

De wonderre wereld van HW Hacking



Platform voor Informatie Beveiliging



Jilles



Jurre

Shoot ALL The Hackers!



Dennis van Zijlekom

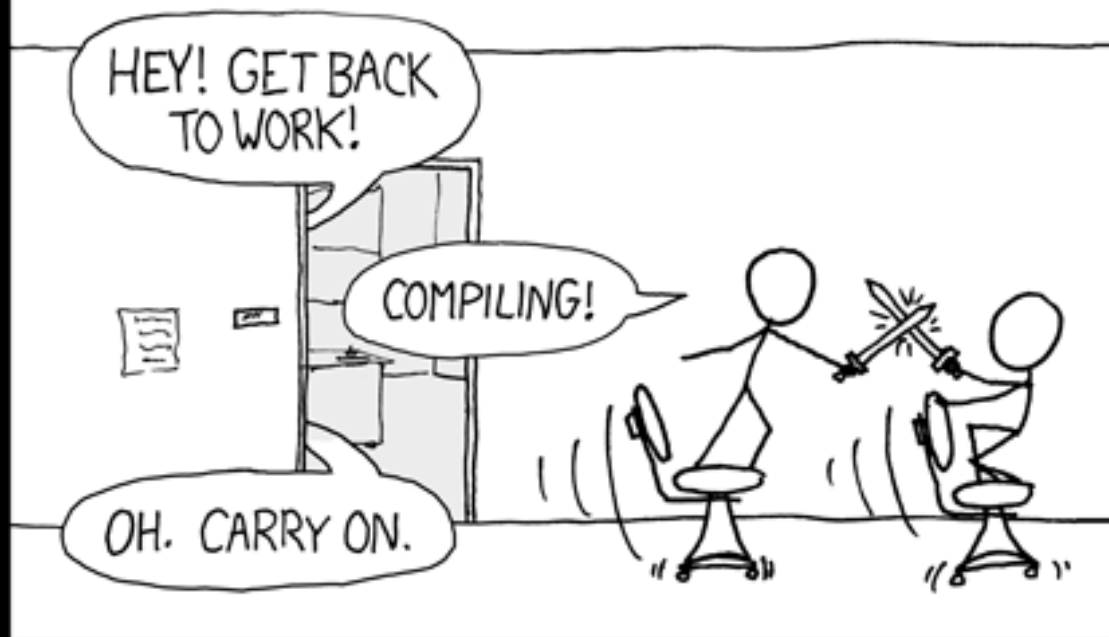
POLL

Poll 1/3: are you a maker?



Poll 2/3: do you program?

THE #1 PROGRAMMER EXCUSE
FOR LEGITIMATELY SLACKING OFF:
"MY CODE'S COMPILING."



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



Poll 3/3: do you hack?

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.



OH, DEAR - DID HE BREAK SOMETHING?

IN A WAY--



DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?



OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.

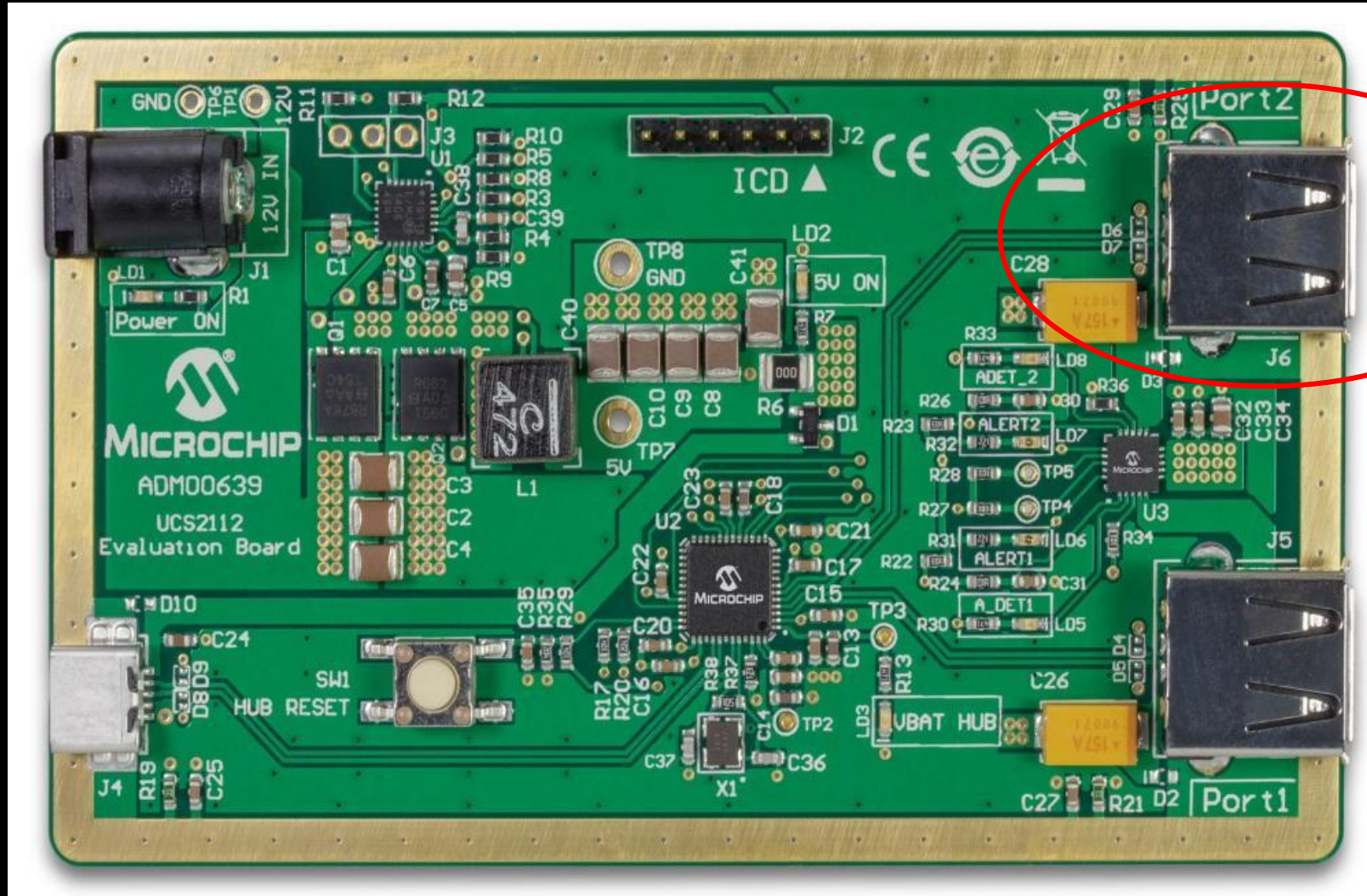
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.



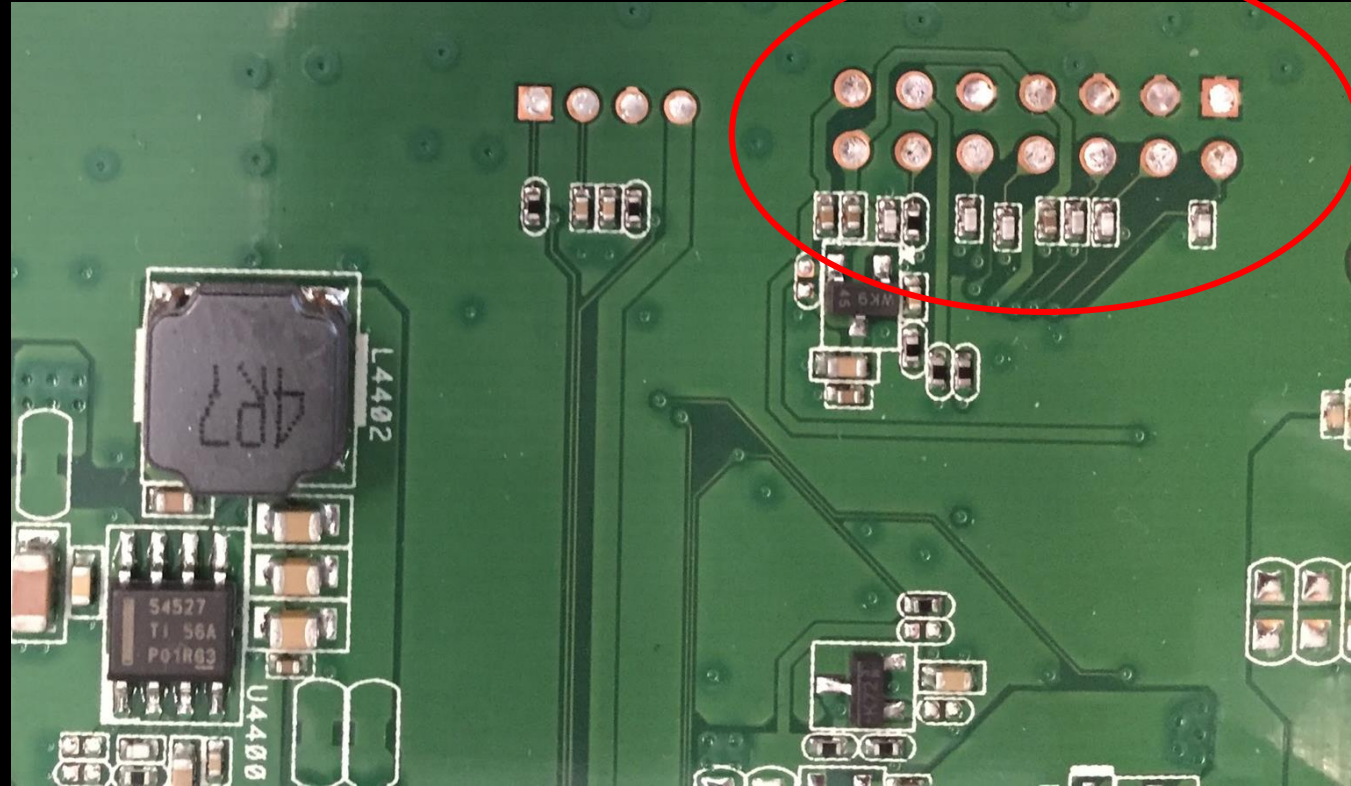
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

