The secret life of a rogue device

by @iammandatory

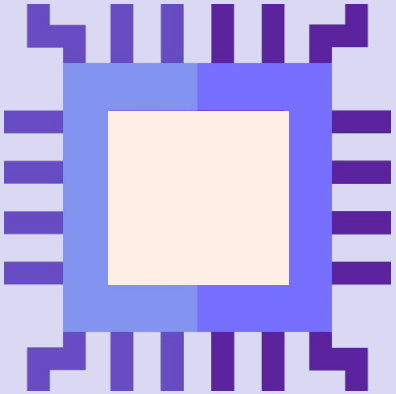
Who am I?

- Matthew Bryant A.K.A. @IAmMandatory
- XSS Hunter, FindThatMeme, TheHackerBlog.com
- Red team @ Snap

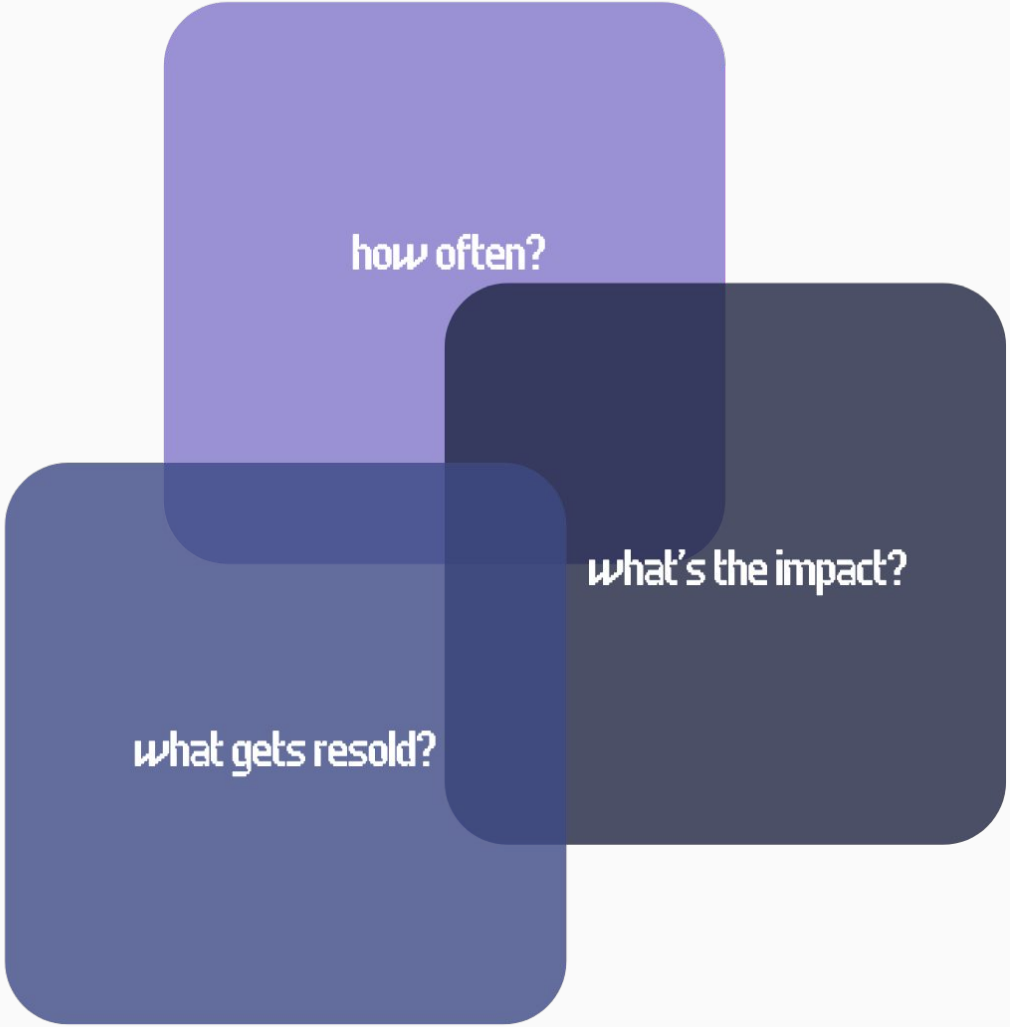


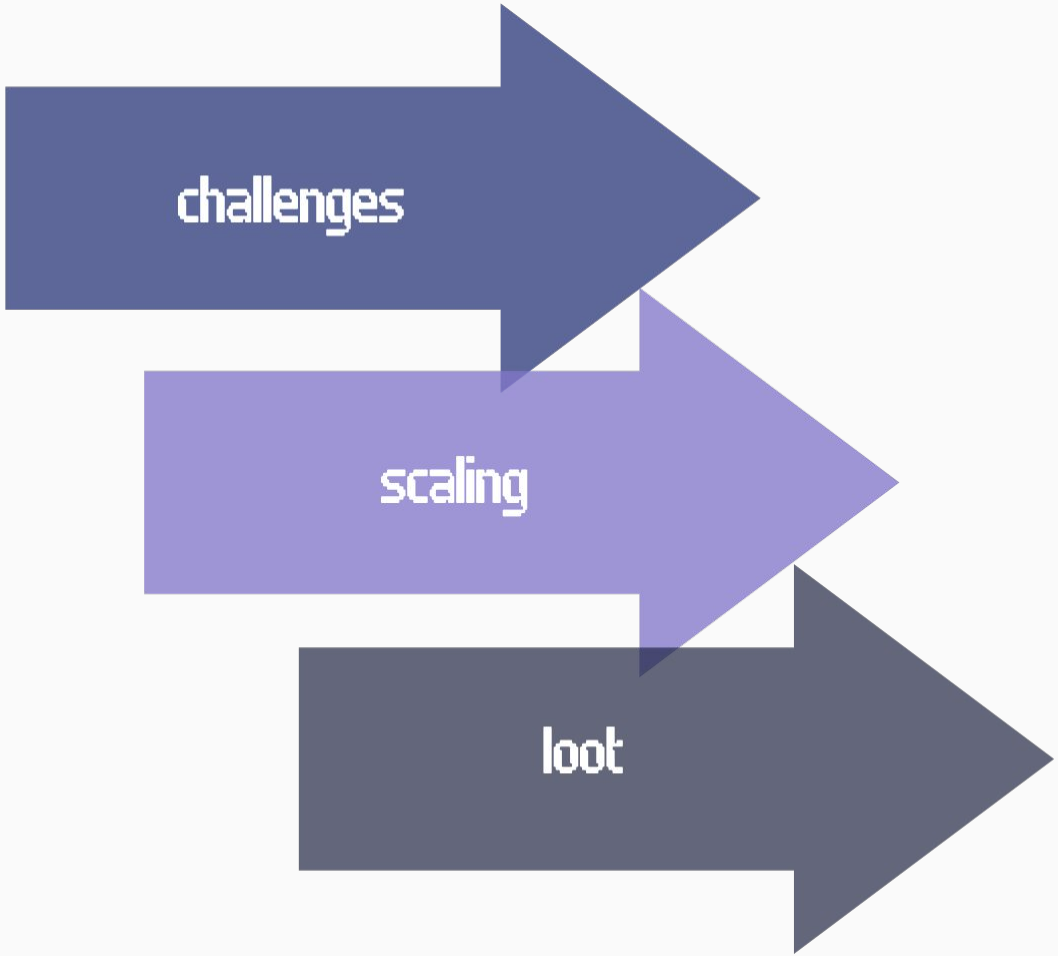
What do you mean "rogue" hardware?








how often?
what's the impact?
what gets resold?


challenges
scaling
loot

Challenges



What are the *challenges* to find rogue hardware?

Challenge #1: Where?



ebay



craigslist



For prototypes: there is a secret bonus market



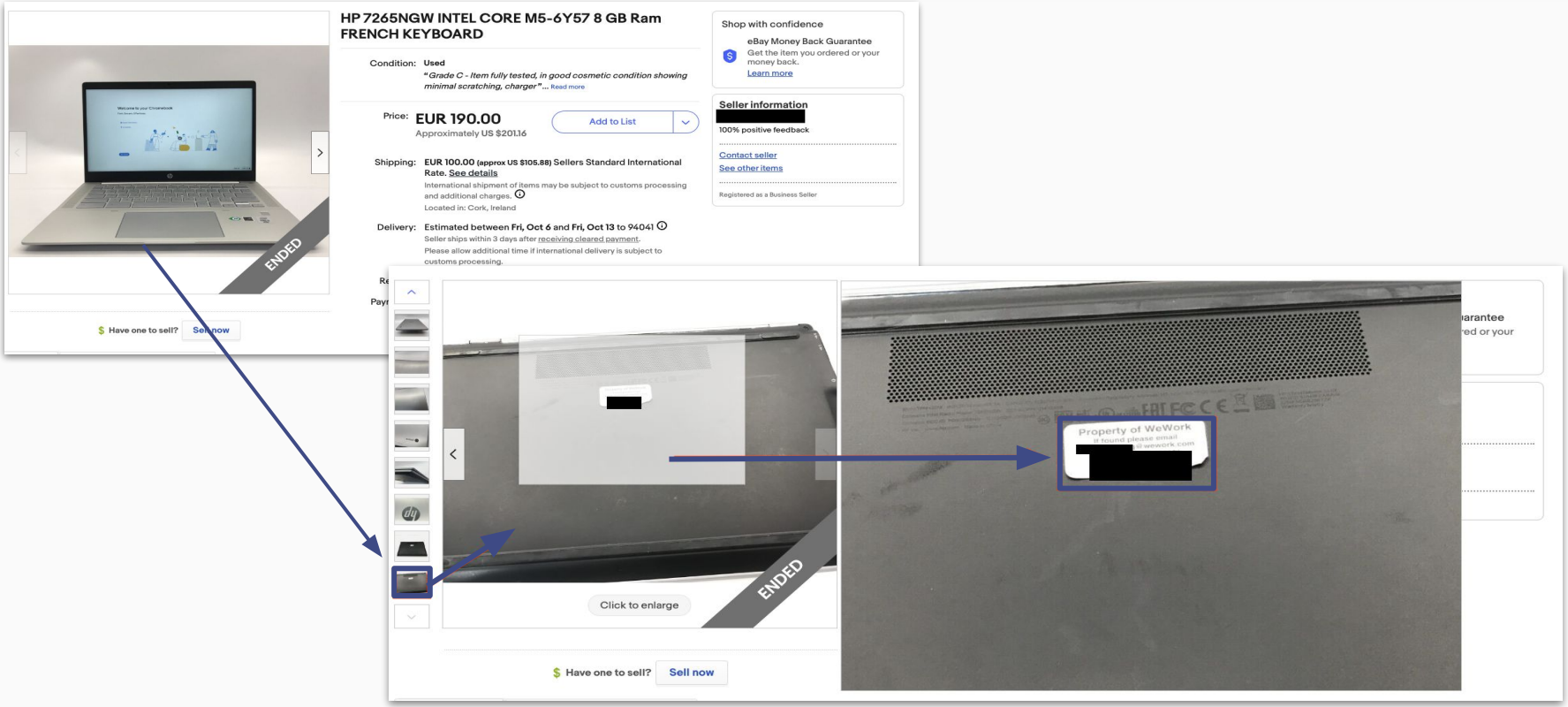
Xianyu (闲鱼): Chinese Second Hand Market



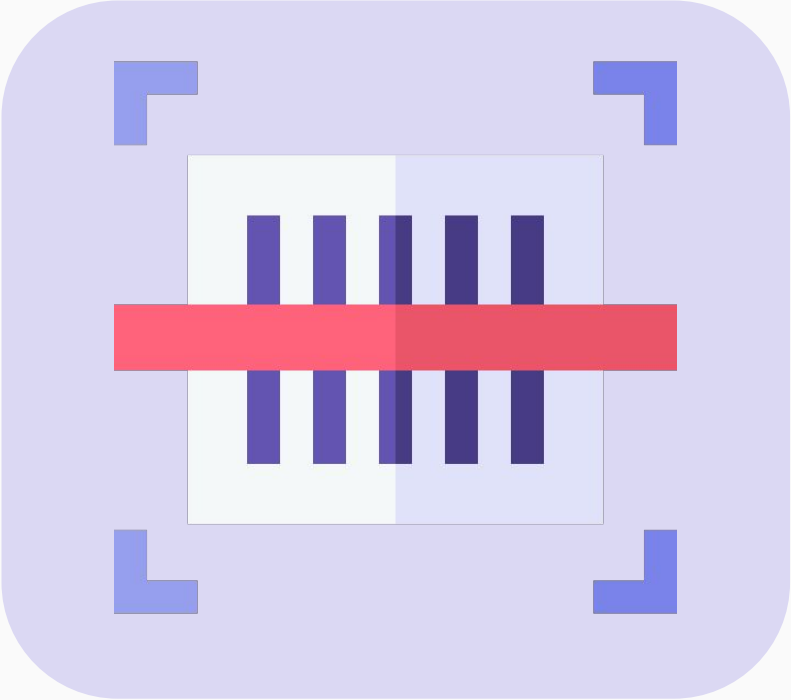
Challenge #2: Secrets are hidden in listings

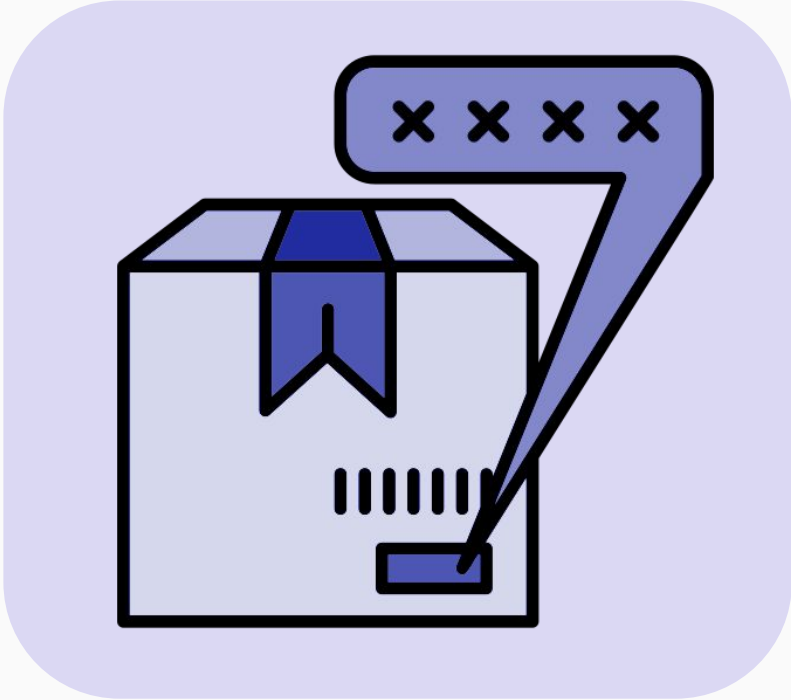


Solution: Images

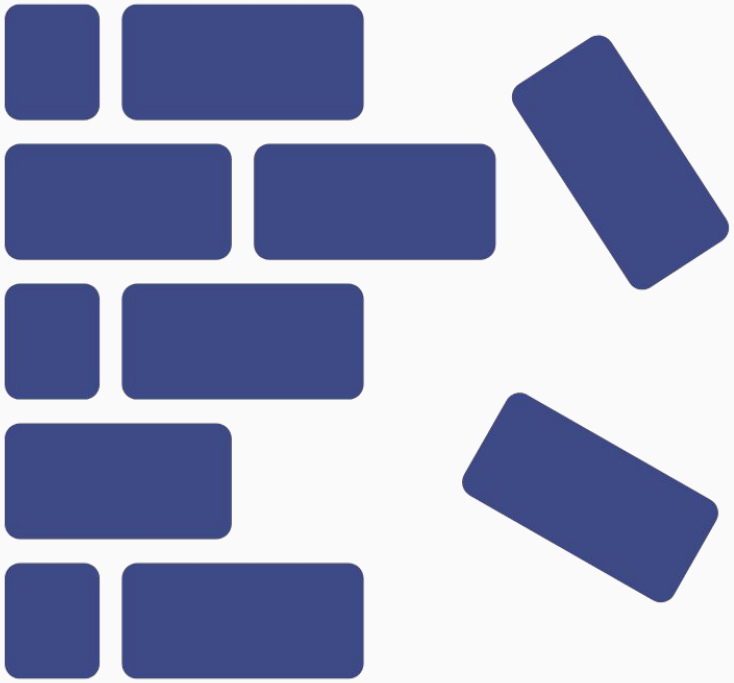


Challenge #3: Knowing what we're looking for





Scaling

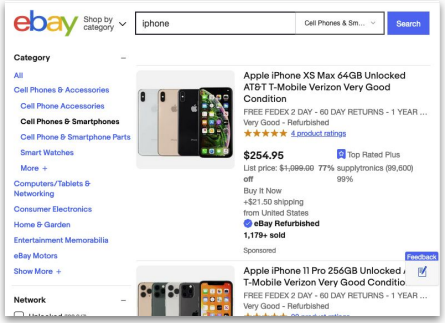


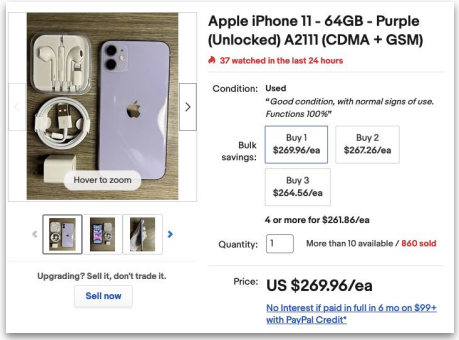
Building a *pipeline* for detecting rogue hardware

Challenge #1: Scraping



Scraping ebay

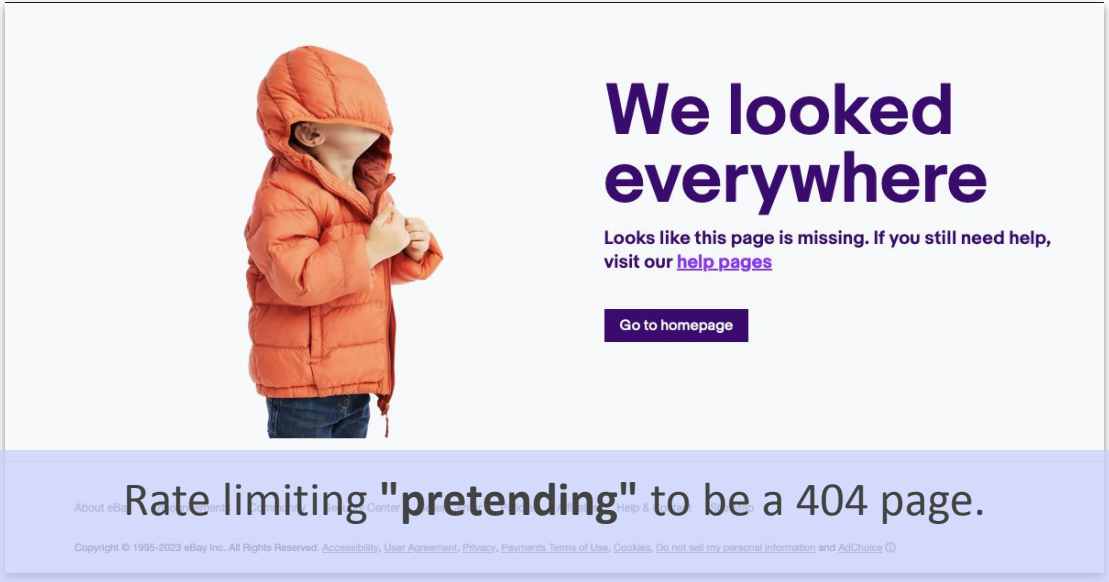






Search → Scrape → Extract

Hurdle: Rate limiting

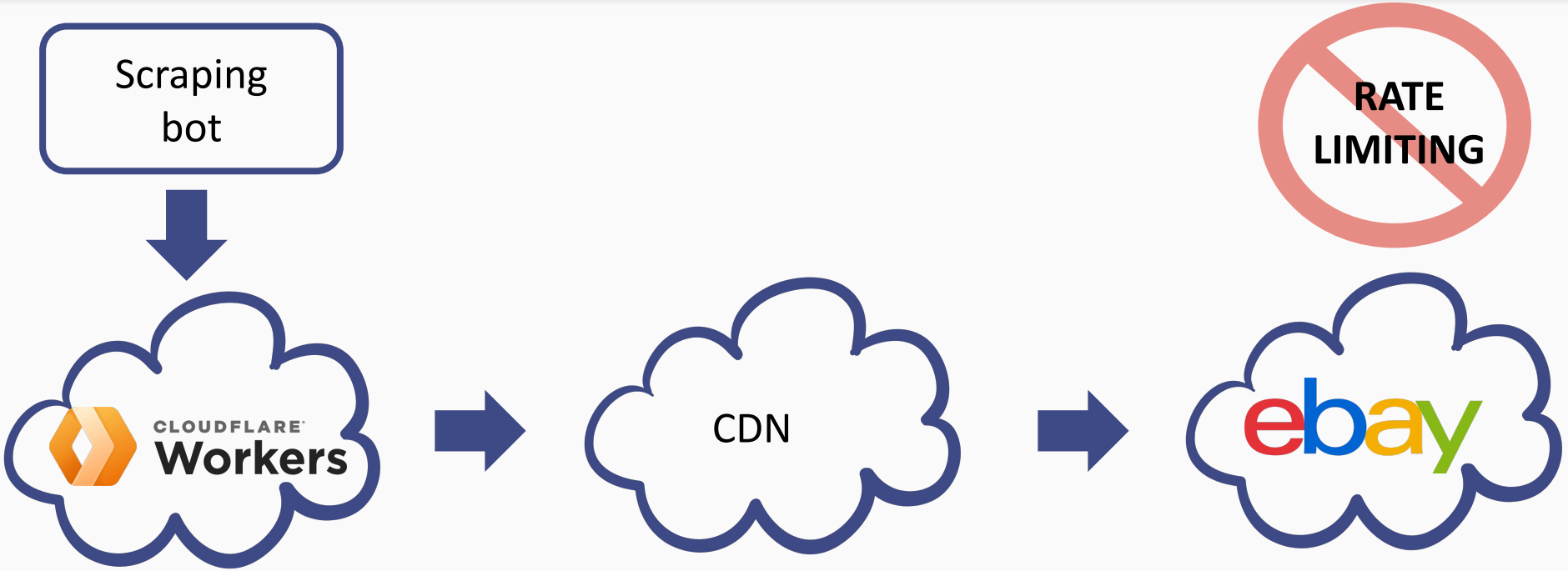


Rate limiting **"pretending"** to be a 404 page.

