Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid

Full-Stack Forensics? Low-Level Digital Forensics in Encryption Era

Aya Fukami

a.fukami@nfi.nl

Netherlands Forensic Institute

WinFC
Women in Forensic Computing

About me …

- Japanese National Police (2007-2020)
- Netherlands Forensic Institute (2020-)
- Forensic data recovery focusing on hardware
- Just completed my PhD “Effective Mobile Forensics Through Exploiting the Memory Security”

Digital Evidence

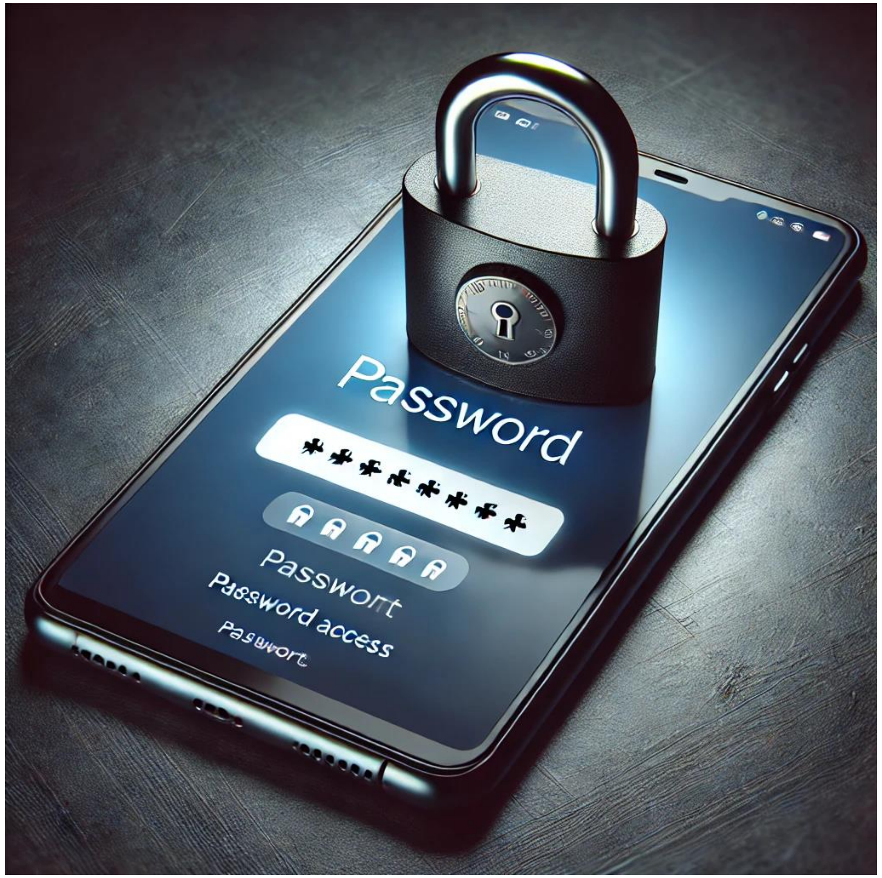
Data can be important evidence in court

Where do you acquire the data

On the device

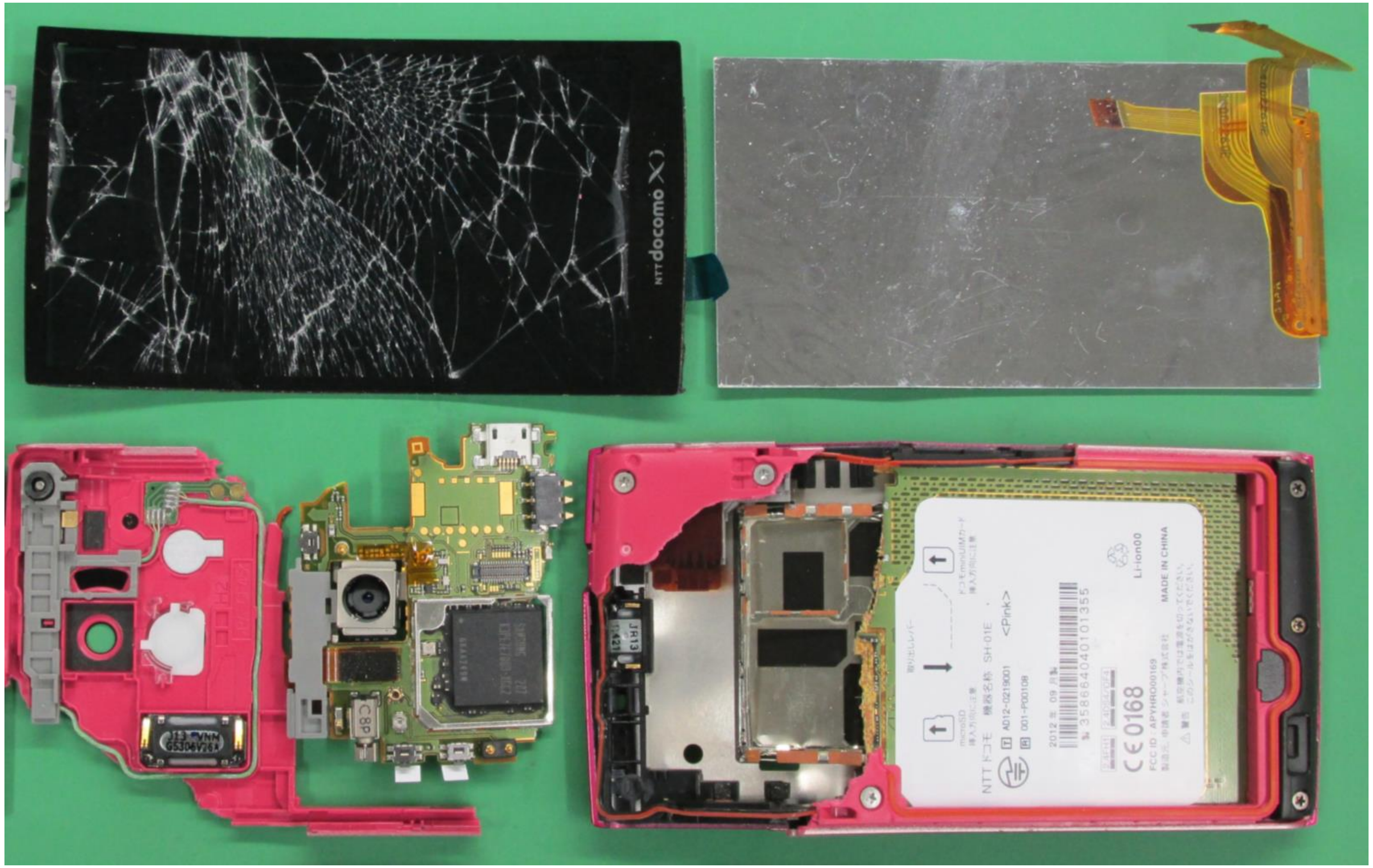
On the network

In Reality

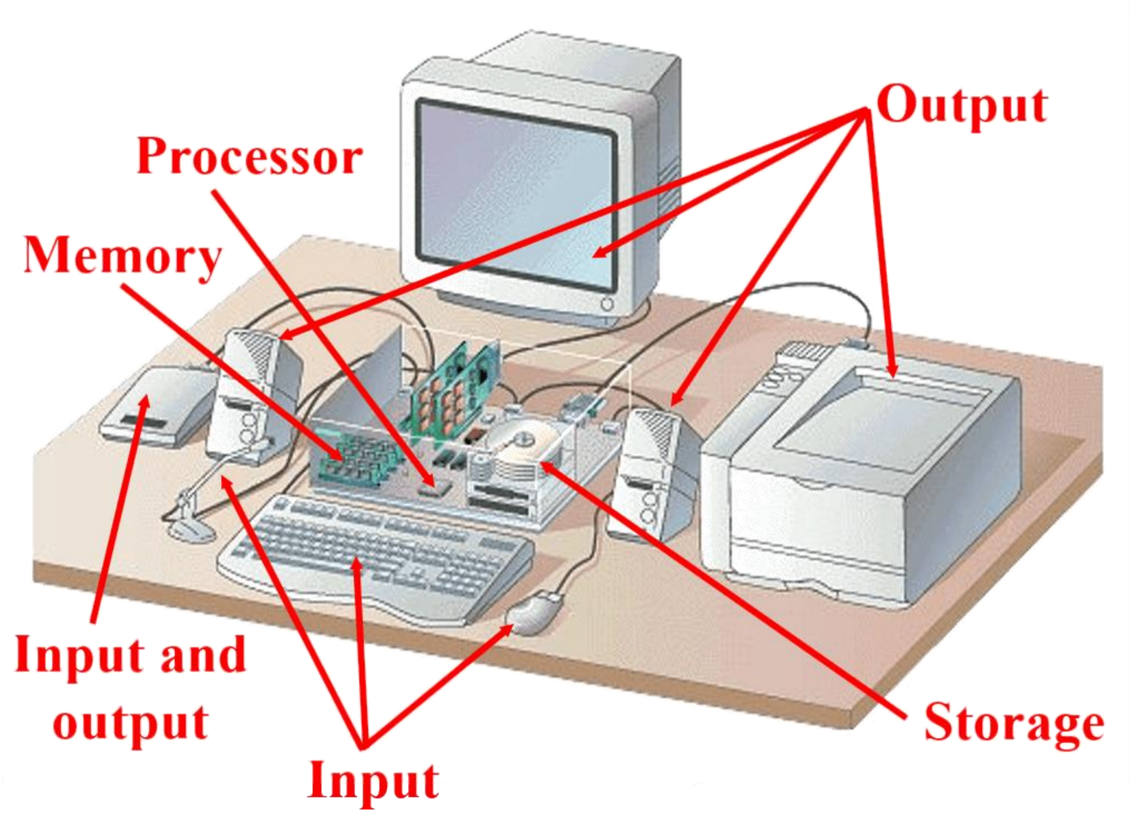

Password
****
Passwort
Password access
Paswort

