MAJ 15/01/2025

Formation « Forensic Mobile : Analyse des Smartphones iOS et Android»

Réf : FORMOB

Cette formation de 3 jours, offre une immersion complète dans l'univers du forensic mobile. Les participants découvriront les techniques d'acquisition et d'analyse des données sur smartphones iOS et Android.

Objectifs

Cette formation vise à :

- **Maîtriser les techniques d'acquisition de données sur smartphones, incluant les approches matérielles et logicielles.**
- **Comprendre les systèmes de fichiers et exploiter leurs contenus (plist, bplist, XML, ABX).**
- **Traiter et analyser les données extraites, comme les bases SQLite, les logs système, et les fichiers multimédia.**
- **Concevoir des scripts Python pour automatiser l'analyse et le post-traitement des données (Triage APP iOS, parsing APP).**
- **Étudier des applications spécifiques (Snapchat, Winamax, ...) et extraire des artefacts intéressants.**
- **Analyser les métadonnées des fichiers.**

Durée & horaires

- **3 jours soit 21 heures**
- **Horaires : de 9h30 à 12h et de 13h30 à 18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

Cette formation s'adresse aux professionnels du domaine de l'investigation numérique souhaitant se spécialiser dans le forensic mobile.

- **Les enquêteurs numériques.**
- **Les analystes forensic.**

Pré-requis

- **Aucune compétence préalable n'est requise, mais une expérience en investigation numérique ou des notions de programmation (Python) seront un atout.**

Méthode pédagogique

- **Alternance d'apports théoriques et pratiques.**
- **Ateliers d'analyse de bases de données SQLite.**
- **Conception de scripts Python pour automatiser l'extraction et le parsing des données.**

Supports

- **Supports pédagogiques (documentations, exemples de scripts).**
- **Acquisition du contenu « DUMP » d'un téléphone (iOS et Android).**
- **Ordinateur portable prêté pour la réalisation des exercices**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyée avant le début de la formation**

- **Un exercice pratique final permettra aux participants de valider la bonne connaissance des points abordé tout au long de la formation.**
  Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **Cette formation n'est pas encore certifiante.**

Programme

Jour 1 : Introduction au Forensic Mobile

- Introduction aux technologies des smartphones et à leur évolution matérielle et logicielle.
- Compréhension des systèmes de fichiers et des formats de données clés (SQLite, plist, protobufs, ...).
- Introduction des structures matérielles (NOR/NAND, cartes SD, chiffrement).
- Techniques d'acquisition existante et leurs limitations.
- Introduction à SQLite.

Jour 2 : Forensic Android

- Évolution des versions Android, impact du chiffrement (FDE/FBE) sur les données.
- Étude des répertoires du file system Android.
- Reverse d'APK : recherche de clés de chiffrement, déchiffrement de mot de passe.
- Analyse de bases de données natives : contacts, logs, SMS/MMS, Google, multimédia.
- Post traitement d'application via script Python.

Jour 3 : Forensic iOS

- Évolution d'iOS et impact des changements entre iOS 5 et iOS 18 sur l'acquisition des données.
- Méthodologies d'acquisition numérique (solutions gratuites et commerciales).
- Analyse des fichiers système iOS (MobileBackup, logs, fichiers utilisateur plist).
- Extraction et analyse des bases de données natives iOS (contacts, SMS/MMS, multimédia).
- Post traitement d'application d'un dump via script Python.