



— **xdadevelopers'** —

ANDROID™

HACKER'S TOOLKIT

The Complete Guide to Rooting, ROMs and Theming

Jason Tyler with Will Verduzco

XDA Developers' Android™ Hacker's Toolkit

Table of Contents

[Introduction](#)

- [First Things First: What Is XDA?](#)
- [The Dragons that Lie Ahead](#)
- [Who This Book Is For](#)
- [What This Book Covers](#)
- [How This Book Is Structured](#)
- [What You Need to Use This Book](#)

[Part I: What You Need to Know](#)

[Chapter 1: Android OS Internals: Understanding How Your Device Starts](#)

- [The Penguin Down Below](#)
- [How Your Android Device Starts](#)
 - [Bootstrapping](#)
 - [Adding a Custom Bootloader](#)
 - [Understanding the Bootloader Process](#)
- [Custom Recoveries: The Holy Grail](#)

[Chapter 2: Rooting Your Android Device](#)

- [Why Should You Root?](#)

[Increasing the Service Life of the Device](#)

[Fixing OEM Defects](#)

[Increasing Capability](#)

[Customizing the Device](#)

[Backing Up Data](#)

[Contact Information](#)

[Applications and Their Data](#)

[Data on the SD Card](#)

[How You Can Root and Leave Your OEM's Control](#)

[OEM Flash Software](#)

[Exploits](#)

[Native Fastboot Flash](#)

[Scripted and One-Click Methods](#)

[Rooting Two Devices](#)

[Nexus One](#)

[HTC Thunderbolt](#)

[The Root of It All](#)

[Chapter 3: The Right Tool for the Job](#)

[Ready, Set, . . . Wait I Have to Have What?](#)

[Connecting a Phone to a Computer](#)

[Hacking Tools](#)

[USB Cables](#)

[USB Debugging](#)

[What's Driving This Thing?](#)

[Using the Android Debug Bridge](#)

[Checking Device Connectivity](#)

[Restarting the ADB Service](#)

[Copying Files to and from Your Device](#)

[Rebooting a Device](#)

[The Power of Fastboot](#)

[Unlocking a Device](#)

[Updating a Device](#)

[Flashing a Device](#)

[Rebooting a Device](#)

[Harnessing the Power of the Penguin with ADB Shell](#)

[File System Navigation](#)

[File Management](#)

[File Access Permissions](#)

[Redirection and Piping](#)

[Concatenation](#)

[BusyBox: Giving the Penguin Back Its Power](#)

[The dd Command](#)

[The echo Command](#)

[The md5sum Command](#)

[Chapter 4: Rooting and Installing a Custom Recovery](#)

[How to Use Exploits](#)

[Exploit Scripts](#)

[Exploit Applications](#)

[Using a Script or Application on a Device](#)

[Hacking Utilities](#)

[OEM Tools](#)

[Developer Utilities](#)

[Image Files](#)

[Recovery Mode](#)

[What Is Recovery Mode?](#)

[Make It All So Easy: Get A Custom Recovery!](#)

[Using ClockworkMod Recovery](#)

[Rebooting the Device](#)

[Updating a Device from the SD Card](#)

[Resetting a Device to Factory Condition](#)

[Wiping the Cache](#)

[Installing a Zip File from the SD Card](#)

[Backing Up and Restoring a Device](#)

[Mounting Partitions and Managing Storage](#)

[Advanced Functions](#)

[Backup and Disaster Recovery](#)

[Precautions for Success and Data Recovery](#)

[Backing Up Applications](#)

[Backing Up Through a Recovery Process](#)

[Backing Up Through an Application](#)

[What Happens if It Goes Really Wrong?](#)

[Chapter 5: Theming: Digital Cosmetic Surgery](#)

[Changing the Look and Feel of Android](#)

[Theming the Launcher](#)

[Theming with an Add-on Launcher](#)

[Tools Used in Theming](#)

[APKManager](#)

