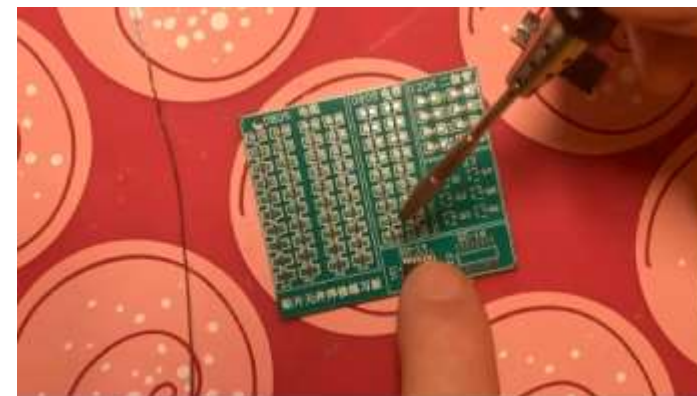
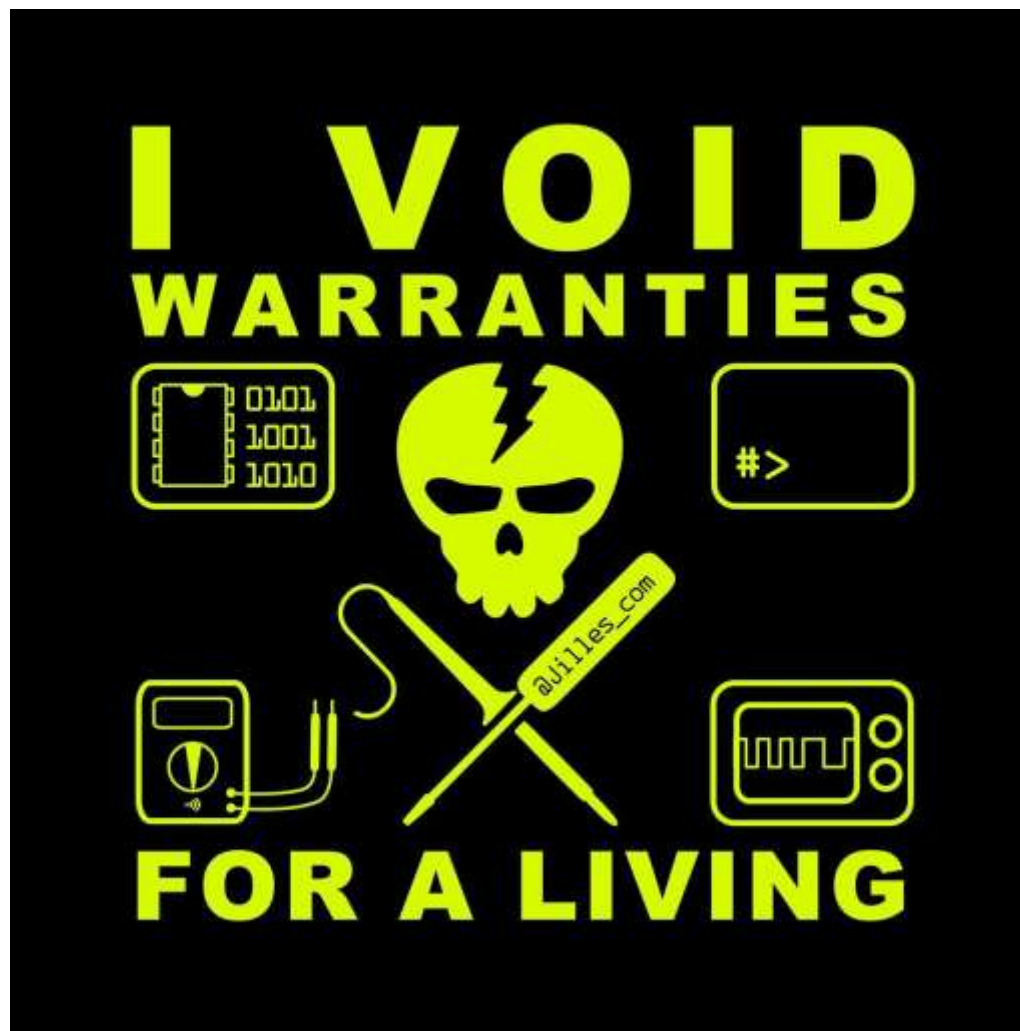


Hardware Hacking

Hardware Hacking
Jilles Groenendijk



twitter.com/jilles_com
twitch.tv/jilles_com
pscp.tv/jilles_com
youtube.com/jilles_com

Hardware Hacking

I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.
I will take personal responsibility for my own actions.