QUIZ

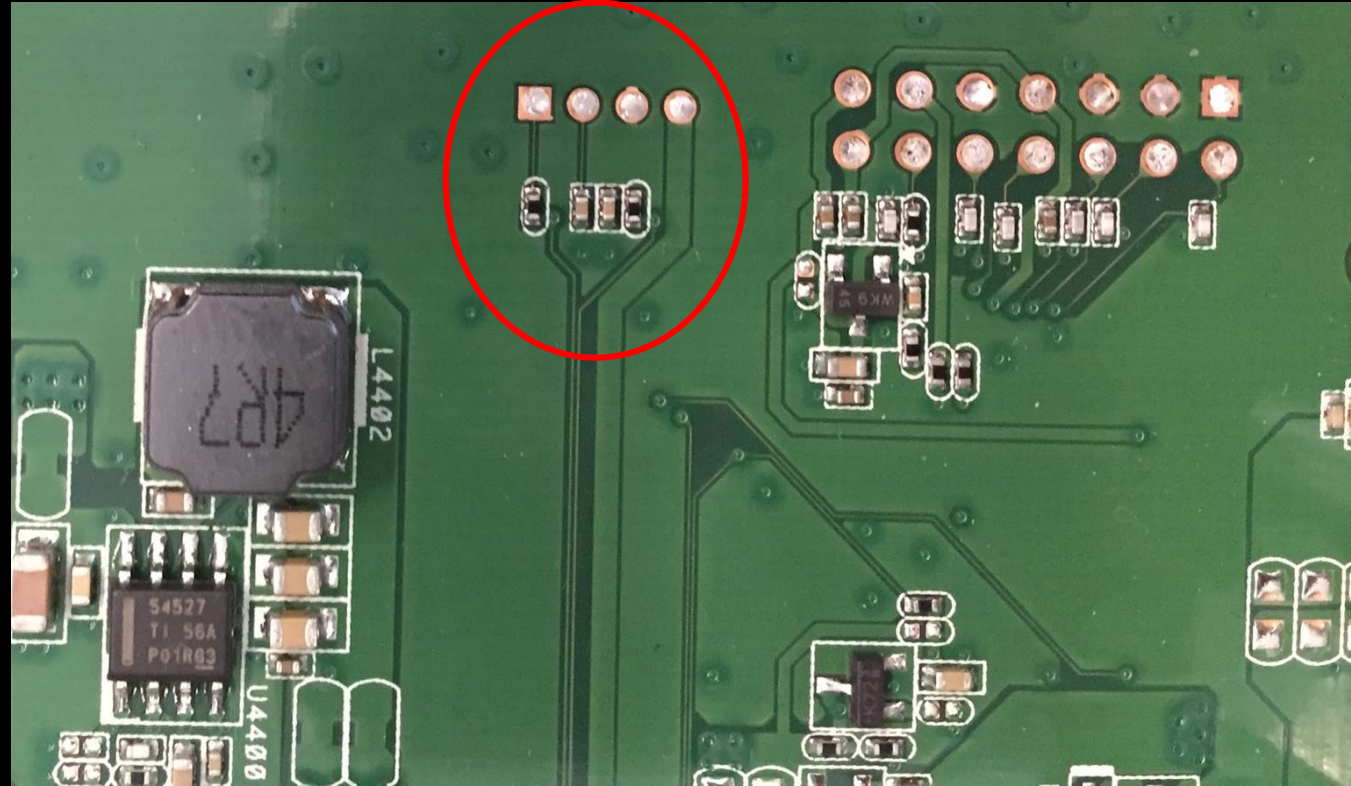
Quiz 1/13: name the port



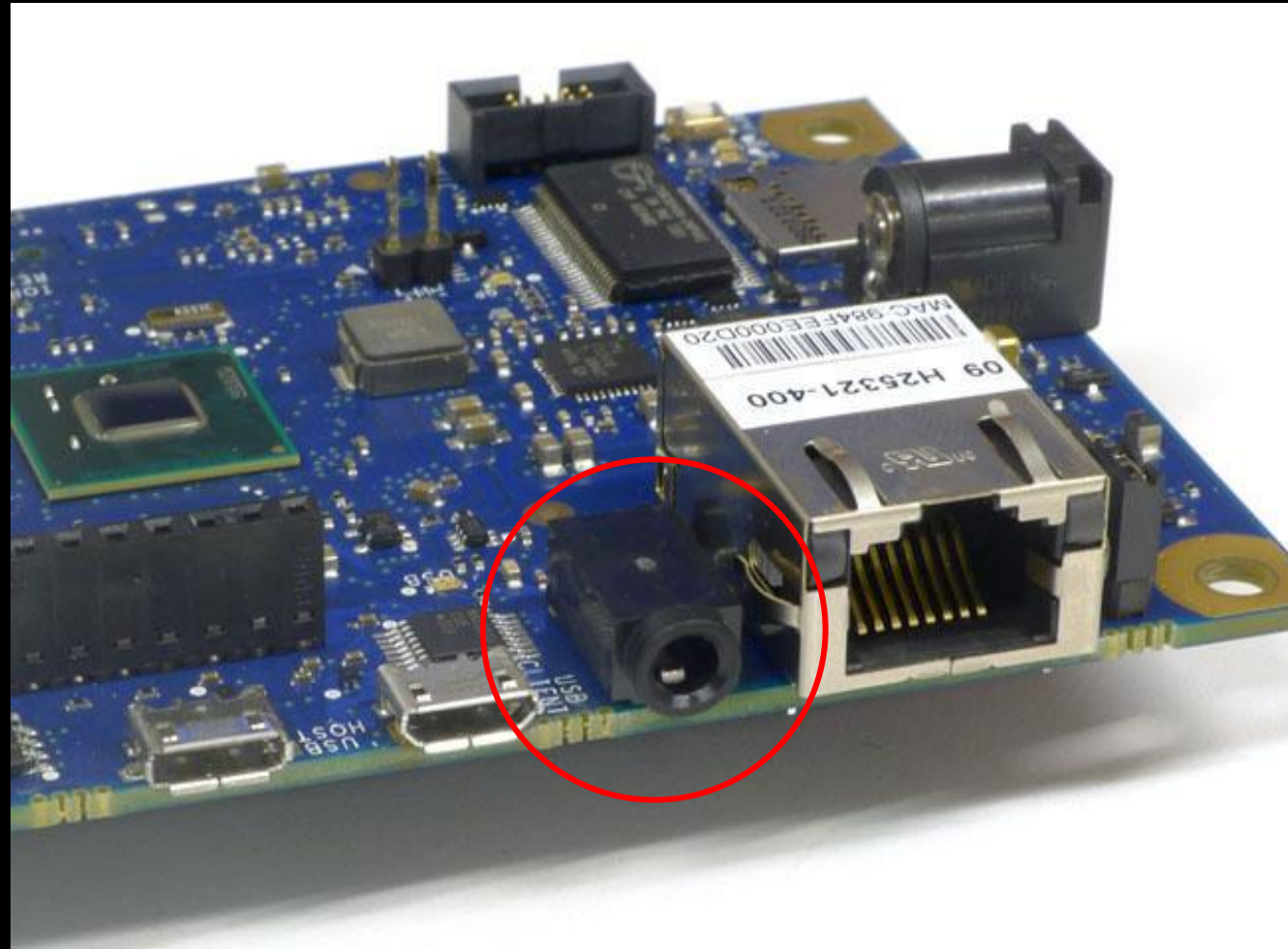
Quiz 2/13: name the port



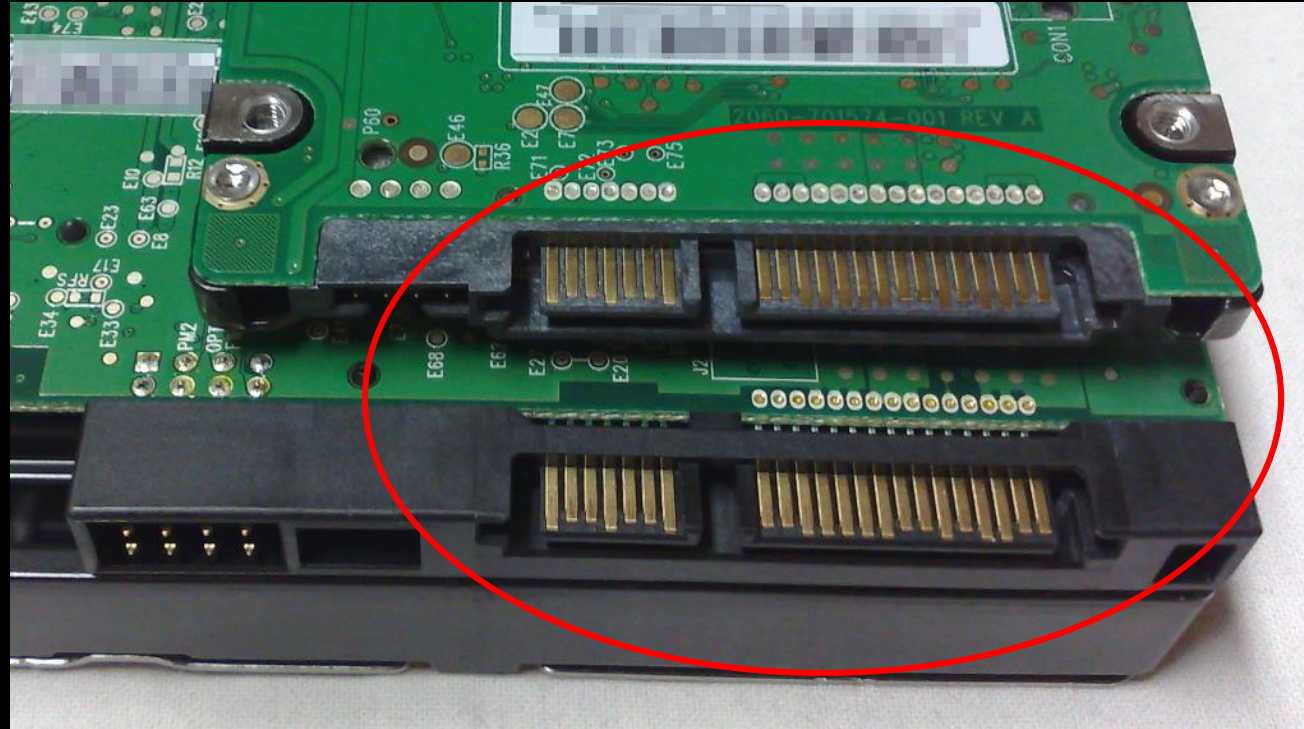
Quiz 3/13: name the port



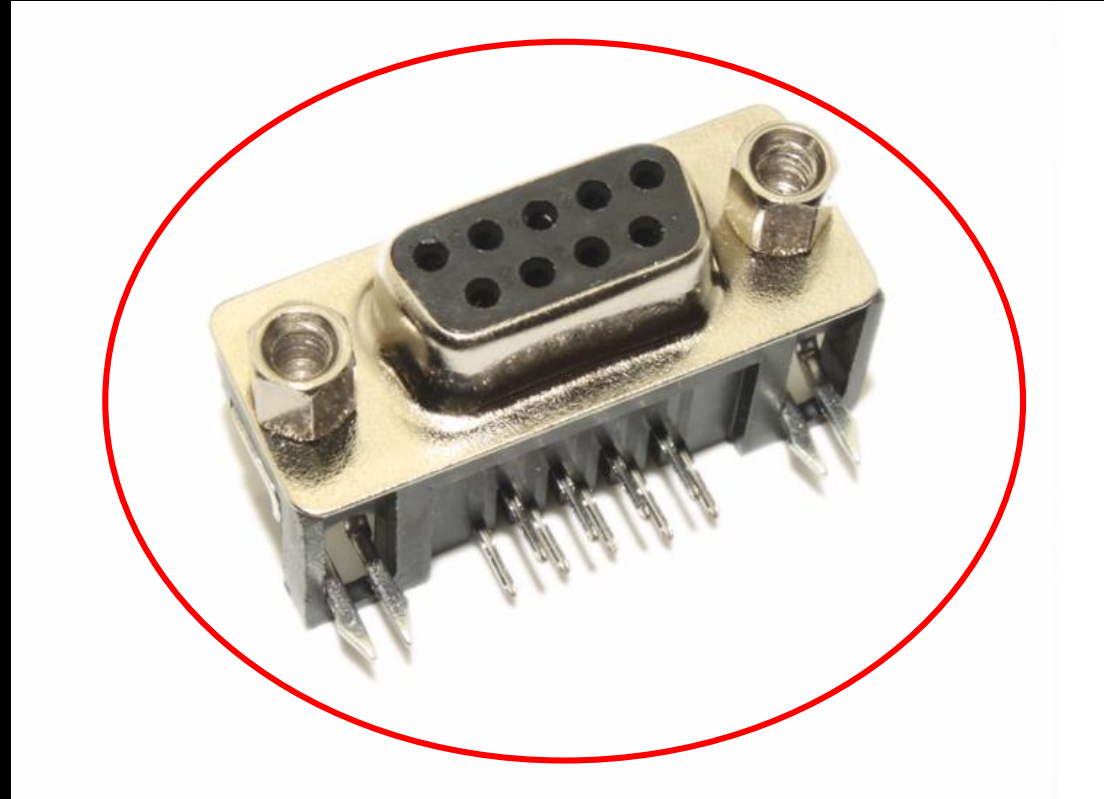
Quiz 4/13: name the port



Quiz 5/13: name the port



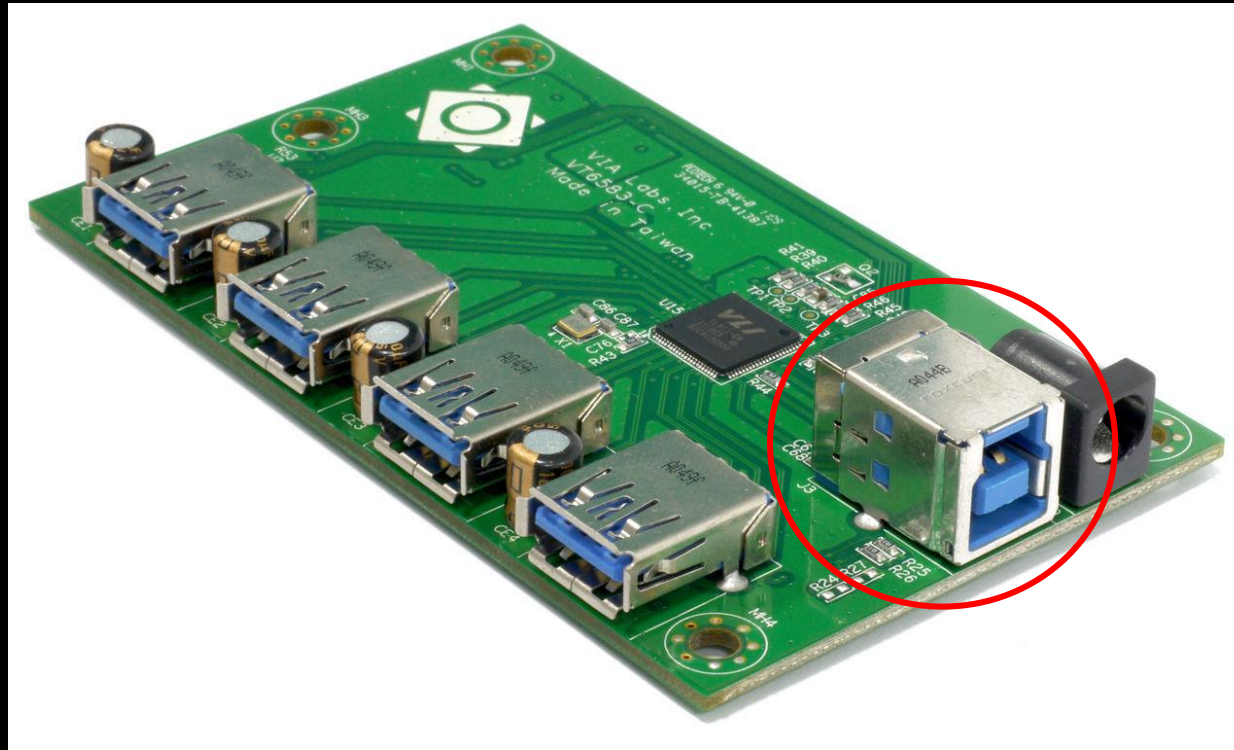
Quiz 6/13: name the port



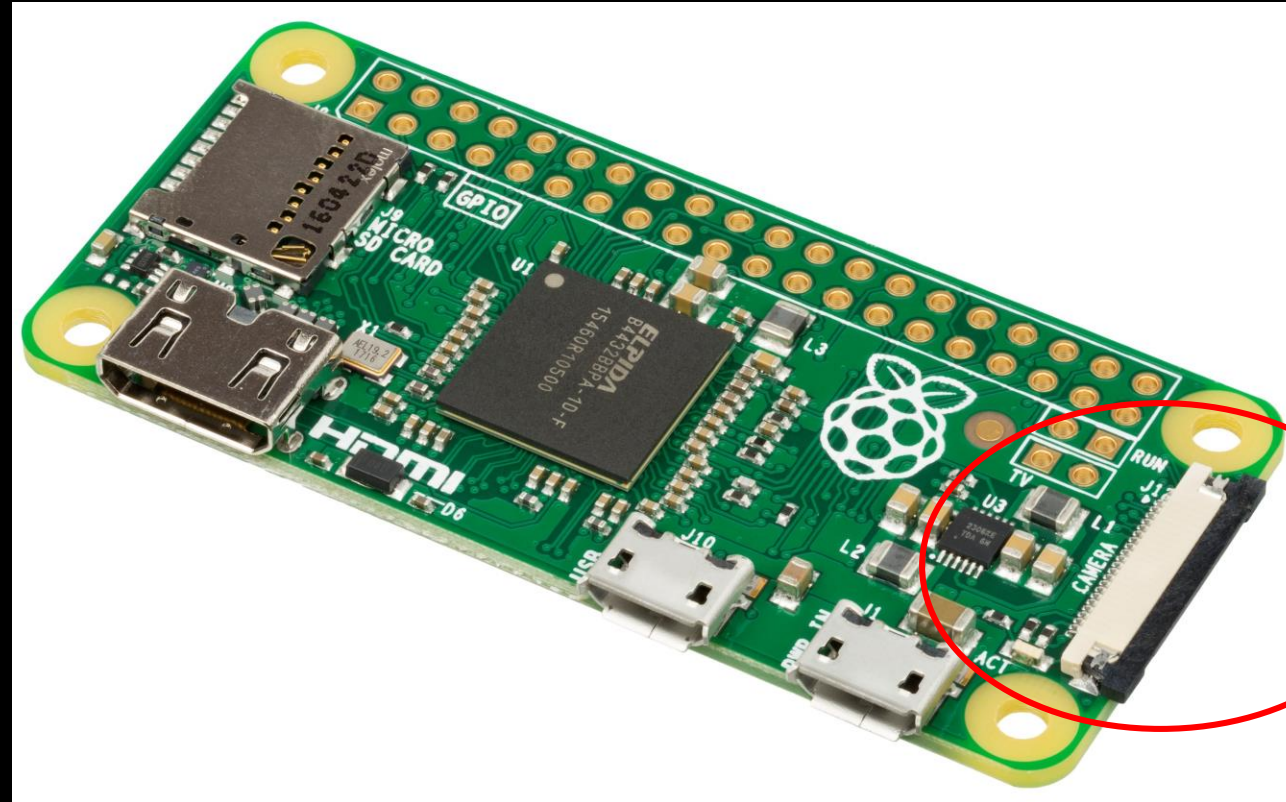
Quiz 7/13: name the port



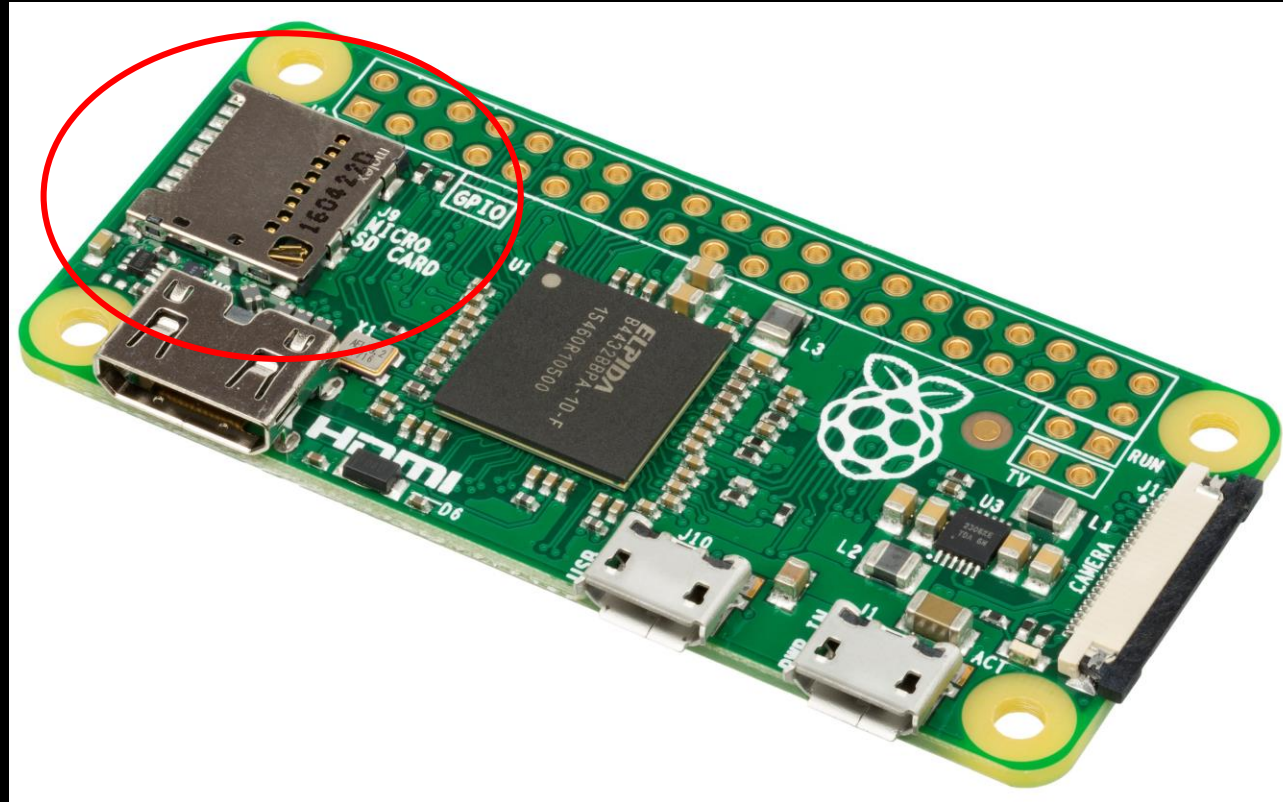
Quiz 8/13: name the port



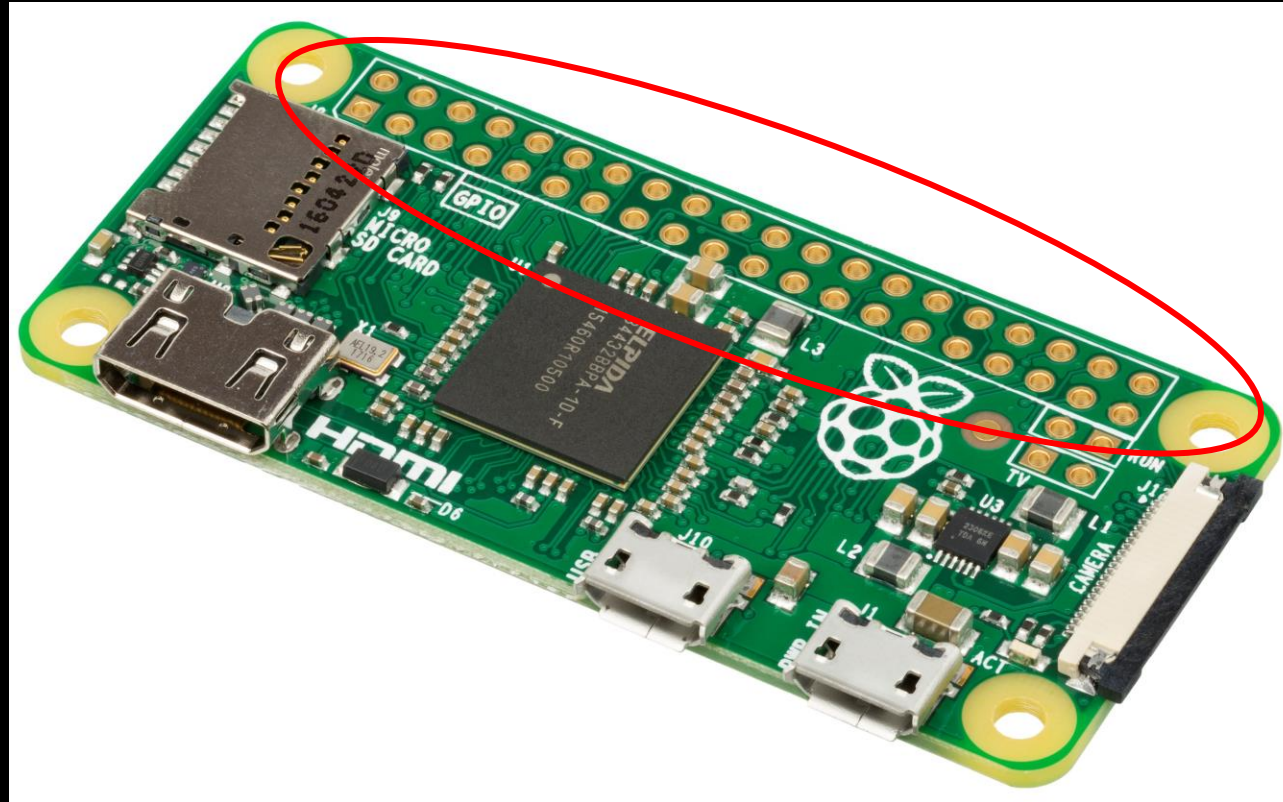
Quiz 9/13: name the port



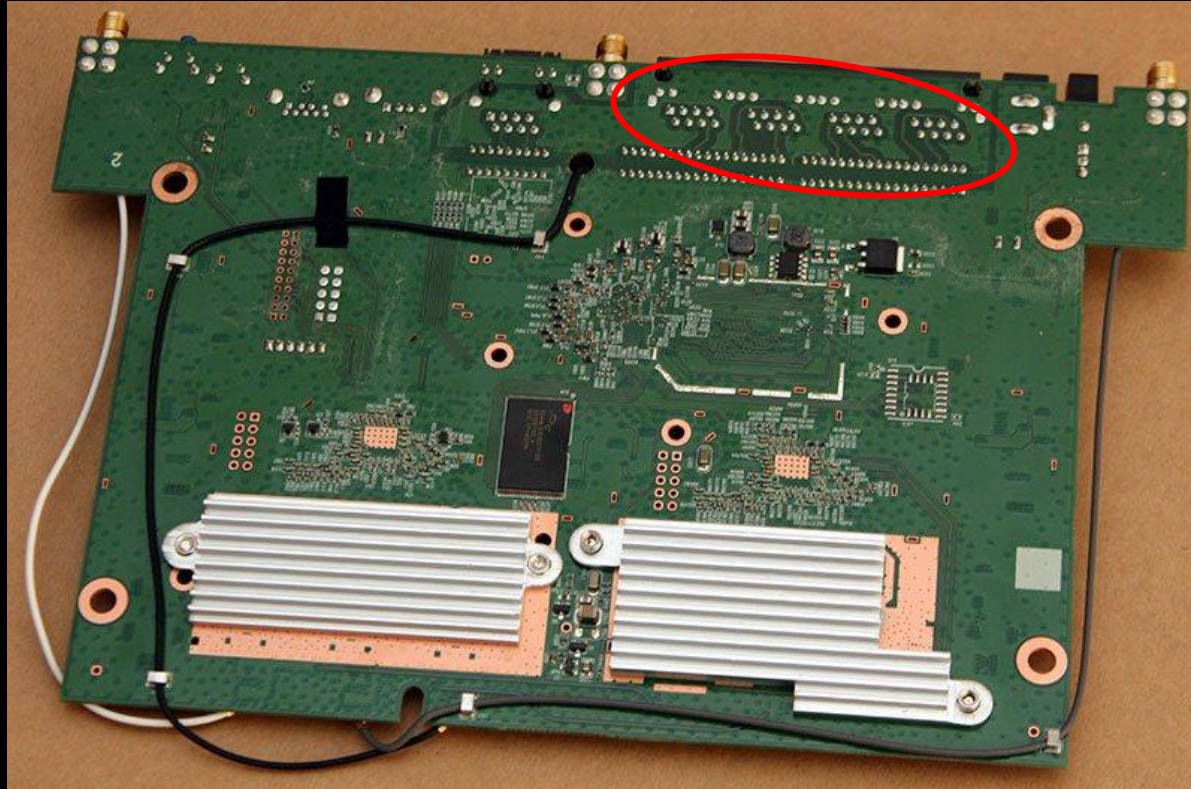
Quiz 10/13: name the port



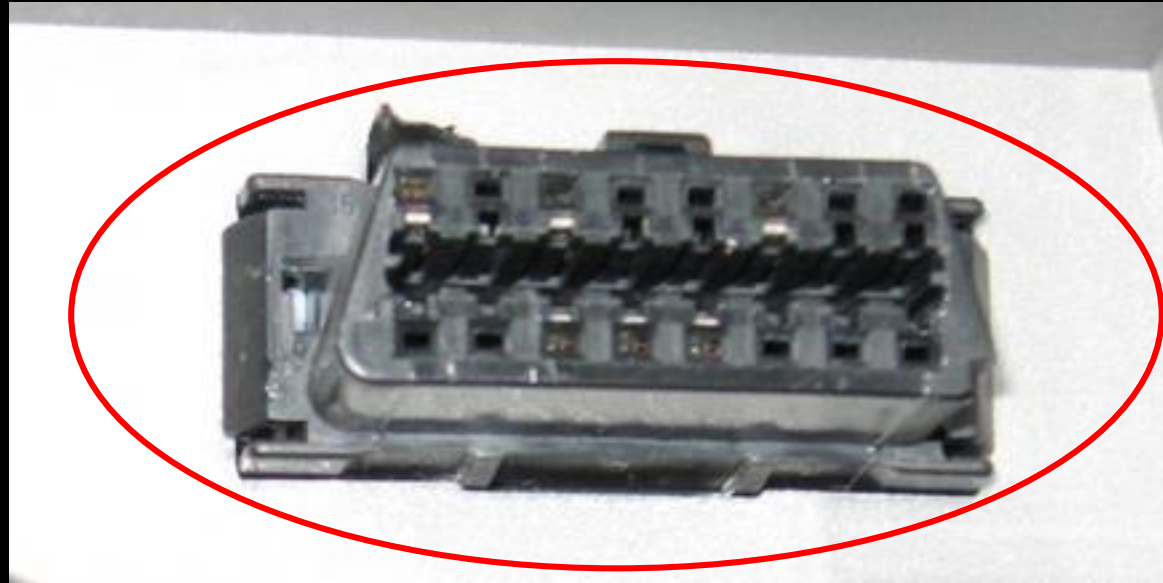
Quiz 11/13: name the port



Quiz 12/13: name the port



Quiz 13/13: name the port



Lets talk about

/me



Jilles Groenendijk
49 years old
LTS Electrotechniek



Trip down memory lane



4 Generations



Scrapbox



Magical box



“Does he take stuff apart?”



Always!

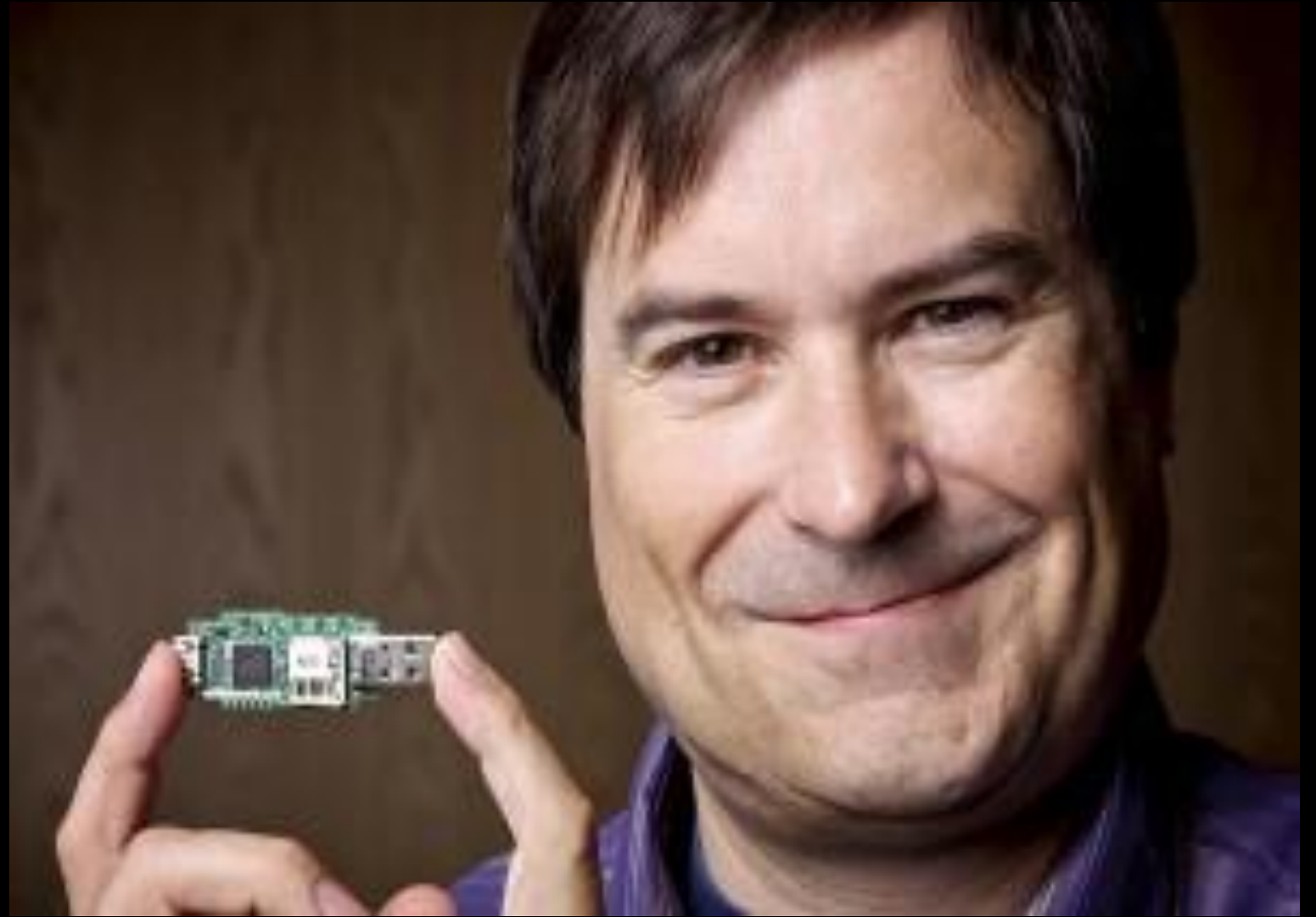
Discovering AC/DC



Causing outages

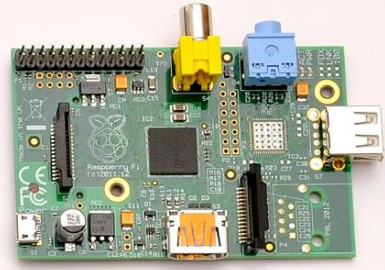


David Braben



Raspberry Pi

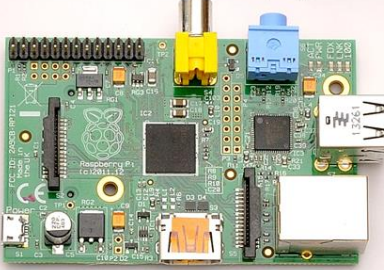
Model A



Rev 1 model B



Rev 2 model B (UK)



Model A+



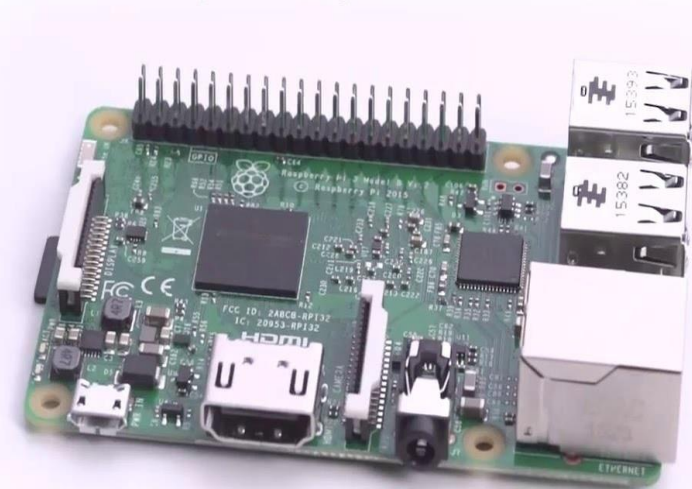
Model B+



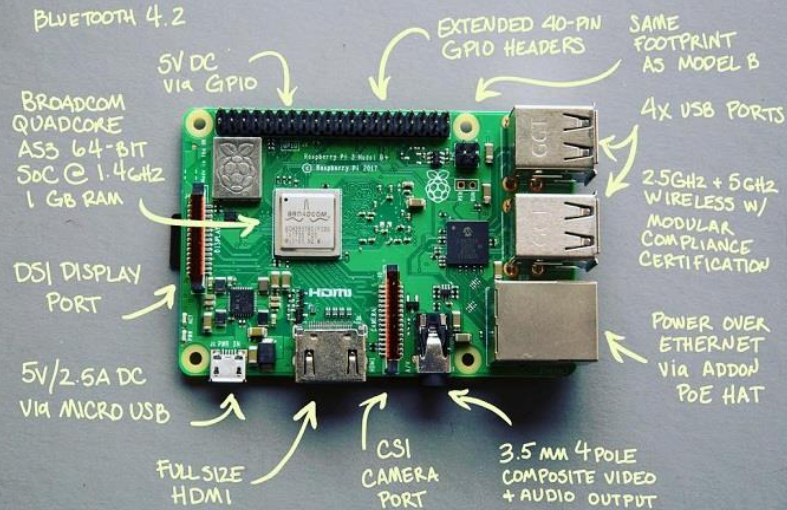
Zero



Raspberry Pi 3 Model B



Meet Raspberry Pi 3 Model B+

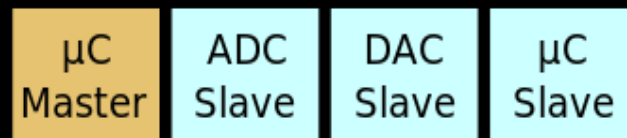


Learning the protocols

| Raspberry Pi2 GPIO Header | | | |
|---------------------------|------------------------------------|--|---------------------------------------|
| Pin# | NAME | | NAME Pin# |
| 01 | 3.3v DC Power | | DC Power 5v 02 |
| 03 | GPIO02 (SDA1, I ² C) | | DC Power 5v 04 |
| 05 | GPIO03 (SCL1, I ² C) | | Ground 06 |
| 07 | GPIO04 (GPIO_GCLK) | | (TXD0) GPIO14 08 |
| 09 | Ground | | (RXD0) GPIO15 10 |
| 11 | GPIO17 (GPIO_GEN0) | | (GPIO_GEN1) GPIO18 12 |
| 13 | GPIO27 (GPIO_GEN2) | | Ground 14 |
| 15 | GPIO22 (GPIO_GEN3) | | (GPIO_GEN4) GPIO23 16 |
| 17 | 3.3v DC Power | | (GPIO_GEN5) GPIO24 18 |
| 19 | GPIO10 (SPI_MOSI) | | Ground 20 |
| 21 | GPIO09 (SPI_MISO) | | (GPIO_GEN6) GPIO25 22 |
| 23 | GPIO11 (SPI_CLK) | | (SPI_CE0_N) GPIO08 24 |
| 25 | Ground | | (SPI_CE1_N) GPIO07 26 |
| 27 | ID_SD (I ² C ID EEPROM) | | (I ² C ID EEPROM) ID_SC 28 |
| 29 | GPIO05 | | Ground 30 |
| 31 | GPIO06 | | GPIO12 32 |
| 33 | GPIO13 | | Ground 34 |
| 35 | GPIO19 | | GPIO16 36 |
| 37 | GPIO26 | | GPIO20 38 |
| 39 | Ground | | GPIO21 40 |

