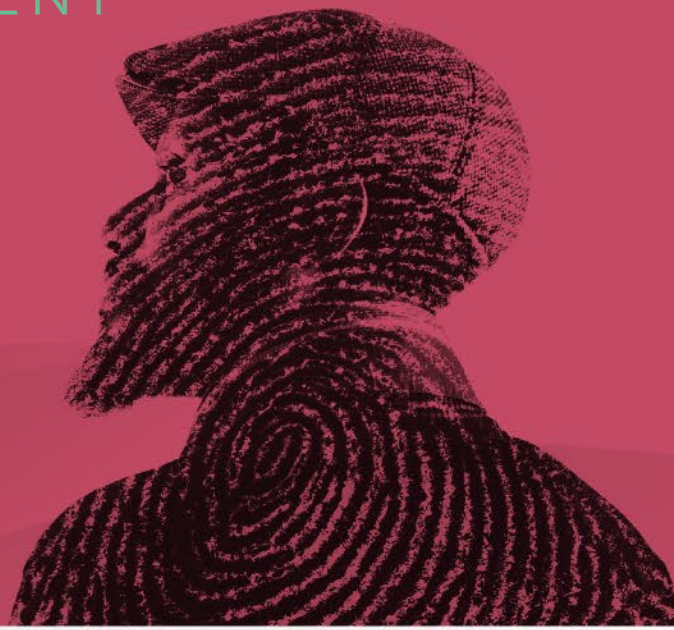
RSAC Sandbox

RSAConference2020

HUMAN ELEMENT



SESSION ID: **HTA-R01**

# Hacking the Unhackable: Pwning the Bitfi Crypto Wallet

**Ken Munro**

Partner
Pen Test Partners
@thekenmunroshow

# Who am I?

A security researcher & penetration tester

Part of a team of ~100 who carry out extensive research in to hardware & software security at @pentestpartners

Planes, trains, automobiles

Known for public research in to hacking Mitsubishi vehicles, My Friend Cayla, wi-fi kettles, Samsung smart TVs, fridges and much more

I’m listening to your child

**** You!

# California Senate Bill 327

## Cited My Friend Cayla

Makes ‘reasonable security features’ mandatory from Jan 1 2020

**Senate Bill No. 327**

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[ Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018. ]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and

Jackson said she’s had “concerns about privacy issues for many, many years,” and was prompted to act last year after hearing from constituents and learning that the My Friend Cayla smart doll, which had been banned in Germany due to concerns about the safety of children, had not been banned in the U.S. She questioned how IoT devices including microwaves, thermostats and security cameras were securitized and was shocked by the lack of security she found.

# Unhackable!

**Bitfi**
@Bitfi6

Bitfi manufactures the world's first and only completely un-hackable hardware wallet for storing cryptocurrency and digital assets. It changes everything.

**John McAfee** 
@officialmcafee

For all you naysayers who claim that “nothing is unhackable” & who don’t believe that my Bitfi wallet is truly the world’s first unhackable device, a $100,000 bounty goes to anyone who can hack it. Money talks, bullshit walks. Details on Bitfi.com

6:12 PM - Jul 24, 2018

 2,523  1,053 people are talking about this 

# Bitfi statement


“your private keys are NEVER stored anywhere except your own brain”

# Unhackable!

The rules for claiming the bounty are simple:

- We deposit coins into a Bitfi wallet
- If you wish to participate in the bounty program, you will purchase a Bitfi wallet that is preloaded with coins for just an additional $50 (the reason for the charge is because we need to ensure serious inquiries only)
- If you successful extract the coins and empty the wallet, this would be considered a successful hack
- You can then keep the coins and Bitfi will make a payment to you of $100,000

# Unhackable!

> This bounty program is not intended to help **Bitfi** to identify **security** vulnerabilities since we already claim that **our security is absolute**

# Unhackable!

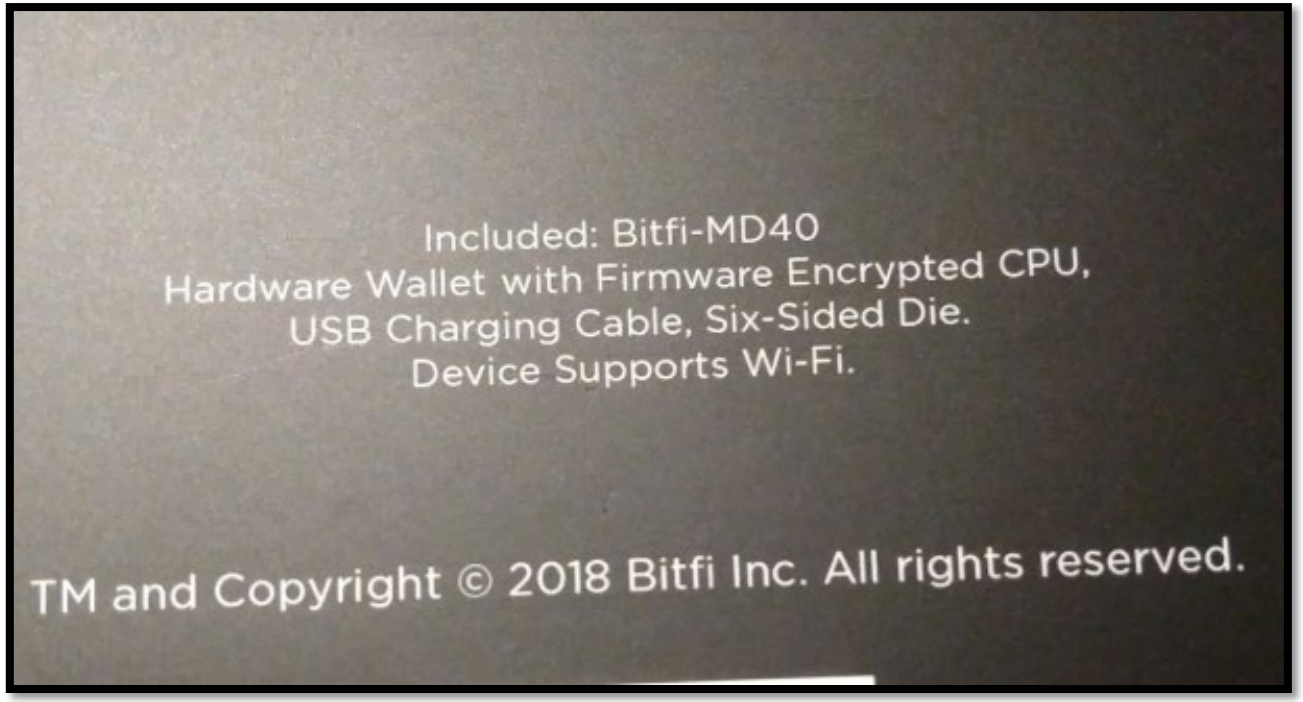
"Bitfi is unhackable"

=

Bitfi is not vulnerable to one very specific attack

# Unhackable!

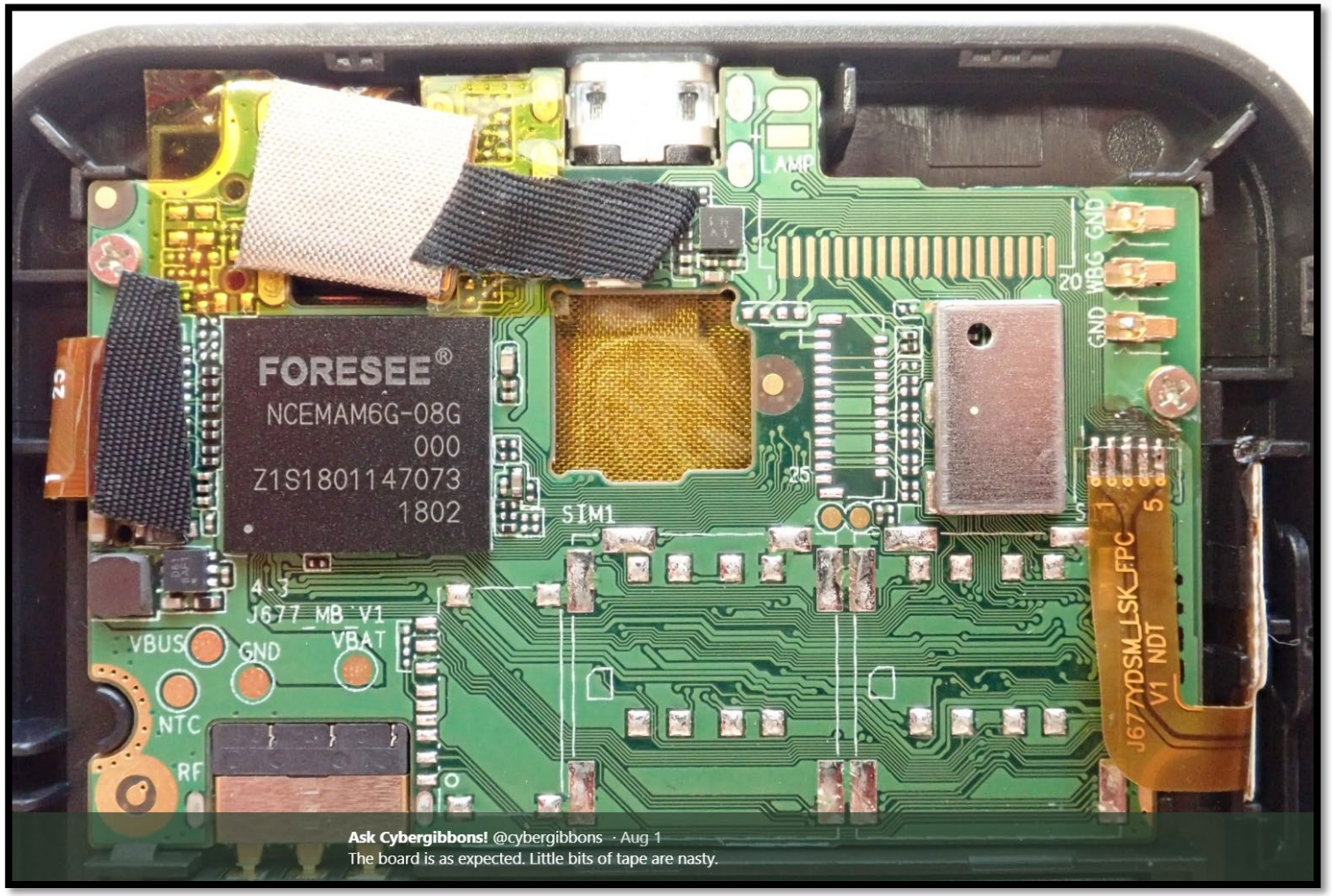

bitfi
bitfi


Included: Bitfi-MD40
Hardware Wallet with Firmware Encrypted CPU,
USB Charging Cable, Six-Sided Die.
Device Supports Wi-Fi.
TM and Copyright © 2018 Bitfi Inc. All rights reserved.

