

Principles and Challenges of Mobile Forensic Analysis

Ce texte traite des principes et des défis complexes de la **criminalistique mobile**, en mettant l'accent sur les systèmes **iOS et Android**. L'auteur expose les obstacles techniques rencontrés par les enquêteurs, notamment le **chiffrement matériel**, la volatilité des données et les mesures de sécurité rigoureuses imposées par les fabricants. Le document illustre ces enjeux par l'affaire du **FBI contre Apple** en 2016, soulignant le conflit entre le droit à la **vie privée** et les nécessités judiciaires. Il détaille diverses méthodes d'investigation, telles que l'analyse des **sauvegardes iTunes**, l'examen des bases de données **SQLite** pour les messages et l'utilisation de captures d'écran système. Enfin, les risques liés au **jailbreak** et les particularités de l'architecture logicielle de chaque plateforme sont analysés pour guider les experts en informatique judiciaire.

Quels sont les plus grands défis de l'analyse forensique mobile ?

L'analyse forensique mobile moderne fait face à plusieurs défis de taille qui compliquent grandement le travail des enquêteurs :

- **Le chiffrement avancé et la sécurité intégrée** : Les fabricants d'appareils mobiles conçoivent désormais la sécurité comme l'un de leurs arguments de vente principaux. Les appareils modernes intègrent des techniques de chiffrement logicielles et matérielles hautement sophistiquées qui empêchent le contournement des verrouillages activés par les utilisateurs. Par exemple, iOS (à partir de la version 10.3) et Android (à partir de la version 6) activent le chiffrement par défaut, ce qui rend l'analyse forensique extrêmement difficile, voire impossible, sans de lourds investissements dans des laboratoires et des technologies de pointe. De plus, certains constructeurs comme Samsung ajoutent des couches de protection supplémentaires.

- **L'obsolescence rapide des méthodes d'investigation :** La criminalistique mobile est un domaine en constante évolution. Dès qu'une faille de sécurité ou une technique d'investigation est découverte, les fabricants déploient rapidement des correctifs et des mises à jour logicielles ou matérielles pour la neutraliser. Une technique d'extraction qui fonctionnait une semaine peut ainsi devenir totalement obsolète la semaine suivante.
- **La volatilité des données et la préservation de leur intégrité :** Empêcher l'état d'un appareil mobile de changer est parfois impossible. Les processus en arrière-plan, les mises à jour logicielles et les connexions à Internet modifient continuellement les données, et ce, même si l'appareil est complètement éteint. Comme les fabricants abandonnent de plus en plus les batteries amovibles, il est devenu difficile d'éteindre complètement un appareil pour empêcher ces altérations automatiques. Ces modifications imprévues nuisent à la reproductibilité de la collecte des preuves, ouvrant la porte à des contestations juridiques devant les tribunaux quant à l'intégrité des données originales.
- **La synchronisation multi-appareils et le stockage cloud :** La généralisation de la synchronisation cloud et multi-appareils fait en sorte que la suppression d'une preuve par un utilisateur à un endroit peut affecter instantanément plusieurs plateformes. À l'inverse, un enquêteur qui examine un appareil connecté court le risque de corrompre par inadvertance des données sur d'autres terminaux synchronisés. De plus, la popularité des sauvegardes cloud (comme iCloud) rend obsolètes les anciennes méthodes d'investigation basées sur la synchronisation locale avec un ordinateur via iTunes.
- **La complexité des codes PIN et les mécanismes anti-force brute :** Les installations modernes d'iOS et d'Android incitent par défaut les utilisateurs à configurer des codes alphanumériques complexes, pratiquement impossibles à deviner. En outre, les systèmes d'exploitation bloquent les attaques par force brute sur l'écran de verrouillage en imposant des délais d'attente progressifs

ou en effaçant automatiquement toutes les données de l'appareil après un certain nombre de tentatives infructueuses.

- **Les limitations des outils commerciaux existants** : Même des outils de référence de l'industrie (tels que la plateforme Cellebrite UFED ou Elcomsoft Forensics Toolkit) éprouvent de grandes difficultés face aux dernières technologies mobiles et ne parviennent pas à contourner les fonctions de chiffrement avancées ou les codes d'accès alphanumériques complexes des systèmes d'exploitation récents.
- **Les risques associés aux méthodes intrusives (jailbreak/rootage)** : Tenter de contourner la sécurité d'un système par des méthodes comme le jailbreak comporte d'importants risques de corruption ou de détérioration des données de l'appareil ciblé. De plus, la recevabilité devant les tribunaux des preuves obtenues par ces procédés intrusifs demeure incertaine.
- **Le risque d'usurpation d'identité (spoofing)** : Les journaux d'appels et de SMS ne peuvent pas être considérés comme des preuves absolues de l'identité d'un correspondant en raison de l'existence de services de spoofing qui permettent de falsifier très facilement le numéro de l'expéditeur.

 Si vous le souhaitez, je peux vous détailler les techniques présentées dans vos sources pour analyser spécifiquement les sauvegardes iOS (comme l'examen d'instantanés) ou pour rooter et extraire l'image disque d'un appareil Android.

Comment rooter un appareil Android ?

Le rootage d'un appareil Android dépend du modèle spécifique et de la version de son système d'exploitation. Il n'existe aucune méthode universelle ou « solution miracle » pour rooter tous les appareils.

Vos sources décrivent principalement deux approches pour y parvenir :

1. **La recherche d'instructions spécifiques en ligne** : Pour la majorité des téléphones, vous devez effectuer une recherche sur Internet en

indiquant le modèle précis et la version du système d'exploitation afin d'obtenir un guide étape par étape. Certains appareils requièrent en effet des manipulations manuelles complexes en plusieurs étapes.

2. **L'utilisation d'applications de rootage en un clic (One-Click**

Root) : Certains téléphones disposent d'outils simplifiés qui automatisent le processus.

- a. **KingoRoot** : Il s'agit de la méthode privilégiée présentée dans le document. Cette application tierce et gratuite est compatible avec la très grande majorité des appareils Android, bien qu'il y ait des exceptions. Sa mise en œuvre est extrêmement simple : **il suffit d'installer l'application et de cliquer sur le bouton pour rooter l'appareil.**

Utilité du rootage dans le cadre de l'enquête : Une fois l'accès root obtenu et le stockage de masse USB (ou le protocole MTP) activé sur l'appareil, l'enquêteur est en mesure de **créer une image physique des disques de stockage interne et de la carte SD** (à l'aide d'outils d'analyse de disques comme FTK Imager). Si le système de fichiers n'est pas chiffré, cette image permet d'extraire et de visualiser des données précieuses telles que les photos (généralement dans le dossier Téléphone/DCIM) ou encore la base de données des SMS (mmssms.db).

 Une fois l'appareil rooté, l'étape suivante consiste à extraire les données : je peux vous détailler la procédure pour créer une image physique avec FTK Imager ou vous montrer comment exécuter une requête SQLite pour déchiffrer et lire l'historique des SMS récupérés.

Comment créer une image avec FTK Imager ?

Pour créer une image physique d'un appareil Android à l'aide de **FTK Imager**, l'appareil doit d'abord être rooté et son stockage de masse USB (ou protocole MTP) doit être activé.

Voici les étapes à suivre pour réaliser cette opération :

1. **Lancez FTK Imager.**
2. Cliquez sur « **Créer une image disque** ».
3. Sélectionnez « **Disque physique** » (si vous chargez l'image d'un disque dur physique Android).
4. Sélectionnez le **périphérique de stockage de masse USB**.
5. **Répétez cette opération** pour la carte SD ainsi que pour le disque de stockage interne de l'appareil Android.

Une fois l'image créée, vous pouvez utiliser FTK Imager pour visualiser et analyser son contenu. Si le système de fichiers de l'appareil n'est pas chiffré, vous pourrez facilement accéder à ses données :

- Les **photos** se trouvent généralement dans le dossier **Téléphone/DCIM**.
- La **base de données des SMS** se situe habituellement à l'emplacement suivant :
/data/data/com.android.providers.telephony/databases/mmssms.db.

💬 Souhaitez-vous que je vous explique comment formuler la requête SQLite détaillée dans vos sources pour lire et déchiffrer proprement l'historique de cette base de données de SMS ?

Explique-moi la requête SQLite pour les SMS

La requête SQL présentée dans vos sources sert à **extraire, formater et trier de manière lisible** les messages texte stockés dans la base de données SQLite des SMS d'un appareil Android.