Hardware Hacking



HACKING
IS NOT A CRIME



hackingisnotacrime.org

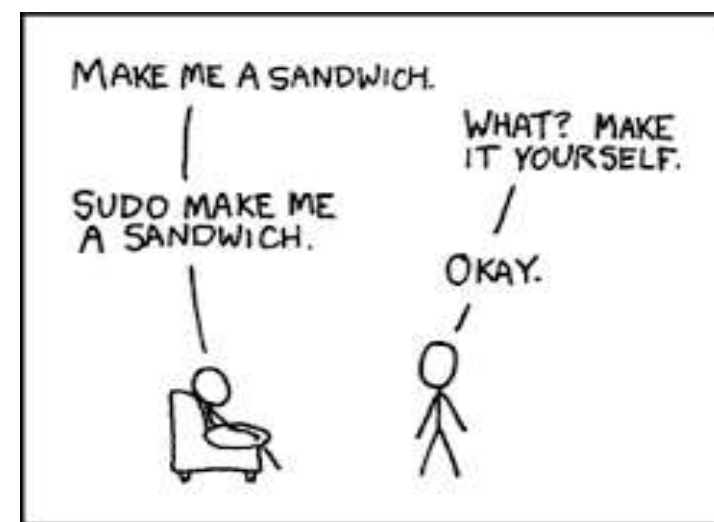
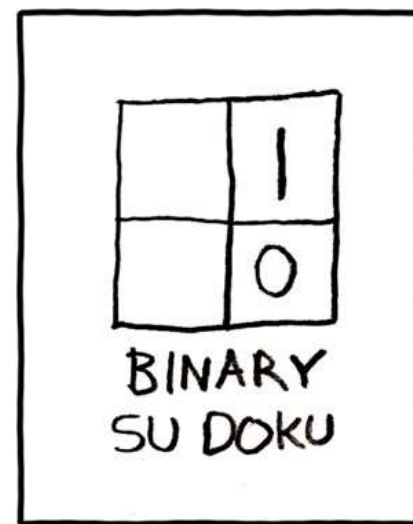


