# Forensics, Malware and Penetration Testing

**Mobile forensics**

David Oswald

University of Birmingham

d.f.oswald@cs.bham.ac.uk

# Outline

1. Disk forensics* ✓
2. Log file forensics ✓
3. Network forensics ✓
4. Memory forensics ✓
5. Mobile devices (Android) ←


* May need RAM forensics, e.g., in case of full-disk encryption

# What a bargain! Computer scientist hacks iPhone for £75 after the FBI paid a firm almost £1 MILLION to do the same thing

- The FBI wanted to hack the passcode of Syed Rizwan Farook's iPhone
- They paid a firm a reported $1.3 million (£900,000) to break the code
- An expert in Cambridge has done the same thing for fraction of the price
- This gives him unlimited attempts to guess the code

By SHIVALI BEST FOR MAILONLINE
**PUBLISHED:** 13:54, 20 September 2016 | **UPDATED:** 14:07, 20 September 2016



In March this year, the FBI reportedly paid a security firm $1.3 million (£900,000) to bypass the passcode of an iPhone 5C belonging to San Bernardino gunman, Syed Rizwan Farook.

And it seems that it may have been ripped off – as a security researcher has revealed how to do the same thing for just £75 ($98).



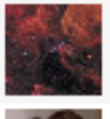
Today's headlines
Most Read

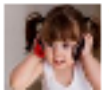

Top scientist insists the Beatles had virtually no influence on pop... and offers a bizarre diagram as his...


Man may be able to survive on Mars more easily than thought: Massive 'stingray' volcano twice the size of...


Does YOUR iPhone randomly switch off? Update it NOW: Apple says iOS 10.2.1 has 'significantly reduced' the...


Do NOT answer if someone asks 'can you hear me?': Major phone scam edits your response to make it appear as...


The supernova with the brightness of 100 million suns: NASA reveals stunning new images of 'titanic' 1987a...


Toddler's knowledge of grammar 'explodes' when they hit 24 months, study finds

# Smartphone forensics at scale

U.S. Customs and Border Protection

## Inspection of Electronic Devices

### Why You May Be Chosen for an Inspection

You may be subject to an inspection for a variety of reasons, some of which include: your travel documents are incomplete or you do not have the proper documents or visa; you have previously violated one of the laws CBP enforces; you have a name that matches a person of interest in one of the government's enforcement databases; or you have been selected for a random search.

https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf

# Smartphone forensics at scale

## What Happens Now?

You're receiving this sheet because your electronic device(s) has been detained for further examination, which may include copying. You will receive a written receipt (Form 6051-D) that details what item(s) are being detained, who at CBP will be your point of contact, and the contact information (including telephone number) you provide to facilitate the return of your property within a reasonable time upon completion of the examination.

The CBP officer who approved the detention will speak with you and explain the process, and provide his or her name and contact telephone number if you have any concerns. Some airport locations have dedicated Passenger Service Managers who are available in addition to the onsite supervisor to address any concerns.