Production services



Solution for rate limiting




GAP
Moving right along…

闲鱼 A.K.A. Xianyu A.K.A. "Idlefish"



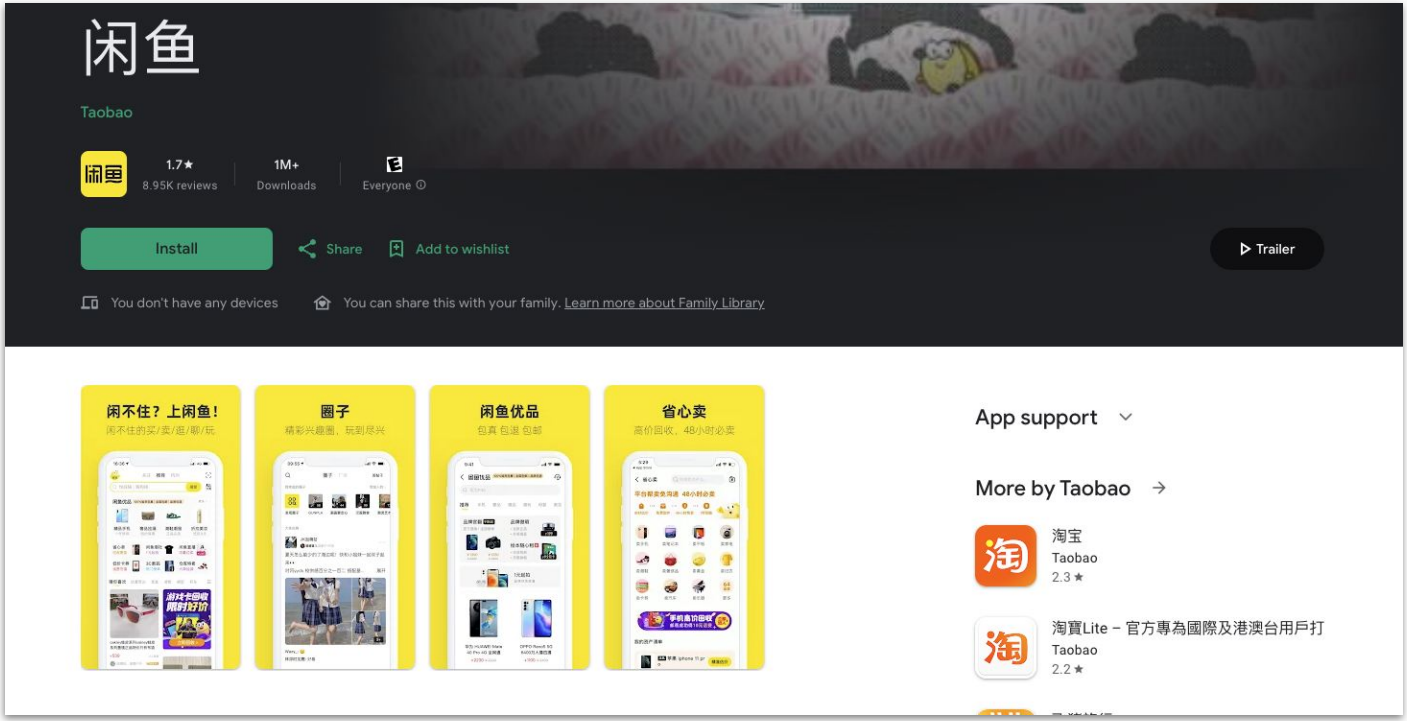
Kind of…





Homepage just tells you to download their iOS or Android app.

Calling their APIs

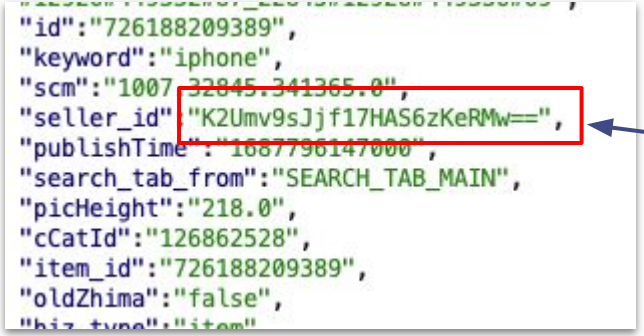


Anti-bot protections



```
POST /gw/mtop.taobao.idlemtopsearch.search/1.0/ HTTP/2
Host: g-acs.m.goofish.com
X-Sgext:
JAziV2[redacted]

Umid: ltEB1[redacted]
X-Sign: azU7B[redacted]
X-Sid: 129e[redacted]
X-Uid: 22[redacted]
X-Nettype: WIFI
X-Pv: 6.3
X-Nq: WIFI
Eagleeye-Userdata: spm-cnt=a2170.8011571.0.0&spm-url=a2170.unknown.0.0
First_open: 0
X-Features: 27
X-App-Conf-V: 0
X-Mini-Wua:
ajgQrqlrh[redacted]

Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 3648
X-T: 1687796153
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Cookie: [redacted]

X-Bx-Version: 6.5.88
F-Refer: mtop
X-Extdata: openappkey%3DDEFAULT_AUTH
X-Ttid: 212200%40fleamarket_android_7.8.49
X-App-Ver: 7.8.49
X-C-Traceid: ZHUu[redacted]
X-Location: 0%2C0
X-Umt: ltEB[redacted]
A-Orange-Q: appKey=21407387&appVersion=7.8.49&clientAppIndexVersion=1120230625090600887&clientVersionIndexVersion=0
X-Utdid: ZHU[redacted]
X-Appkey: 21407387
X-Devid: AgIna[redacted]a
User-Agent: MTOPSDK%2F3.1.1.7+%28Android%3B12%3BGoogle%3BPixel+3a%29
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

data=
[redacted]
```

Some more protections



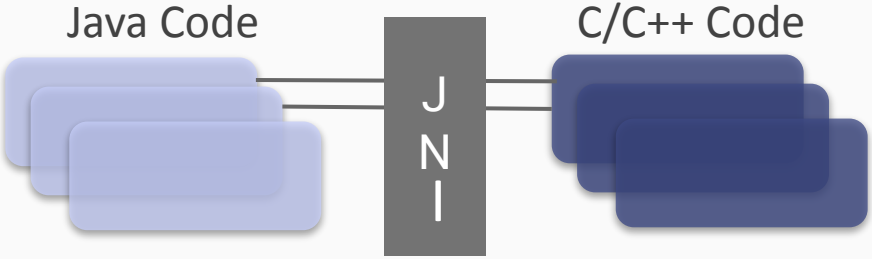
Encrypted in HTTP responses and decrypted by the app.

Even more protections



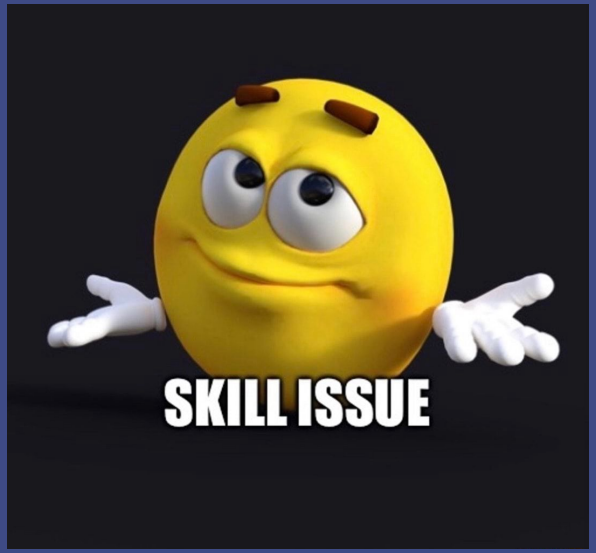
Proprietary CAPTCHA which is required for doing searches regularly if not logged in.

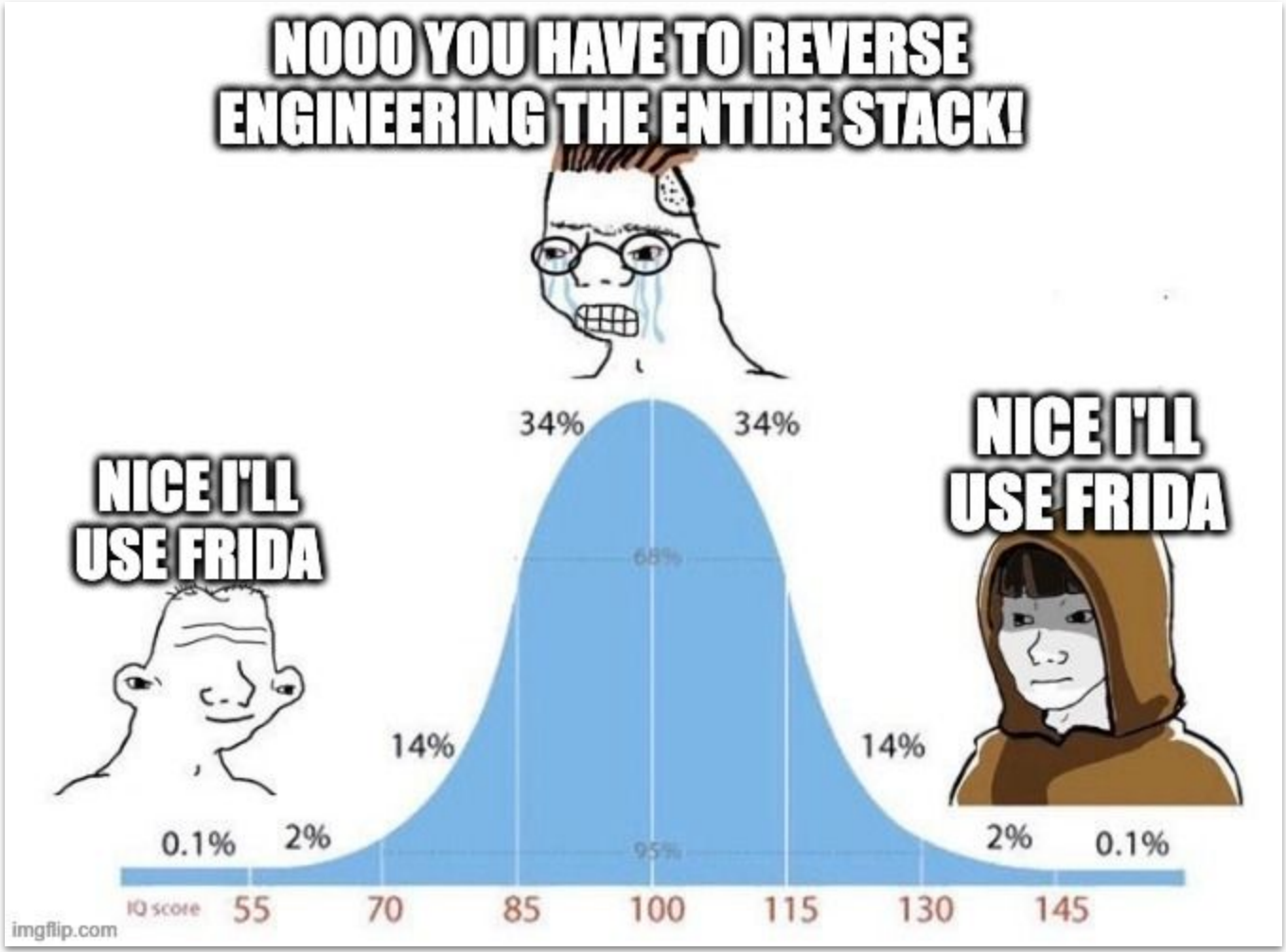
```
POST /gw/mtop.taobao.idlemtopsearch.search/1.0/ HTTP/2
Host: g-acs.m.goofish.com
X-Sgext:
1AzivE
Umid: ltEB
X-Sign: azU7B
X-Sid: 129e
X-Uid: 22
X-Nettype: WIFI
X-Pv: 6.3
X-Nq: WIFI
Eagleeye-Userdata: spm-cnt=a2170.8011571.0.0&spm-url=a2170.unknown.0.0
First_open: 0
X-Features: 27
X-App-Conf-V: 0
X-Mini-Wua:
ajgQrqlrh
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 3648
X-T: 1687796153
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Cookie:
X-Bx-Version: 6.5.88
F-Refer: mtop
X-Extdata: openappkey%3DDEFAULT_AUTH
X-Ttid: 212200%40fleamarket_android_7.8.49
X-App-Ver: 7.8.49
X-C-Traceid: ZHUa
X-Location:
X-Umt: ltEB
A-Orange-Q:
X-Utdid: ZHU
X-Appkey: 21407387
X-Devid: AgIn
User-Agent: MTOPSDK%2F3.1.1.7+%28Android%3B12%3BGoogle%3BPixel+3a%29
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

data=
```





TL;DR:




NOOO YOU HAVE TO REVERSE ENGINEERING THE ENTIRE STACK!
NICE I'LL USE FRIDA
NICE I'LL USE FRIDA
34%
34%
14%
14%
0.1%
2%
2%
0.1%
68%
95%
IQ score
55
70
85
100
115
130
145
imgflip.com




```
// Depending on the current activity, take the appropriate action
if(current_activity == 'com.taobao.fleamarket.home.activity.InitActivity') {
    console.log(`[STATUS][IDLEFISH] Currently on the ToS accept prompt, tapping accept...`);
    await android_tap_element_at_selector(`node[resource-id="com.taobao.idlefish:id/right_btn"]`);
    // Wait a few seconds for the full menu page to load properly.
    await wait(7);
    last_activity = current_activity;
    continue
} else if(current_activity == 'com.taobao.idlefish.maincontainer.activity.MainActivity') {
    console.log(`[STATUS][IDLEFISH] Currently on the main menu, tapping the search bar...`);
    await android_tap_element_at_selector(`node[resource-id="com.taobao.idlefish:id/search_bar_layout"]`);
    await wait(2);
    last_activity = current_activity;
    continue
} else if(current_activity == 'com.ali.user.mobile.login.ui.UserLoginActivity') {
    console.log(`[STATUS][IDLEFISH] Currently on the login menu, tapping the X button...`);
    await android_tap_element_at_selector(`node[content-desc="返回"]`);
    await wait(1);
    last_activity = current_activity;
    continue
} else if(current_activity == 'com.idlefish.flutterbridge.flutterboost.boost.FishFlutterBoostActivity') {
    console.log(`[STATUS][IDLEFISH] Currently on the search overlay menu, entering in a search...`);
    await android_enter_text('iphone');
    await android_hit_button('enter');
    await wait(8);
    last_activity = current_activity;
    continue
} else if(current_activity == 'com.alibaba.wireless.security.open.middletier.fc.ui.ContainerActivity') {
    console.log(`[STATUS][IDLEFISH] Currently on the Idlefish CAPTCHA, solving it...`);
    const { stdout, stderr } = await exec(`${process.env.ADB_PATH} shell "su -c \\"/data/local/tmp/mysendev
    await wait(3);
} else {
    console.log(`[STATUS][IDLEFISH] Uh oh, I'm lost! New menu I've not seen before!`);
    break
}
```

New seller enumeration

Rooted Android with Xianyu



Frida API signing server







Searches routed via residential proxies




ThinkCentre

We have the **relevant sellers**, but not the **items**…

Limited non-app endpoints



Kind of…



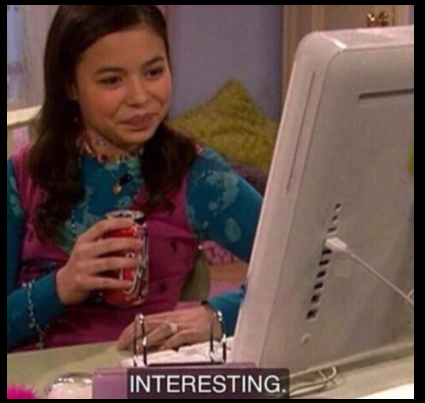
There are "web preview" pages for sellers and items to get people to download the app.

Problem: Rate limiting is *severe.* Just a few previews and it forces you to log in for more.

Doing this at **scale** requires a **ton of IPs**, which is **expensive** even for budget proxy networks.



```
Matthews-MacBook-Pro:~ mandatory$ dig AAAA h5api.m.goofish.com

; <<>> DiG 9.10.6 <<>> AAAA h5api.m.goofish.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60646
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;h5api.m.goofish.com.           IN      AAAA

;; ANSWER SECTION:
h5api.m.goofish.com.    300     IN      CNAME   dualstack-zb-4499.alibaba.alibaba-inc.com.
dualstack-zb-4499.alibaba.alibaba-inc.com. 300 IN CNAME dualstack-zb-4499.alibaba.alibaba-inc.com.gds.alibabadns.com.
dualstack-zb-4499.alibaba.alibaba-inc.com.gds.alibabadns.com. 120 IN AAAA 2408:4001:f00::b9
dualstack-zb-4499.alibaba.alibaba-inc.com.gds.alibabadns.com. 120 IN AAAA 2408:4001:f00::92
dualstack-zb-4499.alibaba.alibaba-inc.com.gds.alibabadns.com. 120 IN AAAA 2408:4001:f00::198
dualstack-zb-4499.alibaba.alibaba-inc.com.gds.alibabadns.com. 120 IN AAAA 2408:4001:f00::17c

;; Query time: 45 msec
;; SERVER: 100.100.100.100#53(100.100.100.100)
;; WHEN: Sun Nov 26 18:03:40 PST 2023
;; MSG SIZE  rcvd: 283

Matthews-MacBook-Pro:~ mandatory$
```



ARIN

American Registry for Internet Numbers



RSP Service Categories and Fees

The table below displays the annual Registration Services Plan fee per service category for ARIN customers. The aggregate block size consists of the total IPv4 or IPv6 resource holdings of an organization.

