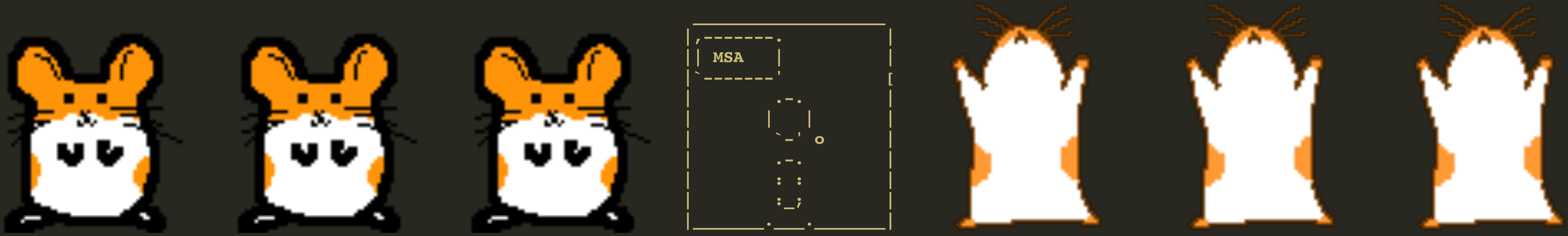
(Security) Research to Improve the World

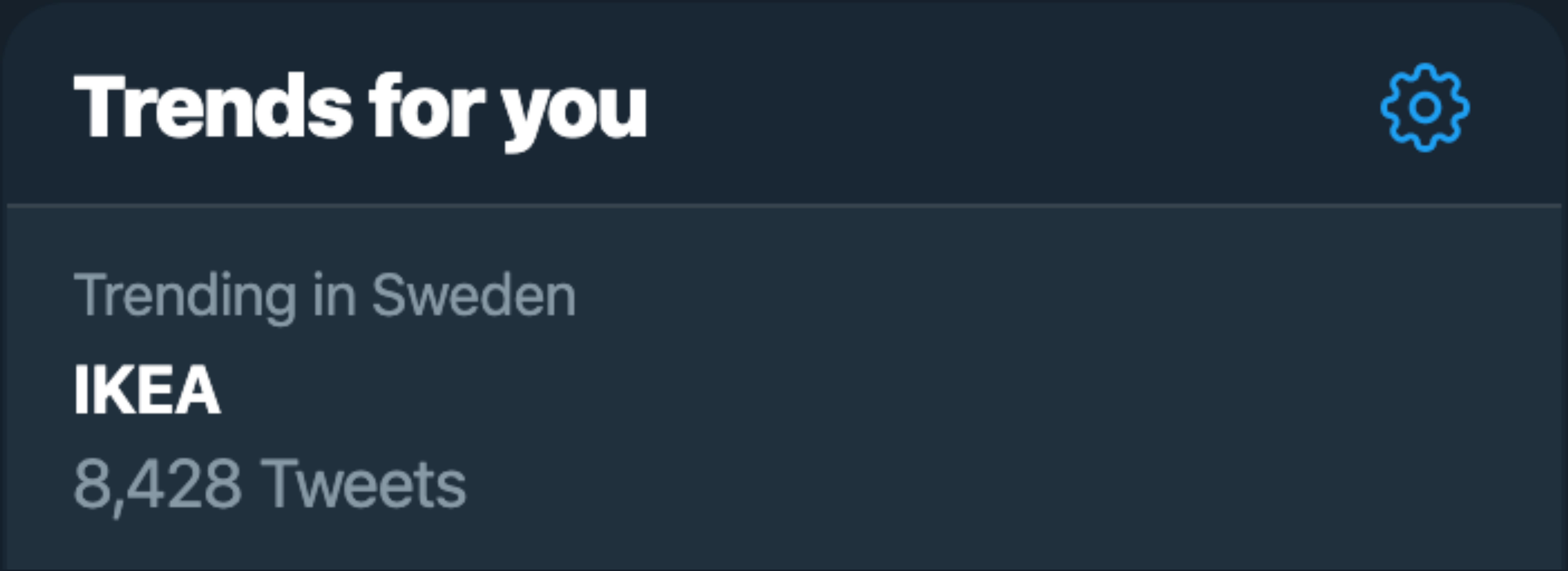
Ed Marczak
@marczak

greetz!



· MAC · SYS · ADMIN ·
GOTHENBURG

IKEA®
FAMILY
Speciella inb
Som medlem i IKE
inbjuden, t.ex. till
Bättre erbju
Som medlem i IKEA
150 bra medlemser
Mer inspiratio
Som medlem får du ma
- Hem & Idéer från IKEA
Fler förmåner
Som medlem i IKEA FAMILY
Som medlem i IKEA FA
kaffe i restaurangen alla vardag
mer.
Medlemmar får mer.
SYS · ADMIN
HENBURG · 2017



Trends for you

Trending in Sweden

IKEA

8,428 Tweets

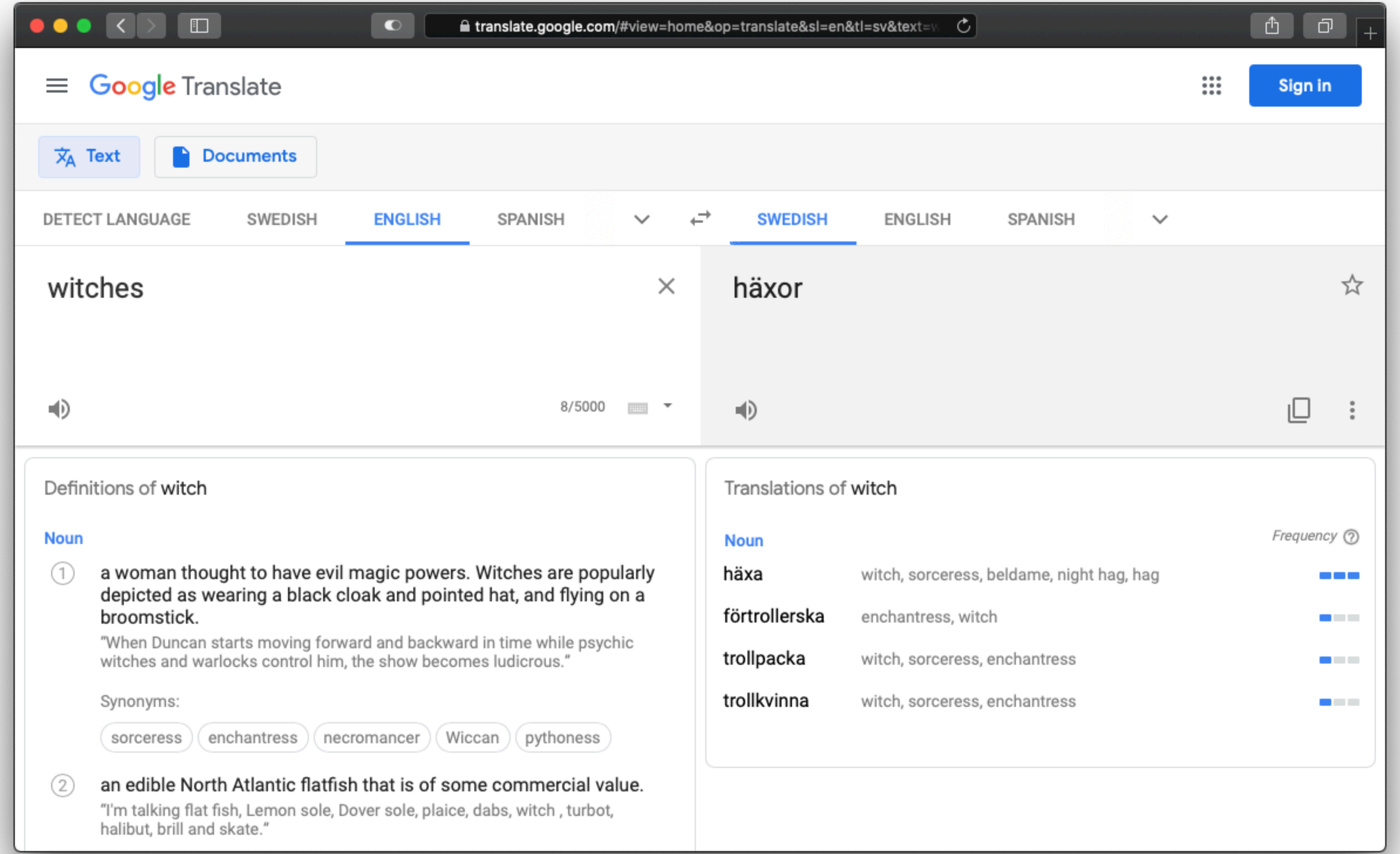
350
ABOUT ▾
RESOURCES
GET INVOLVED
LANGUAGE
Donate
Die Zukunft hängt

STOP FOSSIL FUELS.

BUILD 100% RENEWABLES.

We are standing up to the fossil fuel industry to stop all new coal, oil and gas projects and build clean energy for all.

JOIN IN



translate.google.com/#view=home&op=translate&sl=en&tl=sv&text=w

witches

häxor

Definitions of witch

Noun

1. a woman thought to have evil magic powers. Witches are popularly depicted as wearing a black cloak and pointed hat, and flying on a broomstick.
   "When Duncan starts moving forward and backward in time while psychic witches and warlocks control him, the show becomes ludicrous."

   Synonyms:
   sorceress enchantress necromancer Wiccan pythoness

2. an edible North Atlantic flatfish that is of some commercial value.
   "I'm talking flat fish, Lemon sole, Dover sole, plaice, dabs, witch , turbot, halibut, brill and skate."

Translations of witch

Noun		Frequency
häxa	witch, sorceress, beldame, night hag, hag	■■■
förtrollerska	enchantress, witch	■□□
trollpacka	witch, sorceress, enchantress	■□□
trollkvinna	witch, sorceress, enchantress	■□□

Jag är en häxa!

“Hackers enjoy the intellectual challenge of creatively overcoming limitations of software systems to achieve novel and clever outcomes.”

–Gehring, Verna (2004). The Internet in Public Life.

https://tinyurl.com/duo-research

?

Who/What is a Security Researcher?

Who/What is a Security Researcher?

