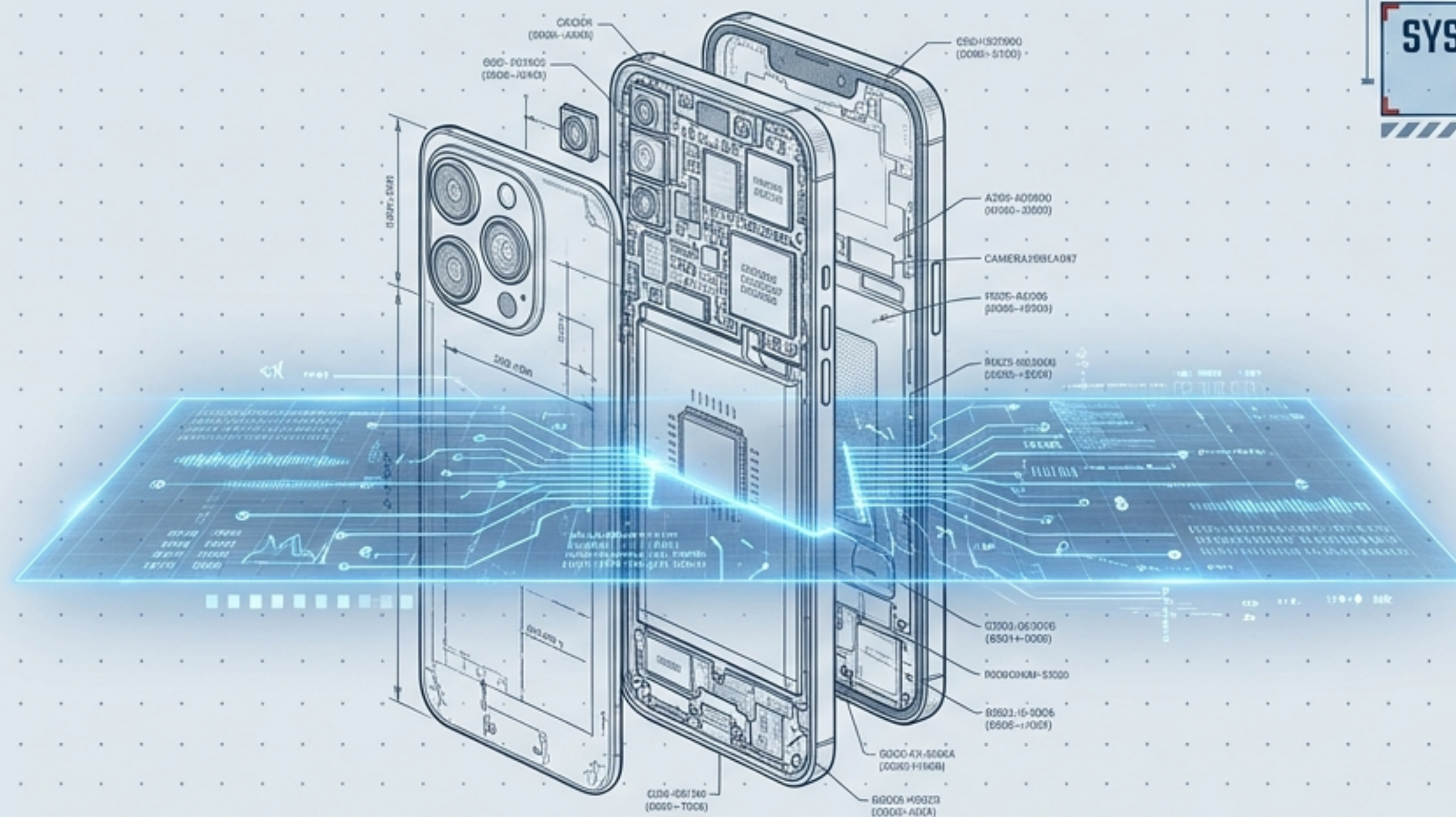


**SYSTEME : RENSEIGNEMENT
CLASSIFIE // FR_CA**



Analyse Forensique Mobile

Décortiquer l'architecture, contourner la sécurité
et extraire la vérité numérique.

Chiffrement & Vie Privée



Refus d'intégration de portes dérobées (backdoors).

