Traitement de téléphones immergés

Fabien THOMAS-BRANS
Thibaut HECKMANN

16 octobre 2023, Atelier de recherche gendarmerie "Des larves et des âmes : sciences exactes et humaines alliées contre le crime"

Introduction

Introduction

Digital Investigation (criminalistique numérique) :

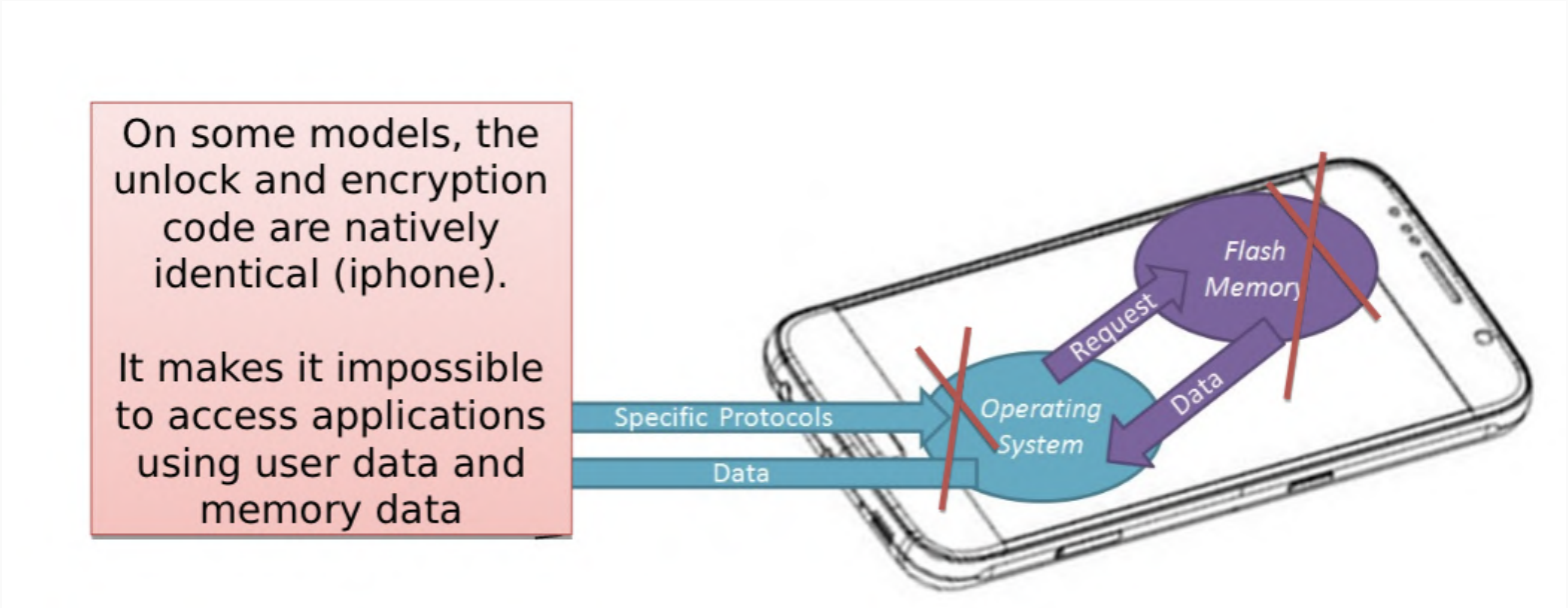
- Extraction : accéder aux données, réparation, rétro-conception, déchiffrement.
- Analyse sans interprétation.
- Analyse avec interprétation (intentionnalité) et récupération de données effacées.

Le chiffrement des données

Le chiffrement des données

Les mécanismes de chiffrement par mot de passe, reconnaissance faciale ou palmaire deviennent la norme (chiffrement natif) :

- Sans la clé de chiffrement impossible de naviguer sur le téléphone (blocage du système de fichier),
- Sans la clé de chiffrement impossible d'accéder aux données des utilisateurs (user data) en mémoire (blocage physique de la mémoire).



La rétro-conception

La rétro-conception

La rétro-conception est la recherche des vulnérabilités du système :

- Elle peut être logicielle (Software),
- ou matérielle (Hardware).