Voici l'explication détaillée, élément par élément, de cette requête :

```
SELECT datetime (date/1000, 'unixepoch','localtime')  
,datetime(date_sent/1000, 'unixepoch','localtime') ,person,body  
FROM sms
```

WHERE thread_id = 310
ORDER BY date

1. La conversion et le formatage des dates (SELECT datetime(...))

Les dates brutes stockées dans la base de données Android sont à l'origine peu lisibles. Cette fonction SQLite permet de les convertir en un format de date et d'heure compréhensible :

- **date/1000 et date_sent/1000** : Les appareils Android enregistrent les horodatages en millisecondes. Diviser la valeur par 1000 permet d'obtenir des secondes, ce qui est indispensable pour l'étape suivante.
- **'unixepoch'** : Ce paramètre indique à l'éditeur SQLite de traiter le nombre obtenu comme un horodatage Unix (le nombre de secondes écoulées depuis le 1er janvier 1970).
- **'localtime'** : Cette option convertit l'heure UTC ainsi obtenue en **heure locale de l'appareil**. Vos sources soulignent que l'horodatage sur Android se limite à cette heure locale, à la différence d'iOS qui enregistre à la fois l'heure locale et l'heure de l'opérateur.

2. La sélection des informations textuelles (person, body)

- **person** : Cette colonne contient l'identifiant ou le numéro de l'expéditeur.
- **body** : Cette colonne contient le **corps du message**, c'est-à-dire le texte de l'SMS proprement dit.

3. La table ciblée (FROM sms)

La clause indique à SQLite d'extraire ces données depuis la table nommée **sms**. C'est l'une des tables clés que l'on retrouve généralement dans la base de données mmssms.db aux côtés des tables threads et _ID.

4. Le filtrage par discussion (WHERE thread_id = 310)

Cette condition permet de cibler uniquement les SMS qui appartiennent à **un fil de discussion spécifique** (ici, la conversation portant l'identifiant unique 310). Cela évite d'afficher l'intégralité des messages de l'appareil en même temps.

5. Le tri chronologique (ORDER BY date)

Cette instruction trie les résultats **dans l'ordre chronologique de leur date de réception**, permettant à l'enquêteur de lire la discussion dans son ordre d'écriture naturel.

 Je peux vous expliquer comment localiser et lire la base de données équivalente des SMS sur un appareil iOS (sms.db), ou vous montrer comment se déroule le contournement d'un code PIN par force brute à l'aide d'un clavier externe.

Où se trouve sms.db sur iOS ?

Sur un appareil iOS, le fichier **sms.db** se trouve dans le répertoire suivant : **/private/var/mobile/Library/SMS**.

Ce fichier est une base de données SQLite qui contient l'historique des **SMS**, des **iMessages** et leurs **horodatages**. Pour y accéder et l'analyser, vous devez d'abord extraire ce fichier à partir d'une sauvegarde de l'iPhone (générée via iTunes ou récupérée depuis un compte iCloud). Une fois extrait, vous pouvez l'ouvrir facilement à l'aide d'un navigateur ou d'un gestionnaire SQLite.

 Souhaitez-vous que je vous explique comment les enquêteurs contournent les codes PIN de verrouillage sur certains téléphones en simulant un clavier externe grâce à un outil comme le Rubber Ducky ?

Comment contourner un code PIN avec un Rubber Ducky ?

Le contournement d'un code PIN à l'aide d'un **Rubber Ducky** repose sur une faille de conception de certains téléphones mobiles : la plupart de ces appareils n'activent pas leurs mécanismes de sécurité habituels (comme l'effacement automatique des données après trop de tentatives infructueuses) lorsqu'un **clavier physique externe** est connecté à la place du clavier virtuel de l'écran de verrouillage.

Le processus se déroule de la manière suivante :

1. **La reconnaissance matérielle** : Le Rubber Ducky (développé par Hak5) est un périphérique USB d'injection de frappes clavier. La majorité des téléphones Android le détectent immédiatement comme un clavier standard ou un périphérique d'interface utilisateur (HID). Pour le brancher sur un appareil mobile, un **adaptateur USB vers micro USB** (ou USB-C) est généralement nécessaire.
2. **L'automatisation par script** : Comme il est impossible de tester manuellement des milliers de combinaisons à la main, un script simple est chargé sur la clé USB du Rubber Ducky pour automatiser et faire défiler les codes d'accès. Le Rubber Ducky peut injecter ces frappes préprogrammées à une vitesse extrêmement rapide de plus de **1 000 mots par minute**.
3. **Le contournement des restrictions de sécurité** : Lors des tests présentés dans le document, un téléphone Android récent a tout de même imposé un délai d'attente de 30 secondes après cinq tentatives infructueuses. Cependant, comme la fonction d'effacement automatique des données de l'appareil reste inactive lors de l'utilisation d'un clavier externe, l'attaque par force brute peut continuer sans risque de détruire les preuves.
4. **Temps requis pour le déverrouillage** :
 - a. Pour un **code PIN à 4 chiffres** (avec 5 tentatives autorisées suivies d'une pause de 30 secondes), le Rubber Ducky parviendra à trouver le bon code en **16,6 heures** au maximum.
 - b. Pour un **code PIN à 5 chiffres**, la recherche par force brute prendra environ **166 heures**.

🔧 Souhaitez-vous que nous examinions comment les solutions commerciales de criminalistique (telles que le boîtier UFED de Cellebrite) effectuent des attaques par force brute pour déverrouiller des téléphones ?

Comment le boîtier UFED déverrouille-t-il les téléphones ?

Le boîtier **Cellebrite UFED** dispose principalement de deux méthodes pour tenter de déverrouiller un appareil mobile :

1. **L'exploitation de vulnérabilités connues** : Si l'appareil cible présente une faille de sécurité ou s'il existe une méthode de contournement documentée (ce qui est généralement le cas sur les appareils plus anciens), le boîtier UFED est capable d'exploiter cette vulnérabilité pour déverrouiller directement l'accès.
2. **L'attaque par force brute manuelle** : Le dispositif peut être relié au téléphone par des câbles de données spécifiques et utiliser une caméra physique pour tenter de deviner le code de verrouillage par force brute.

Conditions requises pour l'attaque par force brute : Pour que cette tentative de force brute manuelle réussisse, deux critères techniques essentiels doivent être réunis :

- L'appareil mobile **ne doit pas être configuré pour s'effacer automatiquement** après un certain nombre de tentatives de saisie infructueuses.
- Le verrouillage doit être basé sur un simple **code PIN numérique**.

Limites de l'outil : Bien que l'UFED soit une référence dans le domaine de la criminalistique mobile, il se heurte à des obstacles majeurs face aux technologies récentes :

- Il **ne peut pas contourner les fonctions de chiffrement avancées** d'Android et d'iOS.
- L'utilisation généralisée de mots de passe alphanumériques complexes sur les smartphones modernes rend les tactiques de force brute obsolètes.
- Son efficacité optimale est donc principalement restreinte aux appareils anciens (comme ceux fonctionnant sous **iOS 9.2** ou **Android 5 et 6**).

 Vos sources mentionnent également un autre outil commercial appelé Elcomsoft Forensics Toolkit — je peux vous détailler ses propres fonctionnalités et limites afin de comparer les deux solutions.

Qu'est-ce qu'Elcomsoft Forensics Toolkit ?

Elcomsoft Forensics Toolkit est un outil commercial d'analyse forensique mobile.

Voici ses principales caractéristiques selon vos sources :

- **Coût** : Son prix catalogue était d'environ **3 000 \$ US** au moment de la rédaction du document.
- **Fonctionnalités et compatibilité** : Il permet de récupérer et d'analyser diverses données et s'avère parfaitement compatible avec des systèmes tels qu'**iOS 9.2 et Android 5**.
- **Limites techniques** : L'outil présente une efficacité réduite sur les appareils protégés par des **codes d'accès alphanumériques complexes** ou fonctionnant sous des **systèmes d'exploitation plus récents**.
- **Réputation** : Elcomsoft possède une longue et brillante expérience dans le domaine de l'investigation numérique, au même titre que Cellebrite. Le document recommande l'utilisation d'un de ces deux outils pour s'équiper d'une suite logicielle d'entreprise robuste, sous réserve de disposer du budget nécessaire.

 Souhaitez-vous que je réalise un tableau comparatif entre Cellebrite UFED et Elcomsoft Forensics Toolkit pour mettre en évidence leurs forces et leurs limites respectives ?

Quels sont les outils forensiques iOS ?

Les sources répertorient plusieurs types d'outils utilisés pour effectuer des analyses forensiques sur les appareils iOS, allant des logiciels gratuits d'extraction de sauvegardes locales aux suites commerciales avancées :

Outils d'extraction et de lecture de sauvegardes

Puisque les méthodes d'accès direct au système de fichiers sont très complexes sur les versions récentes d'iOS, l'examen des sauvegardes générées via iTunes ou stockées dans le cloud est souvent privilégié.

- **iPhone Backup Extractor** : Recommandé dans les sources pour sa gratuité et son efficacité. Cet outil fonctionne uniquement sur **macOS** et permet d'extraire les données d'une sauvegarde locale ou d'un compte iCloud (si l'identifiant et le mot de passe associés sont connus).