Service Category	Fee	IPv4 Aggregate Block Size	IPv6 Aggregate Block Size
3X-Small*	$250	/24 or smaller	/40 or smaller
2X-Small	$500	Larger than /24, up to and including /22	Larger than /40, up to and including /36

**There is a temporary IPv6 fee waiver for organizations in the 3X-Small service category allowing for more IPv6 resources than normal while still remaining in the 3X-Small service category and paying only the 3X-Small service category fee. A 3X-Small organization may receive registry services for up to a /36 of total IPv6 space and remain in the 3X-Small service category rather than being charged the 2X-Small service category fee. This waiver will expire 31 December 2026.*

Stargate

Stargate runs TCP SOCKS proxies on different ports egressing on sequential IPs in the same subnet. This requires the host running stargate to have the subnet routed directly to it.

If you have an IPv6 subnet, stargate can allow you to make full use of it by any program that can speak SOCKS.

Usage

```
Usage of ./stargate: [OPTION]... CIDR
        CIDR example: "192.0.2.0/24"
OPTIONS:
  -listen string
        IP to listen on (default "localhost")
  -port uint
        first port to start listening on
  -random uint
        port to use for random proxy server
  -verbose
        enable verbose logging
```

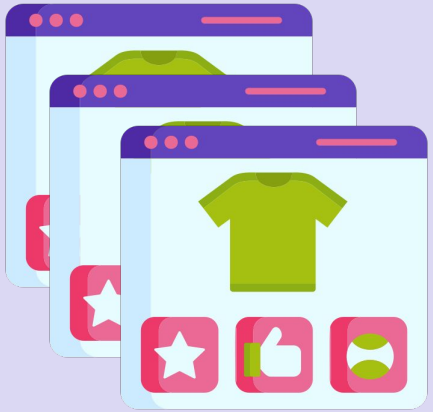


https://github.com/lanrat/stargate

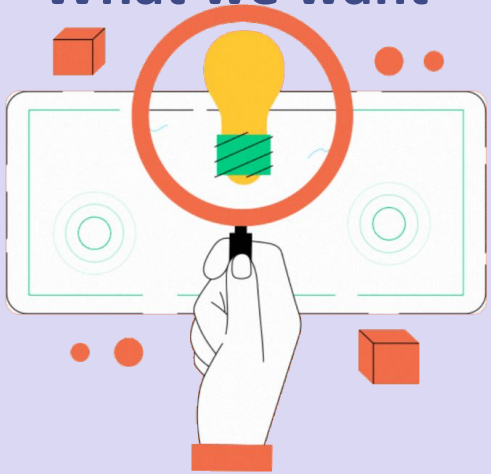
Anyways…Let's just call it solved.

Challenge #2: Secrets are hidden in listings

What we have



What we want





Property of Sharp HealthCare

iPad



Tesseract OCR














```
bash-3.2$ tesseract ~/Downloads/test-ocr.jpeg out && cat out.txt; file out.txt
Estimating resolution as 153
out.txt: empty
```



Google Vision API

Objects | Labels | Logos | **Text** | Properties | Safe Search



+Page 1

+Block 1

Property of Sharp Heal thCare

+Block 2

iPad

+Block 3

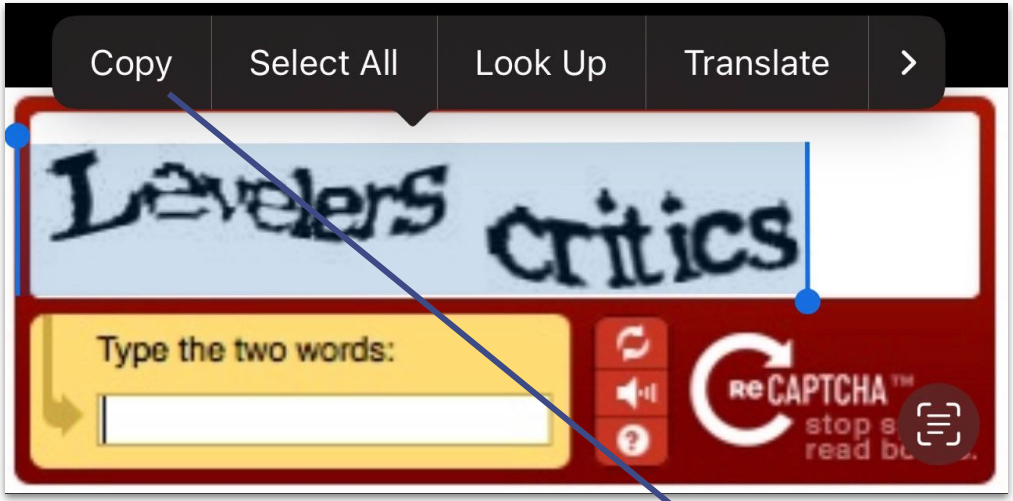
CA A



Feature	Price per 1000 units		
	First 1000 units/month	Units 1001 - 5,000,000 / month	Units 5,000,001 and higher / month
Label Detection	Free	$1.50	$1.00
Text Detection	Free	$1.50	$0.60

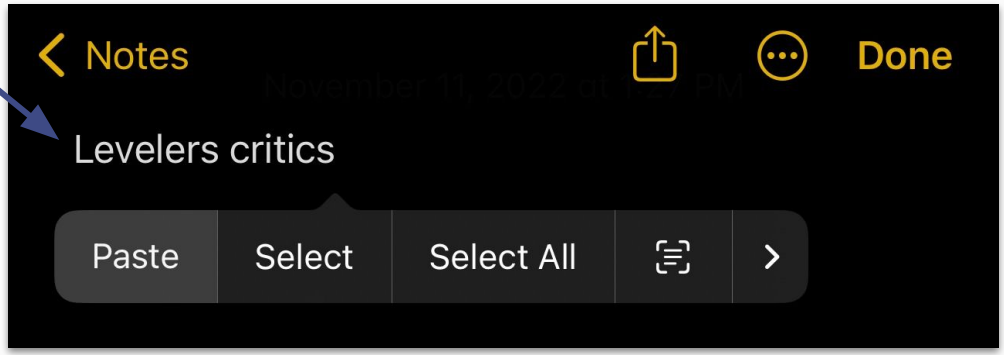
$0.01
per 7 images

$1,500
for 1M images





iOS OCR to the rescue



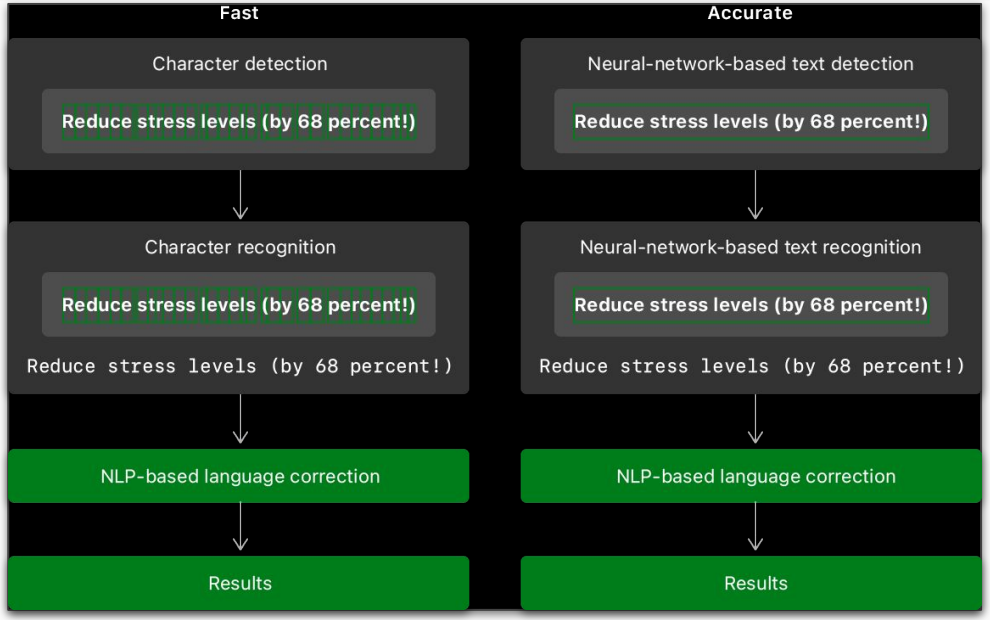
A **quick experiment** showed that this was **automatable**, **fast**, and **reliable**!

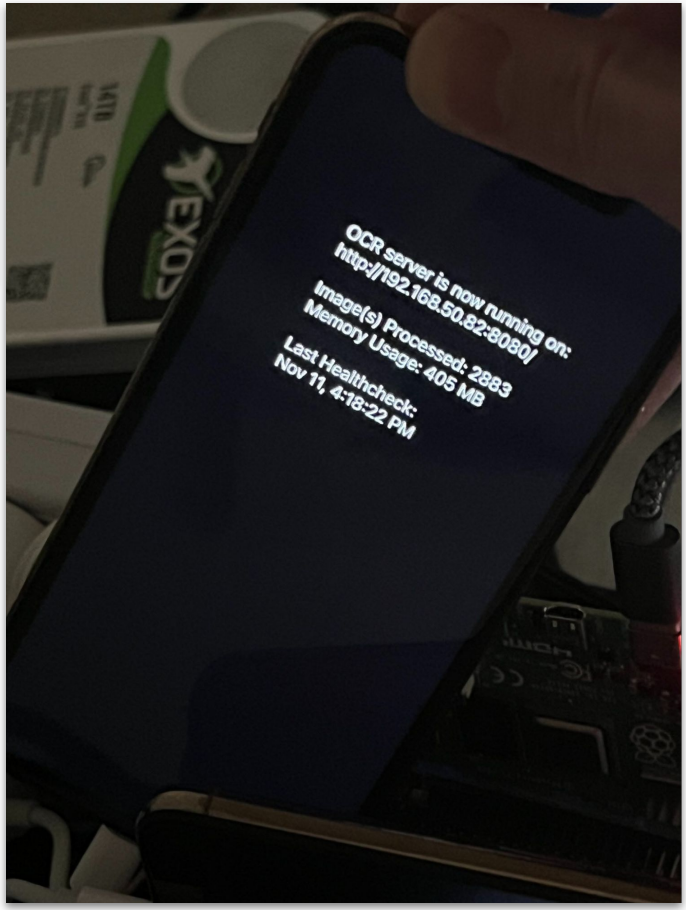
Framework

Vision

Apply computer vision algorithms to perform a variety of tasks on input images and video.

iOS 11.0+ | iPadOS 11.0+ | macOS 10.13+ | Mac Catalyst 13.0+ | tvOS 11.0+ | visionOS 1.0+ Beta





Best of all, it was cost effective!



Sold Nov 3, 2022

Apple iPhone SE (2nd Gen.) 64GB Black Cricket Excellent Condition

Pre-Owned · Apple iPhone SE (2nd Generation) · 3 GB · Cricket Wireless

$39.99

Top Rated Plus

Buy It Now

Free shipping

Free returns

View similar active items

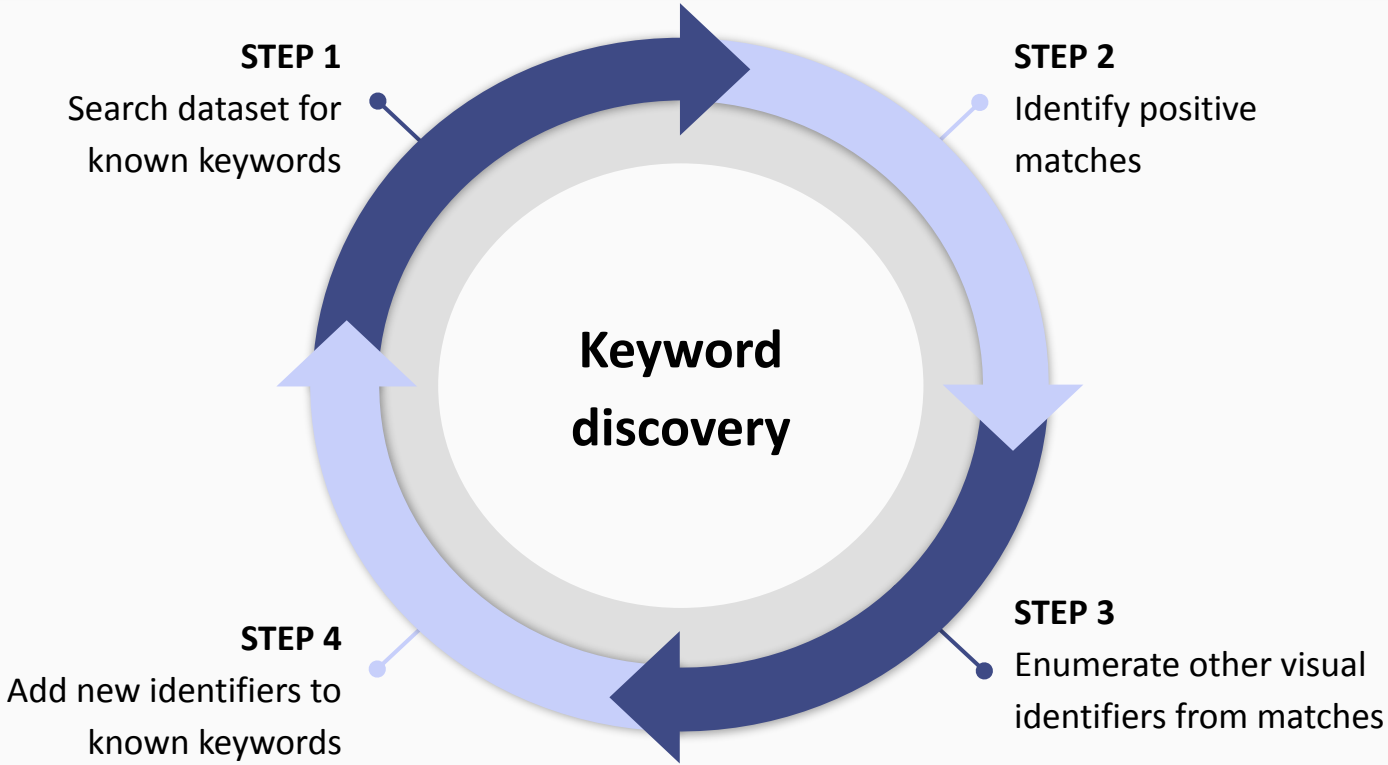
Sell one like this



Roughly **~50/sec** for large HD images with lots of text

Low power draw on efficient mobile GPUs

Challenge #3: Knowing what we're looking for



Search Query | EVT | [Images] Idlefish (闲鱼) | Simple Query

"Scannables" Search | C02* | Has *any* scannable?

-apple (86) -doch (59) -pre-swdl (57) -wtch (48) -evt (46) -jh3/4/5/6 (35) -jh314 (35) -iphone (31) -jh3/4a-evt-463 (29) -jh3/4 (27) -pro (26) -8295 (24)
-186 (21) -6586 (21) -0639 (21) -tlc (17) -dock (17) -tnc (16) -9075 (15) -463 (13) -toshiba (13) -carrier-jhf (13) -x241 (12) -000 (12) -carrier (12)
-1122 (11) -256gb (11) -jhf (11) -jh3j4 (10) -max (10)

Around ~200 results displayed (limited to 200).



OCR Text

```
1-SAS-PHI JH4 -EVT-A 43.1 LY00997
3H4-EVT-A V3.1 LY00994 BTN X241
```

Listing (https://market.m.taobao.com/app/idleFish-F2e/fish-pc/web/detail.html?id=751044586379) [Mobile App Link]

First scraped on November 24th 2023, 7:54:58 pm



OCR Text

```
command Option ciclota return
shift FX-EVT-TC-A-ANSI-MesaDoE1-2
```

Listing (https://market.m.taobao.com/app/idleFish-F2e/fish-pc/web/detail.html?id=750467941664) [Mobile App Link]

First scraped on November 21st 2023, 8:43:02 pm



OCR Text

```
LA2BD-LG-EVT STERIA Z S7 45mm* A
186 0639 6586 Ei##*
```

Listing (https://market.m.taobao.com/app/idleFish-F2e/fish-pc/web/detail.html?id=750063101964) [Mobile App Link]