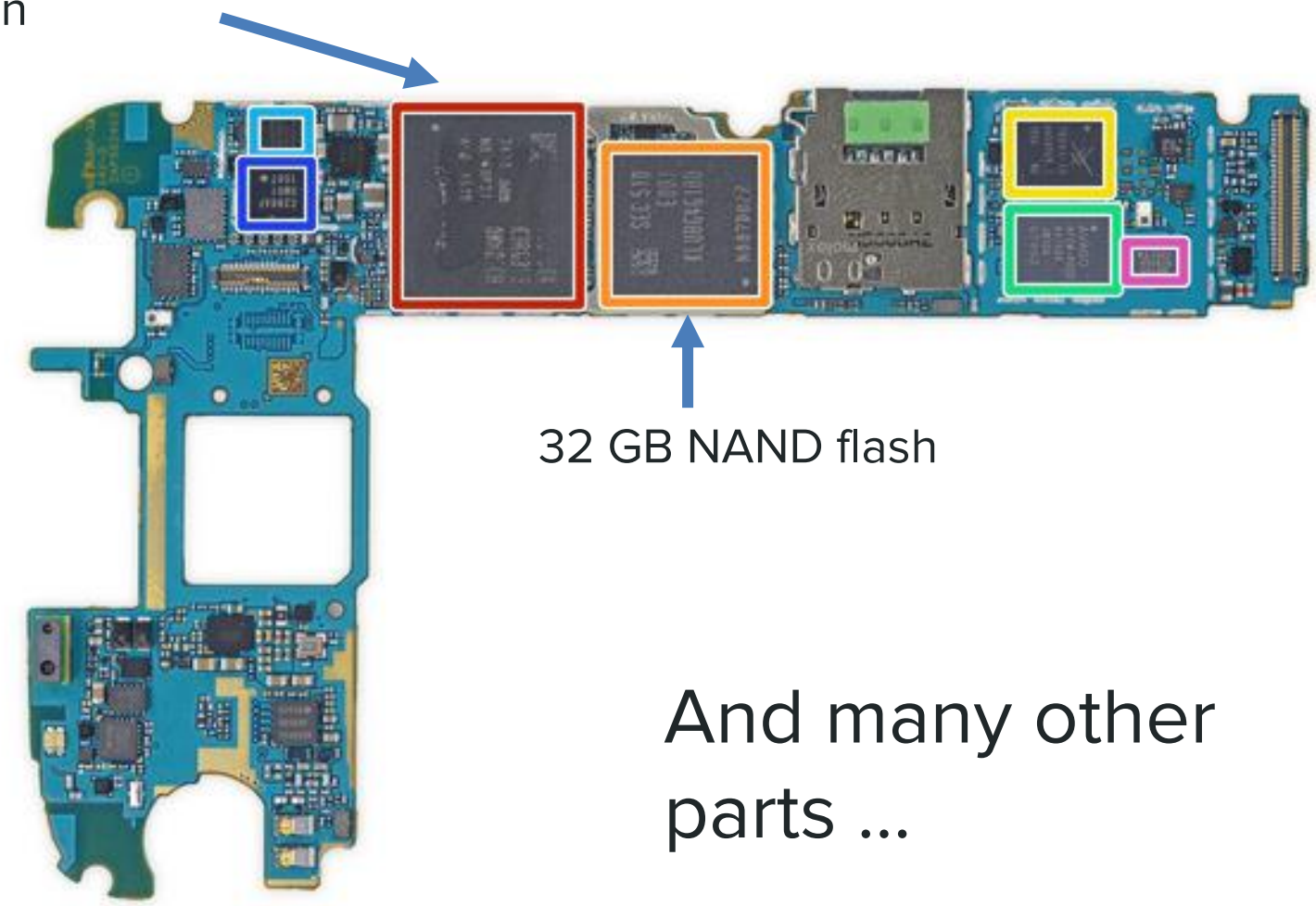
https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf

