FORENSIC : Investigation Numérique Mobile et Analyse des Données iOS et Android

Lien : https://innov-systems.com/formation/forensic-investigation-numerique-mobile-et-analyse-des-donnees-ios-et-android

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC290**	**Sécurité Mobile**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Acquérir une compréhension approfondie des techniques modernes d’investigation mobile sur Android et iOS
- Maîtriser les méthodes d’acquisition, de préservation et d’analyse des données numériques mobiles, y compris les environnements chiffrés
- Identifier, extraire et interpréter les artefacts numériques issus d’applications courantes et systèmes mobiles
- Automatiser les tâches répétitives d’analyse et de corrélation via des scripts Python adaptés au forensic mobile
- Établir une méthodologie de reporting et de documentation rigoureuse pour les enquêtes numériques mobiles

POUR QUI ?

- Enquêteurs numériques et experts en criminalistique informatique
- Responsables et analystes en cybersécurité
- Techniciens d’investigation numérique en charge des dispositifs mobiles
- Agents de conformité et d’investigation au sein d’organismes publics ou privés

Programme détaillé

1 / INTRODUCTION À L'INVESTIGATION MOBILE

- Panorama des systèmes mobiles : architecture Android et iOS
- Évolution matérielle et logicielle des smartphones
- Cadre légal et chaîne de conservation des preuves numériques
- Concepts clés : intégrité, traçabilité, reproductibilité

2 / STRUCTURES DE DONNÉES ET FORMATS SPÉCIFIQUES

- Systèmes de fichiers (EXT4, APFS, HFS+)
- Formats de données : SQLite, plist, protobufs, XML, JSON
- Lecture et interprétation des métadonnées

3 / TECHNIQUES D'ACQUISITION DES DONNÉES

- Méthodes logiques, physiques et avancées (chip-off, JTAG)
- Outils open source et commerciaux : atouts et limites
- Bonnes pratiques de préservation et documentation des preuves

4 / ENVIRONNEMENT ET SÉCURITÉ ANDROID

- Architecture Android et versions majeures (5 à 15)
- Gestion des permissions et modèles de chiffrement (FDE, FBE)
- Récupération des clés et analyse des schémas de sécurité

5 / EXTRACTION ET ANALYSE DES DONNÉES UTILISATEUR

- Exploration du système de fichiers Android
- Analyse des artefacts : journaux, contacts, SMS/MMS, appels, localisation
- Étude des traces d'activités Google (Play Services, compte utilisateur)

6 / ANALYSE D'APPLICATIONS ANDROID

- Reverse engineering d'APK : exploration du code, recherche d'informations sensibles
- Extraction et interprétation de bases SQLite et journaux internes
- Étude de cas : messageries, réseaux sociaux, applications bancaires

7 / ENVIRONNEMENT ET ÉVOLUTION D'IOS

- Évolution d'iOS 10 à 18 : impacts sur les méthodes d'acquisition
- Gestion du chiffrement et du Secure Enclave
- Présentation des solutions d'extraction gratuites et professionnelles

8 / STRUCTURES ET DONNÉES SYSTÈME IOS

- Organisation du système de fichiers iOS (mobile, var, root)
- Analyse des fichiers plist, MobileBackup et journaux systèmes
- Extraction et corrélation des bases natives (contacts, messages, photos, géolocalisation)

9 / ANALYSE D'APPLICATIONS IOS

- Étude d'applications tierces (WhatsApp, Signal, Snapchat, etc.)
- Extraction et parsing des artefacts spécifiques
- Identification des traces de suppression et de synchronisation cloud

10 / AUTOMATISATION DE L'ANALYSE AVEC PYTHON

- Introduction à Python pour le forensic mobile
- Développement de scripts pour le parsing des bases SQLite et plist
- Génération automatisée de rapports de triage et de corrélation

11 / CORRÉLATION MULTI-PLATEFORME

- Comparaison et fusion des données Android/iOS

- Analyse temporelle des événements (timeline et mapping)
- Corrélation avec des artefacts externes (cloud, messagerie, logs réseau)

12 / RÉDACTION ET PRÉSENTATION DU RAPPORT D'INVESTIGATION

- Structuration du rapport forensic : méthodologie, résultats, conclusions
- Bonnes pratiques de présentation des preuves en contexte judiciaire
- Atelier pratique : rédaction d'un rapport d'investigation complet

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 10 Juil. 2026	Présentiel - Casablanca
01 au 04 Sep. 2026	Distanciel
27 au 30 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com