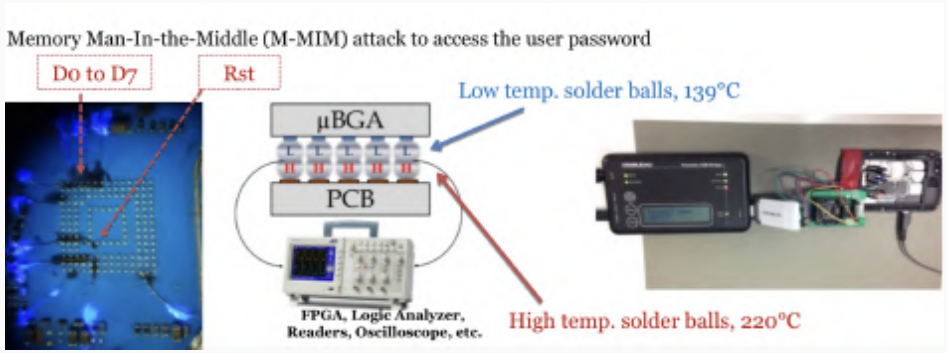


Figure 1

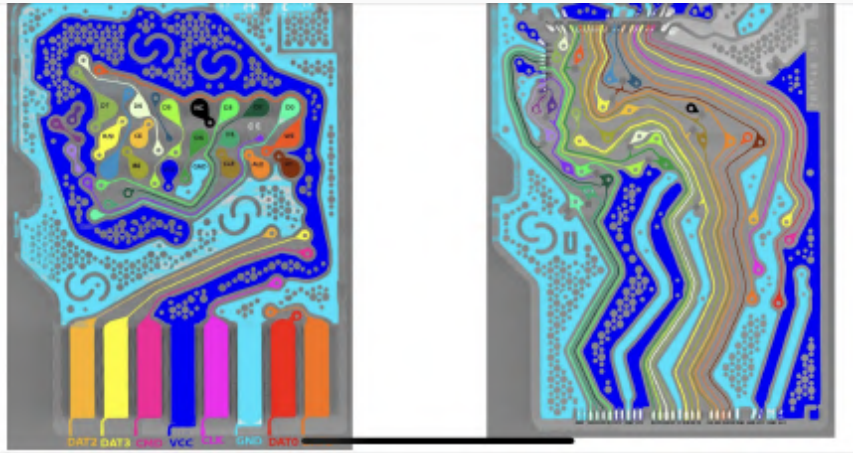


Figure 2

La rétro-conception

La rétro-conception vise donc à connaître le fonctionnement et l'architecture du système.

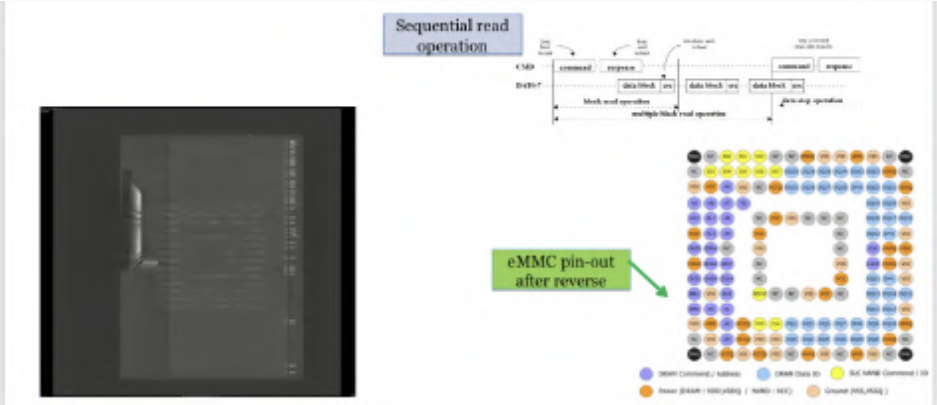


Figure 3

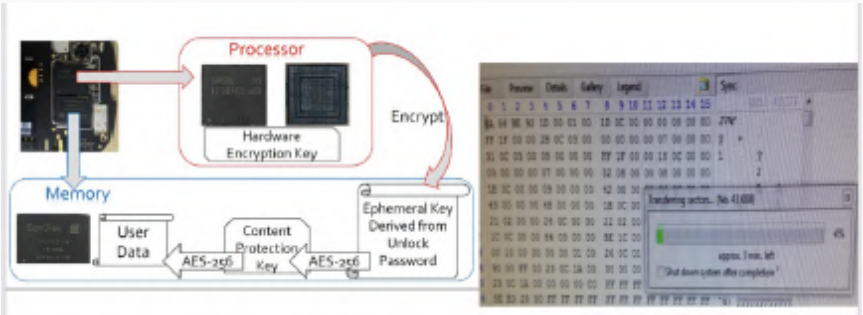


Figure 4

Les attaques matérielles (Hardware)

Les attaques matérielles (Hardware)

Les attaques matérielles visent à exploiter les vulnérabilités pour retrouver la clé de chiffrement