# What’s inside a smartphone


https://www.ifixit.com/Teardown/Samsung+Galaxy+S6+Teardown/39174

# What’s inside a smartphone

Samsung Exynos 7420 Octa-core Processor - 64-bit with 3 GB LPDDR4 RAM built in

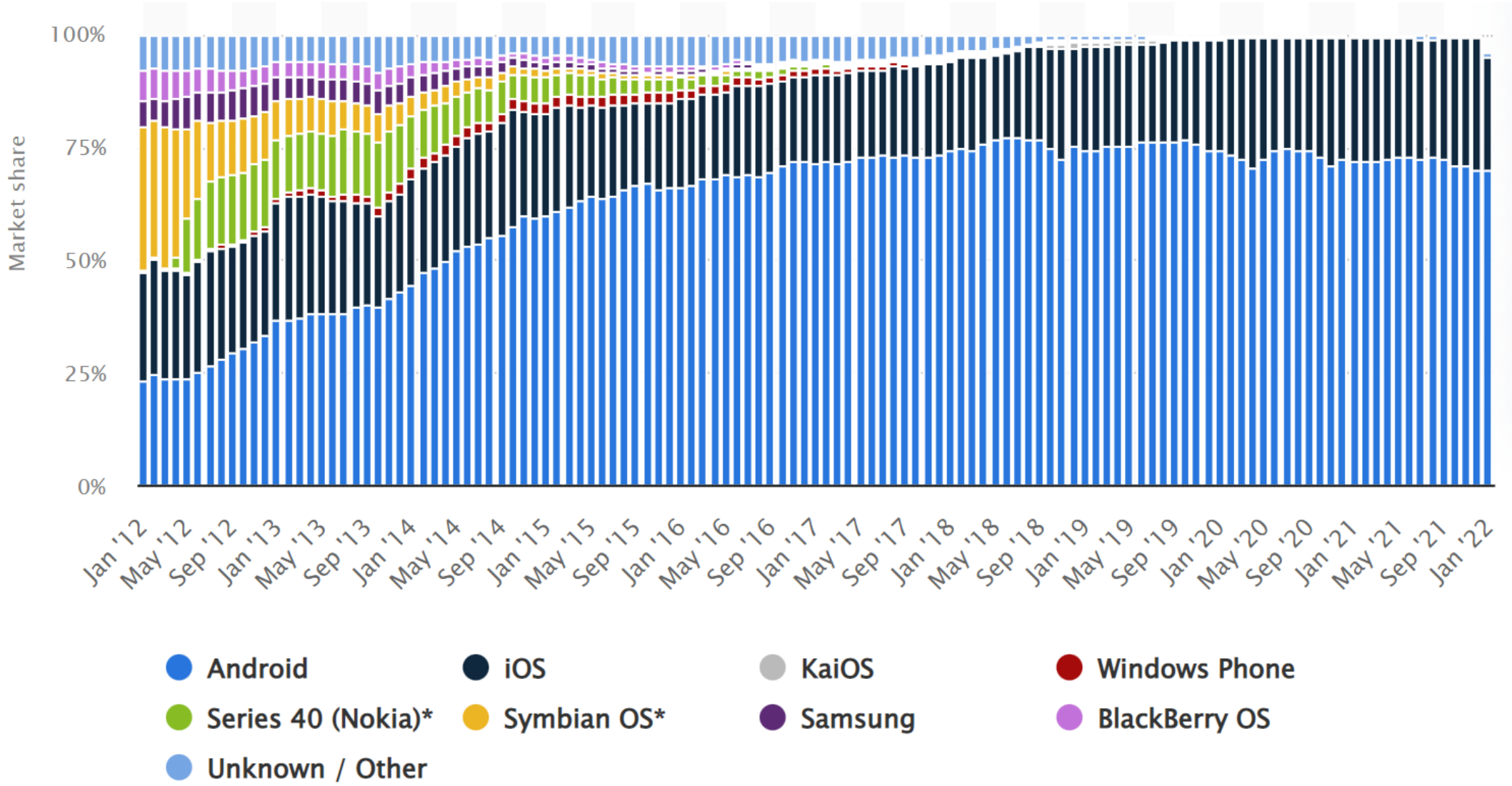


32 GB NAND flash

And many other parts ...

https://www.ifixit.com/Teardown/Samsung+Galaxy+S6+Teardown/39174

# OS on smartphones (smart devices)




https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

# OS on smartphones (smart devices)

- **2022:** Android ~ 70%, iOS ~ 25%

  ➜ we focus on Android and (a bit of) iOS in this lecture
- Other OS likely share (some) characteristics
- Other smart devices (tablets, watches) are also mostly Android / iOS, or PC-like (Windows 10)

# Mobile device forensics – Why?

**Users entrust a lot of data to smart devices:**

- E-mail and instant messenger accounts
- Social media and photos
- Calendars, notes, documents
- Contacts, phone calls and text messages
- Browsing and search history
- Maps, location history, ...
- Wifi passphrase and other passwords

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

# Similarities to “normal“ forensics

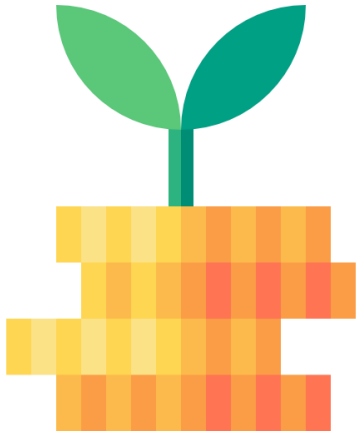
- Most mobile OS based on desktop :
  - Android: Linux
  - iOS: XNU (XNU’s not Unix), mix of FreeBSD and Mach microkernel
  - Windows 10 Mobile: edition of Windows 10
- This means: they store data in a similar way, have similar vulnerabilities, and so on
- **Summary:** Smart device ≈ PC