First scraped on November 19th 2023, 10:24:59 pm



Enumerated Xianyu sellers



IPv6 randomization SOCKS5 proxy





Cloudflare worker proxy



Scraped listings + OCRed image results



Data lake search server

Row data synced



elasticsearch



iPhone OCR Farm

Scraped images to be OCRed



Target site crawler/scraper

Scraped images to be stored



Scale of data collected

Listings Scraped

~50M

Images OCRed

~250M

Challenge #3.5: Getting stuff out of China

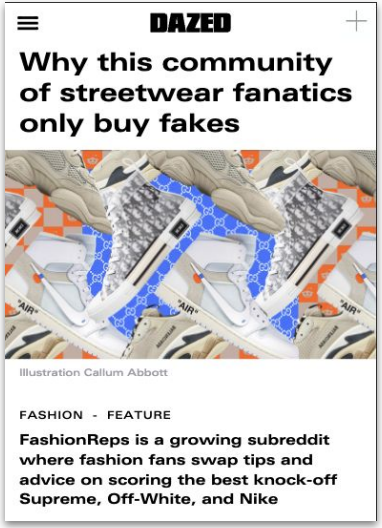
Only Domestic Shipping



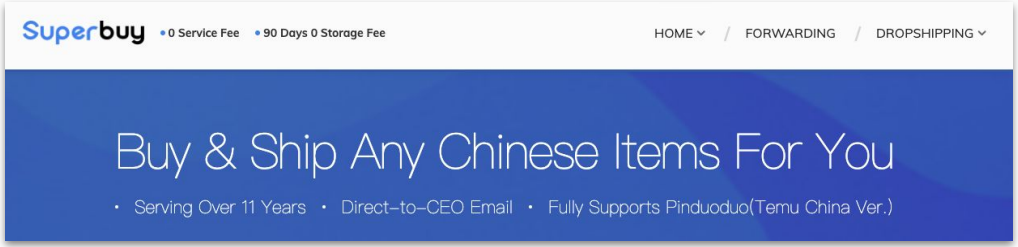
Export Challenges

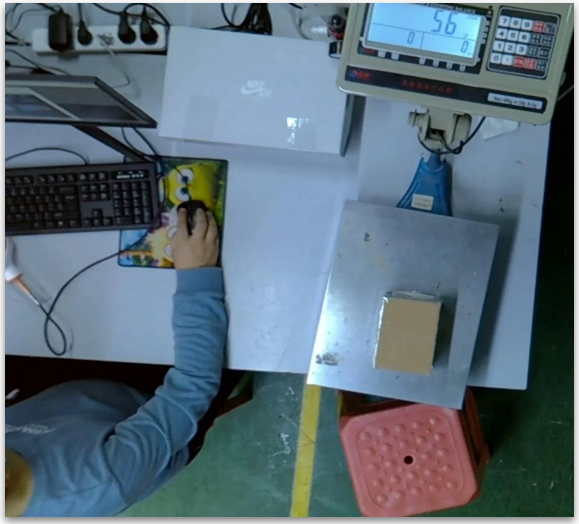


/r/FashionReps & 1:1 drip dropshipping







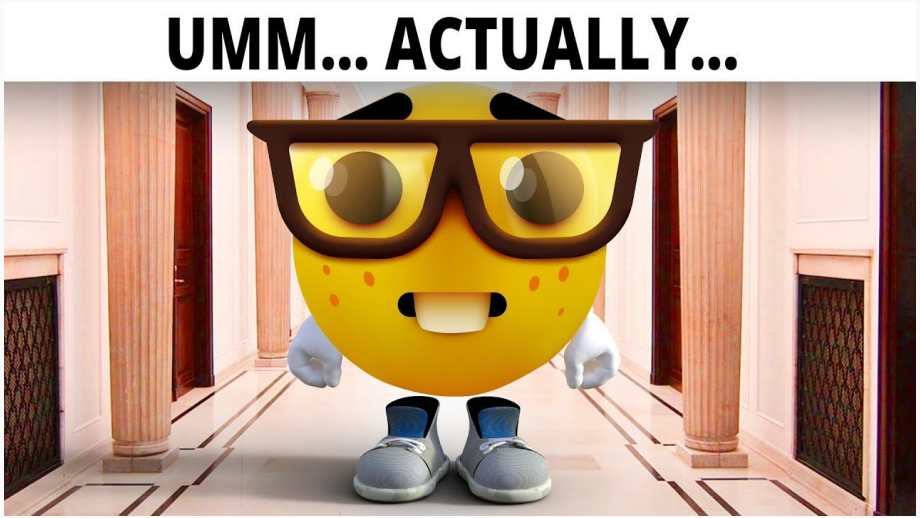




Loot

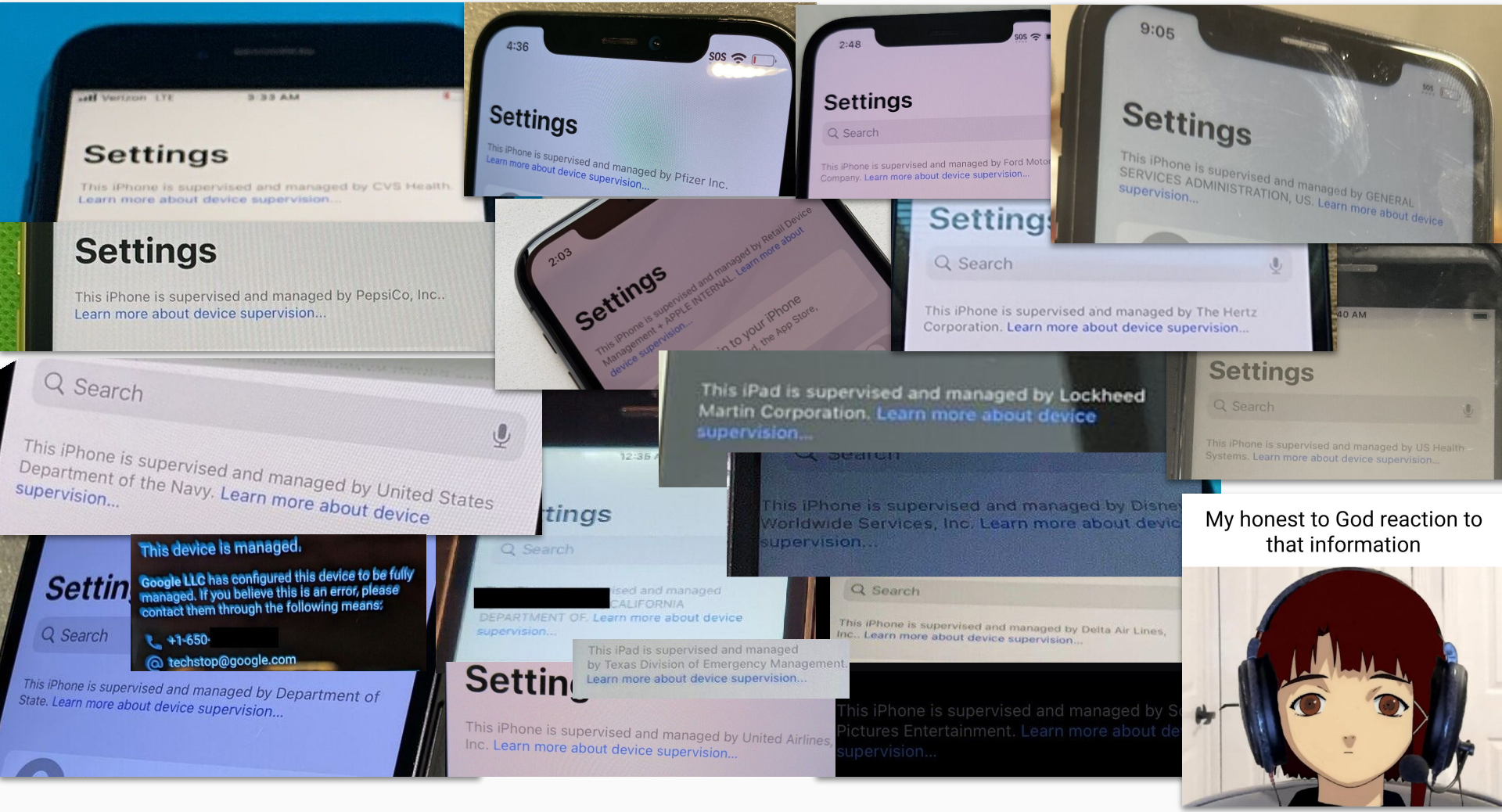


Employee Devices

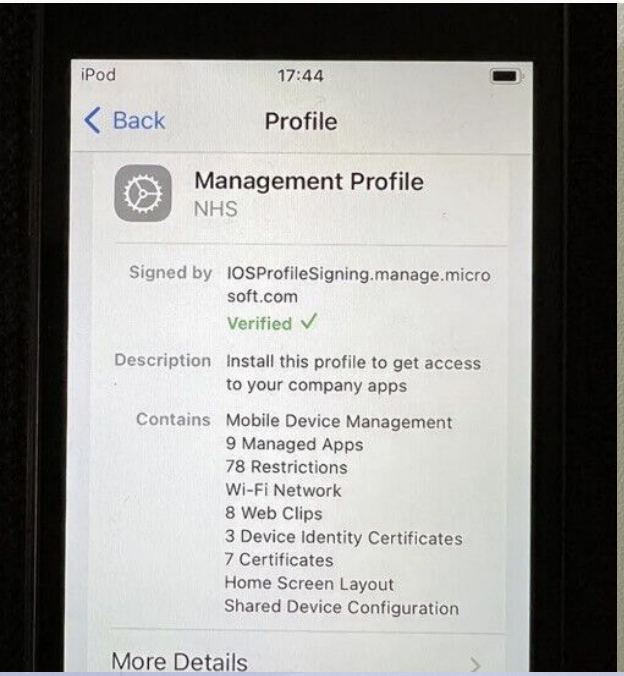


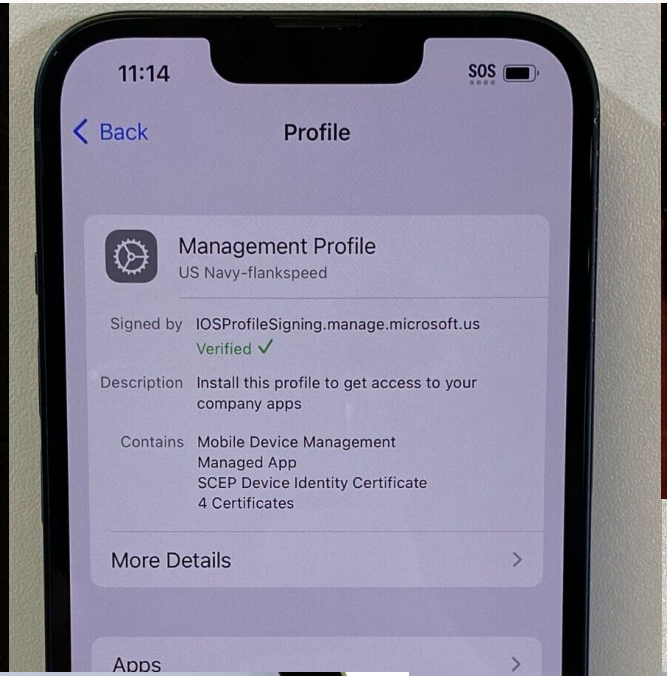
But first, let's dispel some ***"well actually..."***

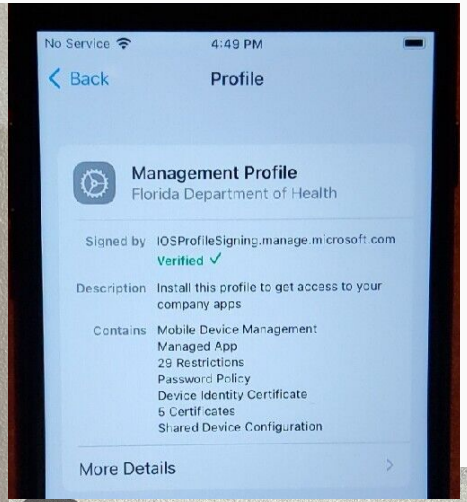
"OK, but they're **probably all locked** and require a password to access them!"


Settings
This iPhone is supervised and managed by CVS Health.
Learn more about device supervision...
4:36
Settings
This iPhone is supervised and managed by Pfizer Inc.
Learn more about device supervision...
2:48
Settings
Search
This iPhone is supervised and managed by Ford Motor Company. Learn more about device supervision...
9:05
Settings
This iPhone is supervised and managed by GENERAL SERVICES ADMINISTRATION, US. Learn more about device supervision...
Settings
This iPhone is supervised and managed by PepsiCo, Inc..
Learn more about device supervision...
2:03
Settings
This iPhone is supervised and managed by Retail Device Management + APPLE INTERNAL. Learn more about device supervision...
Settings
Search
This iPhone is supervised and managed by The Hertz Corporation. Learn more about device supervision...
40 AM
Settings
Search
This iPhone is supervised and managed by US Health Systems. Learn more about device supervision...
Search
This iPhone is supervised and managed by United States Department of the Navy. Learn more about device supervision...
This iPad is supervised and managed by Lockheed Martin Corporation. Learn more about device supervision...
This iPhone is supervised and managed by Disney Worldwide Services, Inc. Learn more about device supervision...
This device is managed.
Google LLC has configured this device to be fully managed. If you believe this is an error, please contact them through the following means:
+1-650-
techstop@google.com
Search
This iPhone is supervised and managed by Department of State. Learn more about device supervision...
Search
This iPhone is supervised and managed by Delta Air Lines, Inc.. Learn more about device supervision...
This iPad is supervised and managed by Texas Division of Emergency Management
Learn more about device supervision...
This iPhone is supervised and managed by United Airlines, Inc. Learn more about device supervision...
This iPhone is supervised and managed by Pictures Entertainment. Learn more about device supervision...
My honest to God reaction to that information

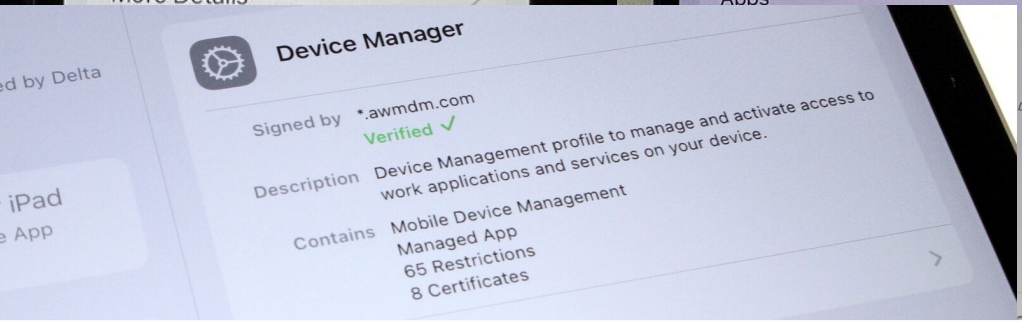
"Sure, but that doesn't mean there's **anything sensitive** on the devices!"


iPod
17:44
Back
Profile
Management Profile
NHS
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
9 Managed Apps
78 Restrictions
Wi-Fi Network
8 Web Clips
3 Device Identity Certificates
7 Certificates
Home Screen Layout
Shared Device Configuration
More Details

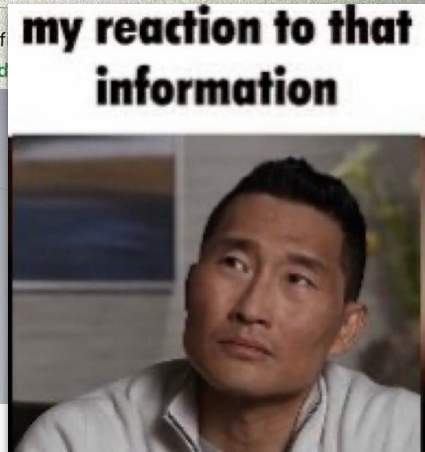

11:14
SOS
Back
Profile
Management Profile
US Navy-flankspeed
Signed by
IOSProfileSigning.manage.microsoft.us
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
Managed App
SCEP Device Identity Certificate
4 Certificates
More Details
Apps


No Service
4:49 PM
Back
Profile
Management Profile
Florida Department of Health
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
Managed App
29 Restrictions
Password Policy
Device Identity Certificate
5 Certificates
Shared Device Configuration
More Details


Management Profile
Rhode Island Disaster Medical Assistance Team
Signed by
IOSProf
Verified


Device Manager
Signed by
*.awmdm.com
Verified
Description
Device Management profile to manage and activate access to work applications and services on your device.
Contains
Mobile Device Management
Managed App
65 Restrictions
8 Certificates


Management Profile
Fresenius Medical Care
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
4 Managed Apps
6 Restrictions
Password Policy
Wi-Fi Network
2 Web Clips
Device Identity Certificate
5 Certificates
Home Screen Layout


my reaction to that information


[redacted] State Auditor Office
Property of WeWork
If found please email
asset.tracking@wework.com
[redacted]
WEB: http://www.Navy311
https://www.Navy311
TEXT: Type Navy311@navy.mil
CHAT: Via Navy 311 unclassified
Property of NBCUniversal
Serial No:
[redacted]
UNIVERSAL TELEVISION PRODUCTION
Property of
Aruba Networks
A5987
PROPERTY OF
Intuit
This Mac is the property of AppleCare and has been provided by Equipment Operations.
Shut Down
Restart
APPLE DEVELOPMENT TEAM
[redacted]
Property of
MoneyGram
[redacted]
For Support, please contact the Helpdesk:
Toll Free:
Global:
1-800
1-952
TOUGHBOOK
Peloton Interactive
125 W 25th Street 11th fl, NY, NY 10001
IF FOUND PLEASE EMAIL
[redacted]@onepeloton.com
PROPERTY OF U.S.
ENVIRONMENTAL PROTECTION
AGENCY
Model: 200
[redacted]
HSARPA ONLY
Property of City of Albuquerque
If found please call [redacted]
This medium is
UNCLASSIFIED
PROPERTY OF APPLE COMPUTER, INC.
EXPENSED EQUIPMENT
[redacted]
If found or for urgent security matters
Please call
+1 (202)
[redacted]
intel
2.5A Max
This product complies with the requirements of European Directives 73/23/EEC
northern telecom
DO NOT REMOVE
[redacted]
PROPERTY OF NORTHERN TELECOM
Property of Pandora
[redacted]@pandora.com
[redacted]
0
Property of American Airlines
If found please contact the Help Desk
[redacted]
USACE-ERDC
US GOVERNMENT PROPERTY
[redacted]
WARRANTY EXPIRATION: 3/2012
FDA
PROPERTY OF FOOD AND DRUG ADMINISTRATION
IF FOUND PLEASE CONTACT 1-[redacted]



The Time Capsule

2TB Time Capsule listed on eBay UK



$ Have one to sell? Sell now

APPLE A1302 TIME CAPSULE 2TB - WHITE (R6GQ)

Condition: **Used**

"Pre-owned but in fair condition. This Time Capsule was part of an office clearance. It has been"... Read more

Ended: May 29, 2023 11:30:01 PDT

Winning bid: **GBP 29.00**

Approximately US $36.87

[12 bids]

Add to List

Shipping: **GBP 31.07 (approx US $39.50)** Expedited Shipping to United States via eBay's Global Shipping Program . See details

Located in: Reading, United Kingdom

Import charges: **Free** amount confirmed at checkout

Delivery: Estimated between **Fri, Jul 14** and **Wed, Jul 19** to 94041

Includes **international tracking**

Returns: 30 days returns. Buyer pays for return shipping. See details

Payments: PayPal, G Pay, VISA, Mastercard, AMEX

Earn up to 5x points when you use your eBay Mastercard®. Learn more

International shipping and import charges paid to Pitney Bowes Inc. Learn more

Shop with confidence

eBay Money Back Guarantee

Get the item you ordered or your money back.

Learn more

Seller information

amafordsolutionsltd (11460)

99.9% positive feedback

Save seller

Contact seller

Visit store

See other items

Registered as a Business Seller


PROPERTY OF APPLE COMPUTER, INC.
EXPENSED EQUIPMENT
EE089729
Designed by Apple in California Assembled in China Model Number: A1302
Complies with the Canadian ICES-003 Class B specifications. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation. 100-240 V~, 50-60 Hz, 1A TM and © 2008 Apple Inc. All rights reserved.
Serial No: 6F93101K6GQ
Time Capsule (2TB)
FCC ID: BCGA1302 IC: 579C-A1302
Ethernet ID: 002436A43C9C
AirPort ID 2.4GHz: 0025BCBD4515
AirPort ID 5.0GHz: 0025BCBD4516

APPLE A1302 TIME CAPSULE 2TB - WHITE (R6GQ)

Condition

Pre-owned but in fair condition. This Time Capsules was part of an office clearance. It has been Powered on and lights up as expected however it has not been tested beyond this as we do not have the applicable cables. There are some noticeable, cosmetic only, marks/scratches/stickers to the front and back of the body. No warranty as untested.

New Apple Campus in London's Battersea Power Station to Open in Early 2023

Monday September 26, 2022 8:09 am PDT by Hartley Charlton

Apple will open its London office space in Battersea Power Station early next year, Apple CEO Tim Cook today announced upon a visit to the all-new campus.