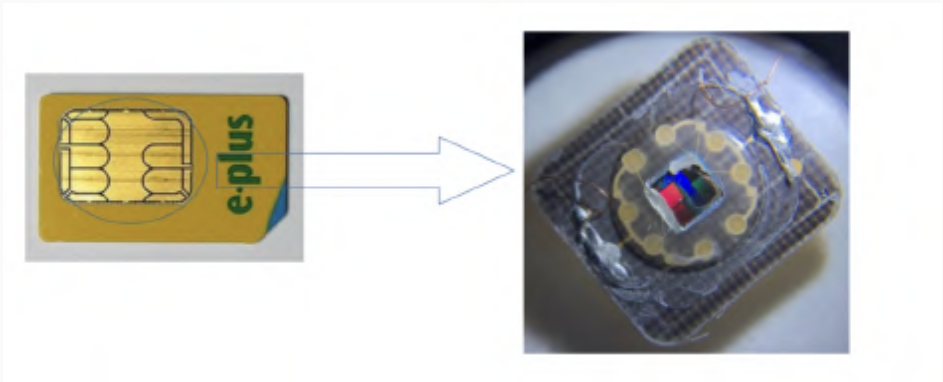


Figure 5

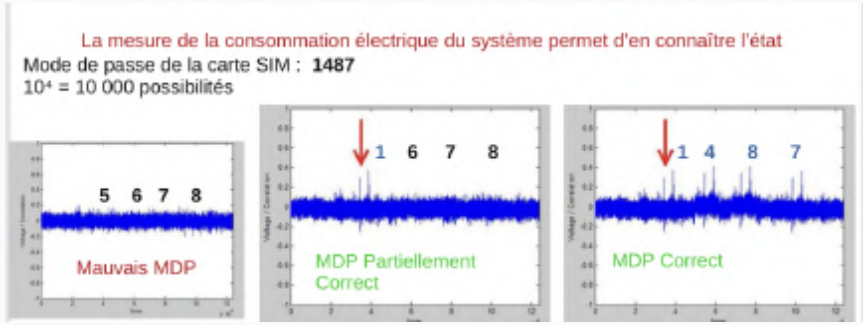


Figure 6

Objectif

Objectif

Extraction des données :

- Pas un SAV
- Réparation suffisante pour un déchiffrement de la donnée (démarrage avancé)
- Réparation suffisante pour accéder à la donnée (connexion USB)
- Pas besoin de toutes les fonctionnalités

Conditionnement

Conditionnement

Mise sous scellés particulière :

- Eau impure (vase, algues...)
- Eau salée
- Conditionnement dans de l'eau claire