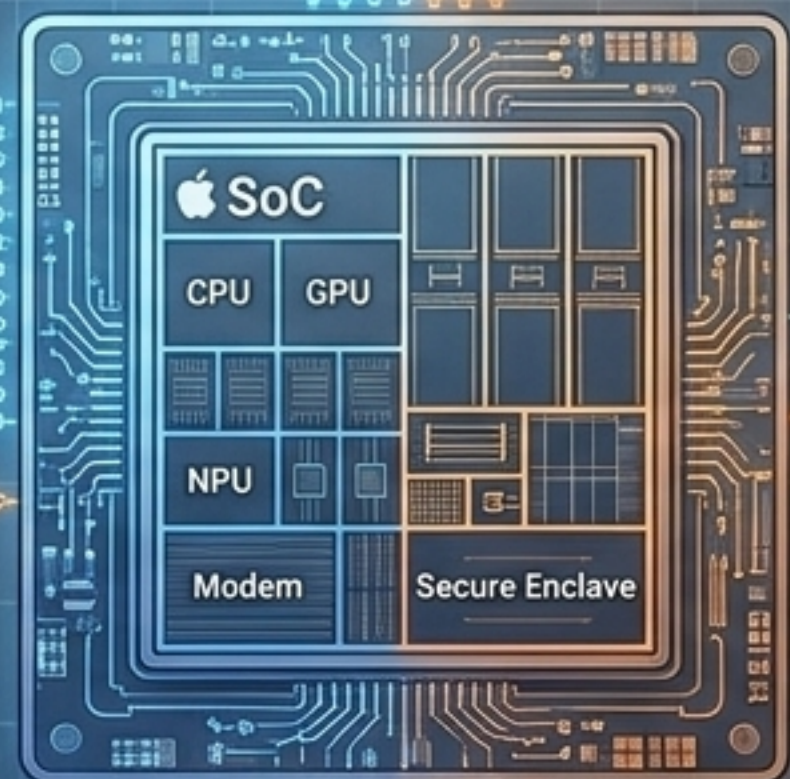
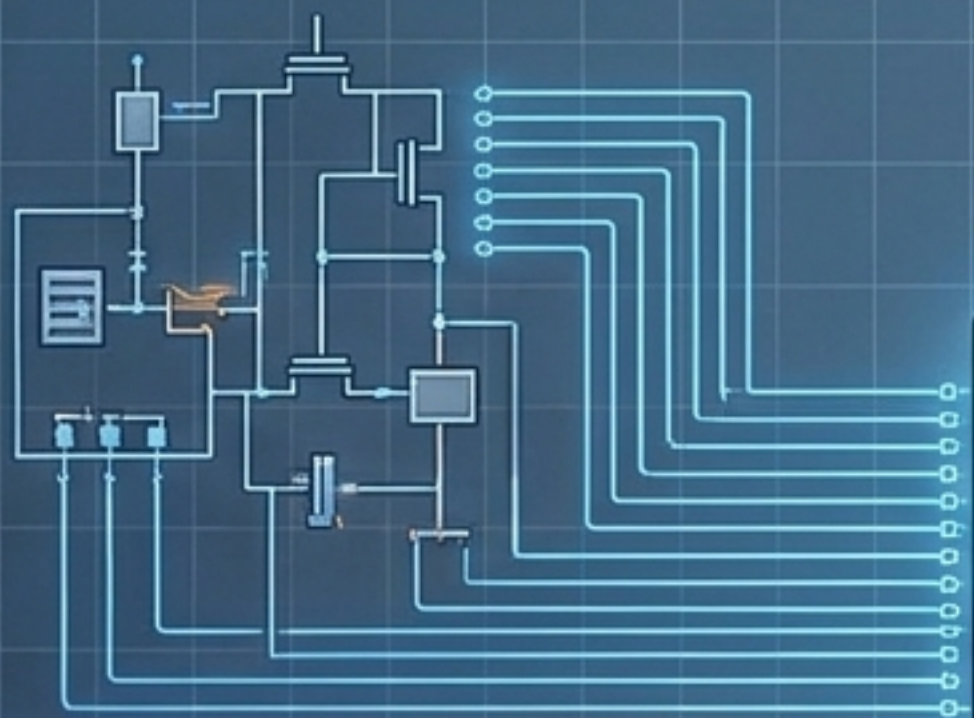
Sécurité Nationale & Enquête



Recours forcé à des failles tierces (Zero-days).

Le précédent de San Bernardino (2016) :
L'affrontement légal et technique entre Apple et le FBI.

Le Paradoxe : Une sécurité accrue pour l'utilisateur signifie une complexité exponentielle pour l'enquêteur.



Volatilité Extrême



Processus en arrière-plan continuellement actifs.

Les modifications automatiques du système altèrent les preuves même lorsque l'appareil semble éteint.



Obsolescence Rapide

Correction quasi instantanée des failles (zero-day) par les fabricants.

Les méthodologies d'investigation sont hautement périssables.



Écosystème Cloud

Synchronisation multi-appareils immédiate.

Une suppression locale par l'utilisateur peut déclencher une destruction globale des données.

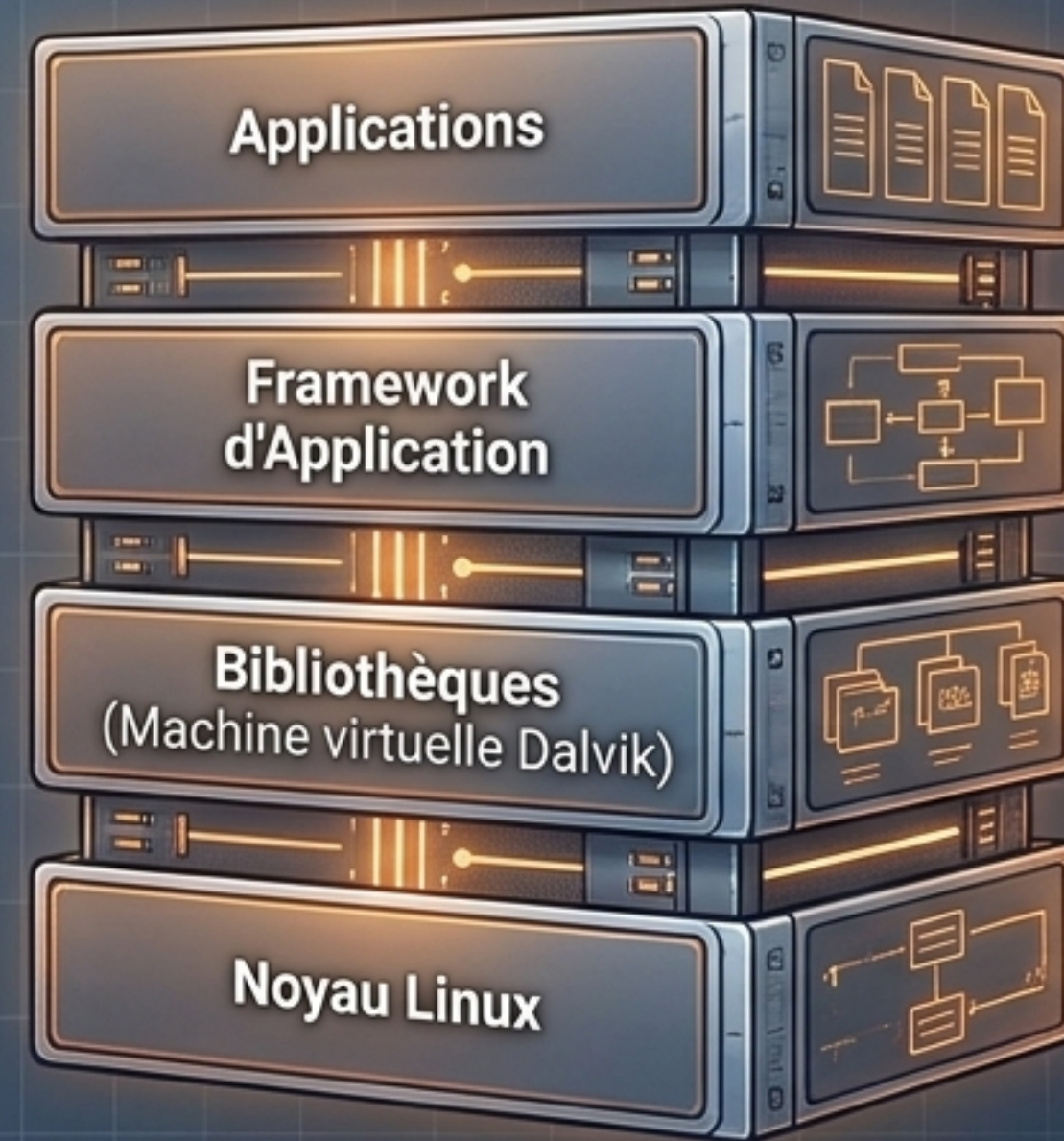
Cartographie Architecturale : iOS vs Android