📍 NEDERLAND
Hacking is not a crime #HackerStories

Hardware Hacking

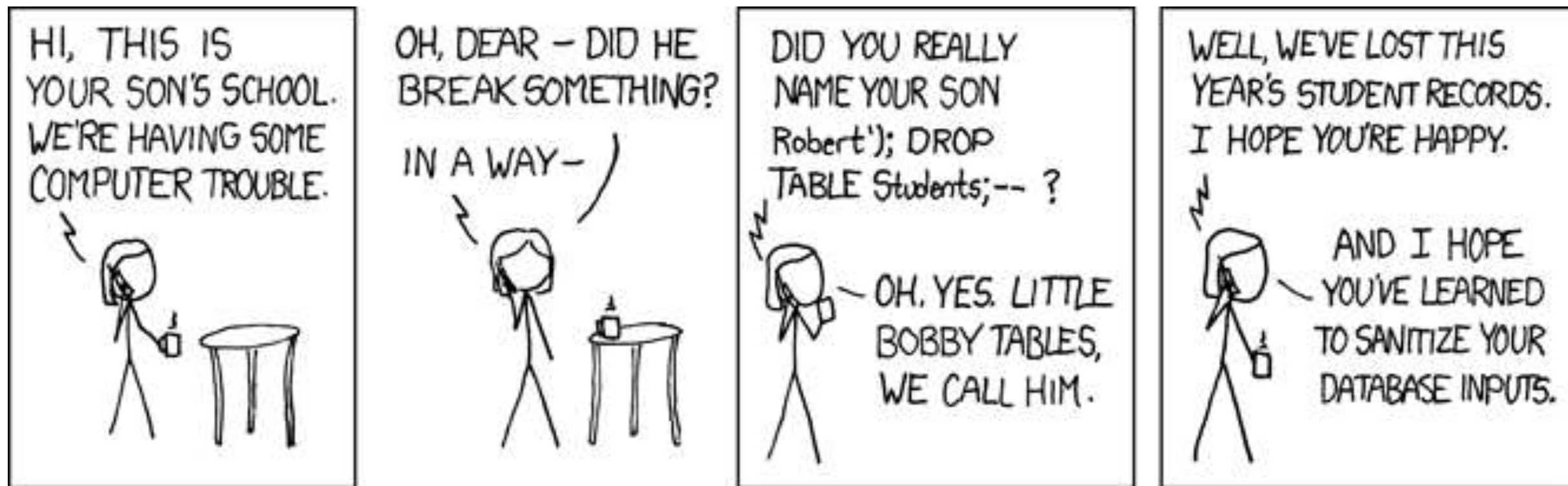


```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```



Learn how to code

Hardware Hacking



Learn how to hack

Hardware Hacking



Tinker with hardware

Hardware Hacking



007^T

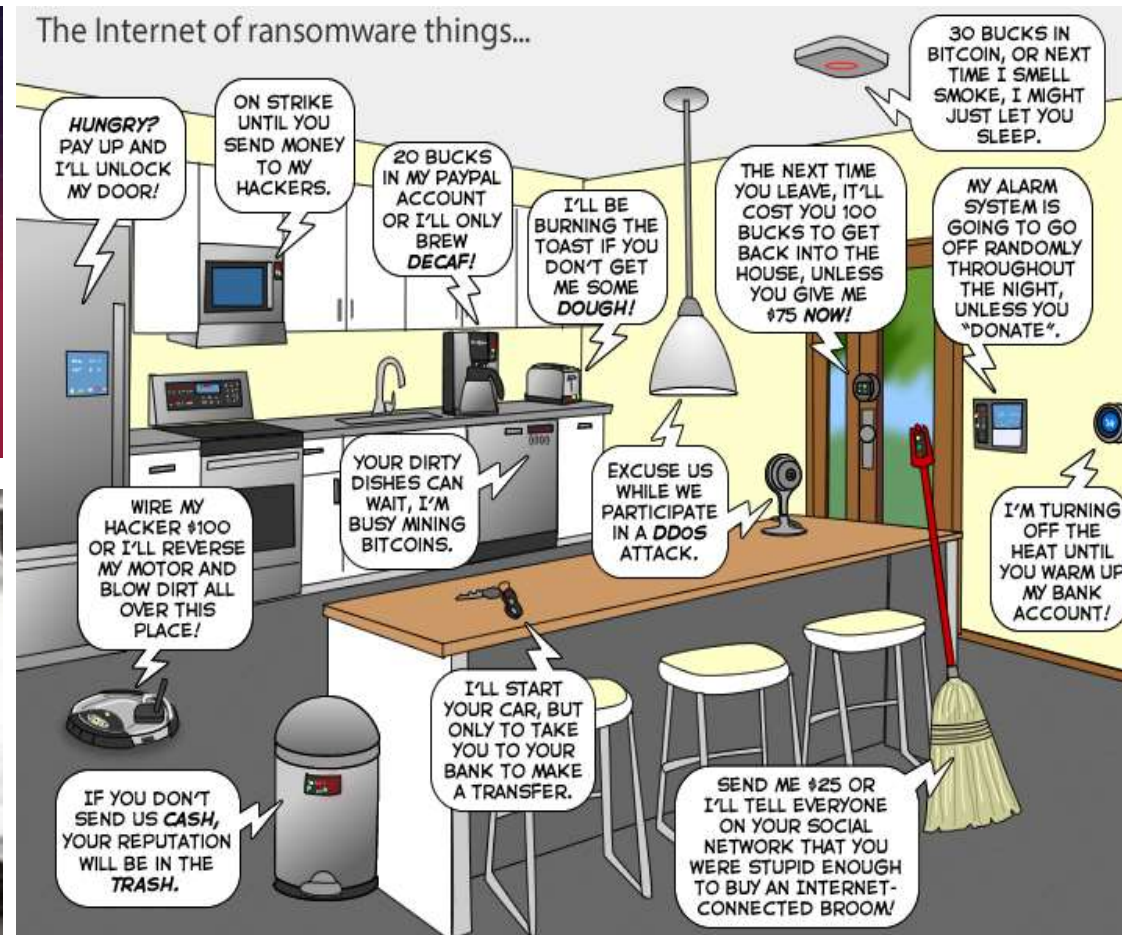
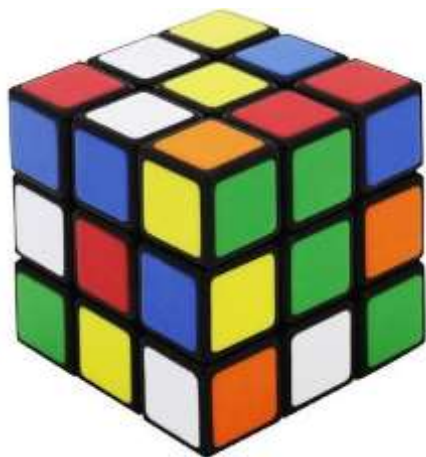


SNEAKERS



**TERMINATOR 2
JUDGMENT DAY**

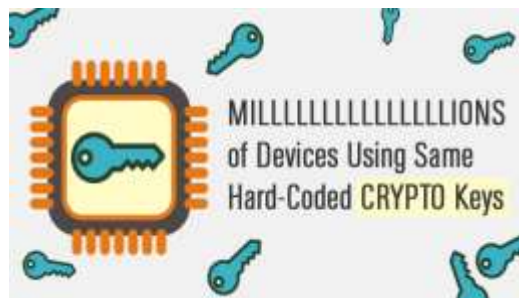
Hardware Hacking



Hardware Hacking



```
root@ubuntu:~# more /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/noologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:mailing list manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```



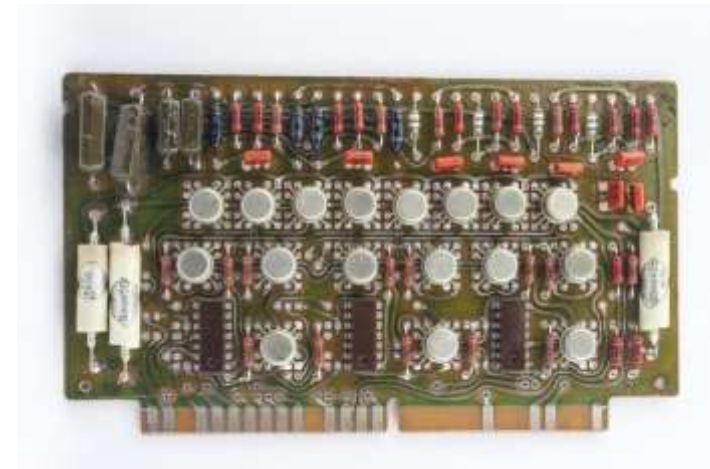
```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
             // guaranteed to be random.
}
```



