Hi-Tech

Enjoy Better Technology!

TechGeek Tutorials

Android Hacking

Jules Ivan C. Garay

https://JIGapps.weebly.com

http://www.facebook.com/HitechPh

Table of Contents

Introduction 4
About Hi-Tech 4
Part 1: Tweaking Android - Boost 5
Part 2: Android Rooting – Gain Root 7
  How to Root? 7
  My Device is Rooted, Now what? 7
Part 3: The Busybox & Terminal Emulator 8
  Terminal Emulator Commands 8
Part 4: Block unwanted Wi-Fi users 9
  Detailed Steps for blocking unwanted Wi-Fi users 9
Part 5: Virtual Private Network (VPN) 10
  Easy VPN installed! 10
  What is VPN and how does it work? 10
Part 6: The Deep Web – TOR Network 14
  Why Should I use TOR? 14
  Wait, what is Deep web anyway? 14
  How to connect to TOR and access Deep Web? 15
Let the fun begin! 15
Part 7: Control a computer using Android 16
Part 8: Unlimited Game Resources 18
  Where to download GameGuardian 18
  How to use Game Guardian? 18
Part 9: The Lucky Patcher 19
Part 10: Android Malwares – Ghost push 20
  How is this part of hacking? 21
  Let’s get started! 21
Part 11: Recover or Shred deleted files 21
  How to recover deleted files? 21
  How to shred deleted files? 21
  Alternative Recovery apps 21
Part 12: Fixing bootloop (soft brick) 22

What is bootloop? 22
What is the cause of Bootloop? 22
How to fix? 22
Warning: This tutorial may not be compatible with all Android devices. 22
Requirements 23
About the author 23

Introduction

Almost everyone in the today wants to know hacking and almost 70% of the population are using android. That's why I created this tutorial for everyone who wants to learn hacking using their Android Smart phones. Android is based on the Hacker's Favorite OS: Linux, that's why it is possible to use android as your new hacking device. This tiny device can become deadly if misused. This book however, deals with simple tricks that many people must have already known.

So, you are reading this book huh? Do you want to be a hacker? Well, after reading the entire book, you will learn a lot of tricks your tiny device can do. This book is your stepping stone to become an Android enthusiast.

"Hacking exist because of the vulnerability in technology." –Tech Viral

No one is Perfect, even android. This book will also deal with the security flaws of android and how to use them in hacking and how to fix these flaws to prevent others from hacking you. I really hope that you will enjoy reading and learning from this book.

Why do you want to be a hacker? Of course! Why not? Hackers are the ninjas of the 21st Century! We can do a lot of things which normal people can't. There are 2 different types of hackers though: The Ethical and the Unethical. Ethical Hackers are hackers who hack to help people. Unethical Hackers on the other hand are the opposite of helping; they can destroy lives and are the reason why the word "Hacker" gained bad reputation. This book combined the both ethical and unethical way of hacking for you to learn how both hackers work. It is then up to you if you want to be ethical or unethical type of hacker. Me? I'm an ethical hacker, and I want to help you learn hacking too! Well, hacking is a broad word. In order to be a hacker, one must be knowledgeable enough about computer's flaws and fixes. I want you to learn hacking in order for you to help people around the world too! Because I want everyone to enjoy better technology the way it supposed to be…

Are you ready to learn your first lesson?

Go ahead and take the risk of the world of hacking!

About Hi-Tech

Hi-Tech is a business partnership that aims to help people enjoy technology the way it supposed to be, located at: Capitol University, Philippines. Visit our Official Facebook page to get InTouch with us! Visit our Website to download and install our Softwares! ☺

Part 1: Tweaking Android - Boost

“When you modify a certain piece of hardware for better performance, it is often referred to as "tweaking" it. Overclocking the computer's CPU or changing jumper settings on the motherboard are common examples of hardware tweaking. Removing system limitations and adding plug-ins or extensions to a computer's operating system are types of software tweaking.”

- https://techterms.com/definition/tweak

Before learning hacking, let’s make sure that your device is responsive and free from lags. To do this, you need to tweak your device. This tutorial is for non-Rooted devices. First things first, let’s ask: what causes android to lag? “*Your Android phone was probably fast when you first bought it, right? Then over time it began running more slowly. This is a common problem and nothing to worry about.”* -Scott Adam Gordon (www.androidpit.com). There are common reasons why your device is lag such as: It can be cause by an App, Too many applications running on background, and/or the system itself.