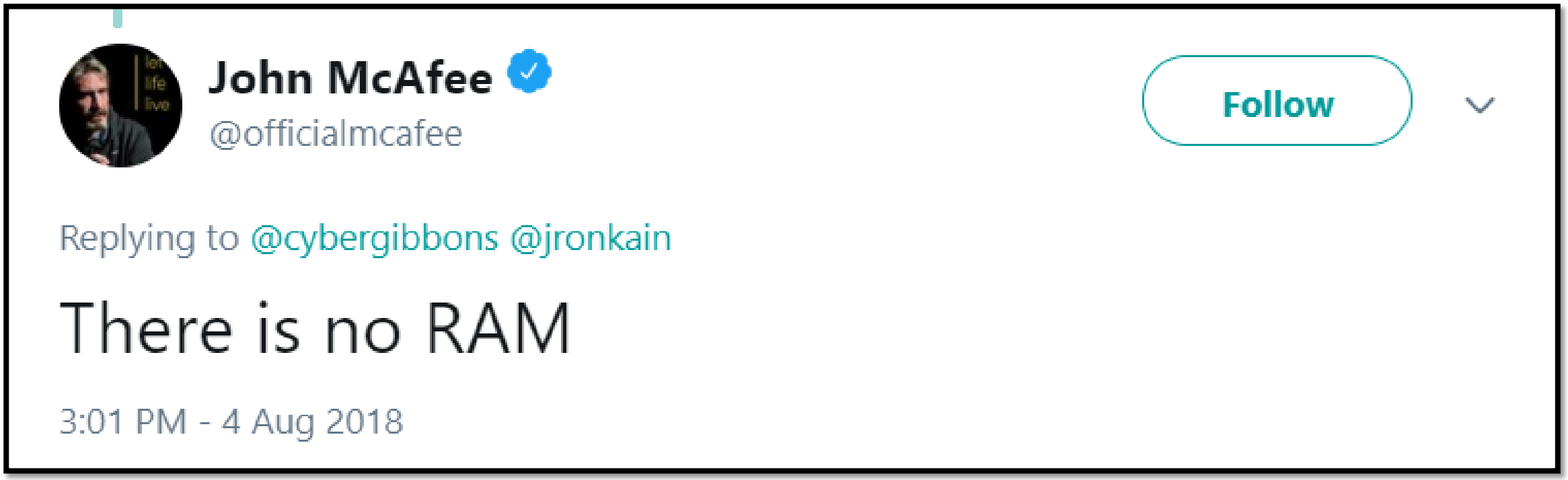
# Claims


John McAfee
@officialmcafee
Follow
Replying to @danialzargoosh
There is no memory to hack. No data. All of your money is stored in a memorable phrase of your choice in your head. That phrase is converted to your seed keys. Wallet is then created for the time of your transaction then is removed. There is nothing but the phrase in your head.

# Evidence


FORESEE®
NCEMAM6G-08G
000
Z1S1801147073
1802
SIM1
J677_MB_V1
VBUS
GND
VBAT
NTC
RF
LAMP
GND
WBG
GND
J677YDSMLSK_FPC
V1 NDT
Ask Cybergibbons! @cybergibbons · Aug 1
The board is as expected. Little bits of tape are nasty.

# Claims

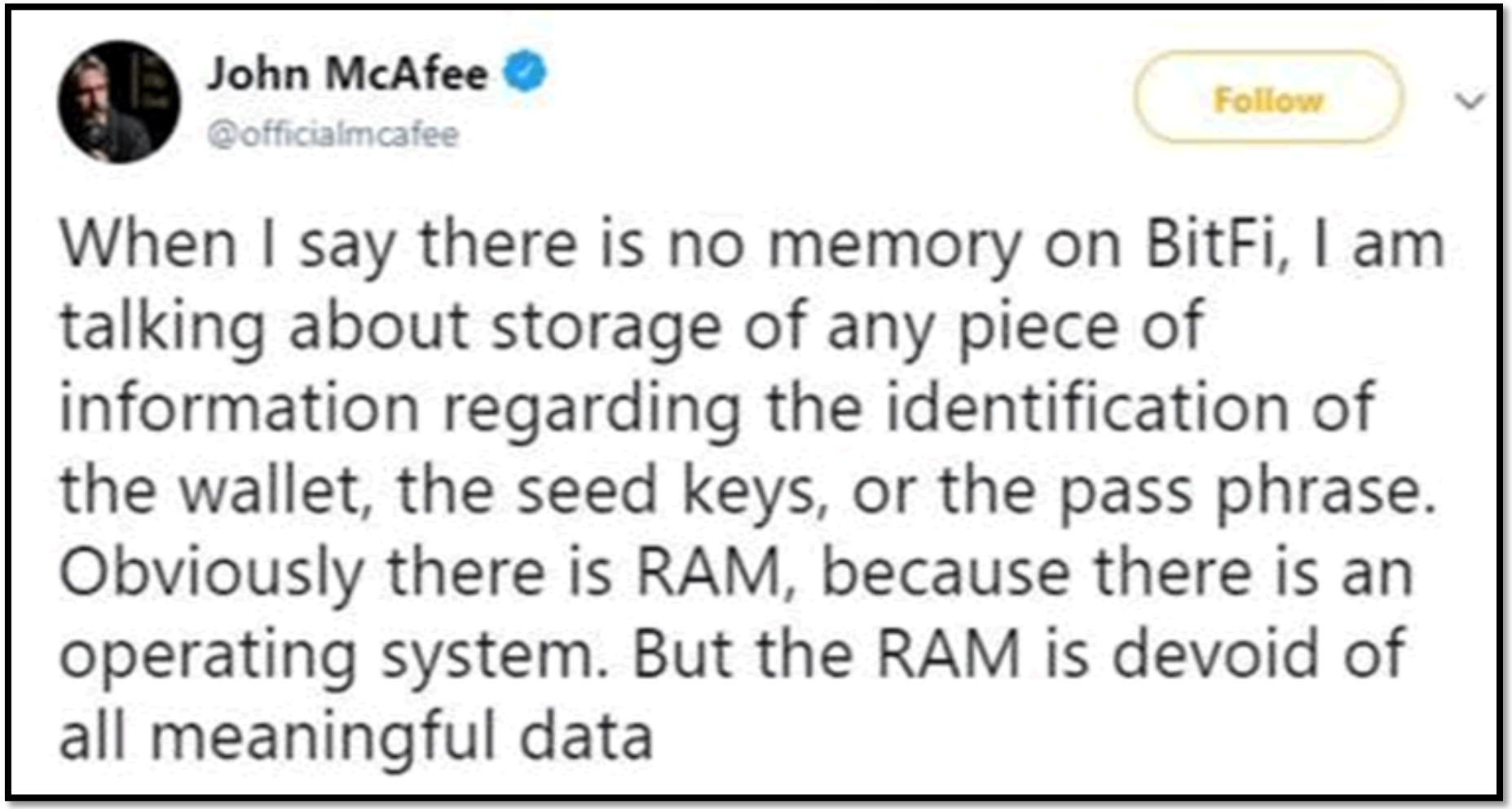

John McAfee
@officialmcafee
Follow
Replying to @cybergibbons @jronkain
There is no RAM
3:01 PM - 4 Aug 2018

# Claims


John McAfee
@officialmcafee
Follow
Replying to @AlexDenStoerste
It can't be hacked. Fact. There is no software on the device, and no memory. So you can't do a software hack. And the pass phrase is stored nowhere. Not in a server, not in the device ... nowhere. There is nothing you can do to the hardware that will give you the pass phrase.

# Evidence

# Claims



John McAfee
@officialmcafee
Follow

When I say there is no memory on BitFi, I am talking about storage of any piece of information regarding the identification of the wallet, the seed keys, or the pass phrase. Obviously there is RAM, because there is an operating system. But the RAM is devoid of all meaningful data

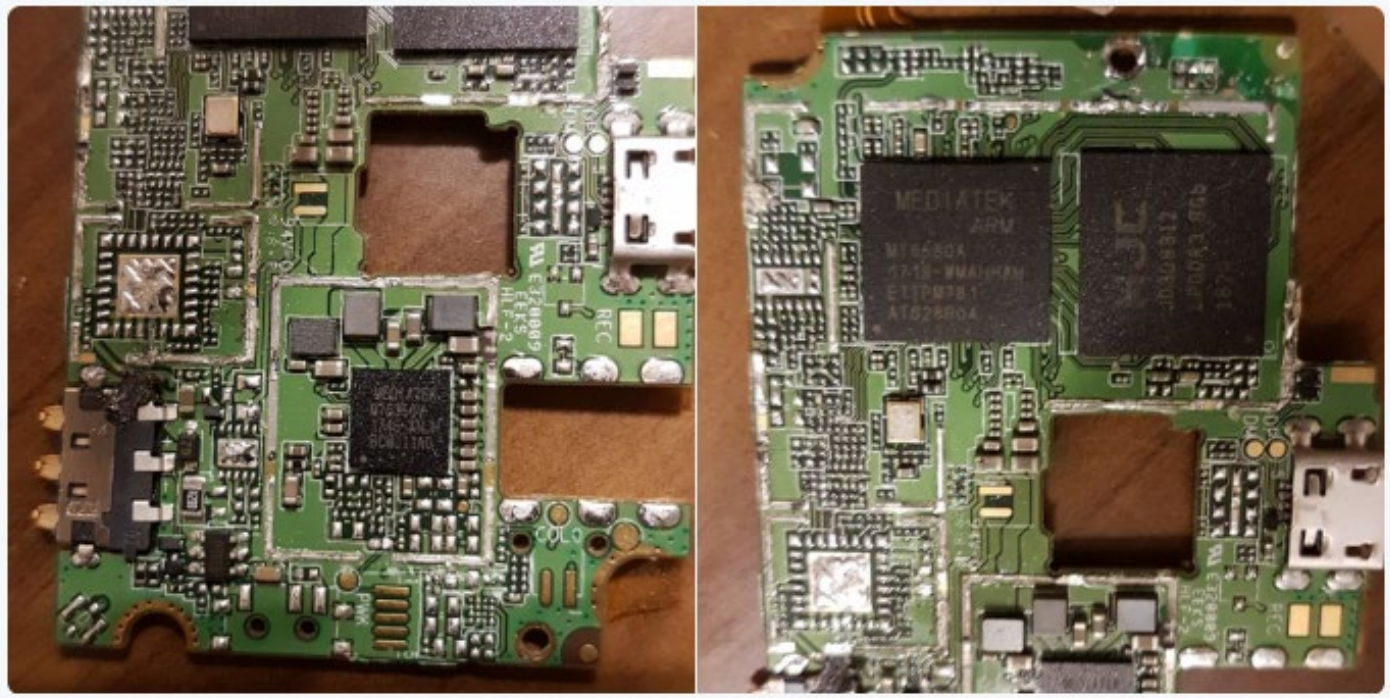
*The Bitfi wallet is only $120 USD. As a computing device it is much more costly to manufacture than ordinary hardware wallets, however, our mission is to make this technology accessible to everyone and to keep it affordably priced as long as possible.*

# Evidence

It's just a MEDIATEK MT6580.

No sign of a secure element.

Thanks to @Mindstalker612



# Claims

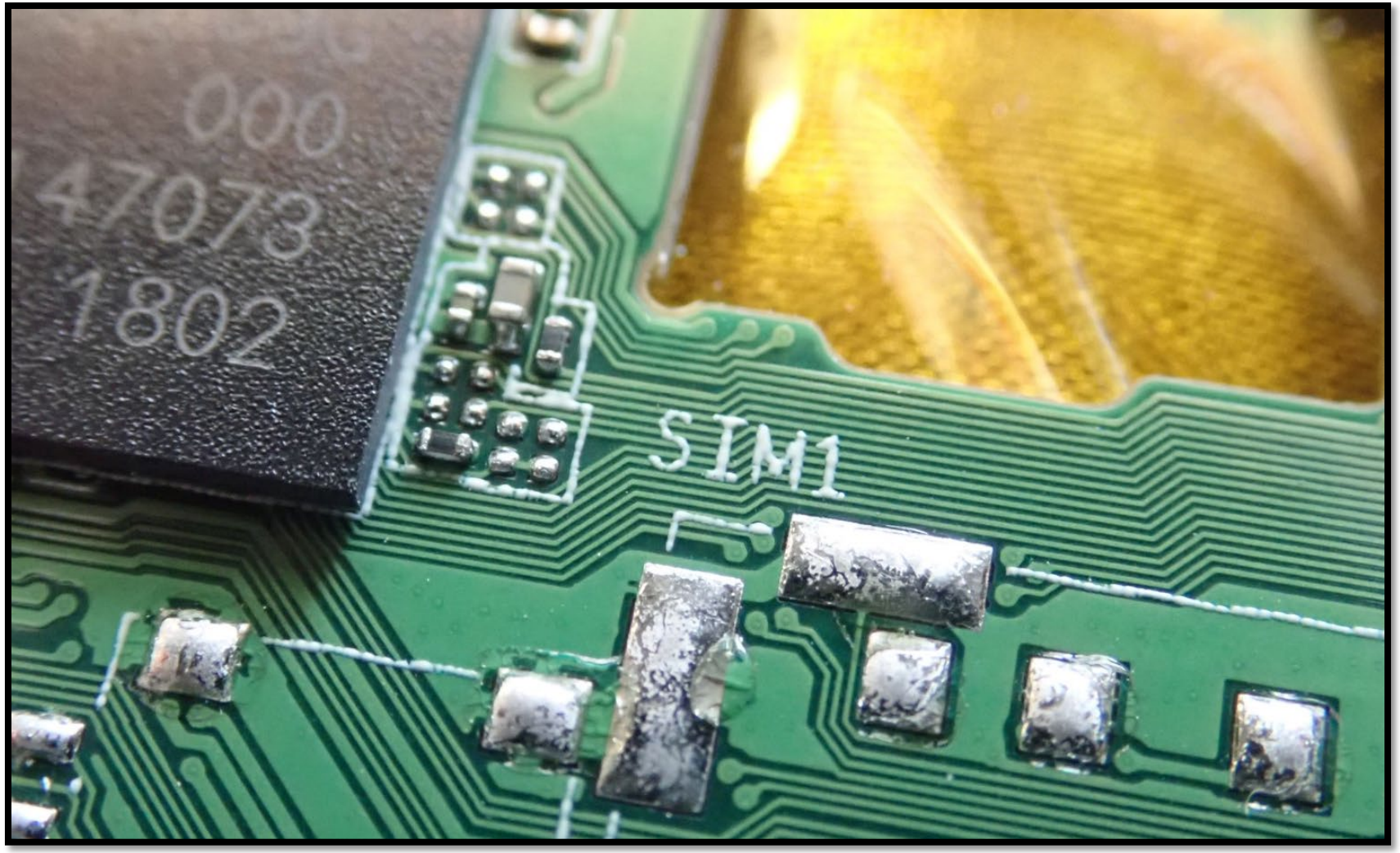
**John McAfee** @officialmcafee · Jul 31