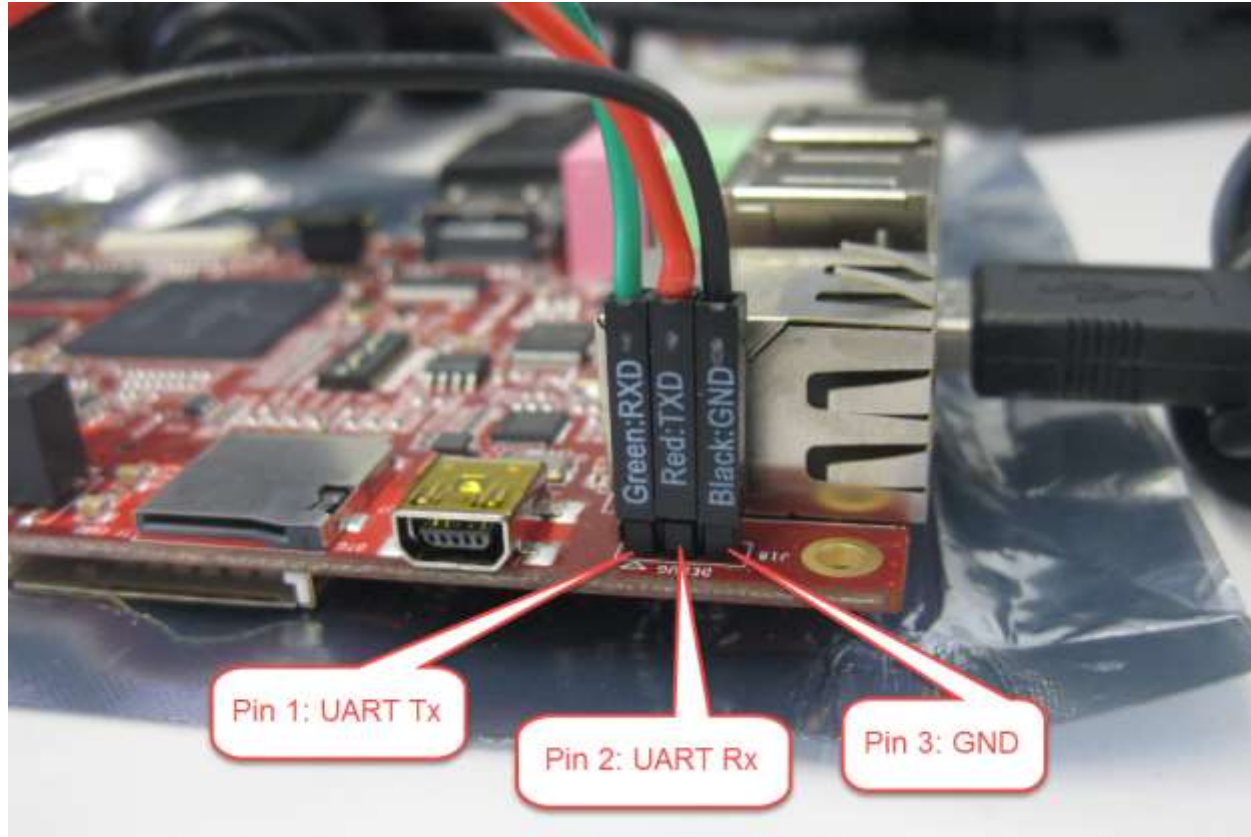
BEFORE



AFTER



Hardware Hacking



Got Root? ■

Hardware Hacking

Default Passwords | CIR

Default Passwords

528 vendors, 2102 passwords
@passdb on Twitter / Firefox Search

3COM	2Wire, Inc.	360 Systems
ACCTON	3M	Accelerated Networks
Adaptec	Acer	Adientec
AddPac Technology	ADC Kentrox	AdComplete.com
Adtech	Adobe	ADT
AIRAYA Corp	Adtran	Advanced Integration
Aironet	Airlink	AirLink Plus
Alcatel	Airway	Aladdin
	Allen Technology	Allied Telesyn