HOW TO FIX

Method 1: Uninstalling, Stopping, and/or Freezing Applications

- You need to sacrifice your apps to gain speedy performance for your device. If you have Facebook app or Facebook messenger installed, you need to say goodbye to them (Unless if you’re not ready to move on...).
- If you don’t want to uninstall applications, you might consider stopping these applications from running on background. To do this, go to settings>Apps> then choose any app then tap “Force stop”.
- Freezing applications/Disabling can be useful if you think that you’re not using a system app often. Go to settings>apps>System Apps> then select any apps then tap on Disable. NOTE: Some System Apps cannot be disabled because if they do, you might end up bricking your device. These methods are completely safe to do.

Method 2: Disabling animations – Enabling Developer Option

Disabling animations could help your device run faster. To do this, you need to enable Developer Option. **On Android 4.2 and higher, you must enable this screen as follows:**

- Open the Settings app.
- (Only on Android 8.0 or higher) Select System.
- Scroll to the bottom and select about phone.
- Scroll to the bottom and tap Build number 7 times.
- Return to the previous screen to find Developer options near the bottom.

Note: If your device is lower than version than 4.2, search online on how to enable Developer Option.

Method 3: Install these apps to boost device performance.

- Clean Master LITE – Helps you stop all the apps processes plus cleans useless files, claimed to be the best booster on play store. See for yourself. (https://play.google.com/store/apps/details?id=com.cmcm.lite)
- Greenify – Works on Rooted and non-Rooted device. Force Stops all applications in one tap! I suggest you to pay for the pro version, it hibernates all the apps including system apps. (https://play.google.com/store/apps/details?id=com.oasisfeng.greenify)

There you go! Your device should be faster now! If you still don't feel any difference, don't worry this is not hacking yet. Later, we'll going to hack your device's system.

Part 2: Android Rooting – Gain Root

WARNING: Search online on the Pros and cons of Rooting before rooting your device! Rooting may void your warranty and worst? You may end up bricking your device!

*"**Rooting** is a process that allows you to attain root access to the **Android** operating system code."* - www.bullguard.com

Root is similar to Administrative permission of Windows. Why Root is necessary for android? according to gizmodo.com, *"When you take your phone out of the box, while there are plenty of settings you can tweak, you can only alter what the manufacturer allows you to. By gaining **root** access you can modify the device's software on the very deepest level."* Root is considered as the highest permission a Linux user can obtain, and because you are learning hacking using your android device, it is necessary to gain Root Permission.

How to Root?

The easiest way to Root your android device is to install a 3rd party application on your android. I recommend **KingRoot** Download Kingroot app on their official website at https://kingroot.net/. The alternative app for KingRoot is **KingoRoot** which is also available for download on their official website at http://www.kingoapp.com/. Choose any of this two Rooters then install the apk file to your device then open the app and enjoy! NOTE: You need to be connected to a Wi-Fi upon the process of rooting.

Let's check if your device is rooted, Download Root Checker on Google play and run, then allow Root checker to gain Root permission (if prompted).

My Device is Rooted, Now what?

Congratulations! Your device is ready for hacking! With Root, You will be able to do a lot of things like: Tweak your device to the deepest level, uninstall useless system apps, cutting someone's Internet connection, purchasing in-app purchases for free (This is illegal, careful), change your device's identity, and many more! If you feel excited, then you should be!

However, Root alone doesn't do any functionality unless you install apps that use Root permissions.