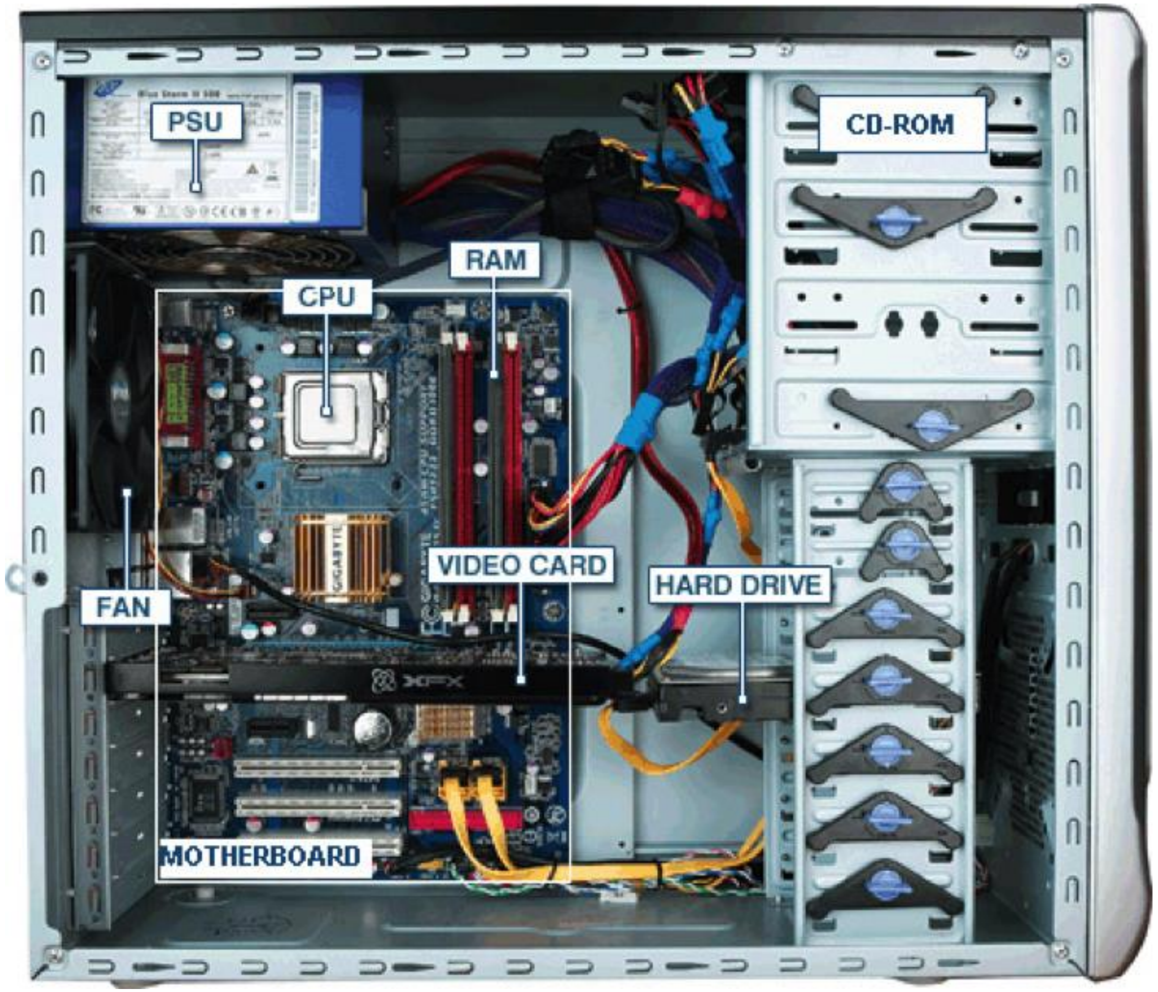
FORENSICS
CLOUD FORENS
CLOUD FOR

In Reality



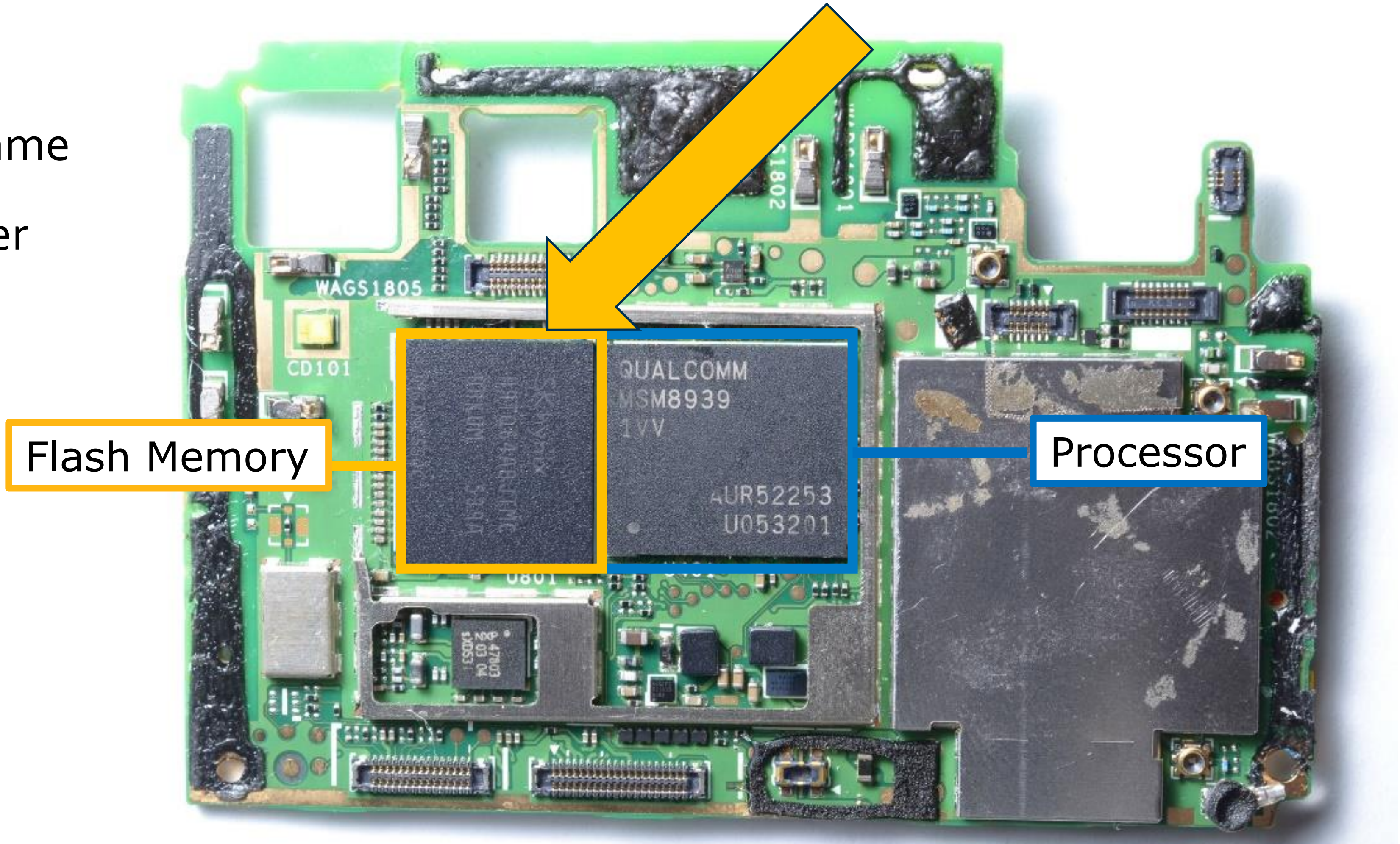
Traditional Computer Forensic





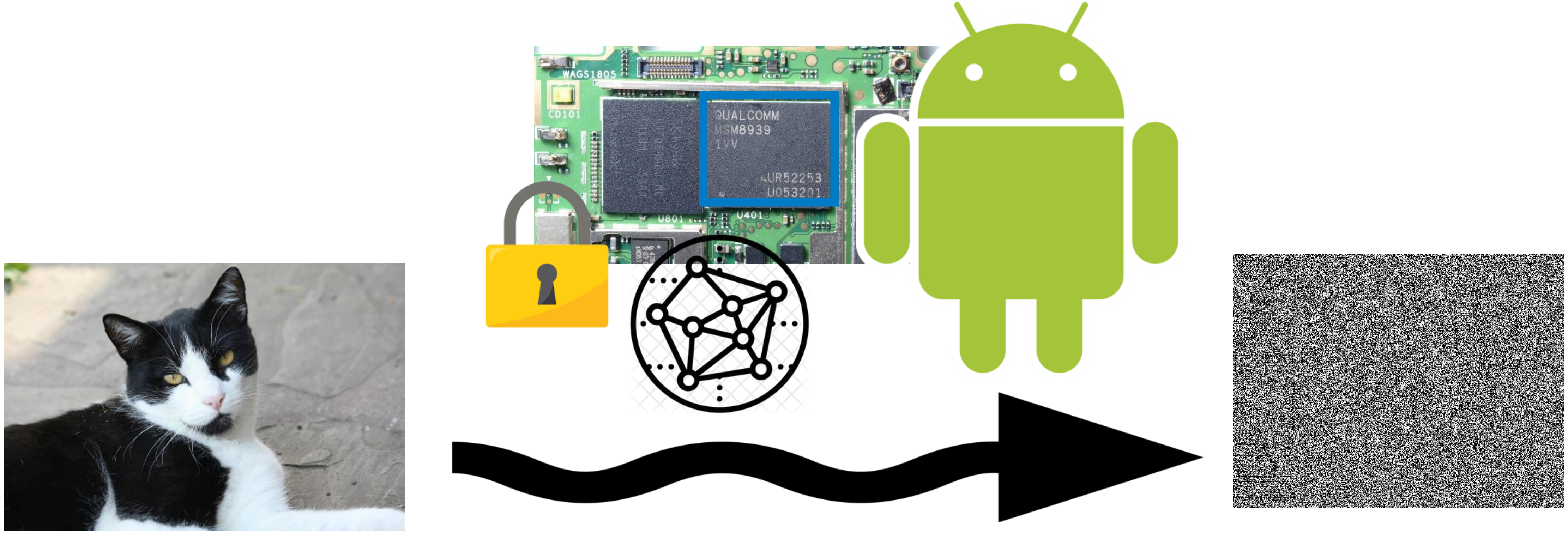
Traditional Approach: Applied to Mobile Phones

- The basic structure is the same as the stand-alone computer
- Flash Memory = HDD in Computer
  - Chip-off
  - JTAG
  - Custom Bootloader

