# Preface

The overwhelming importance and proliferation of computers in the last few decades have no doubt created a massive industry, all under the umbrella term of "software." The ever-increasing importance and complexity of computer software has invariably made it one of the most influentially desired, and coveted commodities. Perhaps unsurprisingly, one of the most prominent side effects of this importance has been efforts to steal and/or appropriate software unethically and illegitimately: in other words, the emergence of software piracy and software copyright infringement. The core area of the book is the forensics of software copyright infringement.

Any software is (or consists of) a collection of code segments, and each code segment is an expression of one or more ideas. This being so, software, as a whole, can be considered a collection of expressions of one or more ideas. Just as for any other idea, these software ideas can also be, and indeed are, copyrighted, thereby bringing it under the purview of intellectual property. When copyrighted software is illegally duplicated (with or without actually pirating the software), the copyrighted ideas and expressions contained therein are also illegally duplicated. In the event of illegal duplication, the owner of the copyright may approach investigation agencies or the judiciary for legal redress. The investigation agency/judiciary, in turn, would seek the help of cyber forensic experts in order to establish and confirm piracy or copyright infringement, as part of the forensic procedure. This book addresses the theoretical, functional, and procedural aspects of matters in the investigation of software piracy (or software copyright infringement).

This book envisages software piracy (or copyright infringement) as a cyber crime and mostly looks into what cyber forensic experts need to know while assisting the law enforcement agencies to establish culpability in the official investigation of a software piracy or copyright infringement suit. As the forensics of software copyright infringement is a judicial task, legal professionals, including the judicial officers/judges, also are to be made aware

of the protocols for investigating such cases because they are expected to use the forensics results appropriately for achieving a high degree of accuracy in legal deliberations. The book addresses these forensic demands.

Establishing software copyright infringement legally and judicially involves a forensic process, which demands a high degree of awareness of the theory and practice of computer science and engineering. As part of their forensic tasks, the forensic experts may have to obtain millions of codes, hundreds of databases, images, and other related segments of the software of both the complainant as well as the accused (through voluntary disclosure or even through a police raid, sometimes, and often even from their client organizations). The experts then may have to sift through these pieces of software segments separately, and finally compare the two sets of software segments in a scientific manner to obtain the required evidence to establish copyright infringement. Hence, this forensic task is complex, voluminous, as well as Herculean. This investigative process will end up with the reporting of the evidence to the court of law by the expert. In most cases, the expert will then have to appear in court as a witness. The judiciary generally expects the forensic results to be presented (both in the expert report and also during the expert witness trial) by the expert in a non-esoteric, jargon-free, and judiciary-friendly manner, though the judiciary is not barred normally from being literate in this forensic technology. Hence, it is both crucial and necessary for the expert's report and other presentations to be as thorough, authentic, and convincing as possible in the interest of proper justice. The implications of the proceedings and activities of this forensic process may not only affect the involved parties, the law enforcement personnel, and the judiciary, but also the (large group of) clientele of the affected parties. Hence, these involved parties, law enforcement personnel, legal officers, software developers, as well as the software users, should be properly informed of these matters. With all these points specifically in view, the book explains all the involved and required procedural aspects clearly and in a lay-friendly manner, and is therefore expected to guide the judicial (and the investigation) officers in the procedural aspects of software copyright infringement forensics.

This material of the book is so arranged to address, at many levels, the techno-legal context of software piracy and copyright infringement. The content covers the processes, procedures, proceedings, activities, reporting, and implications related to the forensic technology for establishing software copyright infringement forensics. Firstly, it introduces the field of cyber forensics and software piracy briefly but clearly to set the context. Secondly,

it gives a comprehensive overview of current research into the area of cyber forensics, and in particular, forensics of software copyright infringement. Thirdly, it provides the relevant insight into the implications of software piracy or copyright infringement leading on to its legal fallout. Fourthly, it explains in detail the litigational aspects of the software forensic practice. Next, it discusses the means and procedures of seeking legal redress in the context of allegations of such piracy and copyright infringement including prevalent globally accepted technical and practical procedures (and also the modern trends) of establishing it. Then, it discusses in detail the pragmatic improvements in validating the procedural aspects in the seeking of legal redress. Finally, it explores ways and means of making the techno-legal process and praxis friendlier and less esoteric to the judiciary and to the involved community at large.

One main objective of the book is to guide people interested in the investigation of software copyright infringement cases, and in particular, the cyber forensic expert, on procedural matters related to software copyright infringement forensics. The material in this book should certainly help them to collect evidence of copyright infringement from the ocean of the software codes and to present these pieces of evidence in a judiciary-friendly manner. In this perspective, the book would serve as a basic primer for forensic experts, investigation officers, and judicial officers.

This book is not just a basic primer. It also ventures to cater to the additional forensic demands of the fast expanding, state-of-the-art software technology.

In addition, the book underscores the importance of incorporating the currently under-valued process of the manual component when comparing two software packages. Such manual elements can successfully address not only comparison-issues related to various parts of the software like source code, object code, databases, and fingerprints (like most existing tools do) but also other piracy-related issues like post-piracy modifications, design patterns, and data piracy (which have already been accepted by modern researchers but are hardly or inadequately addressed in existing books).

The book additionally takes upon itself the task introducing not only the established (legacy) testing procedures but also the state-of-the-art procedures, which are better equipped for the forensics of modern software. In other words, the book emphasizes the need to update existing methods, and it suggests precise ways of doing this by featuring state-of-the-art forensic procedures for investigating software copyright infringement. As such, the book contains introductions and explanations to as well as procedural aspects,

functional aspects, advantages, and disadvantages of each of these protocols so that the content is transparent to a wide spectrum of readers, say, from a law student to a judge and a forensically uninitiated computer science student to a cyber forensic expert.

In a nutshell, this book ultimately aims at explaining all methods and protocols of software copyright infringement forensics for technical experts to practically carry out judicial software piracy forensics. The book's aims are not just the narration of or guidance to the expert's modus operandi, but also to plug the holes in the current practices, and above all, to break down the esotericism of the field to make it accessible to the judiciary and non-professional personnel involved. To be precise, the ultimate objective of this work is to explain the procedures of various software copyright infringement forensic methods that help the police, jurors, and lawyers to establish culpability with the help of technical experts. The absence of such a comprehensive book is often felt in the industry, and this book is intended to fill the gap due to this absence.

This work is expected to be of immediate use to (1) software forensic experts, (2) lawyers specialized in legal aspects of copyright infringement, (3) judges, (4) software professionals, and (5) software development firms. In addition to these, the work is expected to be of immediate help to students pursuing courses in General Law, Digital Law, or Cyber/Digital Forensics, as the syllabi of Bachelor/Masters/Ph D programs in Computer Science, Computer/Digital Forensics, Law, etc. have been amended with copyright infringement forensic aspects.

*Vinod Polpaya Bhattathiripad*
*G J Software Forensics, India*