Part 3: The Busybox & Terminal Emulator

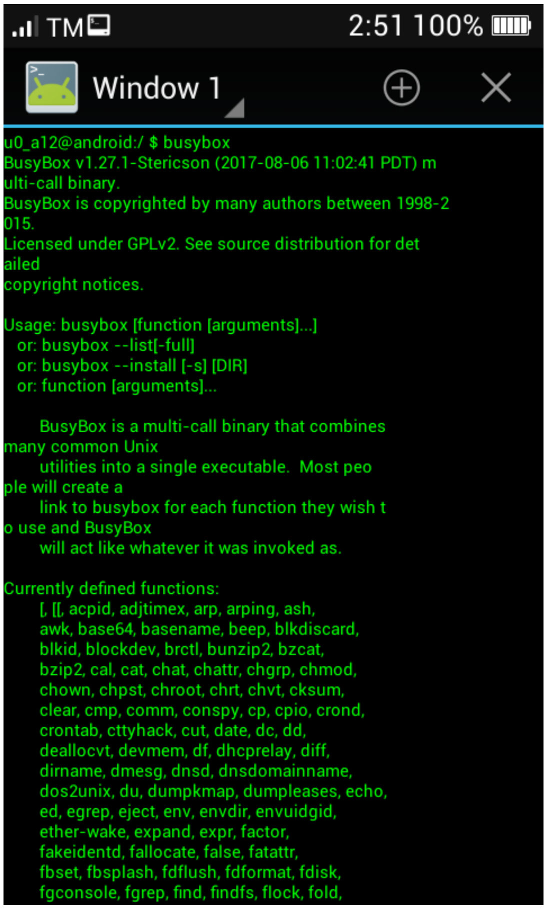
*“**BusyBox** is software that provides several stripped-down UNIX tools in a single executable file”.* - https://en.wikipedia.org/

Install Busybox and Terminal Emulator from Google Play. Open Busybox and press the install button.

If it prompts for Root access, please grant/allow it.

NOTE: The Busybox is not the app but the file that has been extracted by the Busybox app to your device’s /system/bin or /system/xbin. After pressing the install button of Busybox, you can uninstall the app from your device but keeping the app installed will notify you for new versions of Busybox.

Now, let’s see if Busybox in installed in your device, open Terminal Emulator app then type *busybox.* It should look like this picture below.



```
u0_a12@android:/ $ busybox
BusyBox v1.27.1-Stericson (2017-08-06 11:02:41 PDT) m
ulti-call binary.
BusyBox is copyrighted by many authors between 1998-2
015.
Licensed under GPLv2. See source distribution for det
ailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list[-full]
   or: busybox --install [-s] [DIR]
   or: function [arguments]...

        BusyBox is a multi-call binary that combines
many common Unix
        utilities into a single executable.  Most peo
ple will create a
        link to busybox for each function they wish t
o use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, [[, acpid, adjtimex, arp, arping, ash,
        awk, base64, basename, beep, blkdiscard,
        blkid, blockdev, brctl, bunzip2, bzcat,
        bzip2, cal, cat, chat, chattr, chgrp, chmod,
        chown, chpst, chroot, chrt, chvt, cksum,
        clear, cmp, comm, conspy, cp, cpio, crond,
        crontab, cttyhack, cut, date, dc, dd,
        deallocvt, devmem, df, dhcprelay, diff,
        dirname, dmesg, dnsd, dnsdomainname,
        dos2unix, du, dumpkmap, dumpleases, echo,
        ed, egrep, eject, env, envdir, envuidgid,
        ether-wake, expand, expr, factor,
        fakeidentd, fallocate, false, fatattr,
        fbset, fbsplash, fdflush, fdformat, fdisk,
        fgconsole, fgrep, find, findfs, flock, fold,
```

Terminal Emulator Commands

As hackers, we love to play with Terminal commands and you should to! Here are some of the useful terminal commands:

busybox – List all the busybox commands. (Be careful performing its commands, you might end up bricking your device.)

su – Run your next commands as Root

df – displays disk usage information for each file and directory

ls - List all files in current directory.

Reference: https://forum.xda-developers.com/wiki/Guide:Using_the_Terminal

Tip: How to remove lag/boost your device using terminal emulator

1. Type *su* then enter.
2. Type *fstrim –v /data* then enter
3. Type *fstrim –v /cache* then enter
4. Type *fstrim –v /system* then enter
5. Type exit or close Terminal Emulator. Enjoy!

Part 4: Block unwanted Wi-Fi users

Sometimes, your Internet connection becomes slow, maybe because there are a lot of people connected on your Wi-Fi network. So, how are we going to block them and enjoy the bandwidth for ourselves? Thanks to Arp technology provided by the Busybox! All we need to do is to install Netcut on Google Play and let it do the job!

Detailed Steps for blocking unwanted Wi-Fi users

1. Install “Netcut” by Arcai on Play Store

2. Run Netcut then Grant it with Root permission.

3. Wait for it to finish scanning connected devices on your Wi-Fi

4. Tap on the devices you want to block.

How to counter if someone is blocking me from my Wi-Fi?

To protect yourself from Netcut, install “Arp Guard” on Play Store and set your preferences then activate Arp Guard. Netcut users will not be able to block you anymore

NOTE: Don’t use Netcut on public Wi-Fi because it is easy for the authorities to trace you if you do! This Tutorial may be illegal in your country, please proceed with caution.