- **AnyTrans** : Autre utilitaire cité comme permettant d'extraire des données iOS à partir de sauvegardes.
- **iPhone Backup Browser** : Un logiciel gratuit fonctionnant sous **Windows** (idéalement Windows 7 et nécessitant .NET Framework 4 et Visual C++ 2010). Il requiert que la sauvegarde de l'appareil se trouve à son emplacement par défaut sur le PC pour fonctionner.

Outils d'analyse de bases de données

- **SQLite Manager (extension Firefox)** : Utilisé pour ouvrir et lire facilement les fichiers de base de données bruts extraits de l'appareil, comme le fichier de messagerie sms.db. Les sources indiquent qu'il existe également des centaines d'autres méthodes ou visionneuses SQLite équivalentes.

Outils de jailbreak (pour les anciens modèles d'iPhone)

Le jailbreak permet d'obtenir un accès root pour analyser en profondeur le système de fichiers (notamment pour récupérer les instantanés d'applications en arrière-plan). Cependant, cette méthode comporte de lourds risques d'endommagement de l'appareil et son acceptabilité devant les tribunaux est incertaine.

- **RedSn0w** : Développé par l'iPhone Dev Team, cet outil populaire est recommandé pour jailbreaker d'anciens modèles d'iPhone (antérieurs à l'iPhone 5) ou pour forcer des codes PIN à 4 chiffres.
- **Pangu 9** : Un utilitaire publié par l'équipe Pangu permettant de jailbreaker un iPhone 6s sous iOS 9.0 à 9.0.2. Son usage nécessite toutefois un accès physique au téléphone et la connaissance préalable de son code de déverrouillage.

Suites commerciales d'entreprise

Ces suites logicielles professionnelles haut de gamme sont utilisées par les forces de l'ordre, l'armée et les grandes entreprises.

- **Cellebrite UFED** : Considéré comme une référence dans le domaine de l'investigation mobile. L'UFED utilise des câbles de données spécifiques connectés au téléphone et une application compagnon sur Windows pour extraire des photos, SMS (non-chiffrés), historiques d'appels et applications. Il permet également de

contourner la sécurité d'anciens appareils (comme ceux sous iOS 9.2) par force brute.

- **Elcomsoft Forensics Toolkit** : Un outil commercial d'environ 3 000 \$ US, pleinement compatible avec iOS 9.2 pour la récupération de données. Il présente toutefois des limites d'efficacité face aux versions d'iOS plus récentes et aux codes d'accès alphanumériques complexes.

 Je peux vous expliquer comment analyser les instantanés d'écran (snapshots) récupérés par ces outils pour tenter de retrouver des mots de passe saisis par l'utilisateur.

Qu'est-ce que Zerodium ?

Zerodium est une entreprise opérant sur le marché privé de la cybersécurité qui offre d'importantes primes financières pour la découverte de vulnérabilités et de méthodes de contournement de sécurité.

Le document mentionne notamment qu'elle propose une récompense de **500 000 \$** pour l'obtention d'un jailbreak iOS fonctionnel sur des appareils et des systèmes d'exploitation modernes. L'existence de telles primes sur le marché privé illustre la complexité croissante de la sécurité mobile moderne, faisant de la recherche de failles un domaine extrêmement difficile mais aussi particulièrement lucratif.

 Si vous le souhaitez, nous pouvons explorer comment les enquêteurs contournent ces difficultés d'accès direct en analysant plutôt les sauvegardes iTunes pour récupérer les données d'un iPhone sans avoir à le jailbreaker.

Comment utiliser iPhone Backup Browser ?

iPhone Backup Browser est un utilitaire gratuit conçu pour examiner le système de fichiers des appareils iOS à partir de leurs sauvegardes.

Voici les instructions et contraintes de fonctionnement détaillées dans vos sources :

- **Configuration requise** : Ce logiciel est compatible avec les systèmes **Windows**. Pour obtenir des performances optimales, il est recommandé de l'exécuter sur un poste de travail **Windows 7**.
- **Prérequis d'installation** : Pour que l'installation se déroule correctement, vous devez vous assurer que **Microsoft .NET Framework 4** et **Visual C++ 2010** sont bien installés sur votre ordinateur. Le logiciel peut être téléchargé à l'adresse suivante : <http://code.google.com/p/iphonebackupbrowser/>.
- **Contrainte d'utilisation majeure** : iPhone Backup Browser **exige impérativement que la sauvegarde iOS se trouve à son emplacement par défaut** sur votre ordinateur. Si la sauvegarde est stockée dans un autre dossier, le logiciel risque de ne pas fonctionner.

 Souhaitez-vous savoir comment configurer iTunes pour désactiver la synchronisation automatique avant de manipuler ces sauvegardes, afin d'éviter d'écraser accidentellement vos données ?

Quels types de données AnyTrans extrait-il ?

AnyTrans est présenté dans le document comme un outil permettant d'**extraire des données iOS** et de lire les sauvegardes d'iPhone.

Bien que le texte ne fournisse pas une liste exclusive des fonctionnalités propres à AnyTrans, il précise que les informations stockées dans les sauvegardes de téléphones iOS (et donc récupérables par ce type d'utilitaires d'extraction) comprennent :

- Les **photos et vidéos**.
- Les **contacts**.
- Les **e-mails**.
- Les **journaux d'appels**.
- Les **comptes utilisateurs et mots de passe**.
- Les **applications** et les **paramètres de l'appareil**.

- **D'autres données d'applications**, telles que l'historique des SMS et iMessages qui est stocké dans le fichier de base de données sms.db.

💬 Souhaitez-vous que je vous explique comment les enquêteurs analysent les instantanés d'écran (snapshots) également récupérés depuis ces sauvegardes pour retrouver des mots de passe saisis par l'utilisateur ?

Peut-on réinitialiser un compte iCloud par décision de justice ?

Oui, il est tout à fait possible de faire réinitialiser un compte iCloud par Apple en vertu d'une décision de justice.

Normalement, pour examiner et analyser les sauvegardes d'un iPhone stockées sur un compte iCloud (à l'aide d'outils d'extraction comme *iPhone Backup Extractor*), un enquêteur doit connaître l'identifiant et le mot de passe associés. Cependant, si ces informations d'identification sont indisponibles, **Apple peut réinitialiser le compte sur présentation d'une décision de justice valide**. Cela permet aux enquêteurs d'accéder aux précieuses preuves et données sauvegardées dans le cloud, qui sont parfois rendues accessibles grâce à des mandats judiciaires.

i Souhaitez-vous en savoir plus sur la manière dont les données sont récupérées depuis ces sauvegardes iCloud une fois l'accès obtenu, ou sur les types de données spécifiques que l'on peut y trouver ?

Quels sont les risques de corruption de données avec le jailbreak ?

Le jailbreak d'un appareil iOS présente des risques importants de corruption des données, de détérioration du matériel et de compromission globale de la sécurité :

- **Risque direct de corruption lors de l'attaque** : La grande majorité des outils de jailbreak exploitent des failles dans la séquence de démarrage ou dans la conception logicielle du système d'exploitation. Le lancement de ce type d'attaque comporte toujours un **risque inhérent de corruption des données** sur l'appareil ciblé.
- **Dégâts matériels et logiciels (bricking)** : Le jailbreak est une procédure qualifiée d'extrêmement risquée qui **peut endommager de façon permanente l'appareil** en cours d'analyse.
- **Exposition aux logiciels malveillants** : Les utilitaires de jailbreak les plus populaires utilisent généralement un identifiant root et un mot de passe par défaut. Si ces identifiants ne sont pas modifiés, des **programmes malveillants qui scannent les réseaux** à la recherche d'appareils iOS jailbreakés peuvent s'y connecter et y accéder automatiquement.
- **Perte des protections de sécurité d'origine** : Un appareil jailbreaké s'expose à la **non-réception des derniers correctifs de sécurité d'Apple**, ainsi qu'à la divulgation des données de compte de l'utilisateur.
- **Invalidation des preuves devant la justice** : En raison des altérations potentielles et des risques de modification non contrôlée des données originales, **la recevabilité devant un tribunal des preuves obtenues par jailbreak reste très incertaine**.

 Je peux vous expliquer comment analyser les captures d'écran (snapshots) générées automatiquement par iOS en arrière-plan, une méthode qui permet de récupérer des données sensibles sans avoir à jailbreaker l'appareil.

Comment désactiver la synchronisation iTunes ?

Pour désactiver la synchronisation automatique dans iTunes et ainsi éviter l'écrasement accidentel de données durant votre analyse, suivez cette procédure :

1. Ouvrez iTunes et accédez aux **Préférences**.

2. Cliquez sur l'onglet **Appareils**.
3. Cochez l'option permettant d'empêcher la synchronisation automatique (comme l'option « **Empêcher la synchronisation automatique des iPod, iPhone et iPad** » illustrée dans vos sources).