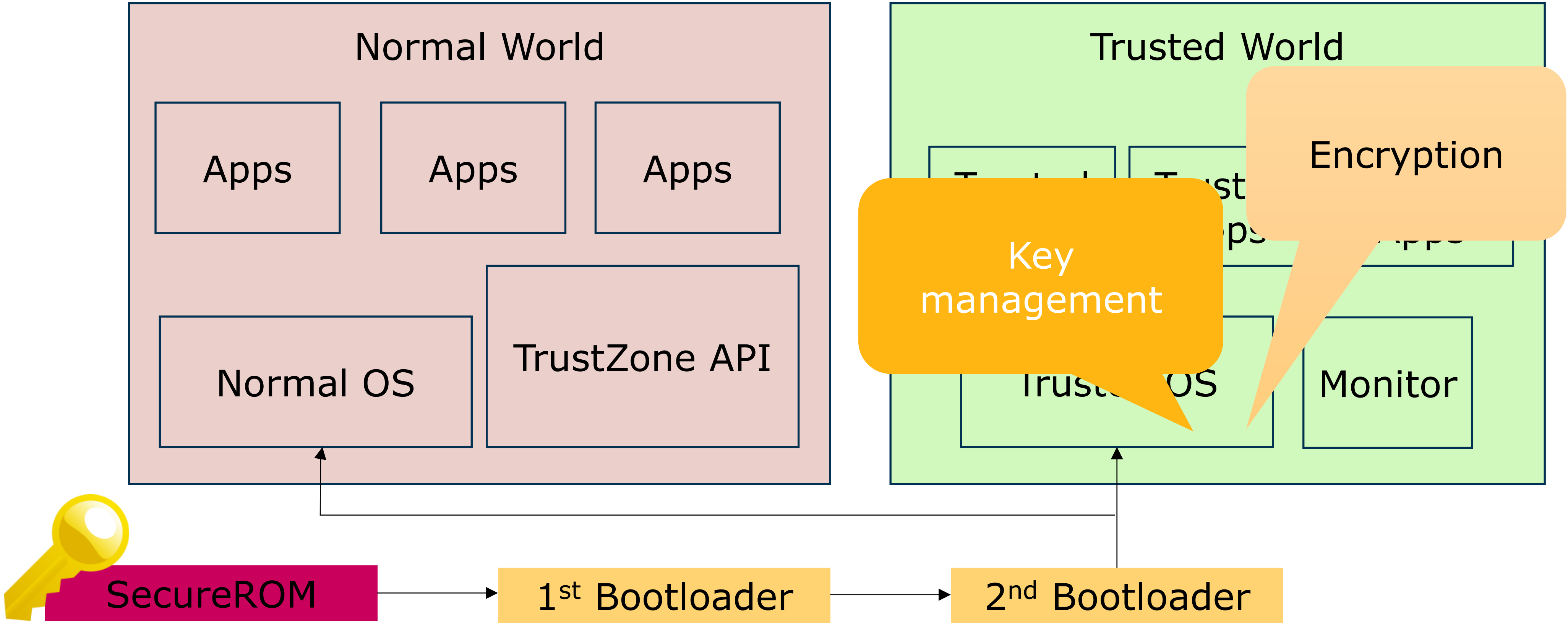


Challenges

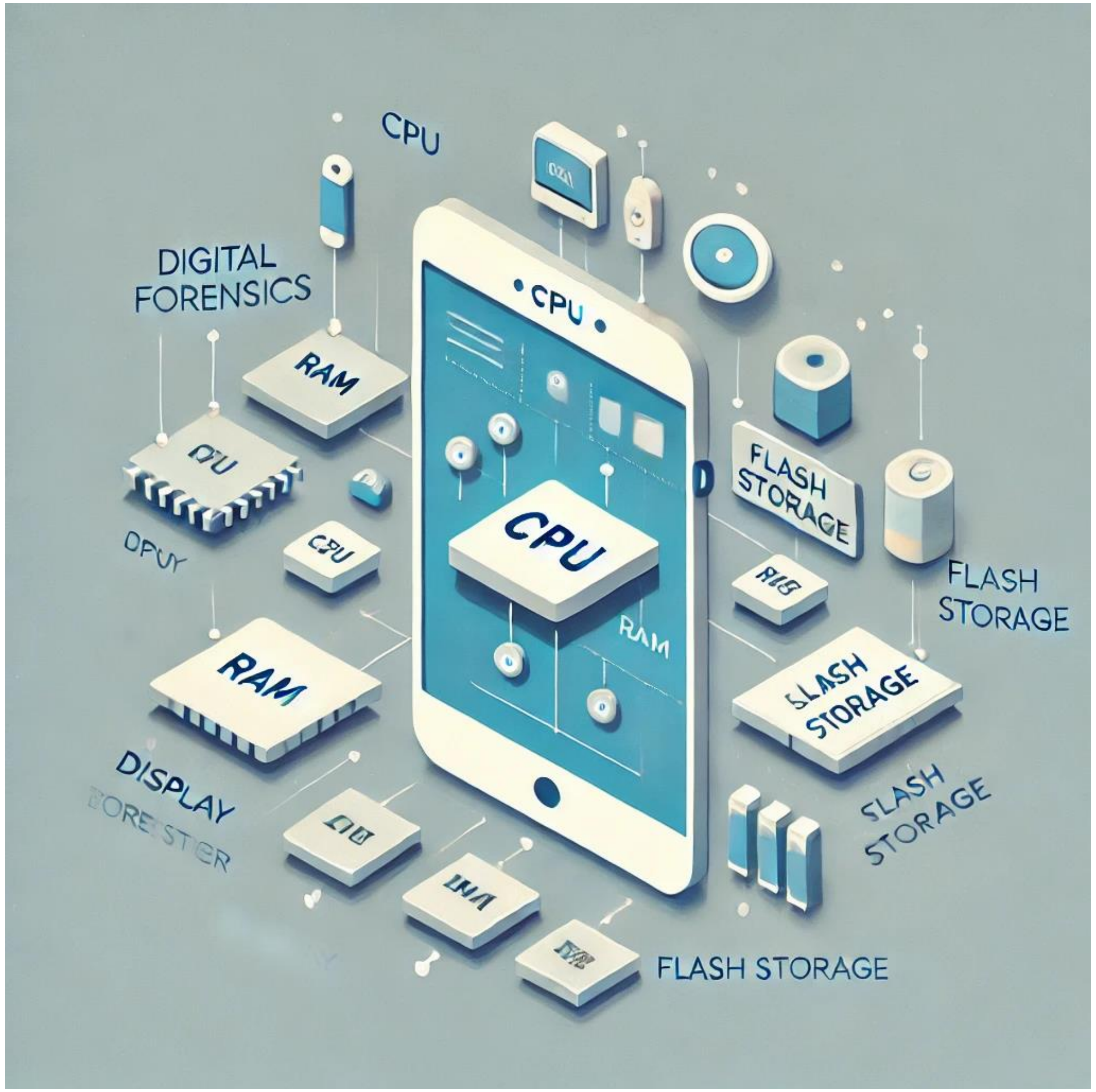
- Encryption
- TrustZone/Secure Enclave/Secure Boot



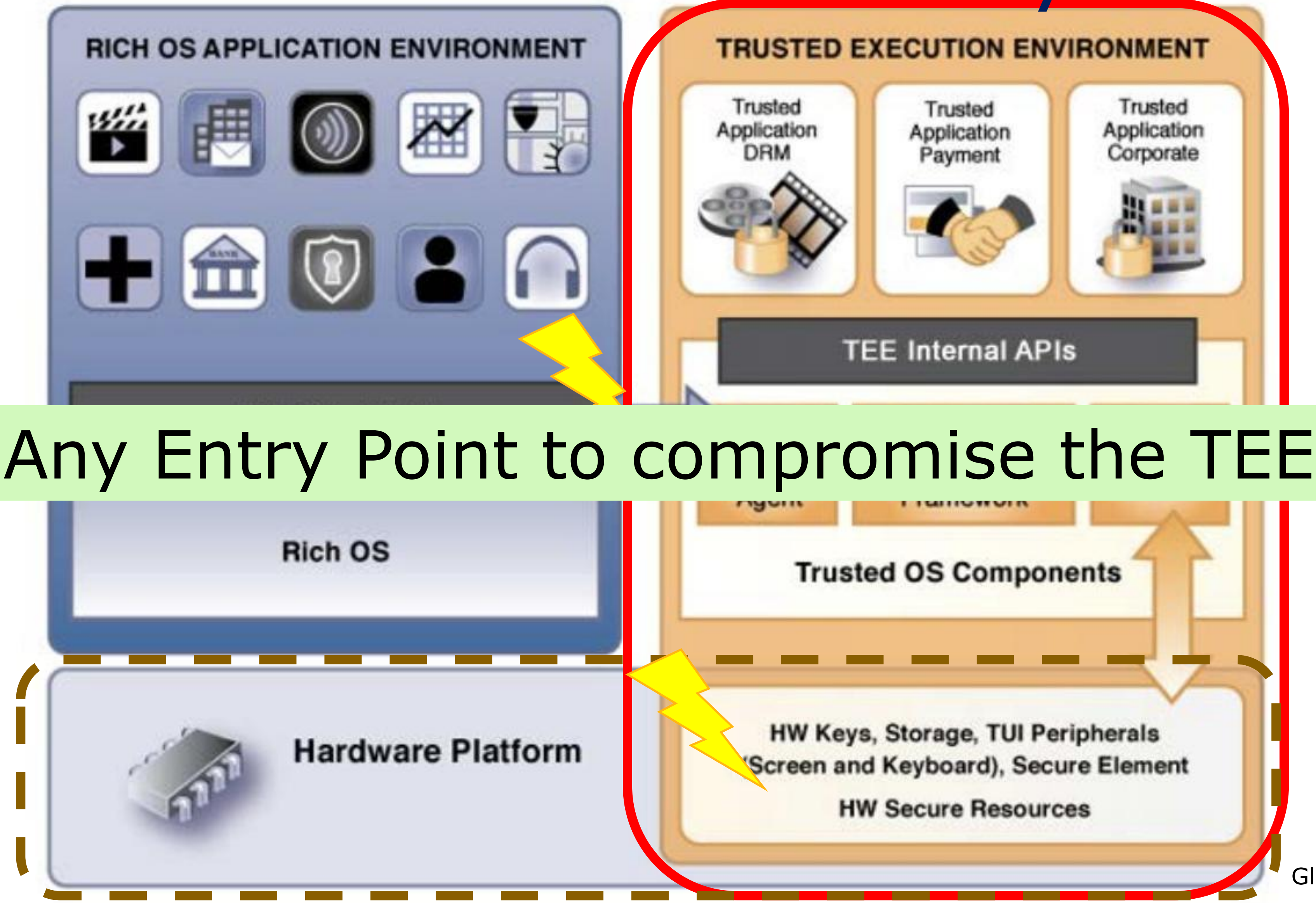
Secure Boot and Secure Enclave



SO NOW WHAT
DO WE DO?