It is absolutely not a cell phone or anything even resembling a cell phone. All cell phones are hackable.

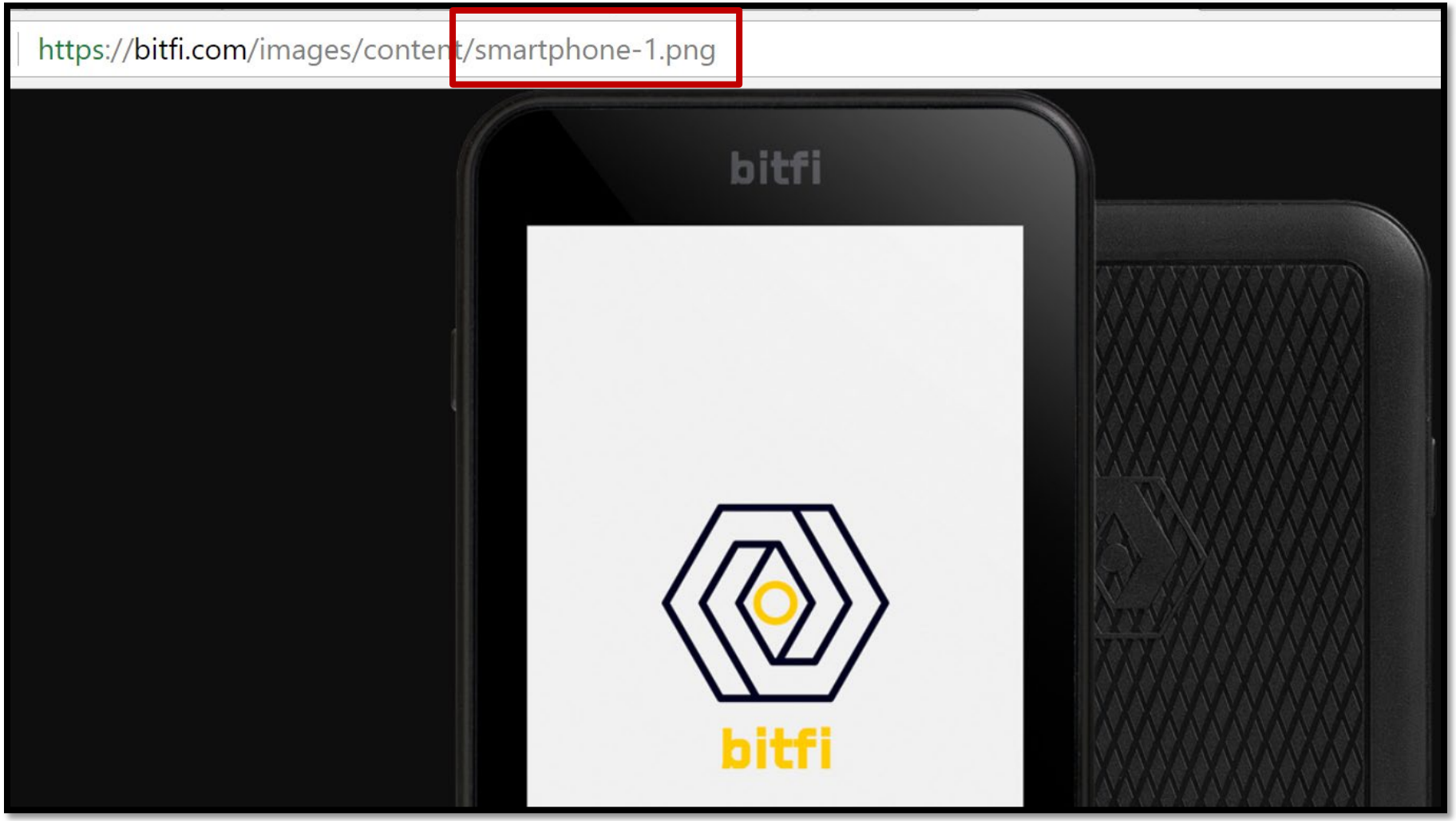
# Evidence


bitfi
Li-ion Battery
Model:GB/T18287-2013
Charging Voltage Limited:4.35V
Nominal Voltage:3.8V
Capacity:1300mAh/4.94Wh
MADE IN CHINA

# Evidence



# Evidence


https://bitfi.com/images/content/smartphone-1.png
bitfi
bitfi

# Evidence

## Key Functions

1. Power Key： On shutdown state ,long press the power key and the system will enter the process of Start-up; on boot state， long press the power key and the system will exit to show shutdown information; on boot state， short press will lock the interface.

2.  :This is returning key, while if short touch, the phone will return back to the previous interface.

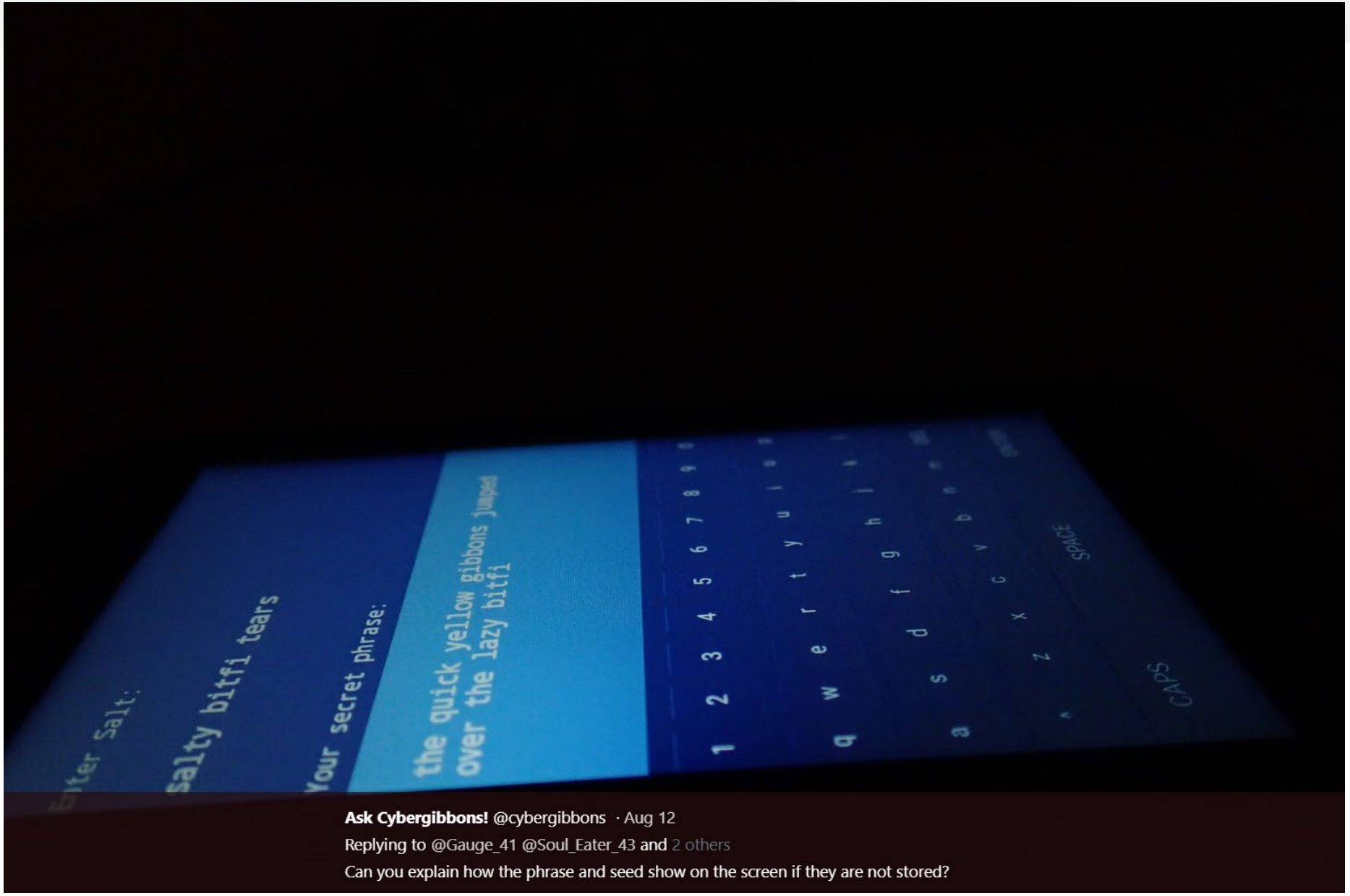
**John McAfee**

@officialmcafee

Follow

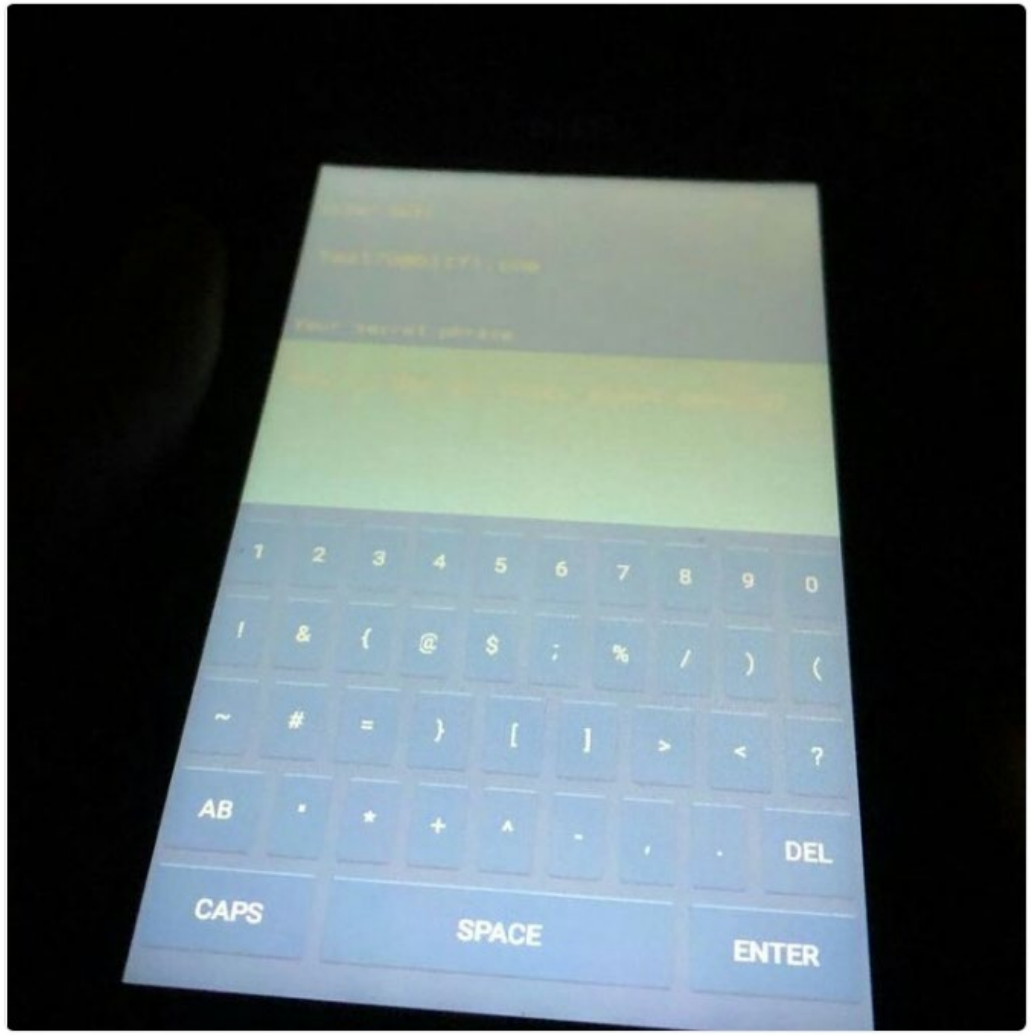
Now people are asking “can’t someone just look over your shoulder and see what phrase you are typing”? No.The Bitfi wallet has a screen with an extremely narrow viewing angle and they won’t be able to see anything. Try it. Bitfi.com

