



— **xdadevelopers'** —

ANDROID™

HACKER'S TOOLKIT

The Complete Guide to Rooting, ROMs and Theming

Jason Tyler with Will Verduzco

**XDA Developers'
Android™
Hacker's
Toolkit**

XDA Developers' Android™ Hacker's Toolkit

THE COMPLETE GUIDE TO ROOTING, ROMS
AND THEMING

Jason Tyler with Will Verduzco

This work is a co-publication between XDA Developers
and John Wiley & Sons, Ltd.



A John Wiley and Sons, Ltd, Publication

This edition first published 2012
© 2012 John Wiley and Sons, Ltd.

Registered office

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex,
PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley and Sons, Inc. and/ or its affiliates in the United States and/or other countries, and may not be used without written permission. Android is a trademark of Google, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Ltd. is not associated with any product or vendor mentioned in the book.

XDA, XDA Developers is a trademark of JB Online Media, LLC
A catalogue record for this book is available from the British Library.

ISBN 978-1-119-95138-4 (paperback); ISBN 978-1-119-96154-3 (ebook);
978-1-119-96155-0 (ebook); 978-1-119-96156-7 (ebook)

Set in 9.5/11.5 Minion Pro Regular by Indianapolis Composition Services

Printed in the United States by Courier Westford

PUBLISHER'S ACKNOWLEDGEMENTS

Some of the people who helped bring this book to market include the following:

Editorial and Production

VP Consumer and Technology Publishing Director: Michelle Leete

Associate Director–Book Content Management: Martin Tribe

Associate Publisher: Chris Webb

Assistant Editor: Ellie Scott

Development Editor: Shena Deuchars

Copy Editor: Shena Deuchars

Technical Editor: Akshay Dashrath

Editorial Manager: Jodi Jensen

Senior Project Editor: Sara Shlaer

Editorial Assistant: Leslie Saxman

Marketing

Associate Marketing Director: Louise Breinholt

Senior Marketing Executive: Kate Parrett

Composition Services

Compositor: Indianapolis Composition Services

Proofreader: Linda Seifert

Indexer: Estalita Slivoskey

About the Authors

Jason Tyler has been an IT instructor and is currently Director of Technology for Typefrag.com. An avid Android hacker, Jason has been rooting and ROMing every Android phone he can get his hands on since the OG Droid.

Will Verduzco is a Johns Hopkins University graduate in neuroscience and is now currently studying to become a physician. He is also Portal Administrator for XDA-Developers, and has been addicted to mobile technology since the HTC Wizard. Starting with the Nexus One, however, his gadget love affair has shifted to Google's little green robot.

Contents

Foreword	xv
Introduction	1
First Things First: What Is XDA?	1
The Dragons that Lie Ahead	3
Who This Book Is For	6
What This Book Covers	6
How This Book Is Structured	6
What You Need to Use This Book	7
PART I: WHAT YOU NEED TO KNOW	9
Chapter 1: Android OS Internals: Understanding How Your Device Starts	11
The Penguin Down Below	12
How Your Android Device Starts	13
Bootstrapping	13
Adding a Custom Bootloader	15
Understanding the Bootloader Process	15
Custom Recoveries: The Holy Grail	17
Chapter 2: Rooting Your Android Device	21
Why Should You Root?	22
Increasing the Service Life of the Device	22
Fixing OEM Defects	23
Increasing Capability	24
Customizing the Device	25
Backing Up Data	26
Contact Information	26
Applications and Their Data	27
Data on the SD Card	27
How You Can Root and Leave Your OEM's Control	28
OEM Flash Software	28
Exploits	30
Native Fastboot Flash	31
Scripted and One-Click Methods	31

Rooting Two Devices	32
Nexus One	32
HTC Thunderbolt	33
The Root of It All	34
Chapter 3: The Right Tool for the Job	37
Ready, Set, . . . Wait I Have to Have What?	38
Connecting a Phone to a Computer	38
Hacking Tools	38
USB Cables	39
USB Debugging	40
What's Driving This Thing?	41
Using the Android Debug Bridge	42
Checking Device Connectivity	43
Restarting the ADB Service	44
Copying Files to and from Your Device	45
Rebooting a Device	48
The Power of Fastboot	49
Unlocking a Device	50
Updating a Device	50
Flashing a Device	50
Rebooting a Device	51
Harnessing the Power of the Penguin with ADB Shell	51
File System Navigation	52
File Management	54
File Access Permissions	57
Redirection and Piping	60
Concatenation	60
BusyBox: Giving the Penguin Back Its Power	61
The dd Command	61
The echo Command	62
The md5sum Command	62
Chapter 4: Rooting and Installing a Custom Recovery	63
How to Use Exploits	64
Exploit Scripts	64
Exploit Applications	65
Using a Script or Application on a Device	66
Hacking Utilities	68
OEM Tools	68
Developer Utilities	68
Image Files	68