CPU
DIGITAL FORENSICS
RAM
CPU
CPU
RAM
DISPLAY
FLASH STORAGE
FLASH STORAGE
SLASH STORAGE
SLASH STORAGE
RAM
FLASH STORAGE

Vertical Overview of a Mobile Phone System


RICH OS APPLICATION ENVIRONMENT
TRUSTED EXECUTION ENVIRONMENT
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
TEE Internal APIs
Rich OS
Trusted OS Components
Hardware Platform
HW Keys, Storage, TUI Peripherals (Screen and Keyboard), Secure Element
HW Secure Resources

Any Entry Point to compromise the TEE??

Global Platform TEE Specification

Data Acquisition != Simple Data Extraction

- Forensic officers need to think about
  - Can we get the encryption key somehow?
  - How can we run arbitrary code on the device?
  - Can we skip the secure boot ?

RAM dump

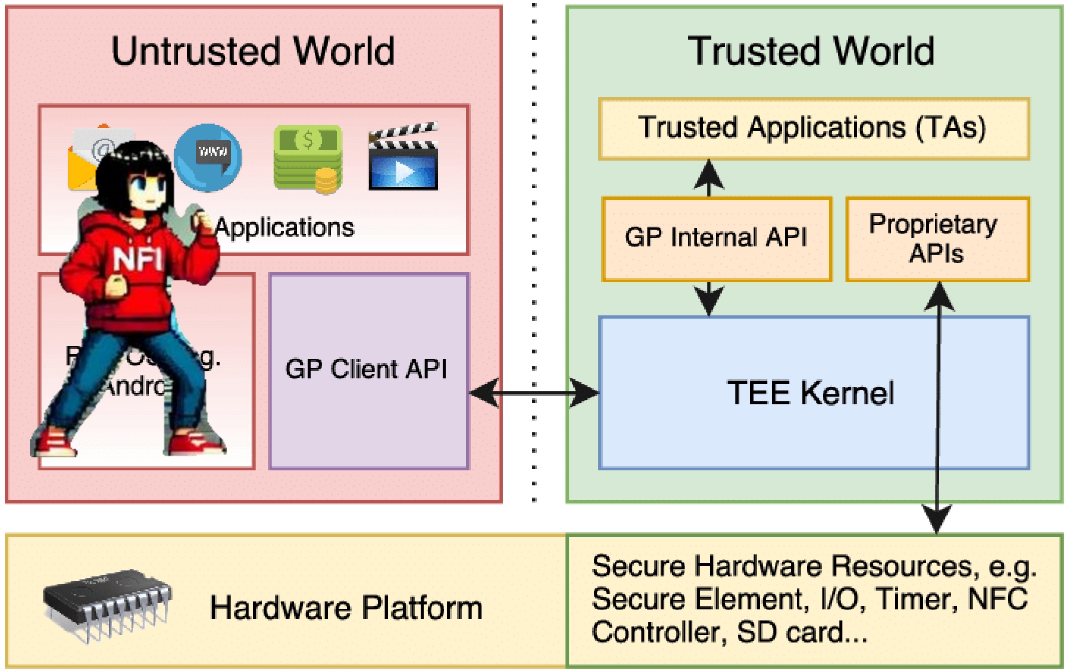
Bootloader exploit

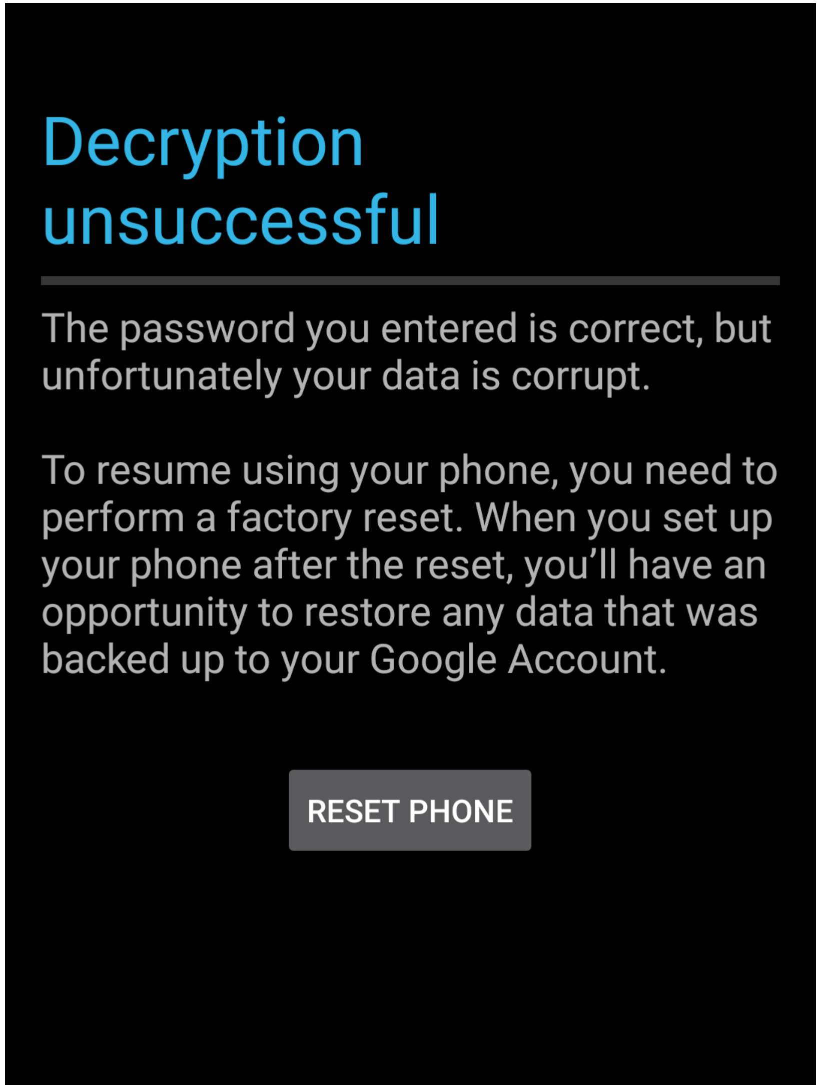
Glitching

Zero-day

Case 1: Anti-Rollback

- Locked telephone through anti-rollback detection



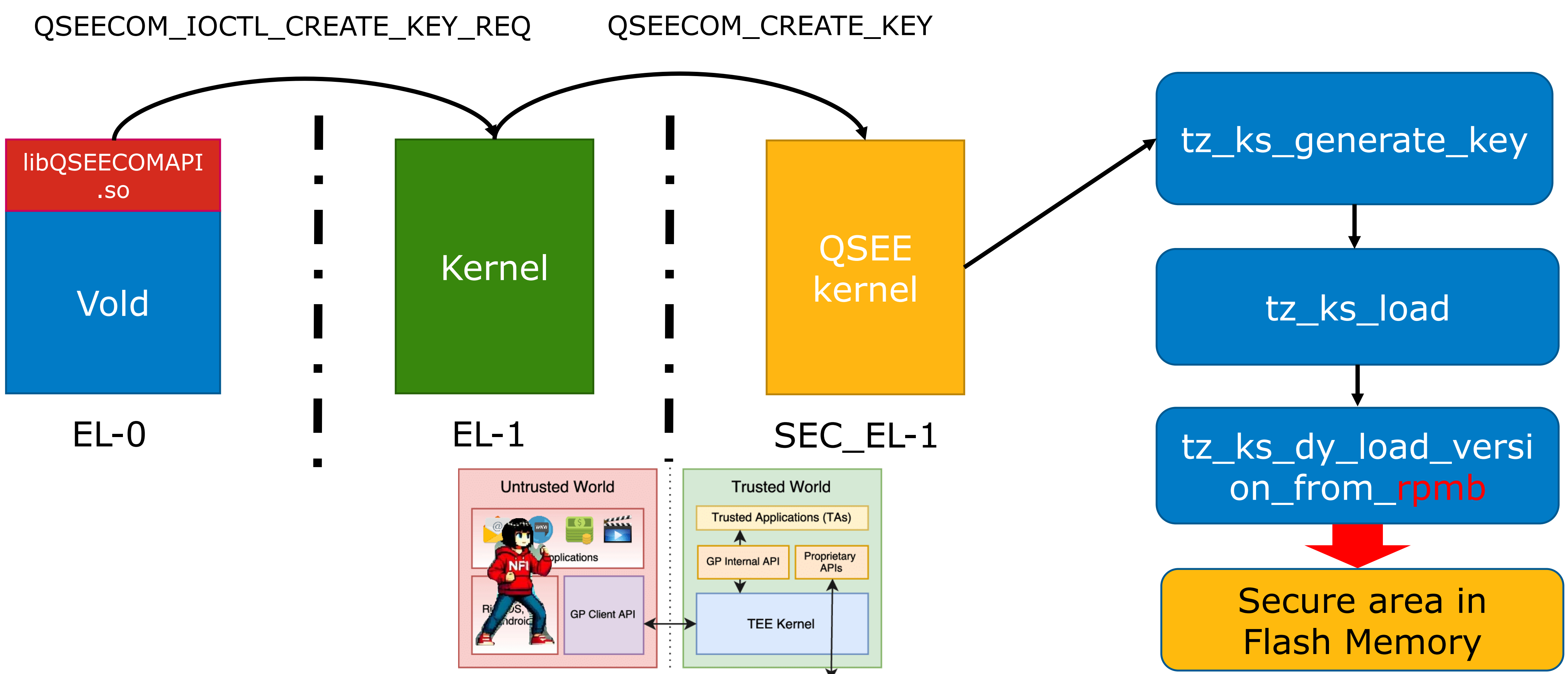


Decryption unsuccessful

The password you entered is correct, but unfortunately your data is corrupt.

To resume using your phone, you need to perform a factory reset. When you set up your phone after the reset, you'll have an opportunity to restore any data that was backed up to your Google Account.