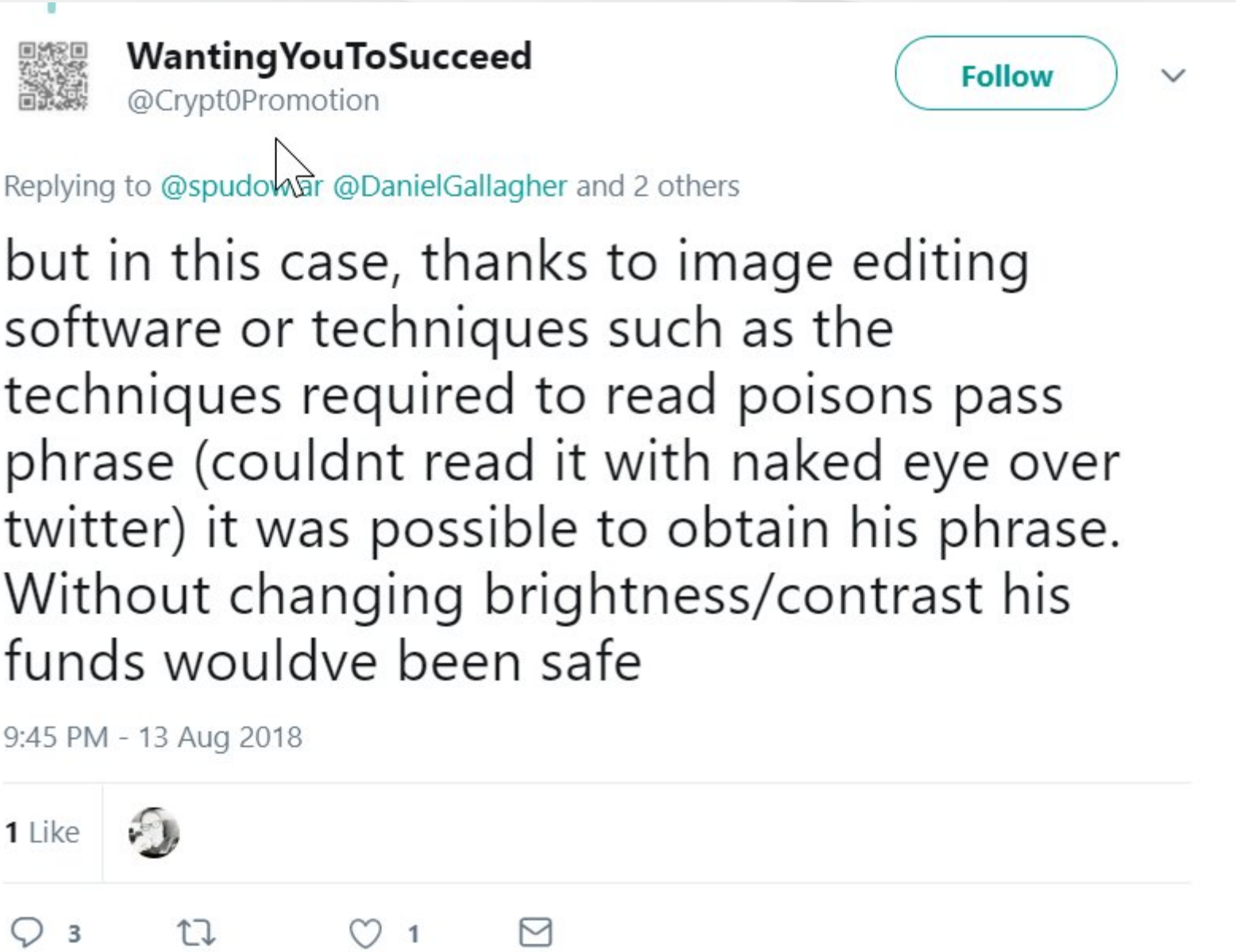
8:46 PM - 25 Jul 2018


Enter Salt:
salty bitfi tears
Your secret phrase:
the quick yellow gibbons jumped
over the lazy bitfi
Ask Cybergibbons! @cybergibbons · Aug 12
Replying to @Gauge_41 @Soul_Eater_43 and 2 others
Can you explain how the phrase and seed show on the screen if they are not stored?

**Ask Cybergibbons!**
@cybergibbons

So yesterday @p0isoNz tweeted a picture to demonstrate the "narrow viewing angle" of the Bitfi.




WantingYouToSucceed
@Crypt0Promotion
Follow
Replying to @spudowar @DanielGallagher and 2 others
but in this case, thanks to image editing software or techniques such as the techniques required to read poisons pass phrase (couldnt read it with naked eye over twitter) it was possible to obtain his phrase. Without changing brightness/contrast his funds wouldve been safe
9:45 PM - 13 Aug 2018
1 Like
3
1

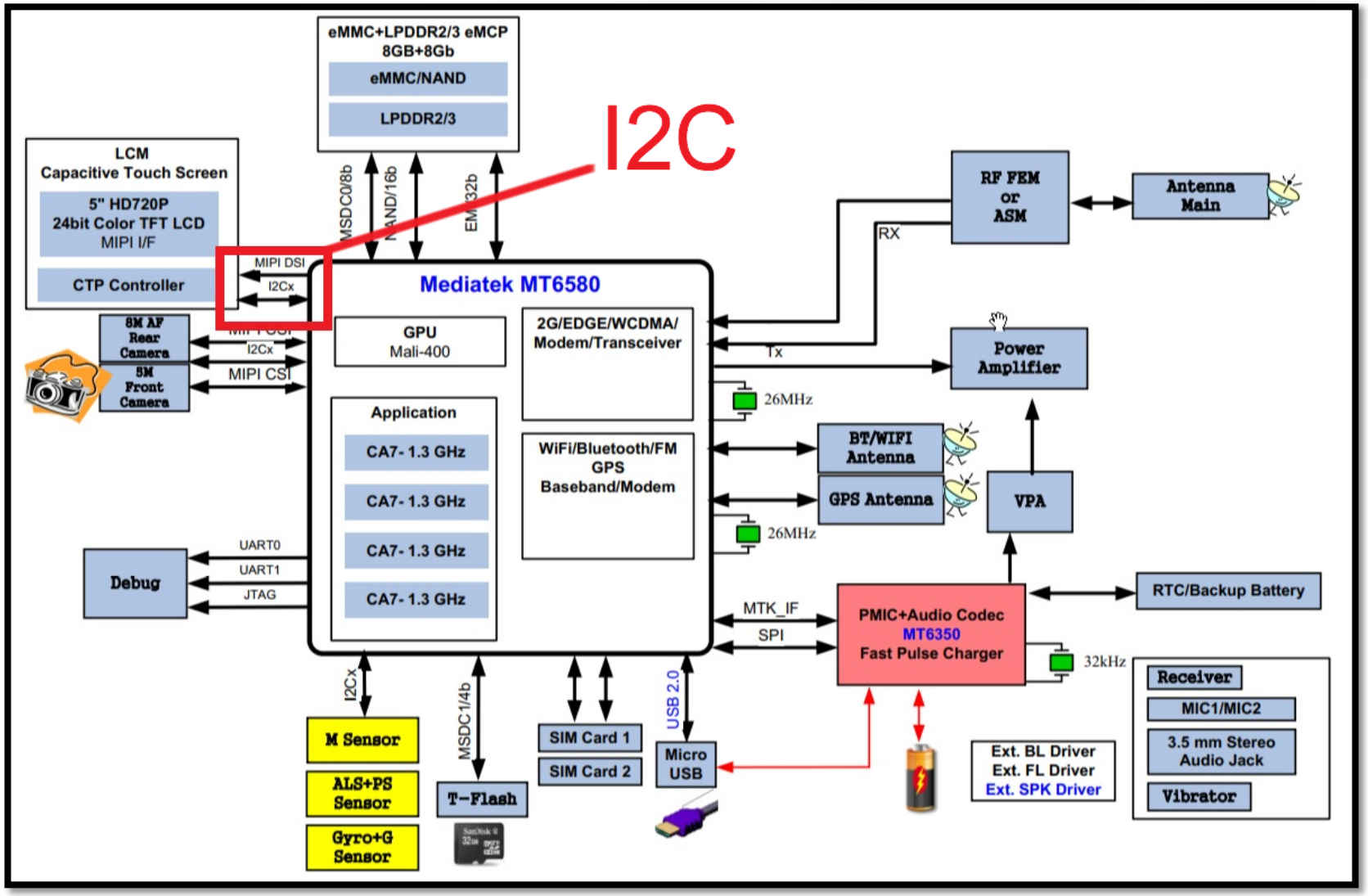
# ~~Unhackable!~~ Uncontrollable!