Render of the redeveloped Battersea campus

Congratulations, you won the auction! | View order details

APPLE A1302 TIME CAPSULE 2TB - WHITE (R6GQ) See original listing



Condition: **Used**
"*Pre-owned but in fair condition. This Time Capsule was part of an office clearance. It has been*" ... Read more

Ended: May 29, 2023, 11:30AM

Winning bid: **GBP 29.00** [12 bids]
Approximately **US $36.87**

Shipping: **GBP 31.07** Expedited Shipping to United States

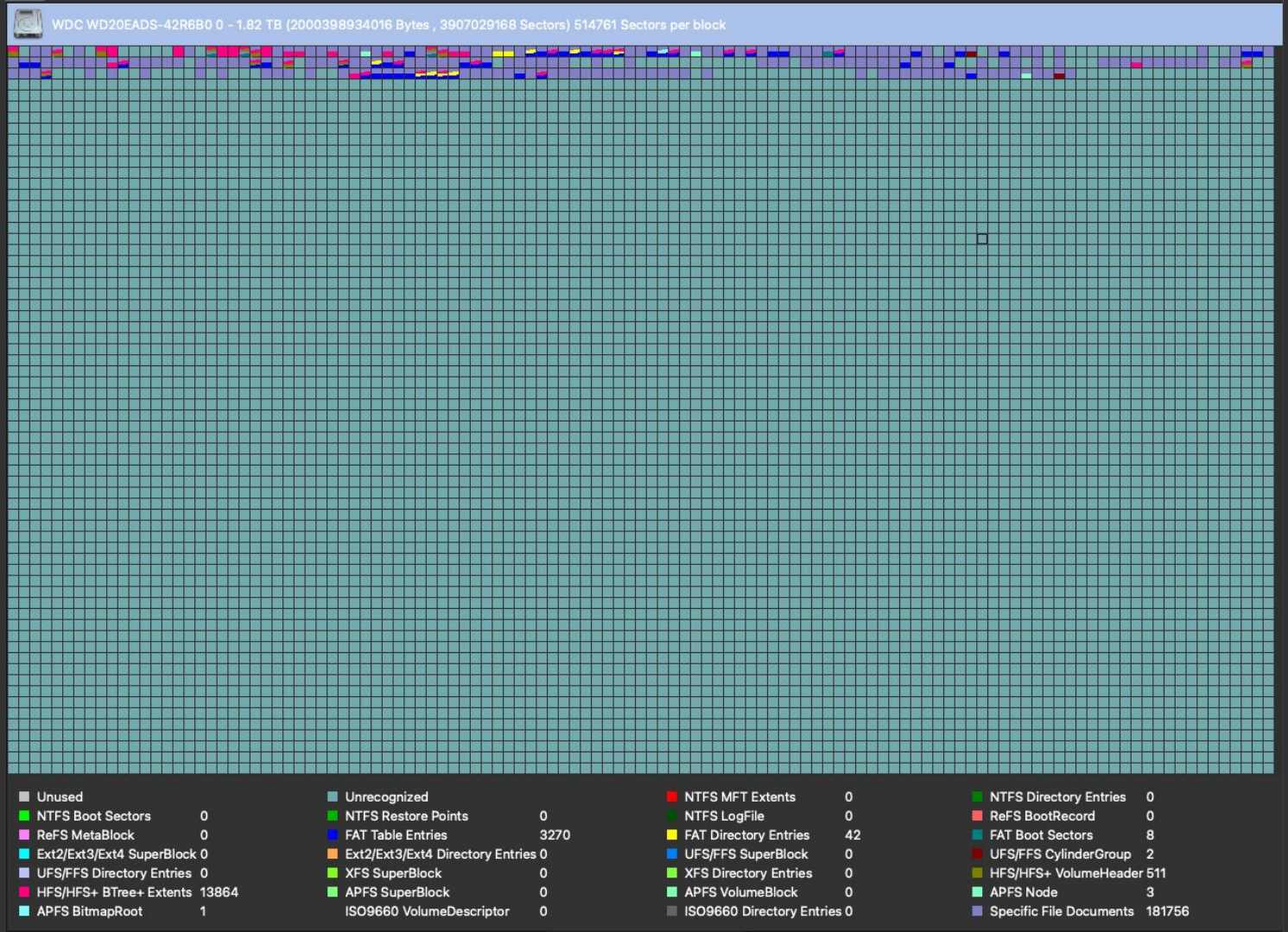
Located in: Reading, United Kingdom

Seller: **amafordsolutionsltd** (11460 ⭐) | Seller's other items

Sell one like this


UGREEN
www.ugreen.com
Model:20231
USB 3.0 to SATA III Hard Drive Adapter
CE FC RoHS
Ugreen Group Limited
Made in China

Bad news, drive appears **empty**…
…or **is it**?


WDC WD20EADS-42R6B0 0 - 1.82 TB (2000398934016 Bytes , 3907029168 Sectors) 514761 Sectors per block
Unused
NTFS Boot Sectors 0
ReFS MetaBlock 0
Ext2/Ext3/Ext4 SuperBlock 0
UFS/FFS Directory Entries 0
HFS/HFS+ BTree+ Extents 13864
APFS BitmapRoot 1
Unrecognized
NTFS Restore Points 0
FAT Table Entries 3270
Ext2/Ext3/Ext4 Directory Entries 0
XFS SuperBlock 0
APFS SuperBlock 0
ISO9660 VolumeDescriptor 0
NTFS MFT Extents 0
NTFS LogFile 0
FAT Directory Entries 42
UFS/FFS SuperBlock 0
XFS Directory Entries 0
APFS VolumeBlock 0
ISO9660 Directory Entries 0
NTFS Directory Entries 0
ReFS BootRecord 0
FAT Boot Sectors 8
UFS/FFS CylinderGroup 2
HFS/HFS+ VolumeHeader 511
APFS Node 3
Specific File Documents 181756

28 hours later


mass appeal
So that was a fucking lie.

Internal credentials

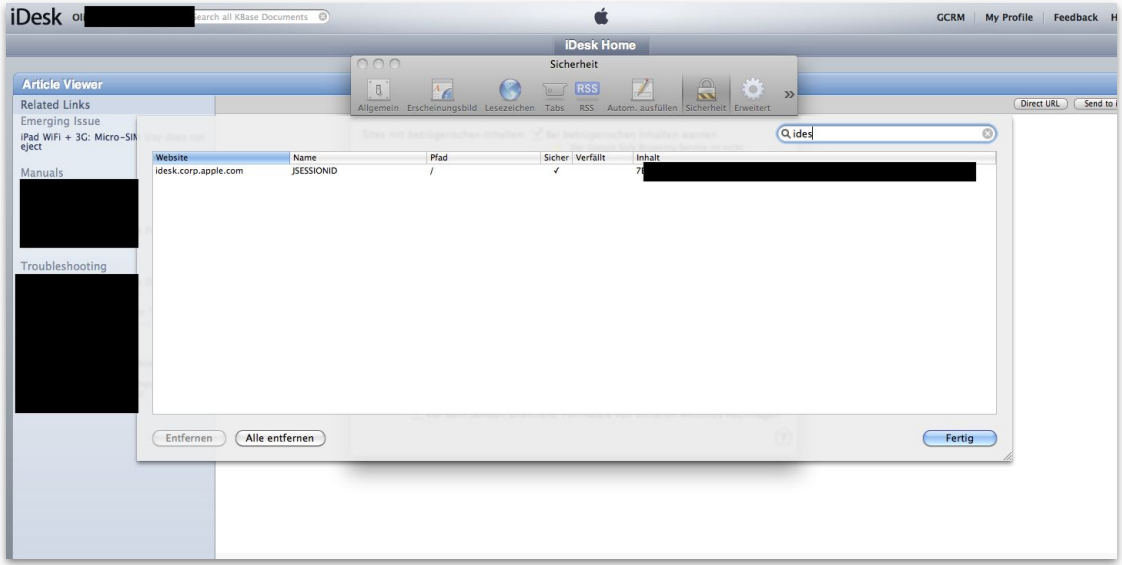
AppleConnect Credentials

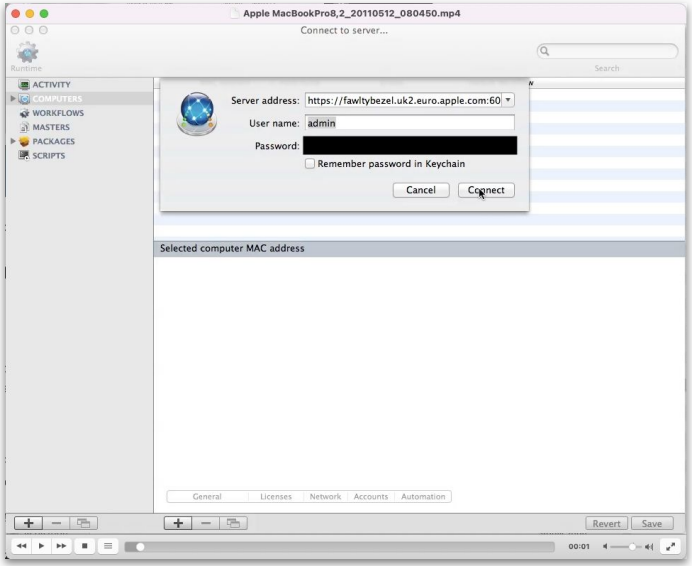
Your AppleConnect account is the key to nearly every application, website or service within Apple. AppleConnect's single sign-on feature means that you sign in once and the rest of the services you access open automatically, without having to re-enter your password. You control your personal level of automatic access in AppleConnect's preferences.

Account Name: ay[redacted]
Password: AY[redacted]

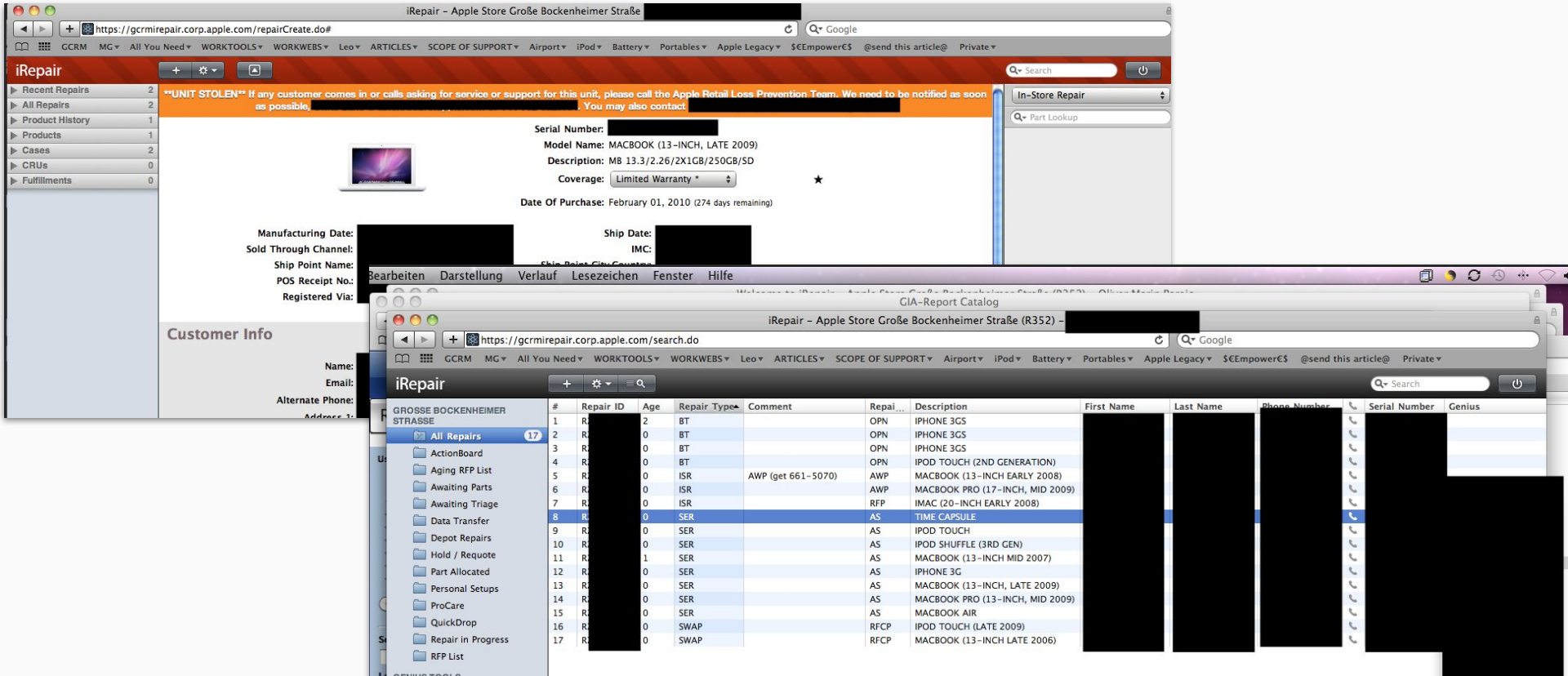
When you first sign in, you will be prompted to change your password. Be sure to select a password that is easy for you to remember but difficult for others to guess. Password selection tips can be found on IS&T Web.

Visit IS&T Web's AppleConnect account page here .

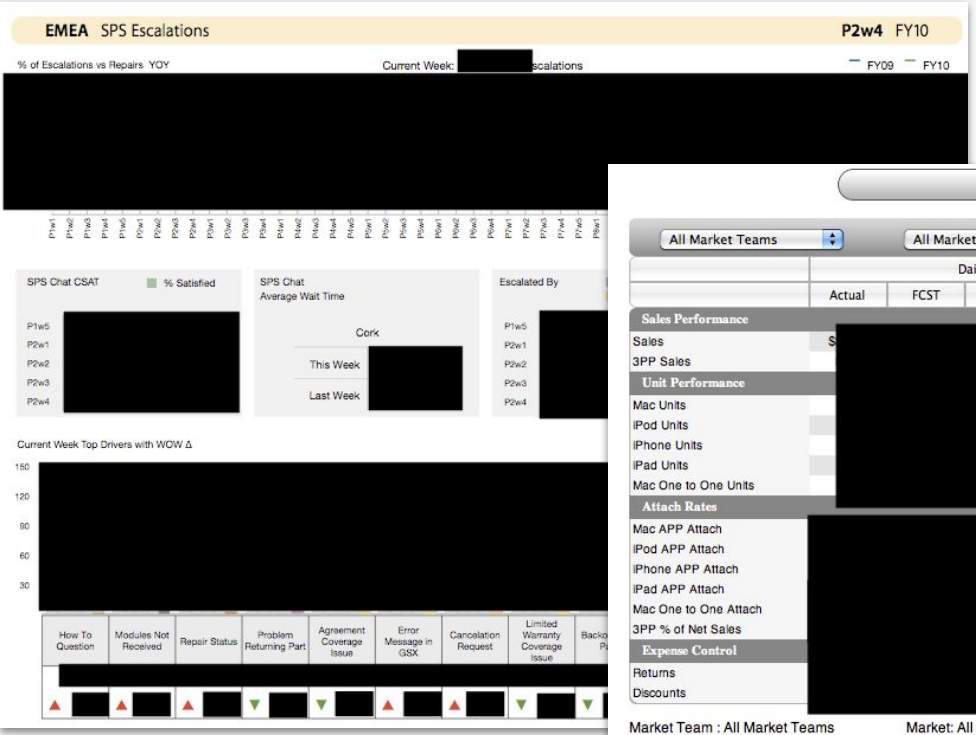


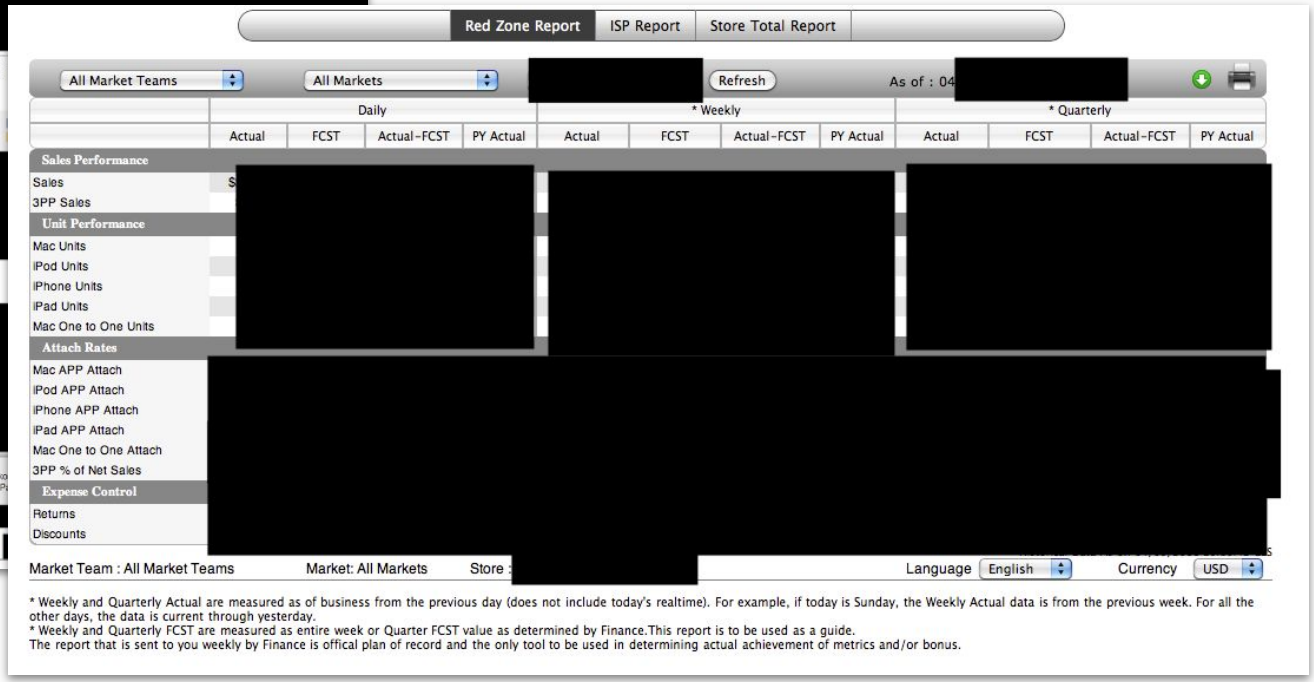


Internal support tickets



Sales reports





Internal documentation, apps, repair guides, etc

Genius Room Standards Guide

Version 2.0

February 15, 2010

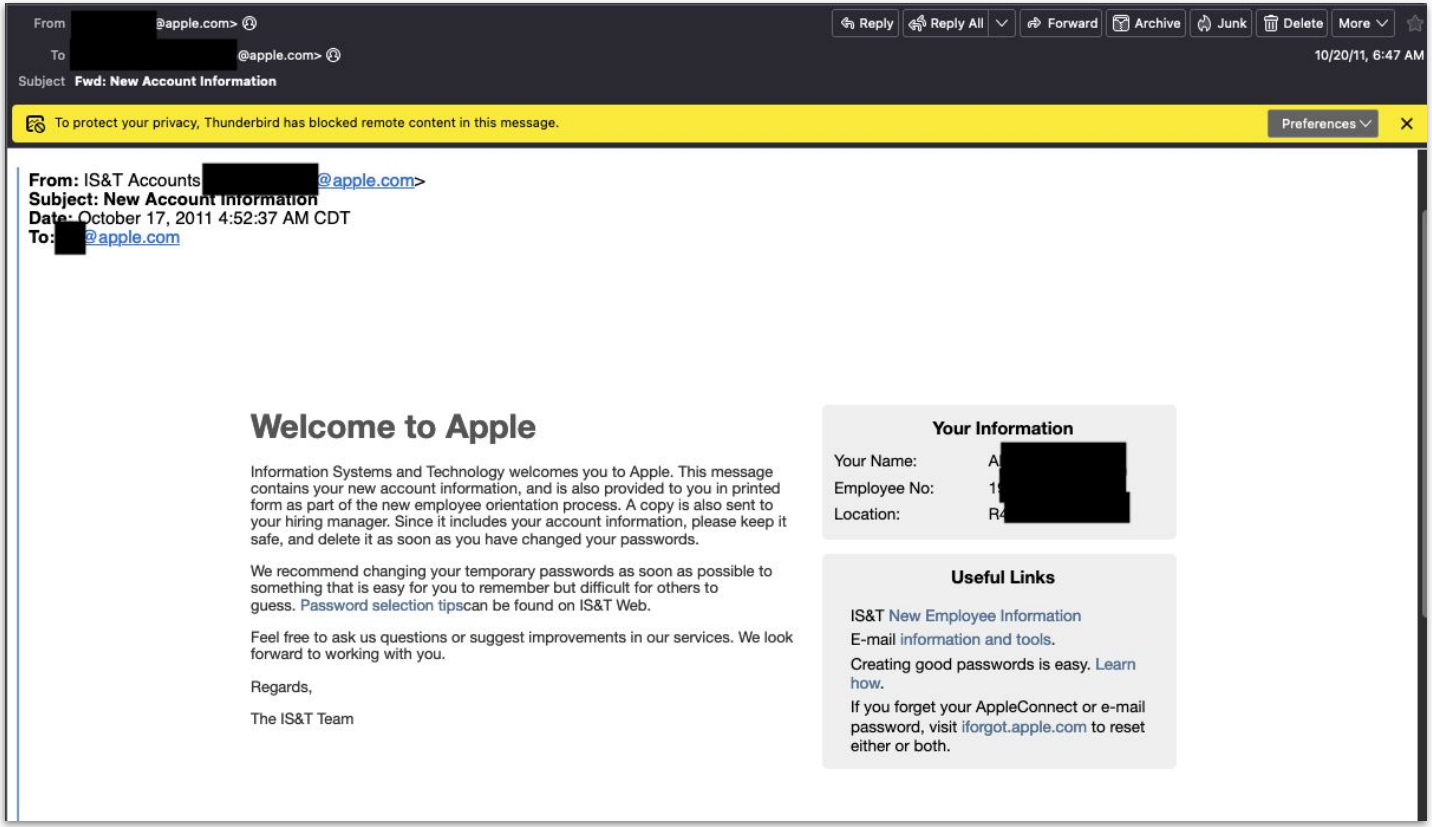
© 2009 Apple Inc. All Rights Reserved.