Discover/defend against network attacks

Take apart malware

OR, HOW ABOUT…

Finding bugs in software/ finding new attack vectors

AppSec teams examining software source code

Research into Security

Research into Security

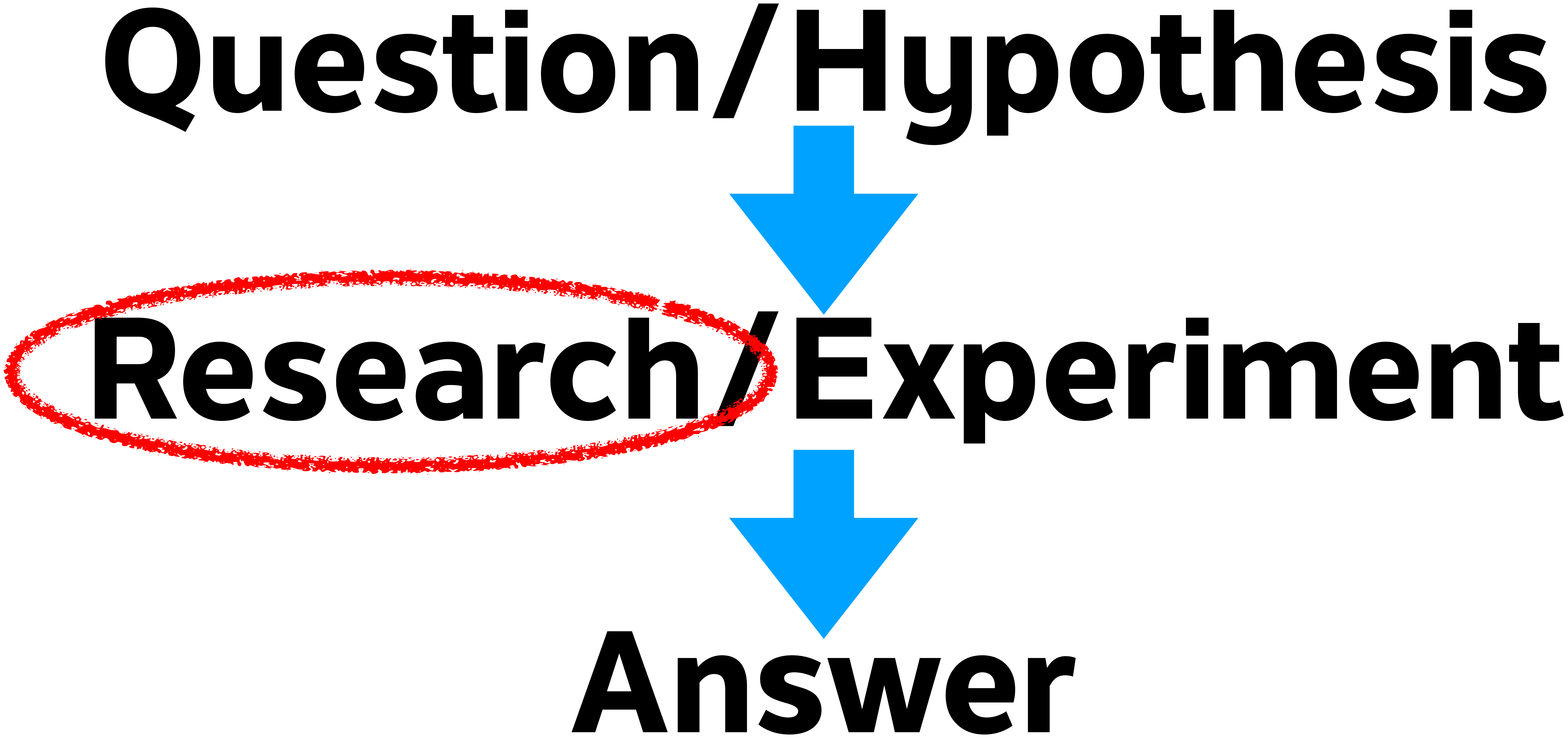
Creating new ways to secure data, devices, services, and end users.

...and breaking stuff

?

Blue Sky Research

Applied Research



Question/Hypothesis

Research/Experiment

Answer

DANGER
QUICKSAND
STAY AWAY
Caring for your safety

Derisking

It’s about the journey

Share the why, the how, the success and failures

Why have a research team?

Advance the state of your product

Help the world

Failure…can be wonderful

Post-it®
Notes/Feuillets
OPEN HERE
OUVRIR ICI
OPEN HERE
OUVRIR ICI
4 50 EA/CHAC. TOTAL 200
1 3/8 IN/PO x 1 7/8 IN/PO
34,9 mm x 47,6 mm
3M

“At that time we wanted to develop bigger, stronger, tougher adhesives. This was none of those.”

–Dr. Spencer Silver

Every team should be empowered to research

Our values

Team Trust

Communication

User-Driven Research

What do we do well?

Open mindedness

Open mindedness

- Approaches
- Procedure
- Ideas and possibilities
- Nothing is set in stone!

Empathy

Empathy

- Put yourself in the user’s place
- Actual interaction with/feedback from customers
- Make yourself customer zero
- Ensure solutions are useful and *usable*

Unconstrained Thinking

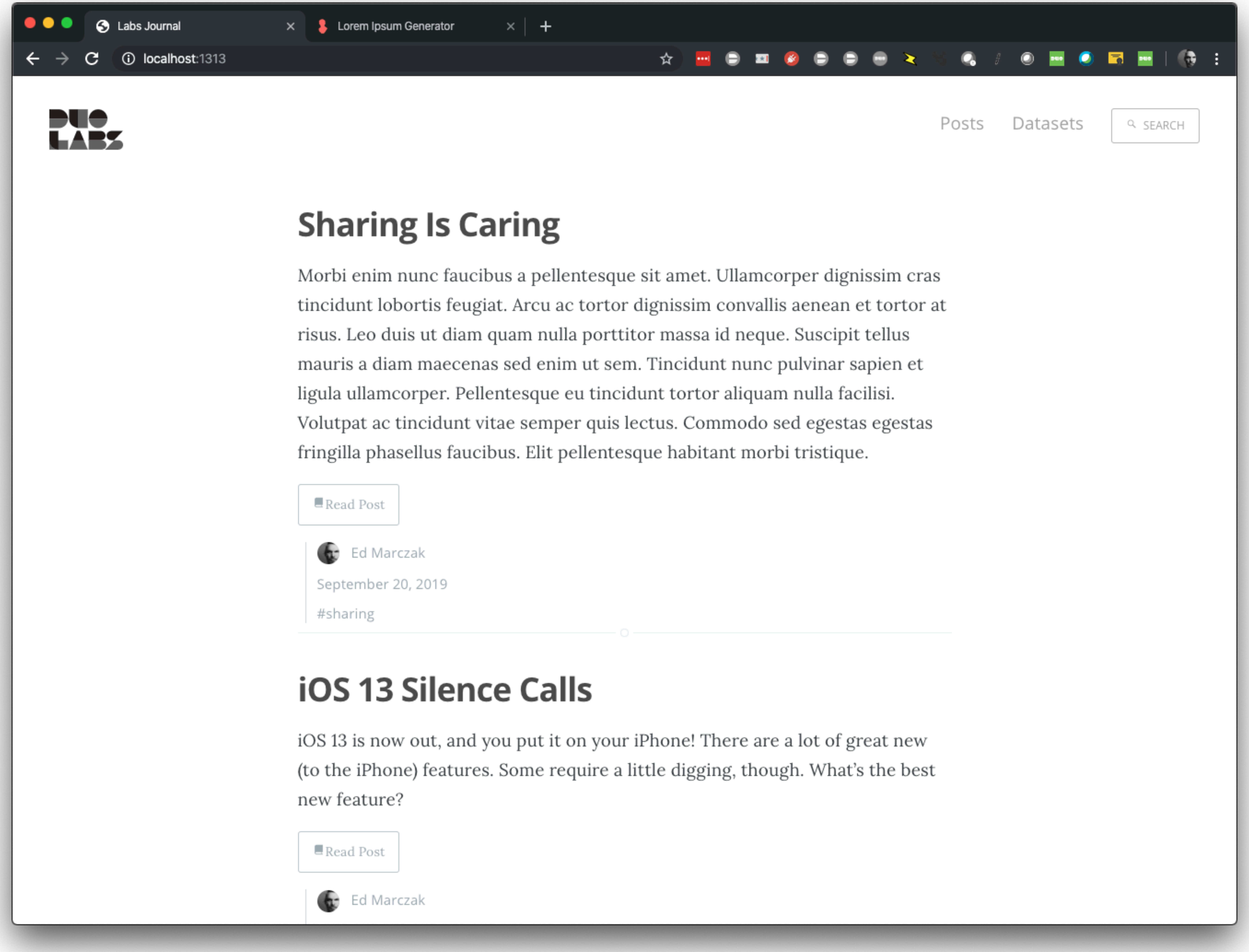
Unconstrained Thinking

- Look for the best possible solution, without bounds
- Don’t discard ideas that seem impossible
- Architect solutions that can be built on

Openly sharing our findings

Openly sharing our findings

- Internal: Journal
- External: Duo Security blog, Duo Labs blog and “Tech Notes”



Sharing Is Caring

Morbi enim nunc faucibus a pellentesque sit amet. Ullamcorper dignissim cras tincidunt lobortis feugiat. Arcu ac tortor dignissim convallis aenean et tortor at risus. Leo duis ut diam quam nulla porttitor massa id neque. Suscipit tellus mauris a diam maecenas sed enim ut sem. Tincidunt nunc pulvinar sapien et ligula ullamcorper. Pellentesque eu tincidunt tortor aliquam nulla facilisi. Volutpat ac tincidunt vitae semper quis lectus. Commodo sed egestas egestas fringilla phasellus faucibus. Elit pellentesque habitant morbi tristique.

Read Post

Ed Marczak

September 20, 2019

#sharing

iOS 13 Silence Calls

iOS 13 is now out, and you put it on your iPhone! There are a lot of great new (to the iPhone) features. Some require a little digging, though. What's the best new feature?