Architecture iOS (Fermée / Sandboxed)



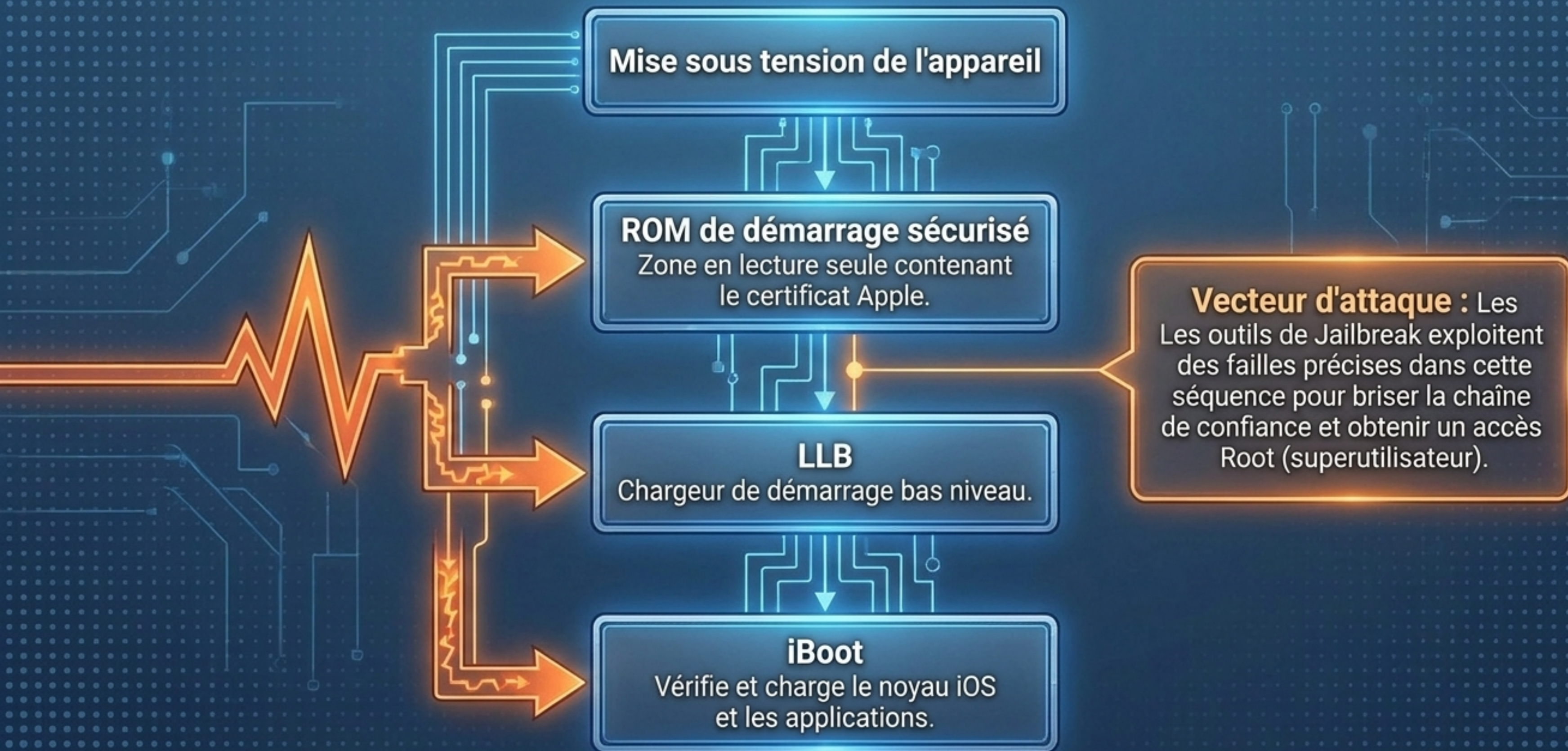
Applications isolées en bac à sable (Objective-C). L'installation de logiciels antivirus est impossible en raison de la segmentation stricte d'Apple.