Rev. 1
28/01/2014

<http://www.element14.com>



```

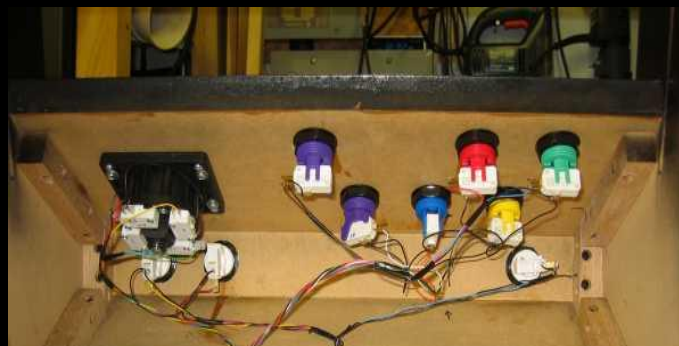
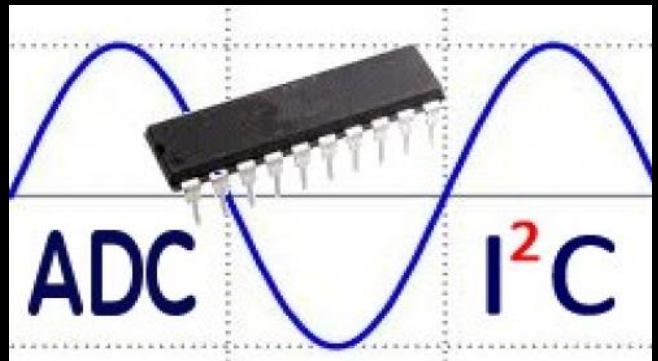
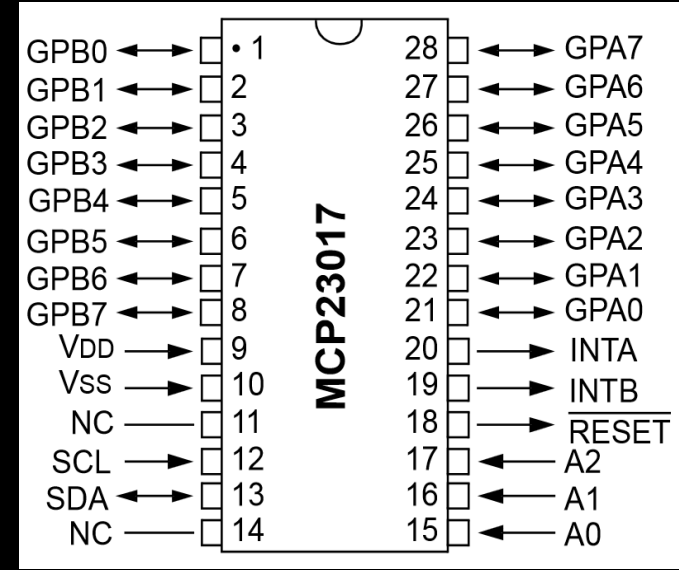
192.168.1.104:22 - pi@raspberrypi: ~ - VT
File Edit Setup Control Window Help
Linux raspberrypi 3.1.9adafruit+ #8 PREEMPT Wed Aug 1 18:02:42 EDT 2012 arm

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Type 'startx' to launch a graphical session

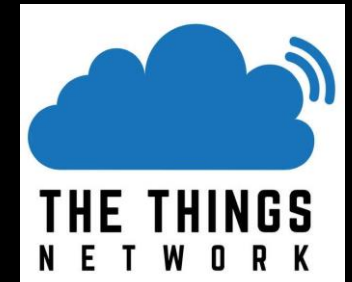
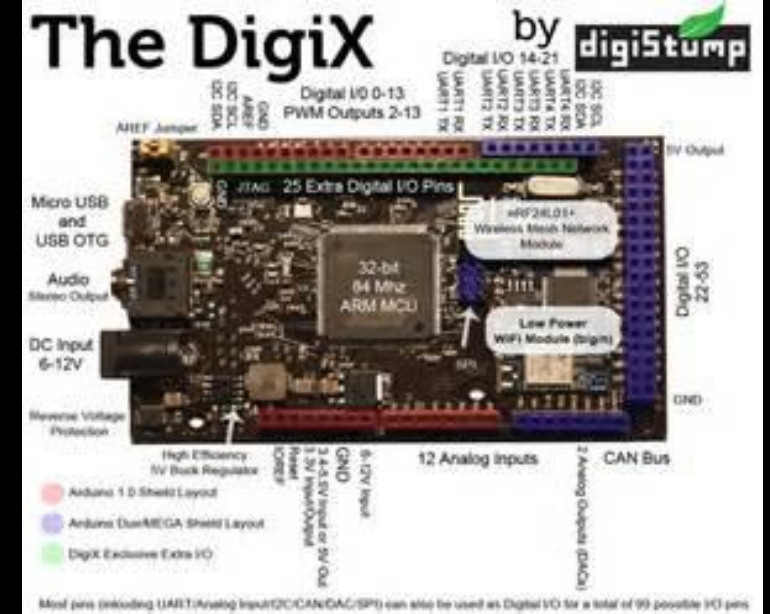
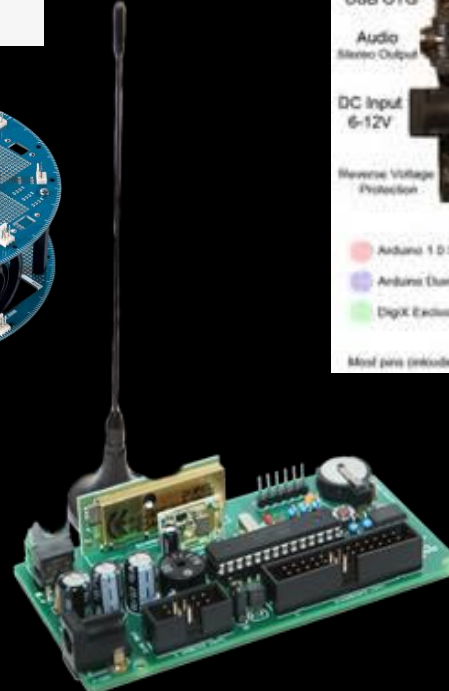
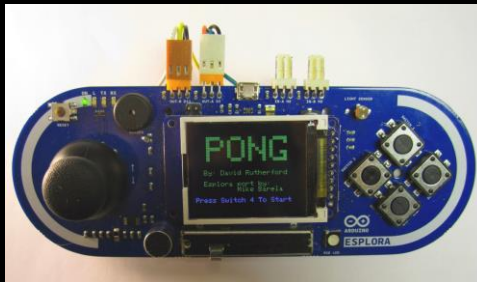
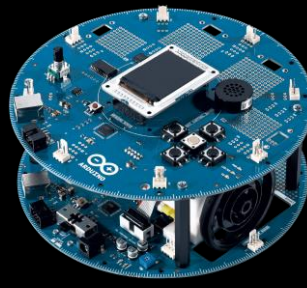
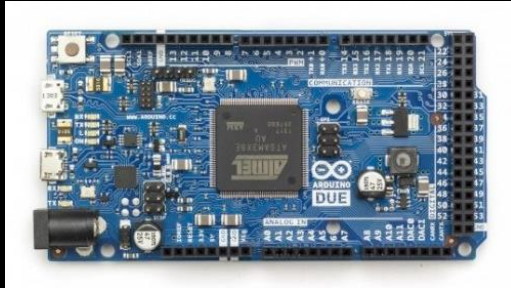
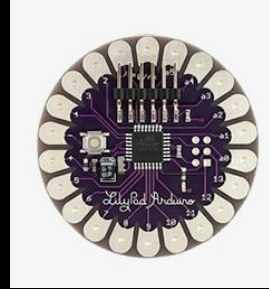
Last login: Thu Aug  9 11:41:58 2012 from 192.168.1.103
pi@raspberrypi ~ $ sudo i2cdetect -y 0
 0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
10: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
20: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
30: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
40: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
50: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
60: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
70: -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
pi@raspberrypi ~ $
    
```



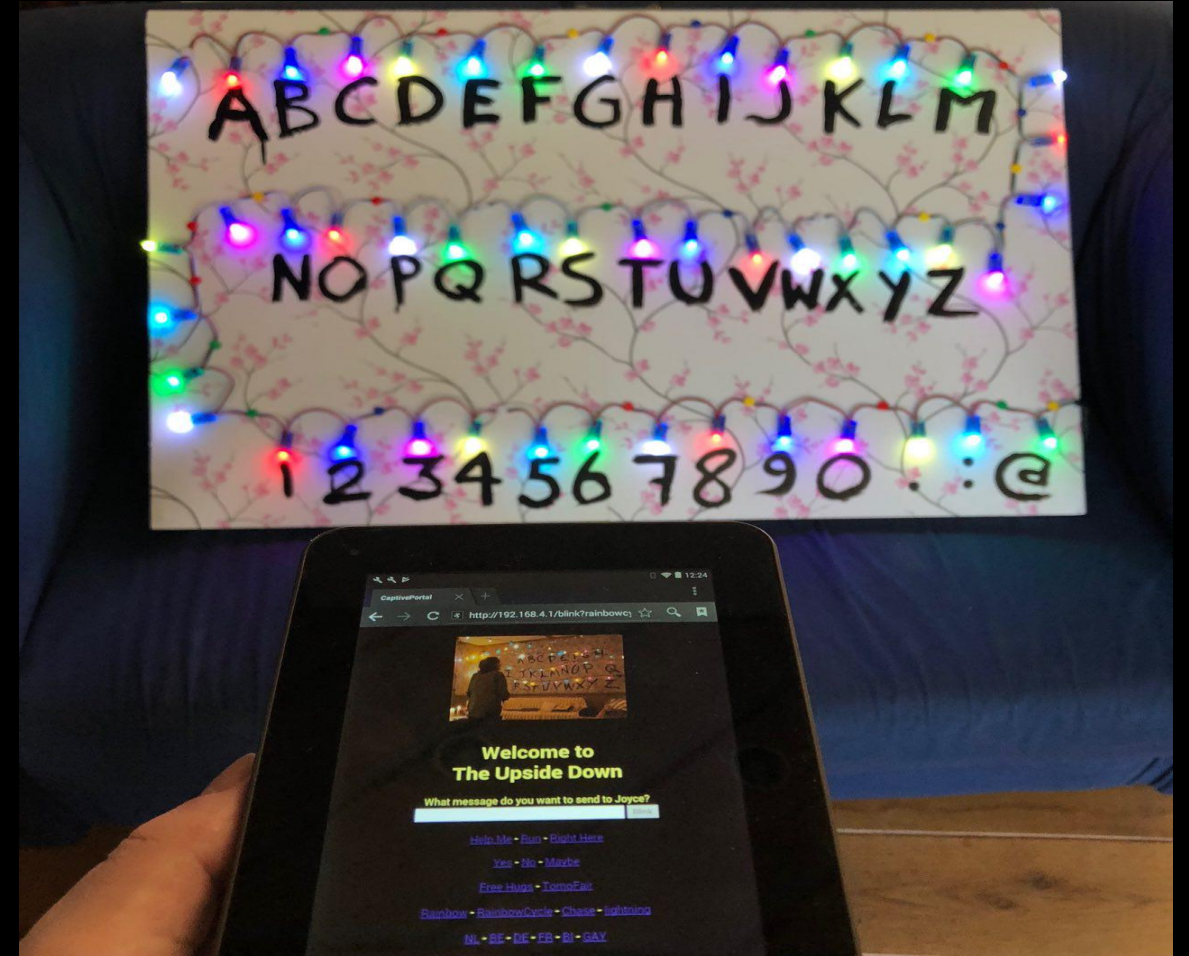
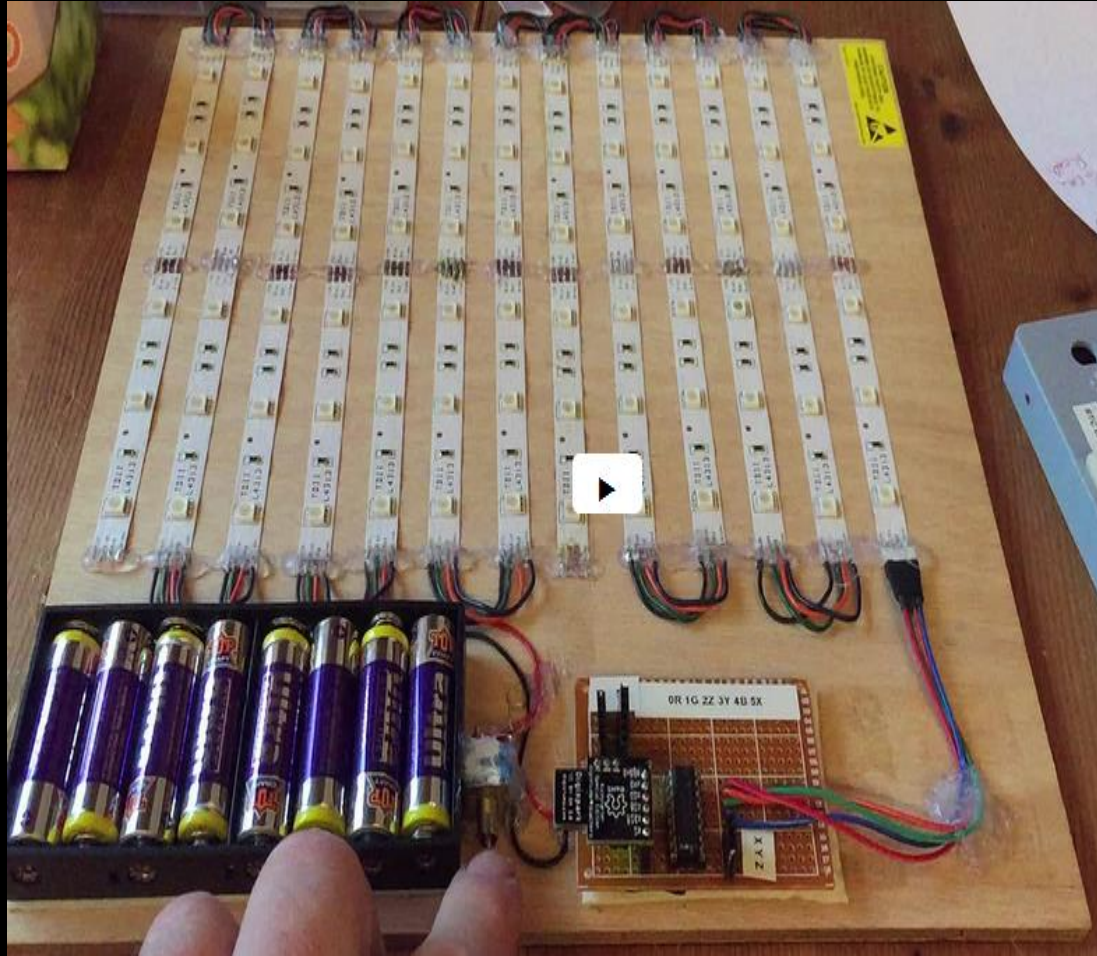
Magical Box 2.0



Arduino

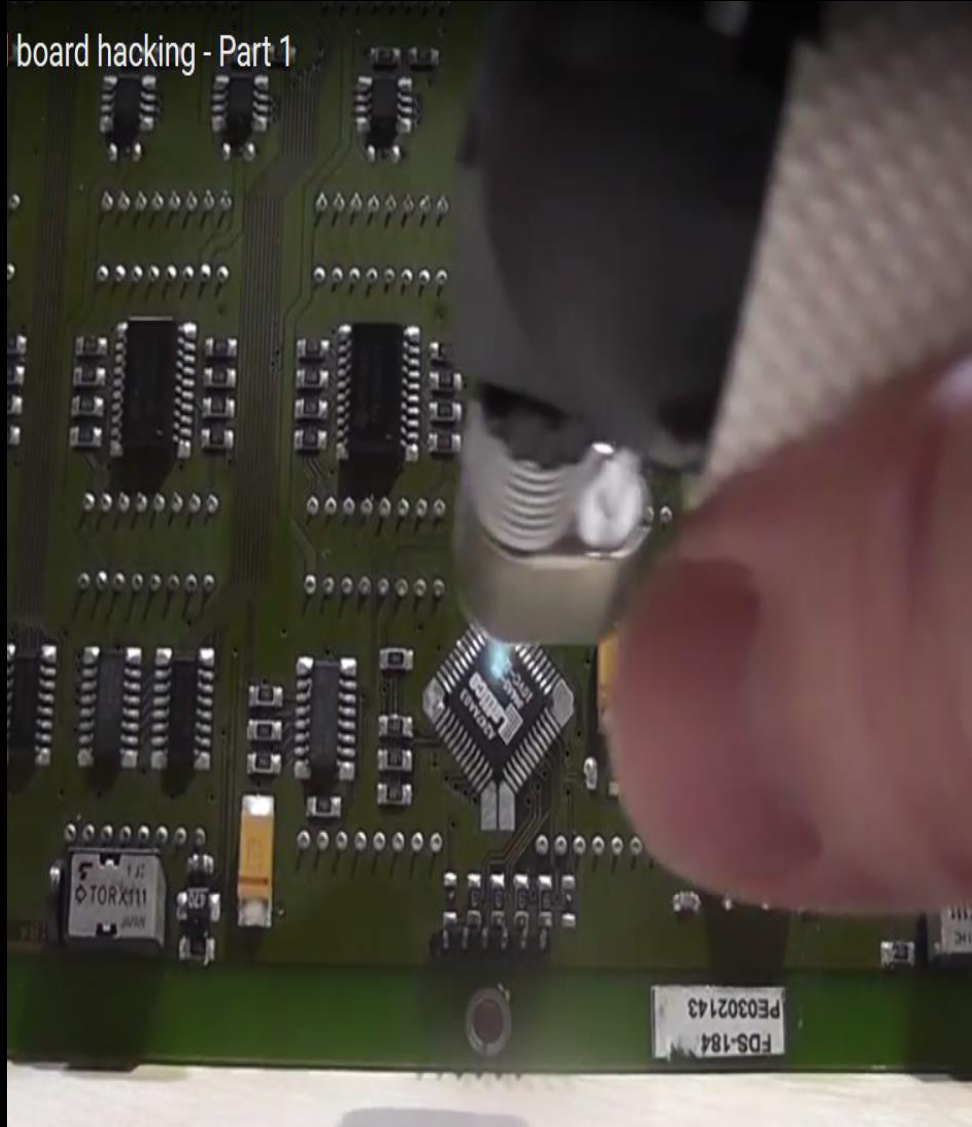


Create stuff



Alter stuff

board hacking - Part 1



#Privacy

Big Brother



```
Id N-WATCH: 73 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile: 0 / 0.00, Glasses:
Id Y-WATCH: 73 - Male-Adult, Attention time: 0 out of 188 - (0.00 / 0.33 / 0.00), Smile: 0 / 1.05, Glass
Id Y-WATCH: 73 - Male-Young adult, Attention time: 0 out of 391 - (0.00 / 0.50 / 0.00), Smile: 0 / 1.42,
Id N-WATCH: 74 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile: 0 / 0.00, Glasses:
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 188 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.24,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 375 - (0.00 / 0.33 / 0.00), Smile: 0 / 0.16,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 578 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.64,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 203 out of 781 - (0.00 / 0.60 / 0.00), Smile: 0 / 0.76
Id Y-WATCH: 74 - Male-Young adult, Attention time: 486 out of 984 - (0.00 / 0.67 / 0.00), Smile: 0 / 0.96,
```

Big Brother

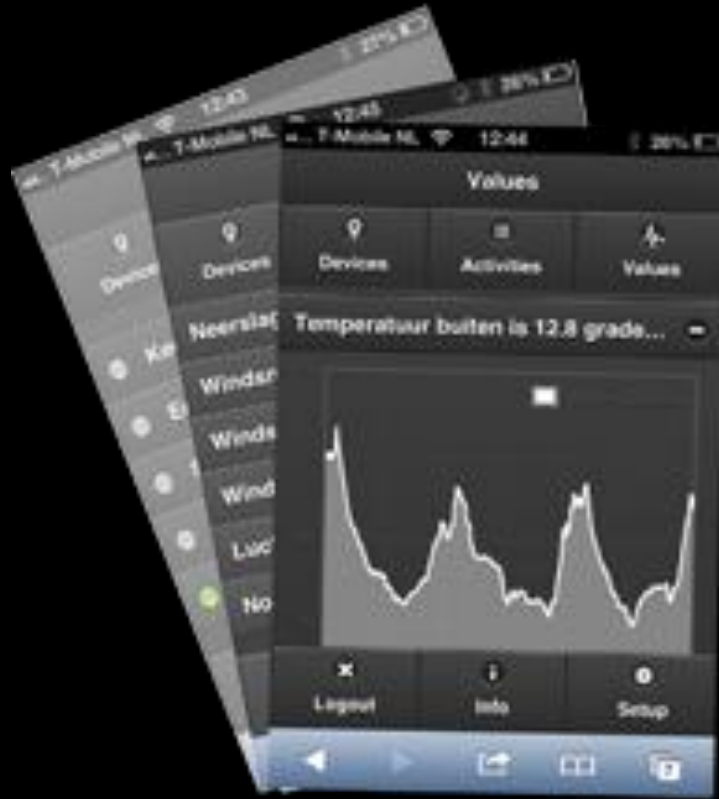


#Domotica

Check Power Consumption



Check Weather



DIY Alarm system



Forumoverzicht < Nederlands < Nodo toepassingen

Help Registreren Aanmelden

Flamingo Rookmelder FA20RF als Nodo alarmsirene

PLAATSREACTIE Doorzoek dit onderw Zoeken 45 berichten • Pagina 4 van 5 • 1 2 3 4 5

Re: Flamingo Rookmelder FA20RF als Nodo alarmsirene

door proza » 07 mei 2013, 19:09

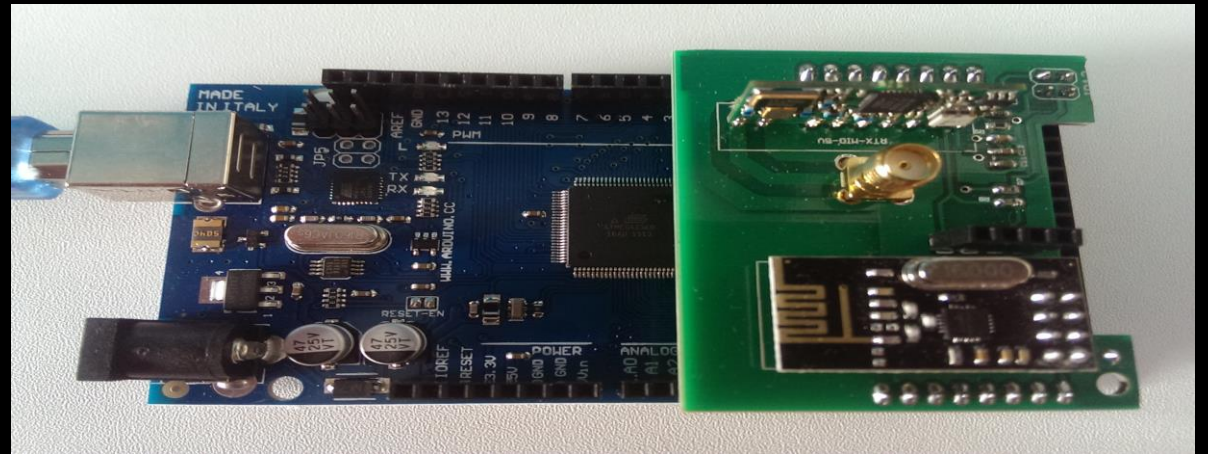
“ mvdbro schreef:
Maar nu gaat met commando "SendSmoke 0,9308102" het groene ledje knipperen op de rookmelder. (om niet doof te worden heb ik het piezo element er tijdelijk afgeklikt...) Morgen eens testen of ie ook echt lawaai gaat maken.

gr
Martinus

CITEER



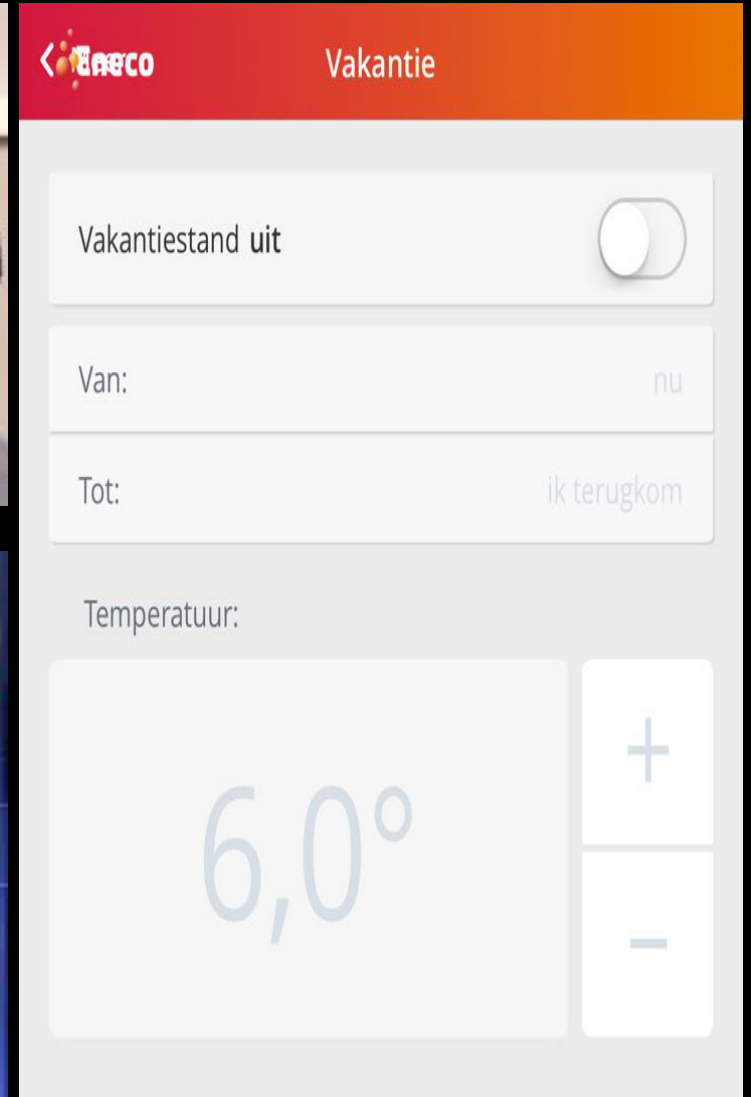
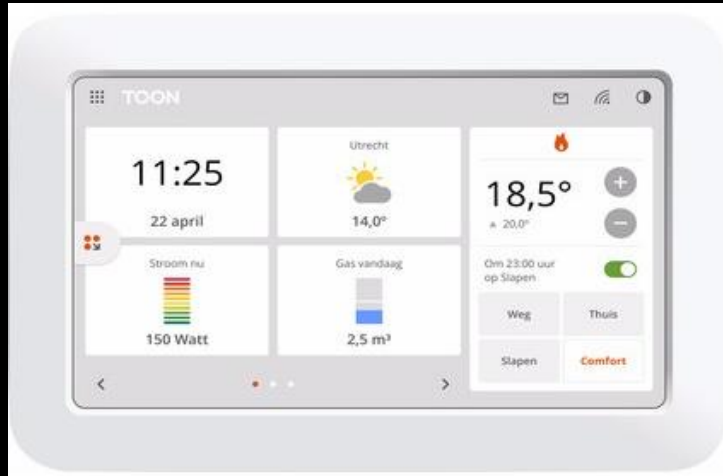
proza
Berichten: 420
Geregistreerd: 03 nov 2011, 22:44



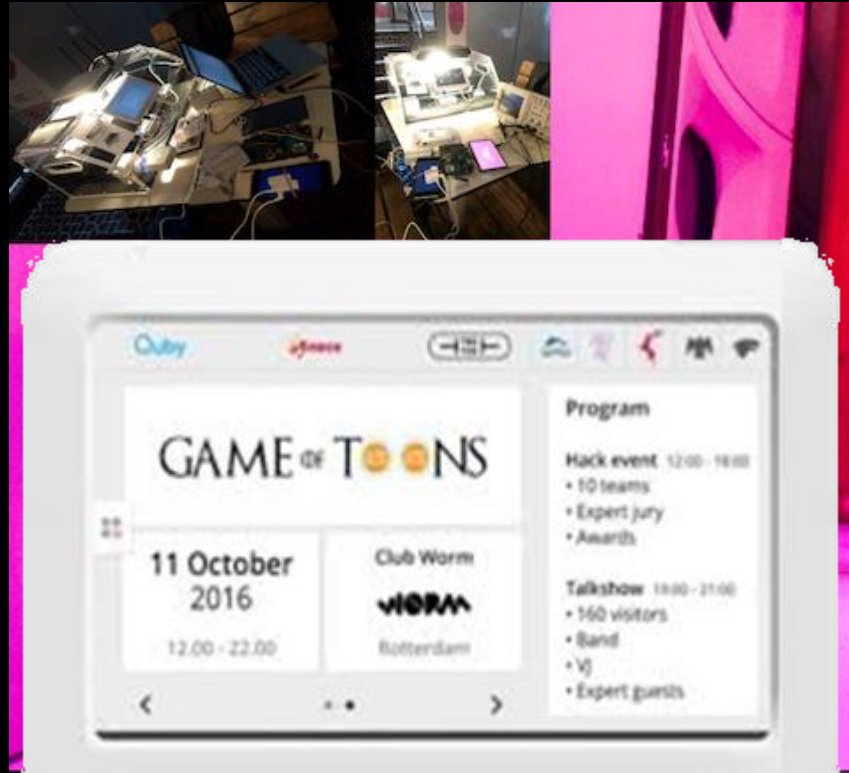
Migraine



Commercial Solution



Hackathon “Game of Toons”



Most techy hack

Team RamseyBolToon, studenten van Forensische ICT van de Hogeschool Leiden, wisten tijdens Game of Toons de meest technisch geavanceerde hack te plegen op Toon van Eneco. Jurylid Michiel Fokke, (CTO Quby) en juryvoorzitter Hans Valk (CEO Quby) vertellen waarom.