Case 1(cont): Software Reverse Engineering



QSEECOM_IOCTL_CREATE_KEY_REQ

QSEECOM_CREATE_KEY

libQSEECOMAPI .so

Vold

Kernel

QSEE kernel

EL-0

EL-1

SEC_EL-1

tz_ks_generate_key

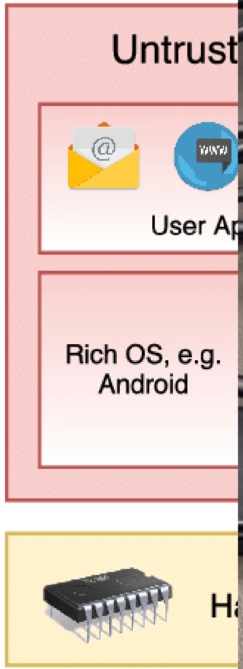
tz_ks_load

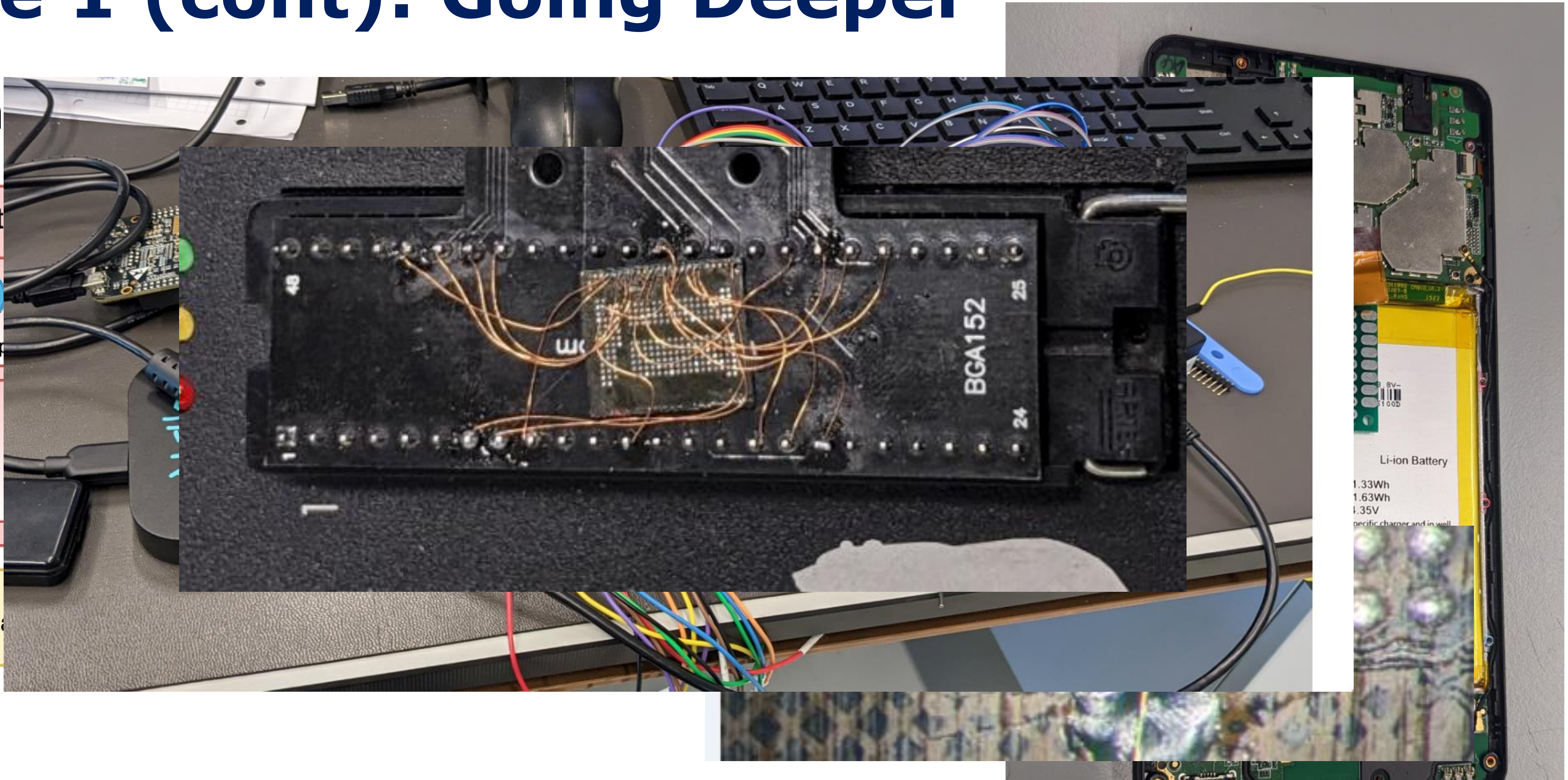
tz_ks_dy_load_version_from_rpmb

Secure area in Flash Memory

Case 1 (cont): Going Deeper

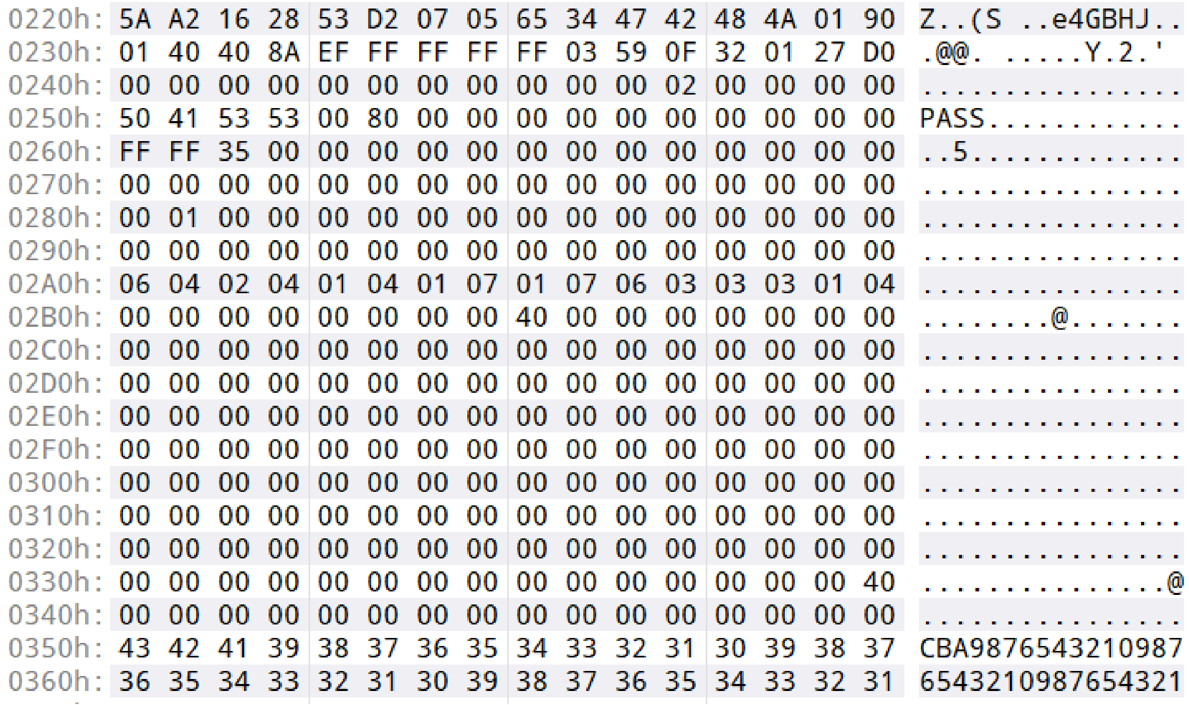
- Mon



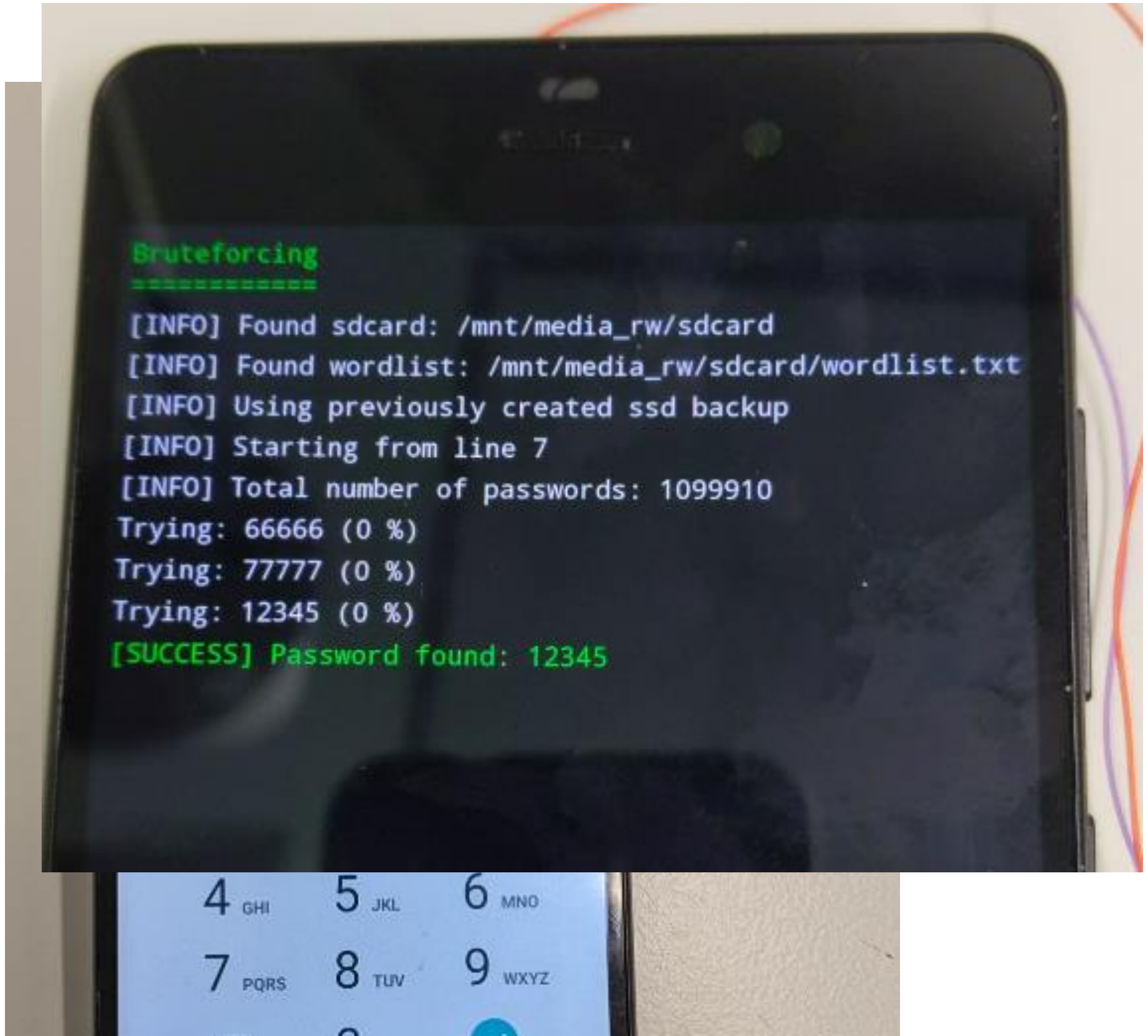


Case 1 (cont): Getting the key and Profit!

- Found the necessary key deep in HW
- Edit the secret area and device was back to the original state!



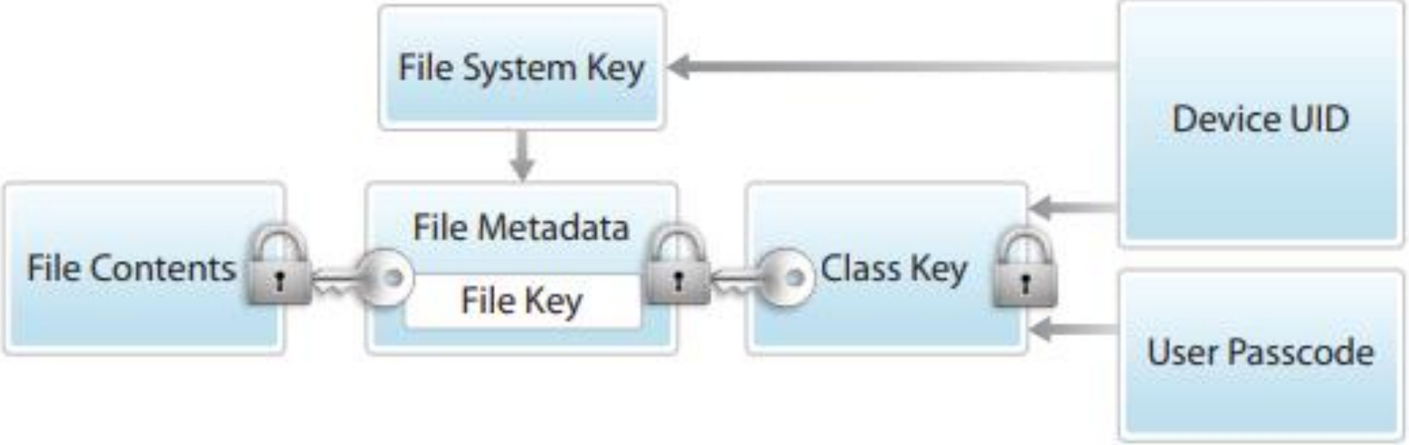
```
0220h: 5A A2 16 28 53 D2 07 05 65 34 47 42 48 4A 01 90  Z..(S ..e4GBHJ..
0230h: 01 40 40 8A EF FF FF FF FF 03 59 0F 32 01 27 D0  .@@. .....Y.2.'
0240h: 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00  ................
0250h: 50 41 53 53 00 80 00 00 00 00 00 00 00 00 00 00  PASS............
0260h: FF FF 35 00 00 00 00 00 00 00 00 00 00 00 00 00  ..5.............
0270h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0280h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0290h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02A0h: 06 04 02 04 01 04 01 07 01 07 06 03 03 03 01 04  ................
02B0h: 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
02C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0300h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0310h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0320h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0330h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40  ...............@
0340h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0350h: 43 42 41 39 38 37 36 35 34 33 32 31 30 39 38 37  CBA9876543210987
0360h: 36 35 34 33 32 31 30 39 38 37 36 35 34 33 32 31  6543210987654321
```



```
Bruteforcing
============
[INFO] Found sdcard: /mnt/media_rw/sdcard
[INFO] Found wordlist: /mnt/media_rw/sdcard/wordlist.txt
[INFO] Using previously created ssd backup
[INFO] Starting from line 7
[INFO] Total number of passwords: 1099910
Trying: 66666 (0 %)
Trying: 77777 (0 %)
Trying: 12345 (0 %)
[SUCCESS] Password found: 12345
```