WARNING! In no instances will Hi-Tech nor will the author of this tutorial be held liable if you use this tutorial the wrong way.

Part 5: Virtual Private Network (VPN)

FAIR WARNING: Virtual Private Networks or VPNs might be illegal on your country.

On some countries like as Turkey, China, and Iran are blocking Facebook, Twitter, and YouTube and if you are in any of this countries, you may not be able to access your favorite sites. The only way to unblock them is by using VPN. For this Tutorial I recommend using Easy VPN, here's the link:

https://play.google.com/store/apps/details?id=easyvpn.free.vpn.unblock.proxy&hl=en

NOTE: Some VPN apps gives free Internet access but not for this tutorial.

Easy VPN installed!

Open Easy VPN and choose the country of your choice or press connect right away. The VPN will fake your device location. You can now enjoy your favorite apps and sites.

What is VPN and how does it work?

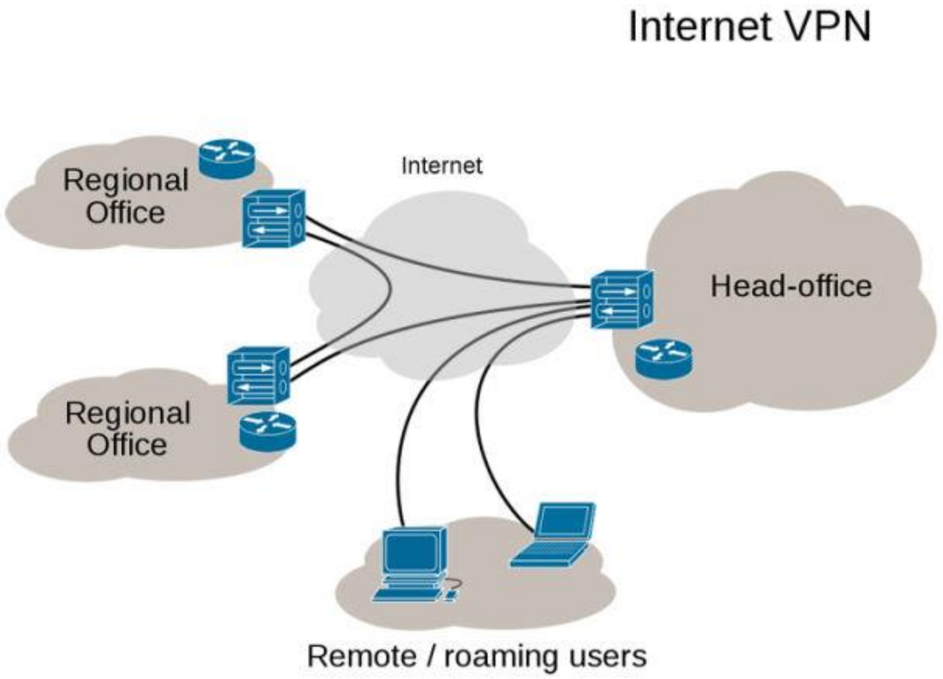
Here's the complete explanation:

Source: https://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one

For as ubiquitous as connectivity has become and how reliant we've grown on it, the Internet is still a digital jungle where hackers easily steal sensitive information from the ill-equipped and where the iron-fisted tactics of totalitarian regimes bent on controlling what their subjects can access are common. So instead of mucking around in public networks, just avoid them. Use a VPN instead. Between Wi-Fi spoofing, Honeypot attacks, and Fire sheep, public networks really are cesspools. But if you're working remotely and need to access sensitive data on your company's private servers, doing so from an unsecured public network like a coffee shop Wi-Fi hotspot could put that data, your company's business, and your job at stake.

VPNs, or Virtual Private Networks, allow users to securely access a private network and share data remotely through public networks. Much like a firewall protects your data on your computer, VPNs protect it online. And while a VPN is *technically* a WAN (Wide

Area Network), the front end retains the same functionality, security, and appearance as it would on the private network.