Process

Démontage

Figure 7: iPhone 6S ouvert

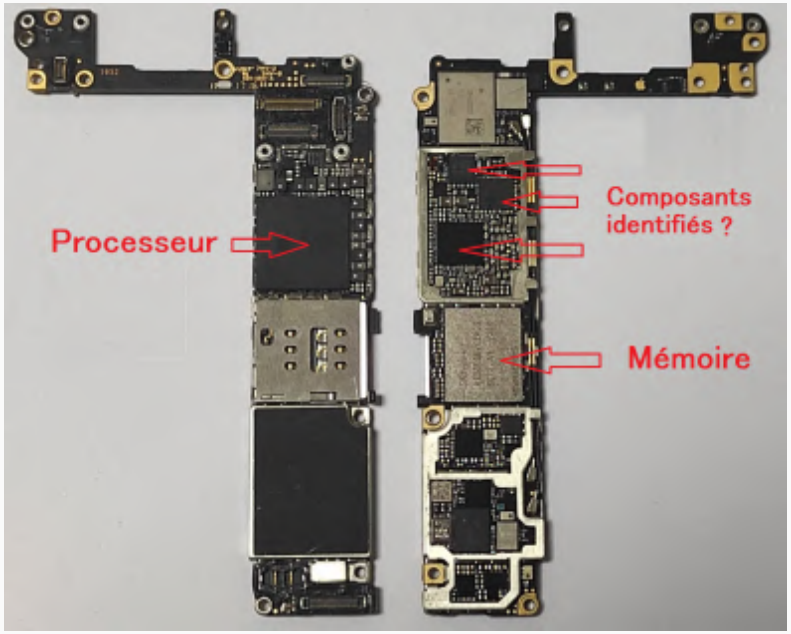


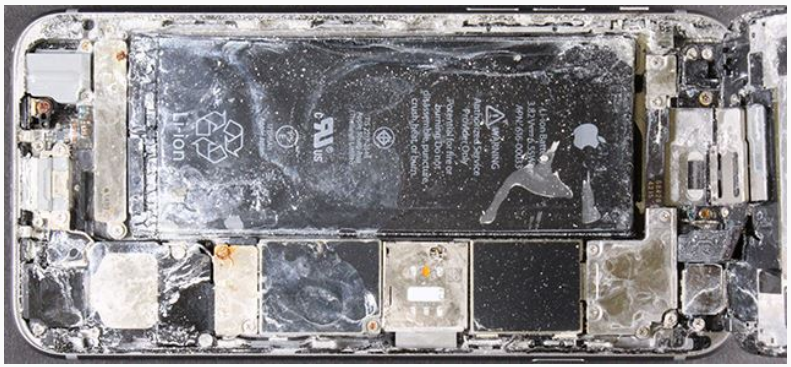
Figure 8: Carte électronique interne

Séchage/Nettoyage

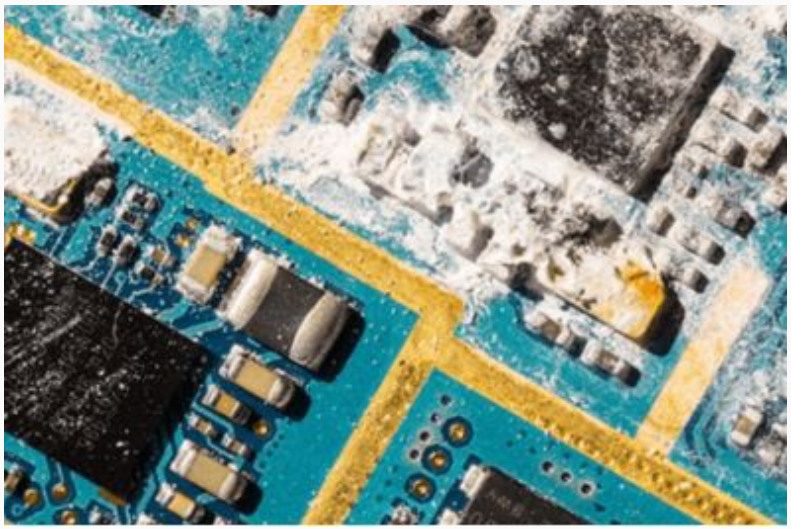
Méthode internet (CNET)

Étuve Binder

Séchage/Nettoyage



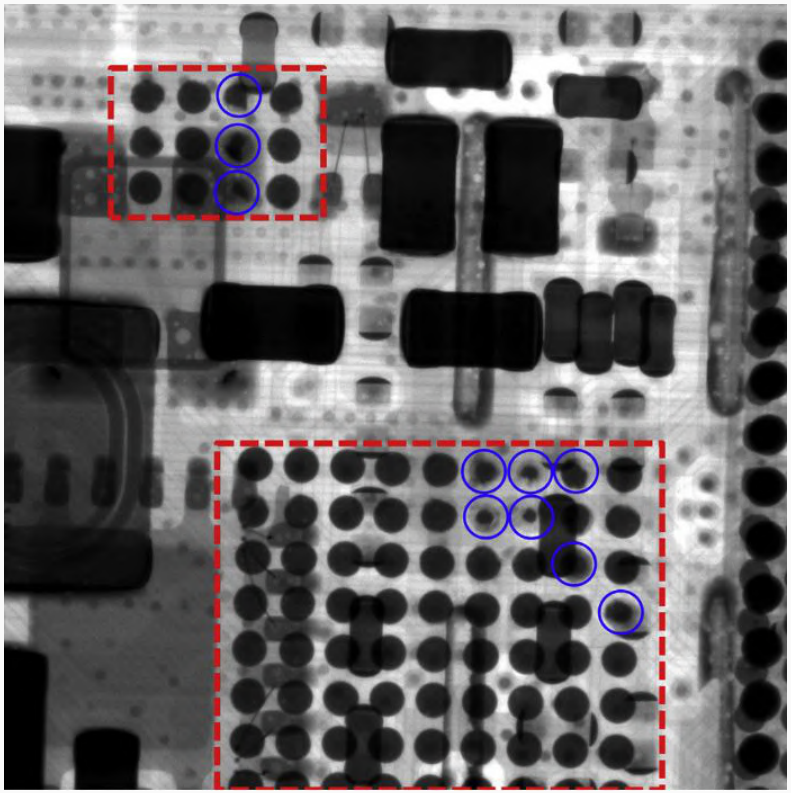
iPhone dans l'eau de mer (Recoveo)



Traces de corrosion sur des composants (victorypcb.com)