# Differences to “normal“ forensics

- **Summary:** Smart device ≈ PC… **not quite**
- **Storage:** removable HDDs (not modern laptops) vs. integrated storage, e.g. flash
- **Architecture:** x86_64 (PC) vs. ARM (mobile)
- **External interfaces:** Many interfaces (PC) vs. very limited on mobile
- **Software architecture:** PCs ➔ flexible, mobile devices ➔ in some way tailored

# An example: imaging mobile devices

- Imaging PC-like HDDs is “**easy**”:
- Shut down
- Remove drive
- Connect to write blocker
- Use `dd` or similar to obtain raw image
- **Profit**



# An example: imaging mobile devices

Imaging mobile storage is **hard**:

- Shut down – you lose access to device if it has a PIN or fingerprint
- Remove drive – Flash memory usually integrated on PCB, sometimes encrypted
- Connect to write blocker – not readily available for Flash as used in smartphones
- **What to do?**

# Imaging mobile devices

**No single correct way to image a mobile device, but multiple options**

- Manual: inspect live device through UI
- Backups: offline (e.g. iTunes) or cloud
- Logical: dump through external interface, e.g. USB usually used for sync'ing
- Jailbreak: obtain root rights, then image
- Physical: open device, connect to JTAG or remove/read Flash memory

# Imaging mobile devices

## NIST proposes 4 levels (2014):

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

4

3

2

1


**Figure 6: Mobile Device Tool Classification System**

# This lecture: logical extraction

- We look at the Samsung Galaxy S6
- Recovery firmware replaced with open-source TWRP (https://twrp.me/devices/samsunggalaxys6.html)
- TWRP can take a full backup and provides access through mass storage and an `abd` root shell:
  - Power down
  - Press and hold: power, volume up, home
  - Connect through USB

# Caveats: logical extraction

- We assume: encryption **disabled** (was standard as of Android 6 and 7 (2017+)
- But: bruteforcing possible: https://forensicswiki.xyz/wiki/index.php?title=How_To_Decrypt_Android_Full_Disk_Encryption
- TWRP install trips KNOX (data within KNOX containers inaccessible, efuse burned)
- **But:** can be used with locked device, since download mode not protected!

# Logical extraction in TWRP

- Option 1: take a backup 😐
  - Locally stores a tar archive to /data/media/0/TWRP/BACKUPS
  - Download via USB mass storage interface (will not copy pictures etc)
- Option 2: via USB mass storage ☹
  - Only exposes part of the filesystem (“internal storage”)
  - The usual “copy from filesystem” problems...

# Logical extraction in TWRP

**Better option 3:** full image of user partition

via `netcat` (see `/dev/block/platform/15570000.ufs/by-name`)

```
adb forward tcp:5555 tcp:5555
adb shell
nc -l -p 5555 -e dd if=/dev/block/sda18
```