For this reason, VPNs are hugely popular with corporations as a means of securing sensitive data when connecting remote data centers. These networks are also becoming increasingly common among individual users—and not just torrenters. Because VPNs use a combination of dedicated connections and encryption protocols to generate virtual P2P connections, even if snoopers did manage to siphon off some of the transmitted data, they'd be unable to access it on account of the encryption. What's more, VPNs allow individuals to spoof their physical location—the user's actual IP address is replaced by VPN provider—allowing them to bypass content filters. So, you may live in Tehran but appear to live in Texas, enabling you to slip past the government filters and commit the treasonous act of watching a YouTube video. *The horror.*

Establishing one of these secure connections—say you want to log into your private corporate network remotely—is surprisingly easy. The user first connects to the public internet through an ISP, and then initiates a VPN connection with the company VPN server using client software. And that's it! The client software on the server establishes the secure connection, grants the remote user access to the internal network and—Bing, bang, boom—you're up to your elbows in TPS reports. *The horror.*

Many security protocols have been developed as VPNs, each offering differing levels of security and features. Among the more common are:

- **IP security (IPsec)**: IPsec is often used to secure Internet communications and can operate in two modes. Transport mode only encrypts the data packet message itself while Tunneling mode encrypts the entire data packet. This protocol can also be used in tandem with other protocols to increase their combined level of security.
- **Layer 2 Tunneling Protocol (L2TP)/IPsec**: The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client. Since L2TP isn't capable of encryption, it instead generates the tunnel while the IPsec protocol handles encryption, channel security, and data integrity checks to ensure all of the packets have arrived and that the channel has not been compromised.
- **Secure Sockets Layer (SSL)** and **Transport Layer Security (TLS)**: SSL and TLS are used extensively in the security of online retailers and service providers. These protocols operate using a handshake method. As IBM explains, "A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session." These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection.
- **Point-to-Point Tunneling Protocol (PPTP)**: PPTP is a ubiquitous VPN protocol used since the mid-1990s and can be installed on a huge variety of operating systems has been around since the days of Windows 95. But, like L2TP, PPTP doesn't do encryption; it simply tunnels and encapsulates the data packet. Instead, a secondary protocol such as GRE or TCP has to be used as well to handle the encryption. And while the level of security PPTP provides has been

eclipsed by new methods, the protocol remains a strong one, albeit not the most secure.

- **Secure Shell (SSH)**: SSH creates both the VPN tunnel and the encryption that protects it. This allows users to transfer information unsecured data by routing the traffic from remote fileservers through an encrypted channel. The data itself isn't encrypted but the channel it's moving through is. SSH connections are created by the SSH client, which forwards traffic from a local port one on the remote server. All data between the two ends of the tunnel flow through these specified ports.

These SSH tunnels are the primary means of subverting the government content filters described earlier. For example, if the filter prohibits access to TCP port 80, which handles HTTP, all user access to the Internet is cut off. However, by using SSH, the user can forward traffic from port 80 to another on the local machine which will still connect to the remote server's port 80. So as long as the remote server allows outgoing connections, the bypass will work. SSH also allows protocols that would otherwise be blocked by the firewall, say those for torrenting, to get past the wall by "wrapping" themselves in the skin of a protocol that the firewall does allow.

To actually create the VPN tunnel, the local machine needs to be running a VPN client. Open VPN is a popular—and free—multi-platform application, as is LogMeIn Hamachi. Windows users also have the option of using the native OS VPN client.

So whether you're a cubicle monkey, file pirate, or just don't want The Man getting all grabby with your personal data, virtual private networks are the best means of securing traffic short of copying it to a flash drive and driving there yourself.

Part 6: The Deep Web – TOR Network

*“**Tor** is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". The intent for Tor's use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.”*

- https://en.wikipedia.org/wiki/Tor_(anonymity_network)

Why Should I use TOR?

Okay, there are some tutorials that I’m not including here because it’s too seriously illegal in nature. If you connect to a TOR network and access the Deep Web, You’ll learn more not just about android hacking but hacking itself.

Wait, what is Deep web anyway?

The **deep web** is the part of the World Wide Web that is not indexed by traditional search engines. Deep Web is only reachable through TOR, This means, you cannot access the deep web with your regular internet connection.