Read Post

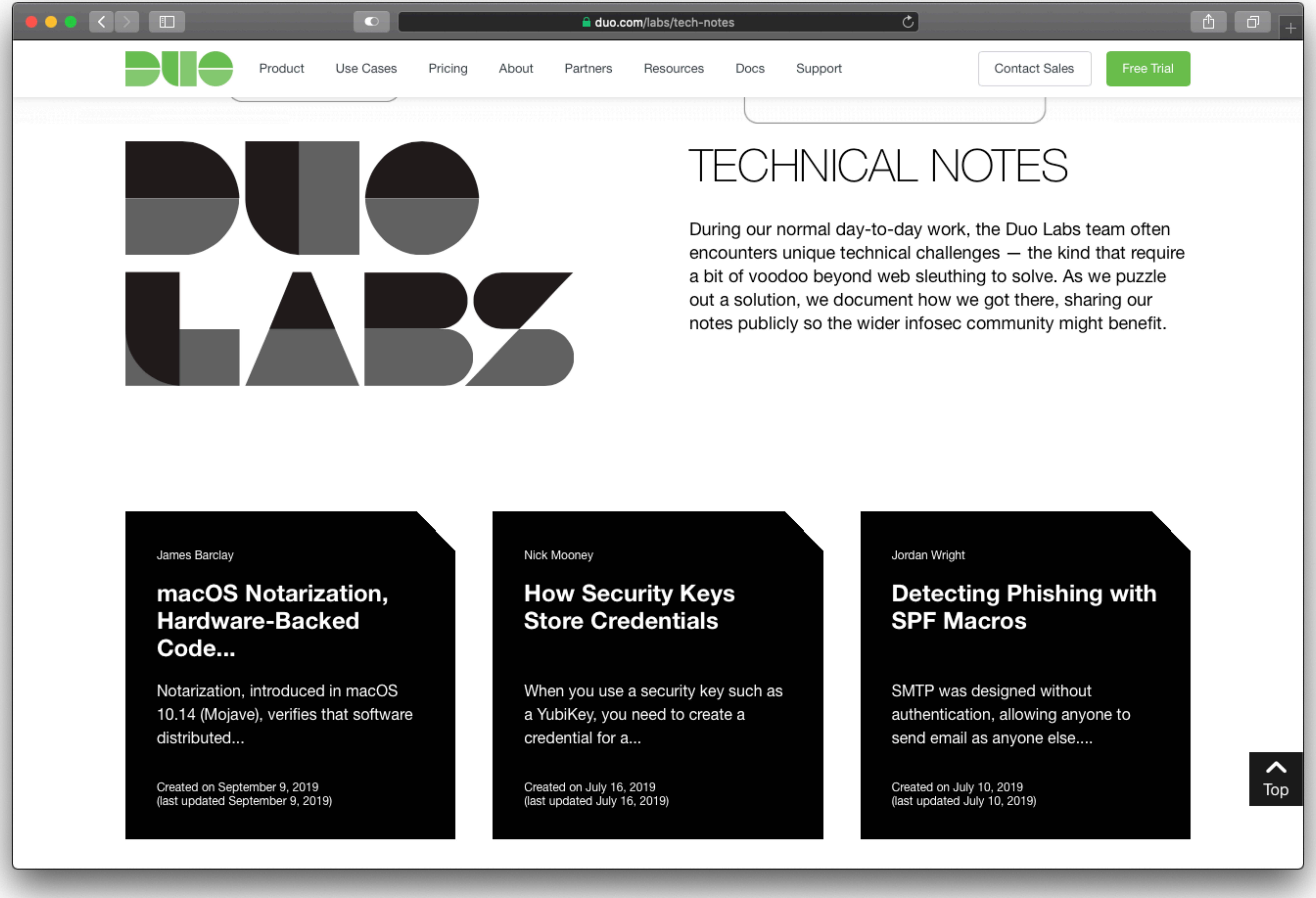
Ed Marczak

Journal: Open Source

https://github.com/duo-labs/journal

Openly sharing our findings

- Internal: Journal
- External: Duo Security blog, Duo Labs blog and “Tech Notes”



TECHNICAL NOTES

During our normal day-to-day work, the Duo Labs team often encounters unique technical challenges — the kind that require a bit of voodoo beyond web sleuthing to solve. As we puzzle out a solution, we document how we got there, sharing our notes publicly so the wider infosec community might benefit.

James Barclay

macOS Notarization, Hardware-Backed Code...

Notarization, introduced in macOS 10.14 (Mojave), verifies that software distributed...

Created on September 9, 2019
(last updated September 9, 2019)

Nick Mooney

How Security Keys Store Credentials

When you use a security key such as a YubiKey, you need to create a credential for a...

Created on July 16, 2019
(last updated July 16, 2019)

Jordan Wright

Detecting Phishing with SPF Macros

SMTP was designed without authentication, allowing anyone to send email as anyone else....

Created on July 10, 2019
(last updated July 10, 2019)

Time-boxed Analysis

Turn intangibles into a working demonstration

31
Register
Login

WebAuthn.io

A demo of the WebAuthn specification

example_username

Attestation Type: None

Authenticator Type: Unspecified

What is WebAuthn?

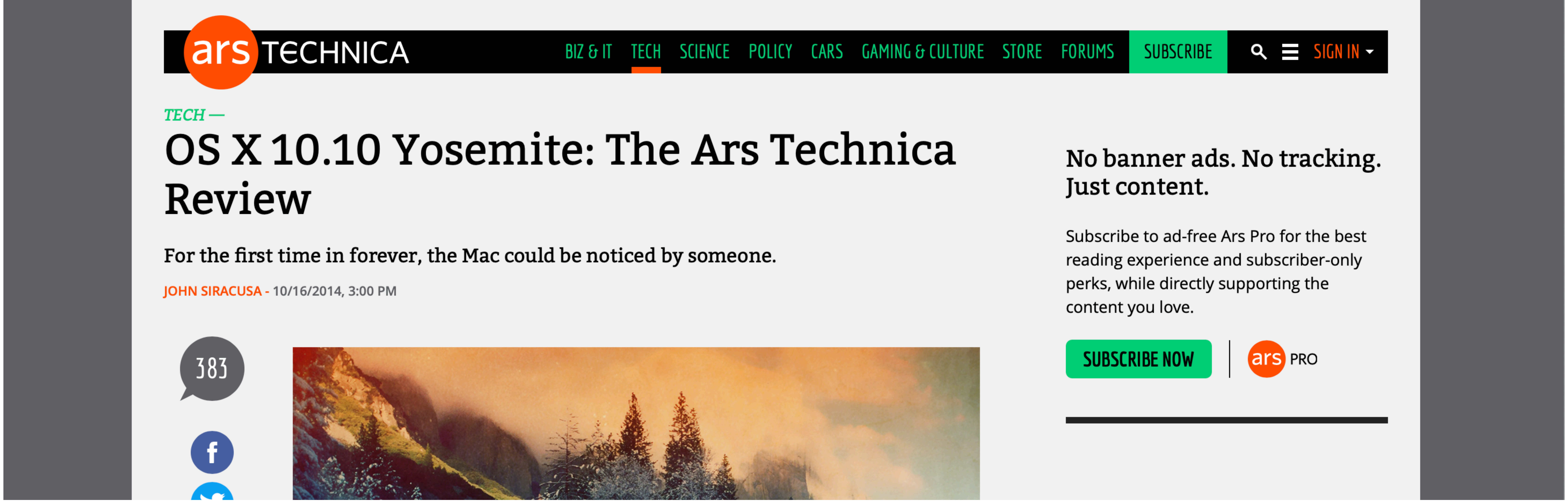
Welcome to webauthn.io! This site is designed by Duo Labs to test the new W3C Specification Web Authentication. WebAuthn is supported in the Chrome, Firefox, and Edge browsers to different degrees, but

What can *you* do?

You don’t need to code!

Reverse engineering

Dig in!



TECH —

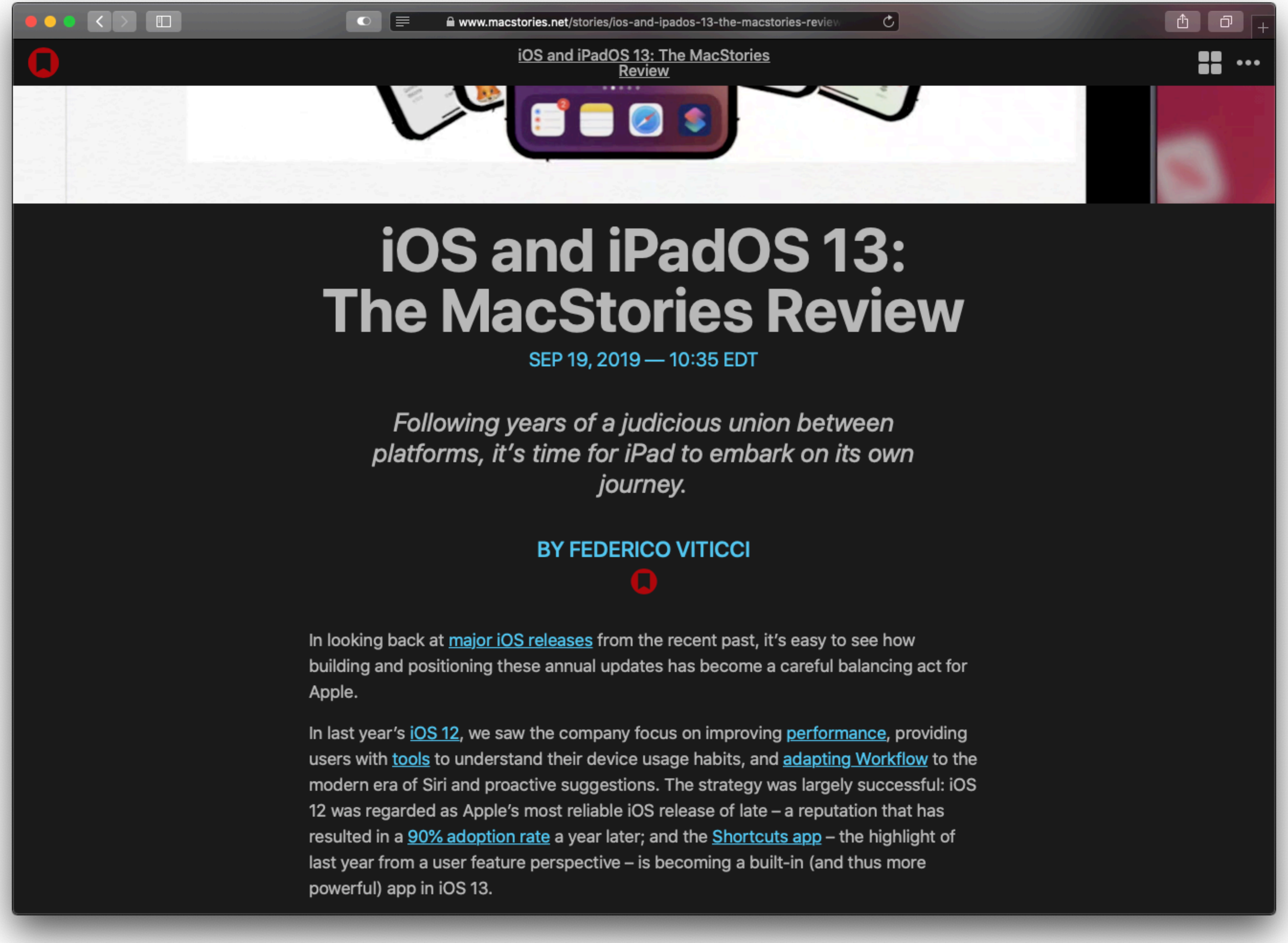
OS X 10.10 Yosemite: The Ars Technica Review

For the first time in forever, the Mac could be noticed by someone.

JOHN SIRACUSA - 10/16/2014, 3:00 PM

No banner ads. No tracking. Just content.