Wierdest hack

Team Sesamstraat wist tijdens Game of Toons de meeste bijzondere hack te plegen. Jurylid Glenn ten Cate (Security Engineer Schuberg Philis) en juryvoorzitter Hans Valk (CEO Quby) vertellen waarom. Tot de uitreiking was dit team anoniem. Toen Patricia Zorko, directeur Cybersecurity bij NCTV, de prijs in ontvangst nam was dat een bijzondere verrassing.



Most dangerous hack

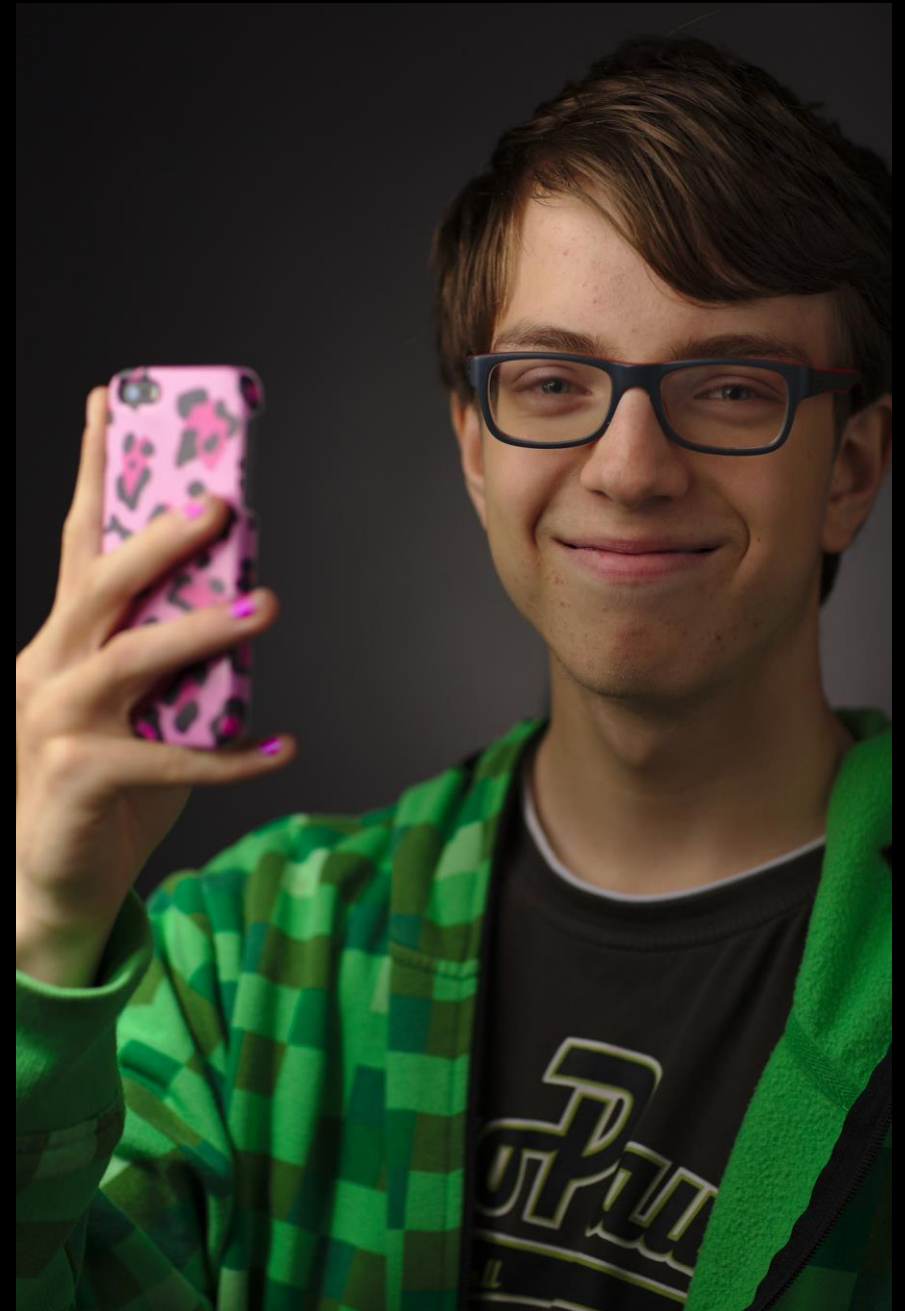
Team LooneyToons van Dearbytes wist tijdens Game of Toons de gevaarlijkste hack te plegen op Toon van Eneco. Jurylid Edwin van Andel (Security Advisor Zerocopter) en juryvoorzitter Hans Valk, (CEO Quby) vertellen waarom.

TEK
TOK

Now over to

Jurree

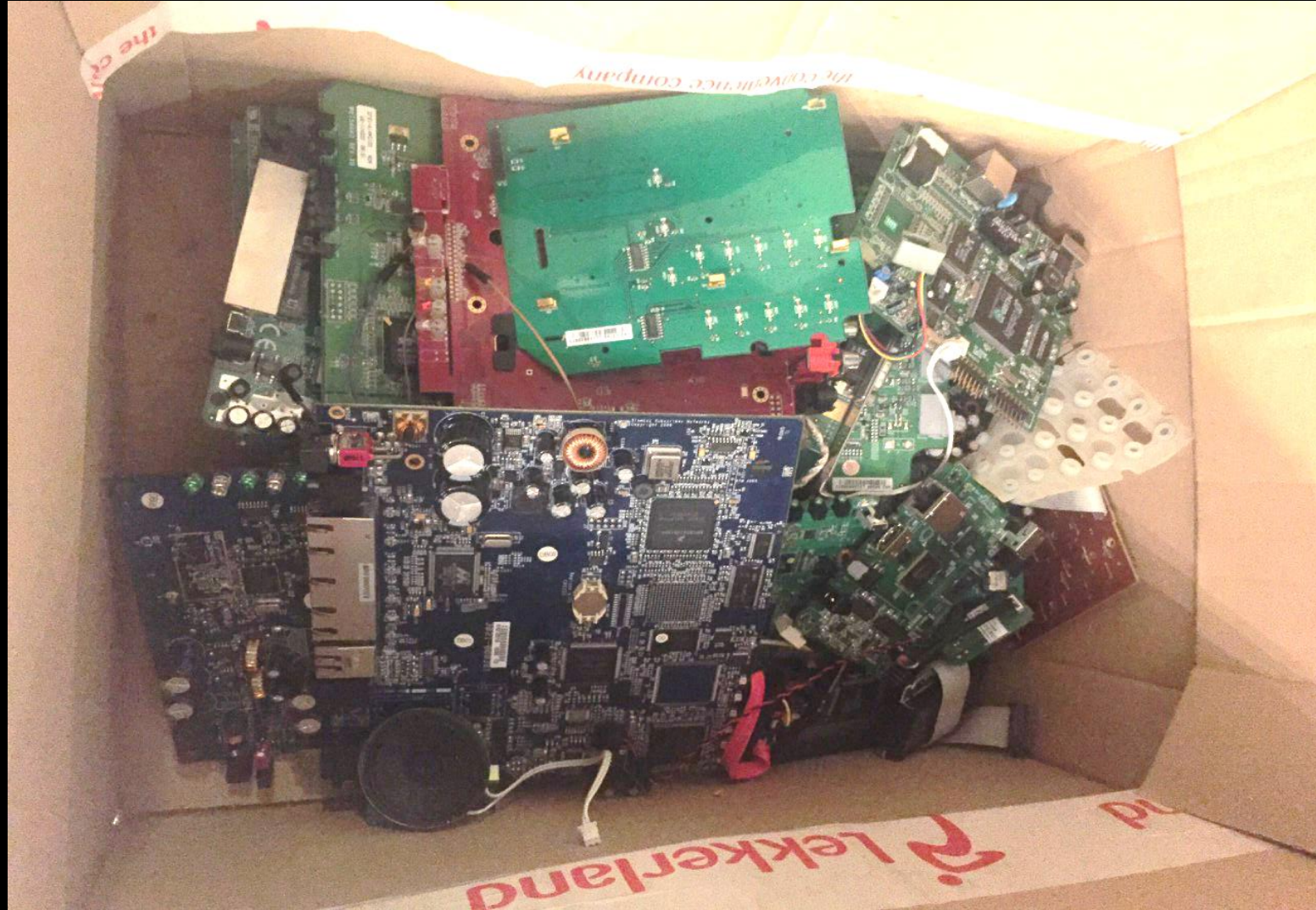
Jurre Groenendijk
16 years old
VWO bilingual NT



See how stuff works



Scrapbox



#PLUSKLAS



Science



Privacy

Privacy Matters (Dutch with English subtitles)



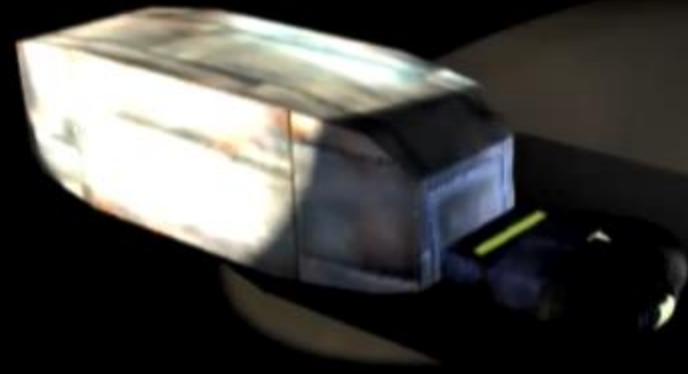
okay, do that. Hey my dear I have to hang up.

0:11 / 10:46







YouTube

Technology

TCP Packet



Programming

| | | |
|---|---|--|
|  <p>25 Exercises</p> <p>Jun 2, 2013</p> |  <p>25 points earned in one day</p> <p>Jun 2, 2013</p> |  <p>Tip Calculator</p> <p>Jun 2, 2013</p> |
|  <p>Python Syntax</p> <p>Jun 2, 2013</p> |  <p>10 Exercises</p> <p>Jun 2, 2013</p> |  <p>First Lesson</p> <p>Jun 2, 2013</p> |

script.py

```
1 # my_int is set to 7 below. What do you think
2 # will happen if we reset it to 3 and print the result?
3
4 my_int = 7
5
6 # Change the value of my_int to 3 on line 8!
7
8 my_int = my_int - 4
9
10 # Here's some code that will print my_int to the console:
11 # The print keyword will be covered in detail soon!
12
13 print my_int
```



Congratulations, you've finished this section!

Next: Whitespace and Statements→

Security



jurre Groenendijk
CS-0904140001

Logout

Home Training Community Premium About Us

My Account: [Profile](#) [Certificates](#) [Toolbox](#) [Preferences](#)

Logged in as: jurre Groenendijk (JurreJelle)

JurreJelle
Level 22

- Safe Internet 100%
- Safe Internet Plus 100%
- Essential Security 100%
- Essential Specialties 100%
- Security Specialist 100%
- Forensic Specialist 100%
- Web Security Specialist 100%
- Aware Programmer 100%
- Aware Administrator 100%
- Server Security Specialist 100%

- Safe Internet Certificate (100%)
- Internet Fundamentals 100%
- Don't click 100%
- Update Fundamentals Instruction Video
- Internet Fundamentals Instruction Video
- SSL Certificates Instruction Video
- Firefox Update Instruction Video
- Google Chrome Update Instruction Video
- Internet Explorer Update Instruction Video
- Windows 7 Update Instruction Video
- Safe Internet Extra Content (72%)
- Malware Memory 100%
- Safe Internet Challenge 100%
- SSL Quiz 60%
- Security.NL Challenge 100%
- Security.NL Winter Challenge 0%

Documentary: "Jurre hack"

YouTube search results for "jurre hack".

Browser: jurre hack - YouTube
URL: https://www.youtube.com/results?search_query=jurre+hack

Search: jurre hack

Ongeveer 274 resultaten

- Mini documentaire: Zo maakt Jurre (15) de wereld veiliger met hacken**
DeloitteNederland • 4,8K weergaven • 1 maand geleden
Deloitte maakte een mini docu over **Jurre**. Deze tienerzoon van een Deloitteer maakt met zijn kennis over hacken de wereld ...
- hack**
Jurre van deursen
HOW TO HACK ANY COMPUTER WITH CMD • 8:10
How to hack a PC and control it • 5:13
VOLLEDIGE AFSPEELLIJST WEERGEVEN (11 VIDEO'S)

Left sidebar (HET BESTE VAN YOUTUBE): Muziek, Sport, Games, Films, News

Be Responsible!



HELPEDE HACKERS

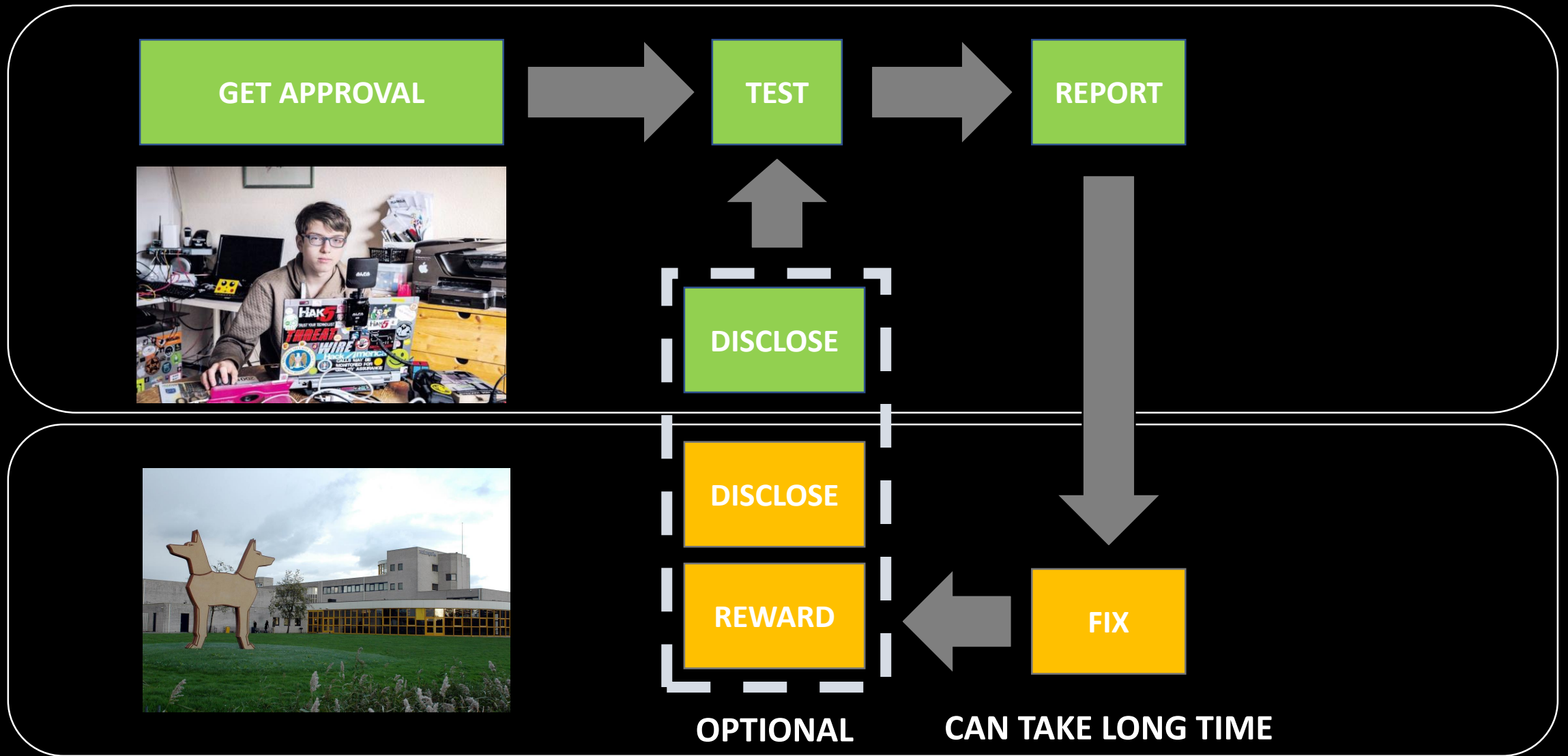
Verantwoorde onthullingen in het digitale polderlandschap



Chris van't Hof



Responsible Disclosure



Agreement upfront

Legal yada yada - OneNote

File Home Insert Draw History Review View

Clipboard: Paste, Cut, Copy, Format Painter

Basic Text: Calibri Light, 20, Bold, Italic, Underline, Text Color, Background Color, Bullets, Numbered List, Indent, Decrease Indent, Increase Indent, Undo, Redo

Styles: Heading 1, Heading 2

Tags: To Do (Ctrl+1), Important (Ctrl+2), Question (Ctrl+3), To Do Tag, Find Tags, Outlook Tasks

Notebooks: J2-OneNote

How-to School Plag CTF

Legal yada yada

woensdag 30 september 2015 8:33

School may be assessed as agreed with:

- [redacted] (math teacher)
- [redacted] (Kernteamleider)

Rules and regulations:

- Test should not impact schools availability
- Reports cannot be discussed with third parties (except for dad)
- Findings should be presented to schoolboard
- If you find an vulnerability, report it. DO NOT USE IT!

N.B. Take Responsible Disclosure definitions in account

Don't break stuff

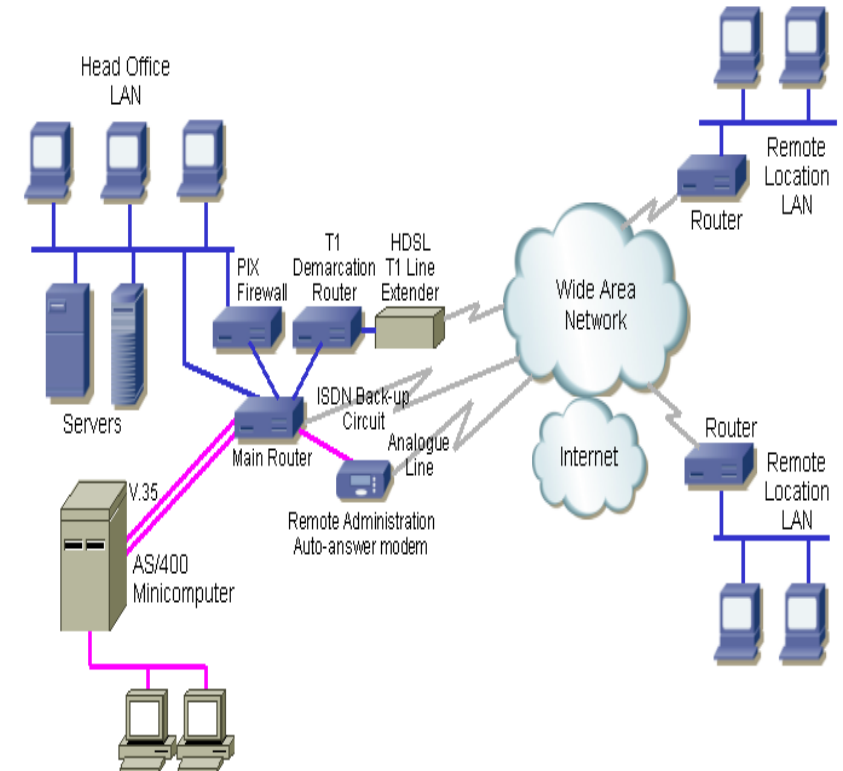
```
Nmap -p- -T4 192.168.0.0/16
```

```
Nmap scan report for [REDACTED]  
Host is up (0.00012s latency).
```

```
Not shown: 985 closed ports
```

| PORT | STATE | SERVICE |
|-----------|-------|------------------|
| 80/tcp | open | http |
| 135/tcp | open | msrpc |
| 139/tcp | open | netbios-ssn |
| 443/tcp | open | https |
| 445/tcp | open | microsoft-ds |
| 1044/tcp | open | dcutility |
| 1433/tcp | open | ms-sql-s |
| 2301/tcp | open | compaqdiag |
| 2381/tcp | open | compaq-https |
| 3389/tcp | open | ms-wbt-server |
| 5633/tcp | open | beorl |
| 5989/tcp | open | wbem-https |
| 6101/tcp | open | backupexec |
| 6106/tcp | open | isdninfo |
| 10000/tcp | open | snet-sensor-mgmt |

Data Network



Always lock your devices



Your passwords are in memory

```
Authentication Id : 0 ; 2858340 <00000000:002b9d64>  
Session          : Service from 0  
User Name       : svc-SQLDBEngine01  
Domain         : ADSECLAB  
SID            : S-1-5-21-1473643419-774954089-2222329127-1607
```

msv :

```
Primary  
* Username : svc-SQLDBEngine01  
* Domain   : ADSECLAB  
* NTLM     : d0abfc0cb689f4cdc8959a1411499096  
* SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
```

tspkg :

```
* Username : svc-SQLDBEngine01  
* Domain   : ADSECLAB  
* Password : ThisIsAGoodPassword99!
```

wdigest :

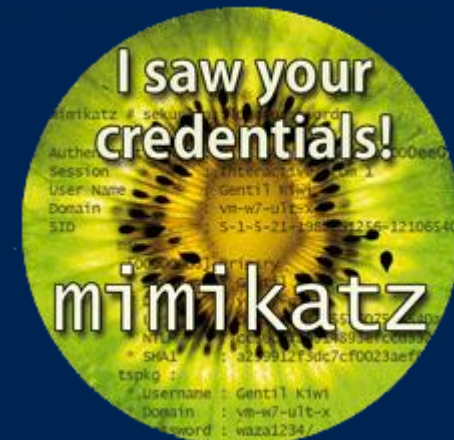
```
* Username : svc-SQLDBEngine01  
* Domain   : ADSECLAB  
* Password : ThisIsAGoodPassword99!
```

kerberos :

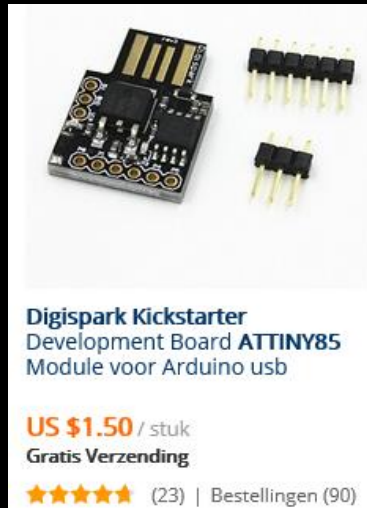
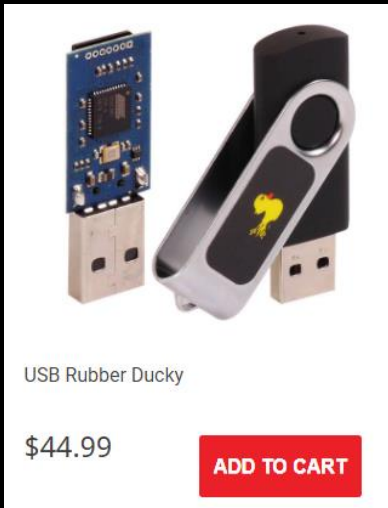
```
* Username : svc-SQLDBEngine01  
* Domain   : LAB.ADSECURITY.ORG  
* Password : ThisIsAGoodPassword99!
```

ssp :

credman :