Cette manipulation est essentielle en criminalistique mobile, car elle garantit que la connexion de l'iPhone à l'ordinateur hôte ne modifiera pas l'état des données d'origine.

 Maintenant que la synchronisation automatique est coupée, je peux vous expliquer comment utiliser un outil gratuit comme **iPhone Backup Extractor** pour analyser le contenu de cette sauvegarde.

Qu'est-ce qu'iPhone Backup Extractor ?

iPhone Backup Extractor est un outil logiciel conçu pour extraire les données et lire les sauvegardes des appareils iOS, particulièrement recommandé dans vos sources pour sa gratuité et son efficacité.

Voici ses caractéristiques principales et ses fonctionnalités détaillées :

- **Compatibilité exclusive** : Cet utilitaire est **exclusivement compatible avec macOS**.
- **Versions disponibles et tarifs** : Il existe une version gratuite téléchargeable en ligne (sur <http://supercrazyawesome.com>) ainsi qu'une version commerciale avec assistance technique (sur www.iphonebackupextractor.com). La version commerciale peut être installée sans licence payante, mais ses fonctionnalités sont alors limitées. Pour débloquer l'intégralité des fonctionnalités de l'outil, le coût est d'environ **70 \$ US**.
- **Analyse des sauvegardes iCloud** : Au-delà des sauvegardes locales, le logiciel permet d'accéder, d'examiner et d'analyser les sauvegardes d'iPhone stockées sur des **comptes iCloud**, à condition de posséder l'identifiant et le mot de passe associés.
- **Extraction d'éléments spécifiques** : Il est couramment utilisé par les enquêteurs pour naviguer dans l'archive de sauvegarde afin d'en

extraire des fichiers spécifiques, tels que les **instantanés d'écran (snapshots)** au format PNG que le système d'exploitation iOS génère automatiquement lorsque les applications passent en arrière-plan.

 Je peux vous expliquer comment analyser en détail ces instantanés d'écran (snapshots) récupérés grâce à cet outil afin de retrouver des mots de passe ou des notes sensibles saisis par l'utilisateur.

Comment analyser un instantané pour trouver un mot de passe ?

L'analyse des instantanés (ou *snapshots*) est une technique très efficace pour récupérer des informations sensibles, car **iOS prend automatiquement une capture d'écran de l'application active** au moment précis où elle bascule en arrière-plan.

Voici comment procéder pas à pas pour analyser ces fichiers et tenter d'y découvrir un mot de passe :

1. Extraction des fichiers d'instantanés

- **Localisation dans le système de fichiers** : Sur l'appareil, ces captures d'écran sont conservées dans le répertoire :
`/private/var/mobile/Library/Caches/Snapshots`.
- **Récupération** : Vous devez extraire ce dossier à partir d'une sauvegarde iTunes ou iCloud de l'iPhone en utilisant un logiciel d'extraction approprié, comme **iPhone Backup Extractor**.
- **Format de fichier** : Les instantanés ainsi récupérés se trouvent sous la forme de fichiers **PNG** standards.

2. Analyse visuelle des captures d'écran

- **Lecture des fichiers** : Puisqu'il s'agit d'images ordinaires, il vous suffit d'ouvrir chaque fichier PNG avec le visionneur d'images par défaut de votre ordinateur.
- **Passage en revue** : Des captures d'écran sont enregistrées pour chaque application qui a été active. L'enquêteur doit donc examiner visuellement les instantanés de toutes les applications d'intérêt (qu'elles soient natives ou tierces).

3. Recherche des indices et des mots de passe en clair

L'examen visuel vous permet d'observer le dernier état de l'application avant sa mise en arrière-plan. C'est là que vous pouvez découvrir des informations critiques :

- **Saisie de mot de passe à l'écran** : L'utilisateur peut avoir écrit son mot de passe dans un champ de texte (par exemple dans le corps d'un e-mail ou dans l'application *Notes*) sans l'avoir encore envoyé ou enregistré, l'utilisant simplement comme une note temporaire. La figure 9-5 montre un exemple concret où l'écran de l'application *Mail* affiche le texte saisi : « *My twitter password is MobyDick* ».
- **Copier-coller de mots de passe complexes** : Les utilisateurs ont fréquemment recours au copier-coller de mots de passe complexes depuis un courriel, un document ou une note afin d'éviter d'avoir à les retaper. L'instantané de l'application source peut ainsi immortaliser le mot de passe affiché en clair à l'écran au moment de la copie.

Limites techniques

Bien que cette méthode d'analyse visuelle fonctionne extrêmement bien sur un appareil jailbreaké ou lorsque le système de fichiers est accessible, elle s'avère **très difficile à mettre en œuvre sur les systèmes iOS récents**. Cela s'explique par l'absence de techniques de jailbreak publiques pour accéder directement au système de fichiers et par l'activation du chiffrement du disque par défaut, qui protège ces instantanés.

 Je peux vous préparer un rapport d'étude complet ou un aide-mémoire structuré résumant l'ensemble de ces méthodes d'investigation mobile (iOS et Android) si vous souhaitez disposer d'un document de synthèse.

Où sont stockées les photos sur Android ?

Sur un appareil Android, l'emplacement de stockage par défaut pour les photos se trouve généralement dans le dossier **Téléphone/DCIM**.

Pour que l'enquêteur puisse y accéder et visualiser ces fichiers, l'appareil ne doit pas être chiffré (ou doit avoir été déchiffré), et une image physique de son stockage doit être créée après avoir obtenu un accès root.

📁 Voulez-vous que nous examinions comment procéder à l'extraction de ce dossier spécifique à l'aide d'une image physique générée sous FTK Imager ?

Comment extraire DCIM avec FTK Imager ?

Pour extraire le dossier **DCIM** contenant les photos d'un appareil Android à l'aide de **FTK Imager**, vous devez suivre un processus en trois grandes étapes : la préparation du téléphone, la création de l'image physique, puis l'exploration de cette image pour récupérer les fichiers.

1. La préparation de l'appareil Android

Avant de pouvoir faire une copie conforme des données avec FTK Imager, l'appareil doit être préparé pour permettre un accès brut à son système de fichiers :

- **Connexion USB** : Connectez le téléphone Android à votre ordinateur à l'aide d'un câble USB.
- **Activation des protocoles** : Activez le **stockage de masse USB** ou le protocole **MTP (périphérique multimédia)** dans les paramètres de l'appareil afin de garantir l'accès à l'ensemble du système de fichiers.
- **Obtention de l'accès Root** : Le téléphone doit impérativement être rooté pour que vous puissiez accéder aux partitions physiques. Vous pouvez utiliser une application de rootage en un clic comme *KingoRoot* pour y parvenir facilement.

2. La création de l'image physique avec FTK Imager

Une fois l'appareil rooté et le stockage de masse activé, procédez à la copie physique :

- **Étape 1** : Lancez **FTK Imager**.
- **Étape 2** : Cliquez sur « **Créer une image disque** ».
- **Étape 3** : Sélectionnez « **Disque physique** ».

- **Étape 4** : Choisissez le **périphérique de stockage de masse USB** correspondant à votre téléphone Android connecté.
- **Étape 5** : Répétez ces étapes pour extraire séparément la **carte SD** et le **disque de stockage interne** de l'appareil.

3. La localisation et l'extraction du dossier DCIM

Une fois la copie physique générée :

- **Chargement de l'image** : Utilisez FTK Imager pour charger et **visualiser le contenu** de l'image disque que vous venez de créer.
- **Navigation** : Si le système de fichiers de l'appareil n'est pas chiffré (ce qui est le cas de nombreux modèles antérieurs à Android 6), vous pourrez naviguer librement dans l'arborescence des dossiers.
- **Localisation du dossier** : Recherchez le répertoire des photos qui se situe par défaut à l'emplacement **Téléphone/DCIM**.
- **Extraction** : Depuis l'interface de FTK Imager, vous pouvez alors sélectionner ce dossier **DCIM** et l'exporter (l'extraire) directement vers votre ordinateur d'analyse pour récupérer toutes les photos et vidéos dans leur état d'origine.

💬 Souhaitez-vous que nous voyions comment récupérer les messages supprimés dans la base de données SMS (mmssms.db) également accessible via cette image, ou comment surmonter le défi du chiffrement par défaut sur Android 6 et supérieur ?

Comment gérer le chiffrement d'Android 6 ?

À partir d'Android 6, le système de fichiers est **chiffré par défaut**, ce qui signifie qu'un déchiffrement préalable est indispensable pour pouvoir lire les données de l'appareil.

Pour gérer cette barrière de sécurité, les enquêteurs s'appuient sur les méthodes et font face aux limites suivantes :

- **L'émulation et l'attaque par force brute** : Puisqu'il n'existe pas de méthode universelle de déchiffrement, la technique la plus courante consiste à **connecter le disque chiffré à un émulateur Android** et

à tenter une attaque par force brute pour deviner le code d'accès ou l'écran de verrouillage.

