a travel book, this primer may at least provide some of the right questions (asked in the appropriate local dialects) that an expert can use to ask for directions as he or she navigates to the interesting places and events often found in the world of litigation. One of many ways you might use this book to prepare for visiting the land of litigation as an expert is to begin with the first chapter to get a quick and entertaining overview of the process of becoming a recognized expert and testifying in court. Chapter 1 introduces technical expert witnesses who testify in criminal and civil trials and focuses on the communities of interest that society ultimately relies upon to certify the genuine expertise of their representatives and members in good standing. When you begin to think about what makes a particular individual an expert in the eyes of the law, and hence entitled to testify about his or her opinions in the course of litigation, you are led back to the specialized knowledge, training, and experience that an organized and socially recognized community of interest creates and maintains. The most peculiar thing about the technical domains that comprise what is generally described as information technology (IT) is how little they resemble the traditional, professional, licensed communities of interest that exist in other areas, such as structural engineering and medicine. These communities become important to the law as it tests the reliability of the expert and his or her methods. Most judges and jurors first hear about such communities when a community member is proffered as an expert witness in the course of litigation. For IT expert witnesses, the lack of an organized, licensed community of interest with the traditional trappings of a socially recognized expert community creates a number of issues that the courts are just beginning to confront. We introduce established experts from a number of communities of interest that lie outside the realm of IT. These experts within ancient areas of expertise as well as new disciplines have coped with the special demands of the legal system. Their stories may provide some organizing analogies for IT professionals who become interested in forensic practices and also enable IT experts to build the lattice of disciplines, processes, and professional networks necessary to assure lawyers and courts that they are competent IT practitioners. The experiences of Raemarie Schmidt and her students bring us back to how some of the pioneers in IT forensics can contribute to recognized expert communities by developing standards and training that have become generally recognized by the courts. A discussion of the film My Cousin Vinny offers a lighthearted account of the problems that a technical expert encounters while testifying in court. In the film, the community of expertise represented by the character Mona Lisa Vito (played to perfection by Marisa Tomei) is that of the automobile mechanic. This particular community reminds us that certain roles associated with IT are rapidly becoming as commonly accepted as those of the car mechanic or washing machine repairperson. That these areas of expertise are generally recognized and often encountered illustrates another aspect of the community of interest. In this scenario, too many members claim an expertise with too little self-regulation, peer review, and evaluation by a recognized community of professionals. This erodes the ability to separate the charlatans from the qualified and recognized practitioners of the IT trades. The choice of a second chapter is not critical to making the best use of this guide. In fact, the techie reader may wish to go directly to Chapter 13, which includes the experiences and lessons learned by several accomplished IT experts. These technical experts, who are all widely recognized as such in their communities of interest, have varying degrees of experience as expert witnesses in criminal and civil litigation. Their observations can serve as either reviews or introductions to the chapters found between the first and the last. Chapter 2 provides a real-world tale of just how serious this kind of communication performance can be to individual and corporate parties. This chapter also explores the kind of expectations that legal and IT social critiques bring to bear on performances by important IT witnesses in landmark cases. Passages from the deposition of Bill Gates in the Microsoft antitrust case introduce a number of the recurring themes and issues associated with expert testimony developed further in the rest of the book. The most important of these is the perception of the demeanor and overall credibility of the witness and his or her performance on the stand. This perception by the fact finder overrides, as it should, all the other components of the process of communicating complex concepts in formal testimony. The return of Bill Gates to the witness stand two years later (and the dramatic change in the reporting of his second coming by the

same IT and legal reporters) is an example of the point of this book. Judicial fact finders and the public have lofty expectations of experts, especially when the expert's testimony is key to understanding the merits of the case. Meeting those expectations requires certain things from the expert: experience, preparation, and a commitment to communicating not only the obvious expertise of the witness but also the credibility and willingness to provide useful information throughout the testimony. This set of requirements might appear excessive, but in certain cases, such as Gates', the members of the public with interest in the expert's testimony number in the millions. Chapter 3 reprises the well-known story of how IT security experts Tsutomu Shimomura and Andrew Gross developed forensic tools to track down the hacker who broke into Shimomura's computer at the San Diego Supercomputer Center. The text recounts the investigation in the form of a hypothetical direct examination of Andrew Gross as the government's expert witness and illustrates the case with graphics designed to introduce and narrate the complex technical steps taken in the