Poor students become creative



```
#include "DigiKeyboard.h"
```

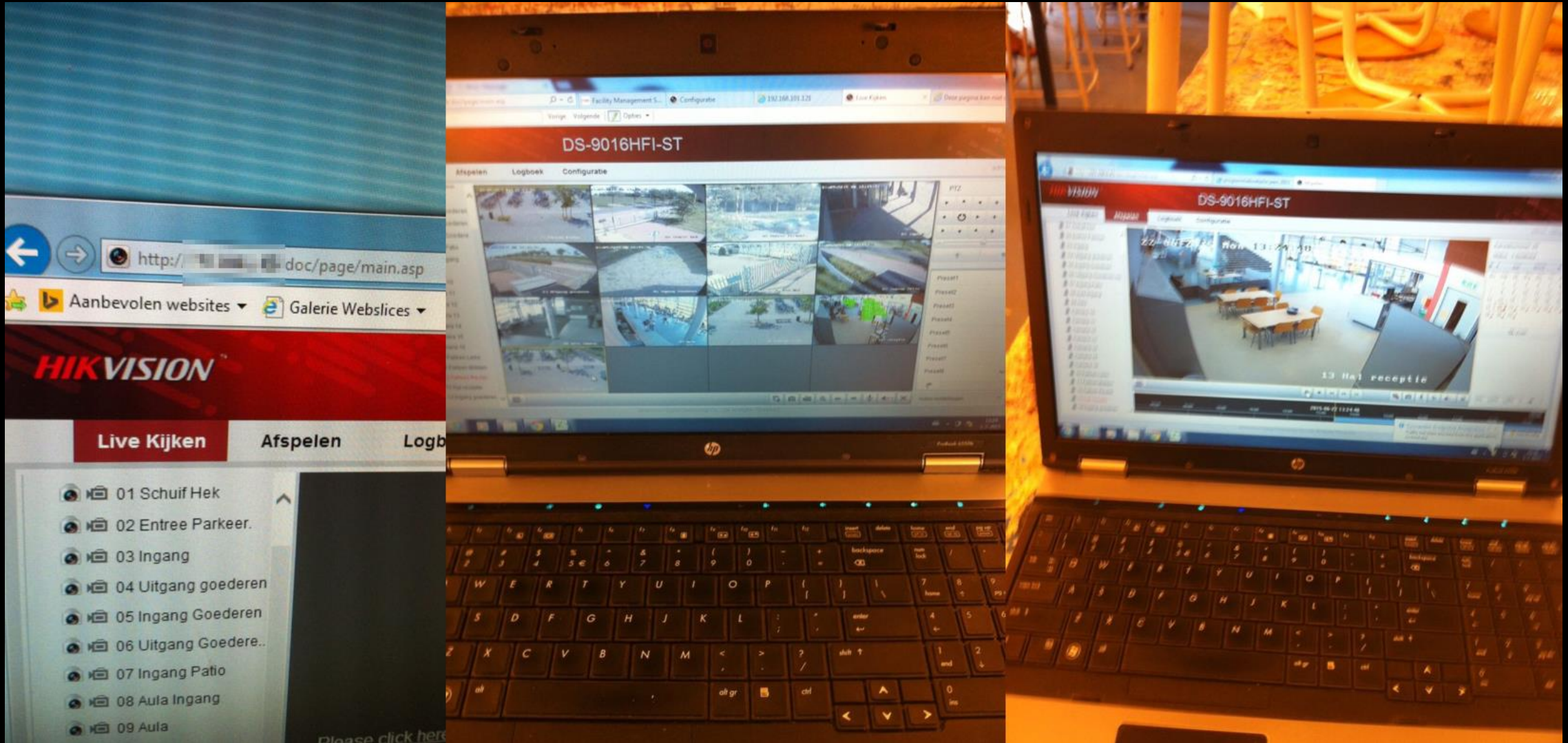
```
int btn = 5;
```

```
void setup(){  
  pinMode(btn, INPUT);  
  pinMode(1, OUTPUT);  
}
```

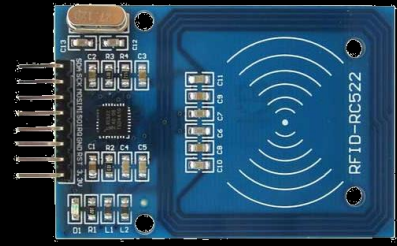
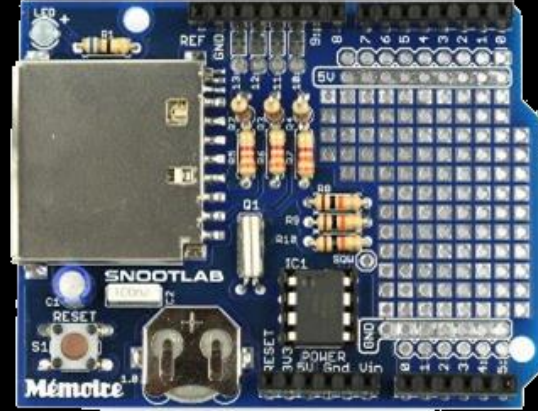
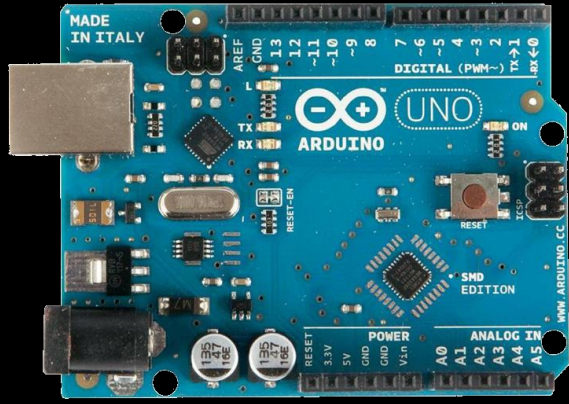
```
void loop(){  
  if(digitalRead(btn) == HIGH){  
    DigiKeyboard.sendKeyStroke(0, MOD_GUI_LEFT);  
    DigiKeyboard.delay(500);  
    DigiKeyboard.print("Windows PowerShell");  
    DigiKeyboard.delay(850);  
    DigiKeyboard.sendKeyStroke(KEY_ENTER);  
    DigiKeyboard.delay(500);  
    DigiKeyboard.print("start https://www.supertwins.nl/troll");  
    digitalWrite(1, HIGH); delay(250); digitalWrite(1, LOW);  
  }  
}
```



Change your default password



Lunchbox electronics



```
GettingStarted | Arduino 1.6.8 Hourly Build 2016/02/16 05:07
File Edit Sketch Tools Help

GettingStarted

Serial.println(F("Now sending"));

unsigned long start_time = micros();           // Take the time, and send it. This will block until complete
if (!radio.write(&start_time, sizeof(unsigned long) )){
  Serial.println(F("failed"));
}

radio.startListening();                       // Now, continue listening

unsigned long started_waiting_at = micros();   // Set up a timeout period, get the current microseconds
boolean timeout = false;                     // Set up a variable to indicate if a response was received or not

while ( ! radio.available() ){               // While nothing is received
  if (micros() - started_waiting_at > 200000 ){ // If waited longer than 200ms, indicate timeout and exit while loop
    timeout = true;
    break;
  }
}

if ( timeout ){                               // Describe the results
  Serial.println(F("Failed, response timed out."));
}
```

Lunchbox challenges



ISO14443-A emulated tag are protected

```
00219 // Notes for ISO14443-A emulated tags:
00220 // * Only short UIDs are supported
00221 // If your UID is longer it will be truncated
00222 // Therefore e.g. an UltraLight can only have short UID, which is
00223 // typically badly handled by readers who still try to send their "0x95"
00224 // * First byte of UID will be masked by 0x08 by the PN53x firmware
00225 // as security countermeasure against real UID emulation
```

From <http://www.libnfc.org/api/nfc-emulate-tag_8c_source.html>

Patch nfc-mfclassic to write 0-byte

File: [libnfc-1.5.1/utils/nfc-mfclassic.c](#)

```
// Try to write the trailer
if (nfc_initiator_mifare_cmd (pnd, MC_WRITE, uiBlock, &mp) == false) {
    printf ("failed to write trailer block %d \n", uiBlock);
    bFailure = true;
}
} else {
    // The first block 0x00 is read only, skip this
    // COMMENT THIS if (uiBlock == 0 && ! write_block_zero)
    // COMMENT THIS continue;
```

From <<https://gist.github.com/alphazo/3303282>>

Lunchbox coding

```
Waiting card
old:00bbfa05
new:00161105
Done

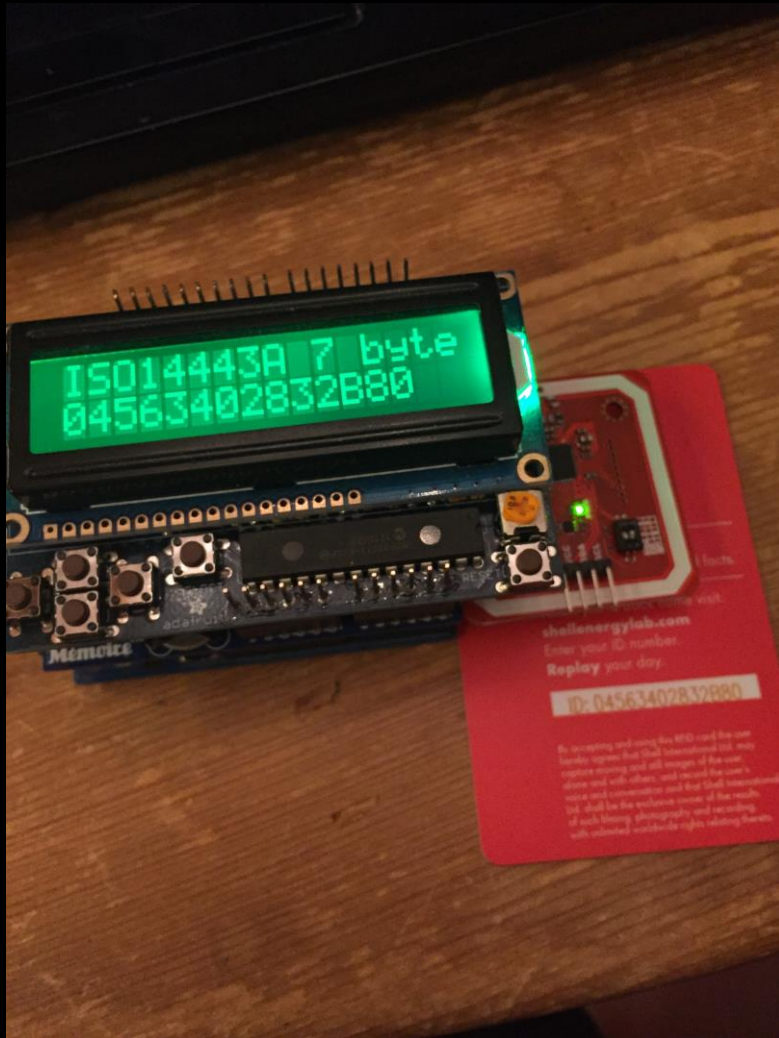
root@Kali:~/copycard# nfc-list
nfc-list uses libnfc 1.7.1
NFC device: ACS / ACR122U PICC Interface opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
  UID (NFCID1): 00 16 11 05
  SAK (SEL_RES): 88

root@Kali:~/copycard#
```

Copycard.sh

```
#!/bin/bash
td=$(date +%Y%m%d_%H%M)
echo -n "Cardname: "
read cardname
toilet --gay -f standard Reading card
old=$(nfc-list | grep UID | cut -d: -f2 | sed -e "s/ //g")
path=${old}_${cardname}
mkdir ${path} 2> /dev/null
mfcoc -f keys.txt -O ${path}/keys.mfd -P 150 -T 50 > ${path}/keys.log
nfc-mfclassic r a ${path}/dump-a.mfd ${path}/keys.mfd > ${path}/dump-a.log
echo "Please remove old card and place empty, Press enter to continue"
read a
toilet --gay -f standard Writing card
tmp=$(nfc-list | grep UID | cut -d: -f2 | sed -e "s/ //g")
nfc-mfclassic W A ${path}/dump-a.mfd ${path}/keys.mfd f > ${path}/write-a.log
new=$(nfc-list | grep UID | cut -d: -f2 | sed -e "s/ //g")
echo old:$old
echo tmp:$tmp
echo new:$new
toilet --gay -f standard Done
```

Lunchbox process







Commercial Alternatives

KPN NL 17:26 77%

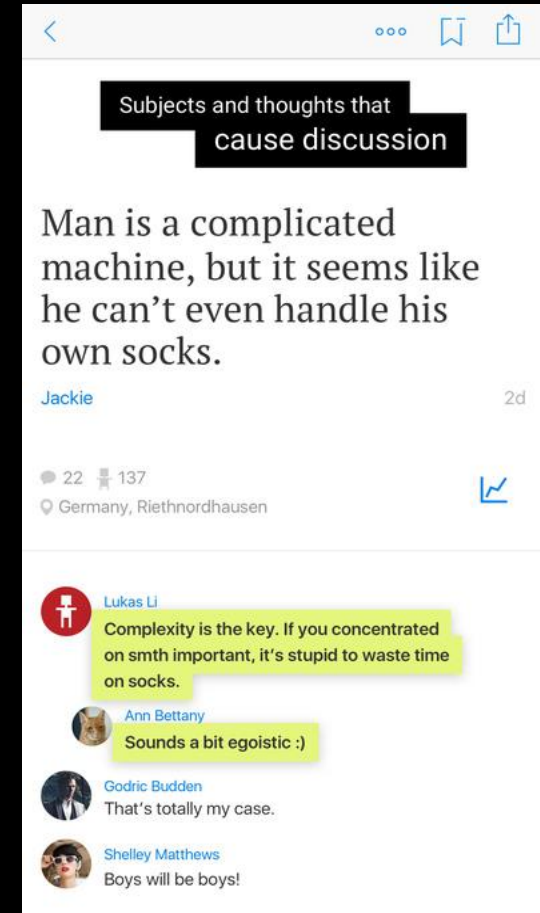
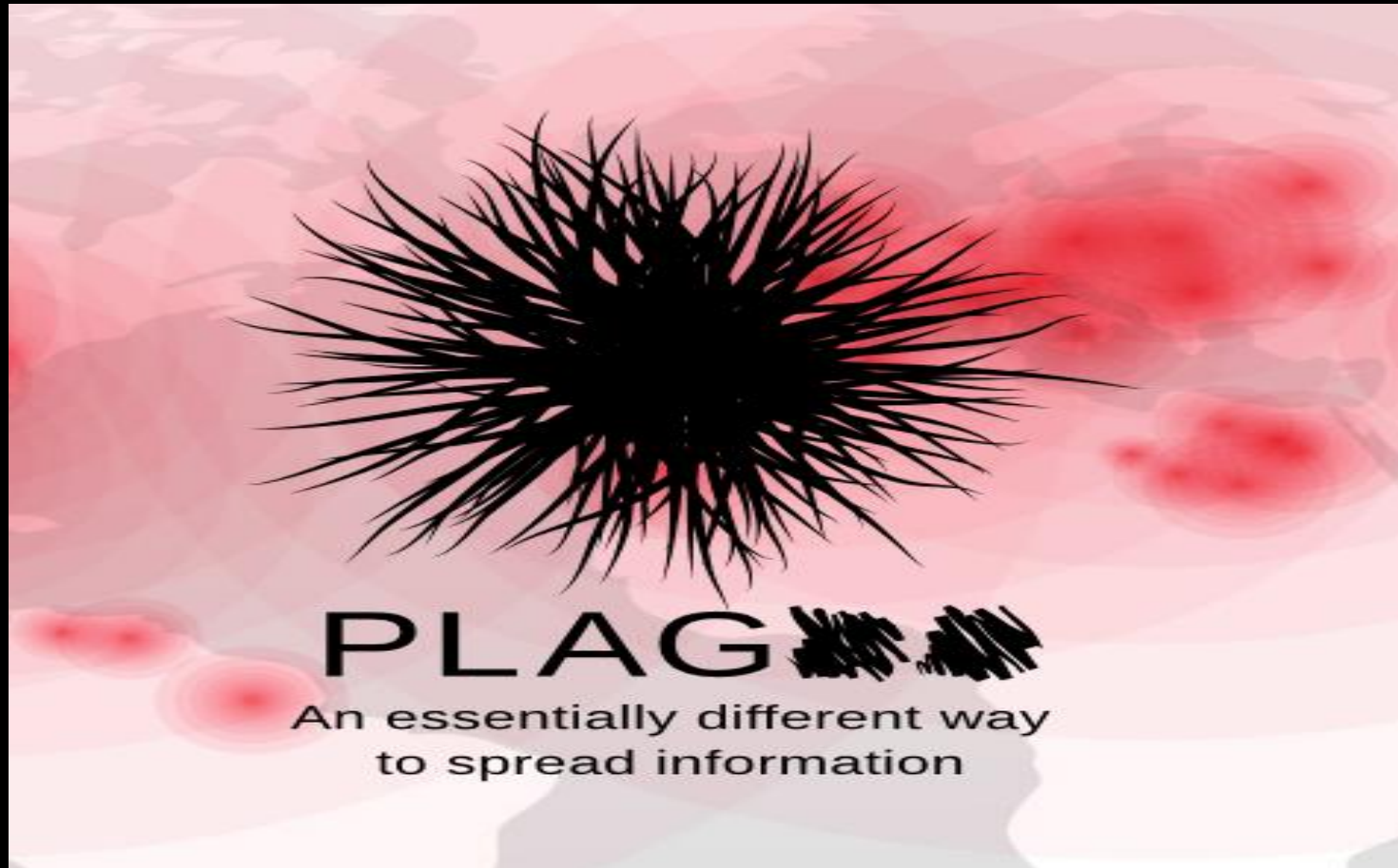
nfc copier

Best match Filter

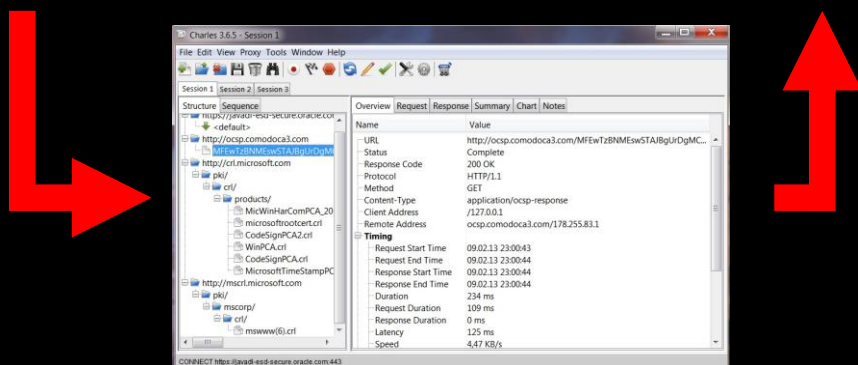
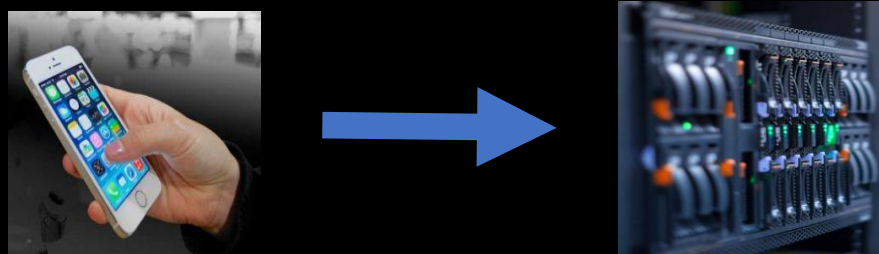
| | |
|--|---|
|  <p>€ 22,17</p> <p>4.8 ★★★★★ 297 Bestellen... Verzenden € 1,02</p> |  <p>€ 35,37</p> <p>4.8 ★★★★★ 296 Bestellen... Verzenden € 0,57</p> |
|  <p>€ 35,51</p> <p>4.7 ★★★★★ 275 Bestellen... Gratis verzenden</p> |  <p>€ 19,37</p> <p>4.7 ★★★★★ 368 Bestellen... Verzenden € 6,16</p> |





Plag** Client / Server




Plag** Man In The Middle







 **Jurre**
@Jurrejelle


 [Volg je nu](#)


.@charlesproxy Thank you so much for the license! I have tried many other products, but Charles Proxy is definitely the best :D





 Vertaling weergeven


21:59 - 10 jan. 2016



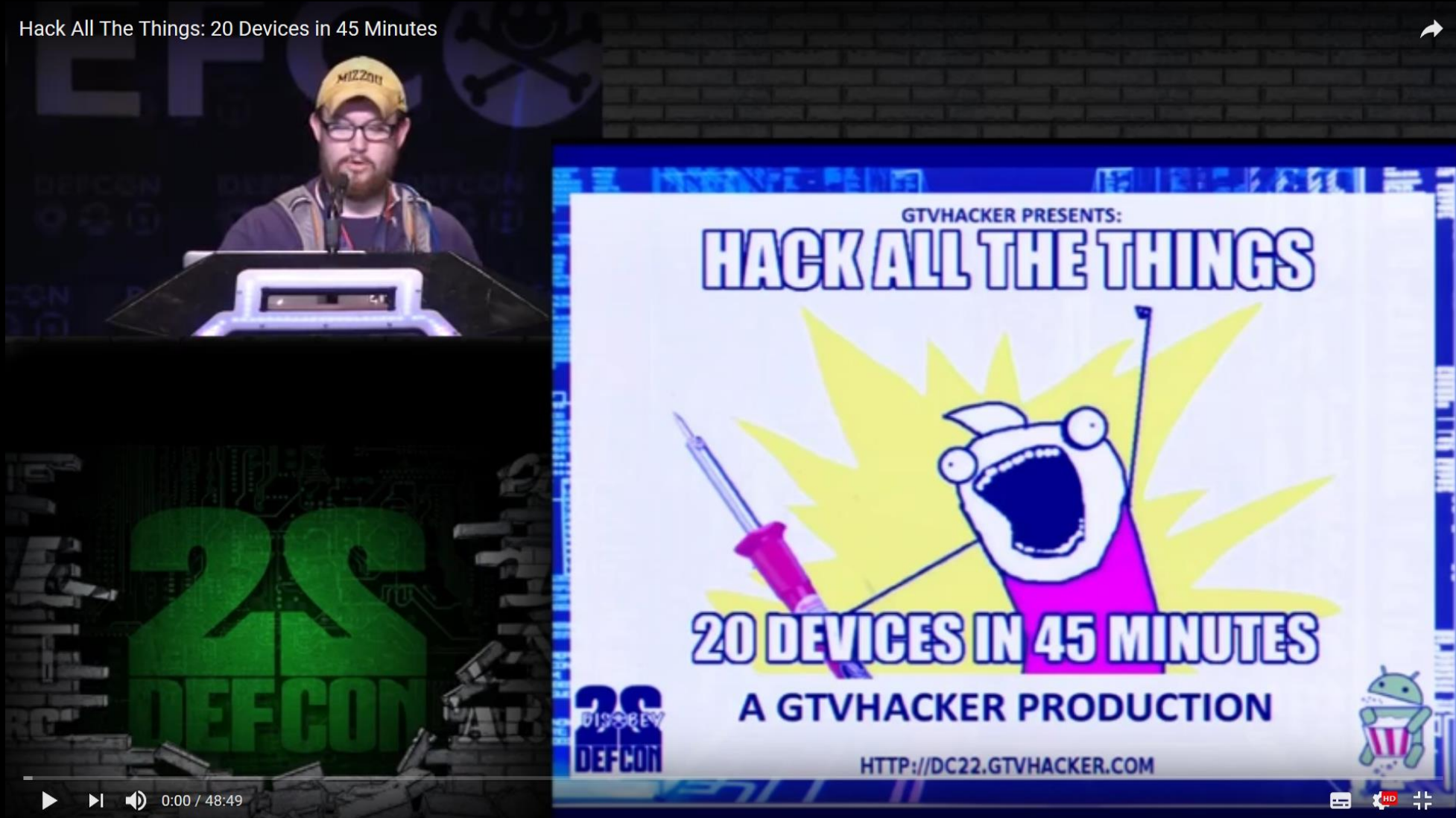
 **Charles Proxy** @charlesproxy · 10 jan.
@Jurrejelle You're most welcome!



Watch hacking videos

Hack All The Things: 20 Devices in 45 Minutes



The video player displays a speaker at a podium on the left and a promotional poster on the right. The poster features a cartoon character with a wide-open mouth, holding a pink screwdriver, set against a yellow starburst background. The text on the poster reads: "GTVHACKER PRESENTS: HACK ALL THE THINGS", "20 DEVICES IN 45 MINUTES", "A GTVHACKER PRODUCTION", and "HTTP://DC22.GTVHACKER.COM". The poster also includes a "DEFCON" logo and an Android robot icon.

0:00 / 48:49

Play Capture The Flag (CTF)

CTF TIME

CTFs

Upcoming

Archive

Calendar

Teams

FAQ

Contact us

About

Sign in

SECCON CTF



[Official URL](#)

Total events: 10

Avg weight: 27.68

DEF CON CTF Qualifier



[Official URL](#)

Total events: 8

Avg weight: 86.88

RuCTFE



[Official URL](#)

Total events: 8

Avg weight: 69.81

PlaidCTF



[Official URL](#)

Total events: 8

Avg weight: 83.99

Plaid CTF :: Hosted by Plaid Parliament of Pwning

Nuit du Hack CTF Quals



[Official URL](#)

Total events: 8

Avg weight: 41.23

HITB CTF Amsterdam



[Official URL](#)

Total events: 8

Avg weight: 30.00

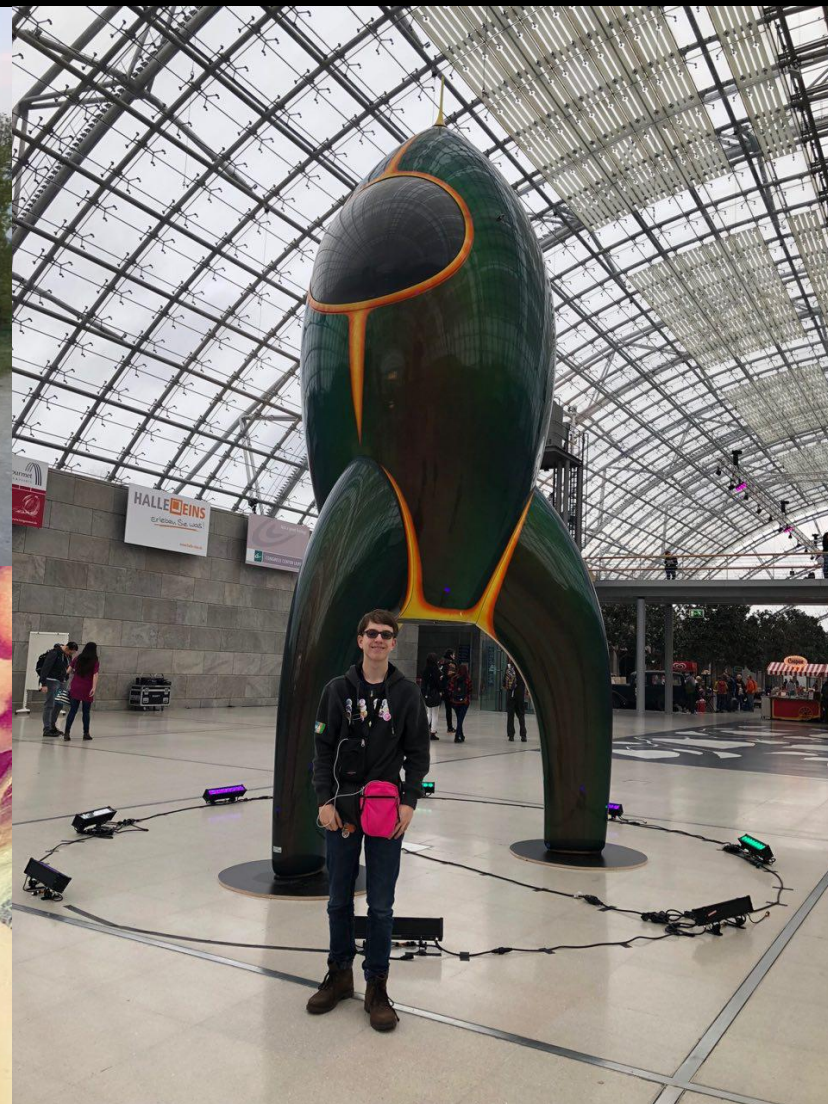
What: Jeopardy style CTF hacking competition

When: April 12th & 13th 2018

Where: On site at HITB2018AMS @ NH Krasnapolsky

Who: Max of 24 teams with up to 3...