Architecture Android (Ouverte / Modulaire)



Code source ouvert (Java). Les applications s'exécutent de manière isolée mais conservent une possibilité d'accès natif au matériel.

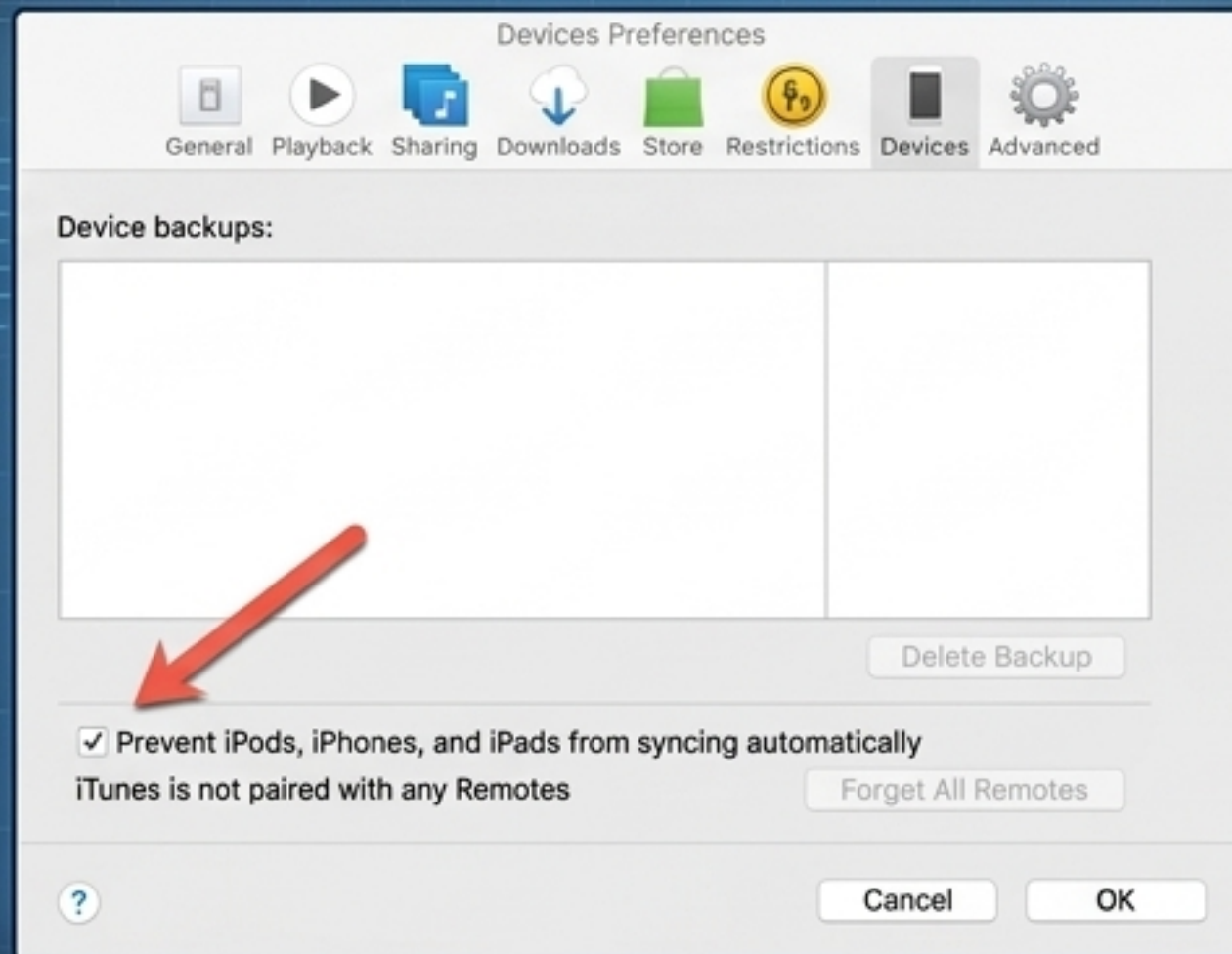
Séquence de Démarrage Sécurisé (iOS)