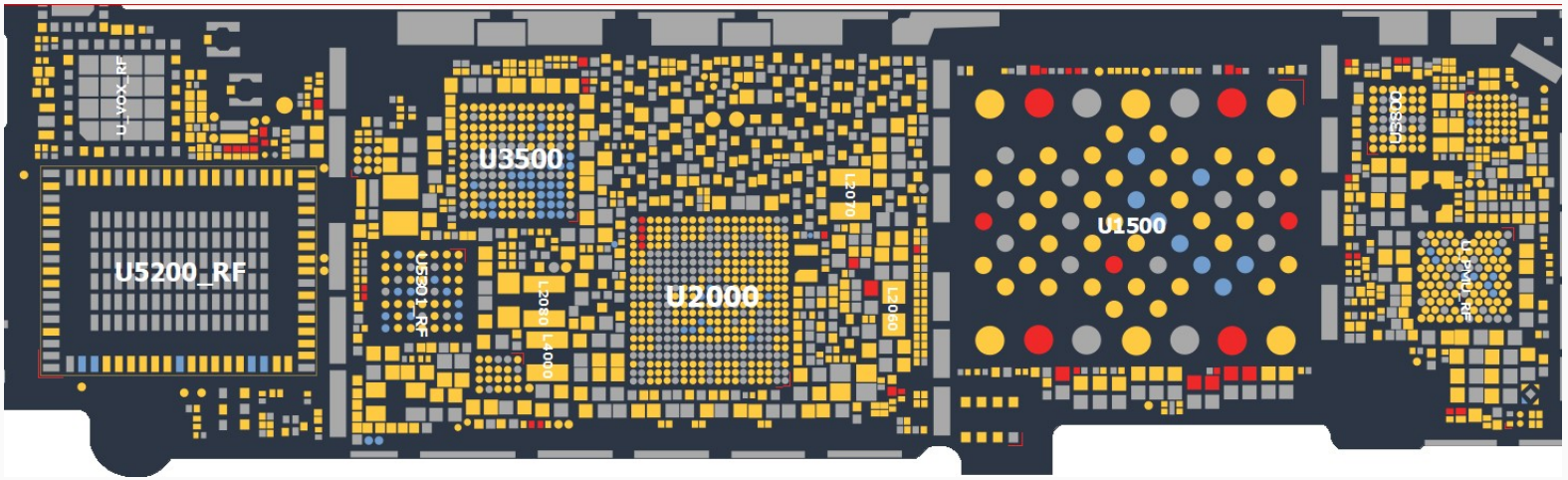
Observation

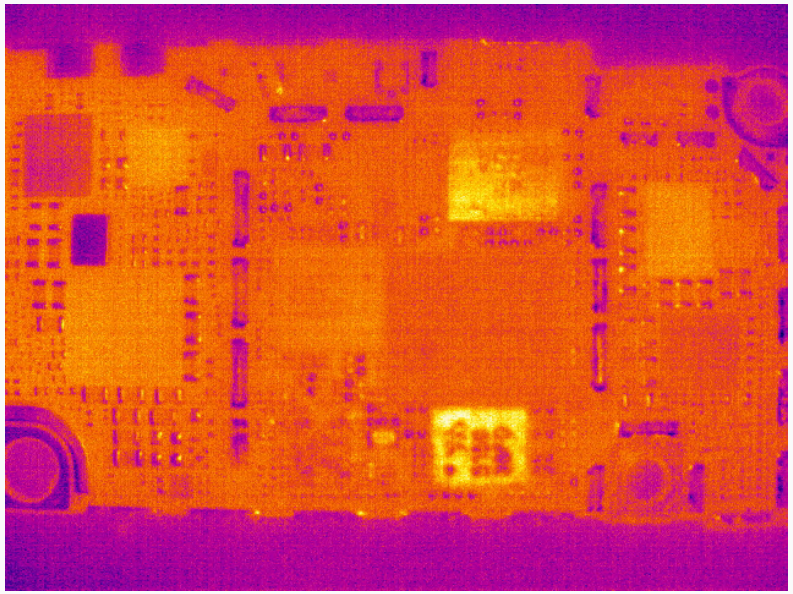
iPhone 12 pro en vue RX (Ifixit)



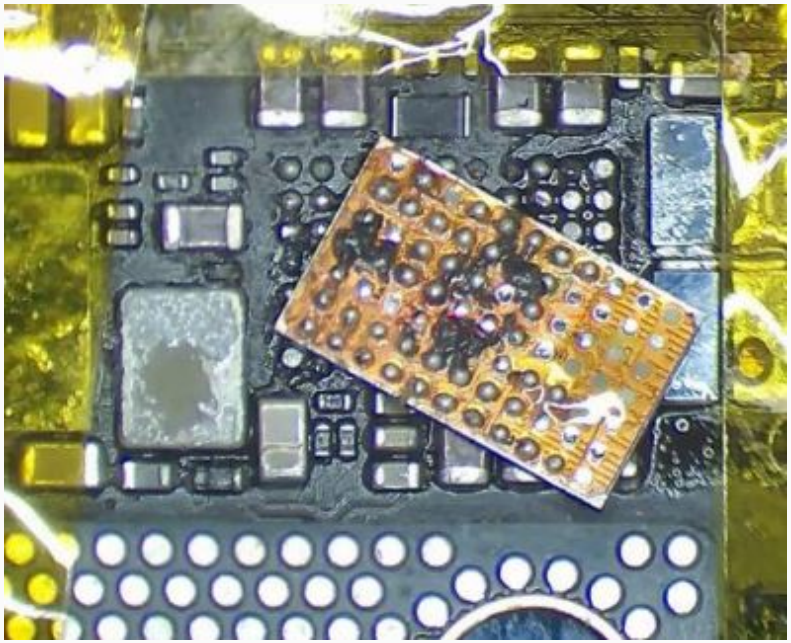
Composants corrodés aux RX (Aya Fukami)