Acquire knowledge



Share knowledge



Next Wednesday Library Veenendaal



Strange requests



Beware of Script Kiddies



Leerlingen Schiedamse school frauderen met cijfers

Tientallen leerlingen van S.G. Spieringshoek in Schiedam hebben waarschijnlijk de cijfers van hun proefwerken aangepast. Een jongen uit havo-4 zou erin geslaagd zijn het leerlingvolgsysteem van de school te hacken.

Redactie 07-06-17, 16:01 Laatste update: 17:22



De politie doet onderzoek en ik ga ervan uit dat deze school dit zorgvuldig aanpakt

- Wethouder Mario Stam

SHODAN

The World's Most Dangerous Search Engine



Search through 1.4 billion leaked accounts
3.1 million in The Netherlands

Gotcha?

Tip: see also @whitehouse.gov or The Netherlands.

Found 18 account(s)

| | |
|--------------------------|---------|
| Pres*****@whitehouse.gov | Cl***** |
| pres*****@whitehouse.gov | 12***** |
| pres*****@whitehouse.gov | Cl***** |
| pres*****@whitehouse.gov | Ke***** |
| pres*****@whitehouse.gov | ad***** |
| pres*****@whitehouse.gov | as***** |
| pres*****@whitehouse.gov | bi***** |
| pres*****@whitehouse.gov | cl***** |
| pres*****@whitehouse.gov | ff***** |

Armitage - windows/smb/ms08_067_smb2

ms08_067 Microsoft Server Service Relative Path Stack Corruption

This module exploits a parsing flaw in the path canonicalization code of netAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seen to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.

| Option | Value |
|---------|--------------|
| LHOST | 192.168.0.29 |
| LPORT | 25309 |
| RHOST | 192.168.0.35 |
| RPORT | 445 |
| SMBPIPE | BROWSER |

Targets: 0 => Automatic Targeting

Use a reverse connection

Show advanced options

De Telegraaf

DDoS-verdachte vond Rusland-theorie 'te grappig'

Hacker Jelle (18) al piepjong slim op internet

07 feb. 2018 in BINDELAND

DONSTERHOUT - De verdachte van grote DDoS aanvallen op Nederlandse banken heeft al sinds 2013 handige bedrijven op internet opgericht. Hij lijkt een slimme jongen, maar toch maakte Jelle S. 'beginnersfouten'. Hoogmoed komt voor de val, weet ook Jelle en.

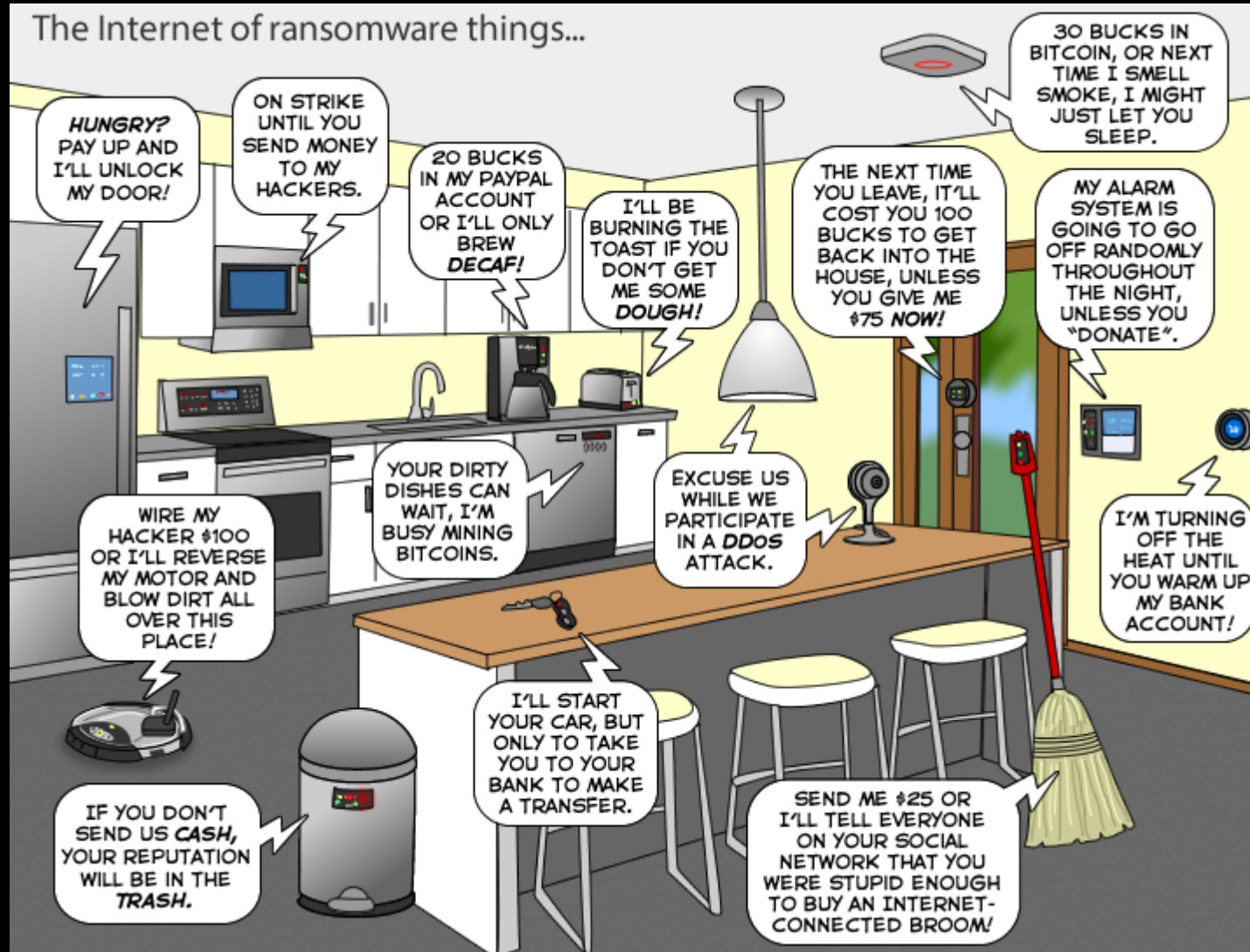
Knowledge Is Free.
We Are Anonymous.
We Are Legion.
We Do Not Forgive.
We Do Not Forget.
Expect Us.



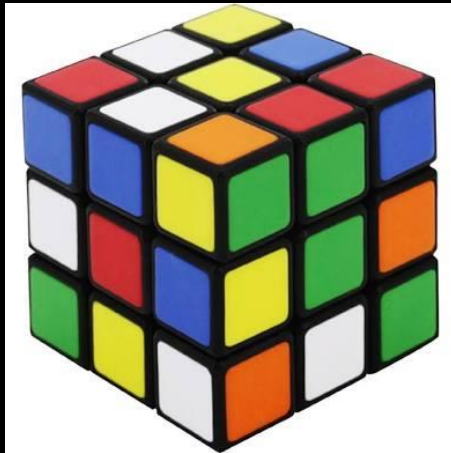
What about

IoT

The "S" in IOT is for SECURITY



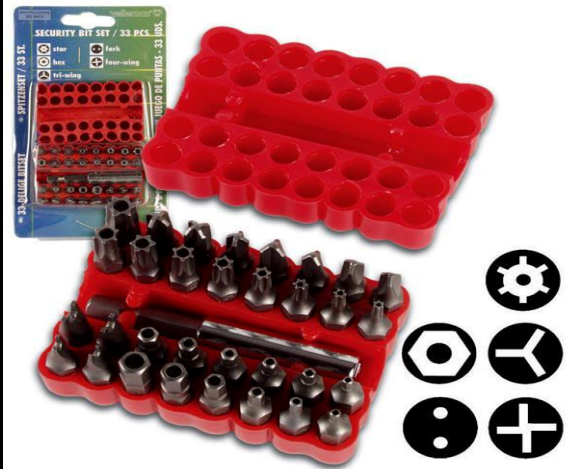
Most IOT security be like



OWASP IOT

- I1 | Insecure Web Interface
- I2 | Insufficient Authentication/Authorization
- I3 | Insecure Network Services
- I4 | Lack of Transport Encryption
- I5 | Privacy Concerns
- I6 | Insecure Cloud Interface
- I7 | Insecure Mobile Interface
- I8 | Insufficient Security Configurability
- I9 | Insecure Software/Firmware
- I10 | Poor Physical Security

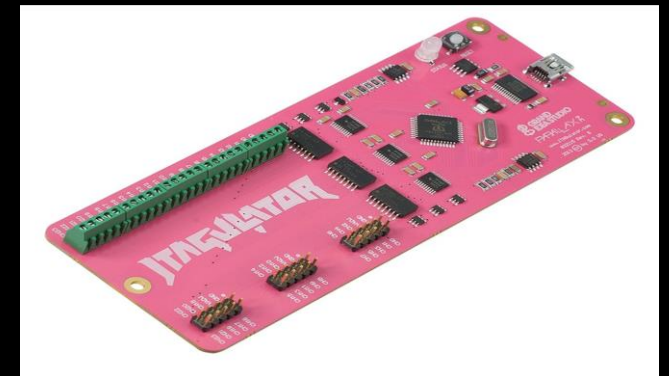
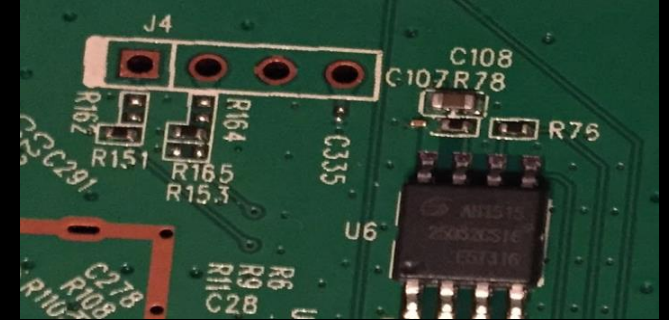
Security Measures



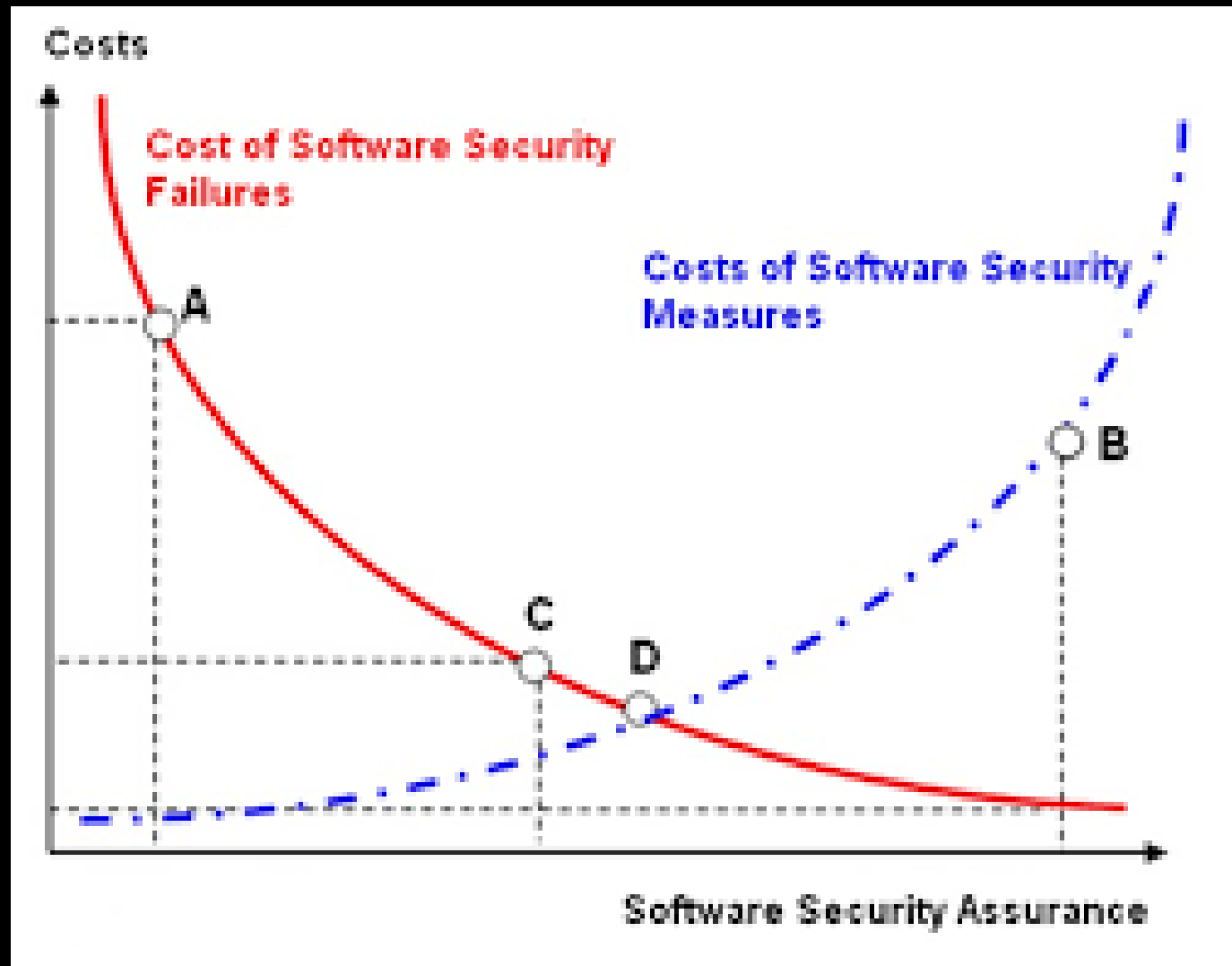
BEFORE



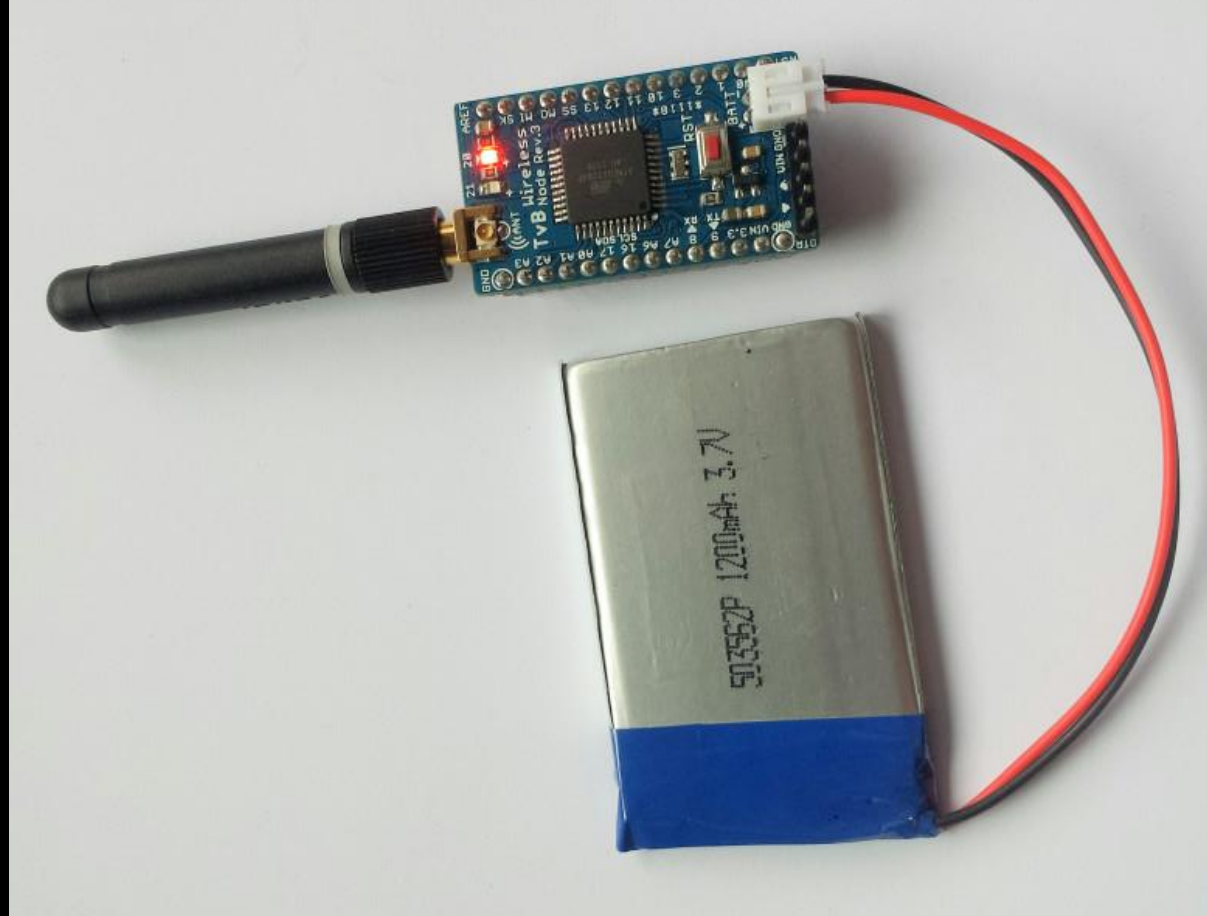
AFTER



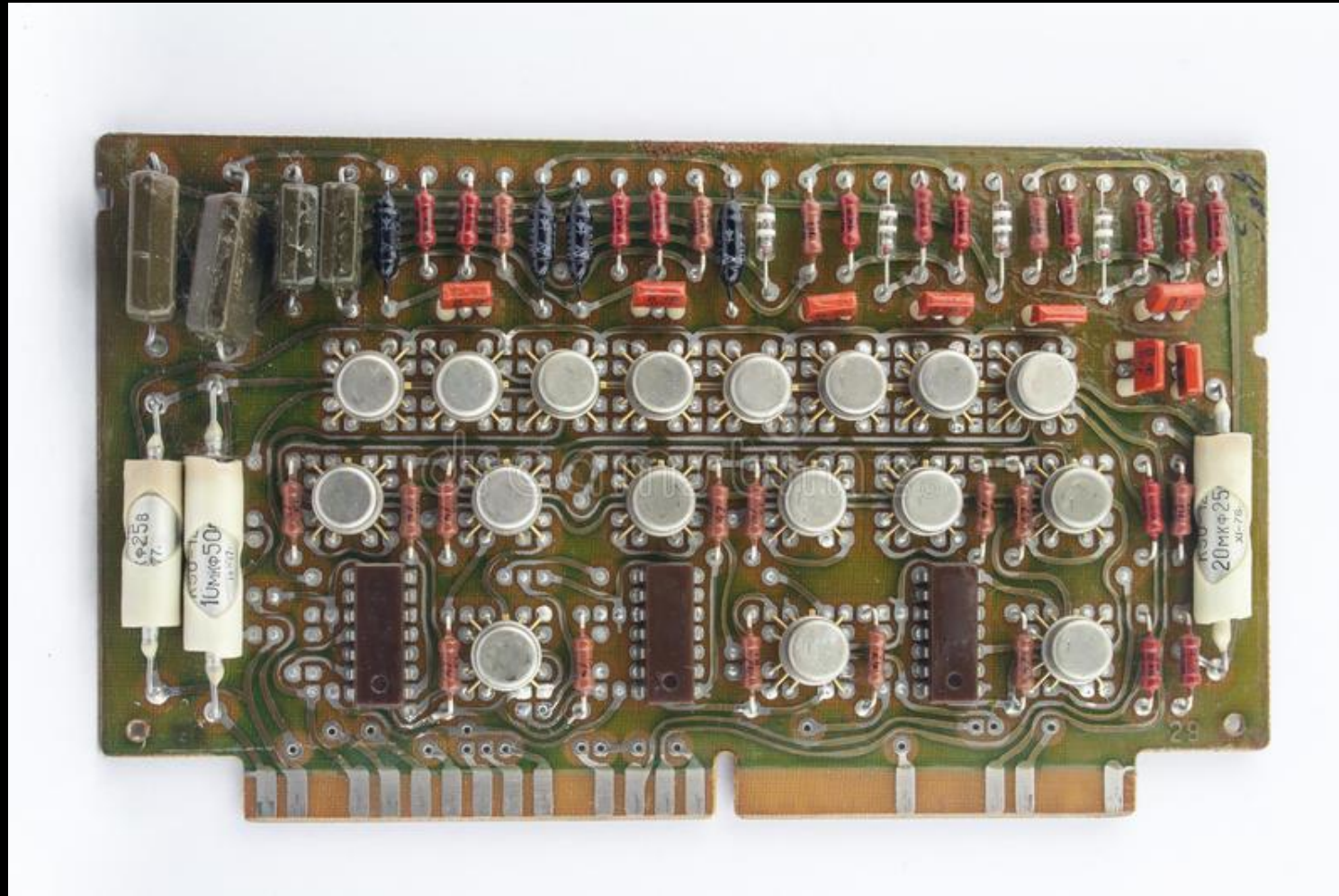
Security vs Cost



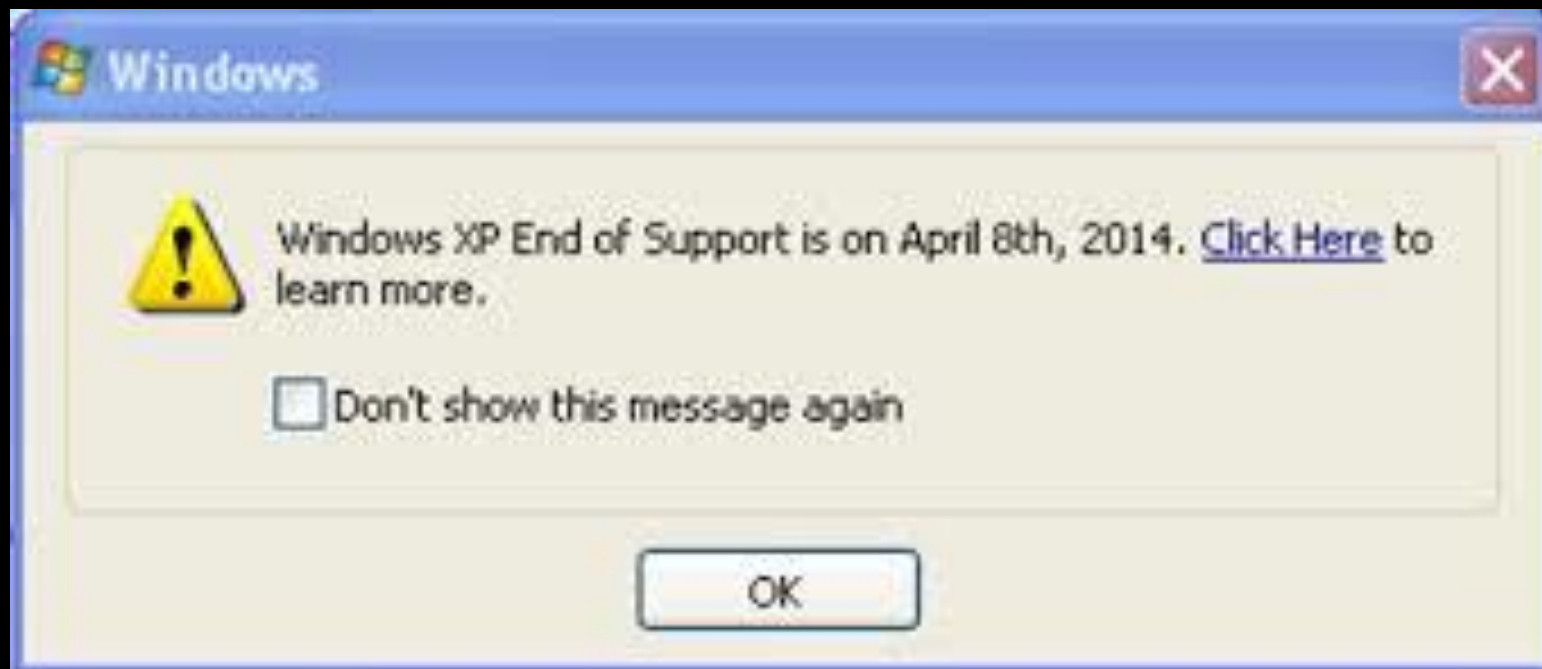
Security vs Battery life



Security vs Lifetime

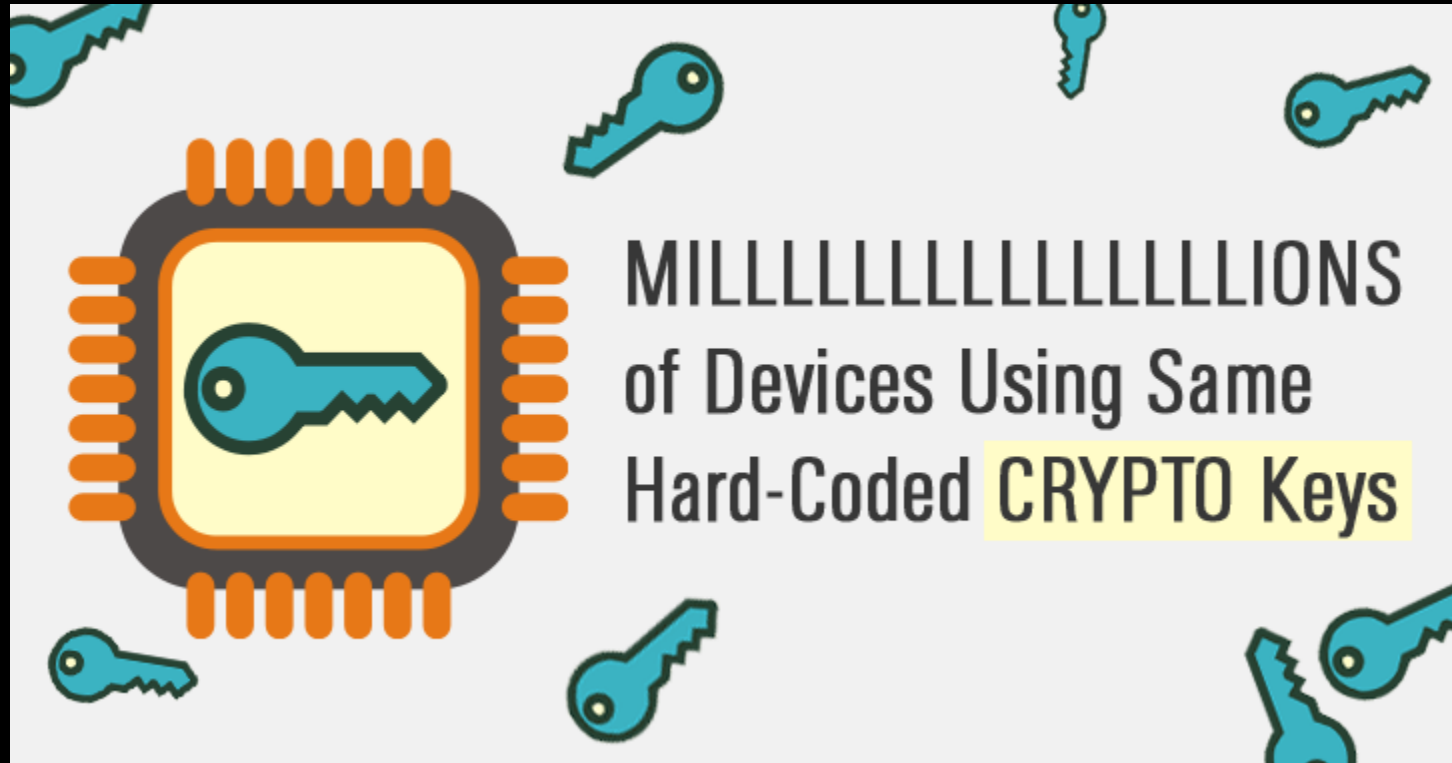


No update = Not safe!