L'Hôte de Confiance : Extraction Logique iTunes

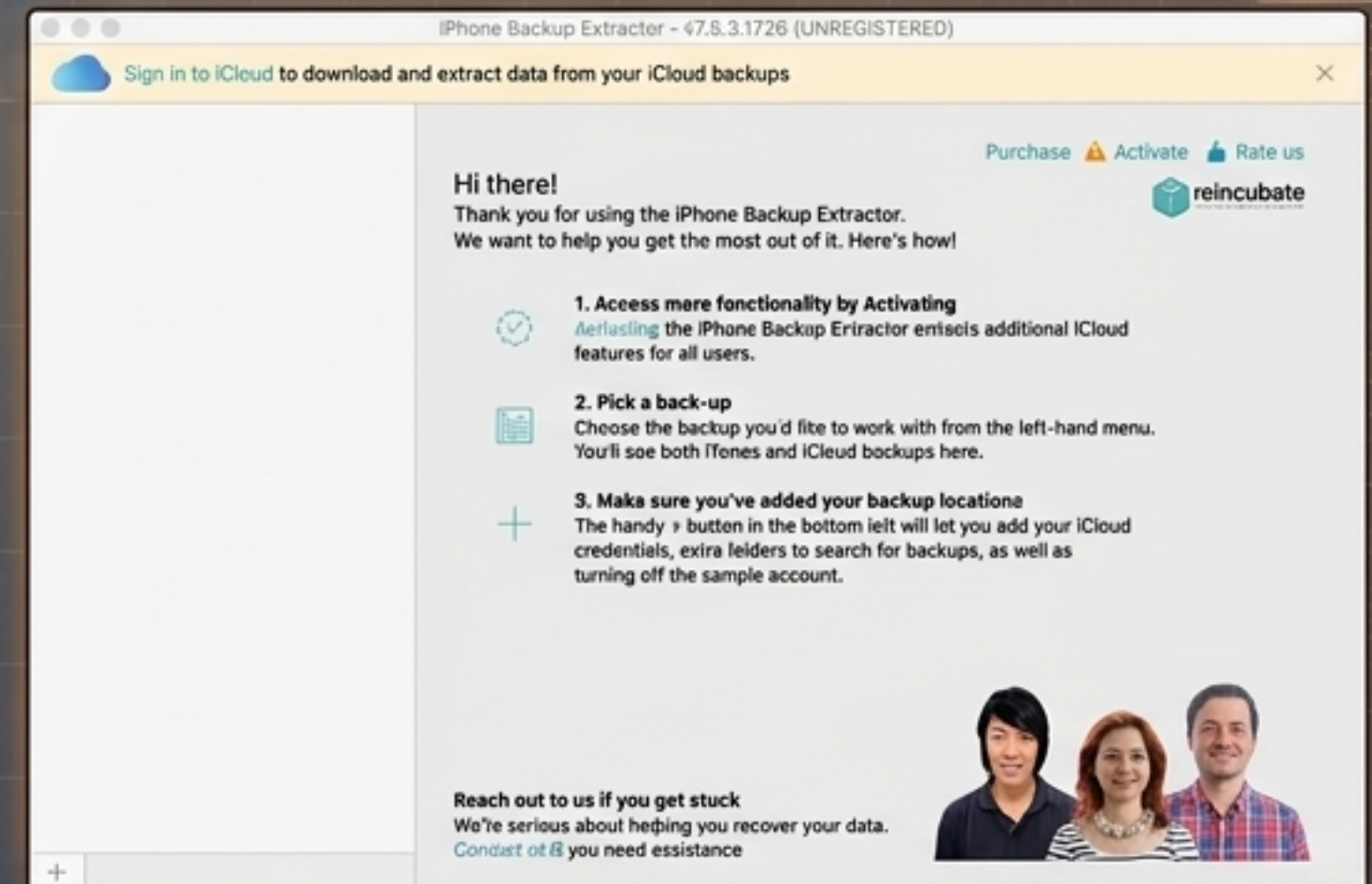
Étape critique : Désactivation

Désactiver la synchro automatique est vital pour éviter l'écrasement irrémédiable des preuves.