Diagnostic

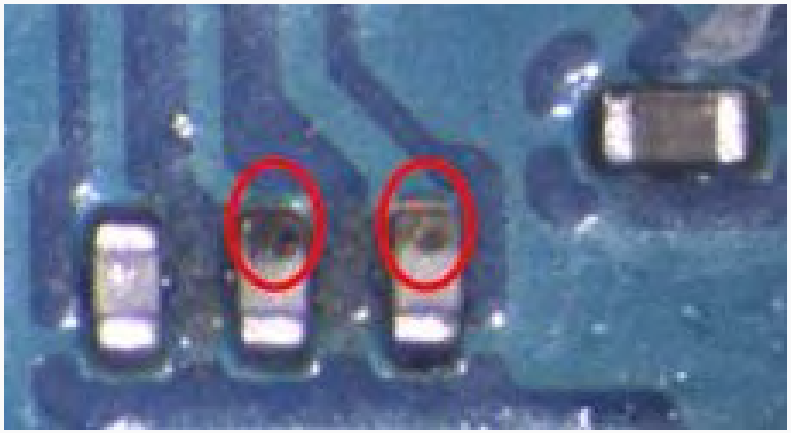




Réparation

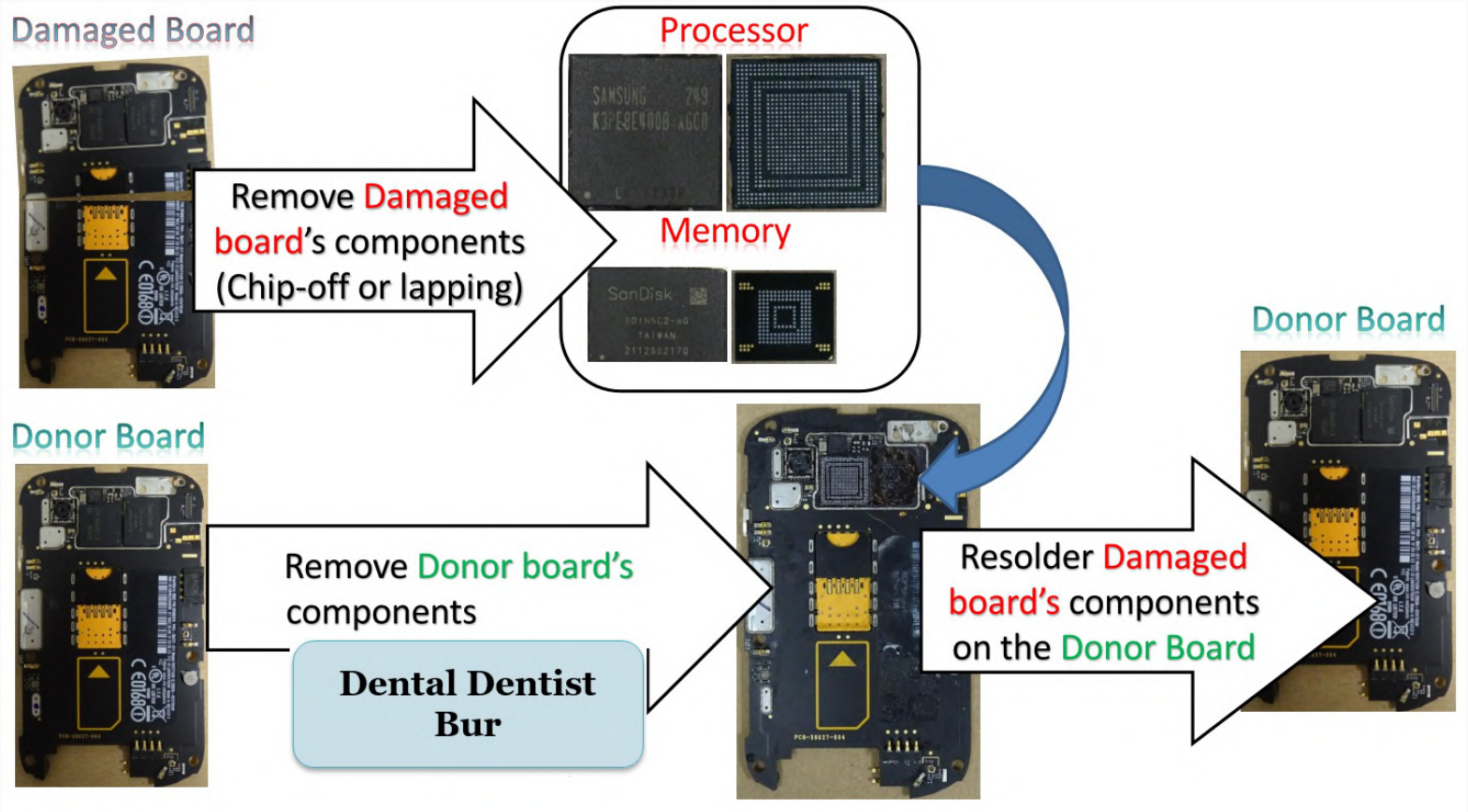


Méthode internet (Rewa tech)