# Hacking the Bitfi, method 1
# Intercept I2C

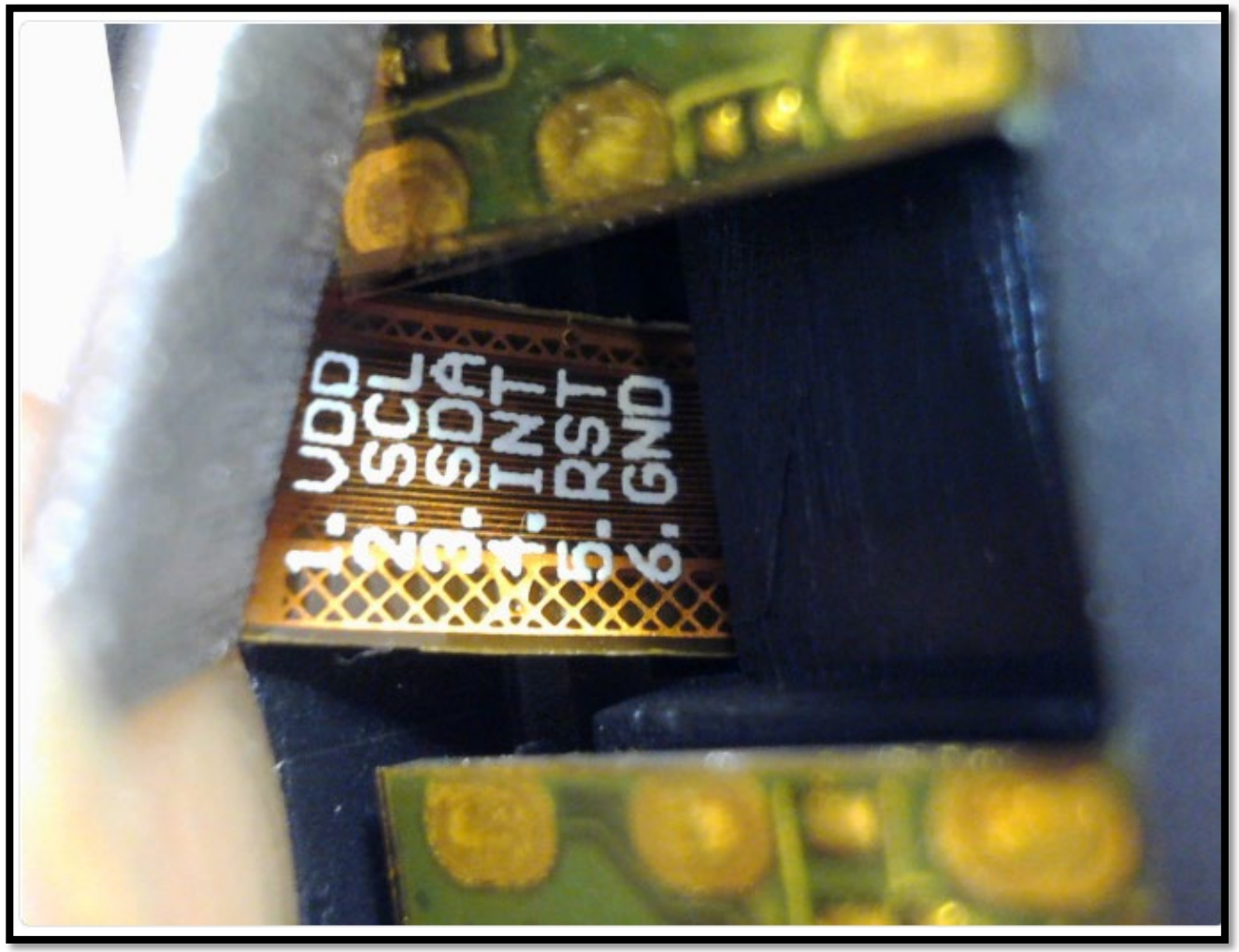
**Credit:**
**@cybergibbons**
**@ryancdotorg**
**@saleemras1d**
**and others**

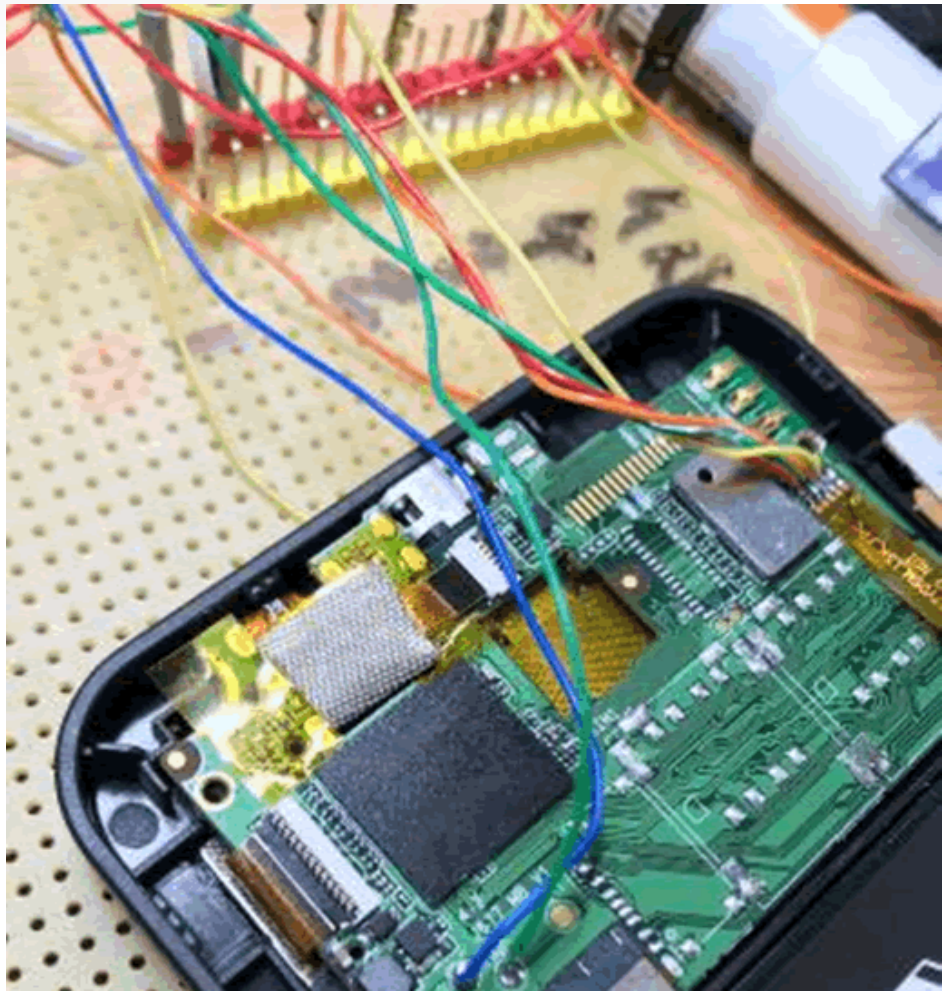
# Supply Chain Issues

# Hacking the Bitfi



# Hacking the Bitfi

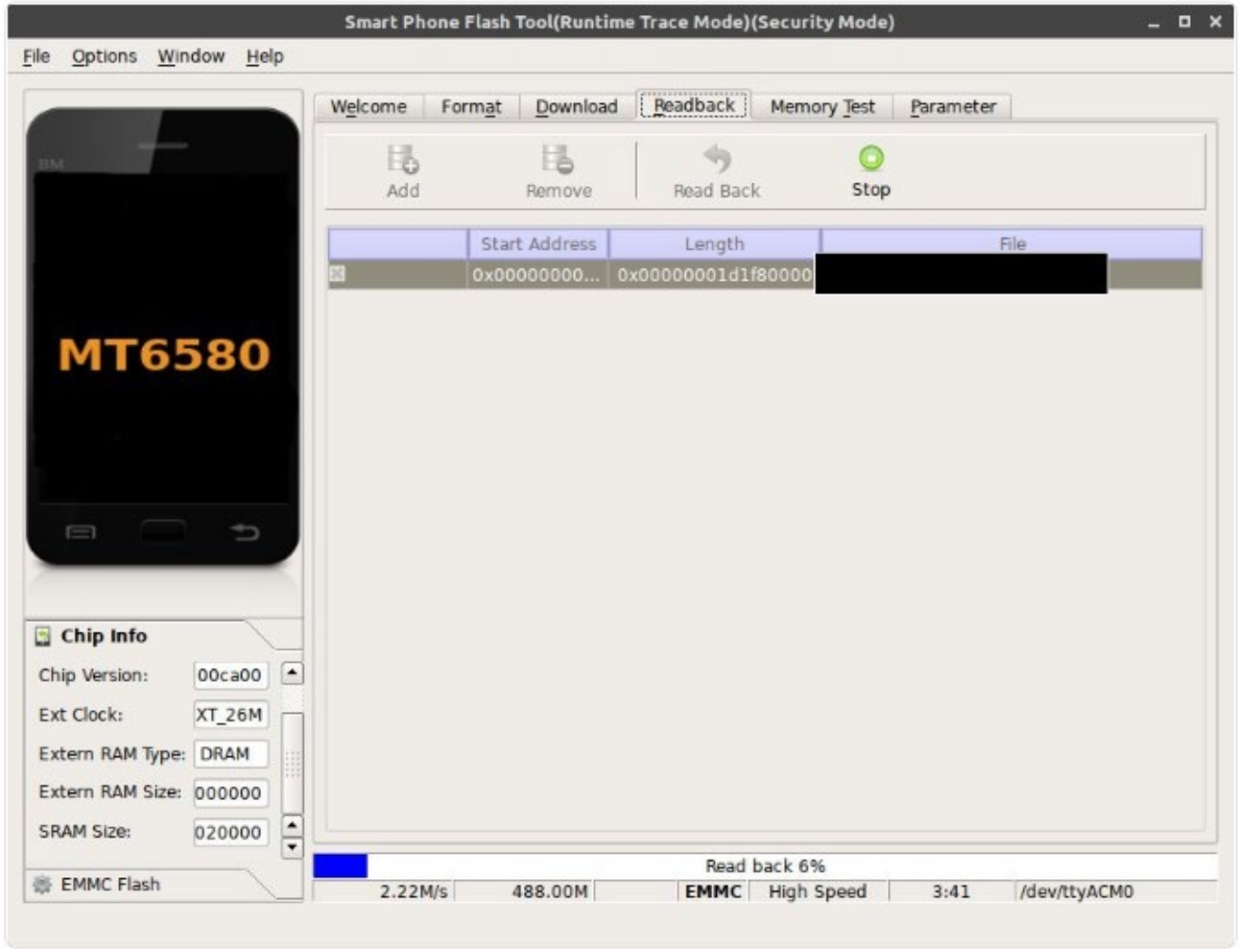


# Hacking the Bitfi, method 2
# Unlocked bootloader, root over USB

# Hacking the Bitfi

Which we read out from the open bootloader.