(open second terminal)

```
nc 127.0.0.1 5555 | pv -i 0.5 > full.img
```

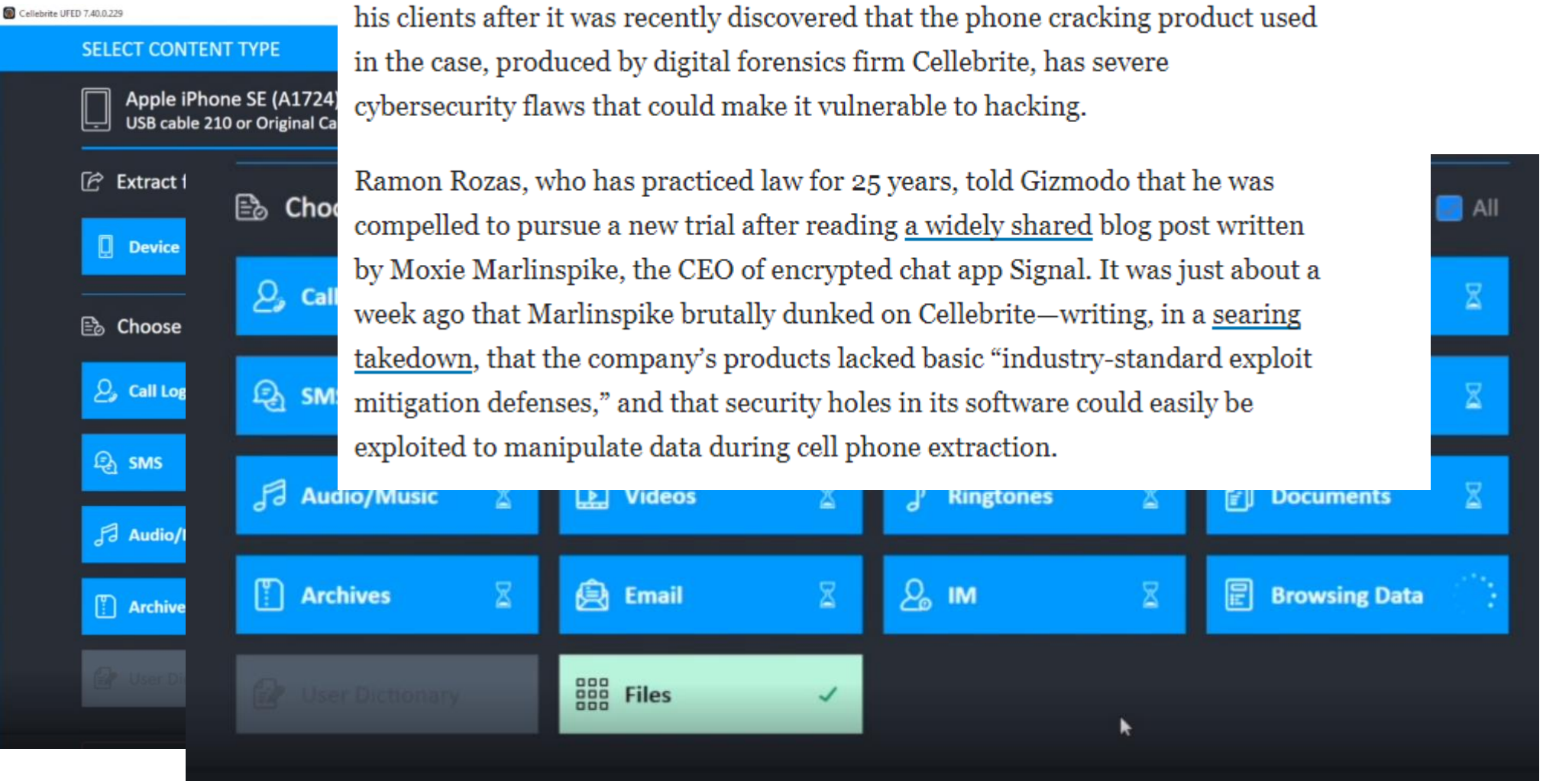
# Logical acquisition: summary

- **In practice**: well-equipped lab would most likely use specialized tools e.g. UFED by Cellebrite
- Should follow a standard forensics procedure:
  a. Documentation
  b. Isolation (beware of remote wipe)
  c. Acquisition (and hashing)
- Android usually easier than iOS
- Encryption defeats direct analysis of images

# A cautionary note

A Maryland defense attorney has decided to challenge the conviction of one of his clients after it was recently discovered that the phone cracking product used in the case, produced by digital forensics firm Cellebrite, has severe cybersecurity flaws that could make it vulnerable to hacking.

Ramon Rozas, who has practiced law for 25 years, told Gizmodo that he was compelled to pursue a new trial after reading a widely shared blog post written by Moxie Marlinspike, the CEO of encrypted chat app Signal. It was just about a week ago that Marlinspike brutally dunked on Cellebrite—writing, in a searing takedown, that the company's products lacked basic "industry-standard exploit mitigation defenses," and that security holes in its software could easily be exploited to manipulate data during cell phone extraction.




https://gizmodo.com/signals-cellebrite-hack-is-already-causing-grief-for-th-1846773797

# Next part:

- Now that we got the image, how to evaluate?
- How do mobile apps store data?
- Comparison between different mobile OS