[Android SDK](#)

[Eclipse](#)

[A ROM of Your Choice](#)

[7-Zip](#)

[Paint.NET](#)

[Update.zip Creator](#)

[Amend2Edify](#)

[The Editing Process](#)

[Walkthrough for Creating Theme Files](#)

[Walkthrough for Creating a Flashable ZIP File](#)

[Chapter 6: You've Become Superuser: Now What?](#)

[Popular Multi-Device Custom ROMs](#)

[CyanogenMod](#)

[Android Open Kang Project](#)

[VillainROM](#)

[Kernel Tweaks](#)

[Backlight Notifications](#)

[Voodoo Enhancements](#)

[Performance and Battery Life Tweaks](#)

[Root Applications](#)

[SetCPU](#)

[Adfree Android](#)

[Chainfire 3D](#)

[Titanium Backup](#)

[Part II: Manufacturer Guidelines and Device-Specific Guides](#)

[Chapter 7: HTC EVO 3D: A Locked Device](#)

[Obtaining Temporary Root](#)

[Using S-OFF and Permanent Root Requirements](#)

[Running the Revolutionary Tool](#)

[Installing a Custom Recovery](#)

[Installing the Superuser Binary](#)

[Installing a SuperUser Application](#)

[Chapter 8: Nexus One: An Unlockable Device](#)

[Root Methods Available](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Placing the Nexus One in Fastboot Mode](#)

[Flashing a Boot Partition](#)

[Getting Full Root Access](#)

[Installing a Custom Recovery](#)

[Chapter 9: HTC ThunderBolt: A Tightly Locked Device](#)

[Root Methods Available](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Pushing Files to the Device](#)

[Gaining Temporary Root](#)

[Checking a File's MD5 Signature](#)

[Writing the Temporary Bootloader](#)

[Downgrading the Firmware](#)

[Gaining Temporary Root to Unlock the MMC](#)

[Rewriting the Bootloader](#)

[Upgrading the Firmware](#)

[Chapter 10: Droid Charge: Flashing with ODIN](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Connecting the Device to ODIN](#)

[Flashing the Device](#)

[Troubleshooting](#)

[Chapter 11: Nexus S: An Unlocked Device](#)

[Connecting the Device to a PC](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Unlocking the Device](#)

[Flashing the Device with a Recovery](#)

[Flashing the Device with the SuperUser application](#)

[Chapter 12: Motorola Xoom: An Unlocked Honeycomb Tablet](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Pushing the Root File to the SD Card](#)

[Unlocking the Xoom](#)

[Flashing the Device with a Recovery](#)

[Flashing the Device with a Universal Root](#)

[Chapter 13: Nook Color: Rooting with a Bootable SD Card](#)

[Resources Required for this Walkthrough](#)

[Walkthrough](#)

[Creating a Bootable SD Card](#)

[Booting the Device from the SD Card](#)

[Making the Device More Usable](#)

[Appendix A: Setting Up Android SDK and ADB Tools](#)

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.

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).