investigation. The sample testimony also explains the expert analysis of the computer network evidence used to establish that Kevin Mitnick was the original intruder and to account for how he came to possess the stolen computer data taken from Shimomura's computer. Chapter 4 provides some historical background, outlining the evolution of the legal process and also exploring the growing importance of expert witness testimony that accompanies the evolution of society's dependence on technology. The different roles of the expert witness as consultant, strategist, and testifying witness are introduced along with some of the problems that can arise when the expert and his or her attorney do not keep these often conflicting roles clear and distinct throughout thecourse of litigation. Chapter 5 gives the beginning expert several examples by analogy of the kinds of problems that may persist due to the pace of advances in IT. Some of the problems are considered to be a direct consequence of the inherent immaturity of the IT field. In particular, issues arise in areas where no rigorous community of interest has been established or where no formal education or training is available. In these cases, the expert cannot point to generally accepted standards or a formal peer review process for determining the reliability of the concepts and techniques that he or she uses to decide what happened in a given case. Discussions of astrologers, phrenologists, handwriting analysts, and fingerprint comparison experts and their communities of interest illustrate the kinds of problems that IT domain experts may encounter when their expertise is challenged in court. Chapter 6 provides examples, many of them extreme, of what can go wrong when commonsense rules of professionalism and ethics are misapplied. It also outlines how the traditions of the legal system regarding the preparation and introduction of expert testimony place certain restrictions on the behavior of IT and other experts who perform expert witness tasks in the course of litigation. Expert witnesses must understand that while in civil litigation they ultimately work for a private party, through their legal counsel, the advocacy decisions made by the party and the attorney about the course of litigation must be segregated from the objective judgments that legal and professional ethical rules require expert witnesses to make about the application of their expertise and the communication of their opinions in court. Chapter 7 shows how some experienced IT experts have handled the challenging task of solidly constructing and maintaining the professional relationship between the expert, the attorney, and the client or party. One of many metaphors for enabling both the lawyer and the expert to reach useful conclusions about issues within the expertise of the witness is an aviation checklist. In this analogy, the expert must learn a lot about his or her role before he or she can reliably check out all the things that need to be in working order and notice all the indicators of problems before taking off. Another approach that has worked for both beginning and experienced IT expert witness practices is to find an agent or agency that specializes in matching appropriate experts with legal teams requiring particular expertise. Chapter 8 presents what is in some ways the most difficult information in the bookinvolved legal material that explores the kinds of criteria courts have established for expert witnesses in general. The legal approach to screening expert witnesses has undergone significant change over the past decade through a series of Supreme Court decisions. The result of this series of decisions, starting with the landmark case Daubert v. Merrell Dow Pharmaceuticals, is that an expert must now pass additional tests in order to testify as an expert. The major differentiation between the old and new qualification processes for expert witnesses involves the addition of a "gatekeeper" function, assigned to trial judges. Although it may be difficult for techies to master the cases and the analysis of the legal issues concerning the gatekeeping duties of trial judges, it is crucial for the beginning expert to understand how the decision to allow a proffered expert to testify at a hearing or trial is made in different courts across the country. A Note on Legal Documents In some of the opinions, rules, and other legal documents cited throughout the book, we took the liberty of editing inline references from the quoted material. We performed this editing for the sole purpose of making the material easier to read and comprehend for readers unaccustomed to reading legal documents. We provide full case references (and for some cases, the complete opinions) in Appendix A in case you want to go to the source. The gatekeeping function that most courts have now accepted in one form or another is a distinct departure from the traditional role of the courts with regard to the use of experts. Under the old system, the courts passively allowed attorneys to proffer their chosen experts, allowing the jury to decide what weight to give to the respective witnesses' opinions. In the post-Daubert world, the judge acts as a gatekeeper, charged with weeding out unqualified experts as well as qualified experts who deliver unreliable opinions irrelevant to the particular case at hand. A process enabling adversaries to challenge the qualifications or relevance of a particular expert often triggers this function. The challenges are conducted in addition to and in advance of the more traditional impeachment of