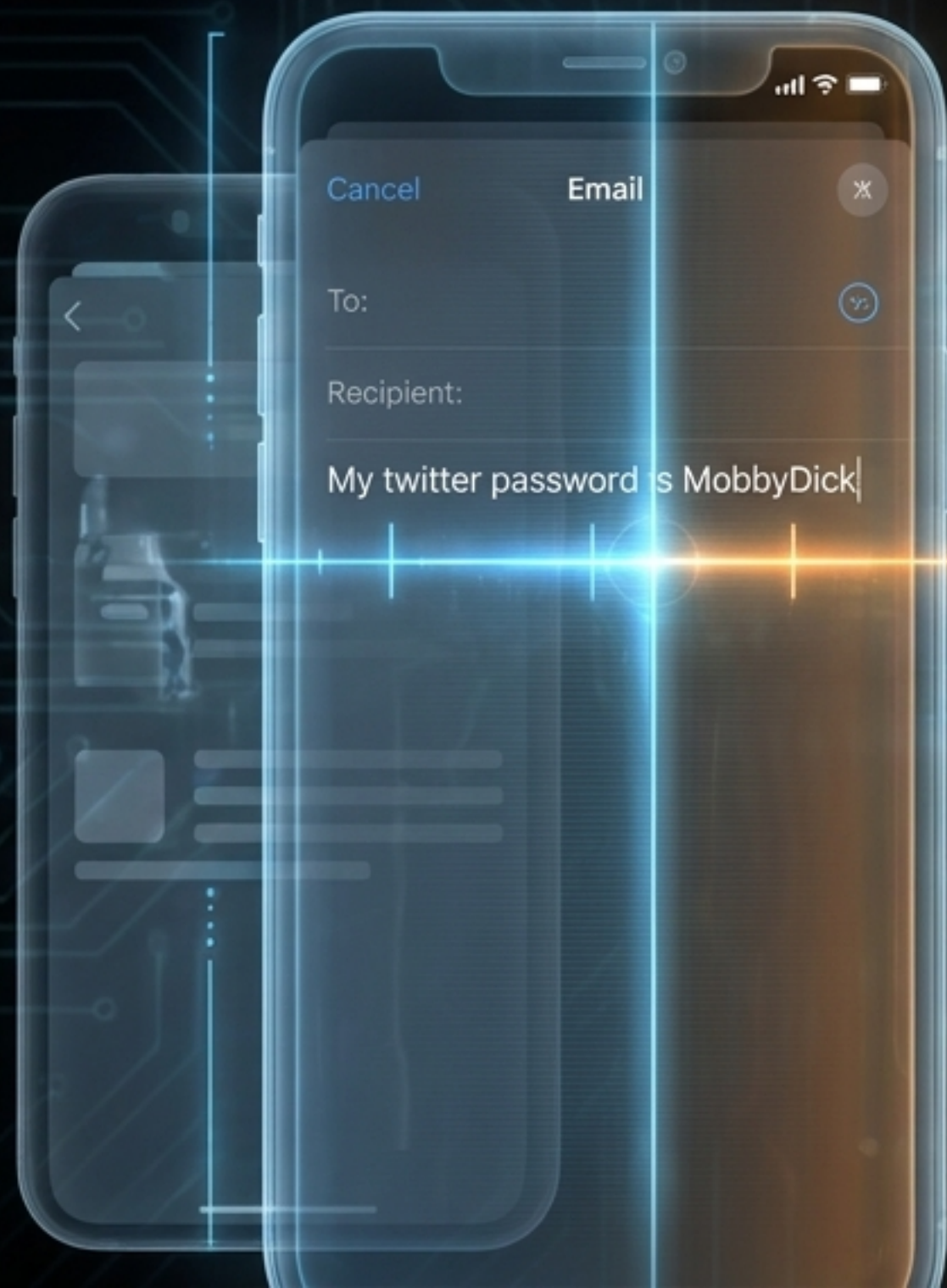
Extraction des Données

La sauvegarde contourne le code PIN (déjà approuvé par le PC hôte). Les données sont transférées et stockées, souvent sans aucun chiffrement.



Les Empreintes Fantômes : Instantanés iOS

Exploitation du fichier PNG système invisible généré lors du basculement multitâche.



Chemin du répertoire :

`/private/var/mobile/Library/Caches/Snapshots`

Le Gain Tactique :

Récupérer un mot de passe copié-collé, un brouillon de courriel supprimé, ou une note éphémère capturée à la milliseconde où l'application est passée en arrière-plan.

Décoder les communications : L'Analyse SQLite

Fichiers Bruts

```
Directory of /private/var/mobile/Library/SMS  
..  
sms.db  
sms.db-shm  
sms.db-wal
```

Reconstruction (Requête SQL)

```
1 SELECT datetime(date/1000,  
2      'unixepoch','localtime')  
3      ,datetime(date_sent/1000,  
4      'unixepoch','localtime')  
5      ,person,body  
6 FROM sms  
7 WHERE thread_id = 310  
8 ORDER BY date
```

Résultat Lisible

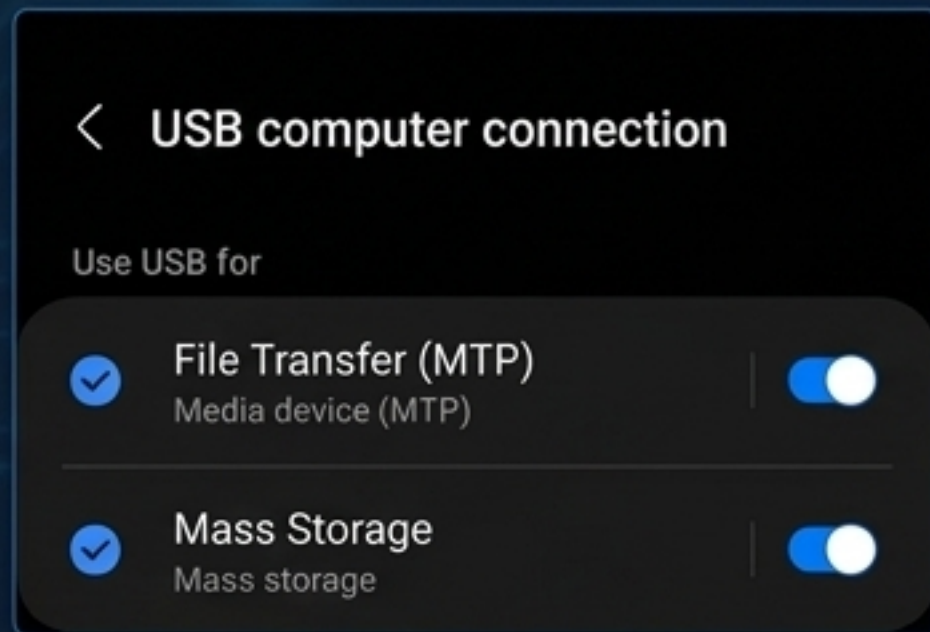
date_sent	person	body
2012-07-19 15:23:45	alakhani@ ymail.com	My twitter password is MobyDick
2012-07-19 15:24:10	alakhani@ ymail.com	Sent from my iPhone

Note forensique : iOS conserve l'heure du réseau de l'opérateur
ET l'heure locale, tandis qu'Android se limite à l'heure locale.

Préparation de l'environnement (Android)

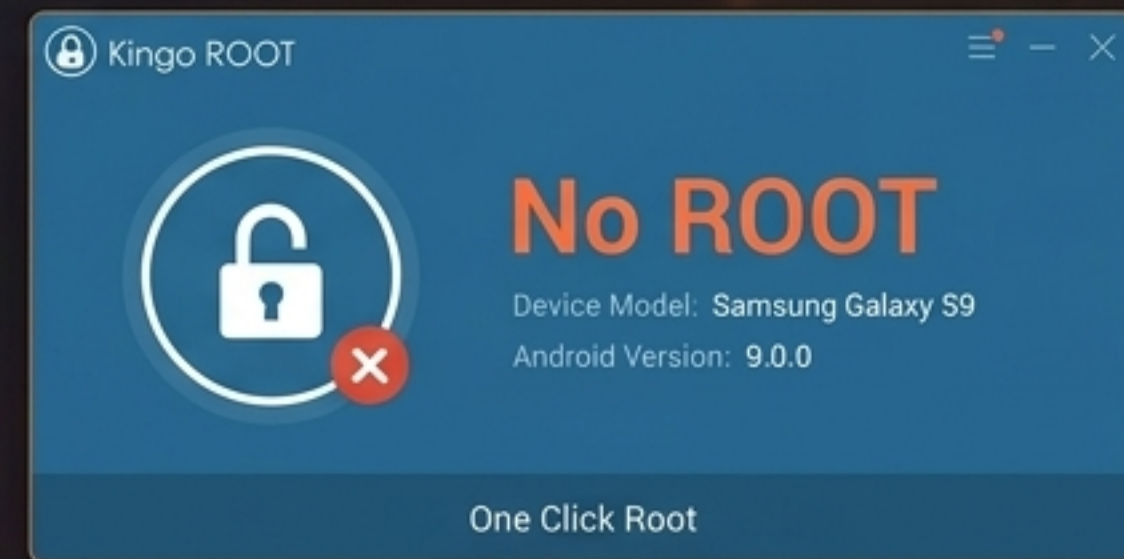
Le Pont Matériel

Activation préalable du périphérique multimédia (MTP) et du stockage de masse.