# Hacking the Bitfi

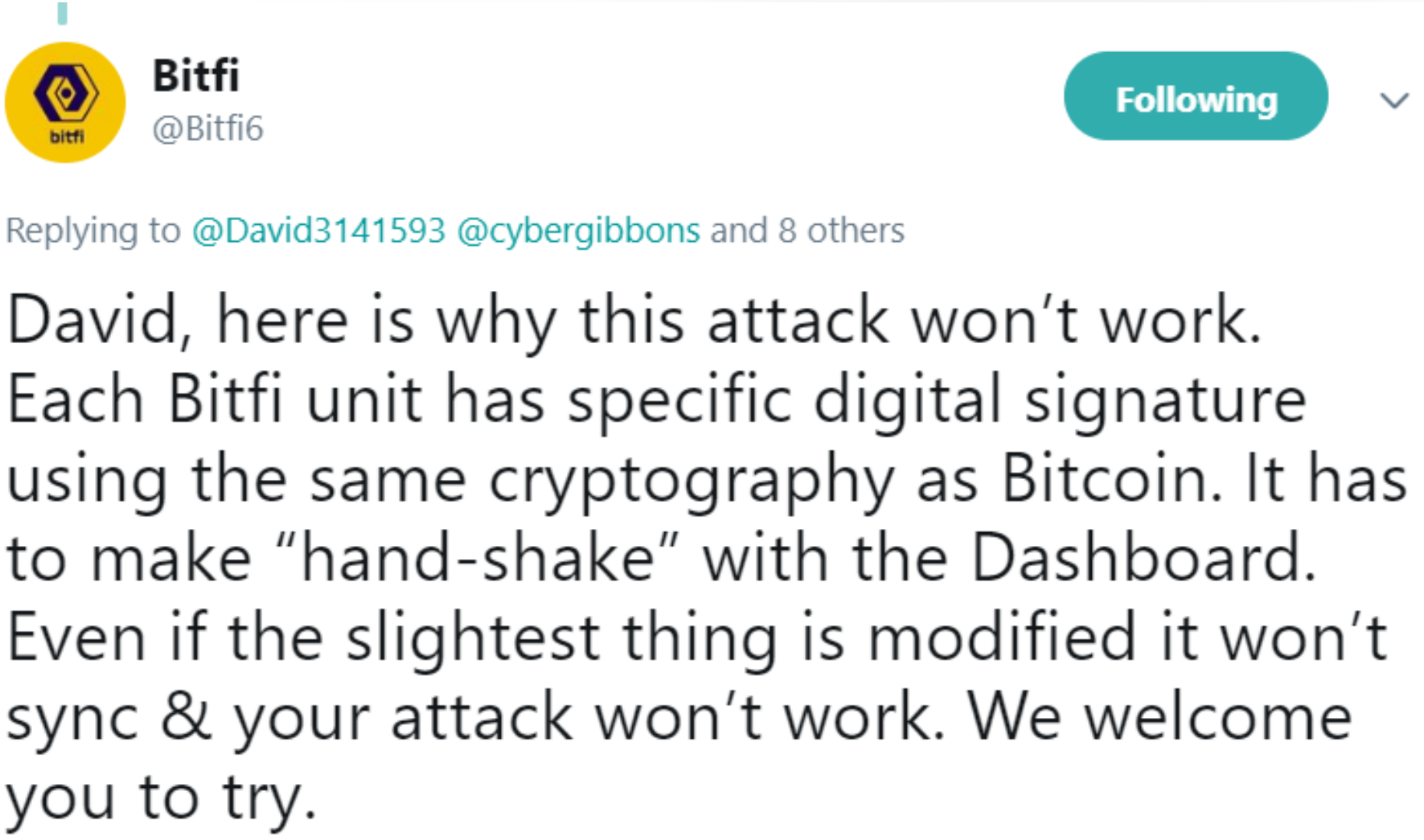
Allowing us to dump the file system.

```
root@ubuntu:/media/sf_tests/bitfi# partx --show ROM_0
NR     START       END   SECTORS SIZE NAME         UUID
 1      1024      7167      6144   3M proinfo     f57ad330-39c2-4488-9bb0-00cb43c9ccd4
 2      7168     17407     10240   5M nvram       fe686d97-3544-4a41-be21-167e25b61b6f
 3     17408     37887     20480  10M protect1    1cb143a8-b1a8-4b57-b251-945c5119e8fe
 4     37888     58367     20480  10M protect2    3b9e343b-cdc8-4d7f-9fa6-b6812e50ab62
 5     58368     58879       512 256K seccfg      5f6a2c79-6617-4b85-ac02-c2975a14d2d7
 6     58880     59647       768 384K lk          4ae2050b-5db5-4ff7-aad3-5730534be63d
 7     59648     60415       768 384K lk2         1f9b0939-e16b-4bc9-a5bc-dc2ee969d801
 8     60416     93183     32768  16M boot        d722c721-0dee-4cb8-8a83-2c63cd1393c7
 9     93184    125951     32768  16M recovery    e02179a8-ceb5-48a9-8831-4f1c9c5a8695
10    125952    126975      1024 512K para        84b09a81-fad2-41ac-890e-407c24975e74
11    126976    143359     16384   8M logo        e8f0a5ef-8d1b-42ea-9c2a-835cd77de363
12    143360    176127     32768  16M odmdtbo     d5f0e175-a6e1-4db7-94c0-f82ad032950b
13    176128    196607     20480  10M expdb       1d9056e1-e139-4fca-8c0b-b75fd74d81c6
14    196608    786431    589824 288M vendor      7792210b-b6a8-45d5-ad91-3361ed14c608
15    786432    788479      2048   1M frp         138a6db9-1032-451d-91e9-0fa38ff94fbb
16    788480    798719     10240   5M tee1        756d934c-50e3-4c91-af46-02d824169ca7
17    798720    808959     10240   5M tee2        a3f3c267-5521-42dd-a724-3bdec20c7c6f
18    808960    874495     65536  32M nvdata      8c68cd2a-ccc9-4c5d-8b57-34ae9b2dd481
19    874496    950271     75776  37M metadata    6a5cebf8-54a7-4b89-8d1d-c5eb140b095b
20    950272    954367      4096   2M oemkeystore a0d65bf8-e8de-4107-9434-1d318c843d37
21    954368    966655     12288   6M secro       46f0c0bb-f227-4eb6-b82f-66408e13e36d
22    966656    983039     16384   8M keystore    fbc2c131-6392-4217-b51e-548a6edb03d0
23    983040   3489791   2506752 1.2G system      e195a981-e285-4734-8025-ec323e9589d9
24   3489792   3719167    229376 112M cache       e29052f8-5d3a-4e97-adb5-5f312ce6610a
25   3719168  15236095  11516928 5.5G userdata    9c3cabd7-a35d-4b45-8c57-b80775426b35
26  15236096  15268863     32768  16M flashinfo   e7099731-95a6-45a6-a1e5-1b6aba032cf1
```


bitfi
Li-ion Battery
Model:GB/T18287-2013
Charging Voltage Limited:4.35V
Nominal Voltage:3.8V
Capacity:1300mAh/4.94Wh
MADE IN CHINA

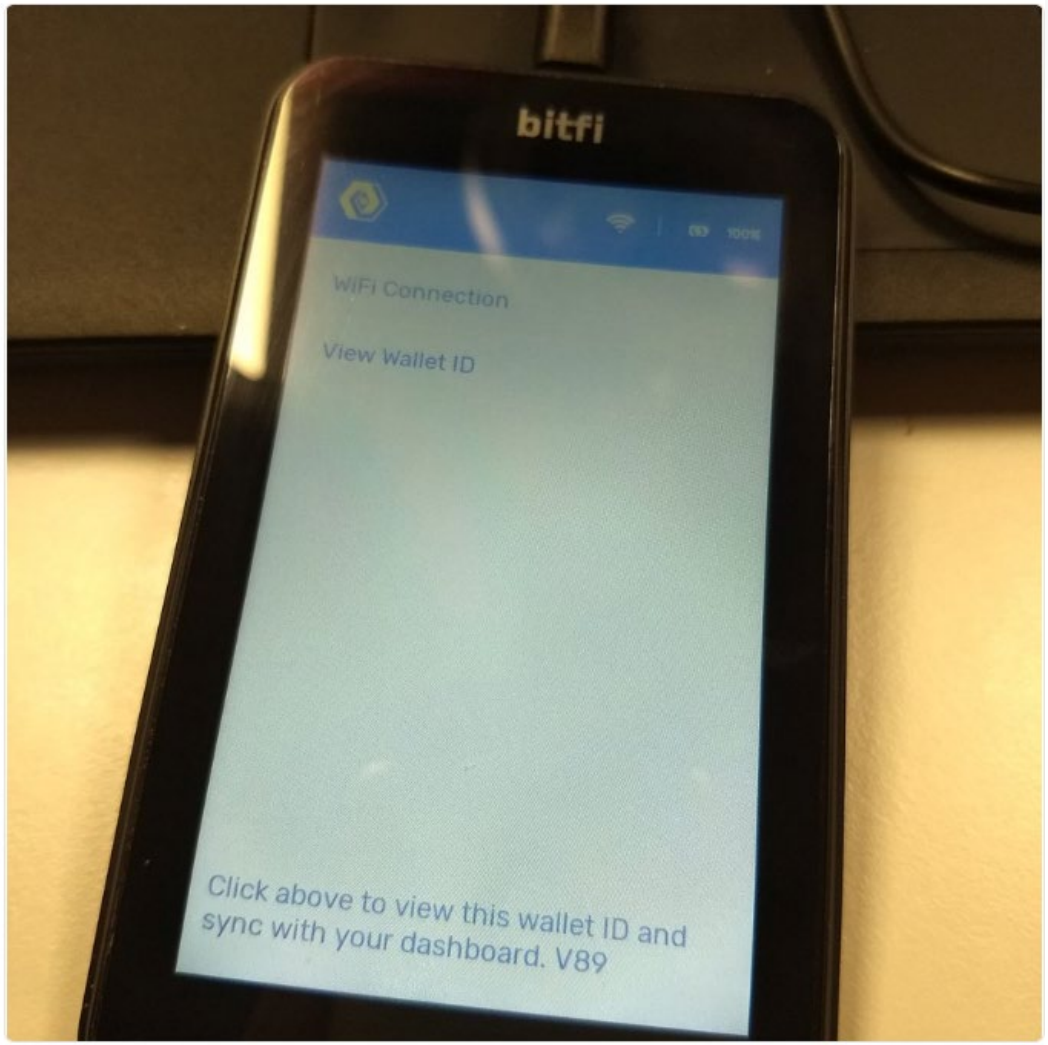
# Hacking the Bitfi, method 3
# MITM transaction

# Hacking the Bitfi



The rules for claiming the bounty :

- The firmware of the Bitfi device is modified
- After the firmware is modified the device still needs to connect to the Bitfi Dashboard
- The device then should be able to transmit either private keys or the users secret phrase to a third party while still functioning normally with the Bitfi Dashboard


bitfi
WiFi Connection
View Wallet ID
Click above to view this wallet ID and sync with your dashboard. V89

The two Bitfi/Rokits apps are running, as expected.

```
/ # whoami
root
/ # ps -A | grep rokit
u0_a57        1114   354 1073144  85480 SyS_epoll_wait aceab1b8 S com.rokits.noxadmin
u0_a58       10159   354 1153432 127772 SyS_epoll_wait aceab1b8 S app.rokits.android
```

What is that IP?

```
/ # netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.12.161:54832    40.69.155.7:https       ESTABLISHED
tcp6       0      0 ::ffff:192.168.12.:2323 ubuntu:42952            ESTABLISHED
```

It's Bitfi of course!

```
/ # ping bitfi.com
PING bitfi.com (40.69.155.7) 56(84) bytes of data.
```

# Oh? What's that? Syncing with the dashboard and being able to intercept traffic.

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Ex |
|---|---|---|---|---|---|---|---|---|---|
| 1 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 558 | XML | as |
| 2 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 3 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 4 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 5 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 6 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 7 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 8 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 9 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 10 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 11 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 12 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |
| 13 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | | 200 | 565 | XML | as |