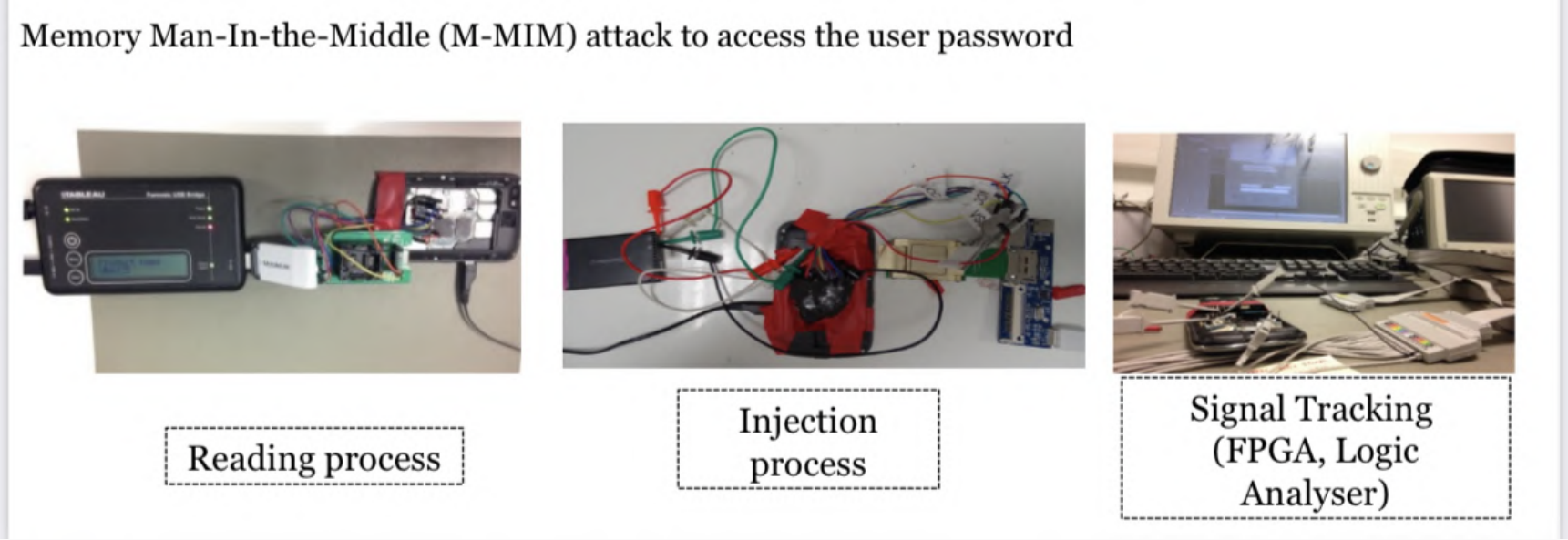
Capacités corrodées (Aya Fukami)

