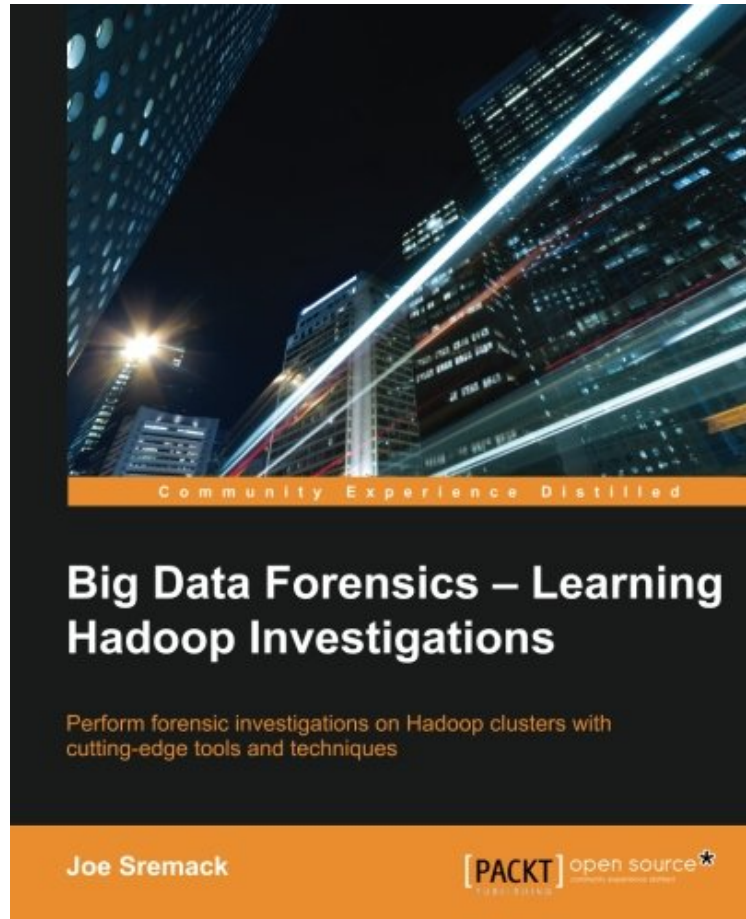


(Get free) Big Data Forensics: Learning Hadoop Investigations

Big Data Forensics: Learning Hadoop Investigations

Joe Sremack

ebooks | Download PDF | *ePub | DOC | audiobook



DOWNLOAD



READ ONLINE

#3571318 in Books 2015-09-01 2015-08-24Original language:EnglishPDF # 1 9.25 x .60 x 7.50l, 1.01 #File Name: 1785288105296 pages | File size: 70.Mb

Joe Sremack : Big Data Forensics: Learning Hadoop Investigations before purchasing it in order to gage whether or not it would be worth my time, and all praised Big Data Forensics: Learning Hadoop Investigations:

1 of 1 people found the following review helpful. The book you need if you need to do the forensic of an Hadoop system!By DavidThe first comment is: read correctly the title ;). A book on using big data for forensic would be great but that book is on doing forensic on big data :-D. Still, it is a topic of interest for people doing forensic and probably a must-have whenever you are confronted to the case. I suspect that this would happen once in every forensic analyst life and probably more and more as data goes to "cloud" and "big-data" storage.The book itself start with a description of Hadoop which is use for the book and on general principles. Then it cover more in details what you can expect to do and recover out of an Hadoop instance. I highly suspect that you could generalise and take profit of the work of the author for author big data systems even if not the primary goal of this book.As a con, I would say that there is a lot of text and discussion in the first half of the book and not enough examples and cheat sheet. If you need to start quickly, probably you could jump to the 2nd half of the book. Be careful that if you don't fully understand underlying concept you could potentially make a mistake and destroy your case.The author take the risk of covering the topic and it's nice.

In a futur release or in a side book maybe he can cover more techniques, examples and demos but the book has the merit to exist and it contains a lot of good work!0 of 0 people found the following review helpful. Great book. Really interestingBy javier vicho sotoGreat book. Really interesting, both if you're working in forensic roles or you're a data professional working with hdfs / hadoop.You will have a lot of useful information in case of disaster recovery by example, in a way that is easy to extract all the relevant info from hdfs or hadoop applications. Very interesting the section about the deep analysis on HDFS, and the most useful tools available.In resume, amazing ebook if you want to know how to perform a deep and reliable investigation on Big Data side.0 of 0 people found the following review helpful. Learn how to use Hadoop to Take your Forensic Analysis to the Next Level!!!!By WinstonBig Data is all the rage today. Each day consumers are leaving big data footprints whether it is from internet use or other distributed computer systems. This book answers the question of how does one go about analyzing big data in a useful way.Note: This book is all about using Hadoop for forensics analysis of Big Data not just Big Data use cases.

Perform forensic investigations on Hadoop clusters with cutting-edge tools and techniques About This Book Identify, collect, and analyze Hadoop evidence forensically Learn about Hadoop's internals and Big Data file storage concepts A step-by-step guide to help you perform forensic analysis using freely available tools Who This Book Is For This book is meant for statisticians and forensic analysts with basic knowledge of digital forensics. They do not need to know Big Data Forensics. If you are an IT professional, law enforcement professional, legal professional, or a student interested in Big Data and forensics, this book is the perfect hands-on guide for learning how to conduct Hadoop forensic investigations. Each topic and step in the forensic process is described in accessible language. What You Will Learn Understand Hadoop internals and file storage Collect and analyze Hadoop forensic evidence Perform complex forensic analysis for fraud and other investigations Use state-of-the-art forensic tools Conduct interviews to identify Hadoop evidence Create compelling presentations of your forensic findings Understand how Big Data clusters operate Apply advanced forensic techniques in an investigation, including file carving, statistical analysis, and more In Detail Big Data forensics is an important type of digital investigation that involves the identification, collection, and analysis of large-scale Big Data systems. Hadoop is one of the most popular Big Data solutions, and forensically investigating a Hadoop cluster requires specialized tools and techniques. With the explosion of Big Data, forensic investigators need to be prepared to analyze the petabytes of data stored in Hadoop clusters. Understanding Hadoop's operational structure and performing forensic analysis with court-accepted tools and best practices will help you conduct a successful investigation. Discover how to perform a complete forensic investigation of large-scale Hadoop clusters using the same tools and techniques employed by forensic experts. This book begins by taking you through the process of forensic investigation and the pitfalls to avoid. It will walk you through Hadoop's internals and architecture, and you will discover what types of information Hadoop stores and how to access that data. You will learn to identify Big Data evidence using techniques to survey a live system and interview witnesses. After setting up your own Hadoop system, you will collect evidence using techniques such as forensic imaging and application-based extractions. You will analyze Hadoop evidence using advanced tools and techniques to uncover events and statistical information. Finally, data visualization and evidence presentation techniques are covered to help you properly communicate your findings to any audience. Style and approach This book is a complete guide that follows every step of the forensic analysis process in detail. You will be guided through each key topic and step necessary to perform an investigation. Hands-on exercises are presented throughout the book, and technical reference guides and sample documents are included for real-world use.

About the AuthorJoe Sremack Joe Sremack is a director at Berkeley Research Group, a global expert services firm. He conducts digital investigations and advises clients on complex data and investigative issues. He has worked on some of the largest civil litigation and corporate fraud investigations, including issues involving Ponzi schemes, stock option backdating, and mortgage-backed security fraud. He is a member of the Association of Certified Fraud Examiners and the Sedona Conference.