SHODAN

Home Search Directory Data Analytics/Exports Developer Center Labs

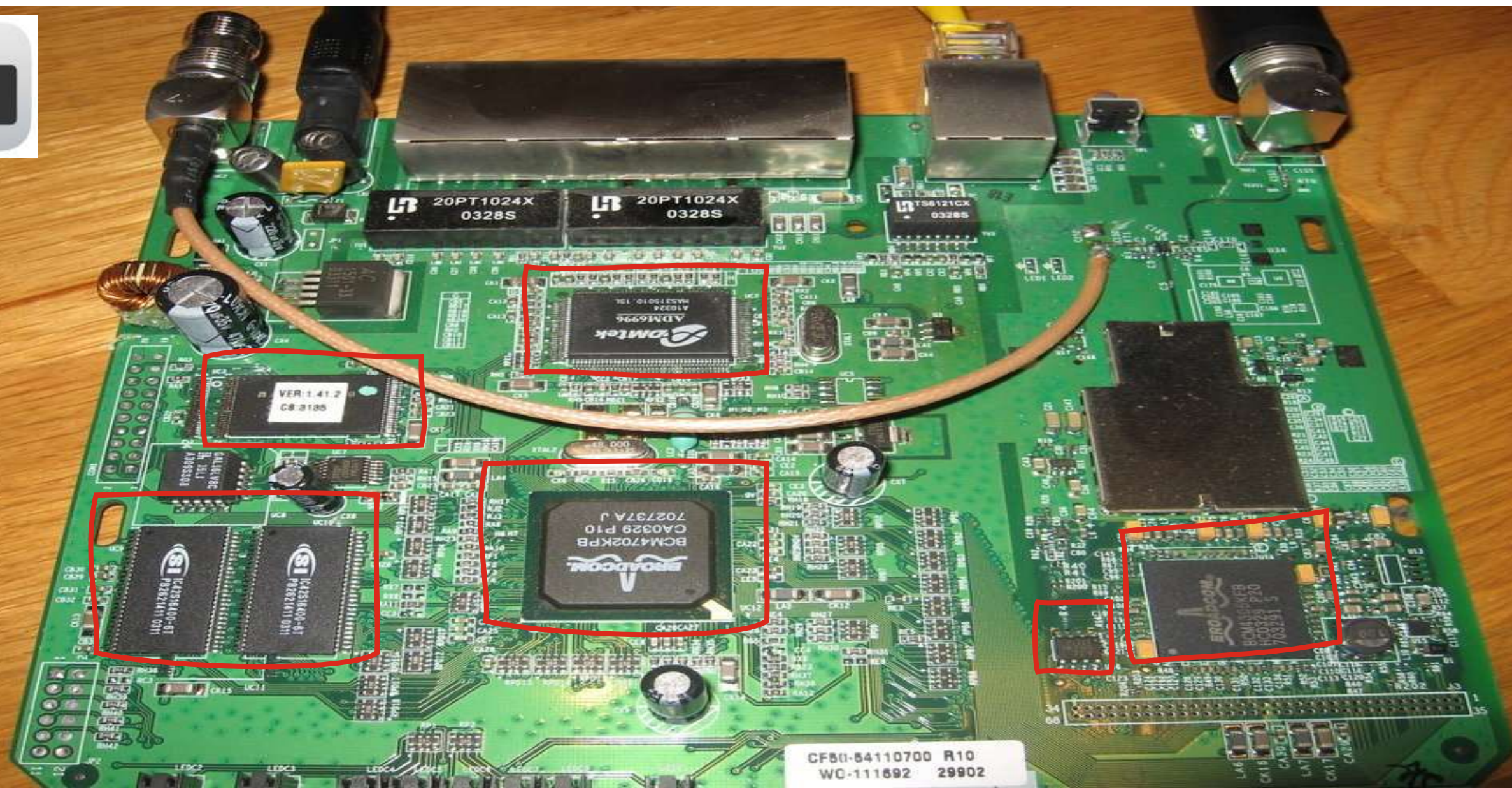
Results 1 - 10 of about 4359 for

Services Telnet 2,530 HTTP 852 HTTP Alternate 697 FTP 172 HTTPS 57	77 Kabel Deutschland Added on 02.09.2013 Gifhorn Details	DD-WRT v24-sp2 shf (c) 2013 NewMedia-NET GmbH Release: 03/25/13 (SVN revision: 21061) kd-router login:
Top Cities Berlin 330 Hamburg 155 Munich 134 Frankfurt Am Main 77 Wehlersbach 75	149 Kabel BW Added on 02.09.2013 Calw Details	DD-WRT v24-sp2 micro (c) 2009 NewMedia-NET GmbH Release: 05/21/09 (SVN revision: 12188) DD-WRT login:





Hardware Hacking



Hardware Hacking



LOGIC



EPROM



EEPROM



Hardware Hacking

STM32H742xI/G STM32H743xI/G

32-bit Arm® Cortex®-M7 480MHz MCUs, up to 2MB Flash, up to 1MB RAM, 46 com. and analog interfaces

Datasheet - production data

Features

Core

- 32-bit Arm® Cortex®-M7 core with double-precision FPU and L1 cache: 16 Kbytes of data and 16 Kbytes of instruction cache; frequency up to 480 MHz, MPU, 1027 DMIPS/2.14 DMIPS/MHz (Dhrystone 2.1), and DSP instructions

Memories

- Up to 2 Mbytes of Flash memory with read-while-write support
- Up to 1 Mbyte of RAM: 192 Kbytes of TCM RAM (inc. 64 Kbytes of ITCM RAM + 128 Kbytes of DTCM RAM for time critical routines), Up to 864 Kbytes of user SRAM, and 4 Kbytes of SRAM in Backup domain
- Dual mode Quad-SPI memory interface running up to 133 MHz
- Flexible external memory controller with up to 32-bit data bus: SRAM, PSRAM, SDRAM/LPDDR SDRAM, NOR/NAND Flash memory clocked up to 100 MHz in Synchronous mode
- CRC calculation unit