- **L'usage de suites commerciales** : L'analyse d'appareils sous Android 6 reste globalement plus simple avec des outils comme **Cellebrite UFED** qu'avec des versions plus récentes du système d'exploitation. Toutefois, si l'utilisateur a correctement activé les fonctions de sécurité, ces outils commerciaux ne parviennent pas à contourner les mécanismes de chiffrement avancés.
- **Les protections supplémentaires des constructeurs** : La difficulté varie selon la marque du téléphone. Des fabricants comme **Samsung** intègrent des dispositifs de sécurité matériels et logiciels exclusifs qui rendent le contournement du chiffrement et la protection de l'appareil encore plus difficiles à surmonter.

 Voulez-vous que nous examinions plus en détail comment l'architecture de sécurité d'un appareil Android (ses différentes couches logicielles) se compare à celle d'un iPhone ?

C'est quoi Samsung Knox ?

Vos sources ne mentionnent pas explicitement **Samsung Knox**.

Cependant, elles indiquent de manière générale que certains fabricants, comme **Samsung**, intègrent des techniques de sécurité supplémentaires à leurs appareils afin de rendre le contournement des mesures de sécurité, du chiffrement et de la protection globale encore plus difficile pour les enquêteurs.

Souhaitez-vous que j'effectue des recherches sur le Web pour vous expliquer en détail ce qu'est Samsung Knox et comment cette technologie fonctionne ?

Rechercher Samsung Knox

Voici ce que j'ai trouvé sur **Samsung Knox** :

J'ai découvert que **Samsung Knox** est une plateforme de sécurité multicouche de niveau militaire, intégrée de façon indissociable au matériel et au logiciel des appareils Samsung Galaxy. Son utilisation d'un fusible matériel physique (**e-fuse**) présente un défi redoutable pour la criminalistique mobile, car toute tentative de rootage ou d'altération du système grille ce fusible de manière irréversible, ce qui révoque instantanément les clés cryptographiques et verrouille à tout jamais l'accès aux données des espaces sécurisés.

Principaux thèmes identifiés :

1. **Une sécurité ancrée dans le matériel (Hardware Root of Trust) :**
Knox s'appuie sur une puce physique entièrement indépendante appelée **Knox Vault** pour protéger de manière étanche les clés de chiffrement, les données biométriques et les codes PIN de l'utilisateur contre les attaques physiques et de canaux auxiliaires.
2. **Le fusible physique irréversible (e-Fuse) :** Lors de l'installation d'un micrologiciel personnalisé ou d'un rootage, une surtension permanente grille un fusible sur le processeur (faisant passer le bit de garantie à 0x1). Cette altération désactive définitivement les services Knox et détruit définitivement les clés d'accès aux conteneurs sécurisés.
3. **Un défi de taille pour l'analyse forensique :** Ce chiffrement renforcé empêche les outils d'extraction d'accéder directement aux partitions mémoires brutes ou de mener des attaques par force brute, obligeant les enquêteurs à se replier sur de l'extraction logique ou des sauvegardes cloud.

Comment contourner Knox avec une extraction logique ?

En criminalistique mobile, l'extraction logique ne cherche pas à briser ou à contourner cryptographiquement le chiffrement matériel robuste ou les conteneurs de sécurité (tels que ceux de Samsung). Elle consiste plutôt à **collaborer avec le système d'exploitation** de l'appareil pour récupérer

les données applicatives et système au moment où elles sont déjà déchiffrées et présentées par l'appareil lui-même.

Voici comment cette approche permet d'accéder aux données et de contourner indirectement les barrières matérielles :

1. L'exploitation d'un appareil actif ou déverrouillé

L'extraction logique repose principalement sur le fait que l'appareil est allumé et déverrouillé, ou que son code d'accès a pu être saisi ou temporairement contourné.

- **Accès par protocoles standards** : Lorsque l'appareil est accessible, l'enquêteur le connecte via USB et active des protocoles d'origine comme le **stockage de masse USB** ou le **protocole MTP (périphérique multimédia)**.
- **Extraction des fichiers déchiffrés** : Le système de fichiers étant déverrouillé par l'utilisateur, l'arborescence logique devient accessible. L'enquêteur peut alors copier directement les données d'intérêt, telles que le répertoire des photos (DCIM) ou les bases de données d'applications non chiffrées à la volée, sans risquer de déclencher les mécanismes de sécurité matériels liés à une tentative de rootage.

2. L'analyse des sauvegardes hors ligne (Ordinateurs hôtes et Cloud)

Si l'accès direct au téléphone est rendu impossible par un verrouillage actif protégé par un conteneur sécurisé, l'enquêteur utilise l'extraction logique en ciblant les **sauvegardes externes**.

- **Bypass de l'écran de verrouillage** : Si le téléphone a été préalablement synchronisé avec un ordinateur de confiance (ordinateur hôte), le processus de synchronisation automatique permet souvent d'extraire les données en contournant complètement le code PIN de verrouillage, même si celui-ci est complexe.
- **Extraction du Cloud ou d'iTunes** : L'enquêteur récupère la sauvegarde logique stockée sur l'ordinateur ou dans le cloud (iCloud/Samsung Cloud). Ces sauvegardes contiennent la quasi-totalité des bases de données applicatives (messages, contacts, journaux d'appels, photos) sous forme déchiffrée. Cette méthode

permet d'obtenir l'intégralité des preuves sans jamais avoir à interagir avec les puces de sécurité physiques du téléphone cible.

3. La préservation de l'intégrité et la conformité légale

L'utilisation de méthodes logiques (qui exploitent des API et des fonctionnalités officielles approuvées par le fabricant) évite d'altérer le système d'exploitation. Contrairement au jailbreak ou au rootage d'un appareil sécurisé — qui peuvent corrompre les données, bloquer définitivement l'accès aux partitions ou détruire les clés cryptographiques —, l'extraction logique garantit que les données d'origine restent intactes. Cela réduit considérablement le risque que les preuves soient contestées ou jugées irrecevables devant un tribunal.



Souhaitez-vous que je rédige un rapport de synthèse détaillé comparant les avantages, les limites et la recevabilité juridique de l'extraction physique par rapport à l'extraction logique pour vos dossiers d'investigation ?

Comment fonctionne l'extraction via MTP sur Android ?

Sur Android, l'extraction de données via le protocole **MTP (Media Transfer Protocol)** s'effectue selon une procédure structurée pour permettre l'accès aux données :

- **La connexion physique** : L'appareil Android doit d'abord être connecté à l'ordinateur d'analyse à l'aide d'un câble USB.
- **La configuration sur l'appareil** : L'enquêteur doit se rendre dans les paramètres du téléphone pour activer l'option de **stockage de masse USB** et sélectionner le mode **périphérique multimédia (MTP)**.
- **L'accès aux fichiers** : L'activation de ce paramètre MTP est essentielle car elle **garantit l'accès à tous les systèmes de fichiers** de l'appareil.
- **L'extraction et l'analyse** : Une fois le protocole MTP activé, l'examen du système Android se déroule de façon quasiment

identique à celui d'un ordinateur de bureau. Si l'appareil n'est pas chiffré (comme c'est le cas pour de nombreux modèles fonctionnant sous des versions antérieures à Android 6), l'enquêteur peut naviguer et copier directement les fichiers non chiffrés, tels que les applications, les photos stockées dans le dossier DCIM, ou les bases de données de l'appareil.

Cependant, pour réaliser une copie conforme et complète (une image physique) de la mémoire interne du téléphone à l'aide d'outils comme FTK Imager, l'activation du MTP doit être complétée par l'obtention d'un **accès root complet** sur l'appareil.

 Souhaitez-vous que je vous explique comment obtenir cet accès root (par exemple avec l'utilitaire KingoRoot) pour pouvoir extraire une image physique complète après avoir activé le MTP ?

Comment récupérer les SMS supprimés (mmssms.db) ?

La récupération et l'analyse des SMS (y compris ceux qui ont été supprimés) à partir de la base de données Android **mmssms.db** s'effectuent en plusieurs étapes techniques :

1. Localiser et extraire le fichier mmssms.db

Par défaut, la base de données contenant l'historique des SMS sur un système Android est située dans le répertoire suivant :

`/data/data/com.android.providers.telephony/databases/mmssms.db`

Note : Chaque installation d'Android étant légèrement différente selon le constructeur, vous devrez peut-être adapter ce chemin d'accès en fonction du modèle d'appareil examiné.

Pour extraire ce fichier sur un smartphone Android moderne, l'enquêteur doit d'abord obtenir un **accès root complet** (par exemple avec un outil comme *KingoRoot*), puis générer une image physique de la mémoire de stockage interne (à l'aide d'un logiciel comme **FTK Imager**) afin de copier le fichier de base de données en toute sécurité.