Subscribe to ad-free Ars Pro for the best reading experience and subscriber-only perks, while directly supporting the content you love.


www.macstories.net/stories/ios-and-ipados-13-the-macstories-review
iOS and iPadOS 13: The MacStories Review

iOS and iPadOS 13: The MacStories Review

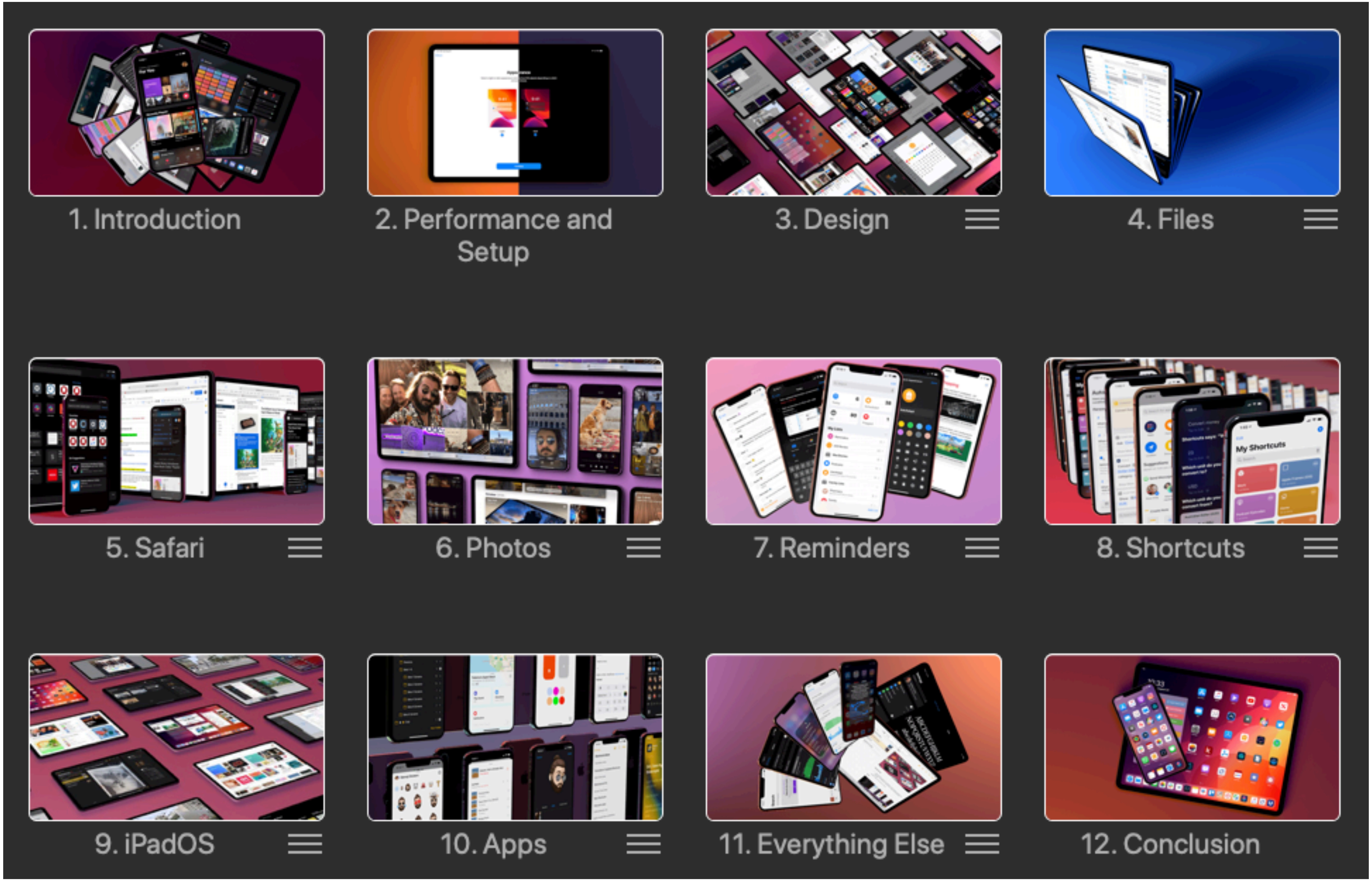
SEP 19, 2019 — 10:35 EDT

Following years of a judicious union between platforms, it's time for iPad to embark on its own journey.

BY FEDERICO VITICCI

In looking back at major iOS releases from the recent past, it's easy to see how building and positioning these annual updates has become a careful balancing act for Apple.

In last year's iOS 12, we saw the company focus on improving performance, providing users with tools to understand their device usage habits, and adapting Workflow to the modern era of Siri and proactive suggestions. The strategy was largely successful: iOS 12 was regarded as Apple's most reliable iOS release of late – a reputation that has resulted in a 90% adoption rate a year later; and the Shortcuts app – the highlight of last year from a user feature perspective – is becoming a built-in (and thus more powerful) app in iOS 13.



1. Introduction

2. Performance and Setup

3. Design

4. Files

5. Safari

6. Photos

7. Reminders

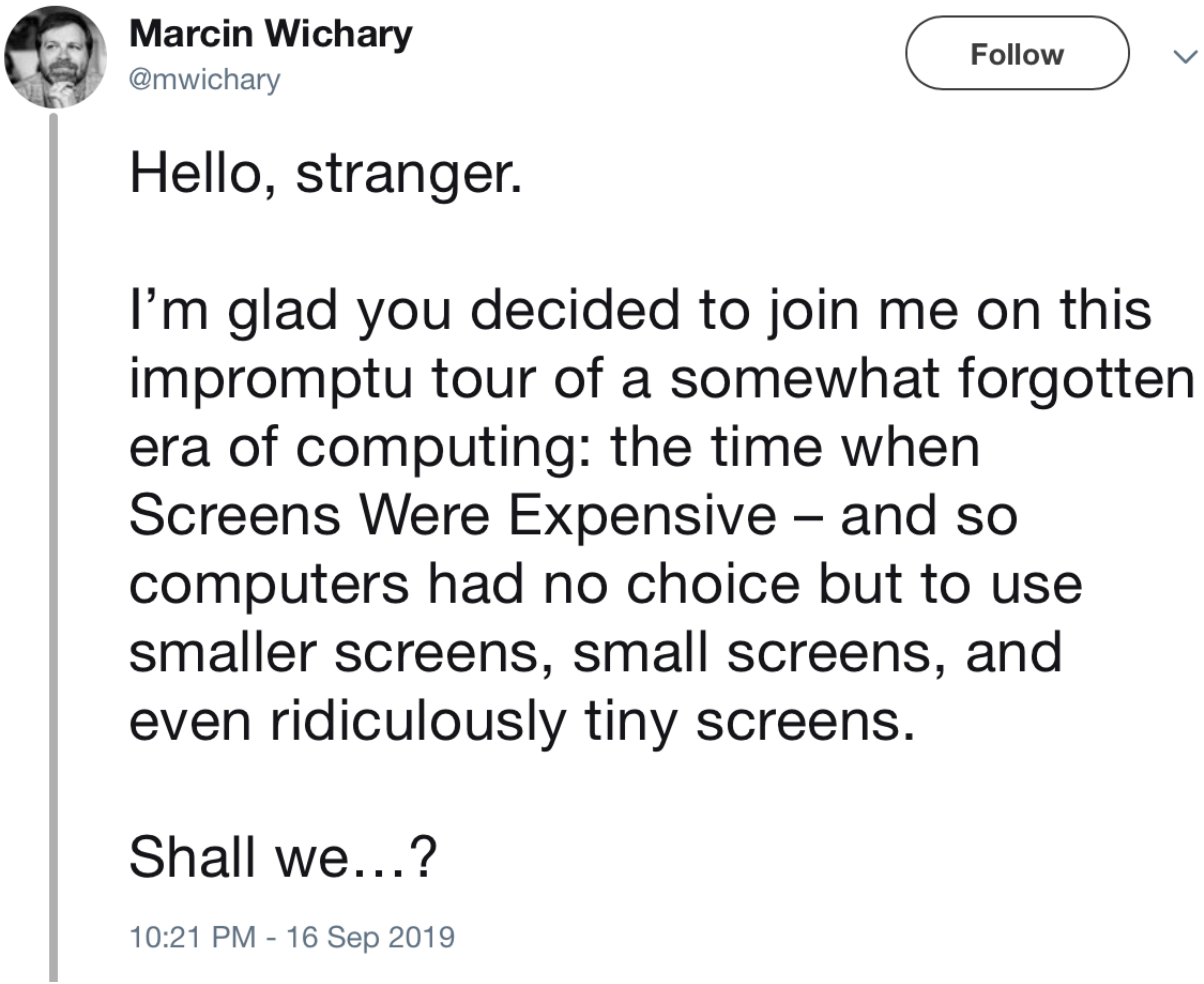
8. Shortcuts

9. iPadOS

10. Apps

11. Everything Else

12. Conclusion



Marcin Wichary
@mwichary

Hello, stranger.

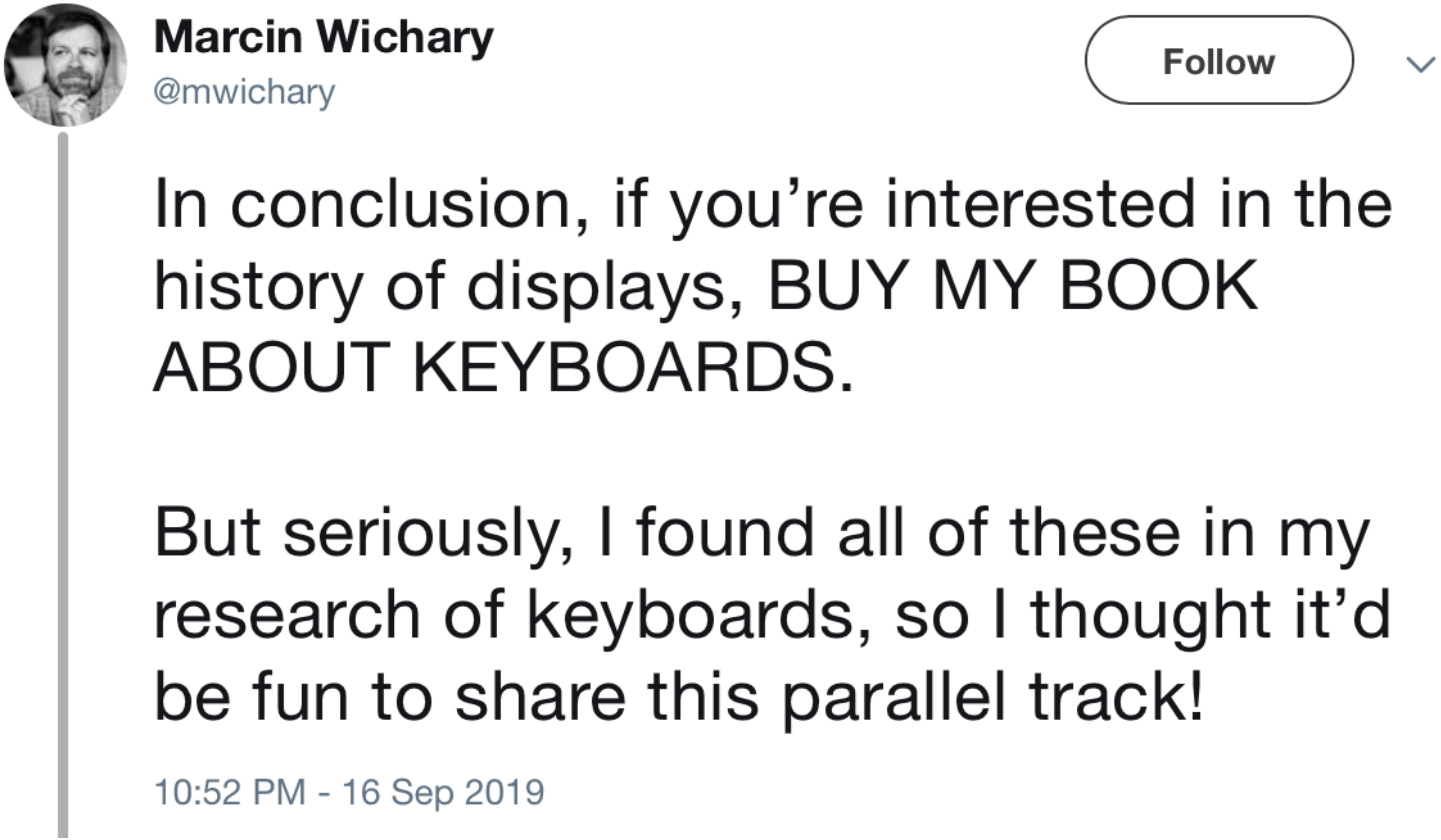
I’m glad you decided to join me on this impromptu tour of a somewhat forgotten era of computing: the time when Screens Were Expensive – and so computers had no choice but to use smaller screens, small screens, and even ridiculously tiny screens.