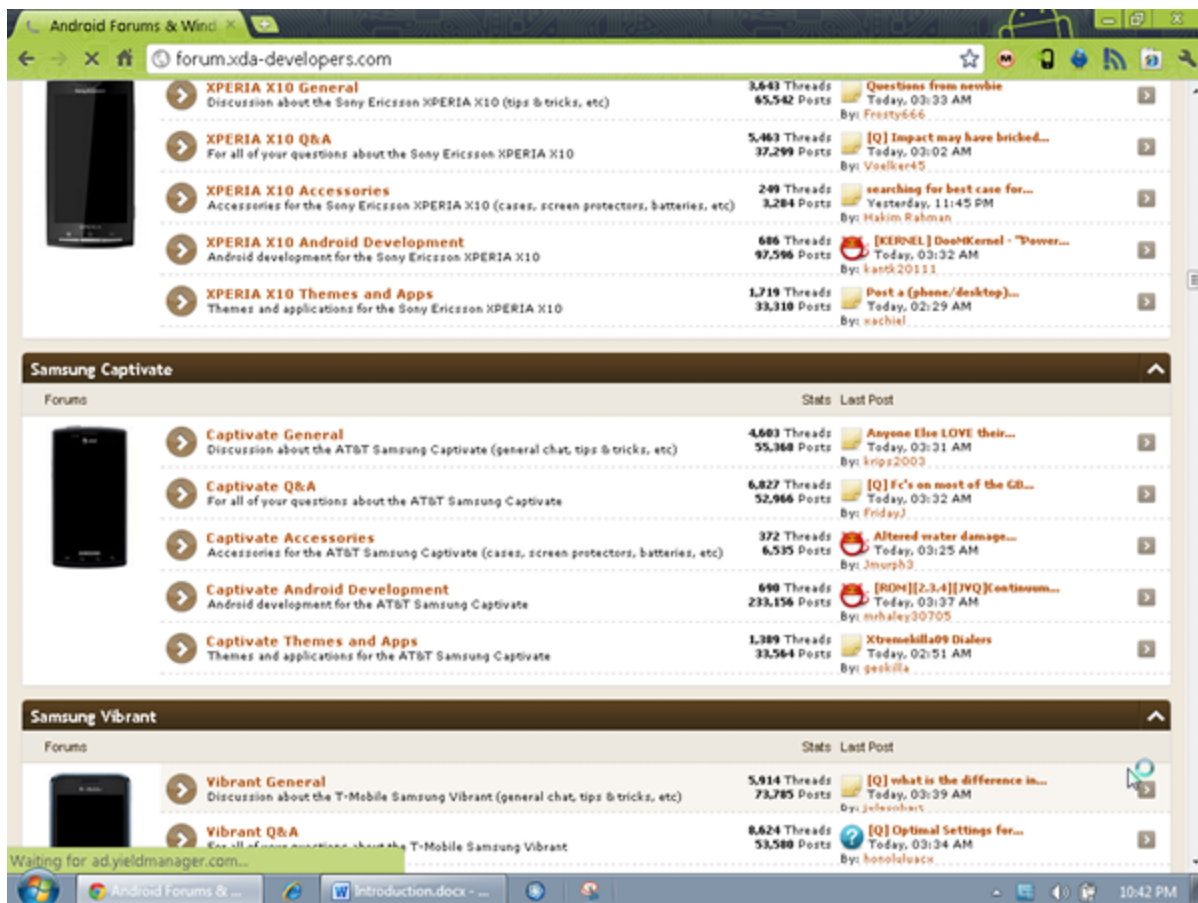


Figure 1: The device-specific forums at <http://forum.xda-developers.com>

The Dragons that Lie Ahead

The freedom offered to you when your device is rooted is liberating. It affords you such wonders as:

- complete backup of all applications and their data
- Google Apps, if they were not included with your device
- overclocking your device (speeding it up to run faster and better)
- fixing manufacturer issues, such as GPS errors or call dropping
- wireless tethering to create a quickie “hotspot”
- completely changing and customizing the device interface.

All of this and more is available to those who step out on a limb and root their Android device. However, there are two caveats to keep in mind before you get started.

You should know before you read any further that by even thinking about rooting your device you may have voided your warranty.

Not really, of course, but attempting any of the customizations that you read about in this book will void your manufacturer’s warranty and any insurance warranty you may have purchased. Manufacturers and mobile service carriers sell millions of devices every week. For every device they sell, they have to support a certain percentage of those devices that are defective. As far as your carrier and OEM are concerned, when you mess with the stuff they have spent millions on making, their responsibility to support you ends.

There are no exceptions to this rule. Most OEMs, carriers and support companies will instantly reject any sort of support or replacement request when they find the device has had its software, firmware or hardware altered outside normal parameters. Even so-called “developer” devices,