2. Explorer la structure avec un gestionnaire SQLite

Ouvrir directement la base de données avec un éditeur de texte brut brut risque de générer une quantité importante de caractères illisibles et de données parasites. Il est donc nécessaire d'utiliser un **gestionnaire de bases de données SQLite**.

Une fois la base de données ouverte, l'enquêteur doit identifier et cibler les trois tables principales qui structurent les conversations :

- **sms** (contenant le corps des messages et les numéros)
- **threads** (regroupant les fils de discussion)
- **_id** (les identifiants uniques)

3. Exécuter une requête SQL pour lire les données

Pour trier, convertir les horodatages (qui sont stockés sous forme de timestamp Unix) et afficher les messages de manière lisible, vous devez exécuter une requête SQL. Le document fournit l'exemple de requête suivant pour interroger une discussion spécifique :

```
SELECT datetime (date/1000, 'unixepoch','localtime')  
,datetime(date_sent/1000, 'unixepoch','localtime') ,person,body  
FROM sms  
WHERE thread_id = 310  
ORDER BY date
```

Cette requête extrait la date de réception, la date d'envoi (toutes deux converties à l'heure locale de l'appareil), le contact associé et le corps du message.

4. Récupérer les messages supprimés

Selon la version du système d'exploitation et de la base de données Android de l'appareil, **les messages supprimés restent stockés et récupérables** dans la base de données. L'analyse de ces tables permet alors de faire réapparaître le contenu textuel des messages supprimés, ainsi que les numéros de l'expéditeur et du destinataire d'origine.

 Je peux vous écrire un script Python automatisé que vous pourrez exécuter pour extraire, décoder et exporter proprement l'intégralité des messages de vos fichiers sms.db (iOS) et mmssms.db (Android) vers un rapport au format CSV.

Quelles sont les métadonnées SMS sur iOS ?

Sur les appareils iOS, les SMS et les iMessages sont stockés dans la base de données SQLite nommée **sms.db**. Sur les versions récentes d'iOS, les métadonnées récoltées sont particulièrement riches et comprennent notamment :

- **Les horodatages détaillés (timestamps) :** Contrairement aux appareils Android (qui se limitent à l'heure locale du téléphone), iOS conserve et affiche à la fois **l'heure locale de l'appareil** et **l'heure de l'opérateur réseau**.
- **Le statut des messages :** La base de données fournit des informations précises permettant de savoir si les messages ont été **envoyés, reçus ou supprimés**.
- **Les coordonnées de l'expéditeur et du destinataire :** Elle enregistre les **numéros d'origine** et de destination associés aux échanges.
- **De nombreuses autres métadonnées complémentaires** qui rendent l'analyse d'autant plus complète sur les versions modernes d'iOS.

 Souhaitez-vous que nous examinions comment les enquêteurs procèdent pour extraire ce fichier spécifique sms.db depuis une sauvegarde iTunes ou iCloud ?

Peut-on récupérer des photos supprimées sur Android ?

Oui, il est possible de récupérer des photos précédemment supprimées sur un appareil Android, mais cela dépend de la version du système d'exploitation et des paramètres de sécurité de l'appareil. Voici comment les enquêteurs procèdent et les limites techniques qu'ils rencontrent :

1. L'extraction par des suites commerciales

Des outils professionnels comme **Cellebrite UFED** permettent d'extraire les photos, les SMS et l'historique des appels d'un téléphone connecté. Dans de nombreux cas, les processus automatisés de ces outils sont capables de récupérer des données et des fichiers qui ont été préalablement supprimés.

2. L'extraction physique (pour les appareils non chiffrés)

Sur les appareils fonctionnant avec des versions antérieures à Android 6, le système de fichiers n'est généralement pas chiffré. Cela permet aux enquêteurs de tenter une récupération brute des fichiers effacés en créant une image physique de la mémoire :

- **Rooter l'appareil** : L'enquêteur doit d'abord obtenir un accès root complet, par exemple avec l'utilitaire *KingoRoot*.
- **Activer les connexions** : Le stockage de masse USB et le protocole MTP doivent être activés dans les paramètres pour garantir l'accès complet aux fichiers.
- **Créer l'image disque** : Un logiciel forensique comme **FTK Imager** est utilisé pour copier bit-à-bit le contenu de la carte SD et du stockage interne.
- **Analyser et reconstruire** : L'enquêteur explore ensuite cette image pour localiser les fichiers (notamment dans le répertoire par défaut **Téléphone/DCIM**) et reconstituer les photos supprimées qui n'ont pas encore été écrasées par de nouvelles données.

3. Les limites sur les appareils récents

La récupération de photos supprimées se heurte à des obstacles majeurs sur les smartphones modernes :

- **Le chiffrement par défaut** : Depuis Android 6, le système de fichiers est chiffré par défaut, ce qui rend les données illisibles tant qu'elles n'ont pas été déchiffrées au préalable.
- **L'activation de la sécurité** : Si l'utilisateur a activé un verrouillage sécurisé, le contournement et l'accès direct aux partitions de stockage deviennent extrêmement difficiles.
- **La synchronisation multi-appareils et cloud** : Les photos d'un appareil Android sont souvent synchronisées avec le cloud. L'extrême volatilité de ces environnements fait que la suppression

d'une image à un emplacement peut affecter et propager la suppression sur l'ensemble des appareils connectés.

✖ Je peux vous expliquer comment utiliser un outil d'injection de frappes de touches comme le Rubber Ducky pour tenter de forcer le code PIN d'un écran de verrouillage Android afin d'accéder à ses données.

Comment fonctionne l'injection de frappes avec le Rubber Ducky ?

L'injection de frappes avec le **USB Rubber Ducky** (développé par Hak5) est une technique d'automatisation qui permet de simuler un clavier physique pour forcer le verrouillage d'un appareil.

Voici son fonctionnement technique détaillé :

1. La reconnaissance en tant que clavier (HID)

Le Rubber Ducky se présente sous la forme d'une clé USB ordinaire.

Lorsqu'il est branché sur un téléphone Android (ce qui nécessite généralement un **adaptateur USB vers micro USB**), le système d'exploitation le reconnaît immédiatement comme un **périphérique d'interface utilisateur (HID)** ou un clavier physique. De ce fait, le téléphone accepte les entrées du Rubber Ducky de manière native et sans poser de questions.

2. L'injection de frappes ultra-rapide

Une fois connecté, le Rubber Ducky exécute un script simple préalablement configuré par l'enquêteur. Il injecte des séquences de frappes clavier préprogrammées à une vitesse phénoménale, pouvant dépasser **1 000 mots par minute**. En plus de tester des codes d'accès, ces scripts peuvent être écrits pour exécuter des fichiers binaires ou lancer des *shells* inversés.

3. Le contournement des protections (L'astuce du clavier externe)

Saisir à répétition de faux codes d'accès sur l'écran tactile d'un téléphone verrouillé déclenche généralement des mécanismes de défense : le système impose des délais d'attente de plus en plus longs, ou peut même

effacer complètement les données de l'appareil après trop de tentatives infructueuses.

C'est ici que réside l'astuce : **les téléphones équipés d'un clavier virtuel n'activent généralement pas le verrouillage ou l'effacement des données lorsqu'un clavier externe est connecté.**

Lors de tests sur un téléphone Android doté d'un système d'origine, le comportement suivant a été observé :

- L'appareil a tout de même instauré un délai d'expiration de 30 secondes après chaque bloc de 5 tentatives.
- Cependant, **la fonction d'effacement du périphérique est restée indisponible** via le clavier externe (alors qu'elle était active via le clavier virtuel sur l'écran tactile). L'automatisation devient donc possible sans risque de détruire les preuves.

4. Temps de traitement pour la force brute

En exploitant cette faille pour faire défiler automatiquement les codes d'accès, l'enquêteur peut estimer le temps requis pour déverrouiller le téléphone :

- **Code PIN à 4 chiffres** : Avec les 5 tentatives autorisées suivies du verrouillage de 30 secondes, le Rubber Ducky trouvera le code en **16,6 heures** au maximum.
- **Code PIN à 5 chiffres** : En suivant le même schéma, le processus nécessite environ **166 heures**.

 Souhaitez-vous que je crée un guide de référence ou un aide-mémoire structuré regroupant l'ensemble de ces techniques d'investigation et d'acquisition (iOS et Android) issues de votre document ?

Quelles sont les couches d'Android ?

Le système d'exploitation Android est structuré en **quatre couches distinctes**, chacune d'elles prenant en charge des fonctions spécifiques du système :

- **Applications.**

- **Framework d'application.**
- **Bibliothèques** : cette couche inclut notamment les bibliothèques d'écriture Android des fonctions principales ainsi que la **machine virtuelle Dalvik**.
- **Noyau Linux.**

La majorité des applications Android sont programmées en Java et s'exécutent chacune dans leur propre instance de la machine virtuelle Dalvik. Cependant, pour améliorer la vitesse ou accéder directement aux composants matériels, certains développeurs écrivent leurs applications dans un langage binaire natif, ce qui leur permet de contourner cette machine virtuelle.