Shall we…?

10:21 PM - 16 Sep 2019

INFOREX

K
Q
P
COGITO 240
CLEAR K
RESET
Q→K
Q→P
P→K
P→Q
P
Q
RECALL
ENTER
EXCHANGE
POS
NEG
DECIMAL
DIV
ACCUM
SCM
MARCHANT



Marcin Wichary

@mwichary

In conclusion, if you’re interested in the history of displays, BUY MY BOOK ABOUT KEYBOARDS.

But seriously, I found all of these in my research of keyboards, so I thought it’d be fun to share this parallel track!

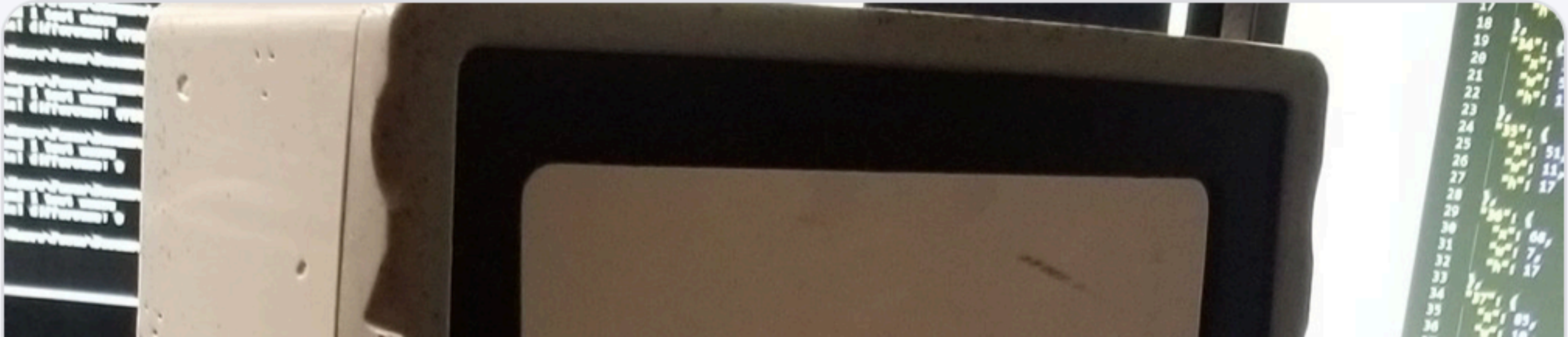
10:52 PM - 16 Sep 2019

foone @Foone · 14h

Check out my latest computer.

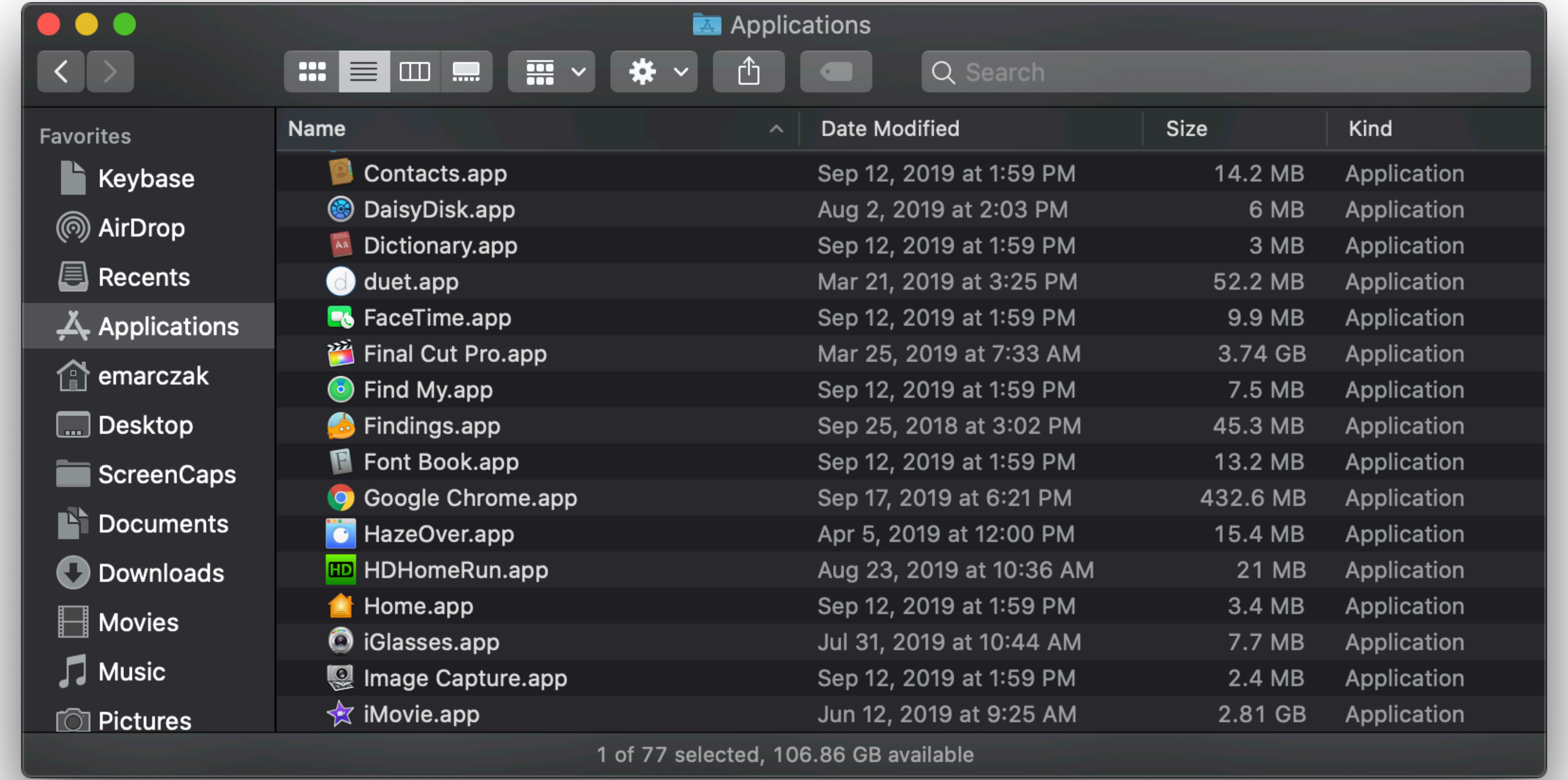
It seems to have been made of stone? and the keyboard is jammed, and the screen is a mirror.

But it is also haunted, so... yeah.



“What can you contribute back to your community?”

–Arek Dreyer



Name	Date Modified	Size	Kind
Contacts.app	Sep 12, 2019 at 1:59 PM	14.2 MB	Application
DaisyDisk.app	Aug 2, 2019 at 2:03 PM	6 MB	Application
Dictionary.app	Sep 12, 2019 at 1:59 PM	3 MB	Application
duet.app	Mar 21, 2019 at 3:25 PM	52.2 MB	Application
FaceTime.app	Sep 12, 2019 at 1:59 PM	9.9 MB	Application
Final Cut Pro.app	Mar 25, 2019 at 7:33 AM	3.74 GB	Application
Find My.app	Sep 12, 2019 at 1:59 PM	7.5 MB	Application
Findings.app	Sep 25, 2018 at 3:02 PM	45.3 MB	Application
Font Book.app	Sep 12, 2019 at 1:59 PM	13.2 MB	Application
Google Chrome.app	Sep 17, 2019 at 6:21 PM	432.6 MB	Application
HazeOver.app	Apr 5, 2019 at 12:00 PM	15.4 MB	Application
HDHomeRun.app	Aug 23, 2019 at 10:36 AM	21 MB	Application
Home.app	Sep 12, 2019 at 1:59 PM	3.4 MB	Application
iGlasses.app	Jul 31, 2019 at 10:44 AM	7.7 MB	Application
Image Capture.app	Sep 12, 2019 at 1:59 PM	2.4 MB	Application
iMovie.app	Jun 12, 2019 at 9:25 AM	2.81 GB	Application

1 of 77 selected, 106.86 GB available

Shell Namespace

```
% echo {a..z}{,a,e,i,o,u}sh
```

```
ash    dsh    gsh    jsh    msh    psh    ssh    vsh    ysh
aash   dash   gash   jash   mash   pash   sash   vash   yash
aesh   desh   gesh   jesh   mesh   pesh   sesh   vesh   yesh
aish   dish   gish   jish   mish   pish   sish   vish   yish
aosh   dosh   gosh   josh   mosh   posh   sosh   vosh   yosh
aush   dush   gush   jush   mush   push   sush   vush   yush
bsh    esh    hsh    ksh    nsh    qsh    tsh    wsh    zsh
bash   eash   hash   kash   nash   qash   tash   wash   zash
besh   eesh   hesh   kesh   nesh   qesh   tesh   wesh   zesh
bish   eish   hish   kish   nish   qish   tish   wish   zish
bosh   eosh   hosh   kosh   nosh   qosh   tosh   wosh   zosh
bush   eush   hush   kush   nush   qush   tush   wush   zush
csh    fsh    ish    lsh    osh    rsh    ush    xsh
cash   fash   iash   lash   oash   rash   uash   xash
cesh   fesh   iesh   lesh   oesh   resh   uesh   xesh
cish   fish   iish   lish   oish   rish   uish   xish
cosh   fosh   iosh   losh   oosh   rosh   uosh   xosh
cush   fush   iush   lush   oush   rush   uush   xush
```

Shell Namespace

🍌sh
💣sh
👽sh
👾sh
👍sh
🤔sh
🥾sh
🐚sh
🤷‍♂️sh

🏝sh
😎sh
🥳sh
🤪sh
🤬sh
😱sh
😈sh
💩sh
👻sh

☠️sh
🤖sh
👊sh
🤙sh
✊sh
🎓sh
🎩sh
👑sh
💍sh

🍣sh
🐲sh
🍄sh
💥sh
☃️sh
🌈sh
🔥sh
🌪sh
🍎sh

🥑sh
🥨sh
🍔sh
🍭sh
🍩sh
🍺sh
🥃sh
⚽sh
🏈sh

🚀sh
🚲sh
🚗sh
🛰sh
🏠sh
🔨sh
🦖sh
🦑sh
🐜sh

sh

Ten-shell ?