#OTA

Hack one = Hacked 'm all



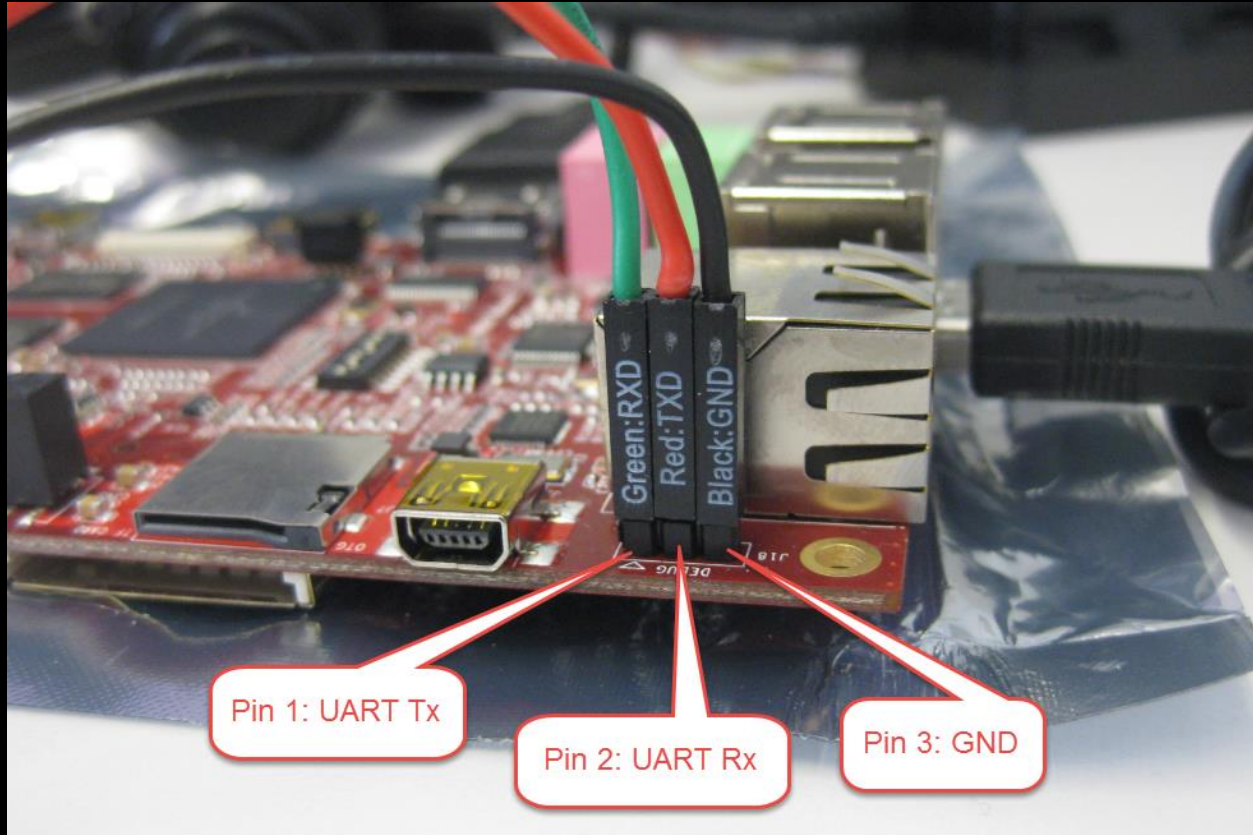
Lack of secure crypto

You failed
at crypto

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

#ecb #entropy

Connect a port & get root

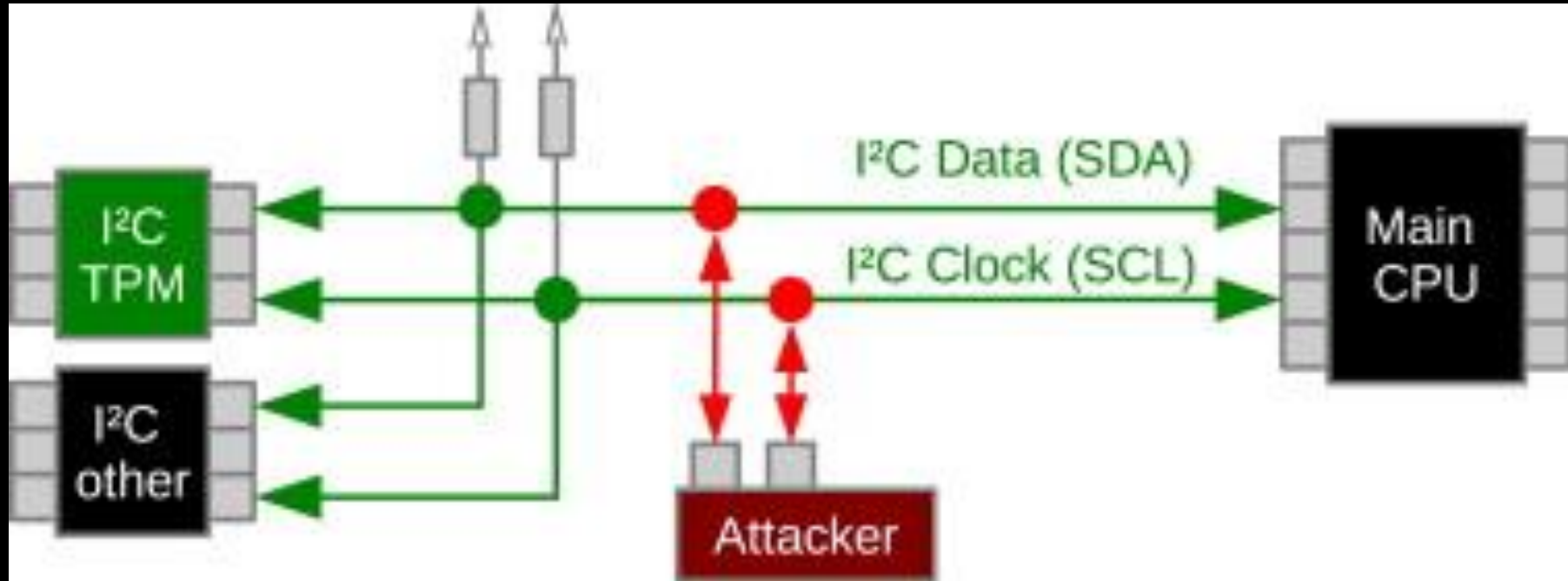


Got Root? █

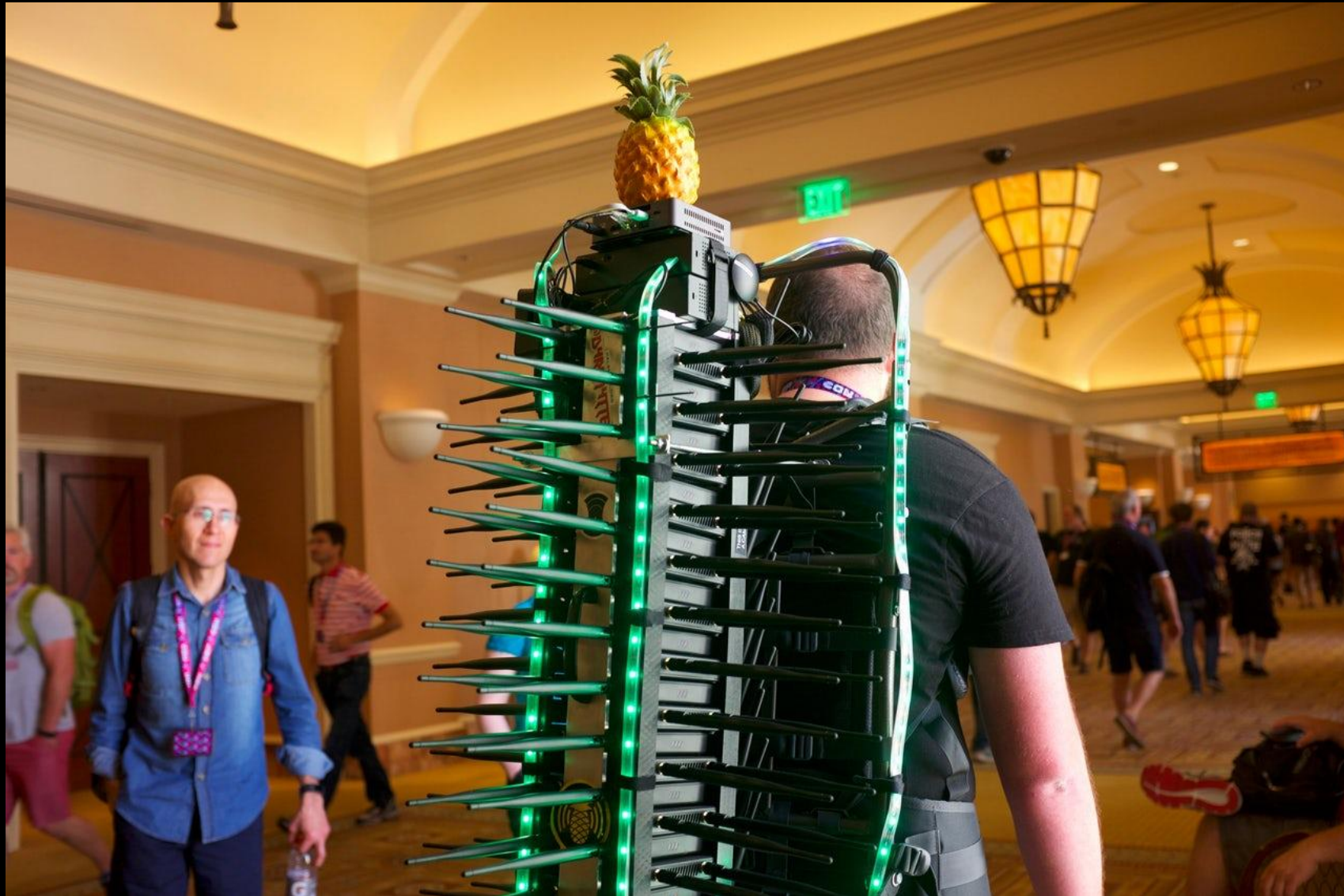
Storage not encrypted

```
root@ubuntu: ~  
root@ubuntu:~# more /etc/passwd  
root:$6$NrGistv6$P4cemGQQwkk0wg2cJn5lh4b9KZHDqr7AiHHNyJQvFtXhP9V0IOhsgf.PleeYIyi  
M44htso86L.3S2RPLitoTe1:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
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
```

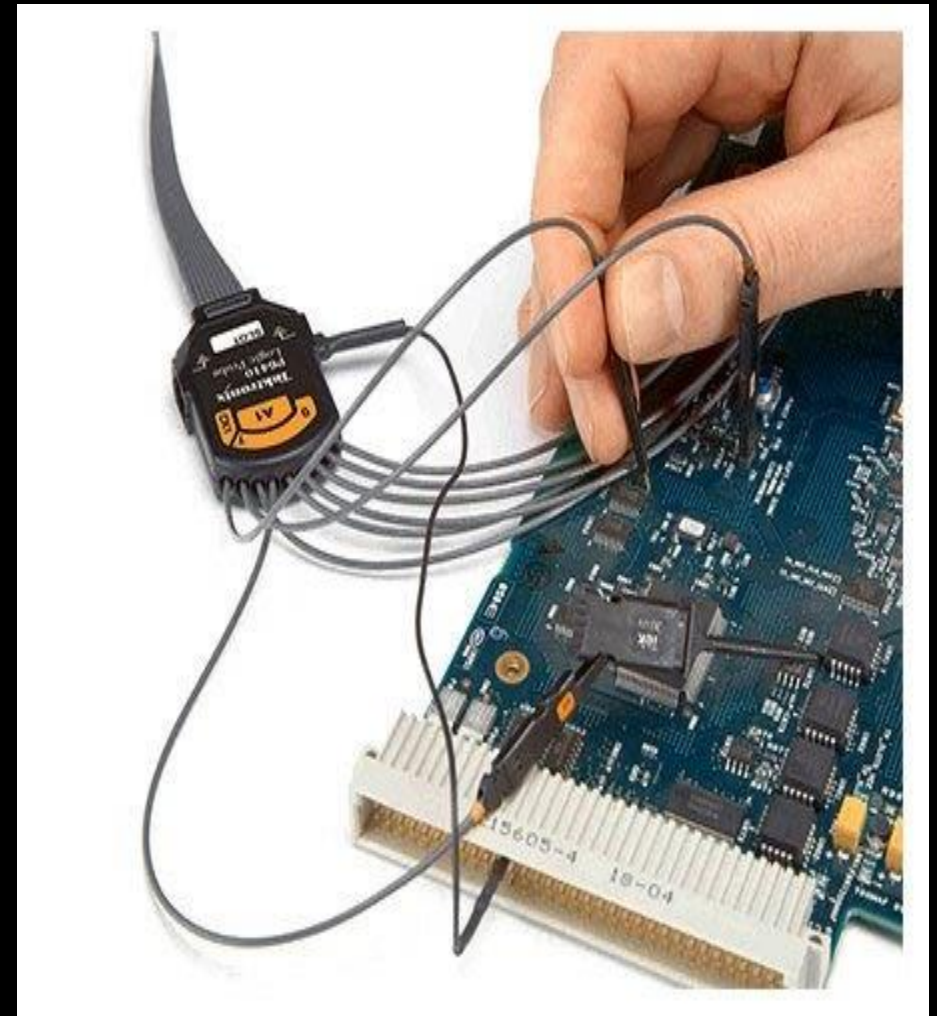
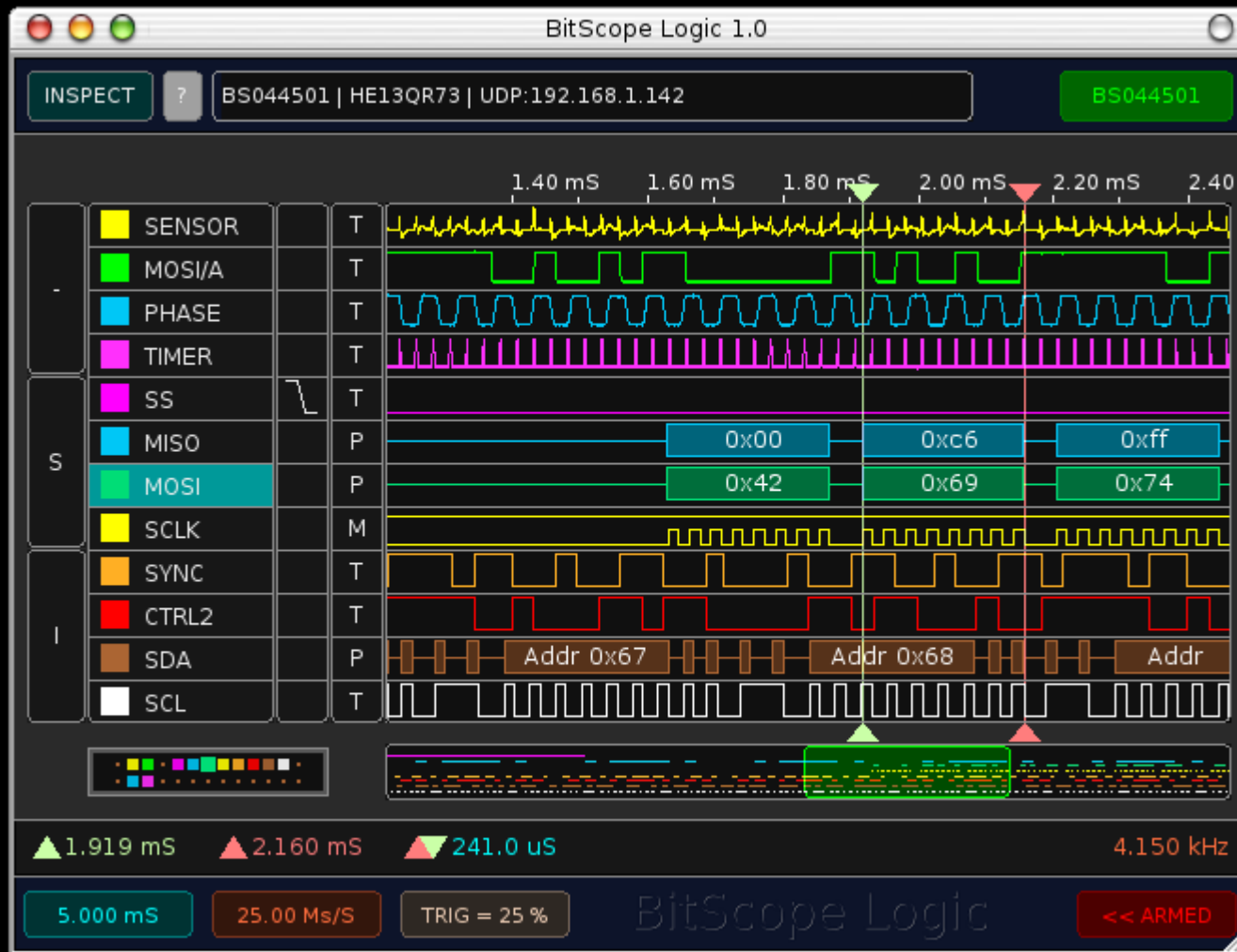
Eavesdropping (MitM)



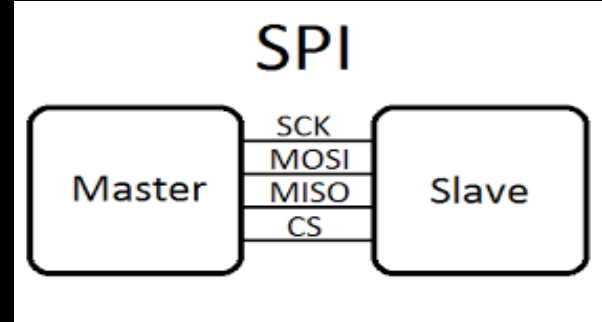
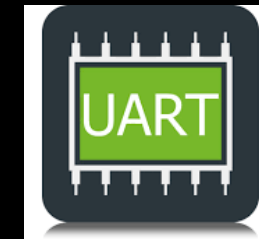
Eavesdropping (WiFi)



Eavesdropping (Logic Analyzer)



Eavesdropping (Protocols)



Release notes are a goldmine

Hardware Requirements:

This firmware requires one of the following Zebra Mobile Printers (where "X" means the value is not important):

P4T (P4D-0XXXXXXXXXX)

RP4T (P4D-XXXXXXXXXX)

Firmware Releases

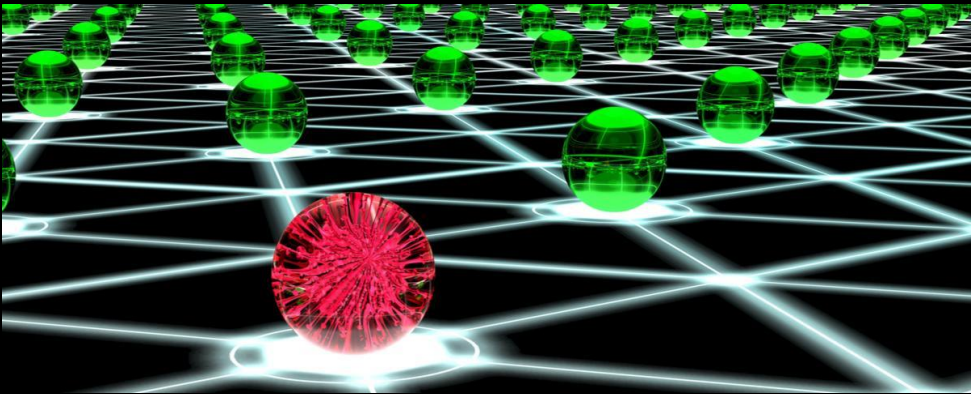
11z42

Release Date: 15 April 2011

Enhancements

- RFID: Increased maximum size of EPC length from 96 to 496 bits [6632]
- Mirror: Added support for encrypted command files (see below for description) [6326]

IOT will be the easy entry point



DDOS



SHODAN Search

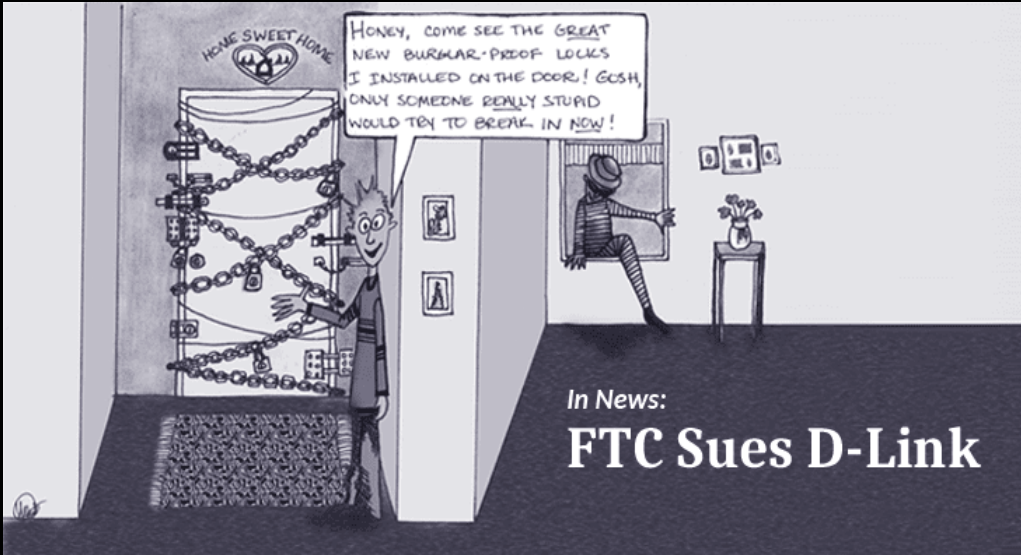
Home Search Directory Data Analytics/ Exports Developer Center Labs

Results 1 - 10 of about 4359 for

| Services | Count |
|----------------|-------|
| Telnet | 2,530 |
| HTTP | 852 |
| HTTP Alternate | 697 |
| FTP | 172 |
| HTTPS | 57 |

| Top Cities | Count |
|-------------------|-------|
| Berlin | 330 |
| Hamburg | 155 |
| Munich | 134 |
| Frankfurt Am Main | 77 |
| Wchtersbach | 75 |

| 77. Kabel Deutschland | 149. Kabel BW |
|--|--|
| Added on 02.09.2013 | Added on 02.09.2013 |
| Germany Gifhorn | Germany Calw |
| Details | Details |
| DD-WRT v24-sp2 std (c) 2013 NewMedia-NET GmbH Release: 03/25/13 (SVN revision: 21061) | DD-WRT v24-sp2 micro (c) 2009 NewMedia-NET GmbH Release: 05/21/09 (SVN revision: 12188) |
| kd-router login: | DD-WRT login: |