Request | Response

Raw | Params | Headers | Hex | XML

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetCurrentSMSToken xmlns="https://bitfi.com/dataservices/">
      <noxsig>HAmHYiZiIVQhuxIwzg6yk5btX2gDme+5uwdDnolfA+p2MCdhVF5rn7Q5w+Z7yxFb0UjuaunY3x3qd0BVUJLm40M=</noxsig>
      <noxmsg>17iJ5Hv7dCdm4HAMx9sv6PyZ1m825j1hF65e583560-ce4a-4fb8-9569-e005a9dd9d39</noxmsg>
      <GCMToken>6219cb85-23f2-4143-9eca-e507a5b5a367</GCMToken>
      <GCMUser>6219CB</GCMUser>
    </GetCurrentSMSToken>
  </soap:Body>
</soap:Envelope>
```

# Hacking the Bitfi

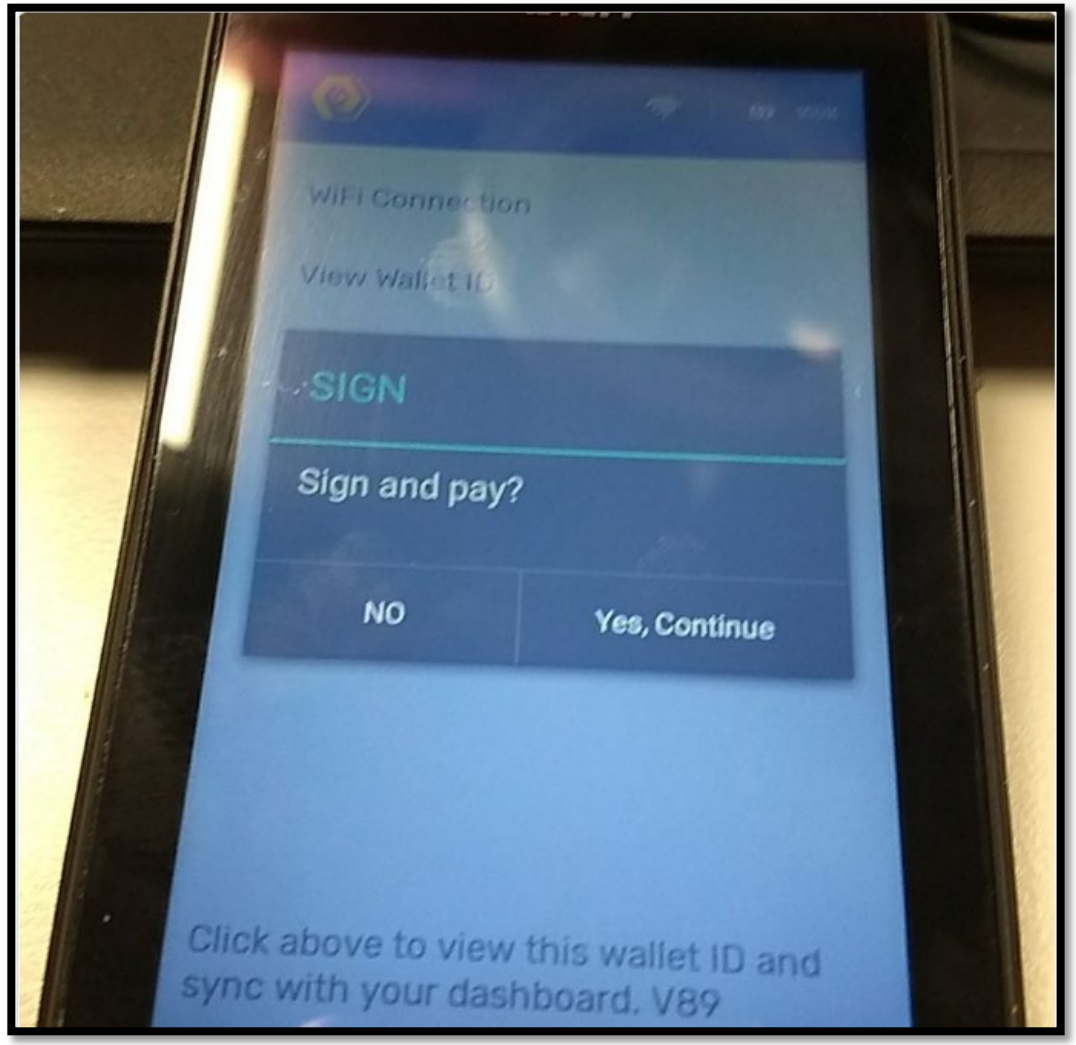
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2699 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | 200 | 2533 | XML | asmx |
| 2700 | https://bitfi.com | POST | /Nox/Site/NOXWSSS.asmx | ✓ | 200 | 642 | XML | asmx |

Request | Response

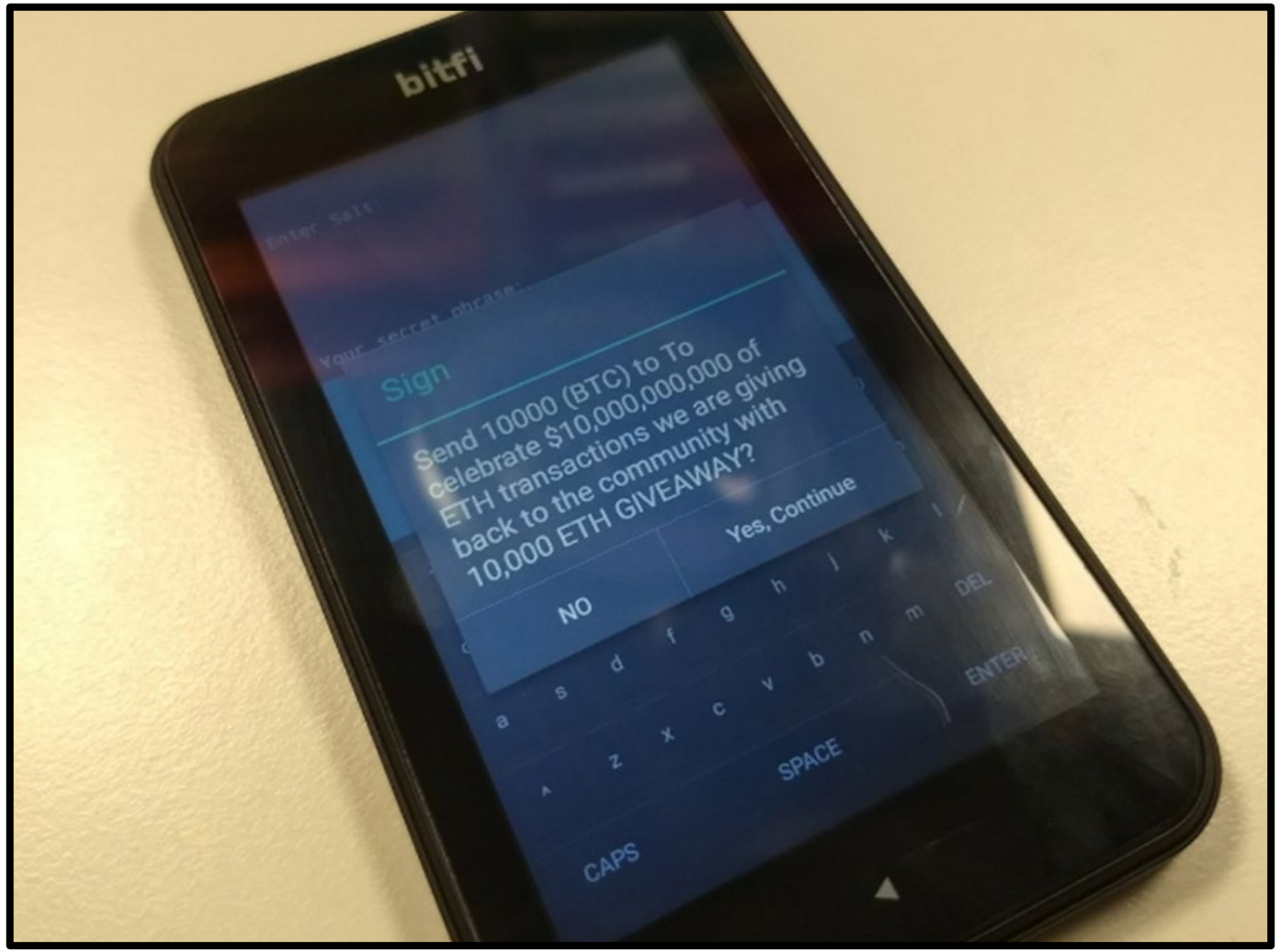
Raw | Params | Headers | Hex | XML

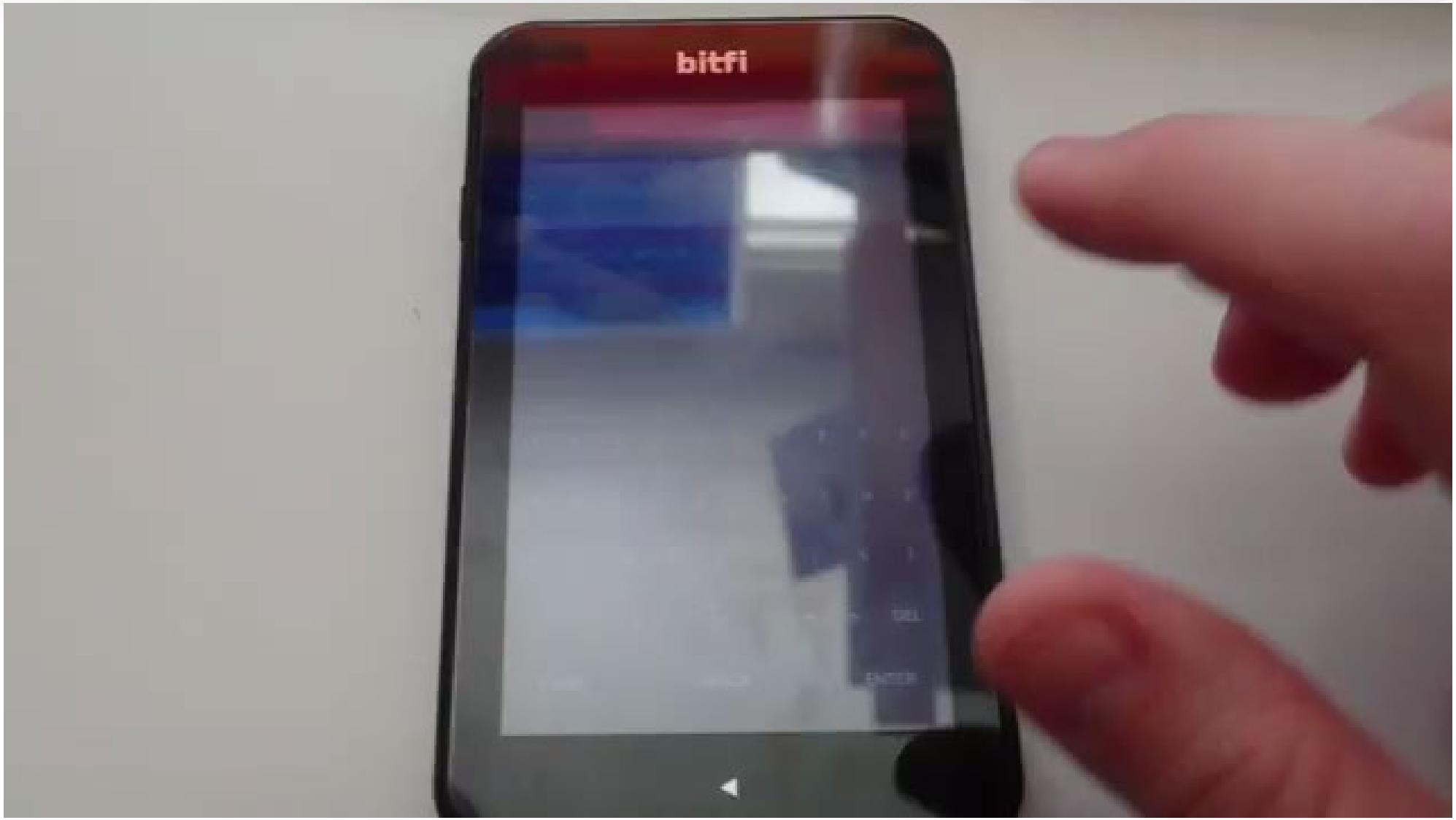
```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap
  <soap:Body>
    <SubmitTxnResponse xmlns="https://bitfi.com/dataservices/">
      <noxsig>G9QNP/Lw1uGFnF9uio/xIYjErYOV30Njl9txEsRboOtYXLN0PcccS2/yXNtYeFrvIDffSm1wfk7VcDpXs9/TxM0=</noxsig>
      <noxmsg>17iJ5Hv7dCdm4HAMx9sv6PyZ1m825j1hF6a070c1da-f7b6-4f65-8c51-91c785d1c2dc</noxmsg>
      <LineID>57beb099-2f03-41b6-9f88-354ea5beef70</LineID>