Recovery Mode	69
What Is Recovery Mode?	69
Make It All So Easy: Get A Custom Recovery!	70
Using ClockworkMod Recovery	71
Rebooting the Device	72
Updating a Device from the SD Card	72
Resetting a Device to Factory Condition	74
Wiping the Cache	74
Installing a Zip File from the SD Card	74
Backing Up and Restoring a Device	76
Mounting Partitions and Managing Storage	79
Advanced Functions	79
Backup and Disaster Recovery	81
Precautions for Success and Data Recovery	82
Backing Up Applications	83
Backing Up Through a Recovery Process	83
Backing Up Through an Application	84
What Happens If It Goes Really Wrong?	84
Chapter 5: Theming: Digital Cosmetic Surgery	87
Changing the Look and Feel of Android	88
Theming the Launcher	89
Theming with an Add-on Launcher	89
Tools Used in Theming	89
APKManager	89
Android SDK	90
Eclipse	90
A ROM of Your Choice	91
7-Zip	91
Paint.NET	91
Update.zip Creator	91
Amend2Edify	92
The Editing Process	92
Walkthrough for Creating Theme Files	92
Walkthrough for Creating a Flashable ZIP File	97
Chapter 6: You've Become Superuser: Now What?	99
Popular Multi-Device Custom ROMs	100
CyanogenMod	100
Android Open Kang Project	101
VillainROM	101

Kernel Tweaks	101
Backlight Notifications	101
Voodoo Enhancements	102
Performance and Battery Life Tweaks	103
Root Applications	103
SetCPU	103
Adfree Android	104
Chainfire 3D	104
Titanium Backup	105

PART II: MANUFACTURER GUIDELINES AND DEVICE-SPECIFIC GUIDES **107**

Chapter 7: HTC EVO 3D: A Locked Device	109
Obtaining Temporary Root	110
Using S-OFF and Permanent Root Requirements	111
Running the Revolutionary Tool	112
Installing a Custom Recovery	115
Installing the Superuser Binary	116
Installing a SuperUser Application	117
Chapter 8: Nexus One: An Unlockable Device	119
Root Methods Available	120
Resources Required for This Walkthrough	120
Walkthrough	121
Placing the Nexus One in Fastboot Mode	122
Flashing a Boot Partition	123
Getting Full Root Access	124
Installing a Custom Recovery	125
Chapter 9: HTC ThunderBolt: A Tightly Locked Device	127
Root Methods Available	128
Resources Required for This Walkthrough	128
Walkthrough	129
Pushing Files to the Device	129
Gaining Temporary Root	130
Checking a File's MD5 Signature	131
Writing the Temporary Bootloader	131
Downgrading the Firmware	132
Gaining Temporary Root to Unlock the MMC	133
Rewriting the Bootloader	134
Upgrading the Firmware	135

Chapter 10: Droid Charge: Flashing with ODIN	137
Resources Required for This Walkthrough	138
Walkthrough	138
Connecting the Device to ODIN	138
Flashing the Device	139
Troubleshooting	140
Chapter 11: Nexus S: An Unlocked Device	143
Connecting the Device to a PC	144
Resources Required for This Walkthrough	144
Walkthrough	144
Unlocking the Device	144
Flashing the Device with a Recovery	145
Flashing the Device with the SuperUser	
Application	146
Chapter 12: Motorola Xoom: An Unlocked Honeycomb Tablet	147
Resources Required for This Walkthrough	148
Walkthrough	148
Pushing the Root File to the SD Card	148
Unlocking the Xoom	148
Flashing the Device with a Recovery	149
Flashing the Device with a Universal Root	150
Chapter 13: Nook Color: Rooting with a Bootable SD Card	153
Resources Required for This Walkthrough	154
Walkthrough	154
Creating a Bootable SD Card	155
Booting the Device from the SD Card	155
Making the Device More Usable	156
Appendix A: Setting Up Android SDK and ADB Tools	159
Installing the Java Development Kit	160
Installing the Android SDK	161
Installing the Platform Tools	162
Setting Up Windows Environment Variables	163
Index	165

Foreword

The XDA Developers (XDA) website was opened in 2003. Nine years may not seem like that long ago, but Facebook wasn't even a thing then. The iPhone and the first Android handset weren't released until 2007. So, in Internet time, XDA is old. In smartphone time, we're ancient.

`xda-developers.com` is a strange URL—not as imaginative, short or catchy as most high-traffic sites. There's a simple reason for this: the site wasn't created for you. We never envisioned a smartphone revolution—or if we did, we never envisioned that millions would care so much about what was happening on our little developer-focused forum.

XDA was created for developers and it is still a site for developers. They are incredibly smart, generally selfless, and hard-working individuals who share their creations (for free) with the world. When they see a book like this, they get concerned that their site will be overrun (more than it already is) by “newbs” with annoying questions and demands. They see the title of this book—with that overused “H”-word—and roll their eyes.

So, why did XDA lend its name to this guide? Honestly? It's because we can't stop you all from coming and we'd rather you be a bit better educated when you arrive. People spend more time touching their phones than their spouses and many of those people want their phones to be completely customizable (even as their spouses are generally not). They want to remove restrictions placed on the devices by carriers and OEMs and make the phone *theirs*.