L'Escalade de Privilèges

Processus de Rooting requis pour générer une image physique intégrale avec des outils comme FTK Imager.



Alerte : À partir d'Android 6.0, le système de fichiers est chiffré par défaut. L'image disque extraite nécessitera un processus de déchiffrement ultérieur.

Évaluation Diagnostique : Le Risque du Root / Jailbreak

Analyse tactique de l'utilisation d'exploits logiciels intrusifs.

Le Gain Potentiel



Obtention des privilèges de superutilisateur (Root).



Extraction physique intégrale du système de fichiers.

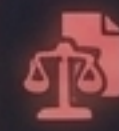


Contournement d'anciens codes PIN (via des utilitaires comme RedSn0w ou Pangu).

La Réalité Forensique (Risques)



Corruption potentielle et irréversible des données de l'utilisateur.



Risque majeur d'invalidation légale des preuves devant un tribunal.



Inefficacité confirmée sur la quasi-totalité des systèmes d'exploitation modernes (> iOS 10.3).

Conclusion Stratégique : Une procédure chirurgicale logicielle présentant un taux de mortalité légale beaucoup trop élevé pour les enquêtes modernes.

Contournement Matériel : Force Brute Automatisée

Exploitation de la confiance en l'interface utilisateur matérielle (HID).

Mécanisme de la Faille

L'OS mobile ne déclenche pas son mécanisme d'autodestruction des données face à une entrée perçue comme un véritable clavier physique USB.



Métriques d'Attaque

Délai système imposé :
Verrouillage de 30 secondes après 5 tentatives infructueuses.

Temps estimé d'exécution :
~16.6 heures d'automatisation totale pour casser un code PIN à 4 chiffres.



L'Artillerie Lourde Commerciale : Cellebrite UFED

Analyse des capacités et des limites de l'outil de référence forensique

Capacités Forensiques

Extraction logique et physique standardisée.

Récupération de données supprimées et attaque par force brute via une caméra physique.



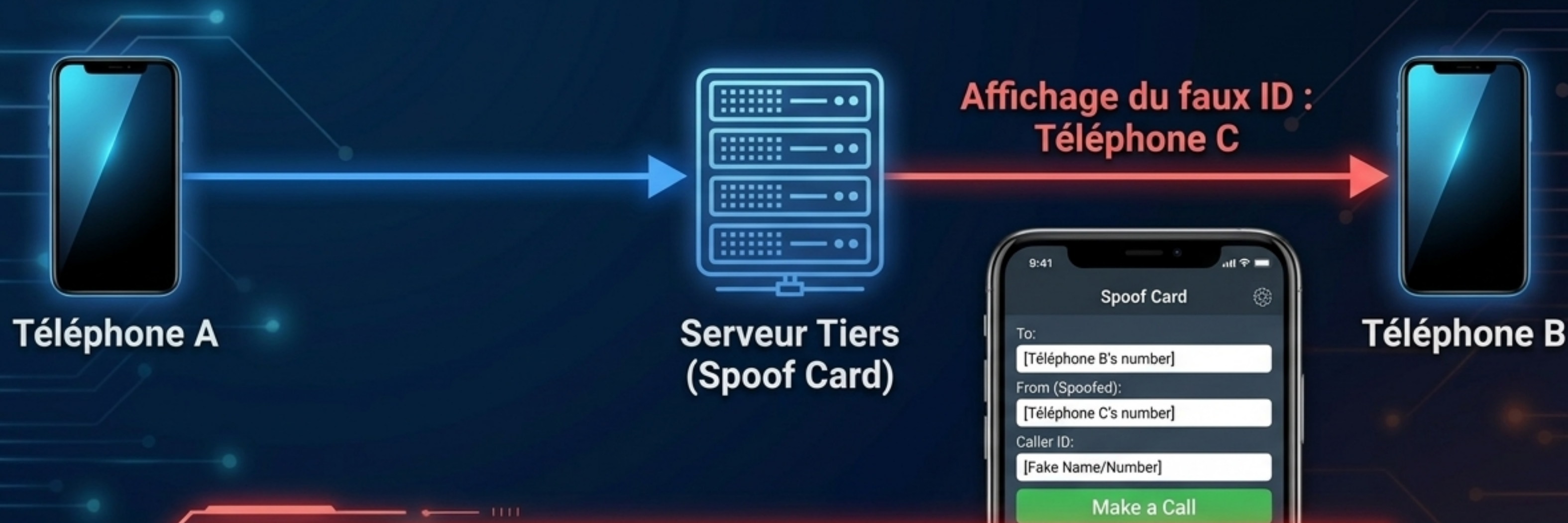
Limites Opérationnelles

Investissement financier majeur (~3000\$ USD).

Devenu inefficace contre les chiffrements modernes (iOS récent / Android 6+) en l'absence de vulnérabilités "zero-day" exploitables.

Conclusion Stratégique : Un outil puissant mais coûteux et obsolète contre la sécurité des appareils modernes sans exploitation spécifique.