Ecks-shell ?

Ten-Ess-Aitch ?

Xish ?

Xsh

Find the new thing, understand how it’s different from the existing thing

Apple T2 vs. TPM

Wireguard vs. SSL VPN (vs. L2TP vs. PPTP)

2FA: SMS Codes vs. TOTP vs. HOTP / Software tokens vs. Hardware Keys

Hardware research

Track metrics

A/B Testing

Be curious!

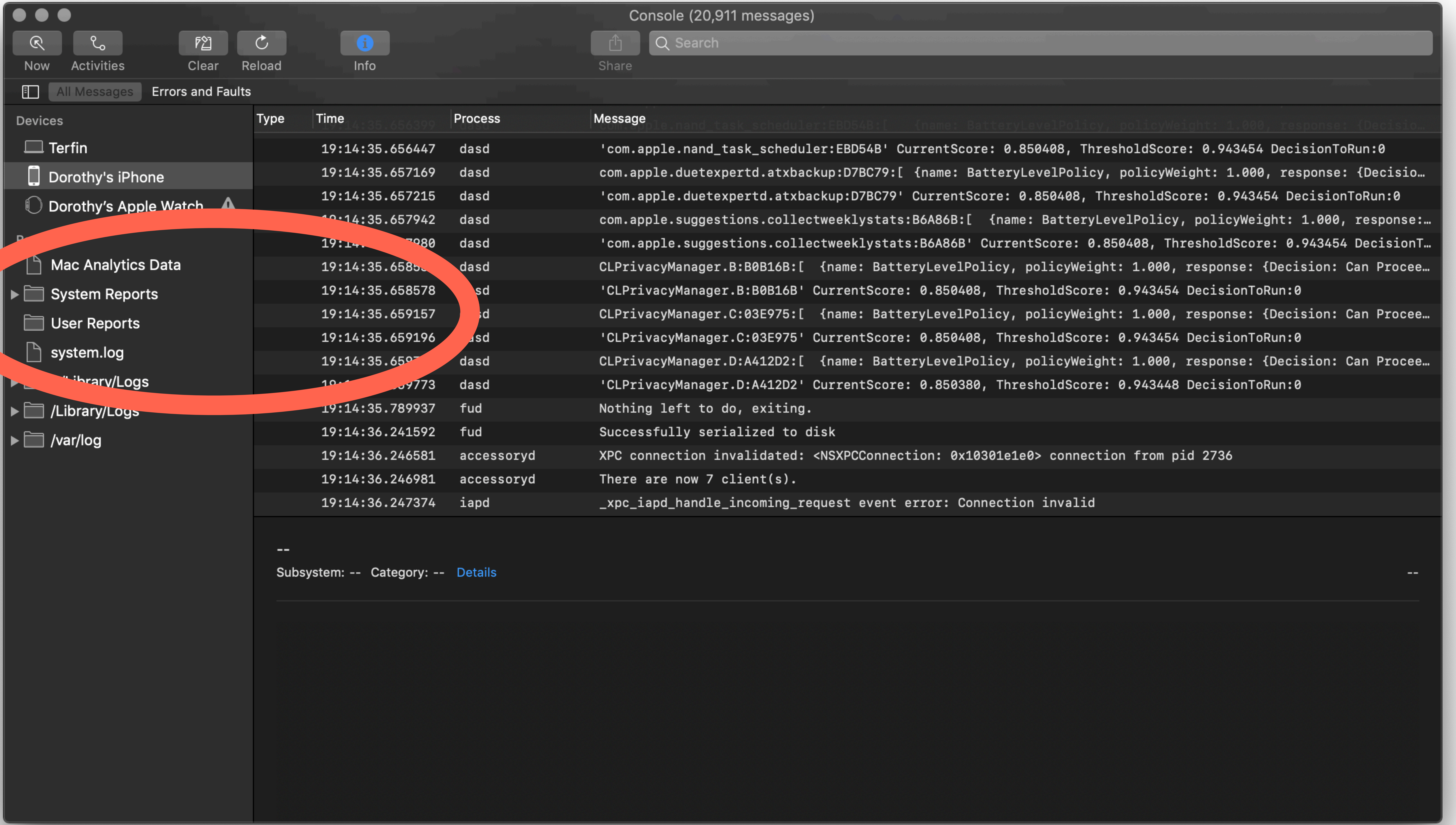
“If it sucks for you, it probably sucks for everyone.”

–Jordan Wright

Show your work
(even if it’s not done.)

Looking för inspiration?

Lögs



```
19:14:35.656447   dasd         'com.apple.nand_task_scheduler:EBD54B' CurrentScore: 0.850408, ThresholdScore: 0.943454 DecisionToRun:0
19:14:35.657169   dasd         com.apple.duetexpertd.atxbackup:D7BC79:[  {name: BatteryLevelPolicy, policyWeight: 1.000, response: {Decisio…
19:14:35.657215   dasd         'com.apple.duetexpertd.atxbackup:D7BC79' CurrentScore: 0.850408, ThresholdScore: 0.943454 DecisionToRun:0
19:14:35.657942   dasd         com.apple.suggestions.collectweeklystats:B6A86B:[  {name: BatteryLevelPolicy, policyWeight: 1.000, response:…
19:14:   7980     dasd         'com.apple.suggestions.collectweeklystats:B6A86B' CurrentScore: 0.850408, ThresholdScore: 0.943454 DecisionT…
19:14:35.6585     dasd         CLPrivacyManager.B:B0B16B:[  {name: BatteryLevelPolicy, policyWeight: 1.000, response: {Decision: Can Procee…
19:14:35.658578     sd         'CLPrivacyManager.B:B0B16B' CurrentScore: 0.850408, ThresholdScore: 0.943454 DecisionToRun:0
19:14:35.659157     sd         CLPrivacyManager.C:03E975:[  {name: BatteryLevelPolicy, policyWeight: 1.000, response: {Decision: Can Procee…
19:14:35.659196    sd          'CLPrivacyManager.C:03E975' CurrentScore: 0.850408, ThresholdScore: 0.943454 DecisionToRun:0
19:14:35.659      dasd         CLPrivacyManager.D:A412D2:[  {name: BatteryLevelPolicy, policyWeight: 1.000, response: {Decision: Can Procee…
19:       9773    dasd         'CLPrivacyManager.D:A412D2' CurrentScore: 0.850380, ThresholdScore: 0.943448 DecisionToRun:0
19:14:35.789937   fud          Nothing left to do, exiting.
19:14:36.241592   fud          Successfully serialized to disk
19:14:36.246581   accessoryd   XPC connection invalidated: <NSXPCConnection: 0x10301e1e0> connection from pid 2736
19:14:36.246981   accessoryd   There are now 7 client(s).
19:14:36.247374   iapd         _xpc_iapd_handle_incoming_request event error: Connection invalid
```

--

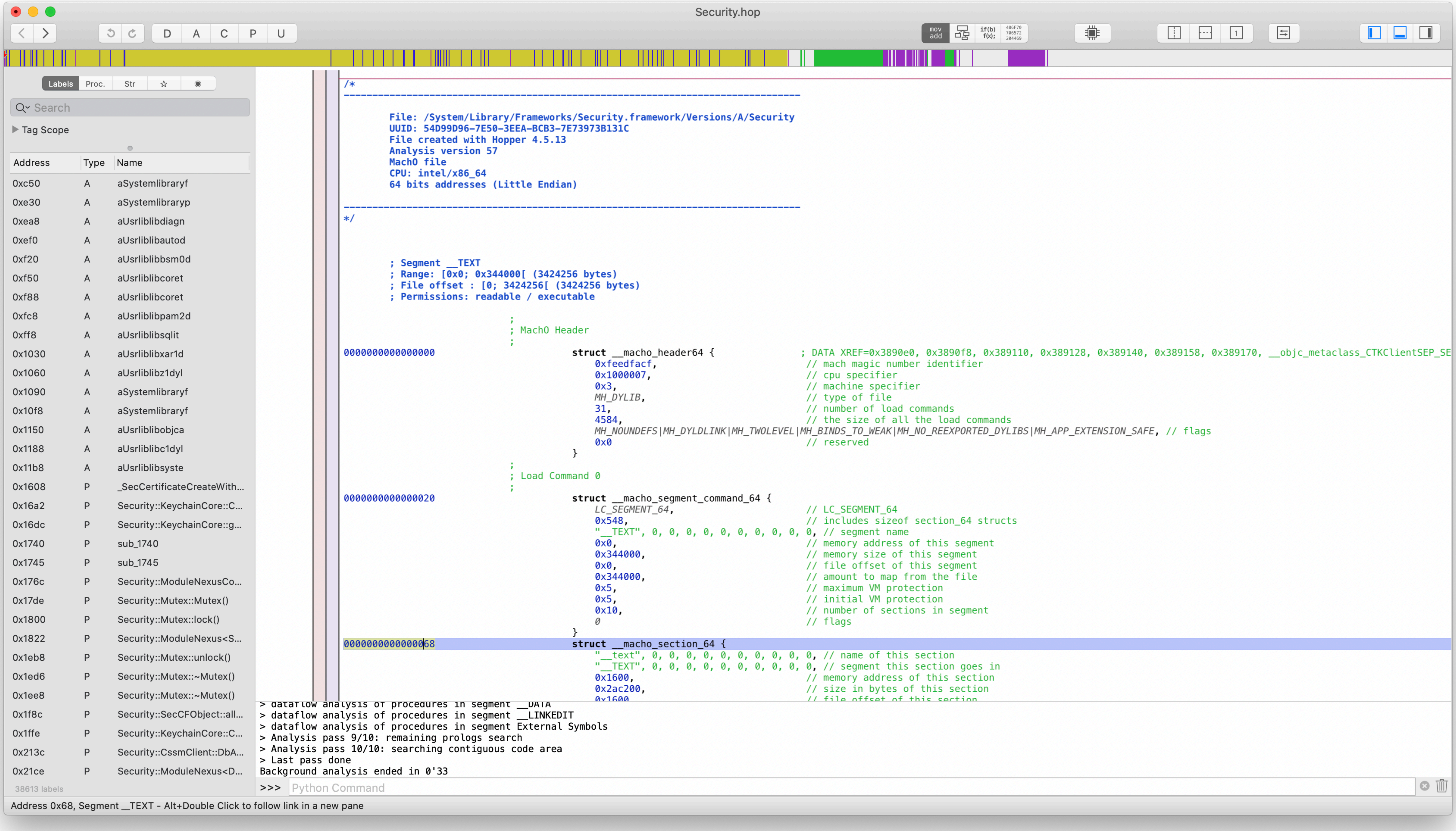
Subsystem: --   Category: --   Details   --

```
[ ~ ]$ log show
--predicate '(eventMessage CONTAINS "Authentication failed")'
--style syslog
--last 2d
```

```
[ ~ ]$ log show
--predicate '(subsystem CONTAINS “com.apple.sso")'
--style syslog
```

```
[ ~ ]$ log stream
-info
--predicate 'sender contains[c] "WirelessProximity"'
```