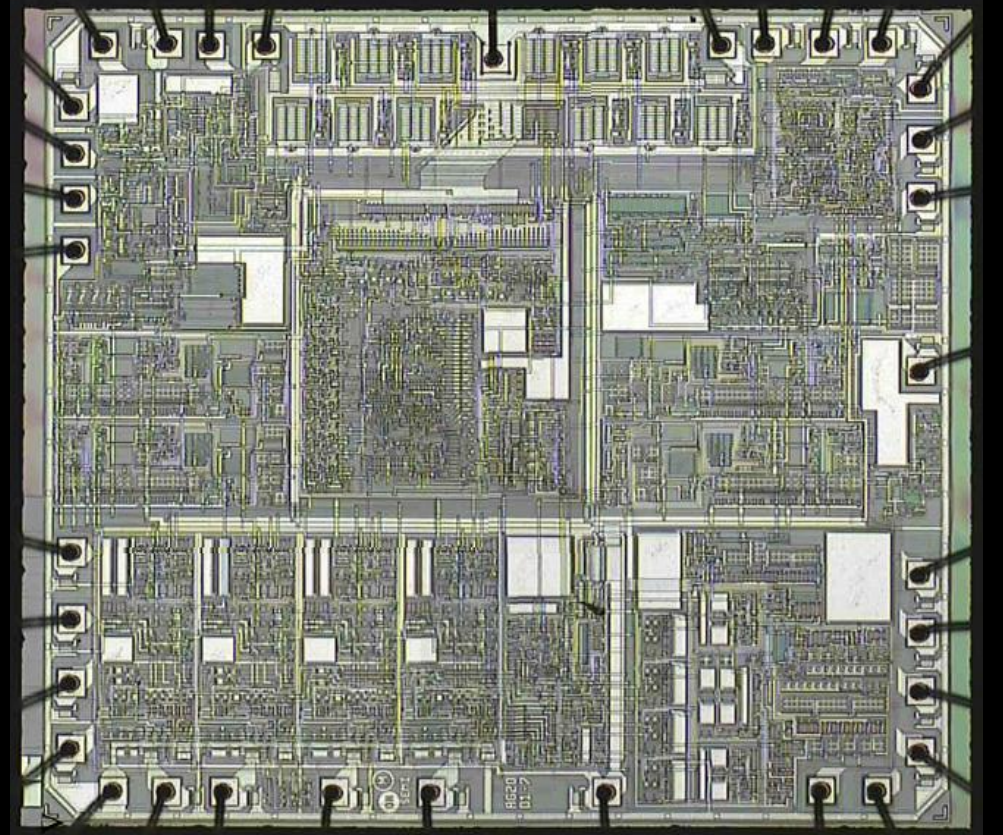
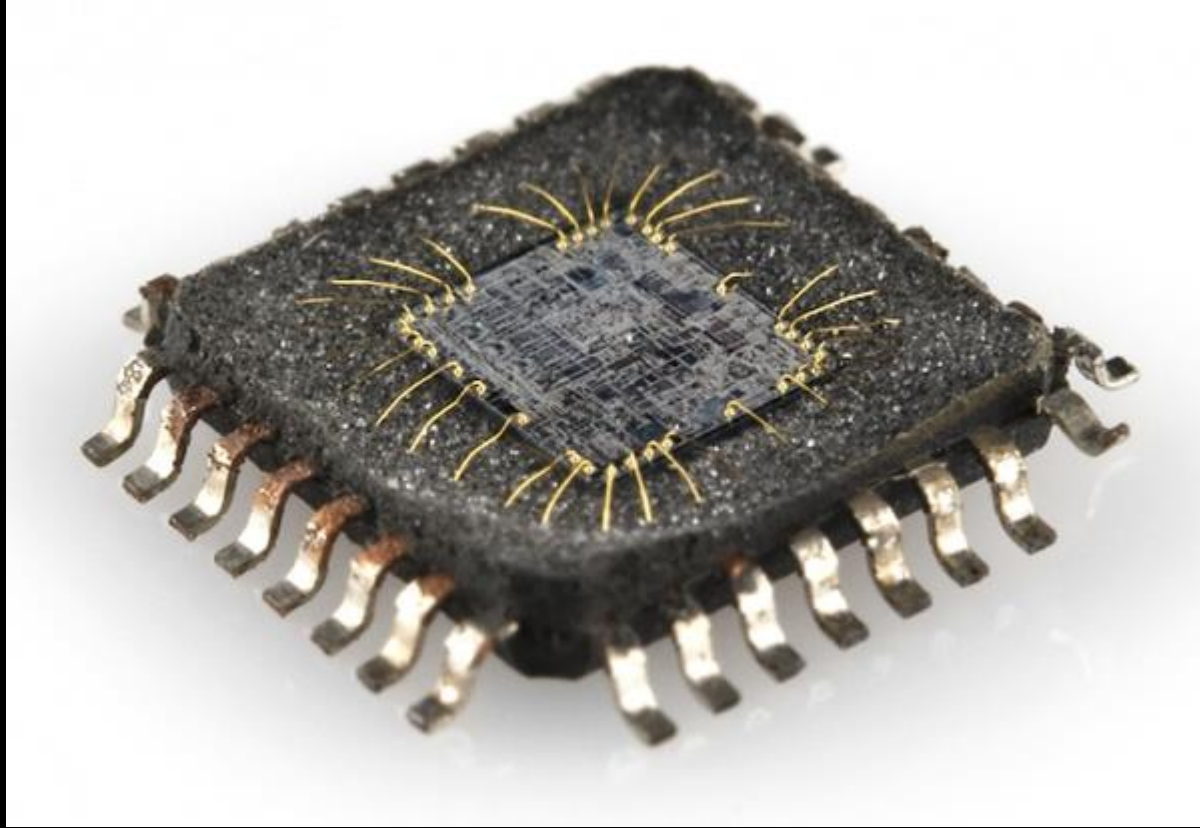


Sidechannel Attacks

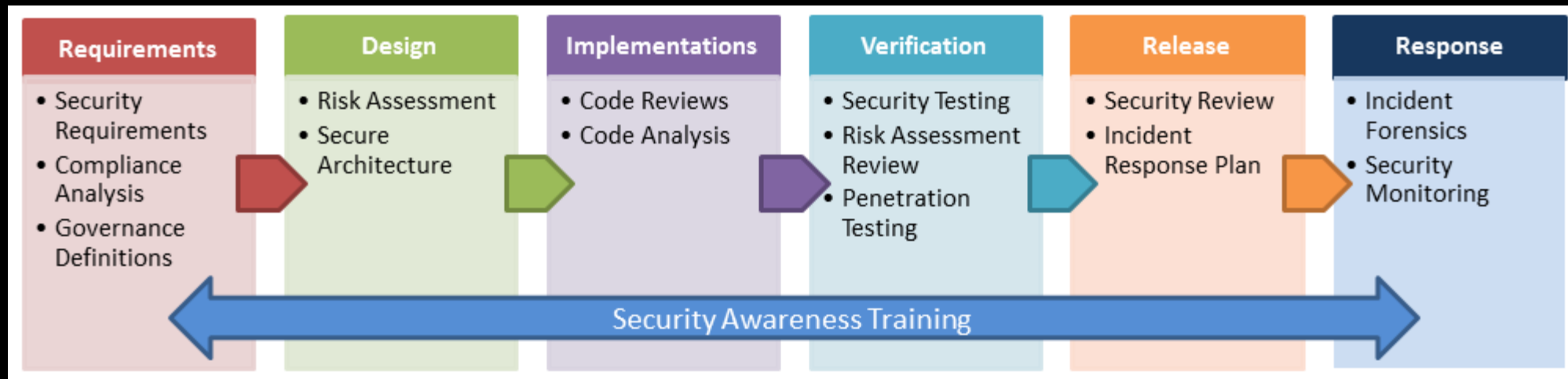


- Clock
- Temperature
- Optical (Light)
- Electromagnetic radiation
- Power

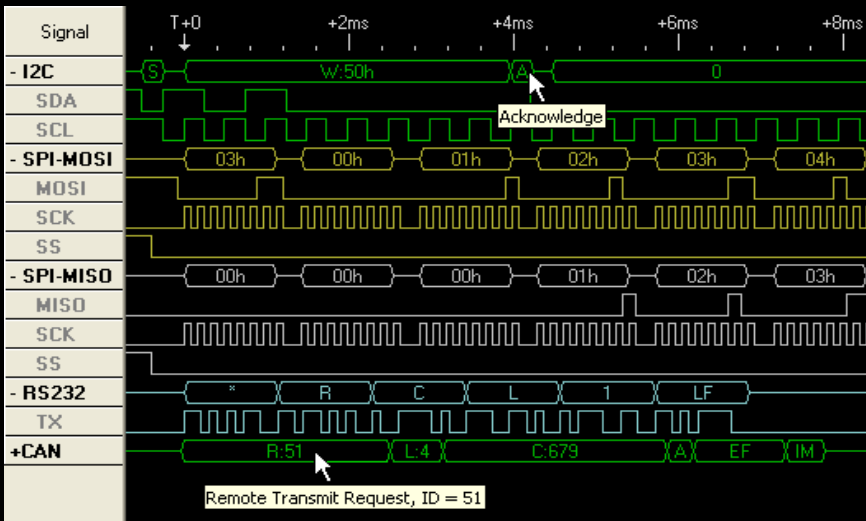
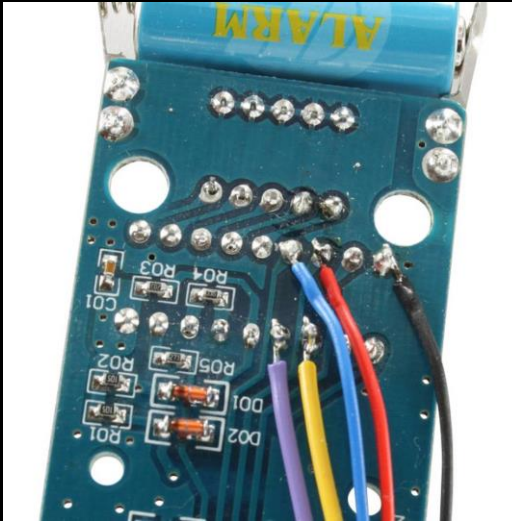
Chip decapping



Security should be part of design



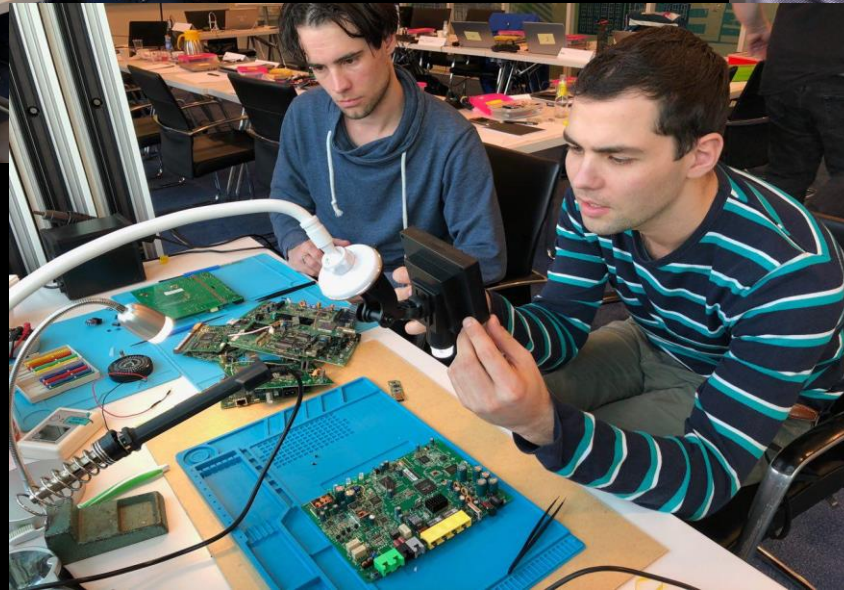
Have your HW tested!



```
→ dll binwalk 027cc450ef5f8c5f653329641ec1fed9
```

| DECIMAL | HEXADECIMAL | DESCRIPTION |
|---------|-------------|--|
| 0 | 0x0 | Microsoft executable, portable (PE) |
| 53088 | 0xCF60 | CRC32 polynomial table, little endian |
| 57184 | 0xDF60 | CRC32 polynomial table, big endian |
| 61463 | 0xF017 | Copyright string: "Copyright 1995-2013 Mark Adler " |
| 84080 | 0x14820 | Microsoft executable, portable (PE) |
| 90208 | 0x16060 | Microsoft executable, portable (PE) |
| 105196 | 0x19AEC | Zlib compressed data, best compression |
| 130156 | 0x1FC6C | Zlib compressed data, best compression |
| 157584 | 0x26790 | Zlib compressed data, best compression |
| 349192 | 0x55408 | Zlib compressed data, best compression |
| 356509 | 0x57090 | Certificate in DER format (x509 v3), header length: 4, sequence length: 1120 |
| 357633 | 0x57501 | Certificate in DER format (x509 v3), header length: 4, sequence length: 1146 |
| 358783 | 0x5797F | Certificate in DER format (x509 v3), header length: 4, sequence length: 1181 |
| 359968 | 0x57E20 | Certificate in DER format (x509 v3), header length: 4, sequence length: 1194 |

Learn to do it yourself!



FREE

TIPS

1: Lock your devices

Lock the computer:



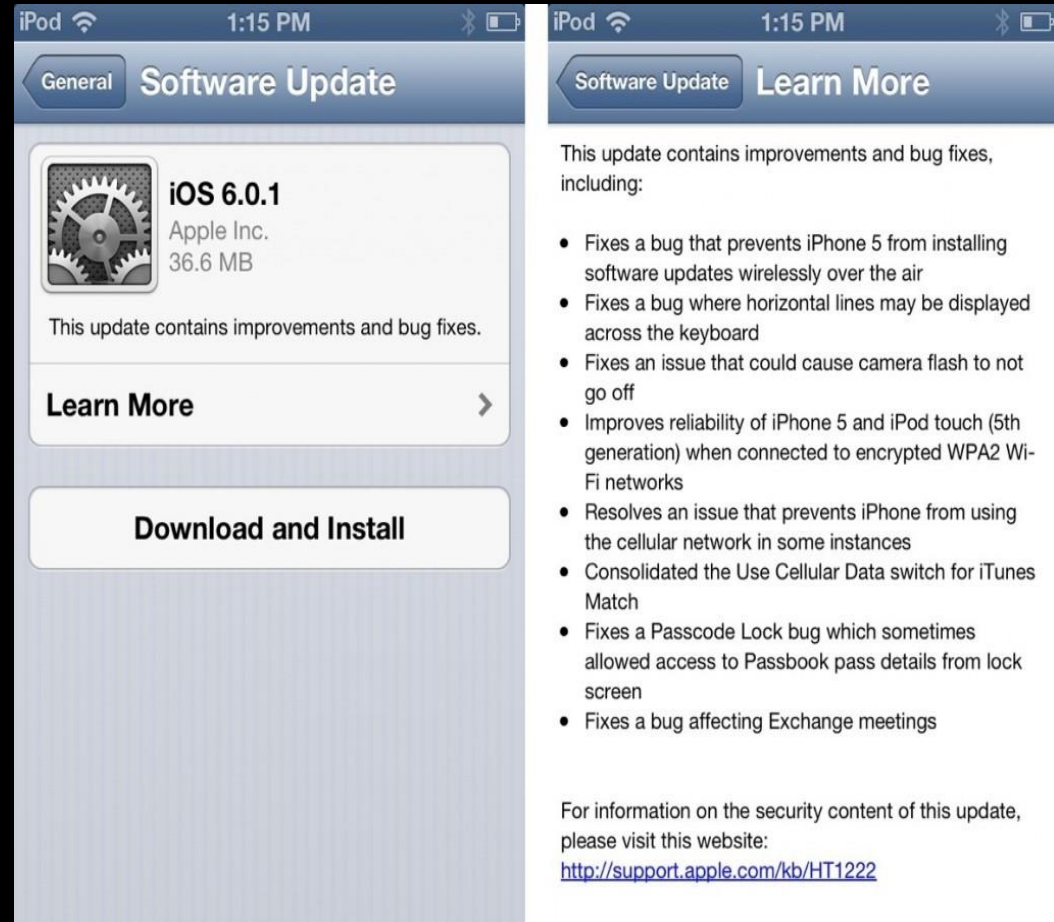
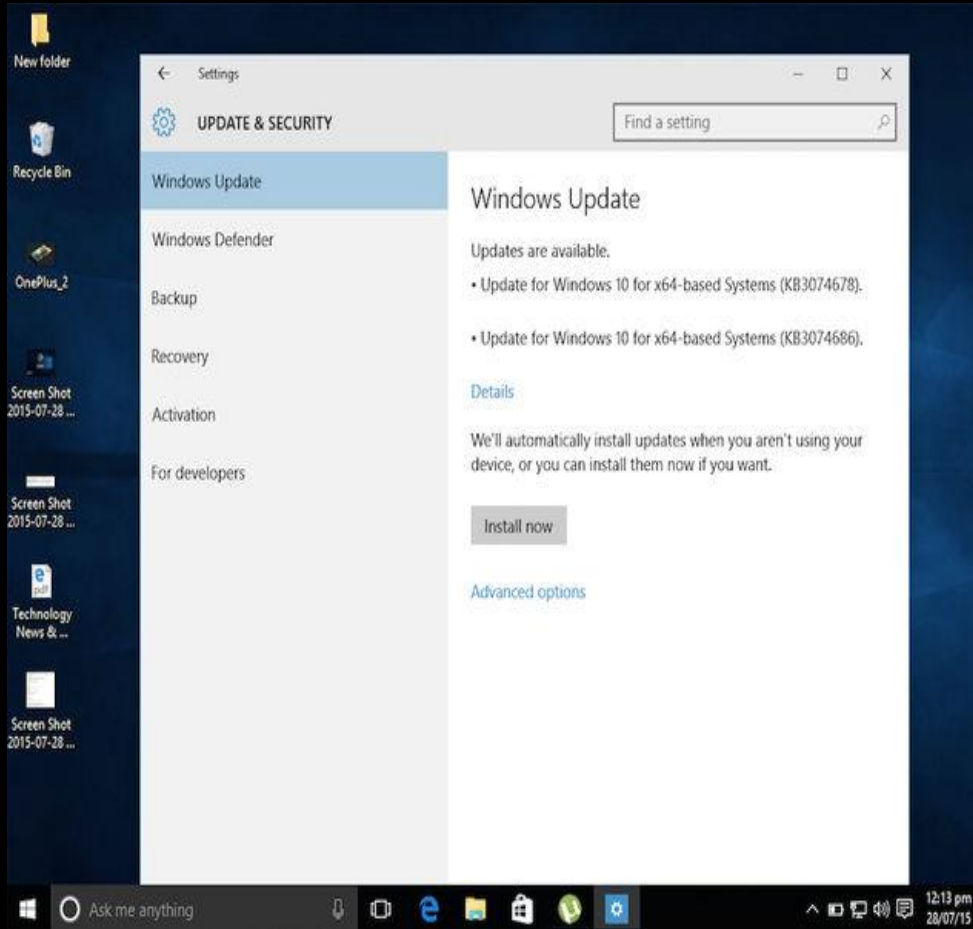
+



2: Create backup & unplug!



3: Update your devices



4: Enable Multi Factor



5: Use long passwords

TIME TO CRACK:
15 HOURS

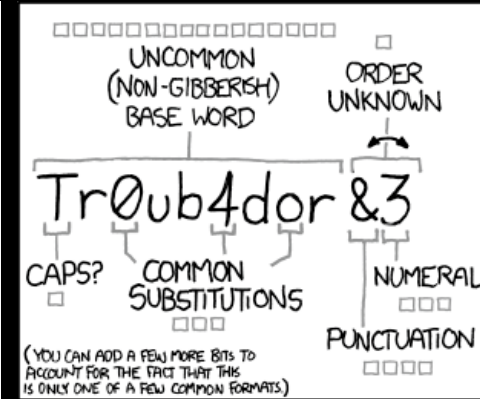
Compl3xi

graded at howsecureismypassword.net

TIME TO CRACK:
4000 YEARS

Compl3xity_

graded at howsecureismypassword.net



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

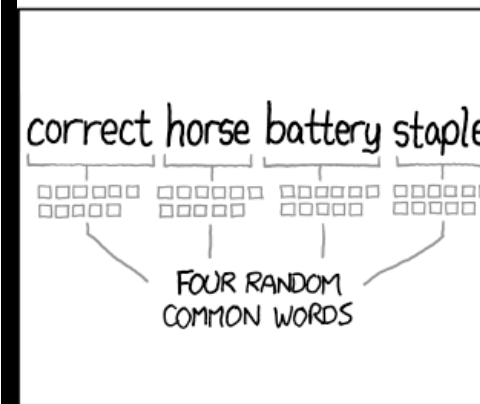
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

6: Password still safe?

Have I been pwned? X
https://haveibeenpwned.com

!;--have i been pwned?

Check if you have an account that has been compromised in a data breach

donald@trump.com **pwned?**

Oh no — pwned!
Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

A **Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Search through 1.4 billion leaked accounts
3.1 million in The Netherlands

Gotcha?

president@whitehouse.gov Search

Tip: see also @whitehouse.gov or The Netherlands.

Found 18 account(s)

| | |
|--------------------------|---------|
| Pres*****@whitehouse.gov | Cl***** |
| pres*****@whitehouse.gov | 12***** |
| pres*****@whitehouse.gov | Cl***** |
| pres*****@whitehouse.gov | Ke***** |
| pres*****@whitehouse.gov | ad***** |
| pres*****@whitehouse.gov | as***** |
| pres*****@whitehouse.gov | bi***** |
| pres*****@whitehouse.gov | cl***** |
| pres*****@whitehouse.gov | ff***** |

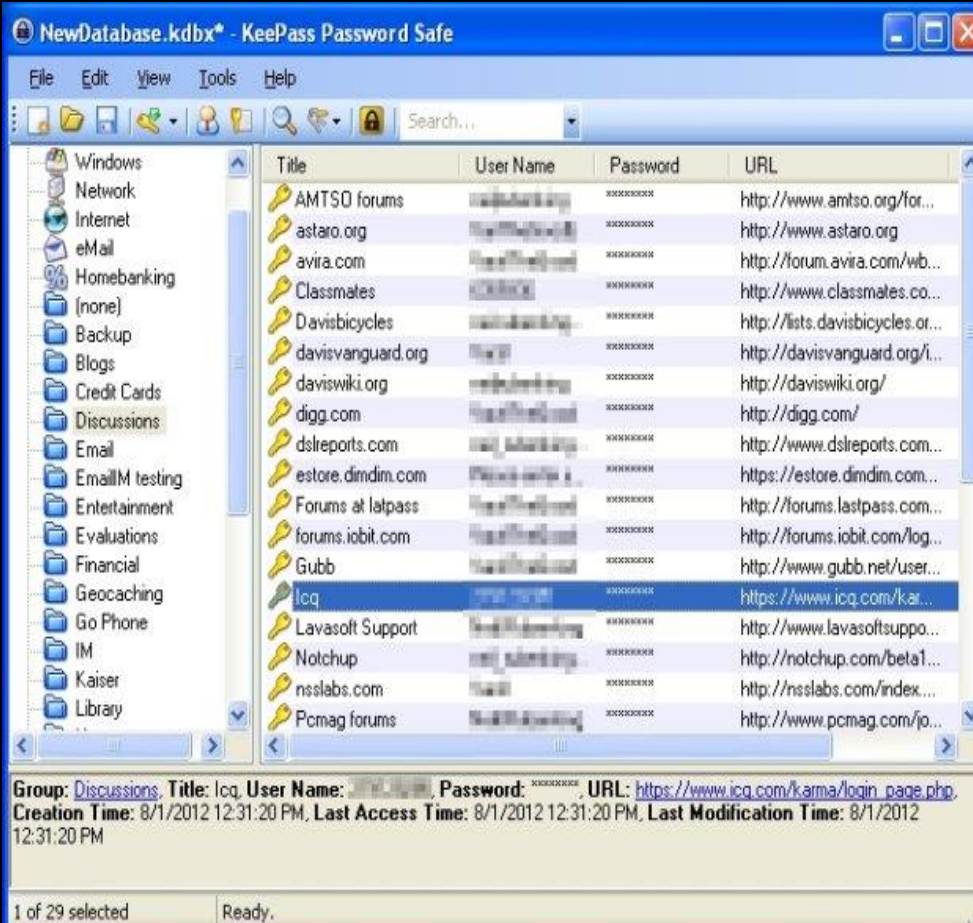
7: Use a password manager



**WORST
PASSWORDS**

- 1 123456
- 2 password
- 3 12345678
- 4 qwerty
- 5 12345
- 6 123456789
- 7 football
- 8 1234
- 9 1234567
- 10 baseball

splashdata



NewDatabase.kdbx* - KeePass Password Safe

File Edit View Tools Help

Search...

| Title | User Name | Password | URL |
|-------------------|--------------|----------|----------------------------------|
| AMTSD forums | web@bank.org | xxxxxxxx | http://www.amtso.org/for... |
| astaro.org | web@bank.org | xxxxxxxx | http://www.astaro.org |
| avira.com | web@bank.org | xxxxxxxx | http://forum.avira.com/wb... |
| Classmates | web@bank.org | xxxxxxxx | http://www.classmates.co... |
| Davisbicycles | web@bank.org | xxxxxxxx | http://lists.davisbicycles.or... |
| davisvanguard.org | web@ | xxxxxxxx | http://davisvanguard.org/i... |
| daviswiki.org | web@bank.org | xxxxxxxx | http://daviswiki.org/ |
| digg.com | web@bank.org | xxxxxxxx | http://digg.com/ |
| dsreports.com | web@bank.org | xxxxxxxx | http://www.dsreports.com... |
| estore.dimdim.com | web@bank.org | xxxxxxxx | https://estore.dimdim.com... |
| Forums at latpass | web@bank.org | xxxxxxxx | http://forums.lastpass.com... |
| forums.iobit.com | web@bank.org | xxxxxxxx | http://forums.iobit.com/log... |
| Gubb | web@bank.org | xxxxxxxx | http://www.gubb.net/user... |
| icq | web@bank.org | xxxxxxxx | https://www.icq.com/k.ar... |
| Lavasoft Support | web@bank.org | xxxxxxxx | http://www.lavasoftsuppo... |
| Notchup | web@bank.org | xxxxxxxx | http://notchup.com/beta1... |
| nsslabs.com | web@ | xxxxxxxx | http://nsslabs.com/index... |
| Pcmag forums | web@bank.org | xxxxxxxx | http://www.pcmag.com/fo... |

Group: Discussions, Title: Icq, User Name: web@bank.org, Password: xxxxxxxx, URL: https://www.icq.com/karma/login_page.php
Creation Time: 8/1/2012 12:31:20 PM, Last Access Time: 8/1/2012 12:31:20 PM, Last Modification Time: 8/1/2012 12:31:20 PM

1 of 29 selected | Ready.

8: Use fake answers

Your question and secret answer

Question:

Secret answer:

Select...

- Mother's birthplace
- Best childhood friend
- Name of first pet
- Favorite teacher
- Favorite historical person
- Grandfather's occupation

We gebruiken cookies om inhoud en advertenties relevanter te maken en je een veiligere ervaring te bieden. Als je op de website klikt of op de website navigeert, ga je ermee akkoord dat we op en buiten Facebook informatie verzamelen via cookies. Meer informatie, zoals over hoe je je instellingen kunt aanpassen, vind je hier: [cookiebeleid](#)

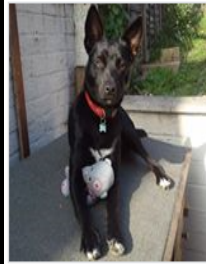
facebook

E-mail of telefoon

Wachtwoord

Aanmelden

[Account vergeten?](#)



Come Home Charlie

@comehomecharlieisleofwight

Startpagina

Info

Foto's

Vind-ik-leuks



Vind ik leuk

Bericht verzenden

Delen

Meer



Come Home Charlie

19 uur · 6

Community

9: VPN while on Free WiFi



Questions?



**KEEP
CALM
AND
HUG A
HACKER**

twitter 



Jilles

@jilles_com

CYBER Security, HW Hacking, IoT, Crypto, DFIR, SecOps, Lock picking, Education, Gadgets, LEGO, ComicCon 🌸
TwitterHippie, 🤖 @syljil @jurrejelle & Jelle



Jurre

@Jurrejelle

Gamer, Hacker, Programmer. Son of @syljil and @jilles_com, brother of Jelle | CS-0904140001