witnesses through cross-examination. This expert qualification and challenge process requires additional work on the part of expert witnesses. First, the expert needs to consider whether he or she is adequately qualified by education, training, and experience to investigate and testify about particular matters before the court. While acting as an expert witness, the expert must also keep abreast of legal developments and make additional efforts to determine all that will be involved in a particular assignment. The expert may also need to determine how a soliciting attorney has dealt with past cases in which judges have entertained gatekeeping challenges against other judges. The expert must accept additional responsibility for anticipating and dealing with serious challenges to his or her qualifications and expertise. Finally, the expert must understand this rapidly changing body of case law on the fly since it has only recently been used to challenge IT experts. The good news is that experts don't have to take this on all by themselves. All competent trial lawyers can be expected to keep up with the most recent changes in the way this challenge round is evolving in their jurisdictions and should be able to explain it clearly to the beginning expert. The information in Chapter 8 is presented in hopes that it will enable IT experts to pose relevant and concise questions about this new area of the law and at the same time prepare them to better understand the significance of the legal advice they receive from trial counsel concerning these new developments and their impact on the performance of the witness. Chapter 9 provides detailed examples of how judges look at qualifications and the different approaches taken by the witnesses when deciding between competing theories and methods of opposing experts, as in the landmark case of Gates v. Bando, which established one of the practice standards for computer forensics. The testimony of Robert Wedig, the expert witness for the defendant who prevailed in that case, illustrates the factors affecting the judge's decision to favor Dr. Wedig's opinion over that of the opposing expert. The historical example of Houdini illustrates the different roles of the expertboth as a performer, demonstrating a known expertise, and as a skeptic uncovering the abuse of known techniques used by an opposing expert to obfuscate the facts or deceive the fact finder. One of the most important tools that any IT expert can employ in court is a visual display. Chapter 10 explores the subject of graphic images in detail and provides a visual metaphor to allow the beginning expert to think about the entire process of approaching a technical problem involved in litigation through the eyes of graphics designers. The litigation graphics consultants who work with lawyers and their technical experts enable them to focus on the most important concepts and to organize their presentations with visual aids. The resulting visual displays vastly enhance the expert's ability to communicate the analysis and conclusions to judges and juries. We have selected several examples of the work and the methodology that Chris Ritter, a former litigator who now works for The Focal Point, LLC, has developed to assist both lawyers and expert witnesses in preparing for court. Although experts are often tempted to focus on the content of their testimony, in court the context of testimony is also very important. This means that even the most brilliant and accurate technical analysis may not be accepted if the demeanor and nonverbal communications skills of the expert witness are lacking. Chapters 11 and 12 contain various analogies and techniques for improving the ways that expert witnesses integrate their demeanor and nonverbal communication with their testimony. With all the provisions and restrictions of the legal process outlined, Chapter 13 provides a wealth of wisdom from the front lines. The chapter presents the advice of three noted IT experts with different degrees of experience. Professor Rebecca Mercuri, a world-renowned specialist in the area of voting technology, offers insights gleaned during a decade of testimony in a wide variety of cases, ranging from a murder trial to the appeal of the 2000 U.S. presidential election results in Florida. Don Allison, whose expertise in the discovery and analysis of digital evidence has placed him on the stand in a number of cases, offers his feedback loop methodology that not only carries him through the trial process but also allows him to refine his expert witness skills. Finally, Professor Gene Spafford, noted for his accomplishments in the software engineering and network security area, offers insights gained testifying in cases involving allegations of intellectual property theft and patent infringement. For many technical experts, manuals and guides serve as references of last resort. These technical gurus enjoy and excel at learning by doing and may welcome the first opportunity to testify as an expert witness as similar to learning a new programming language or system troubleshooting technique. Unfortunately, they often fail to gauge the complexity of the preliminary processes required to get to the moment of truth, when the expert actually explains a technical process to a judge or jury. Furthermore, testifying in a serious legal controversy may be one of the few situations a technical expert will encounter where he or she must prepare for battle. At a minimum, the expert needs to read some rules and some literature before being cross-examined by a lawyer who has spent months preparing to call into question the testimony the expert plans to give. Even with that preparation, the best-planned testimony has a way of making some dramatic detours and complete changes in direction when subjected to crossexamination by an experienced trial lawyer. The expert must assume that the lawyer has had the benefit of reading all the available literature and of being prepared by an equally qualified expert of his or her own.As Bill Spernow (a widely recognized expert in many IT domains) likes to say, "This is not something you can afford to learn by doing, at least if you plan to testify more than once in your life." Spernow proposes that the topic addressed by this book is actually a prime example of the age-old question: "How do you get techies to read the manual before they jump in with both feet and try to make something work?" This is an especially important question for those in IT, where the archetypical personality thrives on improvising solutions in the trenches and getting code and systems to work by tinkering with them, not by formally planning ahead. Spernow also asks whether or not this kind of