La transplantation judiciaire

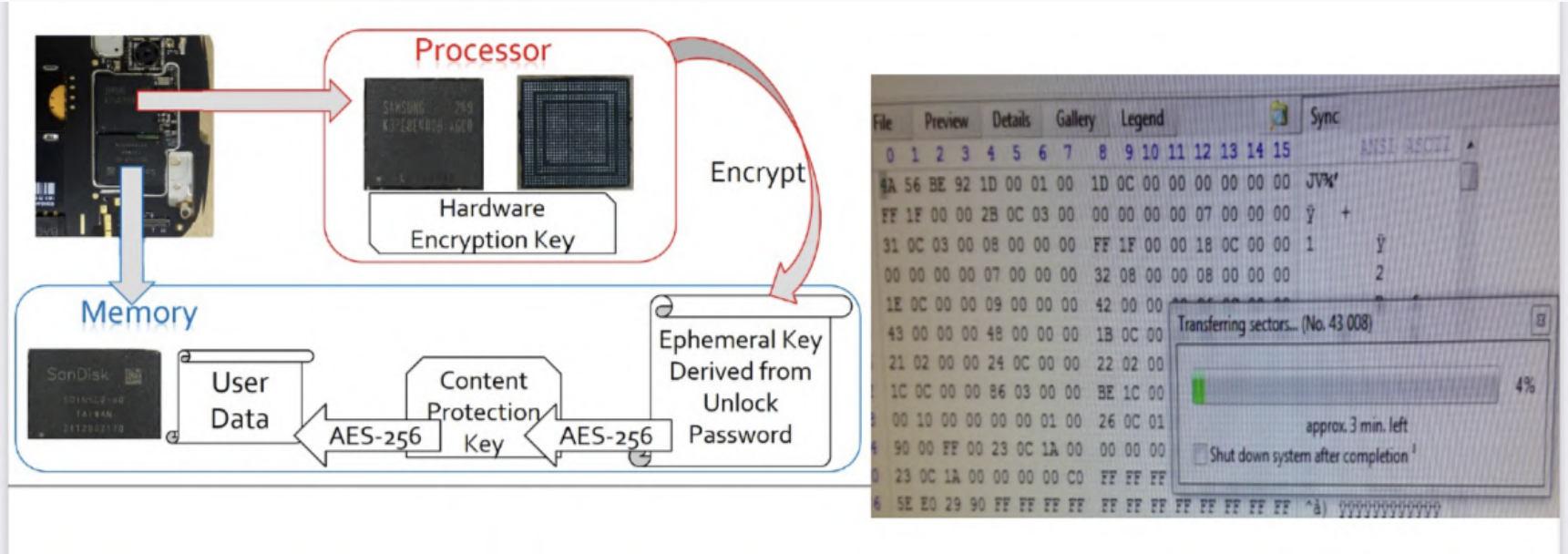


Principe de la transplantation

La transplantation judiciaire 2

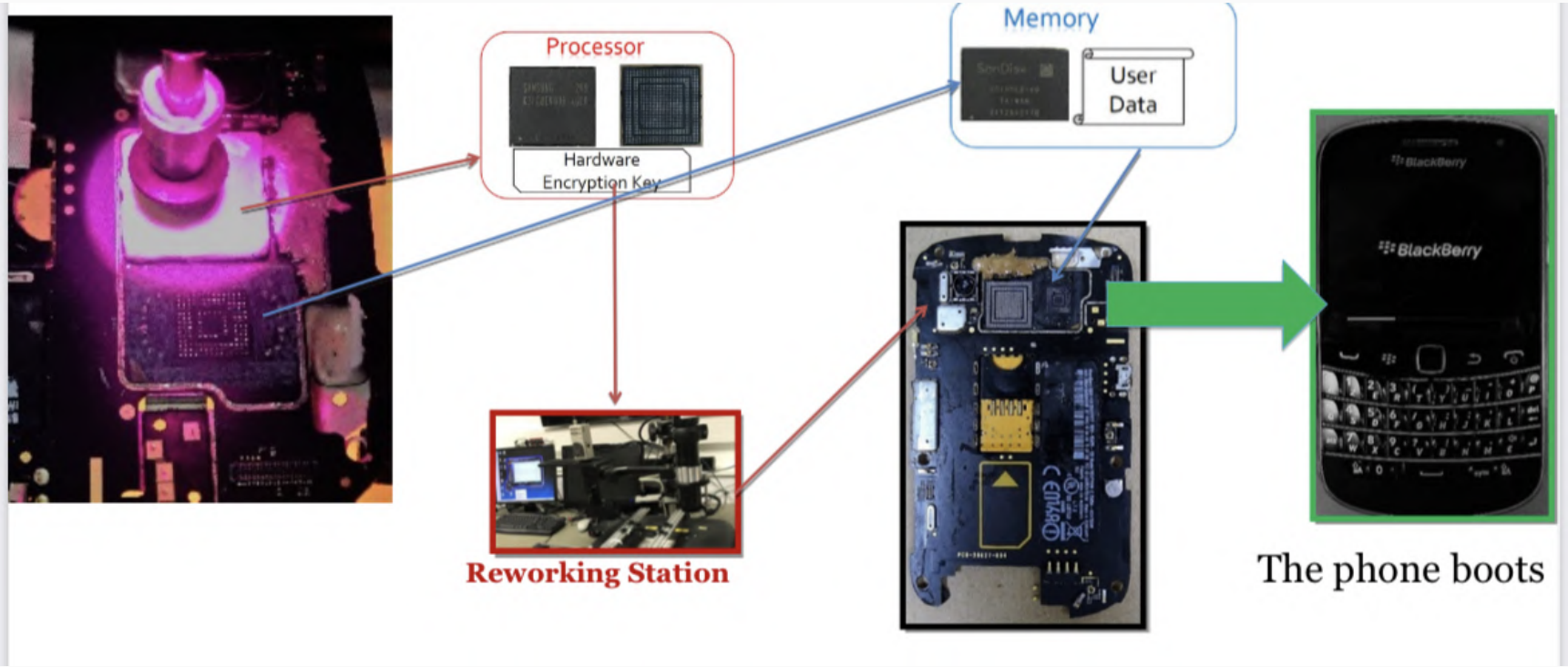


La transplantation judiciaire 3



Récupération des clés de chiffrement du téléphone immergé

La transplantation judiciaire 4



Le téléphone immergé redémarre

Questions ?