Security

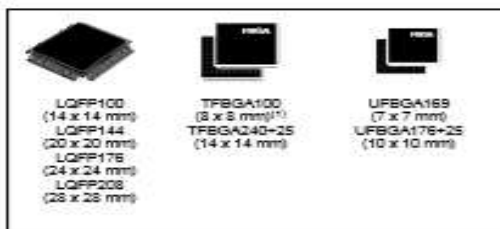
- ROP, PC-ROP, active tamper

General-purpose input/outputs

- Up to 168 I/O ports with interrupt capability

Reset and power management

- 3 separate power domains which can be independently clock-gated or switched off:
 - D1: high-performance capabilities
 - D2: communication peripherals and timers
 - D3: reset/clock control/power management



- 1.62 to 3.6 V application supply and I/Os
- POR, PDR, PVD and BOR
- Dedicated USB power embedding a 3.3 V internal regulator to supply the internal PHYs
- Embedded regulator (LDO) with configurable scalable output to supply the digital circuitry
- Voltage scaling in Run and Stop mode (6 configurable ranges)
- Backup regulator (~0.9 V)
- Voltage reference for analog peripheral/V_{REF}
- Low-power modes: Sleep, Stop, Standby and V_{BAT} supporting battery charging

Low-power consumption

- V_{BAT} battery operating mode with charging capability
- CPU and domain power state monitoring pins
- 2.95 µA in Standby mode (Backup SRAM OFF, RTC/LSE ON)

Clock management

- Internal oscillators: 64 MHz HSI, 48 MHz HSI48, 4 MHz CSI, 32 kHz LSI
- External oscillators: 4-48 MHz HSE, 32.768 kHz LSE
- 3× PLLs (1 for the system clock, 2 for kernel clocks) with Fractional mode

Pin descriptions

STM32H742xI/G STM32H743xI/G

Table 9. Pin/ball definition (continued)

Pin/ball name								Pin name (function after reset)	Pin type	I/O structure	Notes	Alternate functions	Additional functions
LQFP100	TFBGA100	LQFP144	UFBGA169	UFBGA176+25	LQFP176	LQFP208	TFBGA240+25						
68	C9	101	E11	E15	120	143	D15	PA9	I/O	FT_u	-	TIM1_CH2, HRTIM_CHC1, LPUART1_TX, I2C3_SMB, SPI2_SCK/I2S2_CK, USART1_TX, FDCAN1_RXFD_MODE, DCM1_D0, LCD_R5, EVENTOUT	OTG_FS_VBUS
69	D10	102	E10	D15	121	144	D14	PA10	I/O	FT_u	-	TIM1_CH3, HRTIM_CHC2, LPUART1_RX, USART1_RX, FDCAN1_TXFD_MODE, OTG_FS_ID, MDIO8_MDIO, LCD_B4, DCM1_D1, LCD_B1, EVENTOUT	-
70	C10	103	F13	C15	122	145	E17	PA11	I/O	FT_u	-	TIM1_CH4, HRTIM_CHD1, LPUART1_CTS, SPI2_NSS/I2S2_WS, UART4_RX, USART1_CTS/USART1_NSS, FDCAN1_RX, OTG_FS_DM, LCD_R4, EVENTOUT	-
71	B10	104	E13	B15	123	146	E16	PA12	I/O	FT_u	-	TIM1_ETR, HRTIM_CHD2, LPUART1_RTS, LPUART1_DE, SPI2_SCK/I2S2_CK, UART4_TX, USART1_RTS/USART1_DE, SA12_FS_B, FDCAN1_TX, OTG_FS_DP, LCD_R5, EVENTOUT	-
72	A10	105	D11	A15	124	147	C15	PA13 (JTMS/BW DIO)	I/O	FT	-	JTMS-BW DIO, EVENTOUT	-
73	E7	106	D13	F13	125	148	D17	VCAP	S	-	-	-	-
74	E5	107	-	F12	126	149	-	VSS	S	-	-	-	-
-	-	-	D12	-	-	-	C17	VDD_LDO (S)	-	-	-	-	-
75	-	108	-	G13	127	150	K5	VDD	S	-	-	-	-

Hardware Hacking

CE 0984

MODEL : SIP005AFS30
IC : 640E-SIP005AFS30
FCC ID : A3LSIP005AFS30
RATE : 4.2V 5A

삼성전자(주)