lldb / Hopper/ Radare



Address	Type	Name
0xc50	A	aSystemlibraryf
0xe30	A	aSystemlibraryp
0xea8	A	aUsrliblibdiagn
0xef0	A	aUsrliblibautod
0xf20	A	aUsrliblibbsm0d
0xf50	A	aUsrliblibcoret
0xf88	A	aUsrliblibcoret
0xfc8	A	aUsrliblibpam2d
0xff8	A	aUsrliblibsqlit
0x1030	A	aUsrliblibxar1d
0x1060	A	aUsrliblibz1dyl
0x1090	A	aSystemlibraryf
0x10f8	A	aSystemlibraryf
0x1150	A	aUsrliblibobjca
0x1188	A	aUsrliblibc1dyl
0x11b8	A	aUsrliblibsyste
0x1608	P	_SecCertificateCreateWith...
0x16a2	P	Security::KeychainCore::C...
0x16dc	P	Security::KeychainCore::g...
0x1740	P	sub_1740
0x1745	P	sub_1745
0x176c	P	Security::ModuleNexusCo...
0x17de	P	Security::Mutex::Mutex()
0x1800	P	Security::Mutex::lock()
0x1822	P	Security::ModuleNexus<S...
0x1eb8	P	Security::Mutex::unlock()
0x1ed6	P	Security::Mutex::~Mutex()
0x1ee8	P	Security::Mutex::~Mutex()
0x1f8c	P	Security::SecCFObject::all...
0x1ffe	P	Security::KeychainCore::C...
0x213c	P	Security::CssmClient::DbA...
0x21ce	P	Security::ModuleNexus<D...

38613 labels

```
/*
--------------------------------------------------------------------------------

        File: /System/Library/Frameworks/Security.framework/Versions/A/Security
        UUID: 54D99D96-7E50-3EEA-BCB3-7E73973B131C
        File created with Hopper 4.5.13
        Analysis version 57
        MachO file
        CPU: intel/x86_64
        64 bits addresses (Little Endian)

--------------------------------------------------------------------------------
*/



        ; Segment __TEXT
        ; Range: [0x0; 0x344000[ (3424256 bytes)
        ; File offset : [0; 3424256[ (3424256 bytes)
        ; Permissions: readable / executable

                             ;
                             ; MachO Header
                             ;
0000000000000000                     struct __macho_header64 {              ; DATA XREF=0x3890e0, 0x3890f8, 0x389110, 0x389128, 0x389140, 0x389158, 0x389170, __objc_metaclass_CTKClientSEP_SE
                                         0xfeedfacf,                          // mach magic number identifier
                                         0x1000007,                           // cpu specifier
                                         0x3,                                 // machine specifier
                                         MH_DYLIB,                            // type of file
                                         31,                                  // number of load commands
                                         4584,                                // the size of all the load commands
                                         MH_NOUNDEFS|MH_DYLDLINK|MH_TWOLEVEL|MH_BINDS_TO_WEAK|MH_NO_REEXPORTED_DYLIBS|MH_APP_EXTENSION_SAFE, // flags
                                         0x0                                  // reserved
                                     }
                             ;
                             ; Load Command 0
                             ;
0000000000000020                     struct __macho_segment_command_64 {
                                         LC_SEGMENT_64,                       // LC_SEGMENT_64
                                         0x548,                               // includes sizeof section_64 structs
                                         "__TEXT", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, // segment name
                                         0x0,                                 // memory address of this segment
                                         0x344000,                            // memory size of this segment
                                         0x0,                                 // file offset of this segment
                                         0x344000,                            // amount to map from the file
                                         0x5,                                 // maximum VM protection
                                         0x5,                                 // initial VM protection
                                         0x10,                                // number of sections in segment
                                         0                                    // flags
                                     }
0000000000000068                     struct __macho_section_64 {
                                         "__text", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, // name of this section
                                         "__TEXT", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, // segment this section goes in
                                         0x1600,                              // memory address of this section
                                         0x2ac200,                            // size in bytes of this section
                                         0x1600,                              // file offset of this section
```

```
> dataflow analysis of procedures in segment __DATA
> dataflow analysis of procedures in segment __LINKEDIT
> dataflow analysis of procedures in segment External Symbols
> Analysis pass 9/10: remaining prologs search
> Analysis pass 10/10: searching contiguous code area
> Last pass done
Background analysis ended in 0'33
>>> Python Command
```

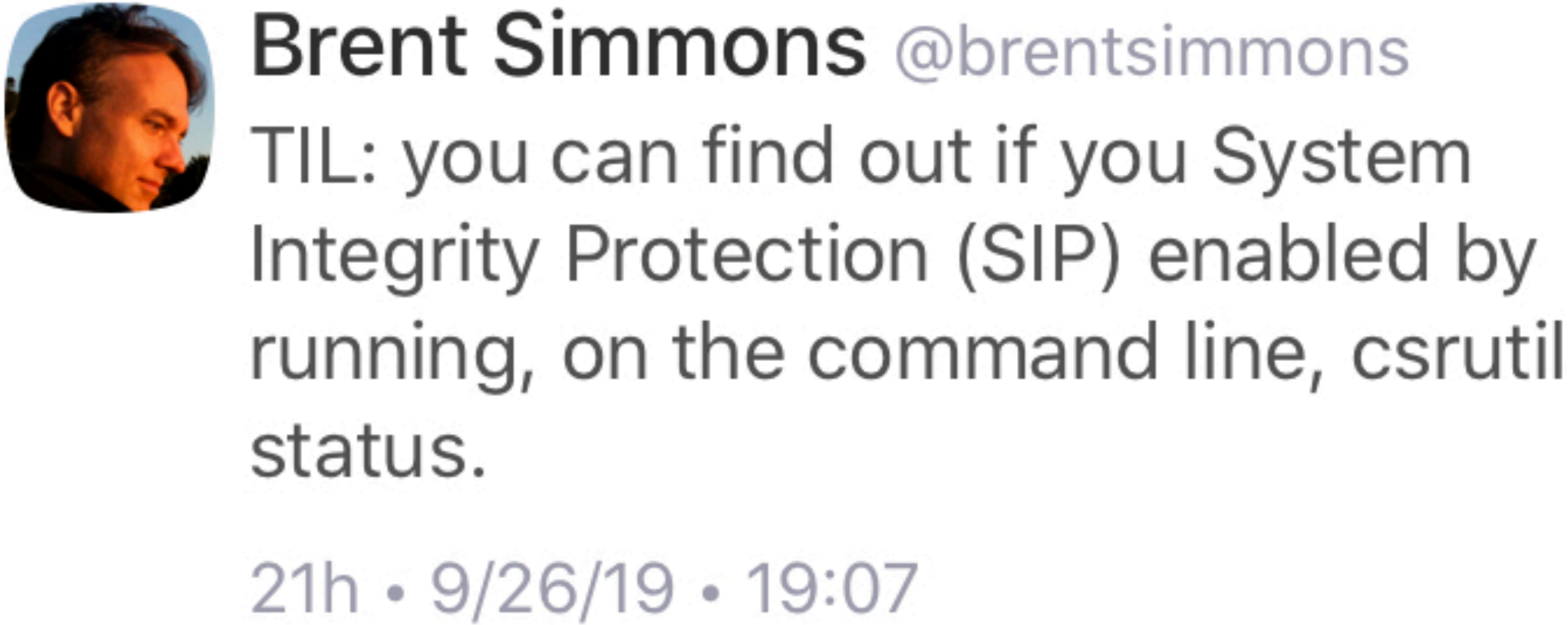
Address 0x68, Segment __TEXT - Alt+Double Click to follow link in a new pane

D̊esïgn

iPhone 7
Concept with iOS 10
iPhone-Tricks.de
100%
Donnerstag
28
Nachrichten
Kalender
Fotos
Kamera
Herzogenrath
Sonnig
28°
Videos
Wallet
Aktien
iTunes Store
App Store

Tålk with your end-üsers!