 **Souhaitez-vous comparer cette structure avec celle d'iOS et ses quatre couches applicatives (comme Cocoa Touch ou Core Services) présentées dans le document ?**

Détails sur Core Services

La **couche Services de base** (Core Services) est l'un des quatre composants majeurs de l'architecture des applications iOS.

Selon vos sources, ses caractéristiques se résument ainsi :

- Elle regroupe les **services système fondamentaux** nécessaires au bon fonctionnement des applications.
- Elle comprend notamment des frameworks clés tels que **Core Foundation** et **Foundation**.
- Ces frameworks ont pour rôle essentiel de **définir les types de base** qui sont utilisés par toutes les applications du système.

 Si vous le souhaitez, nous pouvons examiner en détail les étapes de la **séquence de démarrage sécurisé d'iOS** pour comprendre comment le système d'exploitation valide ces différentes couches logicielles à l'allumage de l'appareil.

Expliquer la séquence de démarrage

Lorsqu'un appareil iOS est allumé, il exécute systématiquement une **séquence de démarrage sécurisé** conçue pour vérifier l'intégrité de chaque composant logiciel avant de l'exécuter.

Voici les étapes de cette séquence :

1. **L'allumage** : L'utilisateur met l'appareil sous tension.
2. **La ROM de démarrage sécurisé (Secure Boot ROM)** : L'appareil lance cette zone mémoire hautement sécurisée et accessible uniquement en lecture seule. Elle contient le code de démarrage initial de base ainsi qu'un **certificat cryptographique d'Apple**. Comme cette zone est gravée dans le matériel, elle ne peut pas être modifiée. Si cette ROM de démarrage sécurisé ne parvient pas à se charger, l'iPhone refuse tout simplement de démarrer.
3. **Le chargeur de démarrage bas niveau (LLB - Low Level Bootloader)** : Une fois la ROM validée, le LLB prend le relais. Son rôle est de charger en mémoire le noyau iOS ainsi que le processus suivant, appelé **iBoot**.
4. **Le démarrage d'iBoot** : iBoot s'exécute à son tour. Cette étape cruciale consiste à **vérifier et charger tout le reste du noyau iOS**, puis à initialiser l'ensemble des applications de l'utilisateur.

Pourquoi cette séquence est-elle cruciale en criminalistique ?

Pour les enquêteurs et les chercheurs en sécurité, la compréhension de ce processus est fondamentale car **la grande majorité des outils de contournement de sécurité et de jailbreak exploitent des failles situées précisément au niveau de cette séquence de démarrage** ou de la conception logicielle d'iOS.

Lancer une attaque à ce stade comporte toutefois un risque persistant de **corruption ou de perte des données** de l'appareil analysé si le démarrage normal est perturbé.

 Si vous le souhaitez, nous pouvons comparer cette chaîne de confiance matérielle d'Apple avec les mécanismes de démarrage sécurisé d'Android (comme le Trusted Boot ou les fusibles matériels e-fuses).

Limites du LLB et d'iBoot

Dans l'architecture de sécurité d'iOS, le **LLB (Low Level Bootloader)** et **iBoot** sont deux maillons essentiels de la chaîne de démarrage sécurisé. Le LLB a pour rôle de charger le noyau iOS et le processus iBoot, tandis qu'iBoot vérifie et charge le reste du noyau ainsi que l'ensemble des applications utilisateur.

En criminalistique mobile, l'exploitation de ces deux composants présente des limites, des risques et des défis majeurs pour les enquêteurs :

1. Le risque inhérent de corruption de données

La majorité des outils de jailbreak et de contournement de sécurité s'appuient sur l'exploitation de failles logicielles situées précisément au niveau de la séquence de démarrage (et donc de composants comme le LLB ou iBoot). Lancer une telle attaque perturbe le processus de démarrage normal, ce qui entraîne **un risque permanent de corruption ou de perte des données** présentes sur l'appareil ciblé.

2. L'obsolescence rapide face aux correctifs d'Apple

Dès qu'un chercheur en sécurité ou un outil forensique découvre une vulnérabilité permettant de contourner les contrôles du LLB ou d'iBoot, Apple réagit très rapidement. Le fabricant déploie des mises à jour matérielles et logicielles pour corriger ces failles de sécurité, ce qui rend **les techniques d'exploitation obsolètes en très peu de temps** (parfois d'une semaine à l'autre).

3. L'inefficacité totale sur les appareils et systèmes iOS modernes

Les failles de démarrage historiques (exploitées par des outils comme *RedSn0w* ou *Pangu*) ne sont pas rétrocompatibles et **ne fonctionnent pas sur les versions récentes d'iOS ou sur les modèles récents d'iPhone**.

Sur les systèmes modernes, l'absence de failles de jailbreak publiques combinée au chiffrement matériel du disque par défaut rend l'accès au système de fichiers via le démarrage presque impossible sans investissements technologiques extrêmement lourds.

 Souhaitez-vous que nous examinions comment les forces de l'ordre s'y prennent pour contourner ces protections de démarrage en faisant appel à

des solutions d'extraction commerciale tierces comme Cellebrite ou Elcomsoft ?

Quels outils les forces de l'ordre utilisent-elles ?

Pour mener à bien leurs enquêtes sur les appareils mobiles, les forces de l'ordre et les organismes gouvernementaux s'appuient sur une gamme d'outils professionnels spécialisés, allant de suites d'extraction haut de gamme à des logiciels d'imagerie et de recherche.

1. Les suites commerciales d'analyse forensique (les références du domaine)

- **Cellebrite UFED (Universal Forensic Extraction Device)** : C'est la plateforme de référence en criminalistique mobile, approuvée et utilisée mondialement par les forces de l'ordre, les organisations militaires et les grandes entreprises. Grâce à un ensemble de câbles de données spécifiques reliant le téléphone à l'appareil UFED, elle permet d'extraire et d'analyser l'historique des appels, les SMS, les photos, les messages vocaux et les applications installées, en parvenant fréquemment à récupérer des données qui ont été préalablement supprimées. L'outil peut également exploiter des failles connues ou utiliser une caméra physique couplée à un câble pour mener des attaques par force brute sur les codes PIN numériques.
- **Elcomsoft iOS Forensic Toolkit (ou Elcomsoft Forensics Toolkit)** : Cette suite commerciale reconnue (coûtant environ 3 000 \$ US) permet aux enquêteurs de récupérer et d'analyser diverses données sur iOS et Android.
- **La restriction d'accès** : Les sources précisent que face à la sécurité extrêmement robuste des téléphones récents (à partir d'iOS 10.3), les investigations nécessitent des technologies de pointe très coûteuses et de nombreux outils forensiques avancés ne sont **accessibles qu'aux forces de l'ordre ou aux agences gouvernementales**.

2. Les outils d'imagerie physique et d'analyse de disques

- **FTK Imager** : Une fois qu'un enquêteur a obtenu un accès root sur un appareil Android (par exemple avec l'application *KingoRoot*), il utilise **FTK Imager** pour effectuer une copie bit-à-bit conforme (une image physique) de la carte SD et du stockage interne afin de naviguer dans le système de fichiers non chiffré et d'extraire les données sensibles, comme le répertoire de photos DCIM ou la base de données SMS mmssms.db.

3. Les extracteurs de sauvegardes locales et cloud

- **iPhone Backup Extractor et iPhone Backup Browser** : Ces logiciels permettent de lire et d'extraire les informations contenues dans les fichiers de sauvegarde d'un iPhone. Ils s'avèrent indispensables pour naviguer dans l'arborescence à la recherche d'éléments comme les bases de données SMS (sms.db) ou le dossier des instantanés d'écran (Snapshots) qui capturent en tâche de fond l'activité des applications. De plus, *iPhone Backup Extractor* permet d'analyser les sauvegardes cloud issues de comptes iCloud.

4. Les outils de contournement matériel (Force Brute)

- **USB Rubber Ducky (de Hak5)** : Ce périphérique USB, reconnu par les téléphones Android comme un clavier physique (périphérique HID), est utilisé pour injecter des séquences de frappes préprogrammées à très grande vitesse (plus de 1 000 mots par minute). Il permet de faire défiler automatiquement et par force brute les codes d'accès de l'écran de verrouillage sans risquer de déclencher les fonctions de sécurité d'effacement automatique des données de l'appareil (ces dernières restant inactives lorsqu'un clavier physique externe est connecté).

5. Les outils de recherche de personnes et de renseignements (OSINT)

- **Bases de données d'investigation** : Pour identifier la personne qui utilise un téléphone jetable ou un numéro anonyme, les enquêteurs agréés et les officiers de justice ont accès à des bases de données commerciales spécialisées comme **IDI**, **TLOxp** et **LexisNexis**.
- **Services de recherche automatisés** : Des plateformes en ligne gratuites ou payantes comme **Pipl**, **Namechk** et **Lullar** sont

également employées pour retrouver des profils sur les réseaux sociaux et regrouper les données d'utilisateurs à partir d'une adresse courriel ou d'un numéro de téléphone.