WSARM530A00
Made in Korea

SN : 530MWB9710400001
MAC ID(W): 702C1F1CE0AF
MAC ID(B): 702C1F1CE0B0

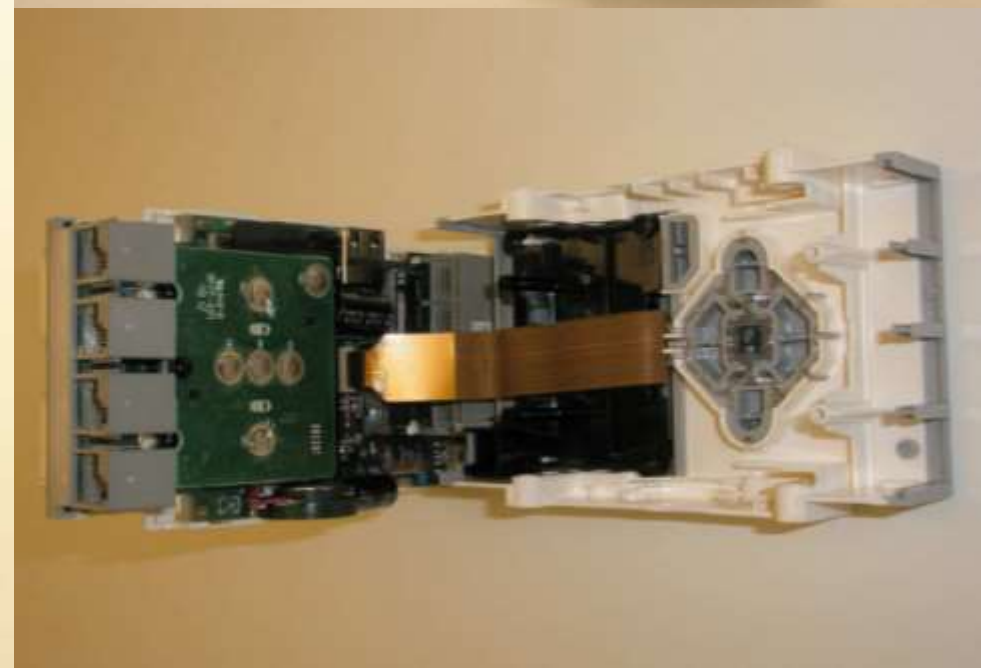
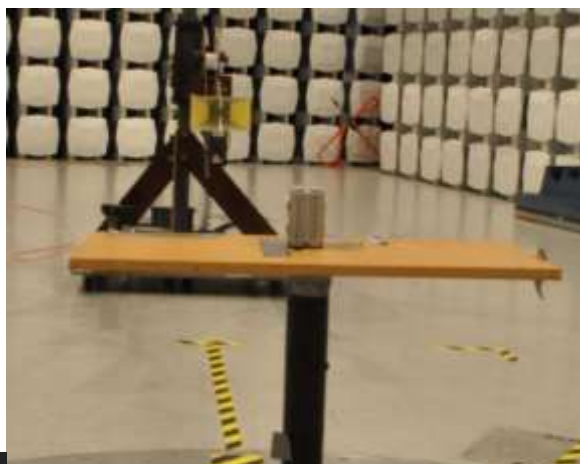


FCC ID: Search

Frequency Range	Power Output	Rule Parts	Line Entry
2.402-2.48 GHz	10 mW	15C	1

Exhibits

Document	Type	Submitted Available
User manual part 3	User Manual Adobe Acrobat PDF (387 KB)	2013-09-26 2013-09-26
User manual part 2	User Manual Adobe Acrobat PDF (1588 KB)	2013-09-26 2013-09-26
User manual part 1	User Manual Adobe Acrobat PDF (2488 KB)	2013-09-26 2013-09-26
Test setup	Test Setup Photos Adobe Acrobat PDF (385 KB)	2013-09-26 2013-09-26
Test report	Test Report Adobe Acrobat PDF (2599 KB)	2013-09-26 2013-09-26
RF Exposure Info MPE	RF Exposure Info Adobe Acrobat PDF (22 KB)	2013-09-26 2013-09-26
Internal photos	Internal Photos Adobe Acrobat PDF (717 KB)	2013-09-26 2013-09-26
Label	ID Label/Location Info JPEG image (1875 KB)	2013-09-26 2013-09-26
External photos	External Photos Adobe Acrobat PDF (288 KB)	2013-09-26 2013-09-26



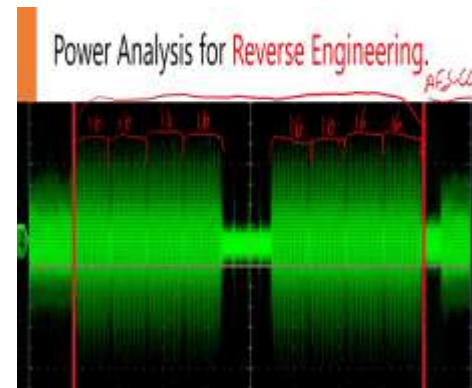
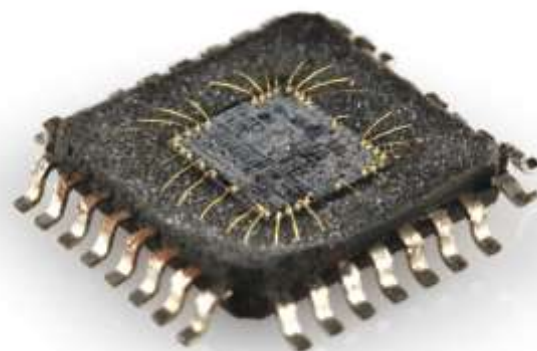
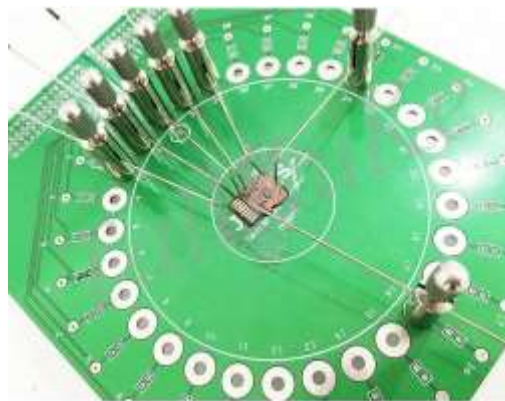
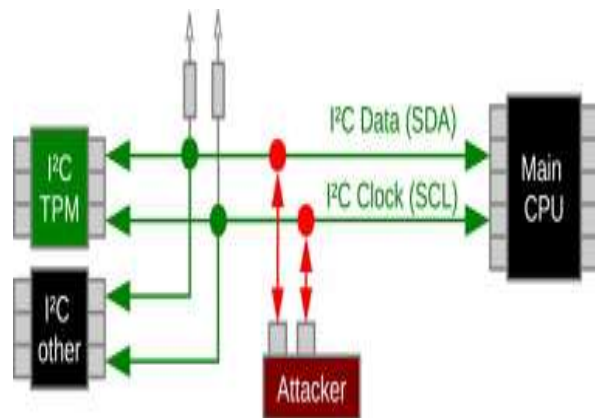
Hardware Hacking