Apple Internal Use Only





Internal emails



From [redacted]@apple.com>
To [redacted]@apple.com>
Subject **Fwd: New Account Information**

Reply | Reply All | Forward | Archive | Junk | Delete | More

10/20/11, 6:47 AM

To protect your privacy, Thunderbird has blocked remote content in this message. Preferences

From: IS&T Accounts [redacted]@apple.com>
Subject: New Account Information
Date: October 17, 2011 4:52:37 AM CDT
To: [redacted]@apple.com

Welcome to Apple

Information Systems and Technology welcomes you to Apple. This message contains your new account information, and is also provided to you in printed form as part of the new employee orientation process. A copy is also sent to your hiring manager. Since it includes your account information, please keep it safe, and delete it as soon as you have changed your passwords.

We recommend changing your temporary passwords as soon as possible to something that is easy for you to remember but difficult for others to guess. Password selection tipscan be found on IS&T Web.

Feel free to ask us questions or suggest improvements in our services. We look forward to working with you.

Regards,

The IS&T Team

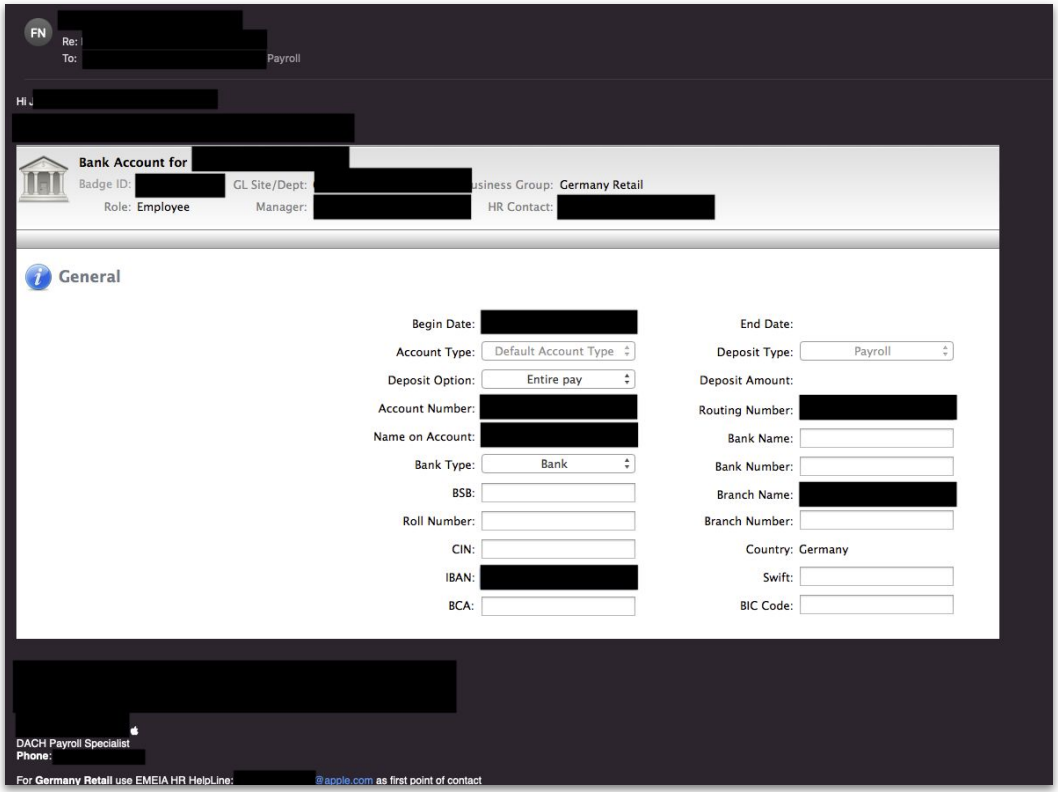
Your Information

Your Name: A[redacted]
Employee No: 1[redacted]
Location: R[redacted]

Useful Links

IS&T New Employee Information
E-mail information and tools.
Creating good passwords is easy. Learn how.
If you forget your AppleConnect or e-mail password, visit iforgot.apple.com to reset either or both.

Bank account details



FN [redacted]
Re: [redacted]
To: [redacted] Payroll

Hi [redacted]

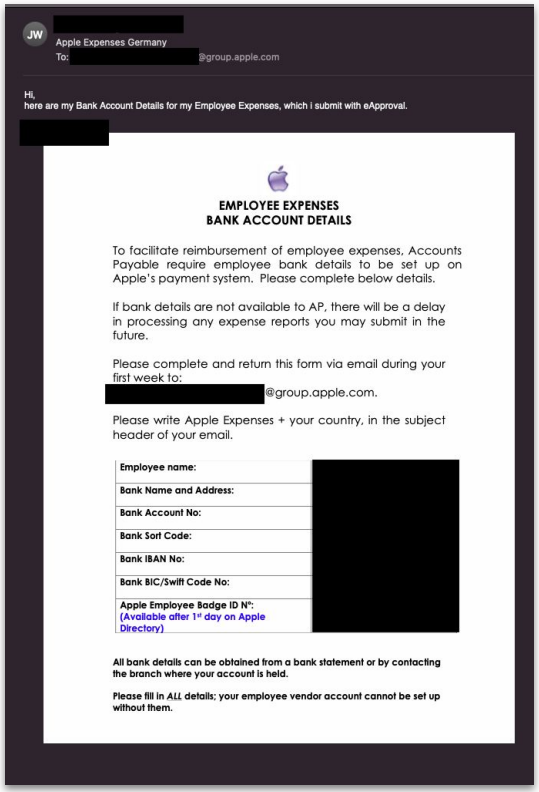
[redacted]

Bank Account for [redacted]
Badge ID: [redacted] GL Site/Dept: [redacted] Business Group: Germany Retail
Role: Employee Manager: [redacted] HR Contact: [redacted]

General

Begin Date:	[redacted]	End Date:	
Account Type:	Default Account Type	Deposit Type:	Payroll
Deposit Option:	Entire pay	Deposit Amount:	
Account Number:	[redacted]	Routing Number:	[redacted]
Name on Account:	[redacted]	Bank Name:	
Bank Type:	Bank	Bank Number:	
BSB:		Branch Name:	[redacted]
Roll Number:		Branch Number:	
CIN:		Country:	Germany
IBAN:	[redacted]	Swift:	
BCA:		BIC Code:	

[redacted]
DACH Payroll Specialist
Phone: [redacted]
For **Germany Retail** use EMEIA HR HelpLine: [redacted]@apple.com as first point of contact



JW [redacted]
Apple Expenses Germany
To: [redacted]@group.apple.com

Hi,
here are my Bank Account Details for my Employee Expenses, which i submit with eApproval.

[redacted]

EMPLOYEE EXPENSES
BANK ACCOUNT DETAILS

To facilitate reimbursement of employee expenses, Accounts Payable require employee bank details to be set up on Apple's payment system. Please complete below details.

If bank details are not available to AP, there will be a delay in processing any expense reports you may submit in the future.

Please complete and return this form via email during your first week to:
[redacted]@group.apple.com.

Please write Apple Expenses + your country, in the subject header of your email.

Employee name:	[redacted]
Bank Name and Address:	
Bank Account No:	
Bank Sort Code:	
Bank IBAN No:	
Bank BIC/Swift Code No:	
Apple Employee Badge ID N°: (Available after 1st day on Apple Directory)	

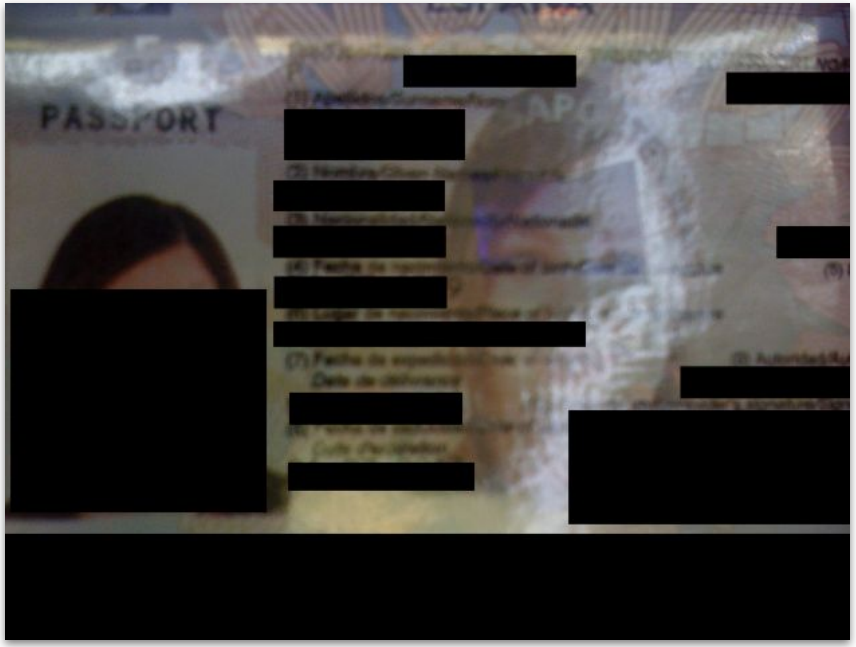
All bank details can be obtained from a bank statement or by contacting the branch where your account is held.

Please fill in *ALL* details; your employee vendor account cannot be set up without them.

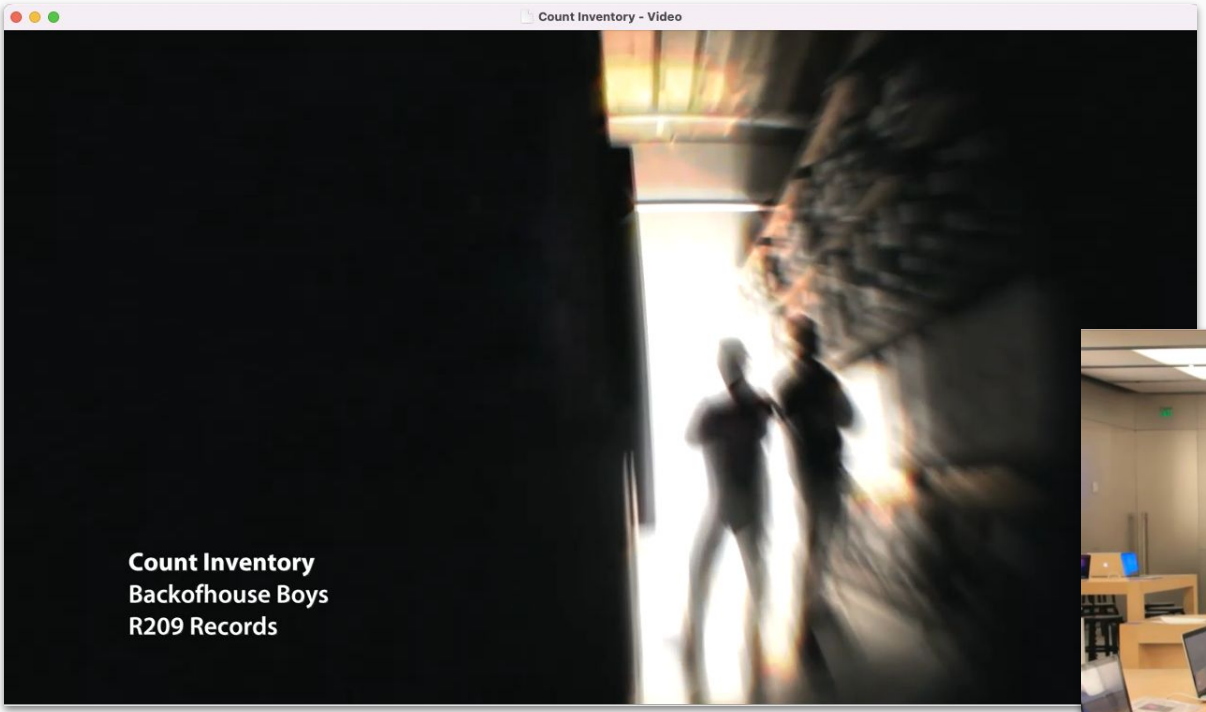
Passport & ID scans







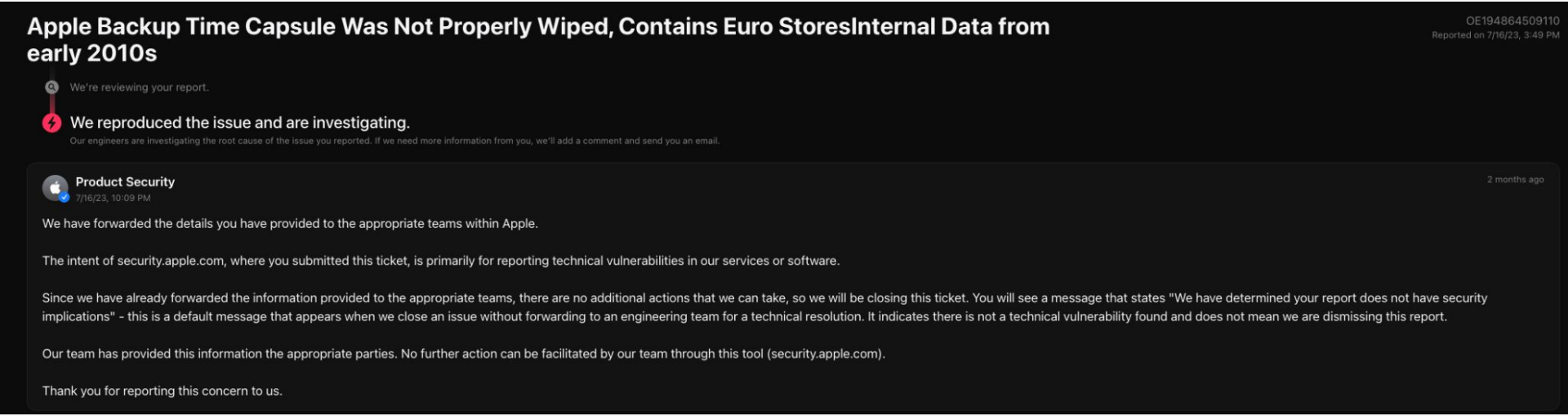
Dank internal memes







Seemed like a short disclosure process…



Apple Backup Time Capsule Was Not Properly Wiped, Contains Euro StoresInternal Data from early 2010s

OE194864509110
Reported on 7/16/23, 3:49 PM

We're reviewing your report.

We reproduced the issue and are investigating.
Our engineers are investigating the root cause of the issue you reported. If we need more information from you, we'll add a comment and send you an email.

Product Security
7/16/23, 10:09 PM

2 months ago

We have forwarded the details you have provided to the appropriate teams within Apple.

The intent of security.apple.com, where you submitted this ticket, is primarily for reporting technical vulnerabilities in our services or software.

Since we have already forwarded the information provided to the appropriate teams, there are no additional actions that we can take, so we will be closing this ticket. You will see a message that states "We have determined your report does not have security implications" - this is a default message that appears when we close an issue without forwarding to an engineering team for a technical resolution. It indicates there is not a technical vulnerability found and does not mean we are dismissing this report.

Our team has provided this information the appropriate parties. No further action can be facilitated by our team through this tool (security.apple.com).

Thank you for reporting this concern to us.

[redacted]@apple.com>

to me

Dear Matthew

I understand you have been communicating with Apple Information Security with regards to some hardware and are willing to pass this to us so we can investigate further.

You mention you are in the South Bay Area and I assume you mean the SCV area? Would you like me to arrange for someone local to make contact?

Many Thanks

[redacted]

Drove 10 minutes to drop it off



Matthew Bryant <mandatory@gmail.com>
to [redacted]

Hey [redacted]

Just following up to close the loop here, I returned the device to [redacted]@) at 11:00 am PDT today.

Thanks for coordinating!

Cheers,
-Matt

Product Security
7/17/23, 6:27 PM

Could you please send us all the files that you consider sensitive? This would greatly help us with our assessment. You can simply attach them to the issue here.

We appreciate your cooperation and look forward to receiving the files. Feel free to reach out if you have any questions or need further assistance.

Matthew Bryant
7/17/23, 10:12 PM

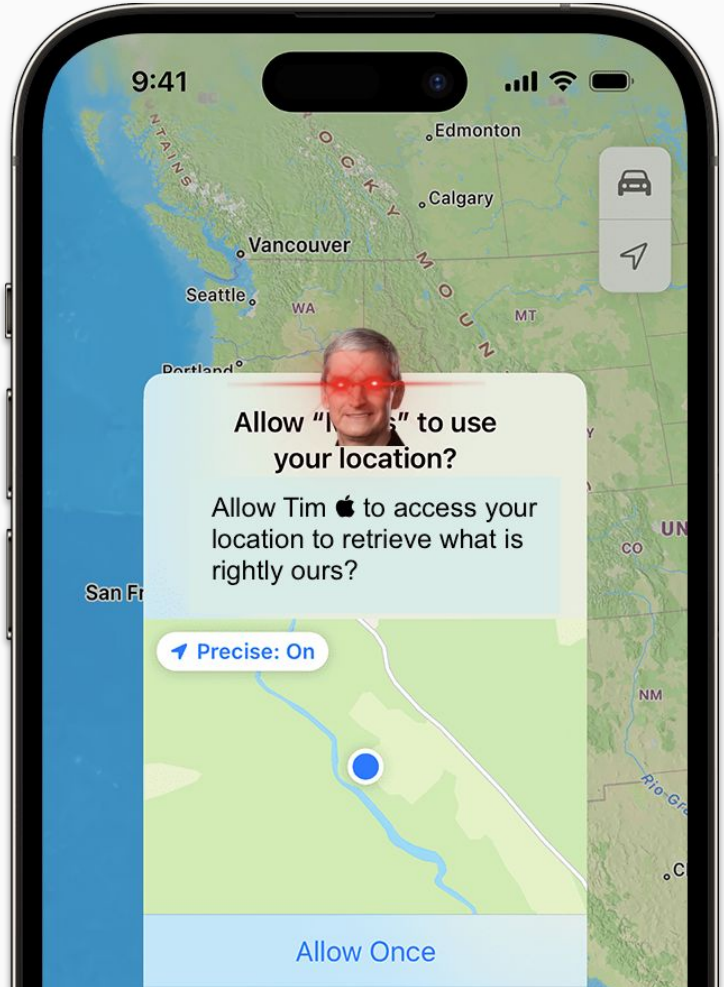
Hey folks,

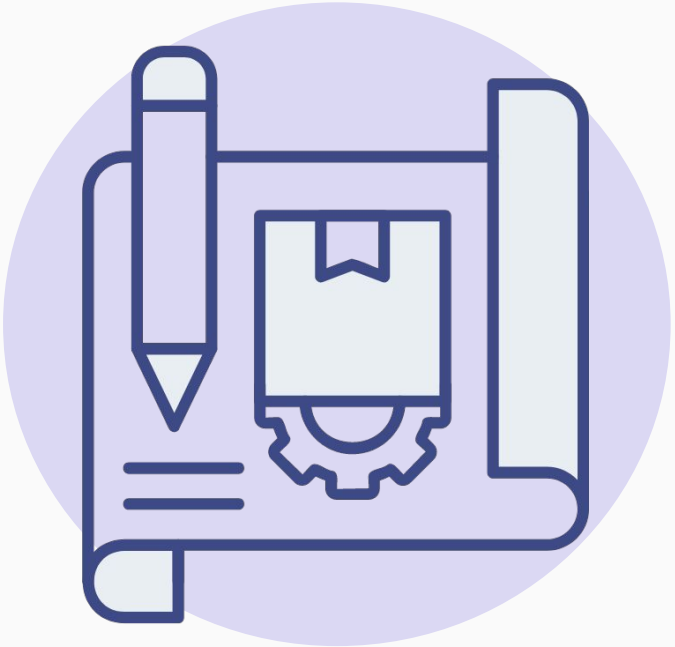
I sent some samples with my original report (not sure if they can be seen on your end?). I handed the drive over to the GSOC earlier today so I don't have access to the data anymore.