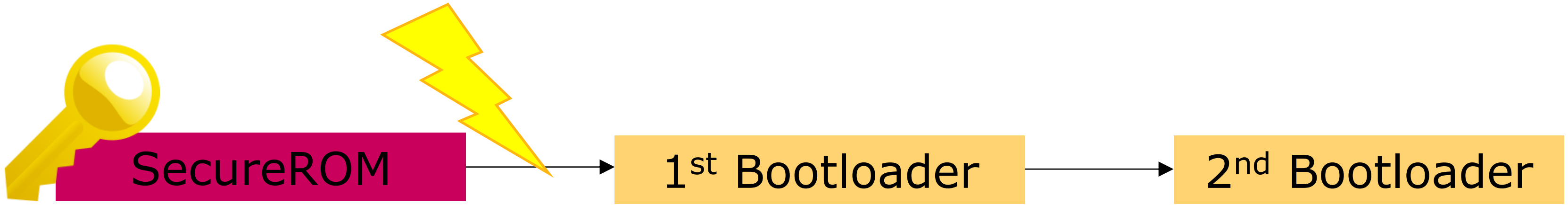
Case 2: Locked iPhone Case

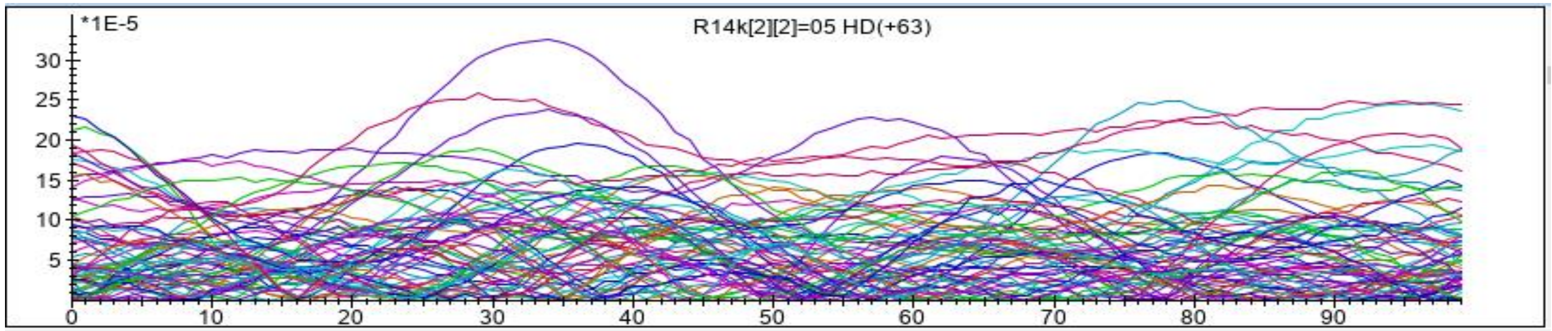
- Old case (before secure enclave)
- Too many wrong password attempts already
- On-device bruteforce: Too slow (device is “password” locked)
- Side-Channel Attack (Paper published in 2021 in CHES)

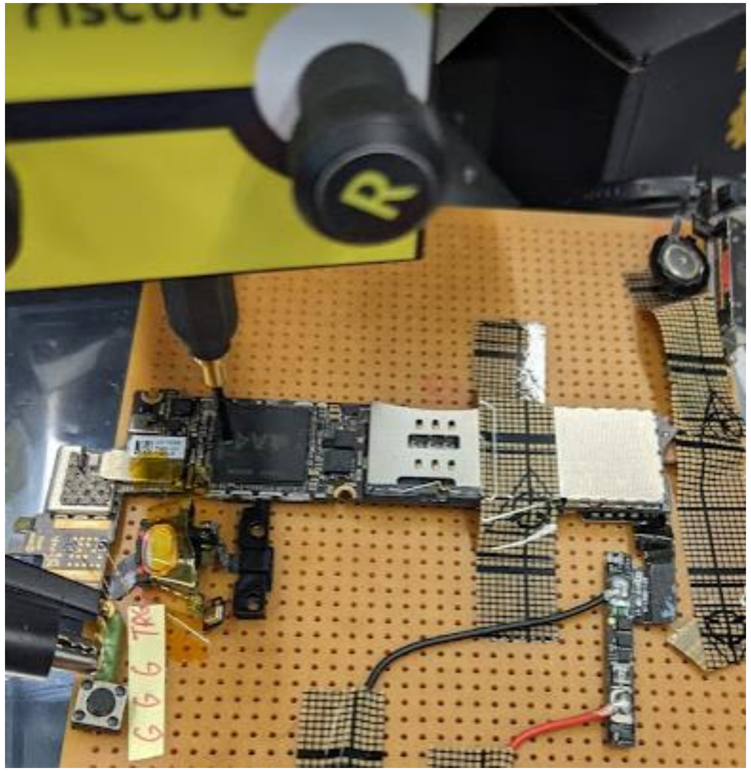


Case 2 (cont): Side Channel Attack

- Preparation:
  - ROM exploit to run arbitrary code
  - Repeat AES computation 400 million times
  - Collect traces and identify the key

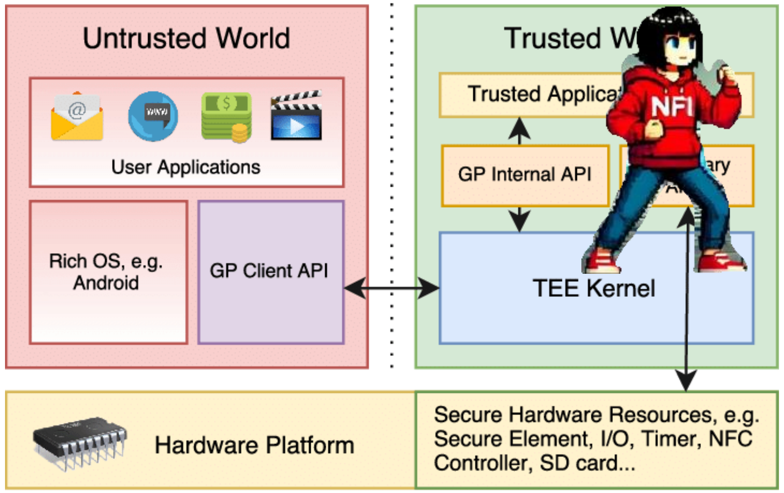






Case 2 (cont): Offline Brute-Force

- UiD Key identified (took years in the end)
- Plist parsed and offline brute-forcing the password
- Password found in 1 day!
- Case data extracted and police officers were so happy



Untrusted World

User Applications

Rich OS, e.g. Android

GP Client API

Trusted W

Trusted Applica

GP Internal API

ary

A

TEE Kernel

Hardware Platform

Secure Hardware Resources, e.g. Secure Element, I/O, Timer, NFC Controller, SD card...

Takeaways

- Mobile forensic investigations getting more complicated than ever
- However there is (almost) always a way to compromise the device
- Do not focus on one layer of the computer system when conducting forensics research
- Think out-of-the-box: Hacker’s mind. Where can we sneak into the system and break the security feature?
- Keep an eye on the recent development of techniques, as well as zero-day, code leak, and other exploits