✱ **Souhaitez-vous que nous examinions plus en détail les limites concrètes que rencontrent ces outils d'extraction commerciale face aux systèmes de chiffrement d'iOS et d'Android les plus récents ?**

Comment rooter avec KingoRoot ?

Pour rooter un appareil Android avec **KingoRoot**, la procédure est extrêmement simple et se réalise en « un seul clic » :

1. **Installez l'application** KingoRoot sur l'appareil.
2. **Cliquez sur le bouton de rootage** (le bouton « **One Click Root** » visible sur l'interface de l'application à la figure 9-9) pour lancer le processus automatique.

Informations et contexte technique :

- **Gratuité et compatibilité** : KingoRoot est une application tierce gratuite compatible avec la quasi-totalité des téléphones Android (mais pas tous). Les sources rappellent qu'il n'existe pas de solution miracle universelle pour le rootage ; si KingoRoot échoue, il est recommandé d'effectuer une recherche en ligne spécifique au modèle et à la version du système d'exploitation pour trouver d'autres instructions.
- **Objectif forensique** : L'obtention de cet accès root complet est une étape indispensable en criminalistique mobile. Une fois l'appareil rooté et le stockage de masse activé, l'enquêteur peut alors créer une image physique (copie bit-à-bit) de la mémoire de stockage interne et de la carte SD à l'aide d'un outil comme **FTK Imager** pour y rechercher des données (comme les photos du dossier DCIM ou la base de données SMS mmssms.db).

 Je peux vous aider à concevoir un aide-mémoire complet sous forme de guide étape par étape reprenant toutes les méthodes d'extraction de données sur Android et iOS abordées dans vos documents.

Comment utiliser iPhone Backup Browser sur Windows ?

Pour utiliser **iPhone Backup Browser** sur Windows et analyser le système de fichiers d'un appareil iOS, vous devez respecter plusieurs exigences techniques et recommandations de configuration :

- **Prérequis logiciels d'installation** : Pour que l'application s'installe et fonctionne correctement, votre système Windows doit disposer de **Microsoft .NET Framework 4** et de **Visual C++ 2010**.
- **Système d'exploitation recommandé** : Les sources recommandent d'exécuter ce logiciel sur un poste de travail équipé de **Windows 7** afin d'obtenir des performances optimales.
- **Emplacement de la sauvegarde** : C'est la condition la plus critique pour le fonctionnement de l'outil. **iPhone Backup Browser exige que la sauvegarde iOS se trouve à son emplacement par défaut** sur votre disque dur. Si la sauvegarde a été déplacée ou enregistrée dans un répertoire personnalisé, le logiciel risque de ne pas fonctionner.
- **Téléchargement** : Ce logiciel gratuit est disponible à l'adresse suivante : <http://code.google.com/p/iphonebackupbrowser/>.

Une fois lancé et connecté à votre dossier de sauvegarde par défaut, cet outil vous permettra de naviguer dans l'arborescence pour extraire des fichiers clés, comme la base de données de messages **sms.db** ou le dossier des **instantanés d'écran (snapshots)**.

 Nous pouvons également comparer les fonctionnalités de cet outil Windows avec celles d'**iPhone Backup Extractor** (qui fonctionne exclusivement sur macOS) si vous souhaitez évaluer l'outil le plus adapté à votre environnement d'analyse.

Comment FTK Imager analyse le dossier DCIM ?

FTK Imager ne réalise pas d'analyse automatisée complexe par lui-même, mais il sert d'outil pour acquérir et visualiser le contenu brut du stockage d'un appareil Android.

Voici comment se déroule l'accès et l'examen du dossier **DCIM** avec cet outil :

1. **La création de l'image physique** : Après avoir connecté l'appareil Android (qui doit être rooté et configuré avec le stockage de masse USB activé), l'enquêteur lance FTK Imager et sélectionne l'option « Créer une image disque ». Il choisit « Disque physique » et sélectionne le périphérique de stockage de masse USB correspondant à l'appareil. Cette opération de copie physique bit-à-bit doit être répétée pour la carte SD et le disque de stockage interne du téléphone.
2. **La visualisation de l'image créée** : Une fois la copie conforme (image disque) générée, l'enquêteur utilise FTK Imager pour charger cette image et visualiser directement l'intégralité de son contenu.
3. **L'accès au dossier DCIM** : Si le système de fichiers de l'appareil Android n'est pas chiffré, l'enquêteur peut facilement parcourir l'arborescence des dossiers à l'écran. Il lui suffit alors de naviguer jusqu'à l'emplacement de stockage par défaut des photos, qui se trouve généralement dans le répertoire **Téléphone/DCIM**, pour inspecter, visualiser et exporter les images.

 Je peux vous aider à rédiger un rapport d'analyse comparatif détaillant les avantages et les limites de l'acquisition physique (via FTK Imager) par rapport à l'acquisition logique (via les sauvegardes iTunes ou iCloud) pour vos dossiers d'enquête.

Comment contourner l'écran de verrouillage avec un pouce ?

Contourner l'écran de verrouillage avec un pouce consiste à exploiter la technologie de reconnaissance biométrique de l'appareil (comme Touch ID).

Voici comment se présente cette pratique, ses limites juridiques et les moyens de s'en protéger :

1. La contrainte physique pour le déverrouillage

- **Utilisation de l'empreinte** : Dans certaines situations d'enquête, les forces de l'ordre ont contraint des suspects à poser leur pouce sur l'appareil mobile verrouillé dans l'espoir d'activer le lecteur d'empreintes et d'accéder instantanément aux données.
- **Parallèle avec la reconnaissance faciale** : Une inquiétude similaire existe concernant l'identification faciale. Un agent pourrait tenter de déverrouiller de force le téléphone d'une personne interpellée et menottée en le présentant simplement devant son visage.

2. Le cadre légal et les risques d'abus

- **Légalité incertaine** : Ce type de comportement peut être **illégal** selon le pays ou la juridiction où se déroule l'enquête. La facilité d'utilisation de ces technologies biométriques peut ainsi donner lieu à des dérives ou à des abus sur le terrain.

3. Comment empêcher ce contournement ?

- **Désactivation de la biométrie** : Il est conseillé d'éviter d'activer ces fonctionnalités (reconnaissance d'empreintes ou faciale) si l'on craint d'être contraint de déverrouiller son téléphone.
- **Authentification multi-facteurs (MFA)** : Activer l'authentification multi-facteurs permet de masquer ou de protéger son mot de passe principal par crainte d'auto-incrimination.
- **Mots de passe complexes** : Obliger l'appareil à exiger un code PIN ou un mot de passe alphanumérique complexe (au lieu d'un simple balayage ou d'une empreinte) complique considérablement la tâche des enquêteurs, car ces codes sont impossibles à deviner et ne peuvent pas être obtenus par une simple contrainte physique passive.

🔒 Je peux vous préparer un rapport détaillé sur les aspects légaux et les techniques de protection contre le déverrouillage forcé (biométrie vs codes complexes) pour vos dossiers d'investigation.

Comment protéger ses données biométriques ?

Pour protéger vos données contre un déverrouillage forcé ou abusif utilisant la biométrie (comme la reconnaissance d'empreintes digitales ou faciale), les sources suggèrent d'adopter les pratiques suivantes :

- **Éviter d'utiliser les fonctionnalités biométriques** : Si vous craignez d'être contraint physiquement par des tiers ou par les forces de l'ordre à déverrouiller votre appareil — par exemple, en vous forçant à poser votre pouce sur le lecteur d'empreintes ou en présentant l'appareil devant votre visage pour la reconnaissance faciale —, il est vivement conseillé d'**éviter d'activer ces options de déverrouillage**.
- **Activer l'authentification multi-facteurs (MFA)** : Si vous avez peur que votre code d'accès classique puisse être compromis ou que l'on tente d'accéder agressivement à vos données, configurer une authentification multi-facteurs permet de **masquer votre mot de passe principal** par crainte d'auto-incrimination. *(Veuillez noter que cela ne constitue pas un avis juridique).*
- **Utiliser des codes d'accès complexes** : Les systèmes d'exploitation modernes (iOS et Android) incitent par défaut à configurer des **codes d'accès alphanumériques complexes**. Contrairement aux codes numériques simples ou aux gestes de balayage, ces mots de passe complexes sont pratiquement impossibles à deviner pour un tiers et compliquent considérablement le travail des enquêteurs cherchant à contourner la sécurité de l'appareil.

🔒 Je peux comparer l'architecture de sécurité d'iOS avec celle d'Android pour analyser comment leurs enclaves matérielles respectives protègent le stockage de ces clés biométriques.