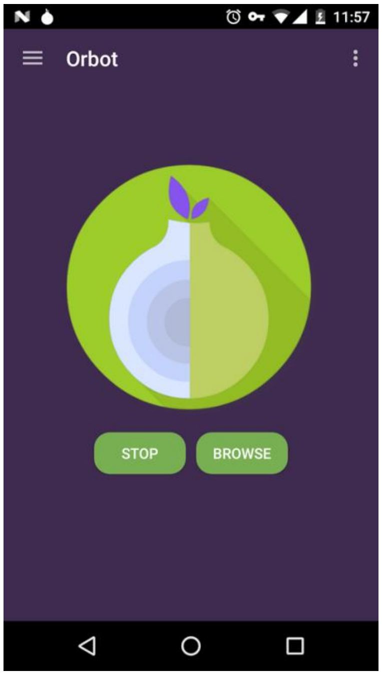
How to connect to TOR and access Deep Web?

1. Install “Orbot” and “Orfox” on Play Store.

2. Open Orbot then Tap on connect.

3. You can now enjoy Deep Web Content using Orfox Browser.

Note: It is possible to configure TOR to use Root access to enable you to access Deep Web using any browser.



Let the fun begin!

Here are lists of websites you can access through TOR:

http://3g2upl4pq6kufc4m.onion/ – DuckDuckGo Search Engine
http://xmh57jrzrnw6insl.onion/ – TORCH – Tor Search Engine
http://uhwiki36pbooodfj.onion/ – Uncensored Hidden Wiki
http://32rfckwuorlf4dlv.onion/ – Onion URL Repository
http://e266al32vpuorbyg.onion/bookmarks.php/ – Dark Nexus
http://5plvrsgydwy2sgce.onion/ – Seeks Search
http://2vlqpcqpjlhmd5r2.onion/ – Gateway to Freenet
http://nlmymchrmnlmbnii.onion/ – Is it up?
http://kpynyvym6xqi7wz2.onion/links.html/ – ParaZite
http://wiki5kauuihowqi5.onion/ – Onion Wiki
http://torwikignoueupfm.onion/ – Tor Wiki
http://hiwiki544q5q4gbt.onion/ – The Hidden Wiki
http://idnxcnkne4qt76tg.onion/ – Tor Project: Anonymity Online
http://torlinkbgs6aabns.onion/ – TorLinks
http://xdagknwjc7aaytzh.onion/ – Anonet Webproxy
http://3fyb44wdhnd2ghhl.onion/ – All You’re Base
http://j6im4v42ur6dpic3.onion/ – TorProject Archive
http://p3igkncehackjtib.onion/ – TorProject Media
http://kbhpodhnfxl3clb4.onion/ – Tor Search
http://cipollatnumrrahd.onion/ – Cipolla 2.0 (Italian)
http://dppmfxaacucguzpc.onion/ – TorDir – One of the oldest links list on Tor
Marketplace Financial:
http://bitmixer3gwvbgzw.onion/ – Bitmixer.io – Bitcoin Mixer
http://bitblendnlwgkhsr.onion/ – BitBlender – Oldest Bitcoin Mixer on darknet

http://torbrokerge7zxgq.onion/ – TorBroker – Trade securities anonymously with bitcoin, currently supports nearly 1000 stocks and ETFs
http://2vx63nyktk4kxbxb.onion/ – AUTOMATED PAYPAL AND CREDIT CARD STORE
http://samsgdtwz6hvjyu4.onion/ – Safe, Anonymous, Fast, Easy escrow service.
http://easycoinsayj7p5l.onion/ – EasyCoin – Bitcoin Wallet with free Bitcoin Mixer
http://jzn5w5pac26sqef4.onion/ – WeBuyBitcoins – Sell your Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and more
http://ow24et3tetp6tvmk.onion/ – OnionWallet – Anonymous Bitcoin Wallet and Bitcoin Laundry
http://qc7ilonwpv77qibm.onion/ – Western Union Exploit
http://3dbr5t4pygahedms.onion/ – ccPal Store
http://y3fpieiezy2sin4a.onion/ – HQER – High Quality Euro Replicas
http://qkj4drtgvpm7eecl.onion/ – Counterfeit USD
http://nr6juudpp4as4gjg.onion/pptobtc.html/ – PayPal to Bitcoins
http://lw4ipk5choakk5ze.onion/raw/4588/ – High Quality Tutorials

Note: If you noticed, Websites that are only reachable through TOR ends with .Onion extensions.

Part 7: Control a computer using Android

Controlling PC?

Yes! It is possible! But not without the help of softwares though. In this Tutorial, we are going to use “Splashtop.” First things first, open your computer then download and install Splashtop on your PC, here’s the link: https://www.splashtop.com/downloads

On your android device, Download and Install Splashtop 2 Remote Desktop.

