

# **PRACTICAL LINUX FORENSICS**

## **BRUCE NIKKEL**

Early Access edition, 6/18/21

Copyright © 2021 by Bruce Nikkel.

ISBN-13: 978-1-7185-0196-6 (print)

ISBN-13: 978-1-7185-0197-3 (ebook)

Publisher: William Pollock

Production Manager: Rachel Monaghan

Production Editor: Miles Bond

Developmental Editor: Jill Franklin

Cover Illustrator: James L. Barry

Technical Reviewer: Don Frick

Copyeditor: George Hale

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

# CONTENTS

Introduction

Chapter 1: Digital Forensics Overview

Chapter 2: Linux Overview

Chapter 3: Extracting Evidence from Storage Devices and Filesystems

Chapter 4: Directory Layout and Forensic Analysis of Linux Files

Chapter 5: Investigating Evidence from Linux Logs

Chapter 6: Reconstructing System Boot and Initialization

Chapter 7: Examination of Installed Software Packages

Chapter 8: Identifying Network Configuration Artifacts

Chapter 9: Forensic Analysis of Time and Location

Chapter 10: Reconstructing User Desktops and Login Activity

Chapter 11: Forensic Traces of Attached Peripheral Devices

Afterword

Appendix A: File and Directory List for Digital Investigators

The chapters in **red** are included in this Early Access PDF.