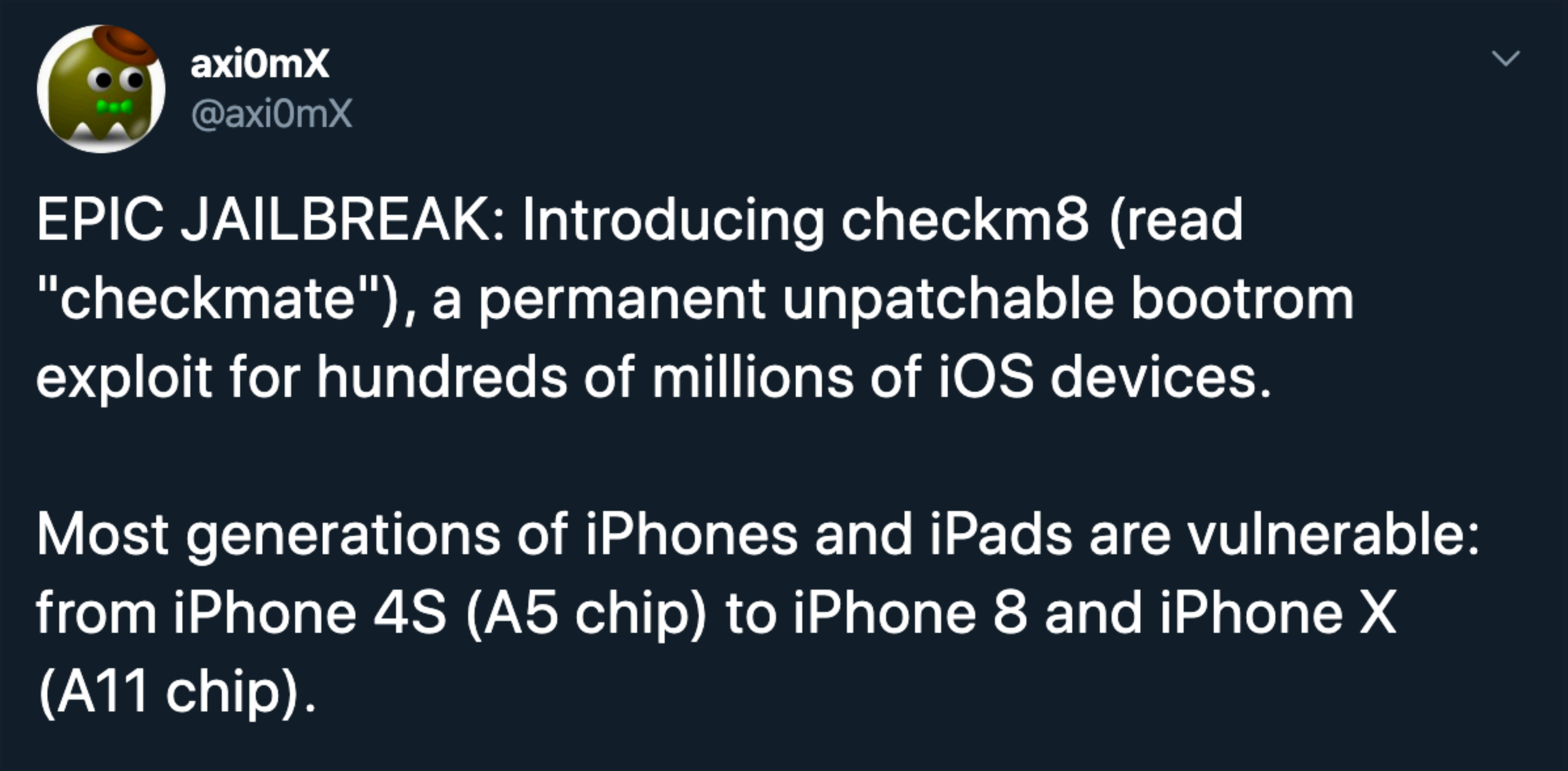
It doesn’t have to be original



Brent Simmons @brentsimmons

TIL: you can find out if you System Integrity Protection (SIP) enabled by running, on the command line, csrutil status.

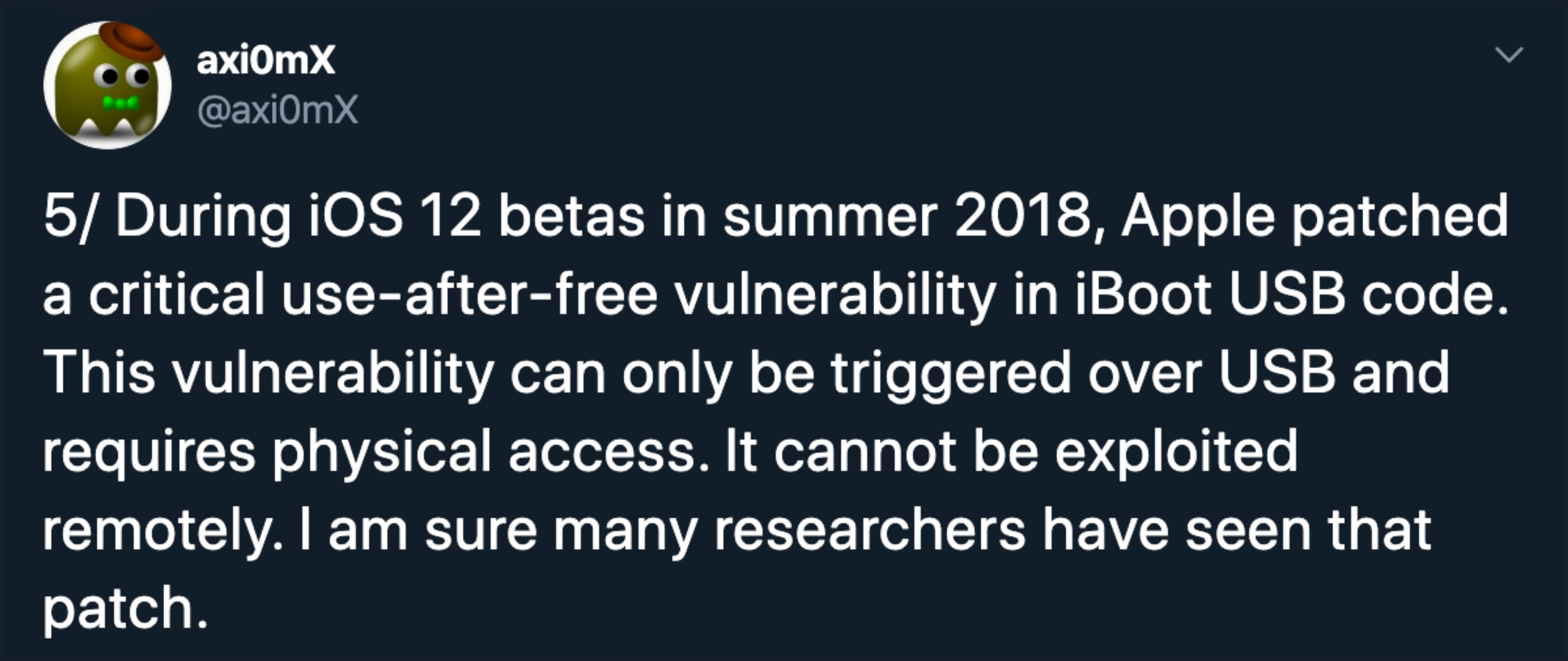
21h • 9/26/19 • 19:07



axi0mX
@axi0mX

EPIC JAILBREAK: Introducing checkm8 (read "checkmate"), a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.

Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip).



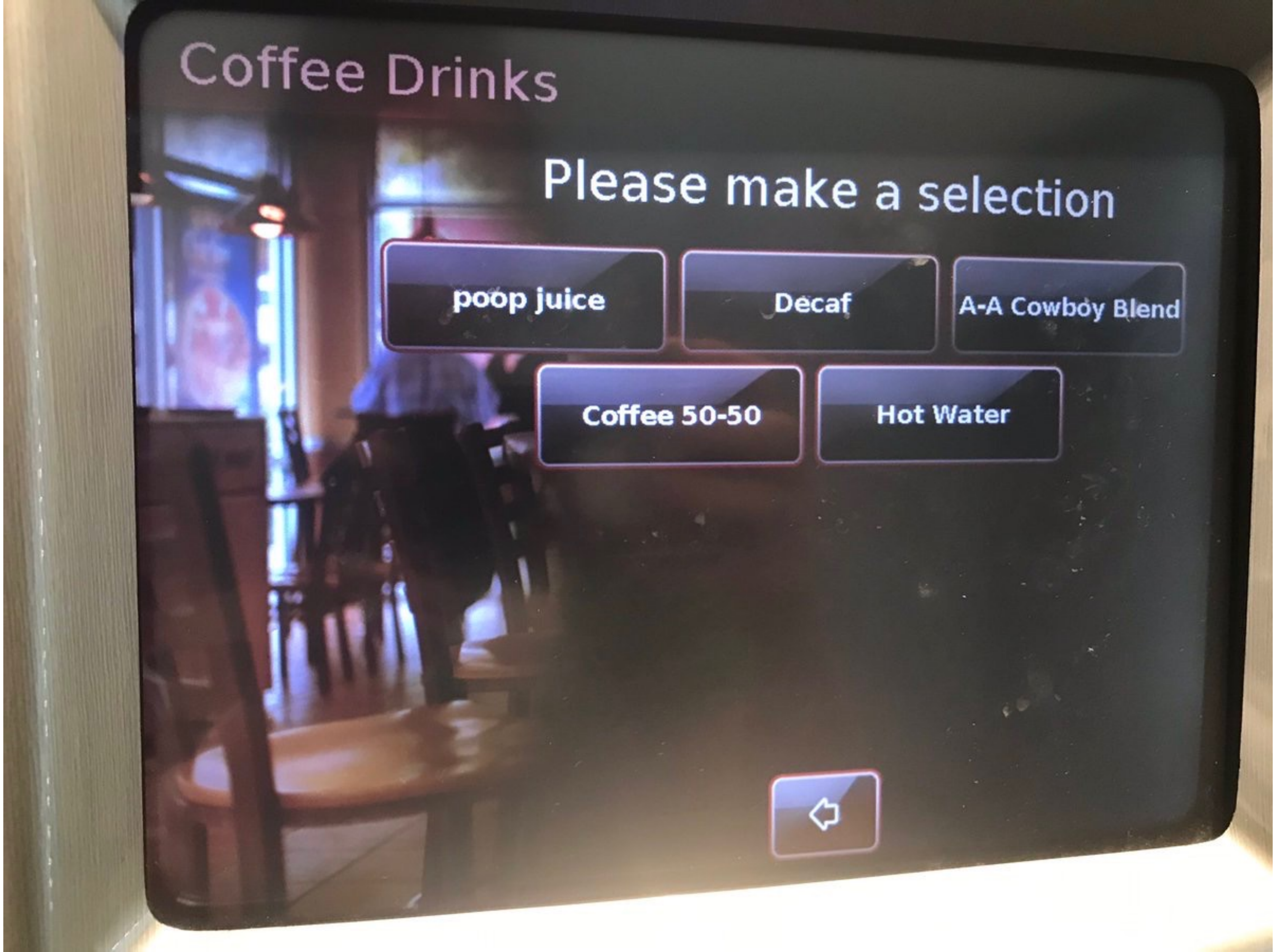
axi0mX
@axi0mX

5/ During iOS 12 betas in summer 2018, Apple patched a critical use-after-free vulnerability in iBoot USB code. This vulnerability can only be triggered over USB and requires physical access. It cannot be exploited remotely. I am sure many researchers have seen that patch.

It doesn’t have to be original

It doesn’t have to be original ...but it has to be *your* work

Enjoy!!



Coffee Drinks

Please make a selection

evi
omething good
You broke Bevi!
JK, we'll be right back.
One moment...

S̸̤̖̓h̥̊ä̸͓́͠r̸̹͑e̸̦͗!̸͓̃

“Why aren’t you sharing this?”

–Ed Marczak

(Security) Research to Improve the World

Ed Marczak
@marczak