This book was written by a member of XDA. His goal was to share his enthusiasm about what he found on the site and across the Internet about the customizability of the Android operating system, to get you just as excited, and to show you the tools you need to put that excitement into action. As with most tech-related books, much of the text herein is outdated by the time it hits the shelves. But that's OK. Even if the content is slightly stale, even if you don't have any of the devices listed in the tutorial chapters, we still urge you to read it carefully so that you are better prepared to understand as you explore XDA for your device.

As a site for developers, XDA's goal is to make sure you have you respect for all those who have blazed the trail to make all this good stuff possible. We want you to use XDA responsibly—read everything before posting, understand the risks of rooting and customizing your device, and, as you learn, become a helpful, contributing member of the community.

The XDA Admin Team

Introduction

There's a reason most Android geeks have such disdain for the other major smartphone operating system. The iPhone shackles the user, with its closed source code and ecosystem ruled with an iron fist. Android, on the other hand, frees developers to tear apart and rebuild nearly every aspect of the user's experience with the operating system. Beyond the world of developer-created applications (apps), there is a vast universe of deeper customizations—custom kernels and ROMs, themes, CPU overlocks, and more.

In most cases, these tasks begin with gaining “root” access to your device. The goal of this book is to get you comfortable with the tools and vocabulary of Android hacking, to get you in the “root” mindset, and to point you towards the best online resources for expanding your knowledge even further.

FIRST THINGS FIRST: WHAT IS XDA?

The XDA Developers (XDA) website, at <http://www.xda-developers.com>, is the largest smartphone community on the Internet. As the name implies, the site—launched in 2003—is a destination for developers. “XDA” was a line of phones based on Windows Mobile that were branded by O2 and developed by a small (at the time) Taiwanese manufacturer called High Tech Computer Corporation (HTC). According to XDA history:

It was these early O2 XDA devices that the founders of our site thought had much more potential than the sellers O2 and HTC were giving them credit for. With their geeky hats on they cracked them open and began to develop them beyond the standard fairly boring branded versions. To spread the word, they set up a small website and naturally called it xda-developers. In the early days they had less than a dozen members (2003).

As more and more phones were released, the XDA administrators launched a new forum for each one. The site was built around the spirit of community and cooperation. XDA itself is not an organization of developers. The site is merely a sandbox where developers congregate.

From those early few members, XDA became known as the go-to source for information on how to make phones do more great stuff and how to fix a phone that was otherwise broken. As more people were attracted to the site, enthusiasts were given a home to share the awesomeness of mobile device development. From that early core of a few dozen enthusiasts, geeks and developers, the XDA website now receives more than ten million visitors per month and thousands of informative posts every day.

The material in this book draws heavily on the work done by the fantastic community at XDA. The book combines the work of the XDA community, my technical teaching experience, and my work as an Android developer to provide a launching point for the budding Android hacker.

The XDA forums have become the foremost Internet destination for information about mobile devices: how to fix them, how to hack them and, generally, how to make them better than the manufacturers make them. <http://forum.xda-developers.com> is laid out in forums dedicated to individual devices. Each forum contains a core group of people who work with and love the device, as well as thousands of helpful individuals on the same journey as you. When you visit XDA, you can use the “Forums” link and navigate through the forums to find your specific device (see Figure 1).

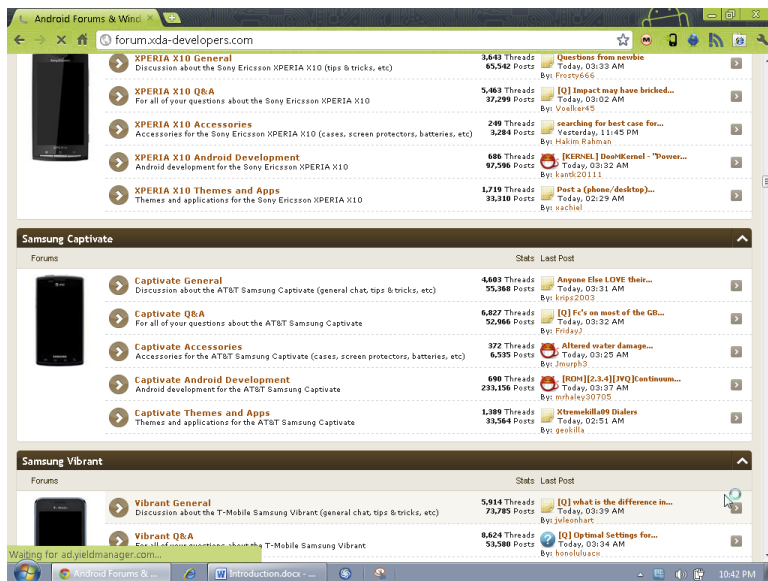


Figure 1: The device-specific forums at <http://forum.xda-developers.com>