perspective would ever fly within the legal community, where ritualistic procedures and time are such serious and constant constraints. Spernow is certainly right to raise these issues about the kind of fit that can be expected between techies and attorneys, and he is correct in his suspicion that it was more likely the legal system and not Benjamin Franklin who first coined the phrase "Time is money." Besides their time, lawyers keep track of the performances of expert itnesses. Even if experts have not yet started to monitor their peers and to evaluate their performances in the courtroom or in recorded depositions, lawyers have created their own networks for efficiently sharing this accumulated wisdom as to whom to trust as an expert in an IT-related case.Make no mistake, the record made of an expert's performance will be consulted to determine whether lawyers can rely on the expert in any future litigation for which they are being considered. The legal profession may not easily understand or embrace the ways of the techie who prefers to tackle problems on the fly. Lawyers may not care about the techie's demonstrated success in using these methods to solve a purely technical problem. It is much more likely that, should the techie decide to play this expert witness game, he or she will need to understand the perspectives of lawyers and judges and consider making certain accommodations to the ritualistic and traditional procedures that the legal process brings with it. Furthermore, the techie must understand and accommodate the accompanying constraints on his or her freedom and time. Consider the function of this book to be twofold. First, a number of the chapters of this book are primarily concerned with acquainting the technical expert with this very different world by using various analogies, cases, and stories of the involvement of other techies in the litigation game to accomplish this goal. Secondly, there are recommendations and tactics for dealing with specific challenges that the legal system presents to the technical expert. It is our hope that this combination of features will eliminate many of the potential headaches you might face as a techie headed for your day in court. James Boyd White, a law professor and respected author, wrote: The law can be seen as a particular instance of a human activity that is far more widespread than law itself, and of which we have splendid exemplars from which to learn: the activity of making meaning in language in relation to others. To see law this way opens a whole set of issues for analysis in the law (and in other instances of meaning-making too): the quality of the language that a particular person inherits and uses; the nature of her transformation of that language in her use of it; and the kind of relation she establishes with the people she speaks to or about. In several thousand times as many words, this book attempts to explain the significance of Mark Twain's single, cynical quote and to do it with the optimism and hope of Professor White. At the outset, we want to make clear that, unlike Samuel Clemens, we are not professional writers, humorists, or entertainers extraordinaire. If we could have figured out how to make a living being professional philosophers, we would have done so already. Instead, we chose to pursue careers in the fields of information technology and law. Nor, in retrospect, are we as clear as we would like to be about the points we set out to make in all these pages. The problem that brought us together to write this book emerged from doubts about the ability to communicate the idealistic goals tempered by the cynical observations that color the world of the expert witness. We concluded that simply sending something as wonderful as the Twain quip and as thoughtful as the White quote to all the potential technical experts who had asked us for advice would be viewed as inadequatethey would still need a path to follow. So, the main impetus for writing this book is to define some paths that can allow technical experts to more easily gain an understanding of why it is critical for those qualified and capable to join the fray. In doing so, they contribute to White's "making meaning in language in relation to others" involved in the litigation of IT issues. Our subject, then, is the art of presenting effective IT expert witness testimony. This testimony, in the best case, enables a judge or juror to make meaning in relation to complex technical concepts involved with information technologies. This art in turn enables the fact finders in litigation to relate that meaning to an important controversy in order to make sound judgments about it. And yet Twain must keep bringing us back with his words to the way we suspect things really are in the world of litigation. And we realize that we must deal with that as well.No one wants to be perceived as a circus clown in a setting where everyone else is pretending to be serious about another game. Our suspicion that we are being foolish or that we will be made the fool by following White in his optimism about the law and our legal rituals makes it all the more difficult to sustain this essential optimism for honest experts to give command performances. Yet the sustained effort to communicate carefully and objectively the professional experiences and special knowledge true experts and great trial lawyers wish to share with others is not difficult to justify. It is both the essence of the scientific method and the most rewarding kind of trial advocacy. We have chosen to undertake the job of overcoming the cynical force of Twain's apothegm with analogies, metaphors, stories, disciplines, opinions, and anecdotes. It is our hope that the humor of some of these stories and the insights and analysis of other experts will go some way in overcoming that convenient cynicism. There will always be those who would rather remain uninvolved, while technical experts and their lawyers increasingly command the center stage of a growing number of legal performances. Our hope is that the number of those temporarily on the sideline will be reduced by some who are encouraged and challenged by the materials collected in this primer. 0201752794P09272002