L'illusion de l'identifiant : Usurpation (Spoofing)



Vecteur d'attaque : Piratage de la messagerie vocale

En usurpant le propre numéro de la victime pour appeler sa boîte vocale, le système est dupé. Croyant à un appel légitime du propriétaire de la ligne, il contourne le mot de passe.

⚠ Les journaux d'appels ne constituent jamais une preuve absolue.

Désanonymiser les Téléphones Jetables (**OSINT**)

Briser l'anonymat matériel grâce à la synchronisation Cloud.

1. La Cible Inconnue



Identification du numéro de la carte SIM prépayée (Burner Phone).

2. Le Leurre



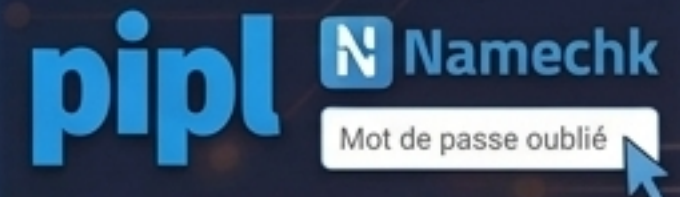
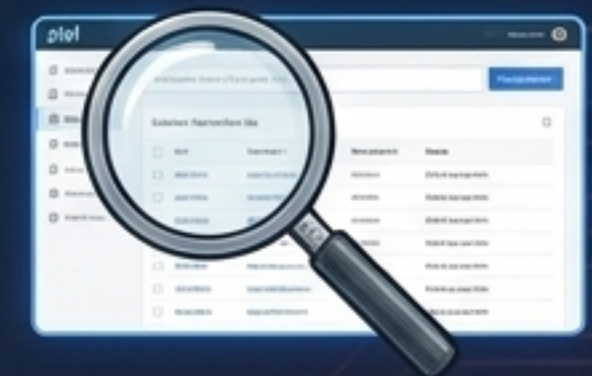
Création d'un "Faux Contact" intégrant ce numéro cible dans un appareil d'analyse forensique vierge.

3. Le Piège Social



Synchronisation agressive de ce répertoire fantôme avec des plateformes d'analyse et des réseaux (WhatsApp, LinkedIn, Instagram, Snapchat).

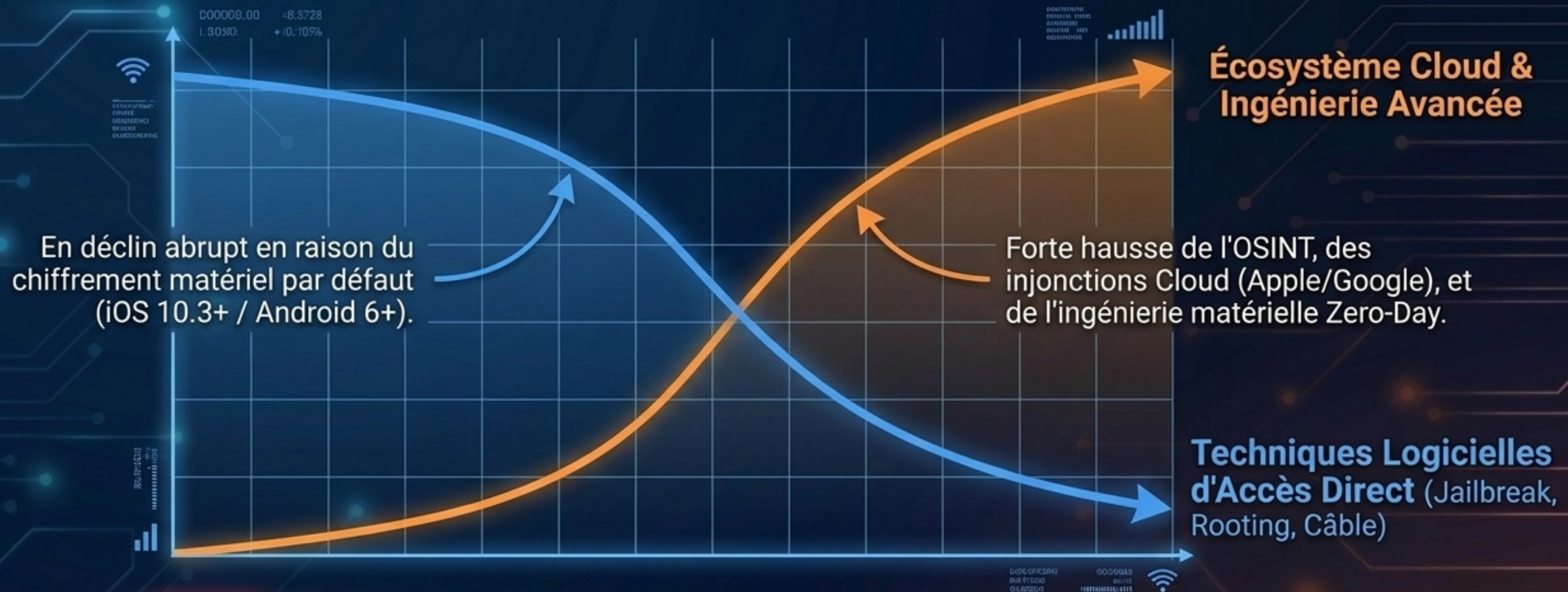
4. L'Extraction OSINT



Exploitation des fonctions "Mot de passe oublié" (via Pipl, Namechk) pour extraire l'identité réelle, le profil, un nom partiel ou un code postal.

ATTENTION: L'efficacité dépend de la compromission de la cible sur les plateformes sociales et de la disponibilité des données publiques.

Synthèse : La Course aux Armements Forensiques



Le Nouveau Paradigme : L'avenir de l'investigation numérique ne réside plus dans le port USB de l'appareil isolé, mais dans l'exploitation de l'écosystème Cloud qui l'entoure.