Defeat security mechanisms that are not possible to defeat via software in order to gain access by using:

- Console ports such as UART
- Provisioning ports such as JTAG
- Read communication between processor and memory module via I2C or SPI
- Dump the contents of the chips to read (is it encrypted at rest/in transit)
- Introduce faults by modifying Clock, temperature, light, magnetic radiation or power



Hardware Hacking



Hardware Hacking



WHOZ DT83B Digital Multimeter AC DC Voltage Current Resistance Diode Tester

★★★★★ 25 Reviews | Questions & Answers ID: 1189566

Price: **4,92€** ~~7,32€~~ **33% Off**

Promo: **SALE** Order 2, get 6% off = [Go to see](#)

Coupon: **\$20 for New User**

Ship From: **CN**

Dispatch: Processing time: 8 business days

Shipping: **2,24€**
to Netherlands via Air Parcel Register +
Shipping time: 20-35 business days (1)

Quantity: **1**

[Buy Now](#)

[Add to Cart](#)

[Add to Wishlist \(14\)](#)



FT232RL FTDI USB To TTL Serial Converter Adapter Module Geekcreit for Arduino - products that work with official Arduino boards

Brand: **Geekcreit** ★★★★★ 2791 Reviews | 10 answered questions ID: 917208

Price: **2,68€** ~~5,44€~~ **58% Off**

Promotion Sale From June 1 to June 30.

Coupon: **\$20 for New User**

Ship From: **CN** **USA** **UK**

Dispatch: **In stock**. Processing time: Ships in 24 hours

Shipping: **2,24€**
to Netherlands via Air Parcel Register +
Shipping time: 20-35 business days (1)

Quantity: **1**

[Buy Now](#)

[Add to Cart](#)

[Add to Wishlist \(6429\)](#)

€13,25



120pcs 20cm Male To Female Female To Female Male To Male Color Breadboard Jumper Cable Dupont Wire Combination For

Brand: **Geekcreit** ★★★★★ 1382 Reviews | 9 answered questions ID: 970206

Price: **4,04€** ~~6,06€~~ **34% Off**

Coupon: **\$20 for New User**

Ship From: **CN** **USA**

Dispatch: **In stock**. Processing time: Ships in 24 hours

Shipping: **2,24€**
to Netherlands via Air Parcel Register +
Shipping time: 20-35 business days (1)

Quantity: **1**

[Buy Now](#)

[Add to Cart](#)

[Add to Wishlist \(774\)](#)



DANIU Mini Alligator Clip Test Lead Cable for Digital Multimeters

Brand: **DANIU** ★★★★★ 143 Reviews | Questions & Answers ID: 930458

Price: **1,61€** ~~2,46€~~ **34% Off**

Promo: **SALE** Order 2, get 6% off = [Go to see](#)

Coupon: **\$20 for New User**

Ship From: **CN**

Dispatch: **In stock**. Processing time: Ships in 24 hours

Shipping: **2,24€**
to Netherlands via Air Parcel Register +
Shipping time: 20-35 business days (1)

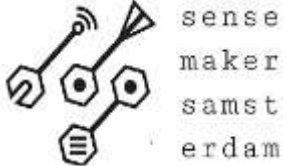
Quantity: **1**

[Buy Now](#)

[Add to Cart](#)

[Add to Wishlist \(774\)](#)

<https://unrollthread.com/t/1282266525781688320/>



Hardware Hacking

The Hacker's Hardware Toolkit awesome hacking hardware toolkit awesome



The best collection of hardware gadgets for Red Team hackers, pentesters and security researchers! It includes more than one hundred of tools classified in eight different categories, to make it easier to search and to browse them.



Google

git hardware hacking toolkit



All

Images

Videos

Shopping

News

More

Settings

Tools

About 503.000 results (0,59 seconds)

github.com › yadox666 › The-Hackers-Hardware-Toolkit ▾

[yadox666/The-Hackers-Hardware-Toolkit: The best ... - GitHub](#)

The best **hacker's** gadgets for Red Team pentesters and security researchers. - yadox666/The-Hackers-Hardware-Toolkit.