<TxnHex>0200000001d05e1cea54f2db94cacb6e15bfe0ffe92758326a0d3b006553e1b1f664a9d4de000000008a47304402207e3d3ae33c4ebfb218327b
f9251a63aead2b45c82f974c29ae187c642bb5d985eea9adf506b4749e149cb38e8d1b5d9cfd692867e56e58d6aab91b27a6f94845680071ffffffff01fe
    </SubmitTxnResponse>
  </soap:Body>
</soap:Envelope>
```

# Hacking the Bitfi



# Hacking the Bitfi




bitfi

# Hacking the Bitfi, method 4
# Cold Boot


Binary initialized
Waiting for unbootable device...

UPDATE: THIS BOUNTY HAS BEEN DISCONTINUED. BITFI WILL ANNOUNCE A NEW BOUNTY PROGRAM THROUGH HACKER ONE

However, the keys do stay in RAM for a brief period of time.

So if someone does a memory extraction very quickly after device is used it is theoretically possible but not a real world attack

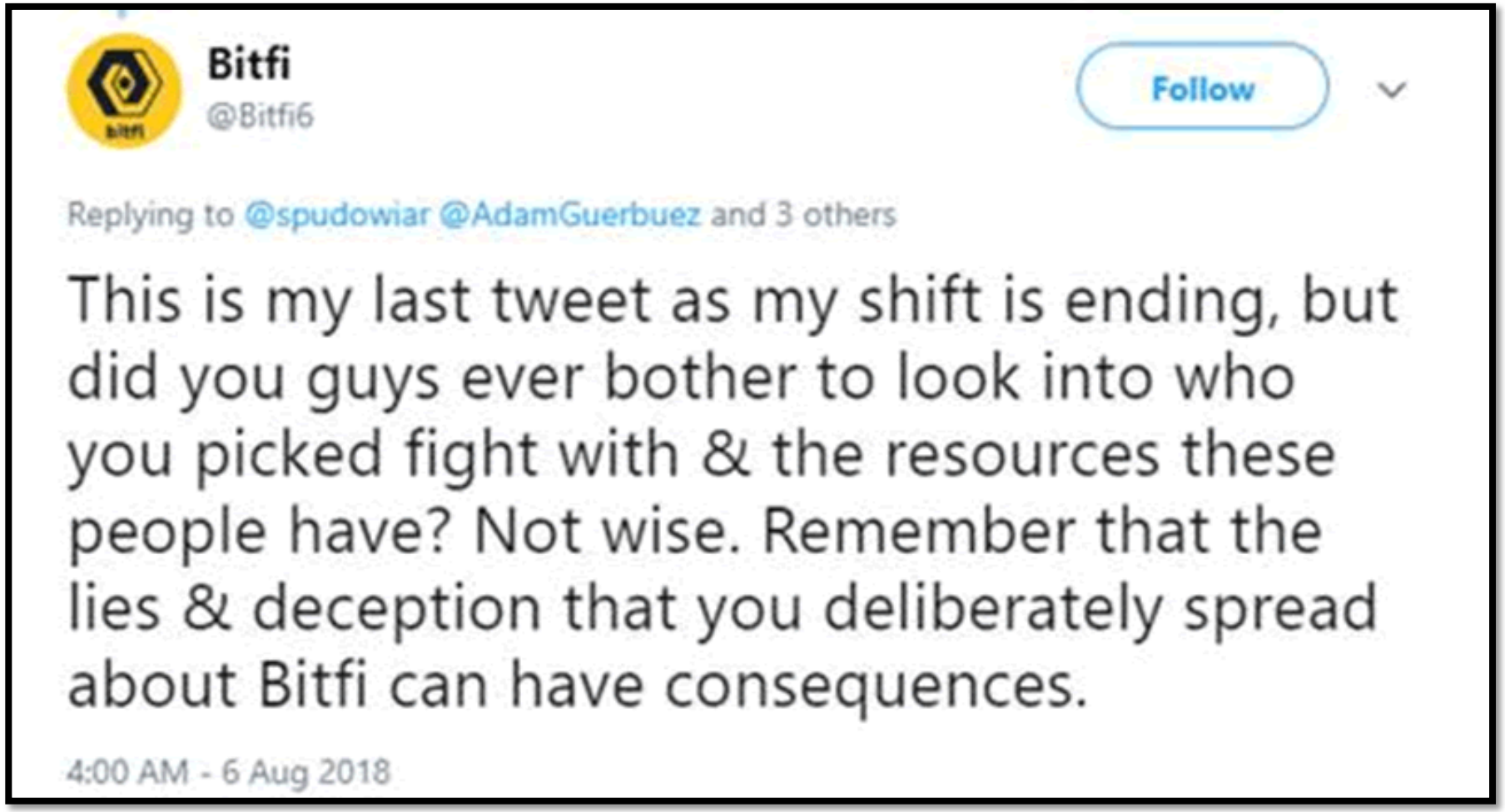
Compare that to any other wallet that permanently stores your private keys


4:56 pm

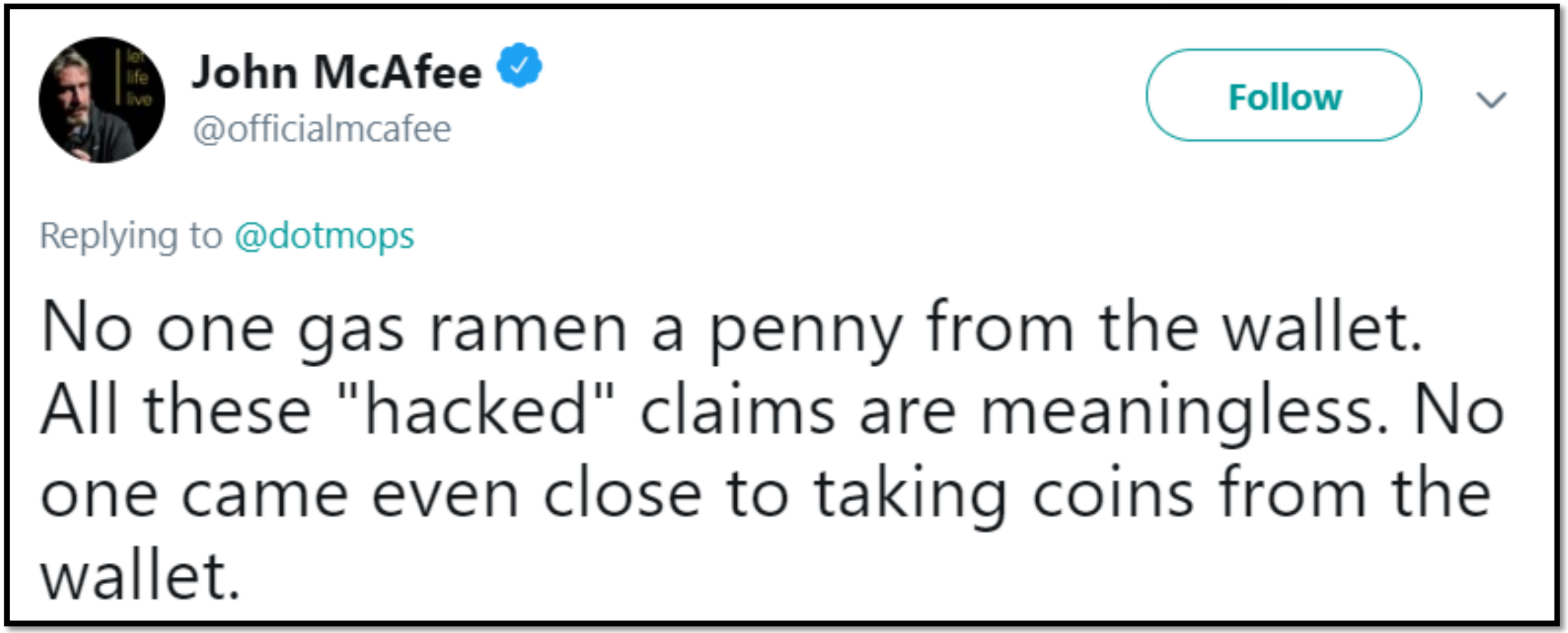
We think that if the guy was able to retrieve the private key from the device or something like that, it would have to have been done on a rooted device. But if you root a device, you have to restart it, and when you restart it, it wipes the RAM clean.

# “When you restart it, it wipes the RAM clean”

# Interesting PR



# Gas Ramen


John McAfee
@officialmcafee
Follow
Replying to @dotmops
No one gas ramen a penny from the wallet. All these "hacked" claims are meaningless. No one came even close to taking coins from the wallet.

# No, we don't want a meeting…

# Pwnie Awards, Las Vegas 2018

# Pwnie!


# Pwnie Awards, Las Vegas 2019

# Pwnie Again!

# Advice

- Don’t ever claim a product is unhackable
- Select your base hardware carefully
- TEE, entropy source, secure storage, lockable bootloader, no CRP bypass, toolchain access etc
- Get firmware & software developed by devs who can demonstrate really good security expertise (e.g. OWASP, good SDLC etc)
- Get third party advice REALLY early on, before you…

# Advice

- DO
- Set up a bug bounty programme

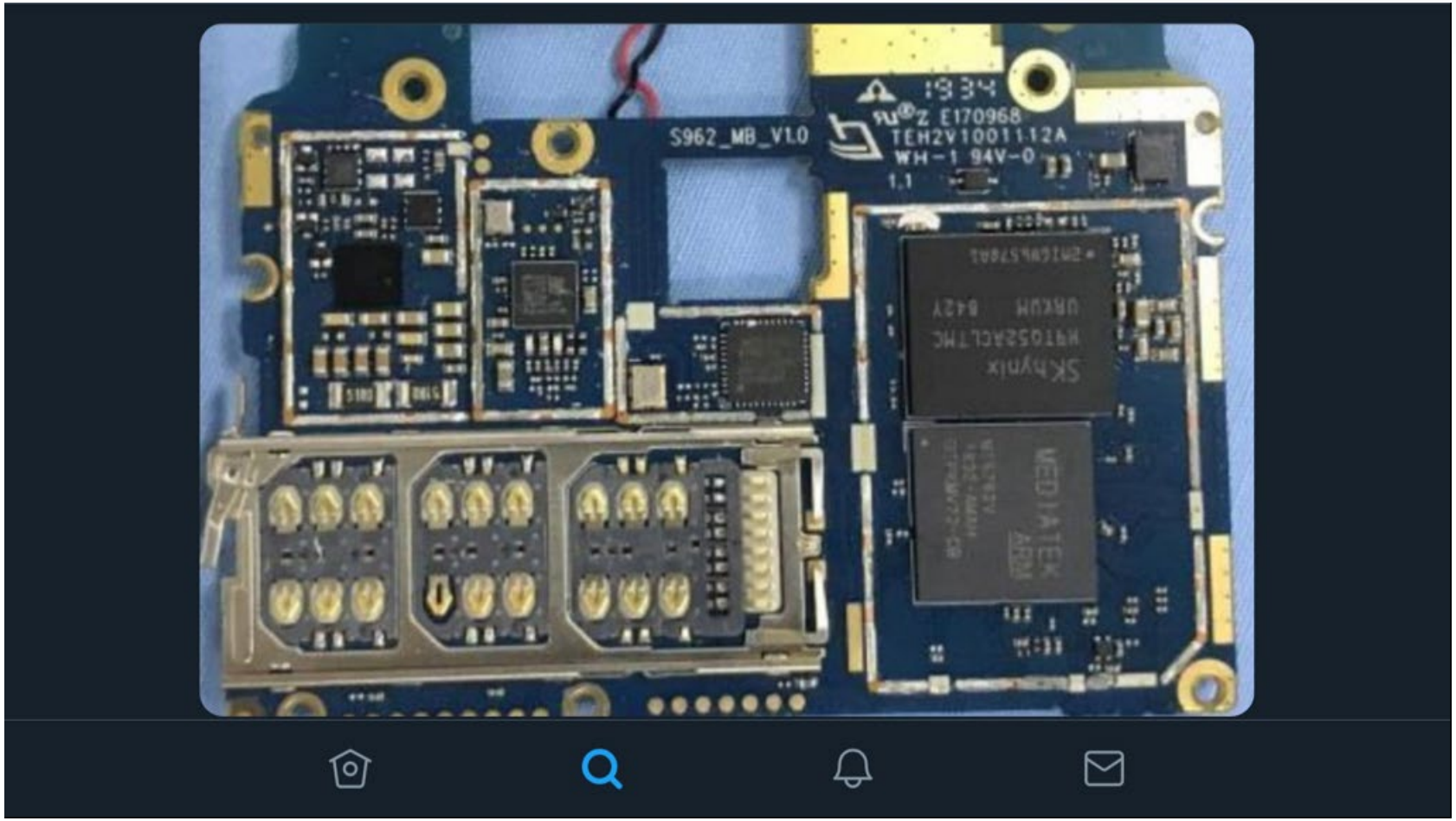
- DON’T
- Rely on it as your only source of security evaluation
- - No substitute for SDLC, pen testing, hardware security review

# Did no-one learn?

# Er – you can have 1BTC if you hack it??


Alex Humes @HumesAlexander · 16h
The most awaited CryptoDATA #competition has officially started!
Do you think you found a way to hack our #IMPulse K1? We highly doubt that, but we are ready to offer you $ 1.000.000 if you prove us wrong.
#karatbars $kbc #hackit #nonhackable #blockchain #vobp
HACK
TOURNAMENT
PRIZE: $1.000.000
www.impulse.technology

# MediaTek MTK6762




Alex Humes @HumesAlexander · 16h
The most awaited CryptoDATA #competition has officially started!
Do you think you found a way to hack our #IMPulse K1? We highly doubt that, but we are ready to offer you $ 1.000.000 if you prove us wrong.
#karatbars $kbc #hackit #nonhackable #blockchain #vobp
HACK
TOURNAMENT
PRIZE: $1.000.000
www.impulse.technology

**Ryan Castellucci**
@ryancdotorg

Following

Much of hacking is about understanding systems better than those who built them, and using that knowledge to do what is supposed to be "impossible".

# Security researchers are generally well intentioned