If you'd like me to re-attach the samples again let me know!

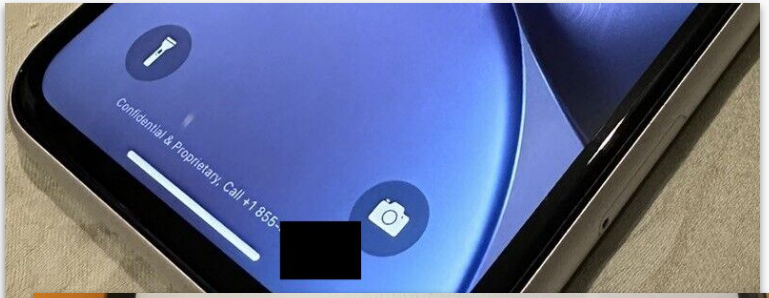


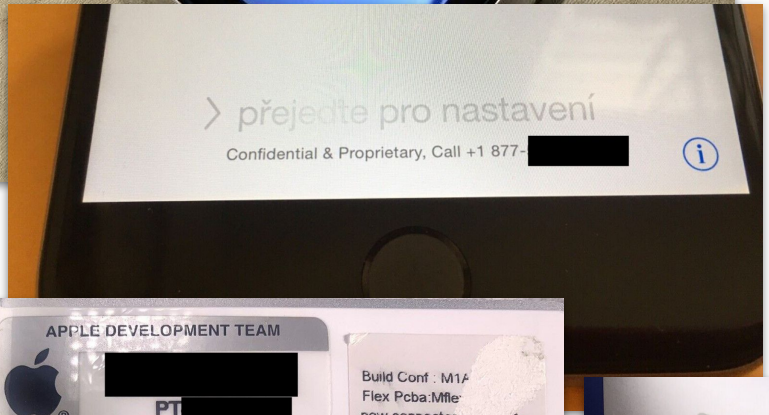




9:41
Edmonton
Calgary
Vancouver
Seattle
WA
MT
Allow "[illegible]" to use your location?
Allow Tim to access your location to retrieve what is rightly ours?
Precise: On
Allow Once

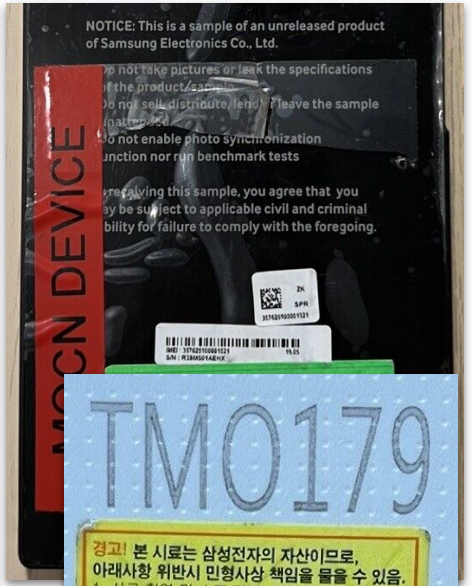


Prototypes

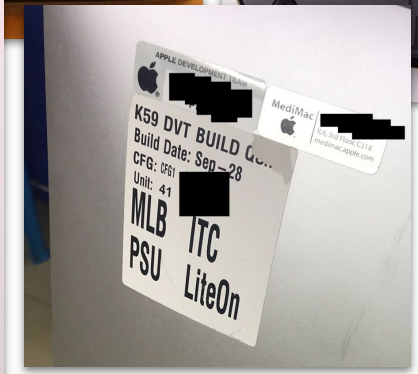

Confidential & Proprietary, Call +1 855-


přejeďte pro nastavení
Confidential & Proprietary, Call +1 877-

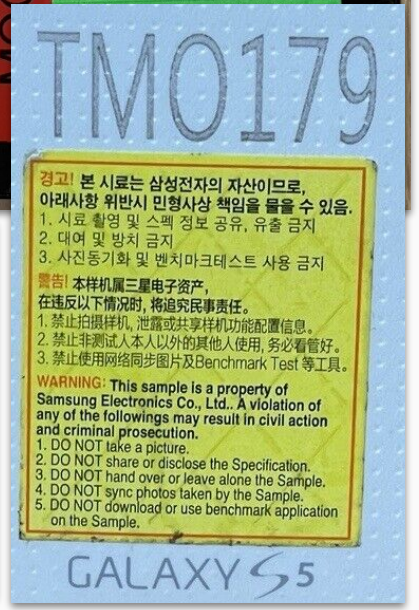

DO NOT REMOVE - THIS DEVICE HAS NOT BEEN AUTHORIZED AS REQUIRED BY THE RULES OF THE FCC.
THIS DEVICE IS NOT AND MAY NOT BE OFFERED FOR SALE OR LEASE, OR SOLD OR LEASED, UNTIL AUTHORIZATION IS OBTAINED.
THIS DEVICE DOES NOT CURRENTLY COMPLY WITH RTTE DIRECTIVE AND IS INTENDED FOR DEMONSTRATED PURPOSES ONLY.
THIS APPARATUS MAY NOT BE MARKETED OR PUT INTO SERVICE UNTIL IT HAS BEEN MADE TO COMPLY WITH THE RTTE DIRECTIVE.
DVX-BIG
TITAN
PROTOTYPE
MOTOROLA CONFIDENTIAL PROPERTY
NOT FOR SALE
DESIGNED BY MOTOROLA
ASSEMBLED IN CHINA
UMTS DS
S/N:NT1T3I0130
IMEI 359296050053751
IMEI2 359296050053769
DVT


NOTICE: This is a sample of an unreleased product of Samsung Electronics Co., Ltd.
MOCN DEVICE


APPLE DEVELOPMENT TEAM
Build Conf : M1A
Flex Pcba:Mfle
new connector
Keyboard Lay
ANSI Engl
Feature
Membr
A1(HMG+Goda+HMG-H34)
Dock Body : GP 1
Bottom Tray : GP 1/1
Bottom pad : PNR 8
Landing pad : GP 1/1


K59 DVT BUILD
Build Date: Sep-28
CFG:
Unit: 41
MLB ITC
PSU LiteOn

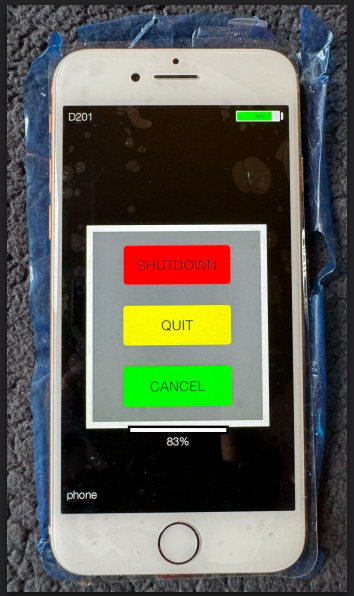

CONFIDENTIAL
(Unauthorized use prohibited)
No photo allowed
Not For Sale
Do not leak info


TM0179
경고! 본 시료는 삼성전자의 자산이므로,
아래사항 위반시 민형사상 책임을 물을 수 있음.
1. 시료 촬영 및 스펙 정보 공유, 유출 금지
2. 대여 및 방치 금지
3. 사진중기화 및 벤치마크테스트 사용 금지
警告! 本样机属三星电子资产,
在违反以下情况时, 将追究民事责任。
1. 禁止拍摄样机, 泄露或共享样机功能配置信息。
2. 禁止非测试人本人以外的其他人使用, 务必看管好。
3. 禁止使用网络同步图片及Benchmark Test等工具。
WARNING: This sample is a property of Samsung Electronics Co., Ltd.. A violation of any of the followings may result in civil action and criminal prosecution.
1. DO NOT take a picture.
2. DO NOT share or disclose the Specification.
3. DO NOT hand over or leave alone the Sample.
4. DO NOT sync photos taken by the Sample.
5. DO NOT download or use benchmark application on the Sample.
GALAXY S5



Apple Prototypes




D201
SHUTDOWN
QUIT
CANCEL
83%
phone


2:58
Thursday, December 28
slide to unlock
Confidential & Proprietary, Call +1 877-595-1124


Kanzi
PASS
BUSY
FAIL
DCSD



Dev-Fused iDevices

MOTHERBOARD
TECH BY VICE

The Prototype iPhones That Hackers Use to Research Apple's Most Sensitive Code

Very few people have heard of them, but "dev-fused" iPhones sold on the grey market are one of the most important tools for the best iOS hackers in the world.

By Lorenzo Franceschi-Bicchierai

Apple Security Research Device Program

How it works.

The Security Research Device (SRD) is a specially fused iPhone that allows you to perform iOS security research without having to bypass its security features. Shell access is available, and you can run any tools, choose your own entitlements, and even customize the kernel. Using the SRD allows you to confidently report all your findings to Apple without the risk of losing access to the inner layers of iOS security. Plus, any vulnerabilities that you discover with the SRD are automatically considered for Apple Security Bounty.

MacRumors

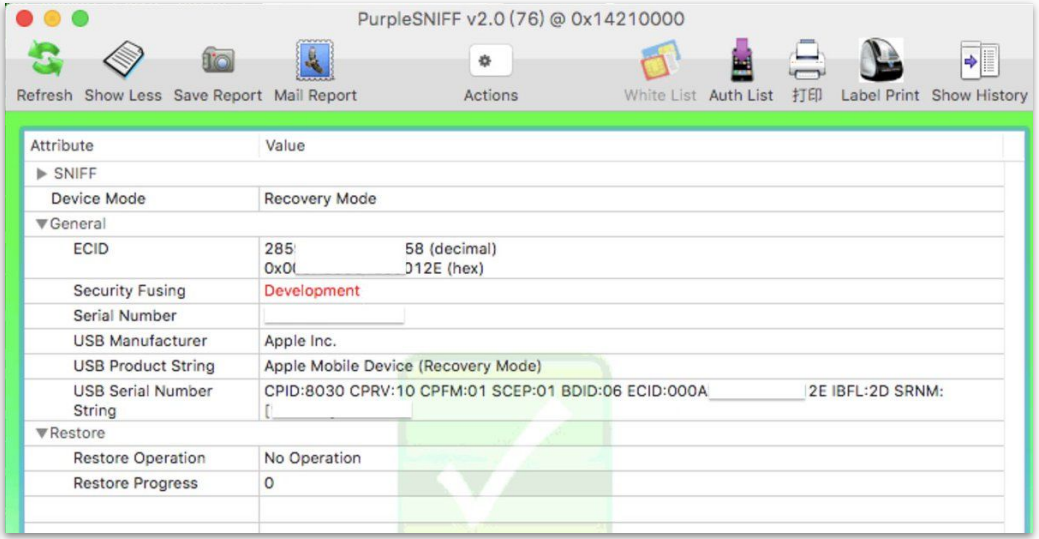
iPhone 15 | iOS 17 | iPhone 15 Pro | iPhone

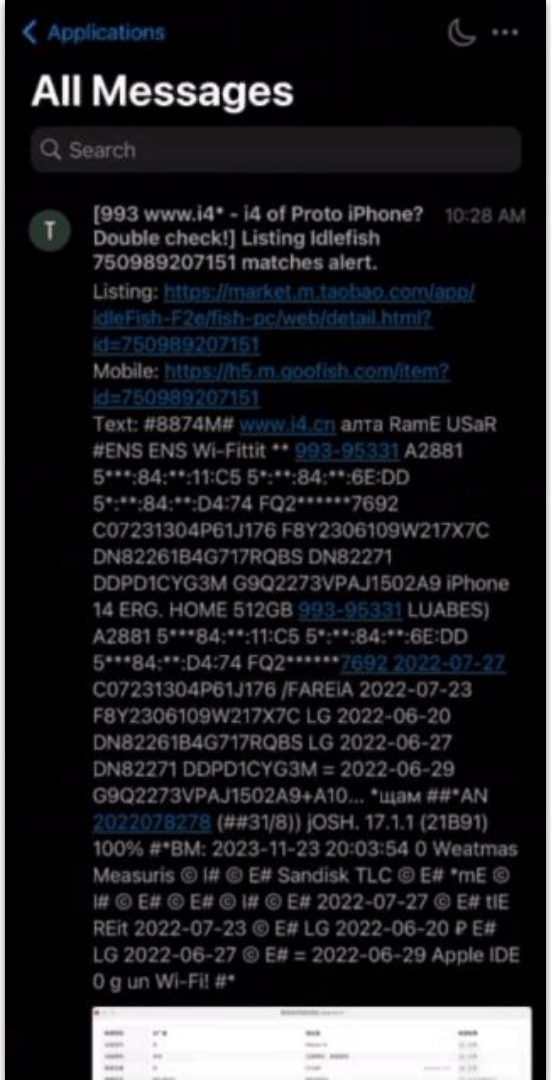
Researchers and Hackers Use Rare Dev-Fused Prototype iPhones to Unlock Security Secrets

The owner of the Twitter account Jin Store, which claims to sell dev-fused or prototype iPhones, shared their catalog with Motherboard. A dev-fused iPhone 8 Plus costs $5,000, an iPhone XR $20,000, and an older iPhone 6 costs $1,300 (there are several different types of dev-fused devices that have different levels of security and varying features on them. The price of the dev-fused device depends on the security and features it includes.)

	SoC mode	AP status	SEP status	SEP UID
CPFM00	Development fused	Development	Development	Development
CPFM03	Production fused	Production	Production	Production
CPFM01	AP demoted	Development	Production	Development



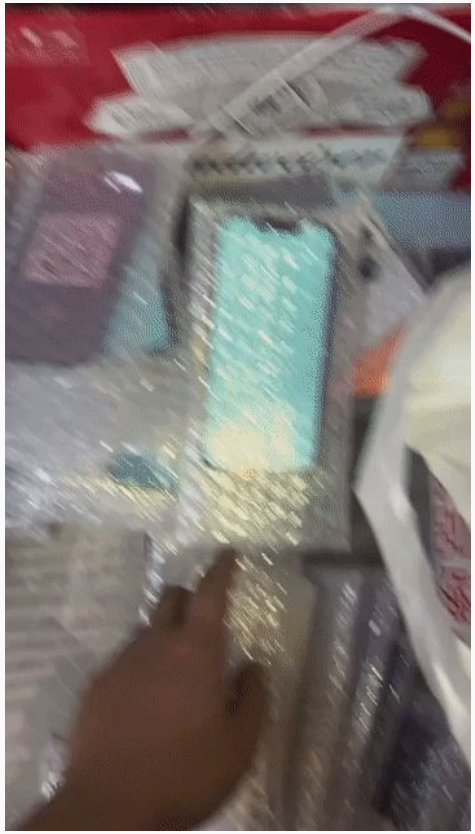




On November 23rd, 2023

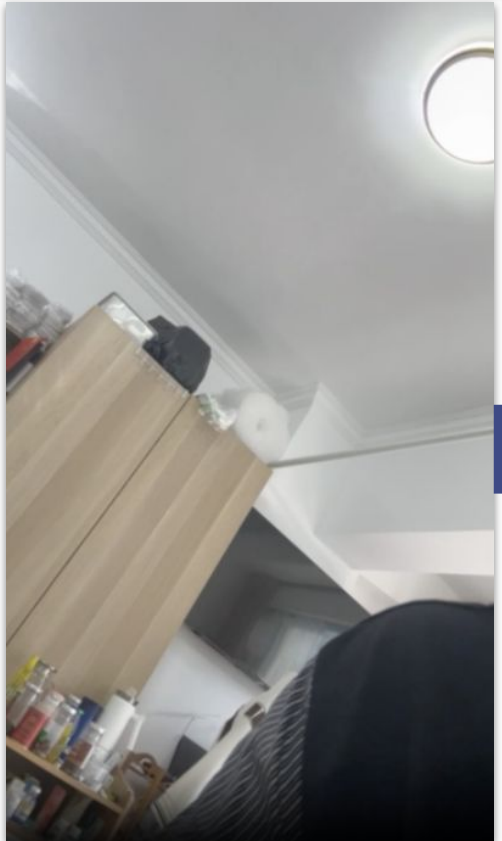
The pipeline detected several prototype iPhone 14s listings

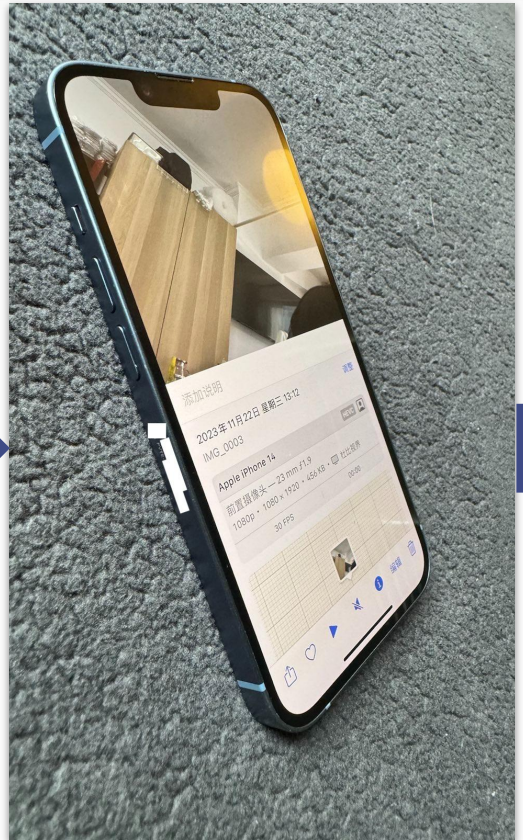
Seller had ~200 prototype iPhone 14s





iPhones Had GPS Tagged Photos of Seller







As well as some selfies…

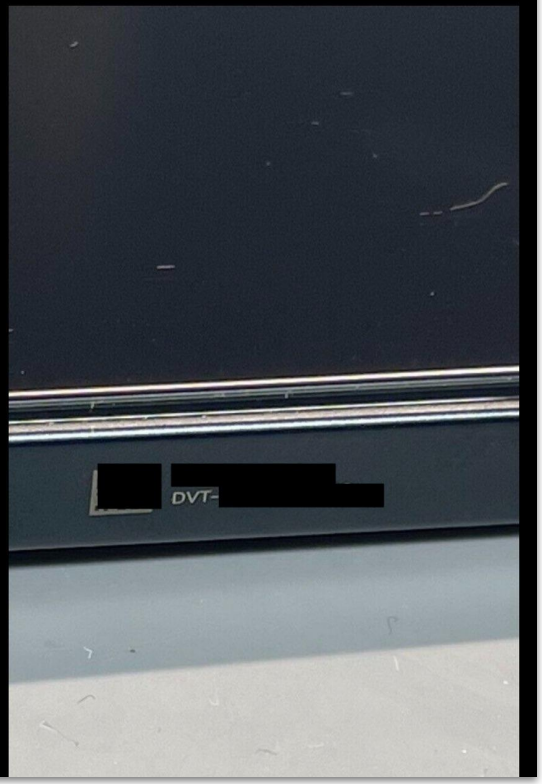


T

[dvt (Maybe Design Validation Test)] Listing eBay [redacted] matches alert. 2:54 PM

Listing: https://www.ebay.com/itm/[redacted]?orig_cvip=true

Text: [redacted] DVT-[redacted]



ebay Categories Search for anything

Order details

Order info

Time placed: Sep 4, 2023 at 2:54 PM
Order number: [redacted]
Total: $186.21 (1 item)
Sold by: [redacted]

Delivery info

Delivered on **Wed, Sep 6, 2023**

Paid Sep 4 — Shipped Sep 4 — Delivered Sep 6

Tracking details

Number: [redacted]

Item info



iPhone 14 Plus For Parts **$165.00**

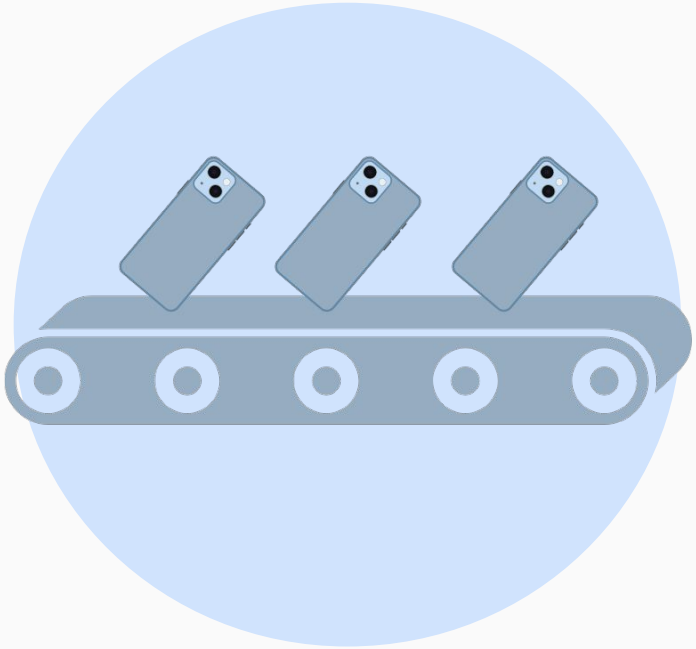
Item number: [redacted]

Returns not accepted.