Note: You PC and Android device must be connected to the same Network/Internet in order to work. You might need to create an account to use Splashtop.

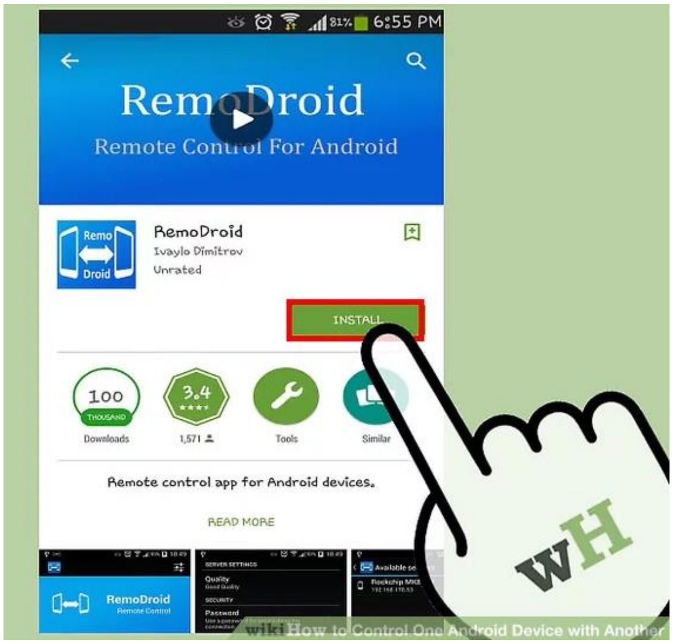
What can else can Splashtop do?

Well, figure it out yourself! I wanted to surprise you of what else Splashtop can do.

Is it possible to control another Android device?

Here’s a Tutorial from Wikihow:

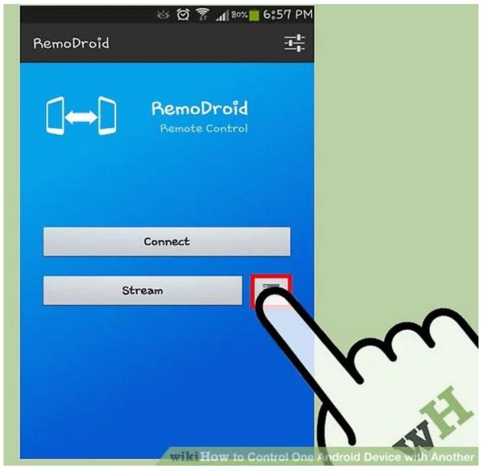
The ability to control on Android device with another can be helpful in many situations. For example, if you're streaming something to your Android TV stick, you might want to control it from your Android tablet or phone. Well, Android doesn’t disappoint. There are apps for Android that can let you control one Android device with another. You can easily download apps like Tablet Remote or RemoDroid to do so.


6:55 PM
RemoDroid
Remote Control For Android
RemoDroid
Ivaylo Dimitrov
Unrated
INSTALL
100
THOUSAND
Downloads
3.4
1,571
Tools
Similar
Remote control app for Android devices.
READ MORE
RemoDroid
wikiHow to Control One Android Device with Another

1. Download and install RemoDroid in both the Android devices. You can download the app for free from the Play Store.

2. Open the app on both the phones. Do this by tapping on its icon from the home screen. The icon is blue with two white mobile devices and arrow in it.

- Once the app opens, you will see two options: “Connect” and “Stream.” Stream is used for the controlling device, which must be rooted, and Connect is used for device being controlled (rooting is not necessary here).
- For the app, to work make sure your devices are connected to the same Wi-Fi network. Also, make sure that the controlling device is rooted.



3. Access the App Settings of the controlling phone. Tap the menu button, and select “Settings” from the option.

4. Tap “Port for Streaming” to check your port. Take note of this port number because you will need it later for streaming.

5. Adjust the quality of streaming. In the same screen, you can change the quality by tapping on the option you prefer. The quality is basically how you control the phone, which depends on the speed of your Wi-Fi connection. For instance, if you choose good quality, it will work perfectly. However, if you chose “High quality,” there may be some lags in the phone being controlled.

6. Link the two devices. Tap the back button of the controlling device and tap “Stream.” A notification “RemoDroid server started” will appear. This means your device is ready as the controller. An IP address of the phone will be displayed at the bottom of the screen. Take note of the IP address.