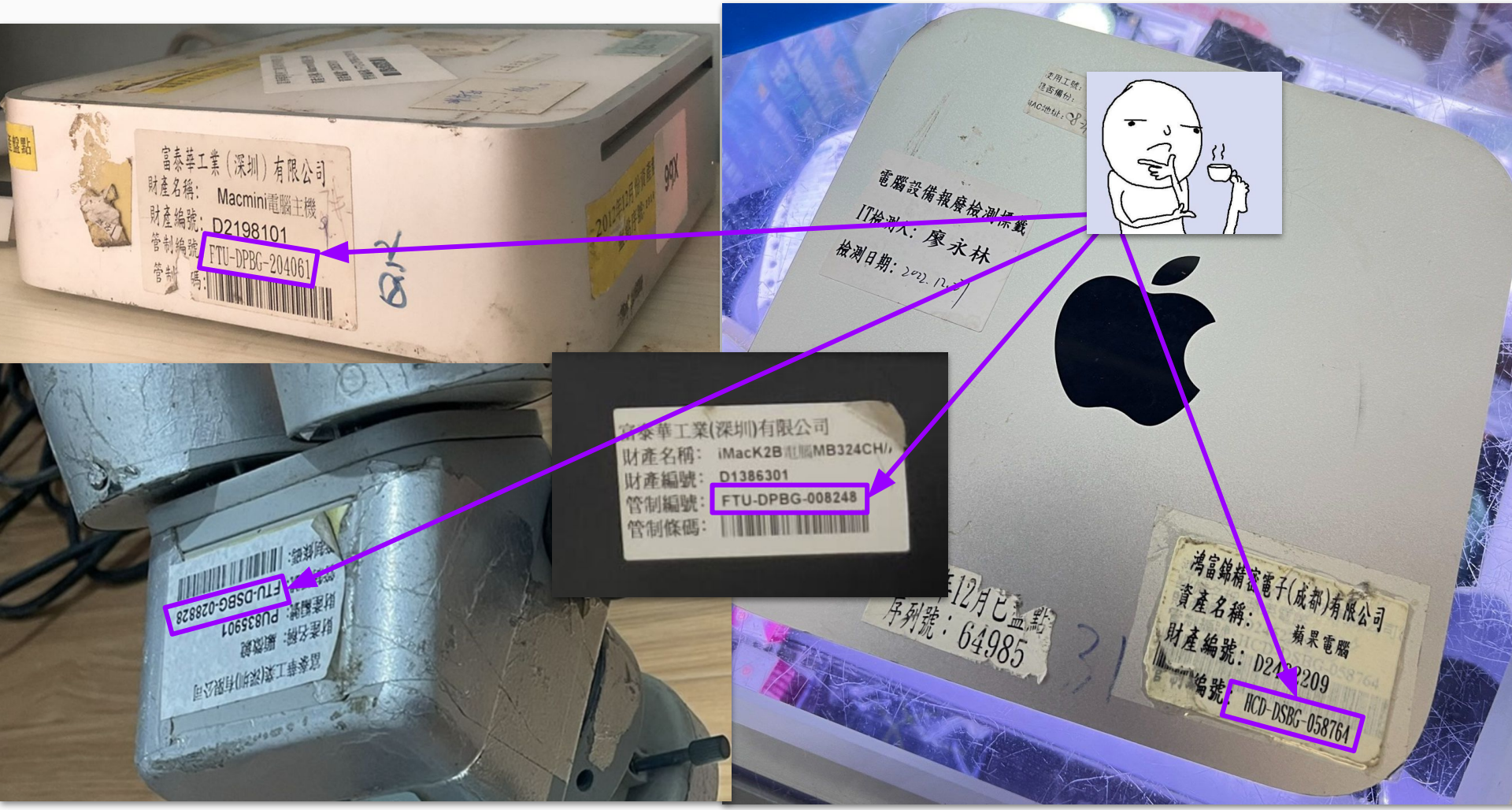
Contact seller More actions

Other actions

Contact seller



Fresh off the Assembly Line


富泰華工業（深圳）有限公司
財產名稱： Macmini電腦主機
財產編號： D2198101
管制編號
管制條碼：
FTU-DPBG-204061
電腦設備報廢檢測標籤
IT檢測人：廖永林
檢測日期：
富泰華工業(深圳)有限公司
財產名稱： iMacK2B電腦MB324CH/A
財產編號： D1386301
管制編號： FTU-DPBG-008248
管制條碼：
序列號：64985
鴻富錦精密電子(成都)有限公司
資產名稱： 蘋果電腦
財產編號： D24[illegible]209
管制編號： HCD-DSBG-058761

```
{
    "name": 'Foxconn Serial Number Format, Foxconn Equipment? (XXX-XXXX-DDDDD)',
    "query": '.*[A-Z]{3}\-[A-Z]{4}\-[0-9]{5}.*',
    "type": "REGEX"
},
```

```
{
    "name": 'FTU DPBG Foxconn Mac Mini?',
    "query": 'FTU DPBG',
},
{
    "name": 'DPBG* Foxconn Equipment?',
    "query": 'DPBG*',
},
{
    "name": 'DSBG* Foxconn Equipment?',
    "query": 'DSBG*',
},
```



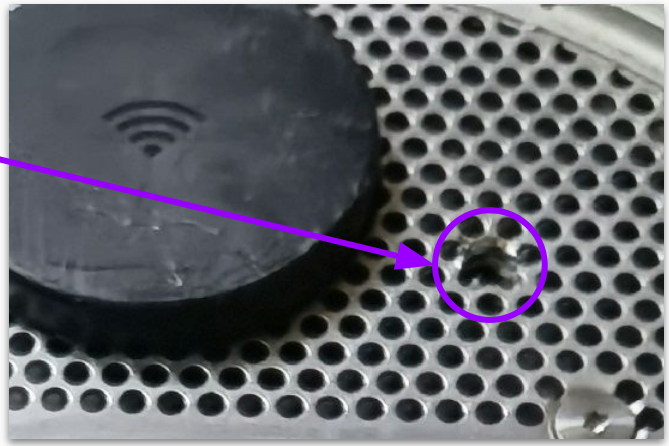
A hit for our alert



鴻富錦精密電子(成都)有限公司
資產名稱:MACMINI電腦主機
資產編号:D0733009
管制编码:HCD-DSBG-019053
C07CN01D0015

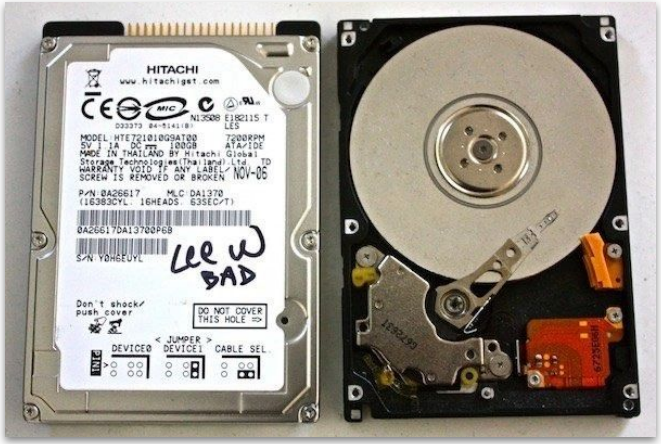
報廢電腦檢查標籤
IT檢測人: 張小川
檢測日期:2021/05/29

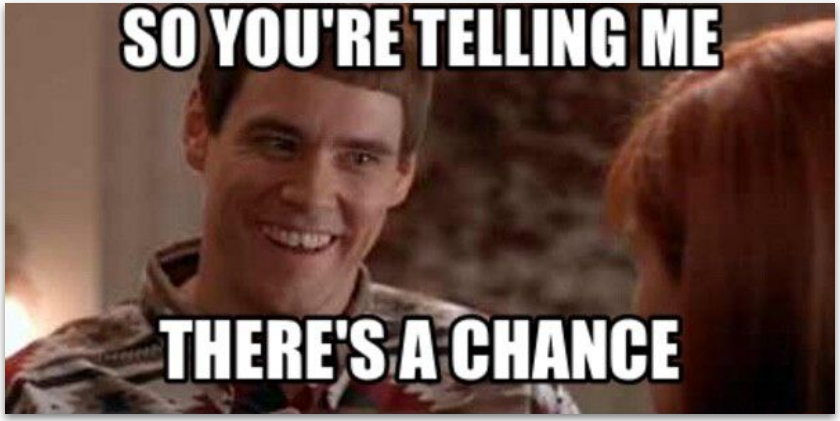

Made in China
M471B2873FHS-CF8
1012
Serial No.: C07CN01D0015
型号：A1347 中国制造








HITACHI
www.hitachigst.com
MODEL: HTE721010G9AT00
7200RPM
ATA/IDE
MADE IN THAILAND BY Hitachi Global
Storage Technologies(Thailand)Ltd
WARRANTY VOID IF ANY LABEL/ NOV-05
SCREEN IS REMOVED OR BROKEN
P/N 0A26617
MLC DA1370
(16383CYL 16HEADS 63SEC/T)
0A26617DA1370P68
S/N Y0H6EUYL
LEW
BAD
Don't shock/
push cover
DO NOT COVER
THIS HOLE =>
< JUMPER >
DEVICE0
DEVICE1
CABLE SEL.


SO YOU'RE TELLING ME
THERE'S A CHANCE




HITACHI
www.hitachigst.com
320GB 2.5inch AT 9.5mm
P/N:0A78253 MLC:DA3350
A145221
320GB PTBFS 655-1539D*IX11600K2DWMA*
DO NOT COVER
THIS HOLE
Don't shock/
push cover



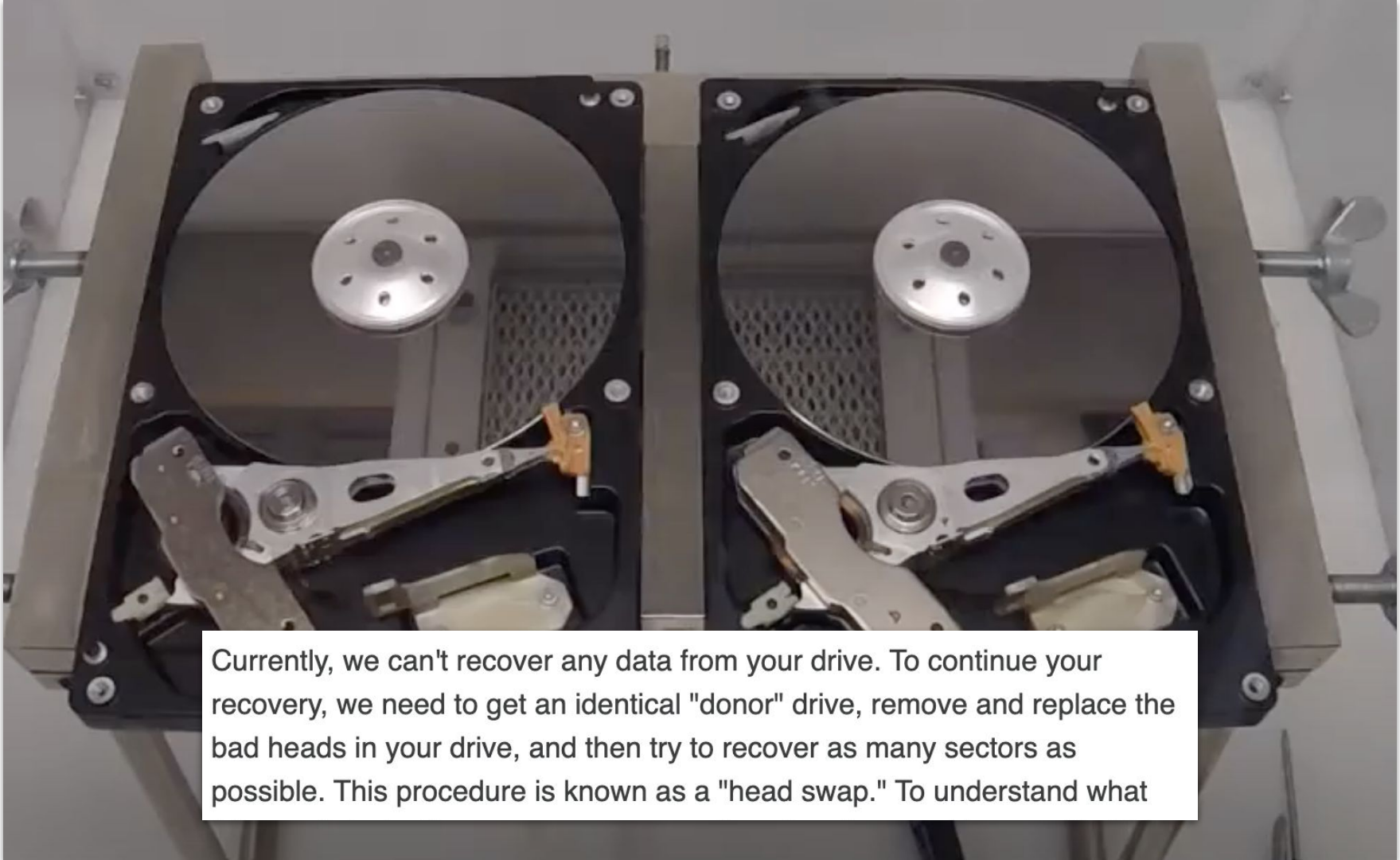


Hi Matthew,

I suppose there is a chance it can be recovered if the platters were not hit. And if they are in good shape after the metal pieces fell on the platters. If it was powered on after, it's probably toast from the metal shards flying around. If not, and if the drill did not destroy the NVRAM/ROM chip on the PCB (I don't think it's located where the hole is), it could be recoverable.

Based on our history with "HTS545032B9SA02" (we've worked on this exact model 67 times) and your device's symptoms, you have a **85% chance of a successful recovery** (again, this assumes there is no platter damage).

- "Successful" means we'll be able to recover at least some data you want (we always try to recover all the data).
- Our history of *successful* recoveries for "HTS545032B9SA02" reflects that we've been able to recover, on average, **93.8%** of our customer's data.



Currently, we can't recover any data from your drive. To continue your recovery, we need to get an identical "donor" drive, remove and replace the bad heads in your drive, and then try to recover as many sectors as possible. This procedure is known as a "head swap." To understand what

Matthew Bryant <mandatory@gmail.com>
to Tim

Oh also this is probably implied but: does this mean the platter is not drilled through and isn't shattered?

Obviously recovery seems slim even in the case that it isn't but just wanted to confirm.

Cheers,
-Matt

No, the drilled hole pretty much missed everything, but it did hit the PCB connector that is attached to the heads, so we'll need new heads. Your drive also doesn't have a top head, so no data is on the top platter, which was the most exposed platter to the dust/debris that got in through the drilled hole. All the platters looks good considering the circumstances, so I'm optimistic we'll be able to recover something.



We were able to recover 99.9998% of the sectors on your device.

We've started moving your recovered data to the transfer drive and we'll touch base when it's all finished and ready to go.



Test Station:	CELL-TEST
Line:	C10-3FR-04A
Station:	2
IP Address:	172.32.21.16
MAC Address:	c8:2a:14:40:5e:0d
Uptime:	16:04 up 29 secs

SFC專用電腦,嚴禁其它用途!

正常開機步驟:

1.連通電腦主機電源.

2.連通顯示器電源.

3.啓動主機電源開關按鈕.

4.啓動顯示器電源開關按鈕.

正常關機步驟:

1.正常關閉SFC程序.

2.點擊電腦桌面左下角<<開始>>按鈕,選擇<<關機>>選項.

3.待出現<<Windows關機>>提示框后,選擇<<關機>>,并點擊確定.

4.待主機出現關機后(顯示器無顯示),關閉顯示器電源按鈕.

5.切斷電腦主機電腦及顯示器電源.

iDSBG-IT-SFC中心:80009

iDSBG-IT-客服中心:560+19116

iDSBG-IT-SFC 宣

```
[Basic]
IP_1=172.17.241.53
Path_1 =\\172.17.241.53\idsbgcdsfc$\iPad FATP\Online Program\GSACD\4 Shop Floor
UserID_1 = idsbgit
Password_1 = [redacted]
Sleep_1=5000

IP_2=172.17.241.53
Path_2 = \\172.17.241.53\idsbgcdsfc$\iPad FATP\Online Program\GSACD\4 Shop Floor
UserID_2 = idsbgit
Password_2 = [redacted]
Sleep_2=5000
```

```
[Data]
Network ID=172.G10
Account ID=GSACD
Account Type=L
Commodity ID=21
Bu Code=DSD
Plant Code=HFJCD0GLDCD
DOM Plant Code=HFJCD0GLDCD
;Plant Code=FTU0DSDLH
;DOM Plant Code=FTU1DSDLH
```

```
Instant Pudding v0.3.12 log starting
[        -      .       - refresh]: Refreshing ghinfo.json file at "/vault/data_collection/test_station_cc
[20120601-043110.233924 - IP_UUTStart]: Entering IP_UUTStart
[20120601-043110.233924 - IP_UUTStart]: Exiting IP_UUTStart
[20120601-043110.233924 - IP_addAttribute]: Trying to add attribute [softwareversion] = [10.0d1879.22]
[20120601-043110.233924 - validateVersion]: Software version Number:10.0d1879.22
[20120601-043110.233924 - IP_addAttribute]: Trying to add attribute [softwarename] = [WiPAS]
[20120601-043110.233924 - IP_addAttribute]: Trying to add attribute [serialnumber] = [DMP21952792DY37B6]
[20120601-043110.233924 - validateSerialNumber]: SubAssembly 17 digit serial number with Checksum: [DMP219
[20120601-043110.233924 - validateSerialNumber]: Valid Serial number
[        -      .       - refresh]: Refresh
```

Takeaways

Obtaining devices and data this way poses an **interesting question**

Has anything "**wrong**" actually been done **ethically** or **legally**?

FDE and **MDM** are not as certain on **custom hardware**

Supply chains are difficult

Leaks point to **sources**

E-Waste does not guarantee **destruction**

Special thanks to…

Thank you